SECURITY OF COMPUTER NETWORKS

Information gathering

Information Gathering is the act of gathering different kinds of information against the targeted victim or system. Information gathering is not just a phase of security testing; it is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing.

Any basic cyber security information gathering process often includes these two types of data collection goals:
1. Collecting network data: Such as public, private and associated domain names, network hosts, public and private IP blocks, routing tables, TCP and UDP running services, SSL certificates, open ports and more.
2. Collecting system-related information: This includes user enumeration, system groups, OS hostnames, OS system type (probably by fingerprinting), system banners (as seen in the banner grabbing blog post), etc.

Recon-ng

- Recon-ng is a framework. It is a very powerful, flexible, and has moving parts similar to the Metasploit framework. Recon-ng is an interactive framework that is not a menu driven UI. Recon-ng uses many different sources to gather data.
- **Installing recon-ng on Kali Linux**
- We are going to install recon-ng on Kali Linux. To install recon-ng and place it in the opt directory, we are going to use git clone by typing in the following command in the terminal window.
- *cd /opt; git clone https://LaNMaSteR53@bitbucket.org/LaNMaSteR53/recon-ng.git*
- *cd /opt/recon-ng*
- *./recon-ng*

Netdiscover

- Net discover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without DHCP server, when you are war driving. It can be also used on hub/switched networks.
- sage: netdiscover [-i device] [-r range | -p] [-s time] [-n node] [-c count] [-f] [-S]

  Ex: `bt ~ # netdiscover -i ath0 -r 192.168.1.0/24`

  `bt ~ # netdiscover -i ath1 –p` (scan common networks)
- -i device: your network device
- -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
- -p passive mode do not send anything, only sniff
- -s time: time to sleep between each arp request (miliseconds)
- -c count: number of times to send each arp reques (for nets with packet loss)
- -n node: last ip octet used for scanning (from 2 to 253)

- -S enable sleep time supression betwen each request (hardcore mode)
- -f enable fast mode scan, saves a lot of time, recommended for auto
- If -p or -r aren't enabled, netdiscover will scan for common lan addresses

Ok so let's look at the flags so that we know what we are dealing with.
"-i" simply put is the network card
"-r" the range to scan that you will insert on the command later
"-p" send no packets out on the network
"-s" time to sleep between the arp requests simply means how long netdiscover should wait.
"-c" count is the number or arp requests to send each time
"-n" node again this is a number you will insert on the command latter.
"-S" this will prevent netdiscover from "sleeping" between arp requests"
"-f" fast as stated above

Nmap

- Nmap is a free, open-source port scanner available for both UNIX and Windows. It has an optional graphical front-end, NmapFE, and supports a wide variety of scan types

Basic Scan Types [-sT, -sS]

- **TCP connect() Scan [-sT]**
- **SYN Stealth Scan [-sS]**
- **FIN, Null and Xmas Tree Scans [-sF, -sN, -sX]**

  Ex: # nmap -sS 127.0.0.1
- **Ping Scan [-sP]**
- **UDP Scan [-sU]**
- **IP Protocol Scans [-sO]**

  Ex: # nmap -sO 127.0.0.1

- **Idle Scanning [-sI]**
- **Version Detection [-sV]**
- **ACK Scan [-sA]**
- **Window Scan, RPC Scan, List Scan [-sW, -sR, -sL]**

DMitry

DMitry - Deepmagic Information Gathering Tool

Syntax

dmitry [Options] host

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line program coded purely in C with the ability to gather as much information as possible about a host.

DMitry has a base functionality with the ability to add new functions. Basic functionality of DMitry allows for information to be gathered about a target host from a simple whois lookup on the target to UpTime reports and TCP portscans.

Options

Options should be passed to DMitry in the form of '-option'. Only options known by DMitry will be used and others will be ignored. If options are not passed as a group block, the trailing options will be considered a host target.

- **-o filename** Create an ascii text output of the results to the "filename" specified. If no output filename is specified then output will be saved to "target.txt". If this option is not specified in any form output will be sent to the standard output (STDOUT) by default. This option MUST trail all other options, i.e. "./dmitry -winseo target".
- **-i** Perform an Internet Number whois lookup on the target. This requires that the target be in the form of a 4 part Internet Number with each octal seperated using the '.' notation. For example, "./dmitry -i 255.255.255.255".

- **-w** Perform a whois lookup on the 'host' target. This requires that the target be in a named character format. For example, "./dmitry -w target" will perform a standard named whois lookup
- **-n** Retrieve netcraft.com data concerning the host, this includes Operating System, Web Server release and UpTime information where available.
- **-s** Perform a Sub Domain search on the specified target. This will use serveral search engines to attempt to locate sub-domains in the form of sub.target. There is no set limit to the level of sub-domain that can be located, however, there is a maximum string length of 40 characters (NCOL 40) to limit memory usage. Possible sub domains are then reversed to an IP address, if this comes back positive then the resulting sub domain is listed. However, if the host uses an asterisk in their DNS records all resolve sub domains will come back positive.

- **-e** Perform an Email Address search on the specified target. This modules works using the same concept as the Sub Domain search by attempting to locate possible e-mail addresses for a target host. The e-mail addresses may also be for possible sub-domains of the target host. There is a limit to the length of the e-mail address set to 50 characters (NCOL 50) to limit memory usage
- **-p** Perform a TCP Portscan on the host target. This is a pretty basic module at the moment, and we do advise users to use something like nmap (www.insecure.org/nmap/) instead. This module will list open, closed and filtered ports within a specific range. There will probably be little advancement upon this module, though there will be some alterations to make it a little more user friendly. There are also other options for this module that can affect the scan and its relative output.
- Ex: **dmitry -w example-host.com**

```
dmitry -winsepo sometextfile.txt example-host.com
dmitry -winsepfbo 127.0.0.1
```

- **-f** This option will cause the TCP Portscan module to report/display output of filtered ports. These are usually ports that have been filtered and/or closed by a firewall at the specified host/target. This option requires that the '-p' option be passed as a previous option. For example, "./dmitry -pf target“.
- **-b** This option will cause the TCP Portscan module to output Banners if they are received when scanning TCP Ports. This option requres that the '-p' option be passed as a previous option. For example, "./dmitry -pb target".
- **-t** This sets the Time To Live (TTL) of the Portscan module when scanning individual ports. This is set to 2 seconds by default. This is usually required when scanning a host that has a firewall and/or has filtered ports which can slow a scan down.

Sniffing

- Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic.
- Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.
- 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.

There are two types:

Active Sniffing:

1. Active sniffing is used to sniff a switch-based network.
2. 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.

Passive Sniffing:

1. Passive sniffing means sniffing through a hub, on a hub the traffic is sent to all ports.
2. It involves only monitoring of the packets sent by others without sending any additional data packets in the network traffic.
3. 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.
4. Hub usage is out-dated today. Most modern networks use switches.

How a Sniffer Works

- **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.

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.

