CEH – Chapter 3 Scanning and Enumeration

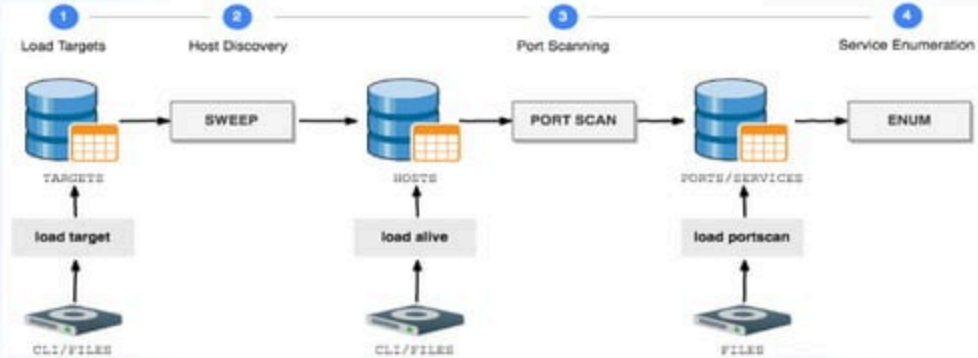
NUSRAT JAHAN

ID: M190305002

Content

- Introduction
- What is Scanning?
  - Types of Scanning
    - ✓ Port scanning
    - ✓ Network scanning
    - ✓ Vulnerability scanning
  - CEH Scanning Methodology
    - ✓ Ping Sweep Techniques
    - ✓ Flags of TCP Protocol
    - ✓ Scan Types
    - ✓ War-Dialing Techniques
    - ✓ Banner Grabbing and OS Fingerprinting Techniques
    - ✓ Scanning Anonymously
    - ✓ Bypassing Through Tunnel
- What is Enumeration?
  - SNMP Enumeration

- Scanning is the first phase of active hacking and is used to locate target systems or networks for later attack.
- Enumeration is the follow-on step once scanning is complete and is used to identify computer names, usernames, and shares.



What is Scanning?

- **Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network.**
- After the reconnaissance and information-gathering stages have been completed, scanning is performed.
- Ethical hackers use scanning to identify target systems' IP addresses, to determine whether a system is on the network and available.

Types of Scanning

Scanning Type	Purpose
Port scanning	Determines open ports and services
Network scanning	Identifies IP addresses on a given network or subnet
Vulnerability scanning	Discovers presence of known weaknesses on target systems

Port Scanning

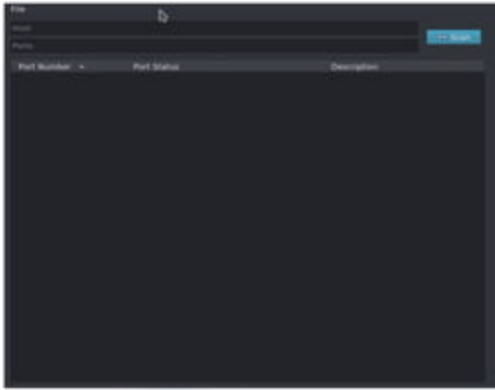
- **Port scanning is the process of identifying open and available TCP/IP ports on a system. Port-scanning tools enable a hacker to learn about the services available on a given system.**

Port Numbers are divided into three ranges:

Well-Known Ports:	0-1023
Registered Ports:	1024-49151
Dynamic Ports:	49152-65535

On Windows, well-known port numbers are located in the

- C:\windows\system32\drivers\etc\services
- Then open it with Notepad

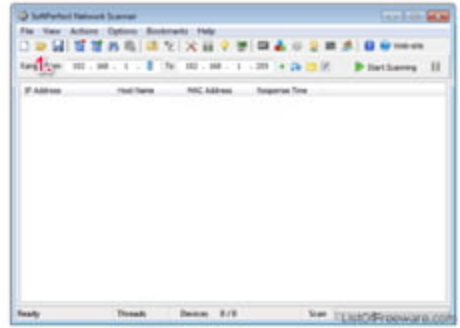


Network Scanning

- **Network scanning is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment.**

Objective Network Scanning

- To discover live hosts/computer, IP address, and open ports of the victim.
- To discover services that are running on a host computer.
- To discover the Operating System and system architecture of the target.
- To discover and deal with vulnerabilities in Live hosts.



Vulnerability Scanning

- Vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network.
- A vulnerability scanner first identifies the operating system and version number, including service packs that may be installed.
- Then, the scanner identifies weaknesses or vulnerabilities in the operating system.

