4.3. Scanning Networks

Scanning

Scanning is the first phase of active hacking and is used to locate target systems or networks for later attack. After the reconnaissance and information-gathering stages have been completed, scanning is performed. It is important that the information-gathering stage be as complete as possible to identify the best location and targets to scan. During scanning, the hacker continues to gather information regarding the network and its individual host systems. Information such as IP addresses, operating system, services, and installed applications can help the hacker determine which type of exploit to use in hacking a system.

Scanning is the process of locating systems that are alive and responding on the network. Ethical hackers use scanning to identify target systems' IP addresses. Scanning is also used to determine whether a system is on the network and available. Scanning tools are used to gather information about a system such as IP addresses, the operating system, and services running on the target computer.

Types of scanning:

Three types of scanning are ,

S.No	Scanning type	Purpose
1	Port scanning	Determines open ports and services
2	Network scanning	Identifies IP addresses on a given network or subnet
3	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. Each service or application on a machine is associated with a *well-known* port number. Port Numbers are divided into three ranges:

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

For example, a port-scanning tool that identifies port 80 as open indicates a web server is running on that system. Hackers need to be familiar with well-known port numbers.

Common port Numbers

On Windows systems, well-known port numbers are located in the C:\windows\system32\ drivers\etc\services file. Services is a hidden file. To view it, show hidden files in Windows Explorer, and double-click the filename to open it with Notepad. The CEH exam expects you to know the well-known port numbers for common applications; familiarize yourself with the port numbers for the following applications:

- ✓ FTP, 21
- ✓ Telnet, 23
- ✓ HTTP, 80
- ✓ SMTP, 25
- ✓ POP3, 110
- ✓ HTTPS, 443

The following list contains additional port numbers not necessarily on the CEH exam but useful for real-world penetration testing:

- ✓ Global Catalog Server (TCP), 3269 and 3268
- ✓ LDAP Server (TCP/UDP), 389
- ✓ LDAP SSL (TCP/UDP), 636
- ✓ IPsec ISAKMP (UDP), 500
- ✓ NAT-T (UDP), 4500
- ✓ RPC (TCP), 135
- ✓ ASP.NET Session State (TCP), 42424
- ✓ NetBIOS Datagram Service (UDP), 137 and 138
- ✓ NetBIOS Session Service (TCP), 139

Network Scanning

Network scanning is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment. Hosts are identified by their individual IP addresses. Network-scanning tools attempt to identify all the *live* or responding hosts on the network and their corresponding IP addresses.

Vulnerability Scanning

Vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network. Generally, 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. During the later attack phase, a hacker can exploit those weaknesses in order to gain access to the system.

Although scanning can quickly identify which hosts are listening and active on a network, it is also a quick way to be identified by an intrusion detection system (IDS). Scanning tools probe TCP/IP ports looking for open ports and IP addresses, and these probes can be recognized by most security intrusion detection tools. Network and vulnerability scanning can usually be detected as well, because the scanner must interact with the target system over the network.

Depending on the type of scanning application and the speed of the scan, an IDS will detect the scanning and flag it as an IDS event. Some of the tools for scanning have different modes to attempt to defeat an IDS and are more likely to be able to scan undetected.

The CEH (Certified Ethical Hacker)Scanning Methodology

This methodology is the process by which a hacker scans the network. It ensures that no system or vulnerability is overlooked and that the hacker gathers all necessary information to perform an attack.