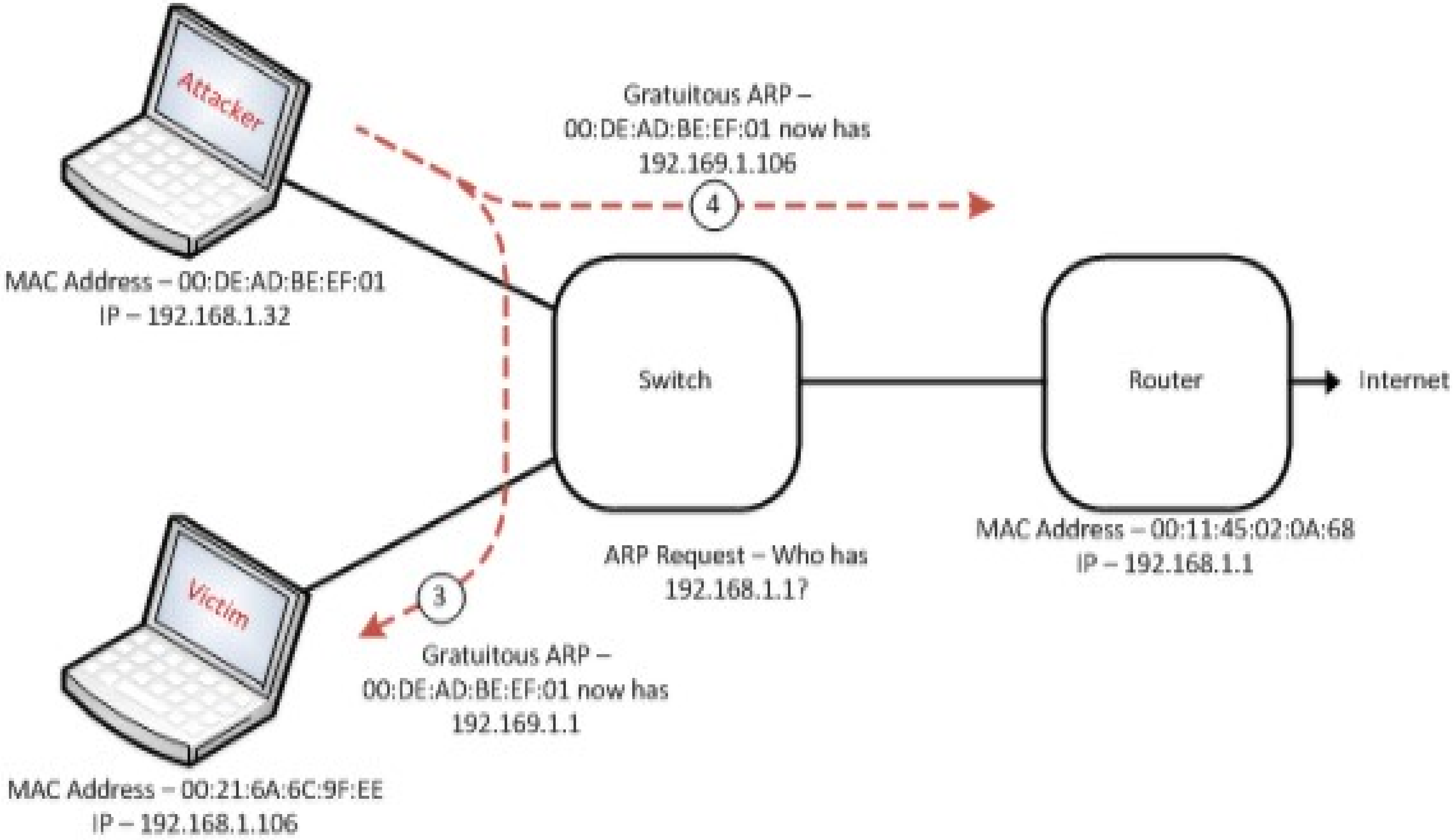
Protocols vulnerable to sniffing

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

Active Sniffing Attacks

Mac-Attacks:

- MAC-flooding is an attack where the CAM table is flooded with fake MAC-IP pairs, so CAM table overflows causing traffic to flood all ports on switch (i.e) changing switch to behave like a hub
- ARP Spoofing:
- In this case, an attacker can spoof the MAC address of a trusted host and forge ARP request/replies to overload the Switch. Then the switch is set in "forward mode" an attacker can now sniff the packets on the traffic.
- ARP Poisoning:
- Attacker chooses targets and floods their ARP cache with forged entries thus replacing the MAC address of targets with MAC address of attacker. ARP poisoning is used in Man in the middle attack.
-


Attacker
Gratuitous ARP –
00:DE:AD:BE:EF:01 now has
192.169.1.106
4
MAC Address – 00:DE:AD:BE:EF:01
IP – 192.168.1.32
Switch
Router
Internet
MAC Address – 00:11:45:02:0A:68
IP – 192.168.1.1
ARP Request – Who has
192.168.1.1?
3
Victim
Gratuitous ARP –
00:DE:AD:BE:EF:01 now has
192.169.1.1
MAC Address – 00:21:6A:6C:9F:EE
IP – 192.168.1.106

Attacks

1. **MAC Attacks**
2. **DHCP Attacks**
3. **ARP Poisoning**
4. **Spoofing Attack**
5. **DNS Poisoning**
6. **Sniffing Tools**

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.

Sniffing Detection Techniques

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.

- 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: 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.

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.

Eavesdropping

- An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smart phone, or another connected device. The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.
- There are two types of eavesdropping attacks; passive eavesdropping and active eavesdropping.
- With passive eavesdropping, the hacker simply “listens” to data that is passing through the network. With active eavesdropping, hackers disguise themselves. This allows them to impersonate a website where users would normally share their private data.
- To prevent being the victim of eavesdropping attacks, make sure that you’re using data encryption in transit.

The different scenarios that attackers leverage on for a malicious Eavesdropping attack.

- **Weak Passwords:** by choosing weak passwords, that can be compromised easily, you are leaving the door to a confidential communication channel wide open. Once the attacker possesses your password, he can easily join the network on which valuable business information is being exchanged.
- **Working remotely:** employees working in the office premises conform to the security standards and are connected to a secure network. However, remote employees may connect their devices to a weak or insecure network that could be prone to an eavesdropping attack
- **Frail networks:** connecting to open networks that do not even require passwords for access and transmits information without encryption is an ideal set up for an attacker to carry an eavesdropping attack.

What is the impact of the Eavesdropping attack?

- **Loss of privacy:** Every business has confidential information that could lead the organization astray if it becomes public. While eavesdropping, the attackers will absorb vital business information, ideas and conversations being exchanged within the organization, thereby affecting its privacy
- **Identity theft:** Say, two employees are having a conversation about their access to critical applications. One of them says, “my password to application XYZ has been changed from abdcde to 1234” now, the attacker who has been eavesdropping on their conversation has easy access to their credentials; will easily access the application and steal all the important information.
- **Financial loss:** Once the cyber attacker has vital business information, essential database or passwords to vital business applications, it can be used to full advantage by exposing the data or selling it to the competitors; the attackers will earn, and the organization will lose in millions.

