
EC-Council
C|EH v13
Module 03
Scanning Networks

Learning Objectives

01 Explain Network Scanning Concepts

02 Demonstrate Various Scanning Techniques for Host Discovery

03 Demonstrate Various Scanning Techniques for Port and Service Discovery

04 Demonstrate Various Scanning Techniques for OS Discovery

05 Demonstrate Various Techniques for Scanning Beyond IDS and Firewall

06 Explain Network Scanning Countermeasures

Objective 01

Explain Network Scanning Concepts

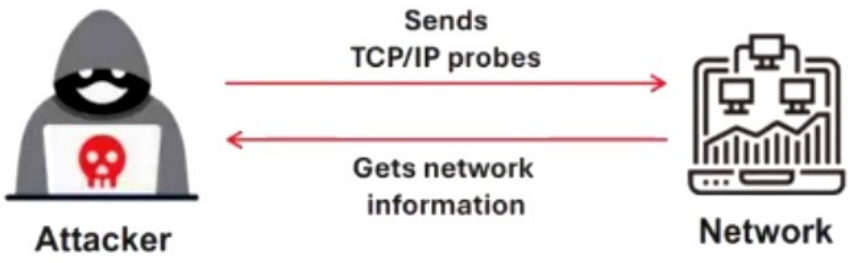
Overview of Network Scanning

Network scanning refers to a set of procedures used for **identifying hosts**, **ports**, and **services** in a network

Network scanning is one of the **components of information gathering** which can be used by an attacker to create a profile of the target organization

Attackers use tools such as **Nmap**, **Hping3**, **Metasploit**, and **NetScanTools** Pro to perform network scanning

Network Scanning Process

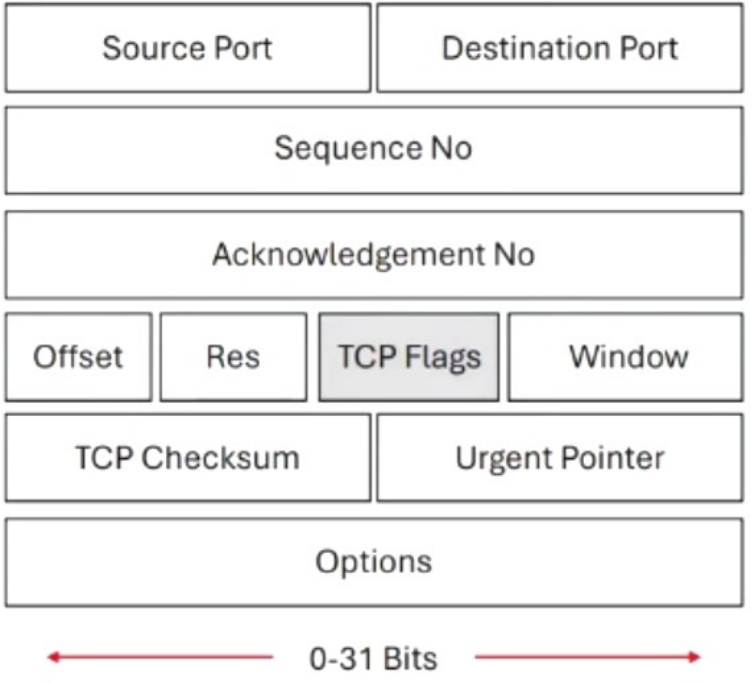


Objectives of Network Scanning

- 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

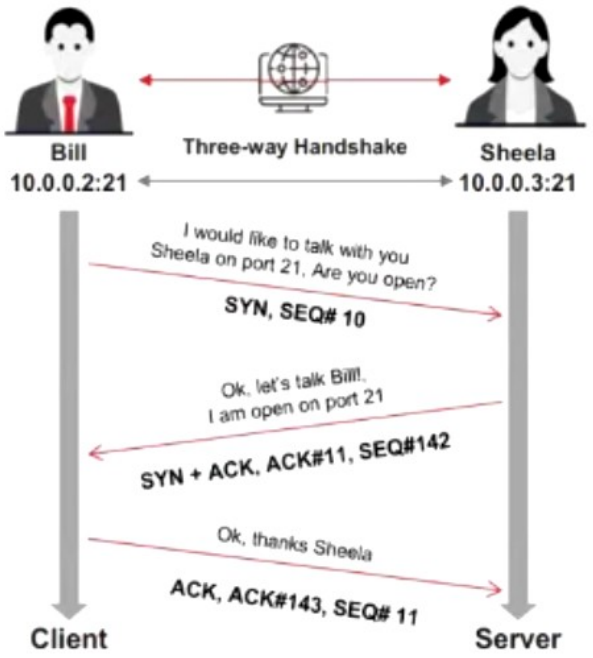
Data contained in the packet should be processed immediately **URG** (Urgent)	There will be no further transmissions **FIN** (Finish)	Resets a connection **RST** (Reset)
Sends all buffered data immediately **PSH** (Push)	Acknowledges the receipt of a packet **ACK** (Acknowledgement)	Initiates a connection between hosts **SYN** (Synchronize)



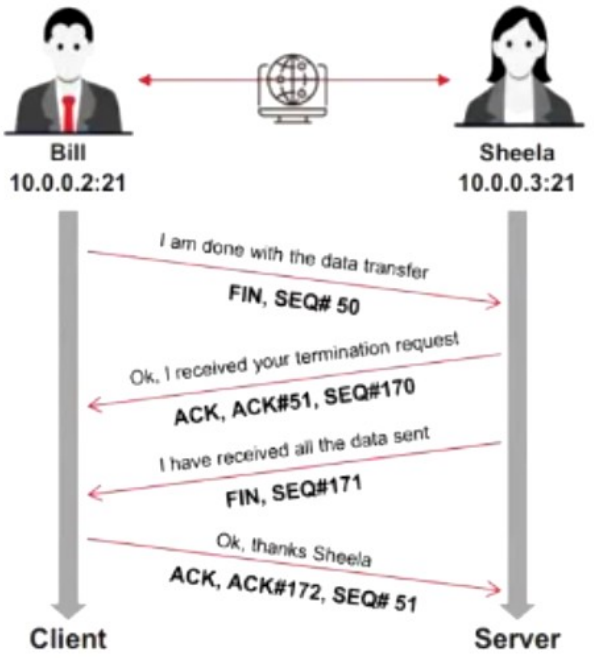
Standard TCP communications are controlled by flags in the TCP packet header

TCP/IP Communication

TCP Session Establishment
(Three-way Handshake)



