UNIT I

HACKING Essential Terminology: Information Security, Cyber Security, Threat, Vulnerability, Exploit. Hackers Motives and Objectives, Penetration Testing and Hacker classes.

Hacking Phases: Footprinting Methodology , Network Scanning and Enumeration

HACKING

Essential Terminology

Information Security

- Information security, sometimes abbreviated to infosec, is a set of practices intended to keep data secure from unauthorized access or alterations, or both.

- When it's being stored and when it's being transmitted from one machine or physical location to another. You might sometimes see it referred to as data security.

Definition:

- Information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

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. To ensure confidentiality one needs to use all the techniques designed for security like strong password, encryption, authentication and defense against penetration attacks.

- **Integrity:** The trustworthiness of data or resources in terms of preventing improper and unauthorized changes.

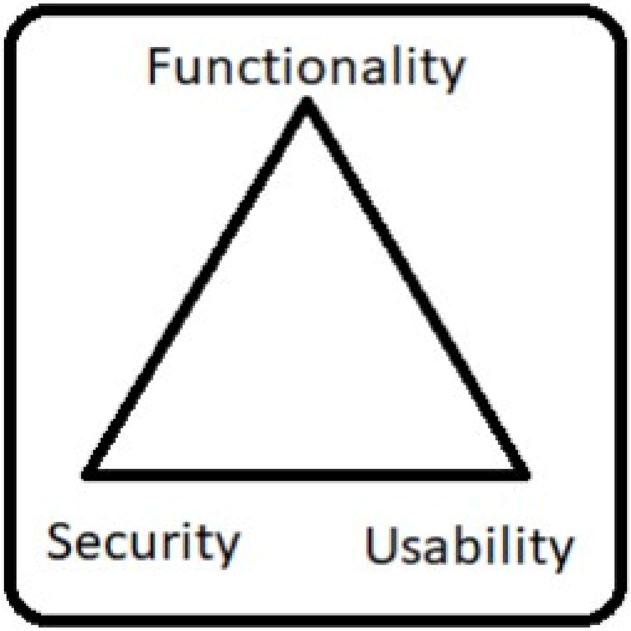
- **Availability:** Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users. Availability in information security means matching network and computing resources to compute data access and implement a better policy for disaster recovery purposes.

- **Authenticity:** Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine
- **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.

The Security, Functionality, and Usability Triangle

Any information system can be defined by the strength of three components:

- Functionality (Features)
- Security (Restrictions)
- Usability (GUI)



Information Security Threats and Attack Vectors

Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

- 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.

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.

Viruses and Worms: Viruses and worms are the most prevalent networking threat that are capable of infecting a network within seconds.

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.

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

Host Threats:

- Malware attacks
- Foot printing
- Password attacks
- Denial-of-Service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Backdoor attacks
- Physical security threats

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

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.

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.

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.

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

Cyber security

- **Cyber security** is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It's also known as information technology **security** or electronic information **security**.

- Information security and cyber security may be used substitutable but are two different things. Cyber security is a practice used to provide security from online attacks, while information security is a specific discipline that falls under cyber security. Information security is focusing on network and App code.

- Strictly speaking, cyber security is the broader practice of defending IT assets from attack, and information security is a specific discipline under the cyber security umbrella

Vulnerability

- A **vulnerability** is a weakness in design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database.

- An exploitable vulnerability is one for which at least one working attack or "exploit" exists. Vulnerabilities are often hunted or exploited with the aid of automated tools or manually using customized scripts.

Threat

The definition of a threat is a statement of an intent to harm or punish, or a something that presents an imminent danger or harm.

Threats can be classified according to their type, and origin:

Types of **threats**:

Physical damage: fire, water, pollution.

Natural events: climatic, seismic, volcanic

Exploit

Exploit: Exploit is defined as to use someone or something to achieve one's own purposes.

There are several methods of classifying exploits. The most common is by how the exploit communicates to the vulnerable software.

- A *remote exploit* works over a network and exploits the security vulnerability without any prior access to the vulnerable system.
- A *local exploit* requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.

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.

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

Hacking Phases

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Hacking Phases: Reconnaissance

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
- 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.

Penetration testing

- Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually.

Types of Penetration Testing

- **Black-box: No prior knowledge of the infrastructure to be tested:**
- Blind Testing
- Double Blind Testing
- **White-box:** Complete knowledge of the infrastructure that needs to be tested.
- **Grey-box:** Limited knowledge of the infrastructure that needs to be tested.

Phases of Penetration Testing

Pre-Attack Phase:

- Planning and preparation
- Methodology designing => 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

Hacking Phases

Footprinting Methodology

- 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.

Footprinting Methodology

- Footprinting through Search Engines
- Footprinting Using Advanced Google Hacking Techniques
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering

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**
- **Determining the Operating System**
- **Collect Location Information**
- **People Search: Social Networking Sites/People Search Services**
- **Gather Information from Financial Services**
- **Footprinting through Job Sites**
- **Monitorming Target Using Alerts**
- **Information Gathering Using Groups, Forums, and Blogs**

Footprinting Using Advanced Google Hacking Techniques

- **Footprint Using Advanced Google Hacking Techniques**
- **Google Advance Search Operators**
- **Google Hacking Databases**
- **Information Gathering Using Google Advanced Search**

Scanning Networks

- 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

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**
- 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.
- Note: CEH- Certified Ethical Hacker

Type	Name
0	Echo Reply
3	Destination Unreachable
8	Echo
11	Time Exeeded for a Datagram

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.
- **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 type of packet filters/firewalls, operating systems and
- OS versions.

CEH Scanning Methodology - Scanning Beyond IDS

- Use fragemented 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

CEH Scanning Methodology - 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 posses and the exploits that might work on a system to further carry out additional attacks

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]

CEH Scanning Methodology - Scan for Vulnerability

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.
- **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.

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.

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.

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

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

NetBIOS Enumeration

- 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

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**

SNMP 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.

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.

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.

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]

ntpdc:

- Monitors operation of the NTP daemon, ntpd
- /usr/bin/ntpdc [-n] [-v] host1 | IPaddress1...

ntpq:

- Monitors NTP daemon ntpd operations and determines performance
- ntpq [-inp] [-c command] [host] [...]

SMTP and DNS 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.

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

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

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
- **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

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.
- Calcuate 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.