How to prevent Eavesdropping attacks?

- **Military-grade encryption:** encryption is a great way to defend an eavesdropping attack. In case an attacker manages to intervene between a communication, he would be successful only if he can read the data that is being exchanged. By using a 256-bit, also known as military-grade encryption, the attacker may gather the data via eavesdropping, but the data will still be safe as it will take him around 500 billion years to decode it.
- **Spread awareness:** training and informing the employees of the organization about cyber security is of utmost importance. An employee, unaware of cybercrimes such as eavesdropping attacks may unknowingly put the organization at risk. So, the employee should have complete knowledge about eavesdropping attacks before he/she downloads an application, software or connects over a weak network.
- **Network segmentation:** it is ideal to split the computer network and allowing only certain teams or key personnel to connect to the network; for instance, the marketing team does not need to access the HR system. Network division or segmenting helps in decongesting the network traffic, improves security and prevents unwanted connectivity.

Spoofing

An attacker alters his identity so that some one thinks he is some one else

- Email, User ID, IP Address, …
- Attacker exploits trust relation between user and networked machines to gain access to machines

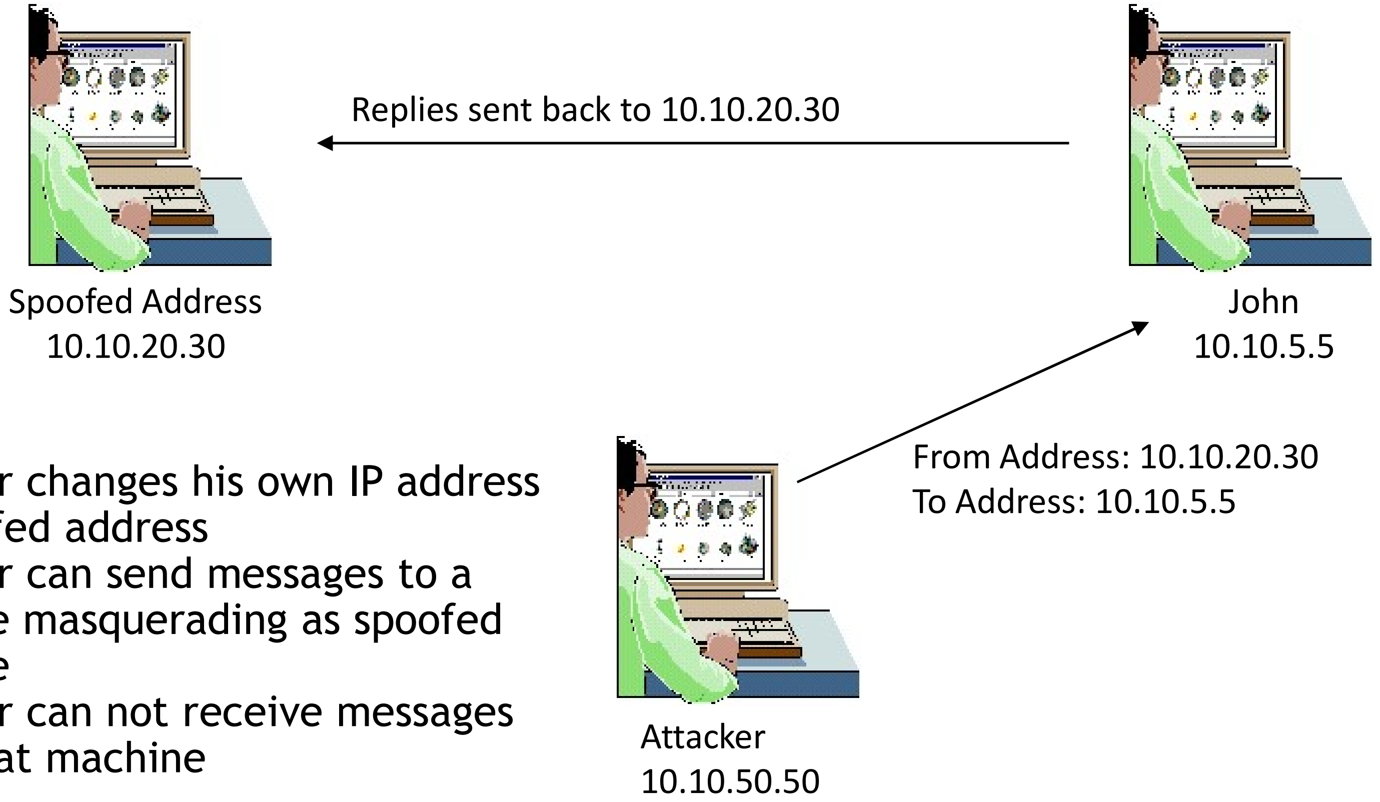
Types of Spoofing:

1. IP Spoofing:
2. Email Spoofing
3. Web Spoofing

IP Spoofing – Flying-Blind Attack

Definition:

Attacker uses IP address of another computer to acquire information or gain access



Replies sent back to 10.10.20.30

Spoofed Address
10.10.20.30

John
10.10.5.5

From Address: 10.10.20.30
To Address: 10.10.5.5

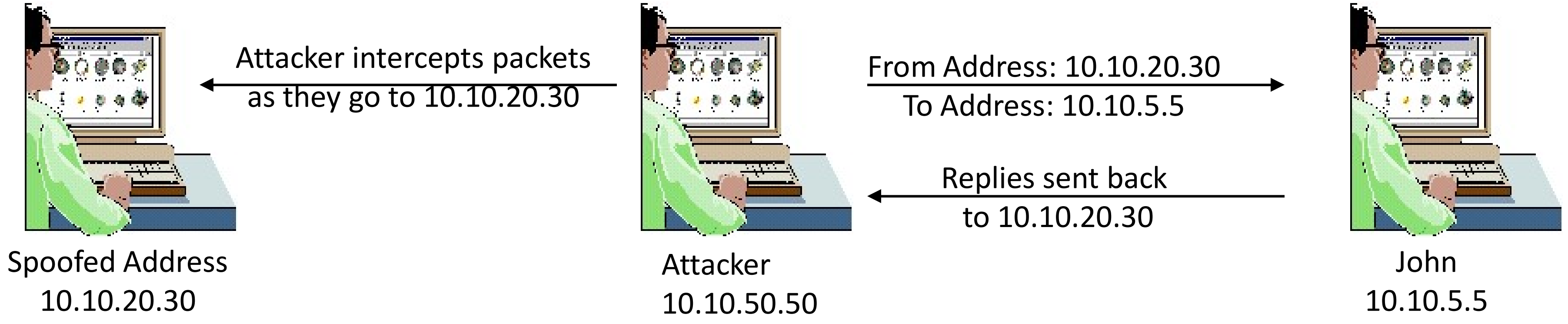
Attacker
10.10.50.50

- Attacker changes his own IP address to spoofed address
- Attacker can send messages to a machine masquerading as spoofed machine
- Attacker can not receive messages from that machine

IP Spoofing – Source Routing

Definition:

Attacker spoofs the address of another machine and inserts itself between the attacked machine and the spoofed machine to intercept replies



Attacker intercepts packets as they go to 10.10.20.30

From Address: 10.10.20.30 To Address: 10.10.5.5

Replies sent back to 10.10.20.30

Spoofed Address 10.10.20.30

Attacker 10.10.50.50

John 10.10.5.5

- The path a packet may change can vary over time
- To ensure that he stays in the loop the attacker uses source routing to ensure that the packet passes through certain nodes on the network

Email Spoofing

Definition:

Attacker sends messages masquerading as some one else

What can be the repercussions?