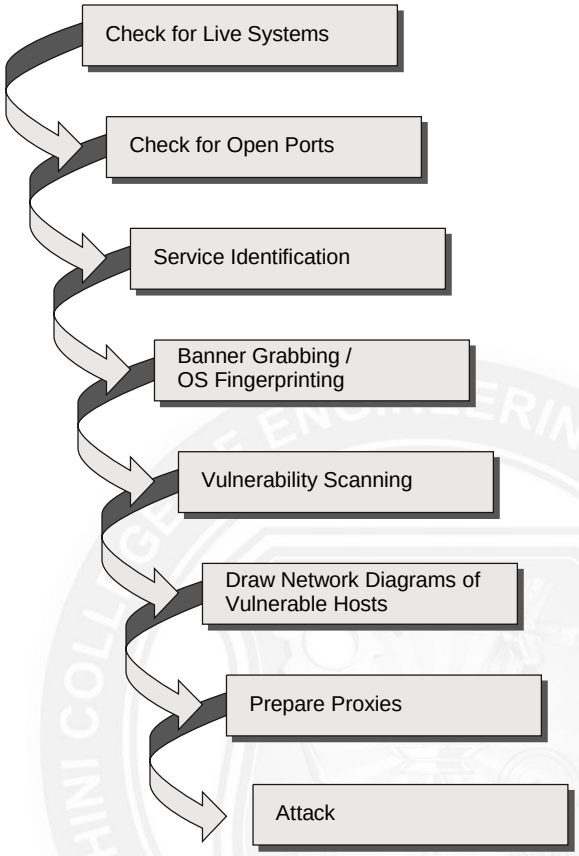


Fig:CEH scanning methodology

Ping Sweep Techniques

The CEH scanning methodology starts with checking for systems that are live on the network, meaning that they respond to probes or connection requests. The simplest, although not necessarily the most accurate, way to determine whether systems are live is to perform a *ping sweep* of the IP address range. All systems that respond with a ping reply are considered live on the network. A ping sweep is also known as Internet Control Message Protocol (ICMP) scanning, as ICMP is the protocol used by the ping command.

ICMP scanning, or a ping sweep, is the process of sending an ICMP request or ping to all hosts on the network to determine which ones are up and responding to pings. ICMP began as a protocol used to send test and error messages between hosts on the Internet. It has evolved as a protocol utilized by every operating system, router, switch or Internet Protocol (IP)-based device. The ability to use the ICMP Echo request and Echo reply as a connectivity test between hosts is built into every IP-enabled device via the ping command. It is a quick and dirty test to see if two hosts have connectivity and is used extensively for troubleshooting.

A benefit of ICMP scanning is that it can be run in *parallel*, meaning all systems are scanned at the same time; thus it can run quickly on an entire network. Most hacking tools include a ping

sweep option, which essentially means performing an ICMP request to every host on the network. Systems that respond with a ping response are alive and listening on the network.

One considerable problem with this method is that personal firewall software and network-based firewalls can block a system from responding to ping sweeps. More and more systems are configured with firewall software and will 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.

Scanning Ports and Identifying Services:

Port scanning is the method used to check for open ports. The process of port scanning involves probing each port on a host to determine which ports are open. Port scanning generally yields more valuable information than a ping sweep about the host and vulnerabilities on the system.

Service identification is the third step in the CEH scanning methodology; it's usually performed using the same tools as port scanning. By identifying open ports, a hacker can usually also identify the services associated with that port number.

Port-Scan Countermeasures:

Countermeasures are processes or toolsets used by security administrators to detect and possibly thwart port scanning of hosts on their network. The following list of countermeasures should be implemented to prevent a hacker from acquiring information during a port scan:

- Proper security architecture, such as implementation of IDS and firewalls, should be followed.
- Ethical hackers use their toolset to test the scanning countermeasures that have been implemented. Once a firewall is in place, a port-scanning tool should be run against hosts on the network to determine whether the firewall correctly detects and stops the port-scanning activity.
- The firewall should be able to detect the probes sent by port-scanning tools. The firewall should carry out stateful inspections, which means it examines the data of the packet and not just the TCP header to determine whether the traffic is allowed to pass through the firewall.
- Network IDS should be used to identify the OS-detection method used by some common hackers tools.
- Only needed ports should be kept open. The rest should be filtered or blocked.
- The staff of the organization using the systems should be given appropriate training on security awareness. They should also know the various security policies they're required to follow.

nmap Command Switches:

Nmap is a free, open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, IP address detection, and operating system detection. Nmap has the benefit of scanning a large number of machines in a single session. It's supported by many operating systems, including Unix, Windows, and Linux.

The state of the port as determined by an nmap scan can be open, filtered, or unfiltered. *Open* means that the target machine accepts incoming request on that port. *Filtered* means a firewall or network filter is screening the port and preventing nmap from discovering whether it's open. *Unfiltered* mean the port is determined to be closed, and no firewall or filter is interfering with the nmap requests.