TCP Session Termination

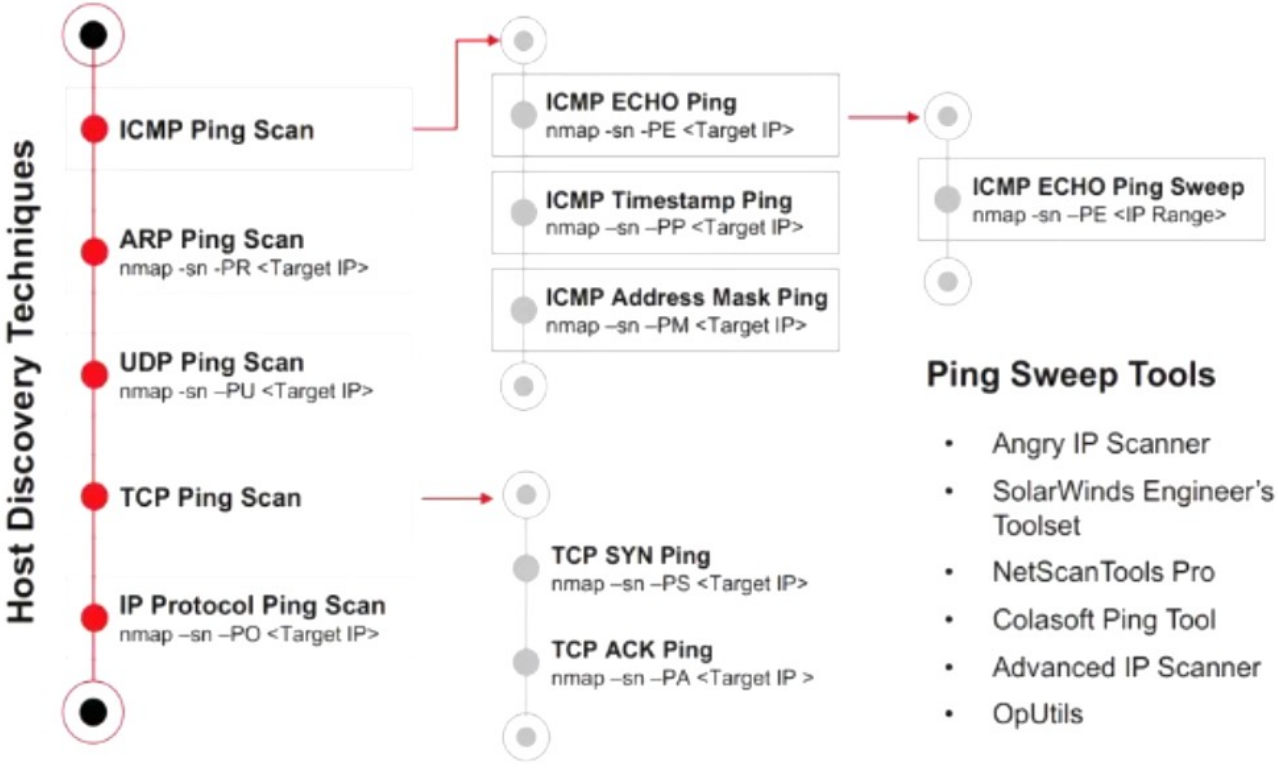


Objective 02

Demonstrate Various Scanning Techniques for Host Discovery

Host Discovery Techniques

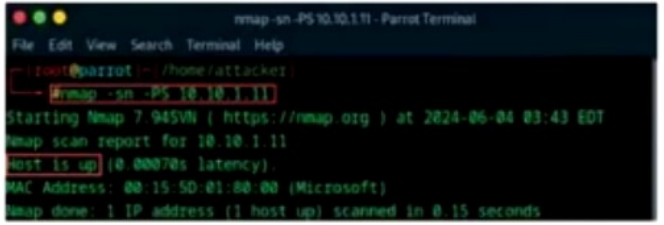
Host discovery techniques are used to **identify the active/live systems** in the network



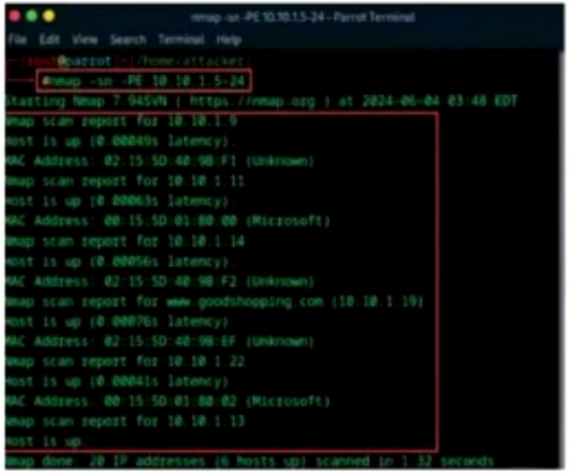
Ping Sweep Tools

- Angry IP Scanner
- SolarWinds Engineer's Toolset
- NetScanTools Pro
- Colasoft Ping Tool
- Advanced IP Scanner
- OpUtils

TCP SYN Ping Scan



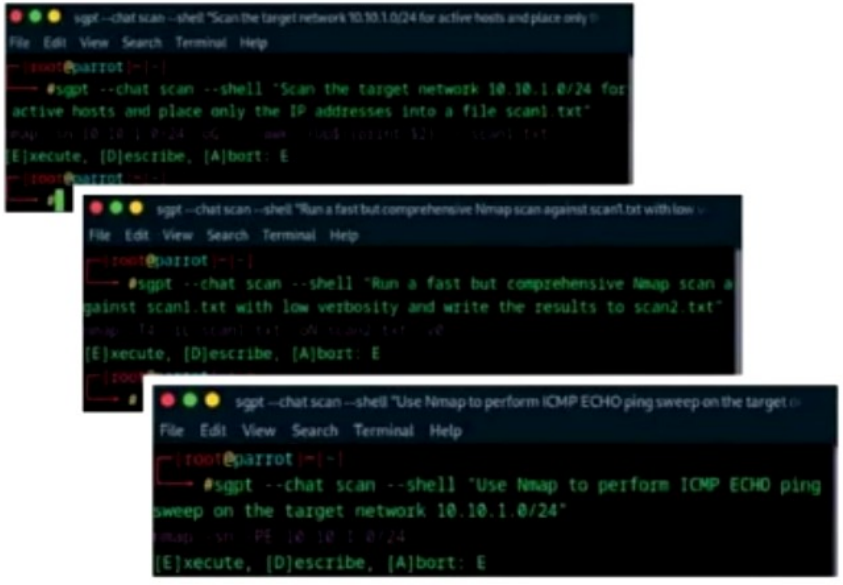
ICMP ECHO Ping Sweep

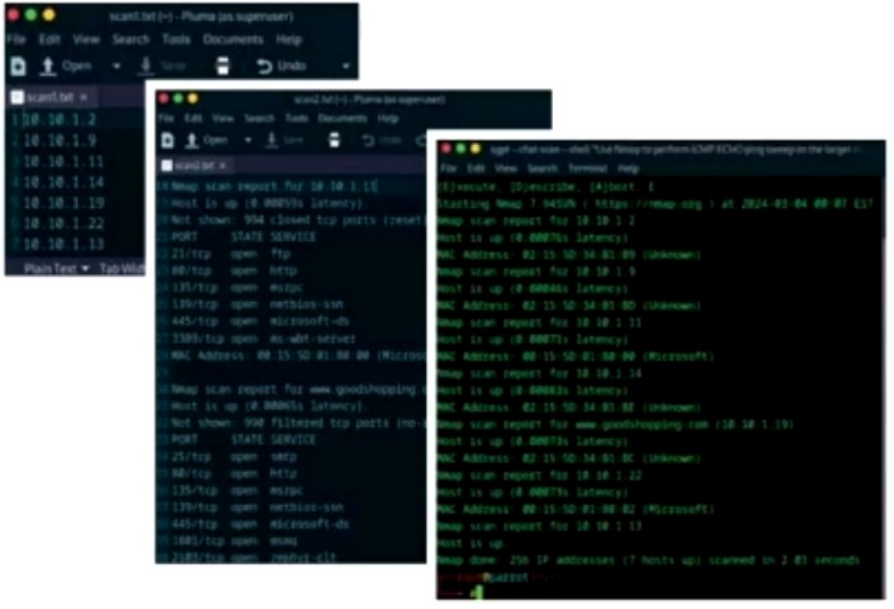


Host Discovery with AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

- *"Scan the target network 10.10.1.0/24 for active hosts and place only the IP addresses into a file scan1.txt"*
- *"Run a fast but comprehensive Nmap scan against scan1.txt with low verbosity and write the results to scan2.txt"*
- *"Use Nmap to perform ICMP ECHO ping sweep on the target network 10.10.1.0/24"*