Types of Email Spoofing:

1. Create an account with similar email address
   - Sanjaygoel@yahoo.com: A message from this account can perplex the students
2. Modify a mail client
   - Attacker can put in any return address he wants to in the mail he sends
3. Telnet to port 25
   - Most mail servers use port 25 for SMTP. Attacker logs on to this port and composes a message for the user.

Web Spoofing

- Basic
  - Attacker registers a web address matching an entity e.g. votebush.com, geproducts.com, gesucks.com
- Man-in-the-Middle Attack
  - Attacker acts as a proxy between the web server and the client
  - Attacker has to compromise the router or a node through which the relevant traffic flows
- URL Rewriting
  - Attacker redirects web traffic to another site that is controlled by the attacker
  - Attacker writes his own web site address before the legitimate link
- Tracking State
  - When a user logs on to a site a persistent authentication is maintained
  - This authentication can be stolen for masquerading as the user

Web Spoofing – Tracking State

- Web Site maintains authentication so that the user does not have to authenticate repeatedly
- Three types of tracking methods are used:

1. Cookies: Line of text with ID on the users cookie file
   - Attacker can read the ID from users cookie file
2. URL Session Tracking: An id is appended to all the links in the website web pages.
   - Attacker can guess or read this id and masquerade as user
3. Hidden Form Elements
   - ID is hidden in form elements which are not visible to user
   - Hacker can modify these to masquerade as another user

Session Hijacking

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 lockout for invalid session IDs.
- Weak session ID generation algorithm or small session IDs.
- Insecure handling of session IDs.
- DNS poisoning, XSS, exploiting a bug in browser
- Indefinite session expiration time.
- Most computers using TCP/IP are vulnerable.
- Most countermeasures do not work unless you use encryption.

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) For example, GET /index.html HTTP/1.0 Host: www.hacksite.com Referrer:

www.webmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75

- 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.

- **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.
- **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).

Types of Session Hijacking

- **Active Attack:** In an active attack, an attacker finds an active session </span> 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.

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.

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

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

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 (side jacking).
- 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.

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.

Counter Measures

- Using secure protocols instead of clear text protocols like HTTP, FTP.Telnet, Rlogin, etc.
- Encrypting session id will increase the complexity of the session id prediction.
- Sending session id over SSL.
- Use long random numbers for session id.
- Implement timeout for the session when the session is logged out, or session id expires.
- Having different session id for each page.
- Use switches rather than hubs.
- Ensure server side and client side protection software.
- Use IDS for detecting ARP spoofing/Poisoning.
- Do not click on suspicious links.
- Check the web application for all errors.
- Using IPSec is a valid defence mechanism.

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.

Man-in-the-Middle Attack

- **A man-in-the-middle attack** is a type of cyber attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.

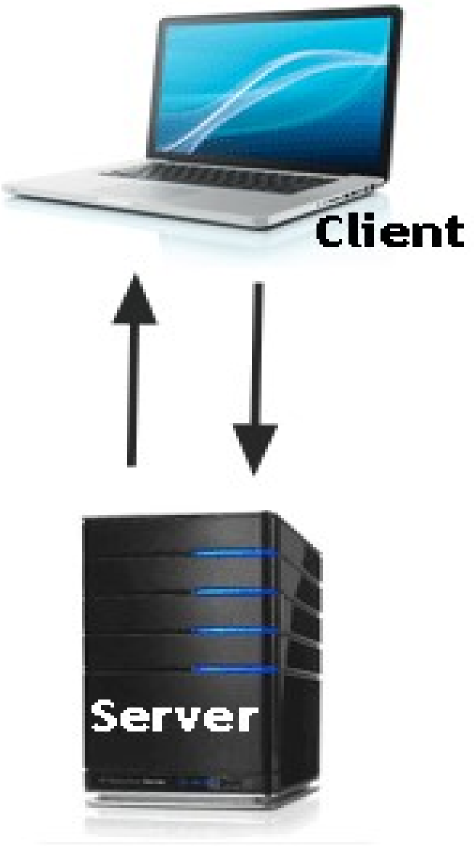
- A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.

- Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.

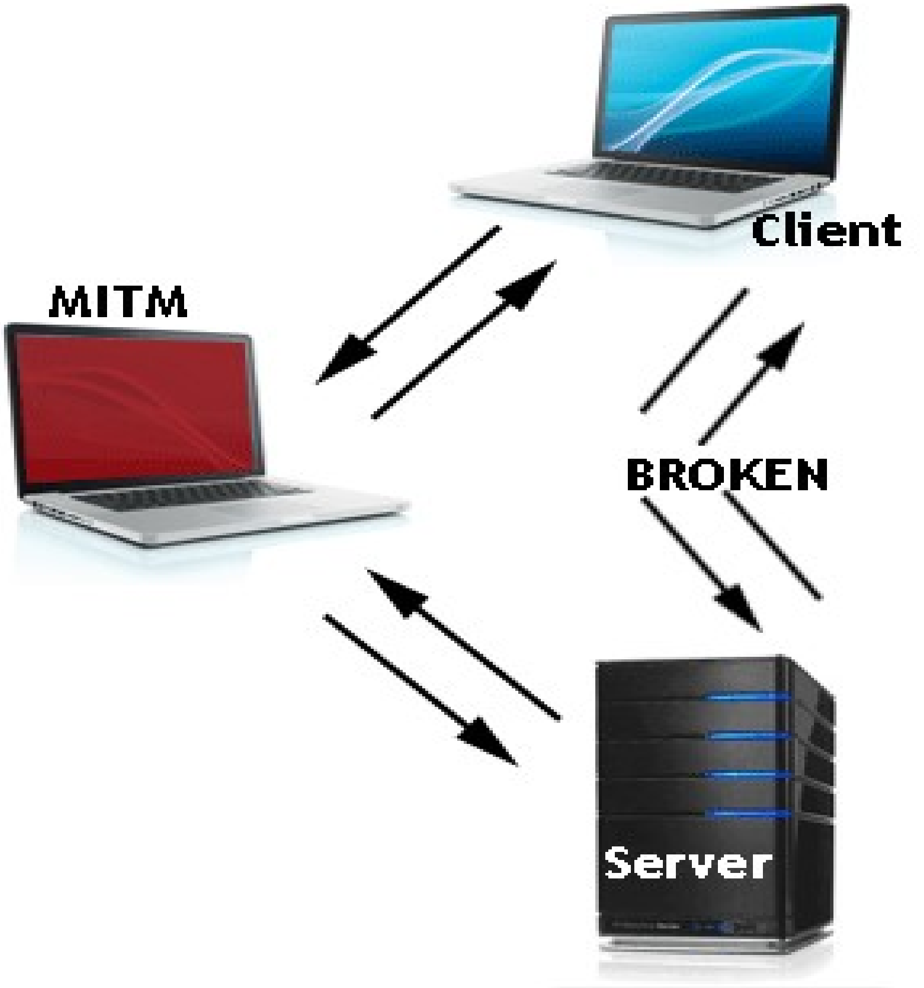
Key Concepts of a Man-in-the-Middle Attack

- Key Concepts of a Man-in-the-Middle Attack
- Man-in-the-middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.
- A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.
- Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.