CEH Scanning Methodology

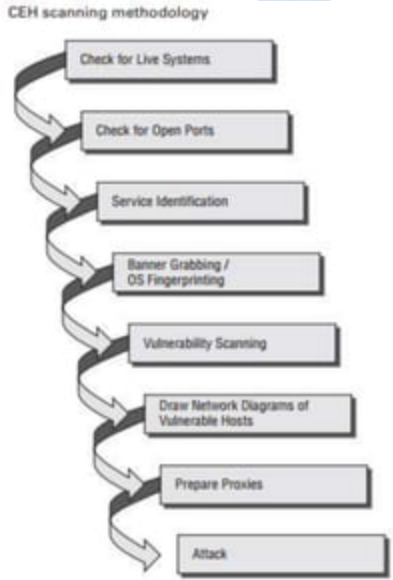
Check for Live Systems: This gives you a list of what's actually alive on your network subnet by ping scanning.

- Ping scan checks for the live system by sending ICMP echo request packets.
- If a system is alive, the system responds with ICMP echo reply packet containing details of TTL, packet size etc.

Check for Open Ports: Once you know which IP addresses are active, find what ports they're listening on.

- Nmap is the powerful tool used mainly for this purpose

Scan beyond IDS: Sometimes your scanning efforts need to be altered to avoid those pesky intrusion detection systems.



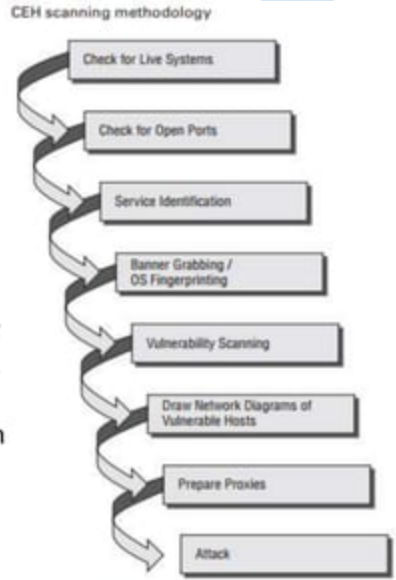
CEH Scanning Methodology

Perform banner grabbing: Banner grabbing and OS fingerprinting will tell you what operating system is on the machines and which services they are running.

Scan for vulnerabilities: Perform a more focused look at the vulnerabilities these machines haven't been patched for yet.

Draw network diagrams: A good network diagram will display all the logical and physical pathways to targets you might like.

Prepare proxies: This obscures your efforts to keep you hidden



Ping Sweep Techniques

- A ping sweep is also known as Internet Control Message Protocol (ICMP) scanning, used to determine whether systems are live or not.
- ICMP is the protocol used by the **ping** command.
- By sending an ICMP **Echo Request** or ping to all hosts on the network **Echo Reply** as a connectivity test to determine which ones are up and responding to pings.

Hacking Tools

Pinger, Friendly Pinger, and WS_Ping_Pro

Ping Sweep Techniques

Drawback

- Personal firewall software and network-based firewalls can block a system from responding to ping sweeps.
  - Block the ping attempt and notify the user that a scanning program is running on the network.
- Another problem is that the computer must be on to be scanned.

Solution

Port Scanning

Just because a ping sweep doesn't return any active hosts on the network doesn't mean they aren't available

Remember, hacking takes time, patience, and persistence

nmap Command Switches

Free and Open Source Tool

Performance

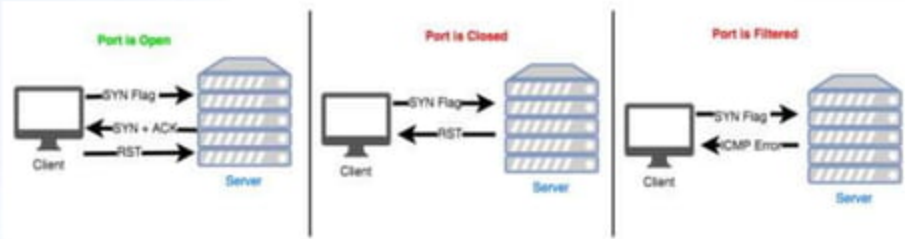
- Ping Sweeps,
- Port Scanning,
- Service Identification,
- IP Address Detection,
- Operating System Detection

Supported OS

- Unix,
- Linux,
- Windows,

nmap Command Switches

- nmap scan can determined **open, filtered, or unfiltered port**.
- Types of Satate of the Port –
  - **Open** – The target machine accepts incoming request on that port
  - **Filtered** – Firewall or network filter is screening the port and preventing nmap from discovering whether it's open
  - **Unfiltered** – The port is determined to be closed, and no firewall or filter is interfering with the nmap requests