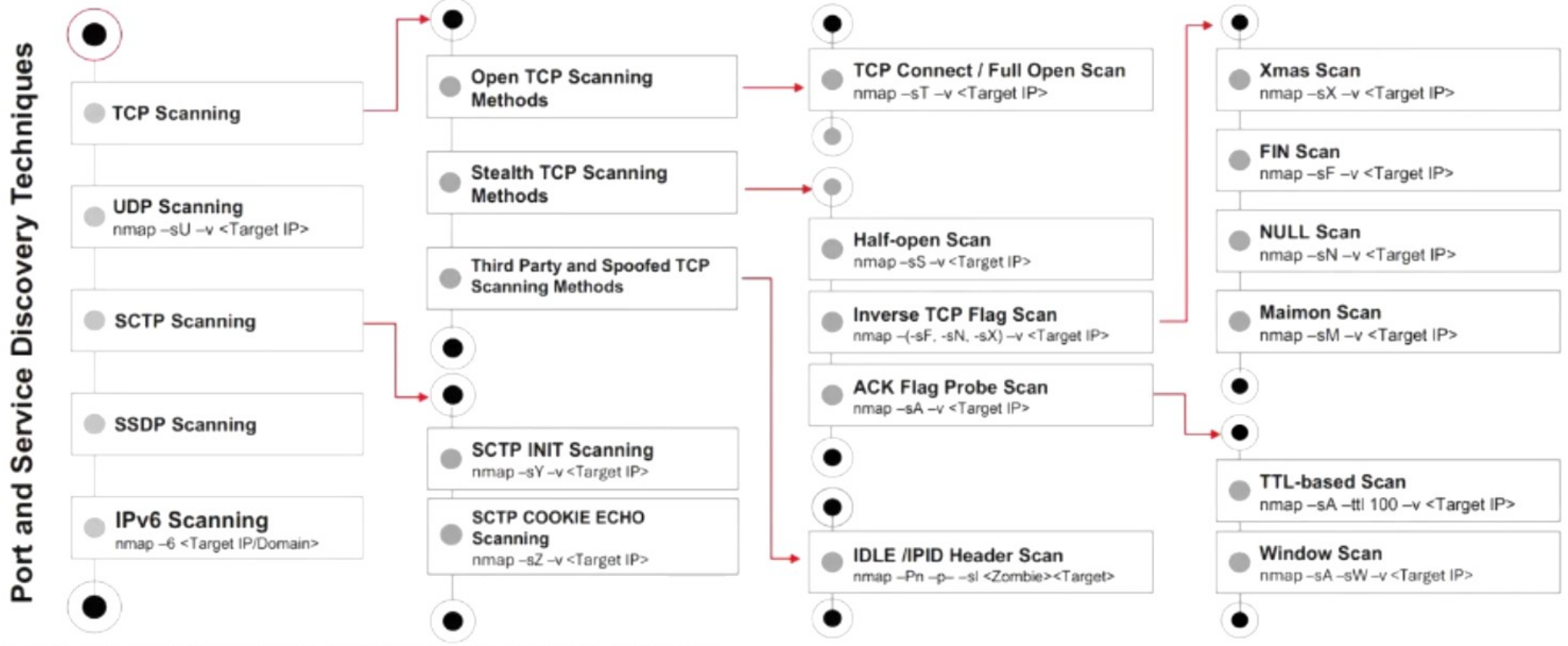


Objective 03

Demonstrate Various Scanning Techniques for Port and Service Discovery

Port Scanning Techniques

The port scanning techniques are **categorized according to the type of protocol** used for communication



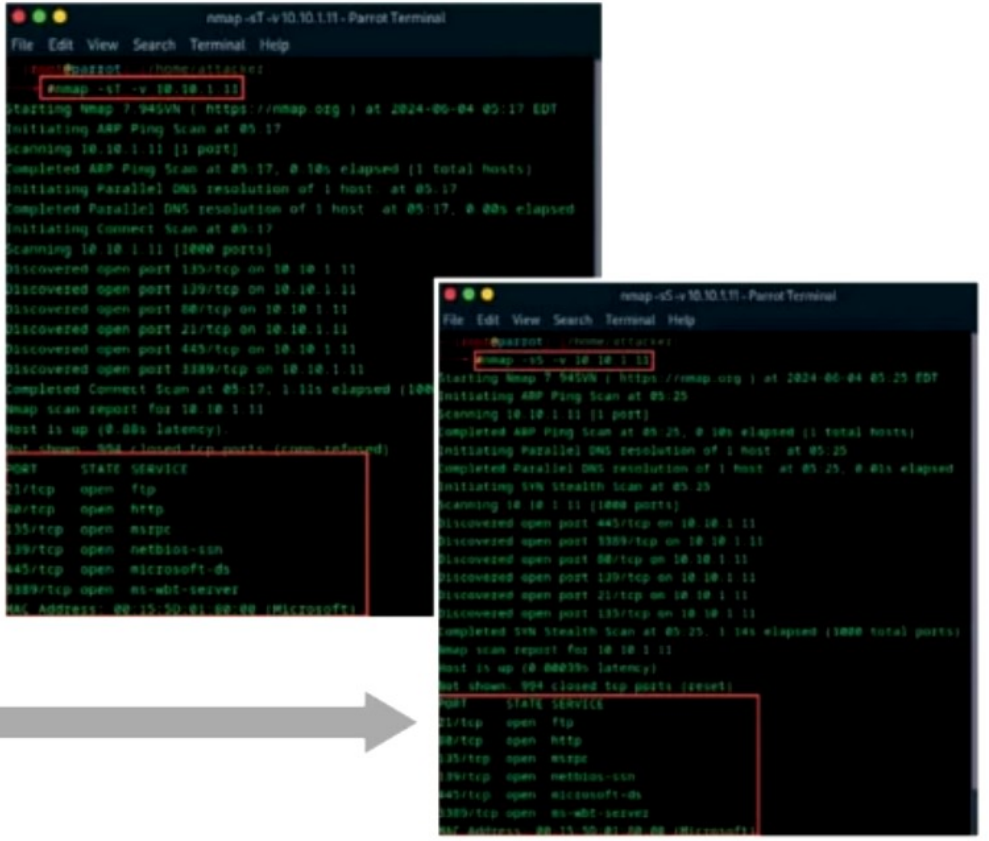
Port Scanning Techniques (Cont'd)