Normal Flow



Man-in-the-Middle Flow



Interactions Susceptible to MITM Attacks

- Financial sites – between login and authentication
- Connections meant to be secured by public or private keys
- Other sites that require logins – where there is something to be gained by having access
- Man-in-the-middle is a form of session hijacking. Other forms of session hijacking similar to man-in-the-middle are:
- Sidejacking - This attack involves sniffing data packets to steal session cookies and hijack a user’s session. These cookies can contain unencrypted login information, even if the site was secure.
- Evil Twin - This is a rogue Wi-Fi network that appears to be a legitimate network. When users unknowingly join the rogue network, the attacker can launch a man-in-the-middle attack, intercepting all data between you and the network.
- Sniffing - This involves a malicious actor using readily available software to intercept data being sent from, or to, your device.

Man in the middle attack prevention

Blocking MITM attacks requires several practical steps on the part of users, as well as a combination of encryption and verification methods for applications.

For users, this means:

- Avoiding WiFi connections that aren’t password protected.
- Paying attention to browser notifications reporting a website as being unsecured.
- Immediately logging out of a secure application when it’s not in use.
- Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions.

DNS Poisoning

- DNS cache poisoning, also known as DNS spoofing, is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones. One of the reasons DNS poisoning is so dangerous is because it can spread from DNS server to DNS server.

How DNS Cache Poisoning and Spoofing Works

- In regard to DNS, the most prominent threats are two-fold:
- **DNS spoofing** is the resulting threat which mimics legitimate server destinations to redirect a domain's traffic. Unsuspecting victims end up on malicious websites, which is the goal that results from various methods of DNS spoofing attacks.

- **DNS cache poisoning** is a user-end method of DNS spoofing, in which your system logs the fraudulent IP address in your local memory cache. This leads the DNS to recall the bad site specifically for you, even if the issue gets resolved or never existed on the server-end.

Methods for DNS Spoofing or Cache Poisoning Attacks

Among the various methods for DNS spoof attacks, these are some of the more common:

- **Man-in-the-middle duping:** Where an attacker steps between your web browser and the DNS server to infect both. A tool is used for a simultaneous cache poisoning on your local device, and server poisoning on the DNS server. The result is a redirect to a malicious site hosted on the attacker's own local server.
- **DNS server hijack:** The criminal directly reconfigures the server to direct all requesting users to the malicious website. Once a fraudulent DNS entry is injected onto the DNS server, any IP request for the spoofed domain will result in the fake site.
- **DNS cache poisoning via spam:** The code for DNS cache poisoning is often found in URLs sent via spam emails. These emails attempt to frighten users into clicking on the supplied URL, which in turn infects their computer. Banner ads and images — both in emails and untrustworthy websites — can also direct users to this code. Once poisoned, your computer will take you to fake websites that are spoofed to look like the real thing. This is where the true threats are introduced to your devices.

Risks of DNS Poisoning and Spoofing

- DNS spoofing poses several risks, each putting your devices and personal data in harm’s way.
- **Data theft** can be particularly lucrative for DNS spoof attackers. Banking websites and popular online retailers are easily spoofed, meaning any password, credit card or personal information may be compromised. The redirects would be phishing websites designed to collect your info.
- **Malware infection** is yet another common threat with DNS spoofing. With a spoof redirecting you, the destination could end up being a site infested with malicious downloads. Drive by downloads are an easy way to automate the infection of your system. Ultimately if you’re not using internet security, you’re exposed to risks like spyware, key loggers or worms.
- **Halted security updates** can result from a DNS spoof. If spoofed sites include internet security providers, legitimate security updates will not be performed. As a result, your computer may be exposed to additional threats such as viruses or Trojans.

How to Prevent DNS Cache Poisoning and Spoofing

- **DNS spoofing detection tools:** As an equivalent of endpoint user security products, these detection tools proactively scan all data received before sending it out.
- **Domain name system security extensions (DNSSEC):** Essentially a DNS “verified real” label, the DNSSEC system helps keep DNS lookup authentic and spoof-free.
- **End-to-end encryption:** Encrypted data sent for DNS requests and replies keeps criminals out as they won’t be able to duplicate the unique security certificate for the legitimate website.

Prevention Tips for Endpoint Users

Never click on a link you don't recognize. This includes email, text messages, or links in social media. Tools that shorten URLs can further mask link destinations, so avoid those as much as possible. To be especially safe, always opt to manually enter a URL into your address bar. But only do so after you’ve confirmed that it is official and legitimate.

- **Regularly scan your computer for malware.** While you may not be able to detect DNS cache poisoning, your security software will help you uncover and remove any secondary infections. Since spoofed sites can deliver all types of malicious programs, you should always be scanning for viruses, spyware, and other hidden issues. The inverse is also possible, as malware could deliver spoofs. Always do so using a local program rather than a hosted version, since poisoning could spoof web-based results.
- **Flush your DNS cache to solve poisoning if necessary.** Cache poisoning stays within your system for the long-term unless you clean out the infected data. This process can be as simple as opening the Windows “Run” program and typing “ *ipconfig /flushdns*” as your command. Mac, iOS, and Android also have flush options. These are usually found in a “network settings reset” option, toggling airplane mode, via device reboot, or in a specific native web browser URL. Look up your specific device’s method for guidance.
- **Use a virtual private network (VPN).** These services give you an encrypted tunnel for all your web traffic and use of private DNS servers that exclusively use end-to-end encrypted requests. The result gives you servers that are far more resilient against DNS spoofing, and requests that can’t be interrupted.

Address Resolution Protocol (ARP) Poisoning

- ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.
- The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa, so his or her target's MAC is now associated with the attacker's IP address).
- Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination. Because ARP Poisoning attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. Besides Man-in-the-Middle Attacks, ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets.

How ARP works

- 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 MAC address.
- If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.

ARP Poisoning Countermeasures

- **Static ARP entries**: these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.
- **ARP poisoning detection software**: these systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC address resolutions can then be blocked.
- **Operating System Security**: this measure is dependent on the operating system been used. The following are the basic techniques used by various operating systems.

  Linux based: these work by ignoring unsolicited ARP reply packets.

