Scanning and Enumeration

Covering Topics :

Introduction

Methodology

Understanding techniques

Nmap commands

Banner grabbing and Os fingerprinting

HTTP tunneling

Enumeration

Introduction :

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. 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.

Basically there are three type of scanning :

(i) Network scanning
(ii) Port scanning
(iii) Vulnerability scanning

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. Networkscanning tools attempt to identify all the live or responding hosts on the network and their corresponding IP addresses.

Scanning methodology starts with identifying alive hosts in the network. 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.

Using windows ping :

- **(i) Open command prompt**
- **(ii) Type ping** www.cyberops.in

```
C:\>ping www.cyberops.in

Pinging www.cyberops.in [31.131.16.183] with 32 bytes of data:
Reply from 31.131.16.183: bytes=32 time=209ms TTL=48
Reply from 31.131.16.183: bytes=32 time=195ms TTL=48
Reply from 31.131.16.183: bytes=32 time=212ms TTL=48
Reply from 31.131.16.183: bytes=32 time=189ms TTL=48

Ping statistics for 31.131.16.183:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 189ms, Maximum = 212ms, Average = 201ms
```

A timeout indicates that the remote system is not responding or turned off or that the ping was blocked. A reply indicates that the system is alive and responding to ICMP requests.

Port Scanning :

Port scanning is the process of identifying open and available TCP/IP ports on a system. Portscanning 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:

- (i) Well-known ports: 0-1023
- (ii) Registered ports: 1024-49151
- (iii) 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.

Some common ports :

- FTP, 21
- Telnet, 23
- HTTP, 80
- SMTP, 25
- POP3, 110
- HTTPS, 443
- DHCP Server (UDP), 67
- LDAP Server (TCP/UDP), 389
- SMB (TCP), 445
- RPC (TCP), 135
- DNS (TCP/UDP), 53
- IMAP (TCP), 143
- IMAP over SSL (TCP), 993
- POP3 over SSL (TCP), 995
- RPC (TCP), 135

Vulnerability Scanning :

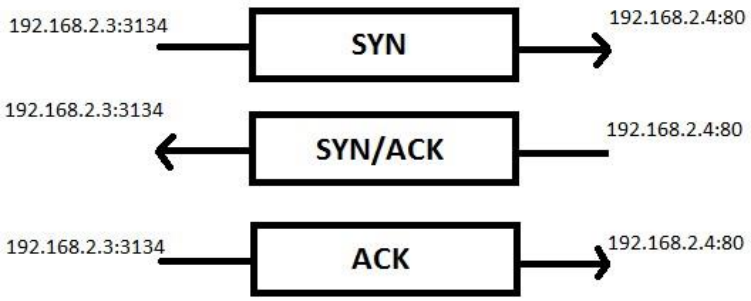
Vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system and version number, including service packs that may be installed. Then, the scanner identifies weaknesses or vulnerabilities in the operating system. During the later attack phase, a hacker can exploit those weaknesses in order to gain access to the system.

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.

TCP communication :

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.



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.

The TCP scan types are used by some scanning tools to elicit a response from a system by setting one or more flags.

Scanning Types :

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 : XMAS 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.

Nmap Command :

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 many types of scan :

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.
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.
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.
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.
Windows scan	This type of scan is similar to the ACK scan and can also detect open ports.

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.

We will see nmap in detail in Penetration testing with backtrack module.

Banner Grabbing and OS Fingerprinting :

Banner grabbing and operating system identification. The process of fingerprinting allows the hacker to identify particularly vulnerable or high-value targets on the network. Hackers are looking for the easiest way to gain access to a system or network. Banner grabbing is the process of 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 software. This aids a hacker in fingerprinting the OS and application software. For example, a Microsoft Exchange email server would only be installed on a Windows OS.

Active stack fingerprinting is the most common form of fingerprinting. It involves sending data to a system to see how the system responds. It's based on the fact that various operating system vendors implement the TCP stack differently, and responses will differ based on the operating system. The responses are then compared to a database to determine the operating system. Active stack fingerprinting is detectable because it repeatedly attempts to connect with the same target system.