TCP Connect/ Full-Open Scan

- The TCP Connect scan detects when a port is open after completing the **three-way handshake**
- TCP Connect scan **establishes a full connection** and then closes the connection by sending an **RST packet**

Stealth Scan (Half-Open Scan)

- Stealth scanning involves abruptly resetting the TCP connection between the client and server before the completion of **three-way handshake signals**, thus leaving the connection half-open
- Attackers use stealth scanning techniques to **bypass firewall rules** as well as **logging mechanisms**, and hide themselves under the appearance of regular network traffic



Port Scanning with AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

- "*Use Nmap to find open ports on target IP 10.10.1.11*"
- "*Perform stealth scan on target IP 10.10.1.11 and display the results*"
- "*Perform an XMAS scan on target IP 10.10.1.11*"

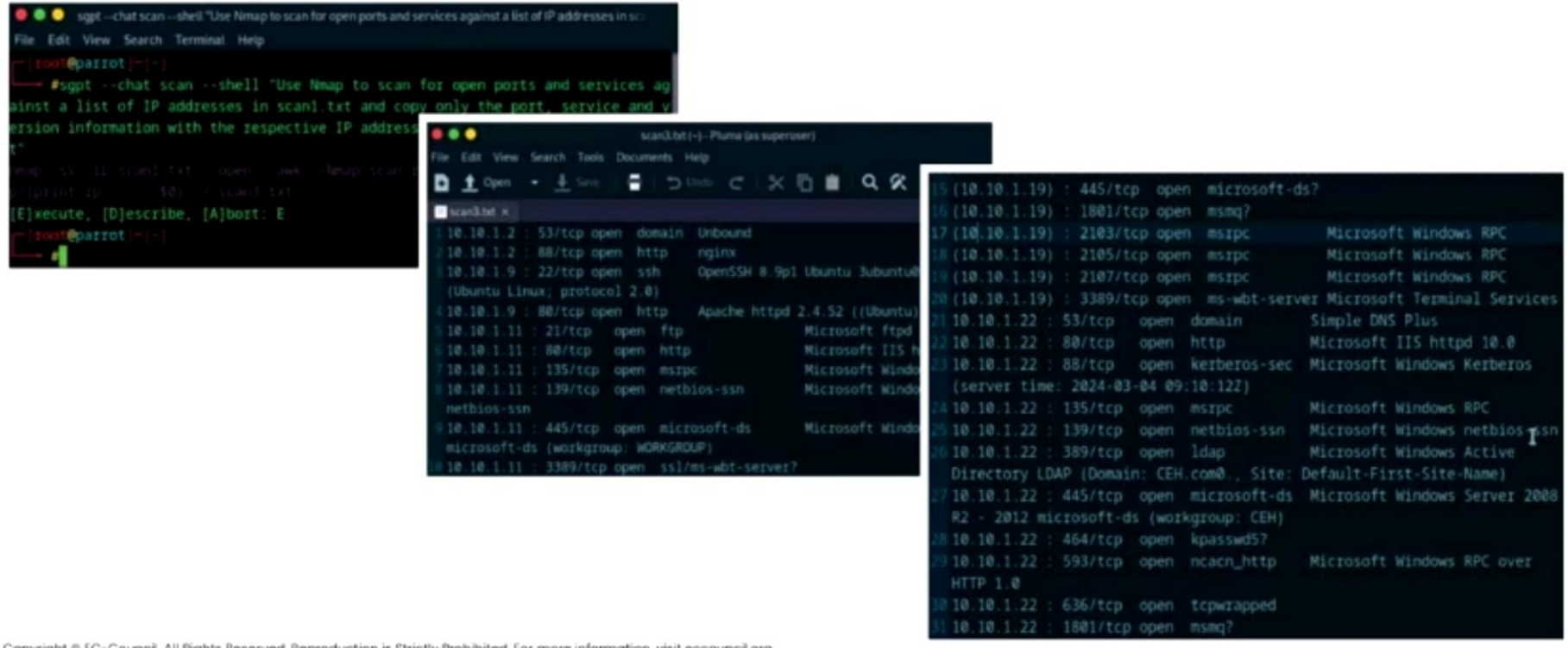
```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat sn --shell " Use Nmap to find open ports on target IP 10.10.1.11"
nmap 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-14 08:16 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00076s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --shell "Perform stealth scan on target IP 10.10.1.11 and display the results"
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 06:12 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00066s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 17.97 seconds
Stealth scan completed on 10.10.1.11
```

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --shell "Perform an XMAS scan on target IP 10.10.1.11"
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 06:22 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00044s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

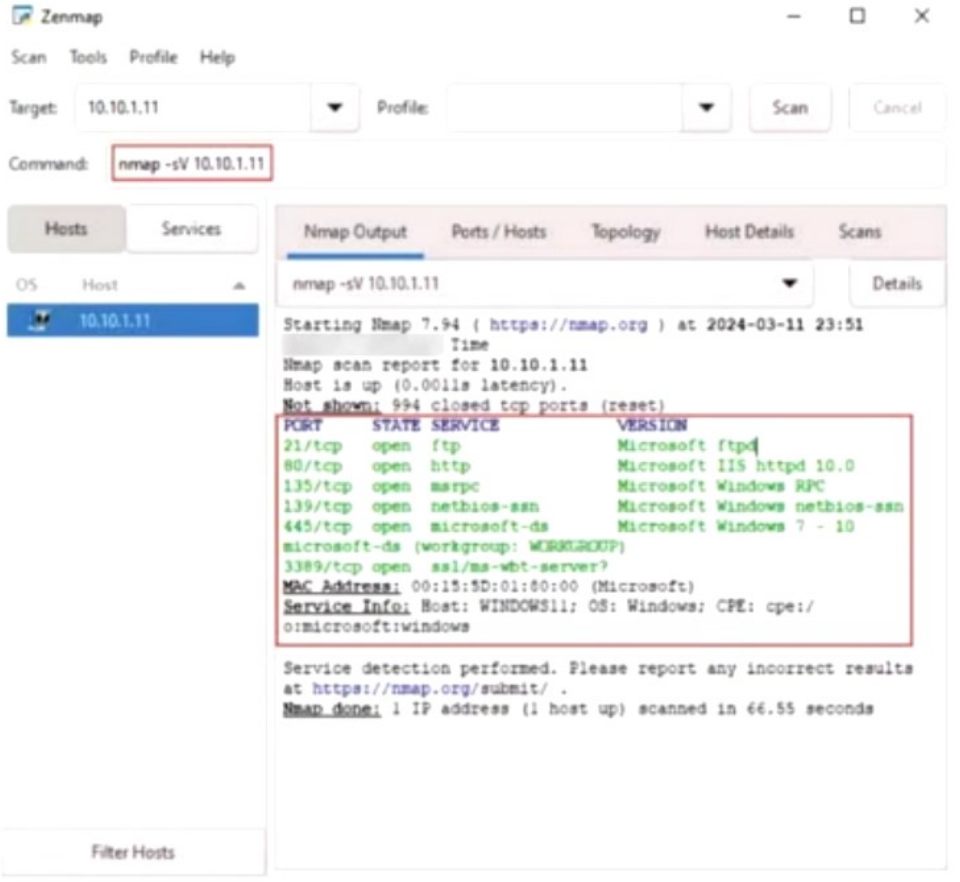
Port Scanning with AI (Cont'd)