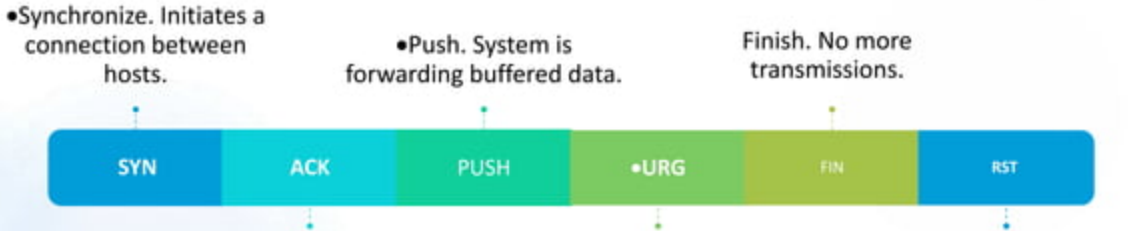
nmap Command Switches

nmap command switch	Scan performed
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan
-sL	List/DNS scan
-sI	Idle scan
-Po	Don't ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp

nmap command switch	Scan performed
-PM	ICMP netmask
-oN	Normal output
-oX	XML output
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T Sneaky	Serial scan; 15 sec between scans
-T Polite	Serial scan; .4 sec between scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan, 300 sec timeout, and 1.25 sec/probe
-T Insane	Parallel scan, 75 sec timeout, and .3 sec/probe

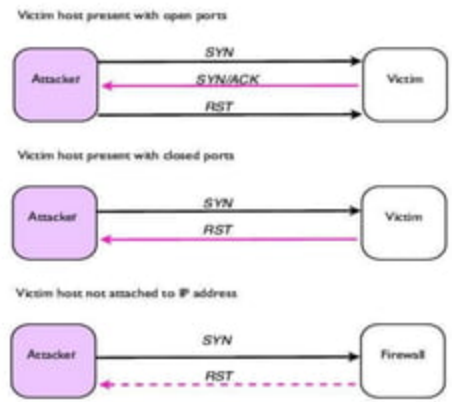
nmap command switch	Scan performed
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan

Flags of TCP Protocol



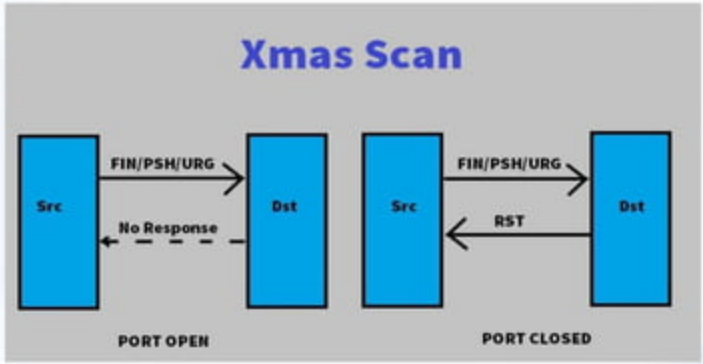
Scan Types

- **SYN:** A **SYN or stealth scan** is also called a **half-open** scan because it doesn't complete the **TCP three-way handshake**.
  - ✓ A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening.
  - ✓ If an RST is received back from the target, then it's assumed the port isn't active or is closed.
  - The advantage of the SYN stealth scan is that fewer IDS systems log this as an attack or connection attempt.



Scan Types

- **XMAS:** XMAS scans send a packet with the **FIN, URG, and PSH** flags set.
  - If the port is **open – there is no response**;
  - If the port is **closed – the target responds with a RST/ACK packet**.
  - XMAS scans work only on target systems that follow the RFC 793 implementation of TCP/IP and don't work against any version of Windows.



Scan Types

- **FIN:**
  - sends a packet with just the **FIN flag** set.
  - FIN scans receive the same response and have the same limitations as XMAS scans
- **NULL:**
  - It just sends a packet with no flags set.
  - Similar to XMAS and FIN in its limitations and response,
- **IDLE**
  - Uses a spoofed IP address to send a SYN packet to a target.
  - Depending
    on the response, the port can be determined to be open or closed.
  - IDLE scans determine
    port scan response by monitoring IP header sequence numbers