Passive stack fingerprinting is stealthier and involves examining traffic on the network to determine the operating system. It uses sniffing techniques instead of scanning techniques. Passive stack fingerprinting usually goes undetected by an IDS or other security system but is less accurate than active fingerprinting.

SolarWinds Toolset, Queso, Harris Stat, and Cheops are network management tools that can be used for detecting operating systems, mapping network diagrams, listing services running on a network, performing generalized port scanning, and so on.

Netcraft and HTTrack are tools that fingerprint an operating system. Both are used to determine the OS and web server software version numbers. Netcraft is a website that periodically polls web servers to determine the operating system version and the web server software version. Netcraft can provide useful information the hacker can use in identifying vulnerabilities in the web server software. In addition, Netcraft has an antiphishing toolbar and web server verification tool you can use to make sure you're using the actual web server rather than a spoofed web server. Exercise 3.3 shows how to use Netcraft to identify the OS or a web server. HTTrack arranges the original site's relative link structure. You open a page of the mirrored website in your browser, and then you can browse the site from link to link as if you were viewing it online. HTTrack can also update an existing mirrored site and resume interrupted downloads.

Use Netcraft to Identify the OS of a Web Server

1. Open a web browser to the Netcraft website, www.netcraft.com.
2. Type a website name in the What's That Site Running? field in the upper-left corner of the screen.
3. Scroll down to Hosting History to see what OS and web server software are running on the server.

A hacker can spoof an IP address when scanning target systems to minimize the chance of detection. One drawback of spoofing an IP address is that a TCP session can't be successfully completed.
Source routing lets an attacker specify the route that a packet takes through the Internet. This can also minimize the chance of detection by bypassing IDS and firewalls that may block or detect the attack. Source routing uses a reply address in the IP header to return the packet to a spoofed address instead of the attacker's real address. The use of source routing to bypass an IDS will be covered in more detail in Chapter 13, "Evading IDSs, Honeypots, and Firewalls." To detect IP address spoofing, you can compare the time to live (TTL) values: the attacker's TTL will be different from the spoofed address's real TTL.

Enumeration :

Enumeration occurs after scanning and is the process of gathering and compiling usernames, machine names, network resources, shares, and services. It also refers to actively querying or connecting to a target system to acquire this information. Hackers need to be methodical in their approach to hacking. The following steps are an example of those a hacker might perform in preparation for hacking a target system:
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.

The object of enumeration is to identify a user account or system account for potential use in hacking the target system. It isn't necessary to find a system administrator account, because most account privileges can be escalated to allow the account more access than was previously granted.
Many hacking tools are designed for scanning IP networks to locate NetBIOS name information. For each responding host, the tools list IP address, NetBIOS computer name, logged-in username, and MAC address information.
On a Windows 2000 domain, the built-in tool net view can be used for NetBIOS enumeration. To enumerate NetBIOS names using the net view command, enter the following at the command prompt:

net view / domain
nbtstat -A IP address

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.
The 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.
The NetBIOS Auditing Tool is another NetBIOS enumeration tool. It's used to perform various security checks on remote servers running NetBIOS file sharing services.

NULL session

Once a hacker has made a NetBIOS connection using a null session to a system, they can easily get a full dump of all usernames, groups, shares, permissions, policies, services, and more using the Null

user account. The SMB and NetBIOS standards in Windows include APIs that return information about a system via TCP port 139.
One method of connecting a NetBIOS null session to a Windows system is to use the hidden InterProcess Communication share (IPC$). This hidden share is accessible using the net use command. As mentioned earlier, the net use command is a built-in Windows command that connects to a share on another computer. The empty quotation marks (“”) indicate that you want to connect with no username and no password. To make a NetBIOS null session to a system with the IP address 192.21.7.1 with the built-in anonymous user account and a null password using the net use command, the syntax is as follows:

C: \> net use \\192.21.7.1 \IPC$ “” /u: “”

Once the net use command has been successfully completed, the hacker has a channel over which to use other hacking tools and techniques.