  Microsoft Windows: the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;

    AntiARP– provides protection against both passive and active sniffing

    Agnitum Outpost Firewall–provides protection against passive sniffing

    XArp– provides protection against both passive and active sniffing

  Mac OS: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

DDOS Concepts

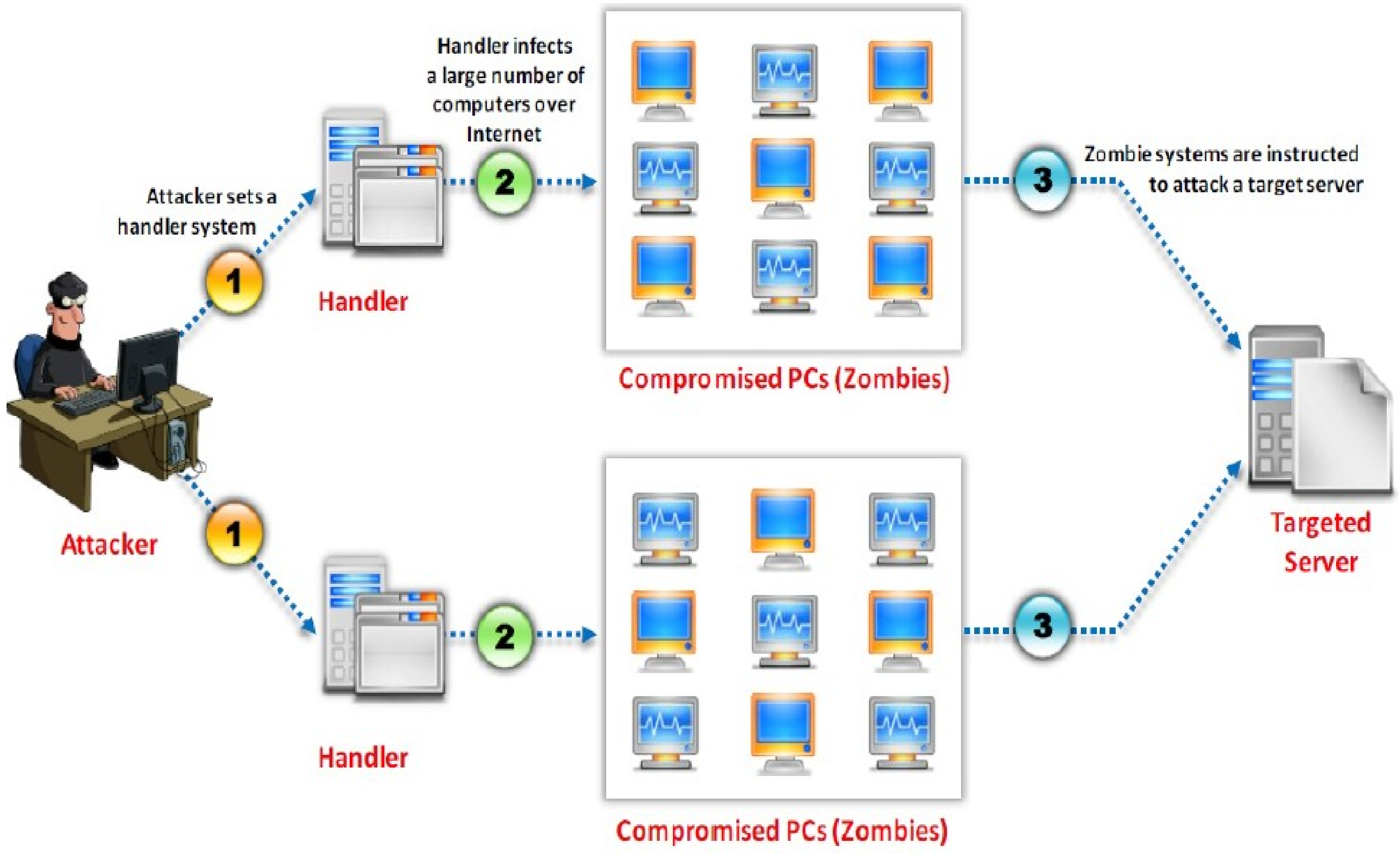
What is a Denial-of-Service Attack?

- 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


Handler infects a large number of computers over Internet
Attacker sets a handler system
1
2
3
Zombie systems are instructed to attack a target server
Handler
Compromised PCs (Zombies)
Attacker
1
2
3
Targeted Server
Handler
Compromised PCs (Zombies)

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.

DoS/DDoS Attack Tools

- **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

- **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 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.

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

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

Denial-of-Service (DoS) Attack PenetrationTesting

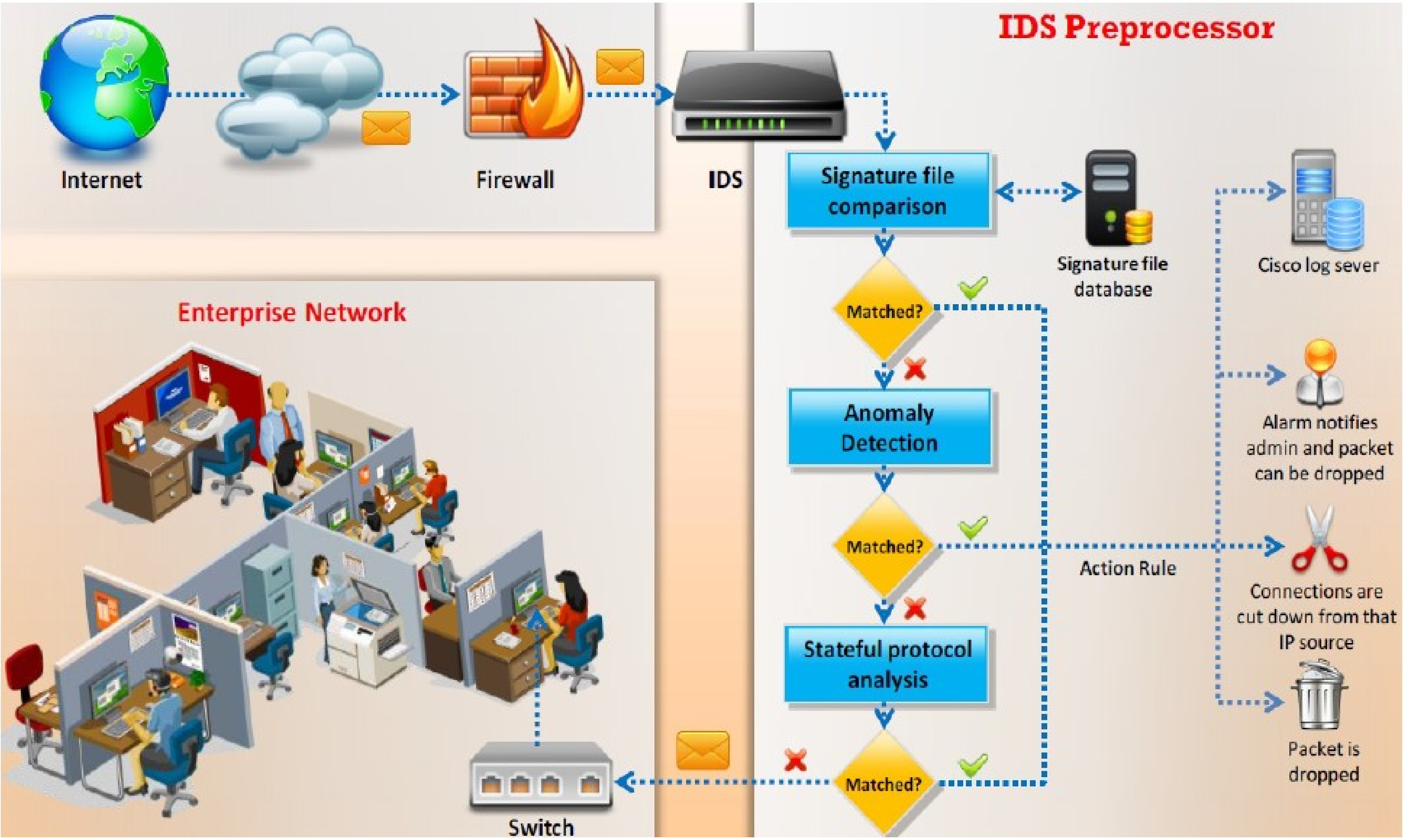
- DoS attack should be incorporated into Pen testing plans to find out if the network
- server is susceptible to DoS attacks.
- DoS Pen Testing determines minimum thresholds for DoS attacks on a system, but the tester cannot ensure that the system is resistant to DoS attacks.
- The pen tester floods 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.

