**Scanning**

Scanning is a process of identifying network and service-related information by communicating with the target. Scanning helps in identifying IP/Hostnames, Ports, Services running on ports, Live hosts, Vulnerable services running on the target network.

**Types of Scanning**

Different number of scanning procedures are used with the objective to identify hosts, ports, and services in the target network. One of the most common types scanning methods that are available.

**Network Scanning**

During the network scanning process, attackers gather a list of IP addresses of computers that are live on the target network. The job of the attacker will be easy if he/she can analyze the network structure and services running on each machine.

**List of Network Scanners**

● Angry IP Scanner

● Advanced IP Scanner

● Netdiscover

● Autoscan

● hping3

● Nmap

**List of Network Scan Methods**

• Ping Sweep

• Arp Scan

**What Are Ports and Port Numbers**

Ports are virtual entry points to any digital device; devices can communicate with one to another using port, there are virtually 65535 ports available in every device, those can be identified with port numbers, ranging from 0 to 65535.

**Port Scanning**

Port scanning is a technique where the attacker will send communication probes to targets to see how the target is responding to them, based on the www.hackerschool.in response attacker will determine what ports are open and several other port details, like service running on the port numbers, and OS the target is running.

A picture containing text

Description automatically generated

**List of Port scanners**

● Nmap

● SuperScan

● Strobe

● Zenmap

**List of Port Scan methods**

• SYN Scan/Stealth Scan/

• TCP Connect Scan

• ACK Scan

• XMAS Scan

• FIN Scan

• NULL Scan

• OS Detection Scan

• Script Scan

• UDP Scan

• Service Detection Scan

**Few Well-Known Ports**

**Application Port Number(s) Application Port Number(s)**

**FTP 20–21**  DNS 53

Telnet 23 IRC 194

SMTP 25 POP3 110

DNS 53 SNMP 161

HTTP 80 HTTPS 443

SSH 22 NetBIOS 139

TFTP 69 SQL 156

For details on other port numbers and services refer RFC-1700

**Live Host identification scan**

Identifying the turned-on computers by sending ICMP packets or ARP packets or some other kind of packets is called Live Host Identification Scan.

**ICMP**

ICMP stands for Internet Control Messaging Protocol; this is widely used for internet communication troubleshooting or to generate errors related to IP operations, this will send packets to the target machine and will see whether the packets are delivered or not.

**TCP**

Transmission Control Protocol (TCP), which is a widely used protocol for data transmission over a network. This protocol establishes a reliable connection between two hosts before transmitting data, to ensure that data transmitted over the network reaches the destination without fail. TCP also known as a connection-oriented protocol, establishes a reliable connection between sender and receiver. TCP provides error and flow control mechanisms which help in orderly transmission of data and retransmission of lost packets.

**UDP**

UDP stands for User Datagram Protocol, which is connectionless protocol, mostly used for connections that can tolerate data loss. UDP is used by applications on the internet that offer voice and video communications, which can suffer some data loss without adversely affecting the quality. UDP does not provide error and flow control mechanisms because of which it does not require a connection before transmitting data over the network.

**TCP 3-way Handshake**

To start a proper TCP conversation, the sender and receiver perform 3- way handshake before exchanging data over the network. It is a process used by two hosts to agree upon some protocol stack to start sharing data. Following image represents the process of 3-way handshake

**TCP COMMUNICATION FLAGS**

1. **SYN (Synchronize):** SYN flags will be used to initiate a data transfer of the start of a communication process.

2. **ACK (Acknowledgement):** ACK flags will be used to send the receipt of successful packet transmission.

3. **FIN (Finish): FIN** flags will be used to close or finish an existed packet transmission. No more packets to be received.

4. **RST (Reset):** RST flags will be used to terminate or reset a connection.

5. **URG (Urgent):** Data in this flagged packet should be processed immediately.

6. **PSH (Push):** Sends all buffered data immediately.

**Types of Port Scanning Techniques**

• **TCP Connect Scan / Full Open Scan**

Nmap directly communicates with the operating system to establish a connection with the target machine and port by issuing the connect system call.

• **SYN Scan / Half-Open Scan / Stealth Scan**

SYN scan is the most popular scan option. It can scan thousands of ports in a short period on a fast network not hampered by restrictive firewalls.

• **ACK Scan/Firewall Detection**

This scan is different from others scanning operations discussed before; it never determines open ports. It is used to identify firewall rules, determining the type of firewall and identify filtered ports.

• **XMAS Scan**

The Xmas-Tree scan sends a TCP packet with the following flags:

URG — Indicates that the data is urgent and should be processed immediately

PSH — Forces data to a buffer

FIN — Used when finishing a TCP session

• **FIN Scan**

FIN scan, which attempts to close a connection that isn't open. The operating system generates an error if service is not running on target port. If a service is listening, the operating system will silently drop the incoming packet. Therefore, no response indicates a listening service at the port.

• **NULL Scan**

A data packet with zero flag values will be sent to a TCP port. (In a regular TCP communication, at least one bit or flag is set). In TCP connect / SYN scans, a response indicates an open port, but in a NULL scan, a response indicates a closed port.

**Importance of Scanning**

Scanning will provide an exact outline of the network structure of the target workspace. It is beneficial for hacking target servers or individual computers. Scanning will provide a blueprint of entire network and details about devices running on the network, information related to network topology and helps in deciding what operating system is running on target computers.

**Countermeasures**

● Block ICMP and UDP inbound.

● Disable unused ports with support of policy settings.

● Block internal IP addresses from coming inbound.

● Change system and application banners to counter software detection attacks.

● Always use a genuine operating system, update it frequently.

● Use IDS & IPS to detect and prevent attacks.

● Use “duckduckgo” or “StartPage” search engine to protect privacy.