TCP Scanning Hacking Tools

- **FIN:**
  - sends a packet with just the **FIN flag** set.
  - FIN scans receive the same response and have the same limitations as XMAS scans
- **NULL:**
  - It just sends a packet with no flags set.
  - Similar to XMAS and FIN in its limitations and response,
- **IDLE**
  - Uses a spoofed IP address to send a SYN packet to a target.
  - Depending
    on the response, the port can be determined to be open or closed.
  - IDLE scans determine
    port scan response by monitoring IP header sequence numbers

Scanning Hacking Tools- Wireshark

TCP Scanning

```
root@kali:~# nmap -sT -p 445 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 02:05 EDT
Nmap scan report for 192.168.1.102
Host is up (0.087s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 0C:D2:92:82:EE:02 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

```
root@kali:~# nmap -sT -p 3389 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 03:54 EDT
Nmap scan report for 192.168.1.102
Host is up (0.049s latency).

PORT     STATE  SERVICE
3389/tcp closed ms-wbt-server
MAC Address: 0C:D2:92:82:EE:02 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

FIN Scanning

```
root@kali:~# nmap -sF -p 22 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:20 EDT
Nmap scan report for 192.168.1.102
Host is up (0.085s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 14.29 seconds
```

```
root@kali:~# nmap -sF -p 3389 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:22 EDT
Nmap scan report for 192.168.1.102
Host is up (0.065s latency).

PORT     STATE  SERVICE
3389/tcp closed ms-wbt-server
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
```

Hacking Tools

- **IPEye** is a TCP port scanner that can do SYN, FIN, Null, and XMAS scans.
- It's a command line tool

IPSecScan is a tool that can scan either a single IP address or a range of addresses looking for systems that are IPSec enabled

It contains a host of other features besides OS finger printing such as TCP, UDP, ICMP, and raw-IP ping protocols, traceroute mode, and the ability to send files between the source and target system.

SNMP Scanner allows to scan a range or list of hosts performing ping, DNS, and SNMP queries

War-Dialing Techniques

War dialing is **a technique to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for modems, computers, bulletin board systems (computer servers)** and fax machines.

- It finds another network connection that may have weaker security than the main Internet connection.
- Many organizations set up remote-access modems that are now antiquated but have failed to remove those remote-access servers.
  - This gives hackers an easy way into the network with much weaker security mechanisms.
    - ✓ Many remote-access systems use the Password Authentication Protocol (PAP), rather than VPN technology that encrypts passwords.

THC-Scan, PhoneSweep, and TeleSweep are tools that identify phone numbers and can dial a target to make a connection with a computer modem.

Banner Grabbing and OS Fingerprinting Techniques

Banner grabbing or OS Fingerprinting is the process to determine the OS running on a remote target system – opening a connection and reading the banner or response sent by the application.

- Many email, FTP, and web servers will respond to a telnet connection with the name and version of the OS

Hacking Tools

1. SolarWinds Toolset, Queso, Harris Stat, and Cheops – network management tools
2. Netcraft and HTTrack

Banner Grabbing and OS Fingerprinting Techniques

Active Fingerprinting

- **Specially crafted packets are sent to remote OS and the responses are noted**
- The responses are then compared to a database to determine the operating system.
- Various operating system vendors implement the **TCP stack differently**, and responses will differ.
- Easily detected by an IDS or other security system

Passive Fingerprinting

- **Banner Grabbing from Error messages**
  Error messages provide information such as type of server, type of OS and SSL tool used by the remote system
- **Sniffing the network traffic**
  Capturing and analyzing pkts from the target, attacker can determine OS
- **Banner Grabbing from page extension**
  Looking for an extension in the URL may assist in determining the application version
- Usually undetected by an IDS or other security system but less accurate then Active fingerprinting

Scanning Anonymously

Preparing proxy servers

- A *proxy server* is a computer that acts as an intermediary between the hacker and the target computer.
  Using a proxy server can allow a hacker to become anonymous on the network.
- The hacker first makes a connection to the proxy server and then requests a connection to the target computer via the existing connection to the proxy.
- The proxy requests access to the target computer, not the hacker's computer. This lets a hacker surf the Web anonymously or otherwise hide their attack.

Hacking Tools

SocksChain

Bypassing Through Tunnel

- A popular method of bypassing a firewall or IDS is to tunnel a blocked protocol (such as **SMTP**) through an allowed protocol (such as **HTTP**).
- Almost all IDS and firewalls act as a proxy between a client's PC and the Internet and pass only the traffic defined as being allowed.

Hacking Tools

HTTPort, Tunneld, and BackStealth are tools to tunnel traffic through HTTP. These tools allow the following potentially to be used from behind an HTTP proxy:

Email, IRC, ICQ, News, AIM,FTP

What is Enumeration?