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 knwon as misuses detection. Signature recognition tries to identify events that indicate misuse of a system resource.

- **Anomaly Detection:** It detects the intrusion based on the fixed behavioral characteristics of the users and components in a computer system.

- **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

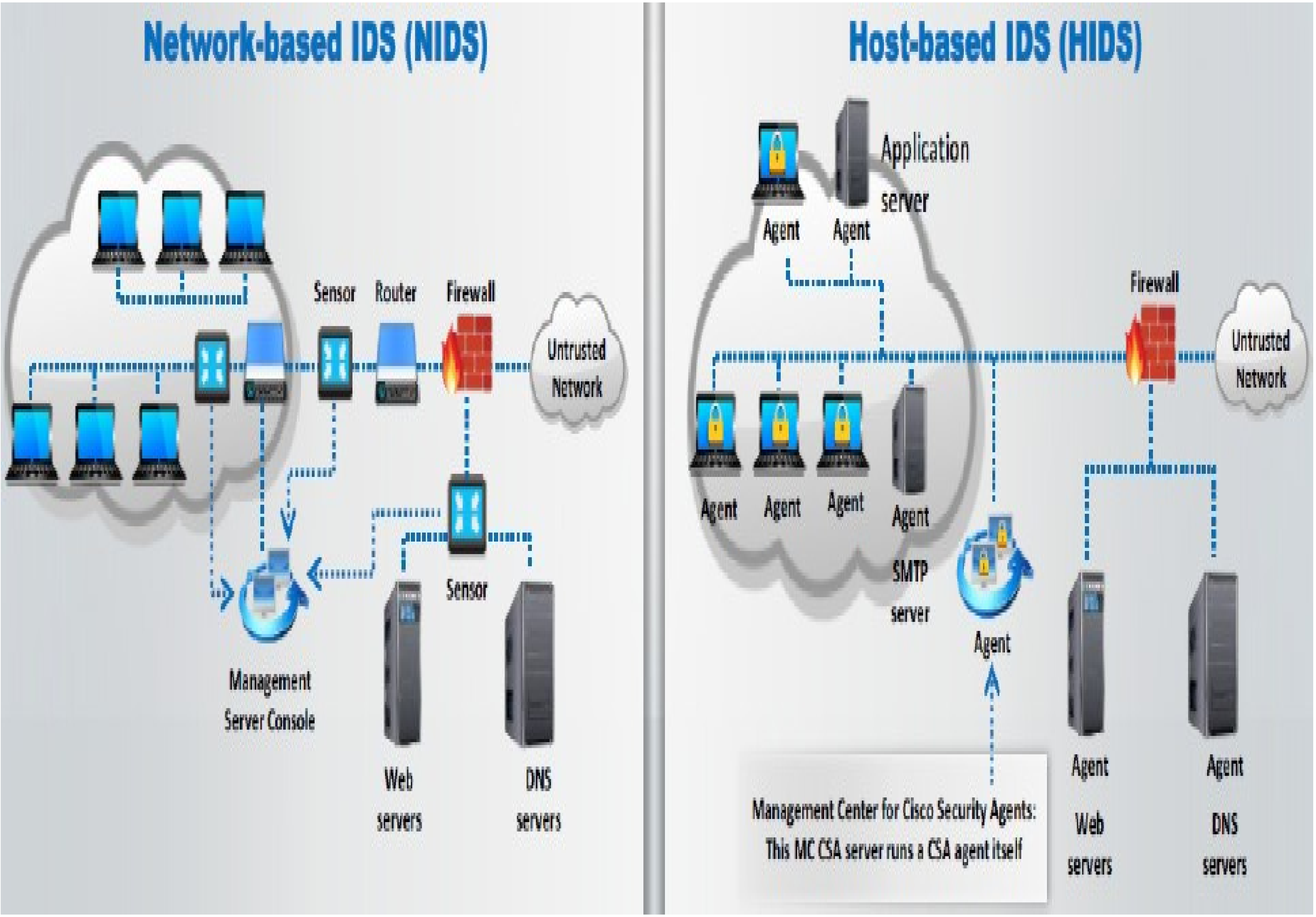
Types of Intrusion Detection Systems

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.

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.



Network-based IDS (NIDS)

Host-based IDS (HIDS)

Management Center for Cisco Security Agents: This MC CSA server runs a CSA agent itself

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.

Intrusion Detection Tool: Snort

- Snort is an open source network intrusion detection system, capable of performing realtime 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

Evading IDS

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

- 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.