- "Use Nmap to scan for open ports and services against a list of IP addresses in scan1.txt and copy only the port, service and version information with the respective IP address to a new file called scan3.txt"



Service Version Discovery

- Service version detection helps attackers to obtain information about running **services and their versions** on a target system
- Obtaining an accurate service version number allows attackers to **determine the vulnerability of target system to particular exploits**
- In Zenmap, the **-sV** option is used to detect service versions



https://nmap.org

Service Version Discovery with AI

An attacker can also leverage AI powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

- "Use Nmap to scan open ports, MAC details, services running on open ports with their versions on target IP 10.10.1.11"

```
└──╼ $sgpt --chat sn --shell "Use Nmap to scan open ports, MAC details, services
 running on open ports with their versions on target IP 10.10.1.11"
nmap -sV --reason -v -sT 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-14 09:20 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 09:20
```

```
Initiating NSE at 09:21
Completed NSE at 09:21, 0.04s elapsed
Initiating NSE at 09:21
Completed NSE at 09:21, 0.02s elapsed
Nmap scan report for 10.10.1.11
Host is up, received conn-refused (0.00047s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE            REASON  VERSION
21/tcp   open  ftp                syn-ack Microsoft ftpd
80/tcp   open  http               syn-ack Microsoft IIS httpd 10.0
135/tcp  open  msrpc              syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn        syn-ack Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       syn-ack Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
3389/tcp open  ssl/ms-wbt-server? syn-ack
Service Info: Host: WINDOWS11; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Objective 04

Demonstrate Various Scanning Techniques for OS Discovery

OS Discovery/Banner Grabbing