Nmap supports several types of scans

S.No	Nmap scan type	Description
1	***TCP connect***	The attacker makes a full TCP connection to the target system. The most reliable scan type but also the most detectable. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.
2	***XMAS tree scan***	The attacker checks for TCP services by sending XMAS-tree packets, which are named as such because all the "lights" are on, meaning the FIN, URG, and PSH flags are set (the meaning of the flags will be discussed later in this chapter). Closed ports reply with a RST flag.
3	***SYN stealth scan***	This is also known as half-open scanning. The hacker sends a SYN packet and receives a SYN-ACK back from the server. It's stealthy because a full TCP connection isn't opened. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.
4	***Null scan***	This is an advanced scan that may be able to pass through firewalls undetected or modified. Null scan has all flags off or not set. It only works on Unix systems. Closed ports will return a RST flag.
5	***Windows scan***	This type of scan is similar to the ACK scan and can also detect open ports.
6	***ACK scan***	This type of scan is used to map out firewall rules. ACK scan only works on Unix. The port is considered filtered by firewall rules if an ICMP destination unreachable message is received as a result of the ACK scan.

Scan Types

As a CEH (Certified Ethical Hacker), you need to be familiar with the following scan types and uses:

SYN : A SYN or stealth scan is also called a half-open scan because it doesn't complete the TCP three-way handshake. (The TCP/IP three-way handshake will be covered in the next section.) 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.

XMAS: X MAS scans send a packet with the FIN, URG, and PSH flags set. If the port is open, there is no response; but 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.

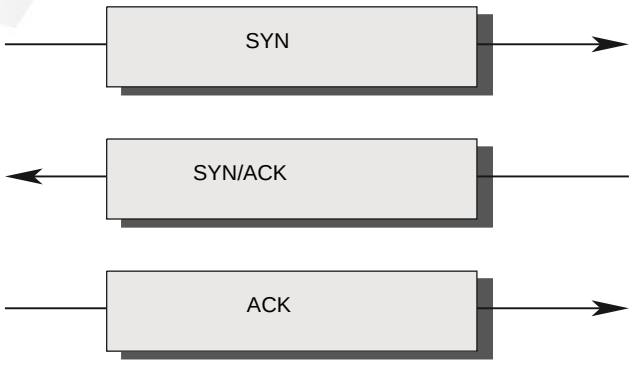
FIN : A FIN scan is similar to an XMAS scan but sends a packet with just the FIN flag set. FIN scans receive the same response and have the same limitations as XMAS scans.

NULL : A NULL scan is also similar to XMAS and FIN in its limitations and response, but it just sends a packet with no flags set.

IDLE : An IDLE scan 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 Communication Flag Types

TCP scan types are built on the *TCP three-way handshake*. TCP connections require a three-way handshake before a connection can be made and data transferred between the sender and receiver. Figure shows the steps of the TCP three-way handshake.



To complete the three-way handshake and make a successful connection between two hosts, the sender must send a TCP packet with the synchronize (SYN) bit set. Then, the receiving system responds with a TCP packet with the synchronize (SYN) and acknowledge (ACK) bit set to indicate the host is ready to receive data. The source system sends a final packet with the ACK bit set to indicate the connection is complete and data is ready to be sent.

Because TCP is a connection-oriented protocol, a process for establishing a connection (three-way handshake), restarting a failed connection, and finishing a connection is part of the protocol. These protocol notifications are called *flags*. TCP contains ACK, RST, SYN, URG, PSH, and FIN flags. The following list identifies the function of the TCP flags:

SYN Synchronize. Initiates a connection between hosts.

ACK Acknowledge. Established connection between hosts.

PSH Push. System is forwarding buffered data.

URG Urgent. Data in packets must be processed quickly.

FIN Finish. No more transmissions.

RST Reset. Resets the connection.

A hacker can attempt to bypass detection by using flags instead of completing a normal TCP connection.

TCP scan types

S.No	XMAS scan	Flags sent by hacker
1	XMAS scan	All flags set (ACK, RST, SYN, URG, PSH, FIN)
2	FIN scan	FIN
3	NULL scan	No flags set
4	TCP connect/full-open scan	SYN, then ACK
5	SYN scan / half-open scan	SYN, then RST