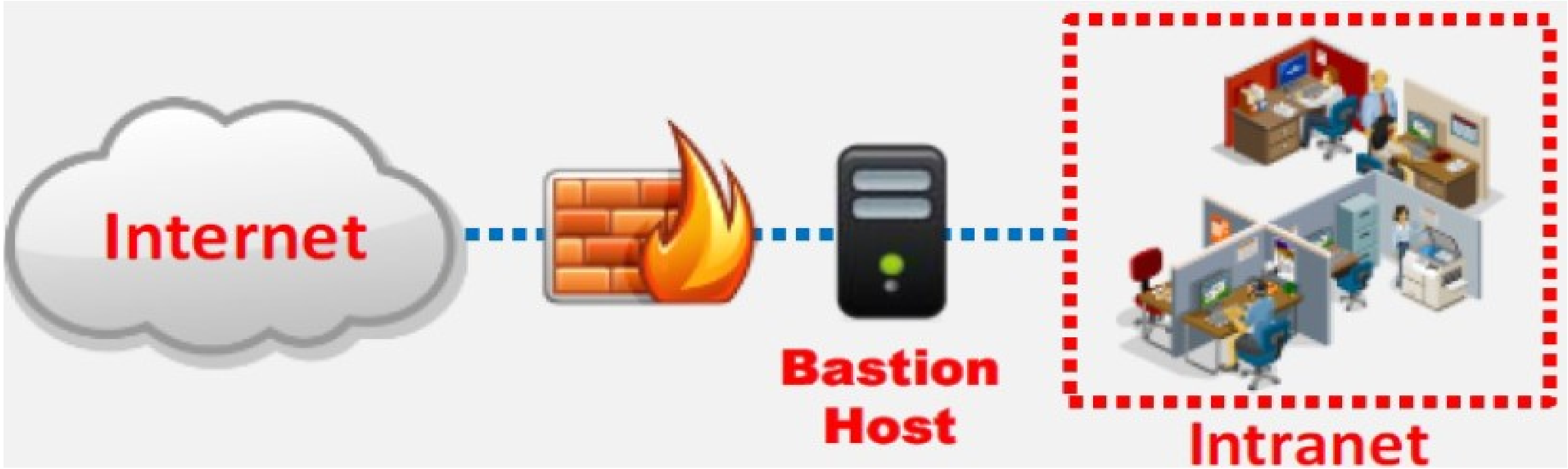
Firewall Architecture

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:

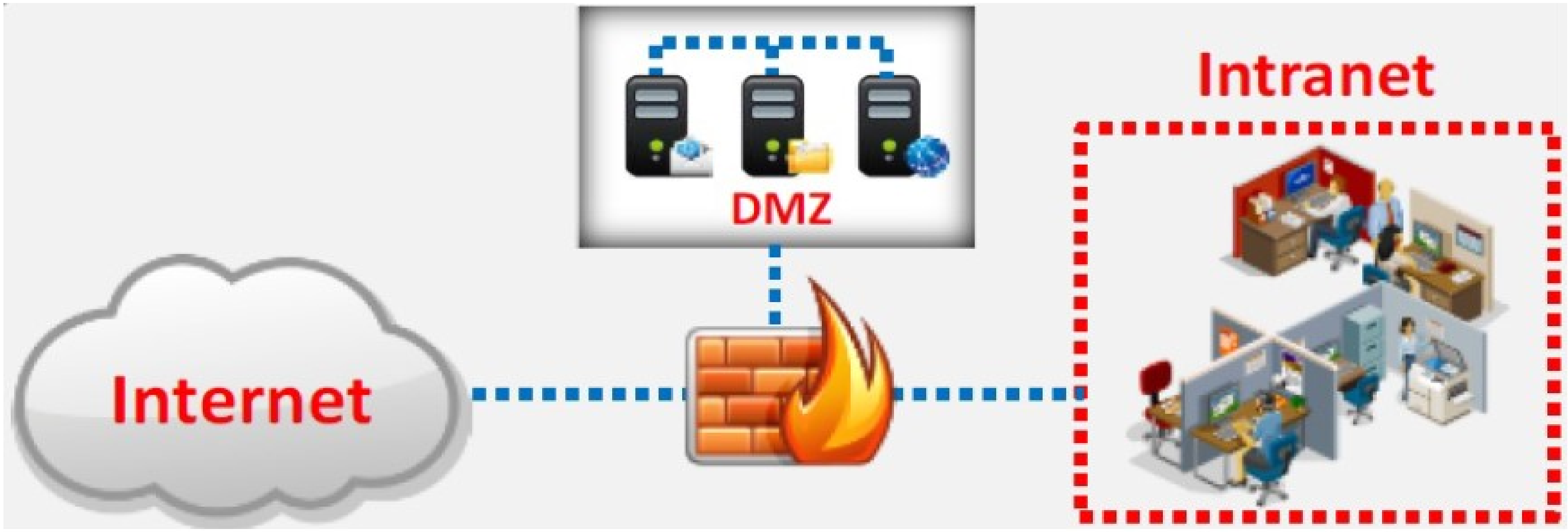
  public interface directly connected to the Internet.

  private interface connected to the Intranet.



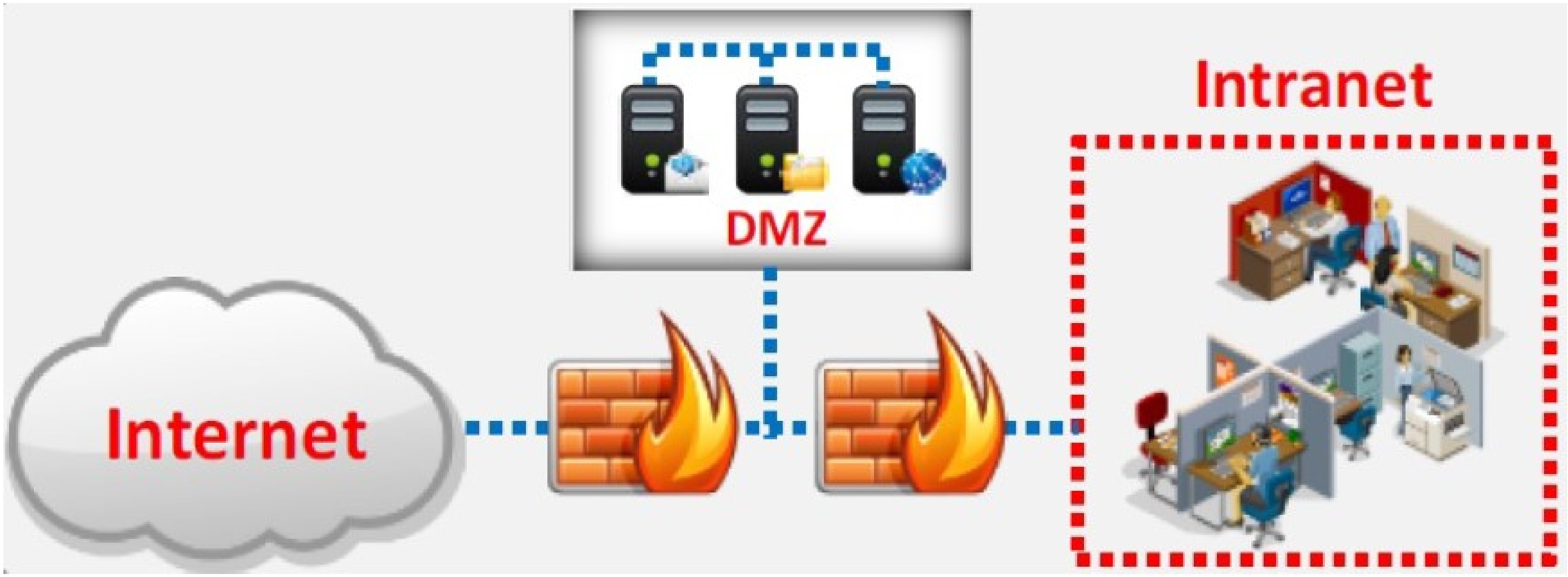
Screened Subnet

- 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.



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.



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

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.