Banner grabbing or OS fingerprinting is the method used 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 possessed by the system** and the exploits that might work on a system to further **carry out additional attacks**

Active Banner Grabbing

- **Specially crafted packets** are sent to the remote OS and the responses are noted
- The responses are then compared with a database to **determine the OS**
- Responses from different OSes vary due to differences in the **TCP/IP stack implementation**

Passive Banner Grabbing

- **Banner grabbing from error messages**

Error messages provide information such as the type of server, type of OS, and SSL tool used by the target remote system.

- **Sniffing the network traffic**

Capturing and analyzing packets from the target enables an attacker to determine the OS used by the remote system.

- **Banner grabbing from page extensions**

Looking for an extension in the URL may assist in determining the application's version.

- Example: .aspx => IIS server and Windows platform

Note: We will discuss passive banner grabbing in later modules.

How to Identify Target System OS

- Attackers can identify the OS running on the target machine by looking at the **Time To Live (TTL)** and **TCP window size** in the IP header of the first packet in a TCP session
- **Sniff/capture the response** generated from the target machine using packet-sniffing tools like Wireshark and observe the TTL and TCP window size fields

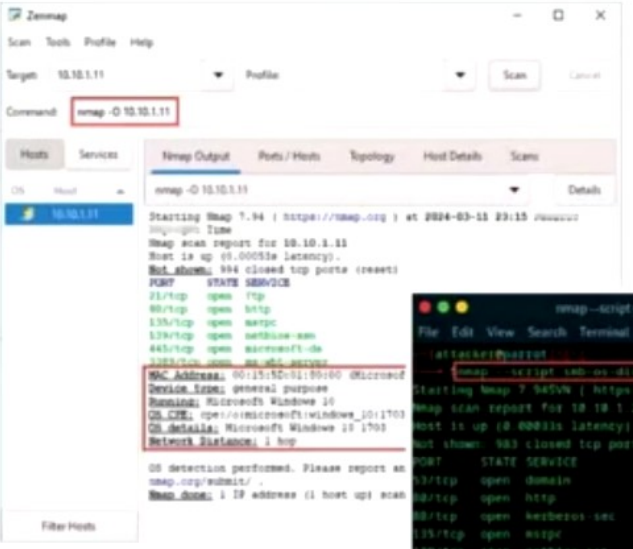
Window size values for OS

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

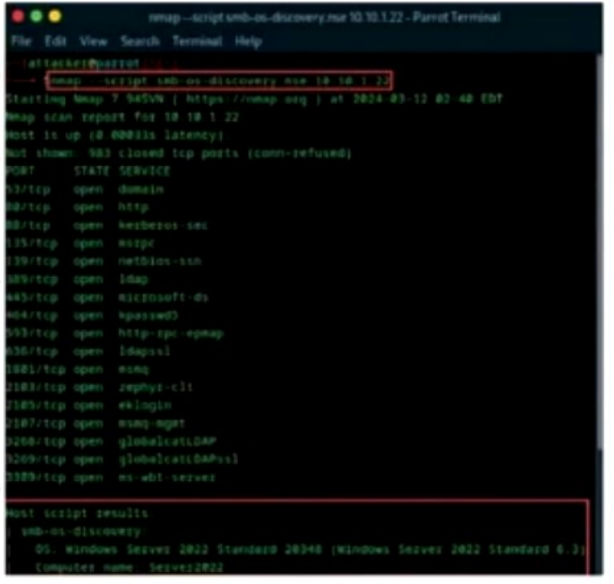
OS Discovery using Nmap and Nmap Script Engine

In **Nmap**, the **-O** option is used to perform OS discovery, providing OS details of the target machine

https://nmap.org



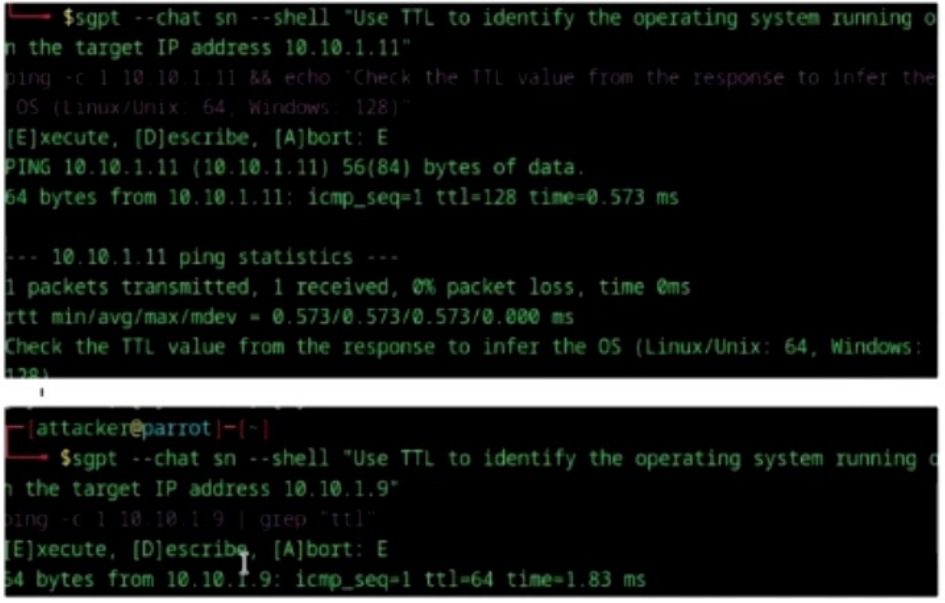
Nmap, **smb-os-discovery** is an inbuilt script that can be used for collecting OS information on the target machine through the **SMB protocol**



OS Discovery with AI