- Enumeration occurs after scanning **extracting user names, machine names, network resources, shares, and other services from a system**.
- All the gathered information is used to identify the vulnerabilities or weak points in system security and then tries to exploit it.
- Some steps of performing hacking operation

  1. Extract usernames using enumeration.
  2. Gather information about the host using null sessions.
  3. Perform Windows enumeration using the SuperScan tool.
  4. Acquire the user accounts using the tool GetAcct.
  5. Perform SNMP port scanning.

Hacking Tool

- **DumpSec** is a NetBIOS enumeration tool. It connects to the target system as a null user with the net use command. It then enumerates users, groups, NTFS permissions, and file ownership information.
- **Hyena** is a tool that enumerates NetBIOS shares and additionally can exploit the null session vulnerability to connect to the target system and change the share path or edit the Registry.
- **SMB Auditing** Tool is a password-auditing tool for the Windows and Server Message Block (SMB) platforms. Windows uses SMB to communicate between the client and server. The SMB Auditing Tool is able to identify usernames and crack passwords on Windows systems.
- **NetBIOS Auditing** Tool is another NetBIOS enumeration tool. It's used to perform various security checks on remote servers running NetBIOS file sharing services

SNMP Enumeration

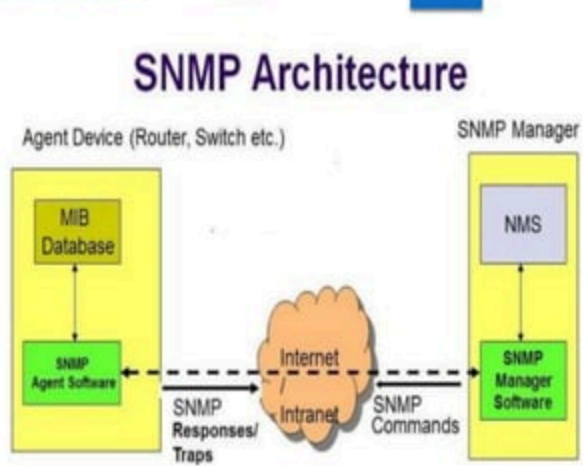
- SNMP (**Simple Network Management Protocol**) is an **application layer protocol** which uses **UDP protocol** to maintain and manage routers, hubs and switches other network devices on an IP network.
- **SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.**
- It consists of three major components:
  1. Managed Device
  2. Agent
  3. Network Management System (NMS)

SNMP Enumeration

- **Managed Device:** A managed device is a device or a host (technically known as a node) which has the SNMP service enabled. These devices could be routers, switches, hubs, bridges, computers etc.

- **Agent:** An agent can be thought of as a piece of software that runs on a managed device. Its primary job is to convert the information into SNMP compatible format for the smooth management of the network using SNMP protocol. It is located on the networking device

- **Network Management System (NMS):** These are the software systems that are used for monitoring of the network devices and communicates with the agent.



SNMP Enumeration

- The SNMP management station sends requests to agents, and the agents send back replies.
- The requests and replies refer to configuration variables accessible by agent software.
- Management stations can also send requests to set values for certain variables. Traps let the management station know that something significant has happened in the agent software, such as a reboot or an interface failure.
- Management Information Base (MIB) is the database of configuration variables that resides on the networking device.
- MIB is organized hierarchically and is a virtual database containing a formal description of all the network objects.

SNMP Enumeration

- **Community strings:**
- Community strings is a text string used to authenticate communications between the management stations and network devices on which SNMP agents are hosted.
- Community Strings travel in clear text over the network, hence are subject to network sniffing attacks.
- Community Strings are sent with every network packet exchanged between the node and management station.

1. ***read community string*** - this password lets you view the configuration of the device or system. This mode permits querying the device and reading the information, but does not permit any kind of changes to the configuration. The default community string for this mode is "public."
2. ***read/write community string*** – it's for changing or editing the configuration on the device. In this mode, changes to the device are permitted; hence if one connects with this community string, we can even modify the remote device 's configurations. The default community string for this mode is "private."

SNMP Enumeration

Hacking Tools

SNMPUtill

- SNMPUtil gathers **Windows user account information via SNMP in Windows systems.**
- Some information—such as routing tables, ARP tables, IP addresses, MAC addresses,
- TCP and UDP open ports, user accounts, and shares—can be read from a Windows system that has SNMP enabled using the SNMPUtil tools.

IP Network Browser

IP Network Browser from the SolarWinds Toolset also uses SNMP to gather more information about a device that has an SNMP agent.

Thank You