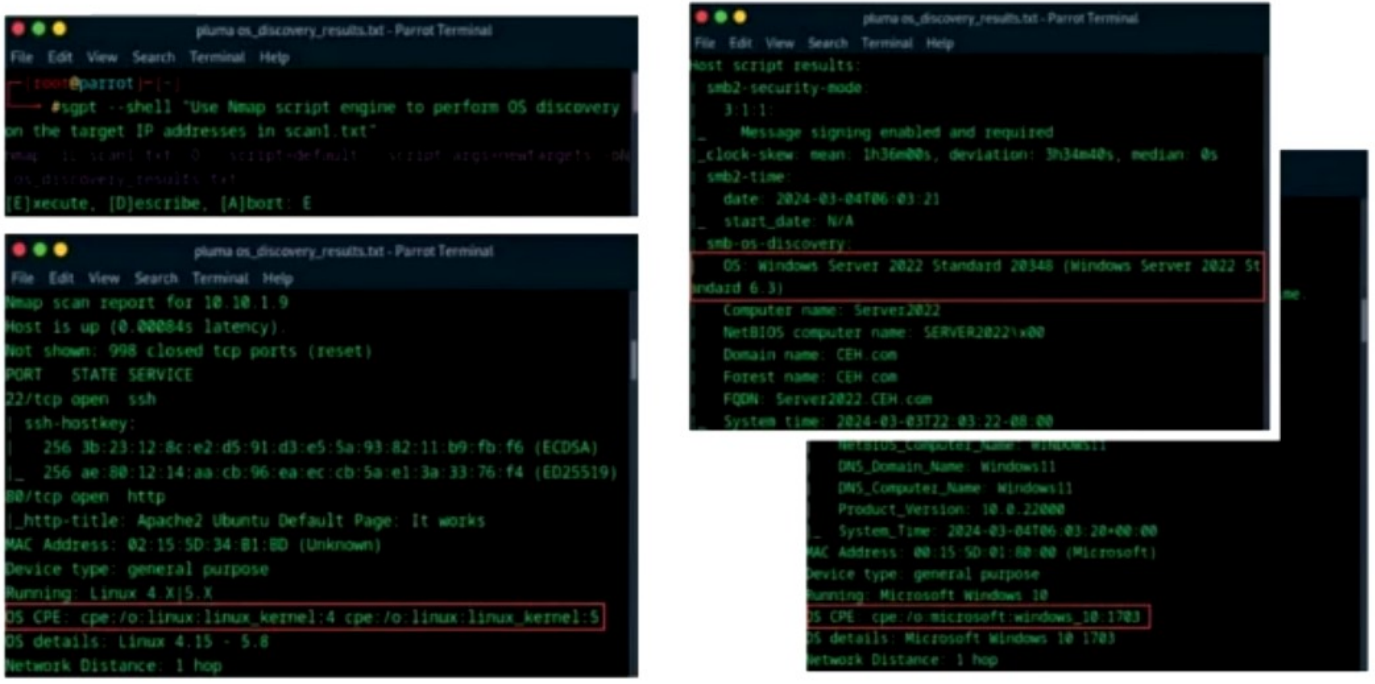
An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

- *"Use TTL to identify the operating system running on the target IP address 10.10.1.11"*
- *"Use TTL to identify the operating system running on the target IP address 10.10.1.9"*



OS Discovery with AI (Cont'd)

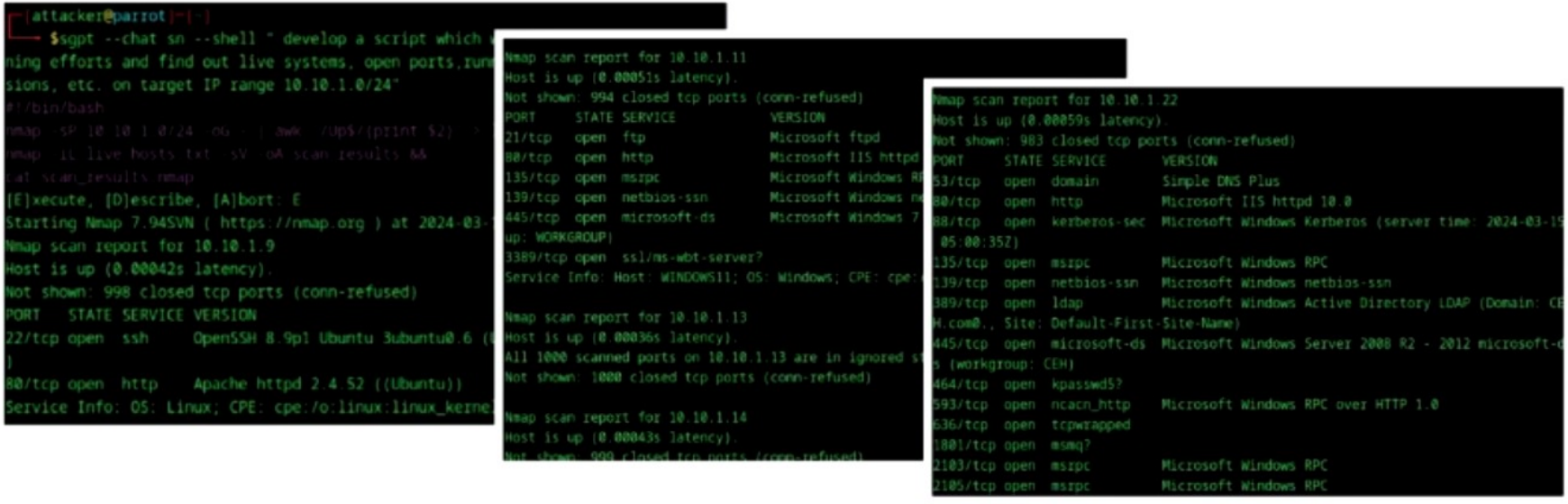
"Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt"



Create and Run Custom Script to Automate Network Scanning Tasks with AI

- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to automate various network scanning tasks by creating custom script that will run automatically and fetch the desired result. Attacker can use appropriate prompt like as follows to create custom scripts

"Develop a script which will automate network scanning efforts and find out live systems, open ports, running services, service versions, etc. on target IP range 10.10.1.0/24"

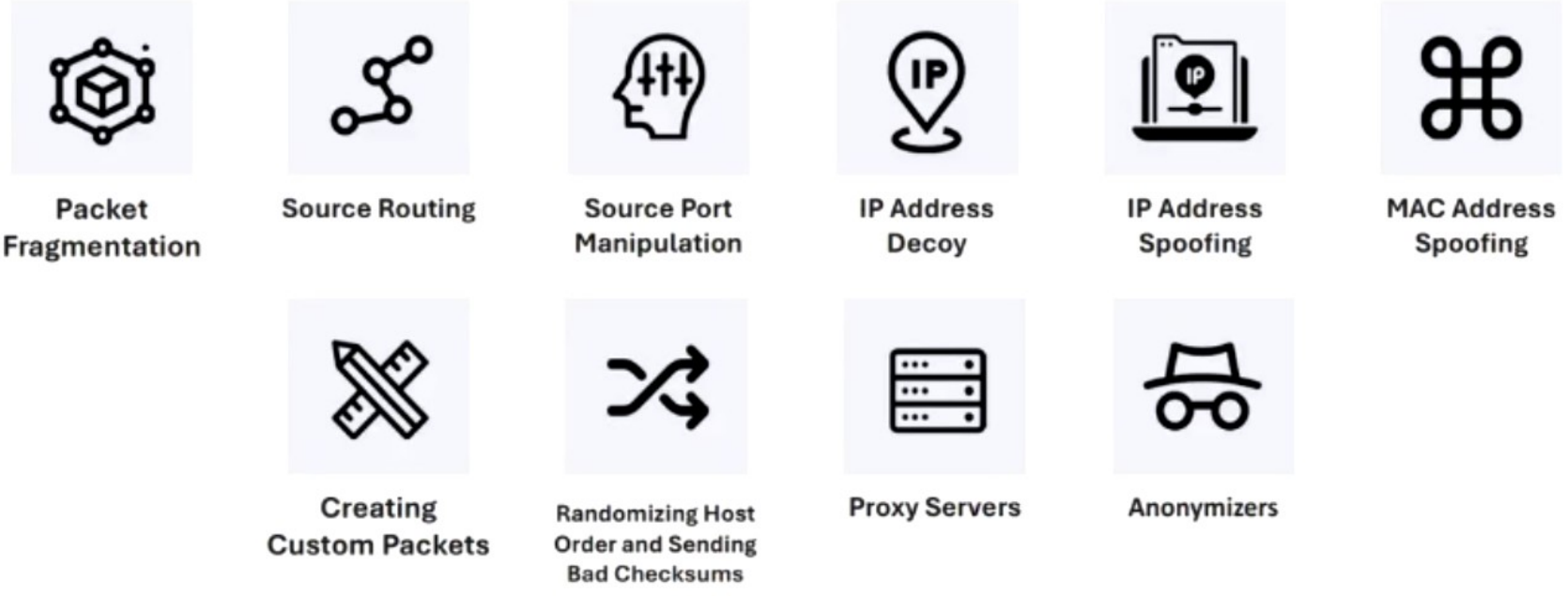


Objective 05

Demonstrate Various Techniques for Scanning Beyond IDS and Firewall

Scanning Beyond IDS and Firewall

Though firewalls and IDSs can prevent malicious traffic (packets) from entering a network, attackers can manage to **send intended packets to the target** by **evading an IDS or firewall** through the following techniques:

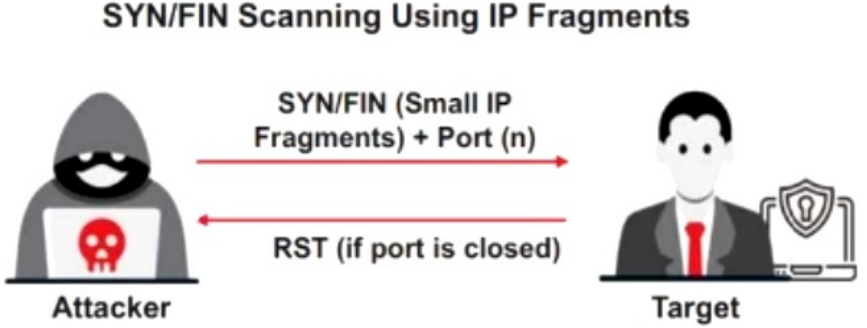


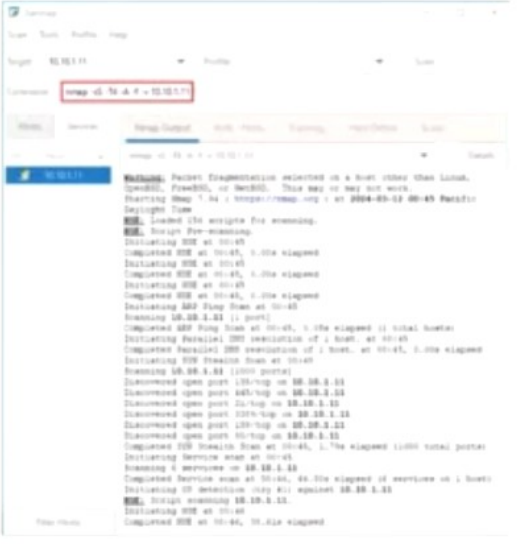
Packet Fragmentation

Packet fragmentation refers to the **splitting of a probe packet into several smaller packets** (fragments) while sending it to a network

It is not a new scanning method but a **modification** of the previous techniques

The **TCP header** is split into several packets so that the packet filters are not able to detect what the packets are intended to do

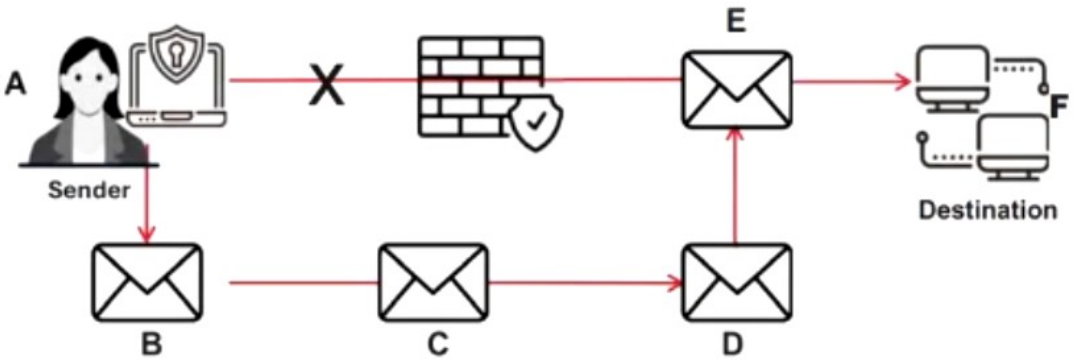




Source Routing

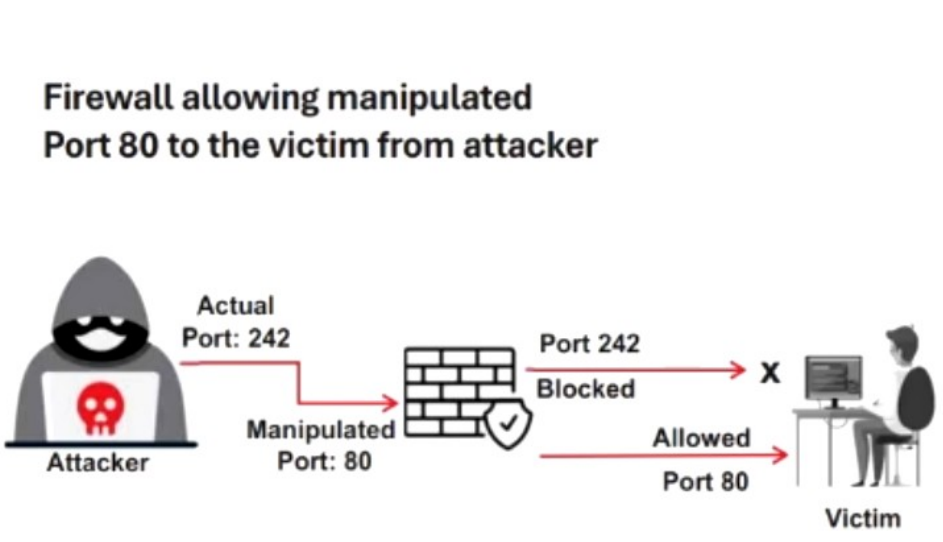
- As the packet travels through the nodes in the network, each **router examines** the destination IP address and **chooses the next hop** to direct the packet to the destination
- Source routing refers to sending a packet to the intended destination with a partially or completely **specified route** (without firewall-/IDS-configured routers) in order to evade an IDS or firewall
- In source routing, the **attacker** makes some or all of these decisions on the router

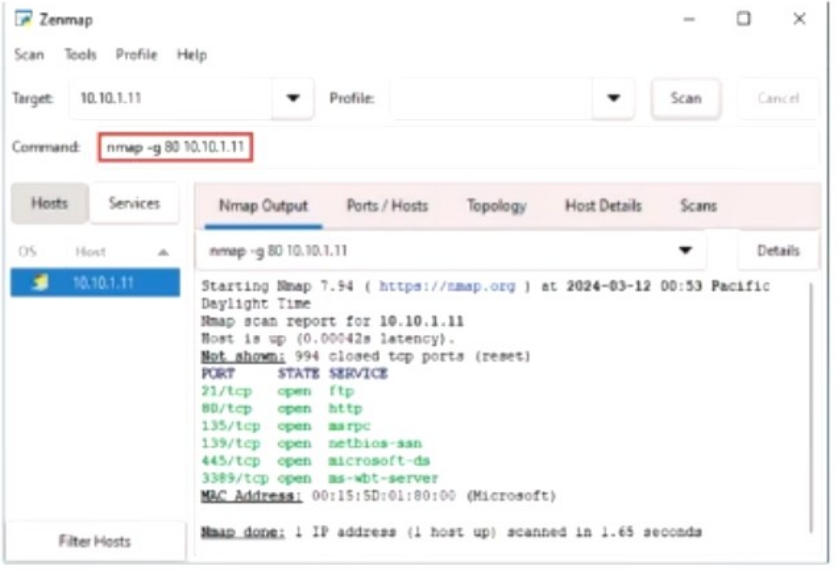
This figure shows source routing, where the originator dictates the eventual route of the traffic



Source Port Manipulation

- Source port manipulation refers to **manipulating actual port numbers with common port numbers** in order to evade an IDS or firewall
- It occurs when a firewall is **configured to allow packets** from well-known ports like HTTP, DNS, FTP, etc.
- **Nmap** uses the **-g** or **--source-port** options to perform source port manipulation





https://nmap.org

IP Address Decoy

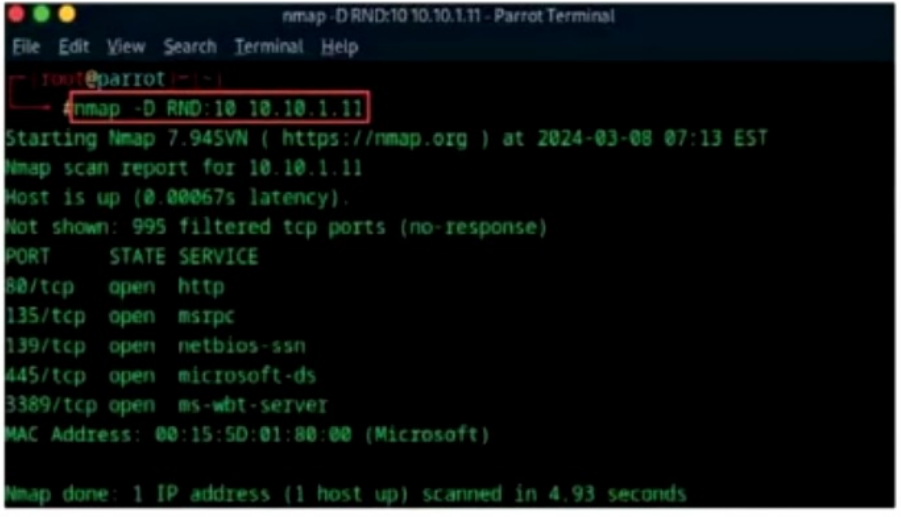
- IP address decoy technique refers to **generating or manually specifying the IP addresses of decoys** in order to evade an IDS or firewall
- It appears to the target that the **decoys as well as the host(s)** are scanning the network
- This technique makes it **difficult for the IDS or firewall to determine** which IP address was actually scanning the network and which IP addresses were decoys

Decoy Scanning using Nmap

Nmap has two options for decoy scanning:

`nmap -D RND:10 [target]`
(Generates a random number of decoys)

`nmap -D decoy1,decoy2,decoy3,..` etc.
(Manually specify the IP addresses of the decoys)



https://nmap.org

IP Address Spoofing

- IP spoofing refers to **changing the source IP addresses** so that the attack **appears to be coming from someone else**
- When the victim replies to the address, it goes back to the **spoofed address** rather than the **attacker's real address**
- Attackers modify the **address information** in the IP packet header and the source address bits field in order to bypass the IDS or firewall

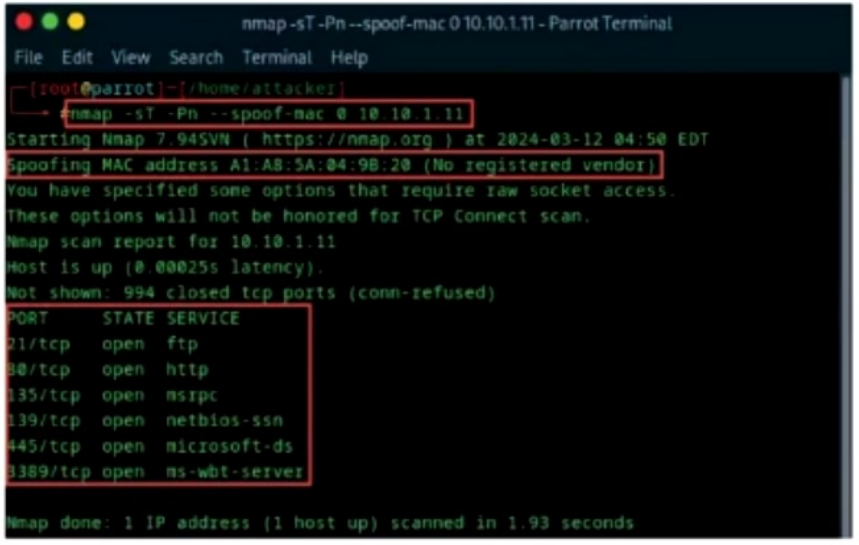
IP spoofing using Hping3:

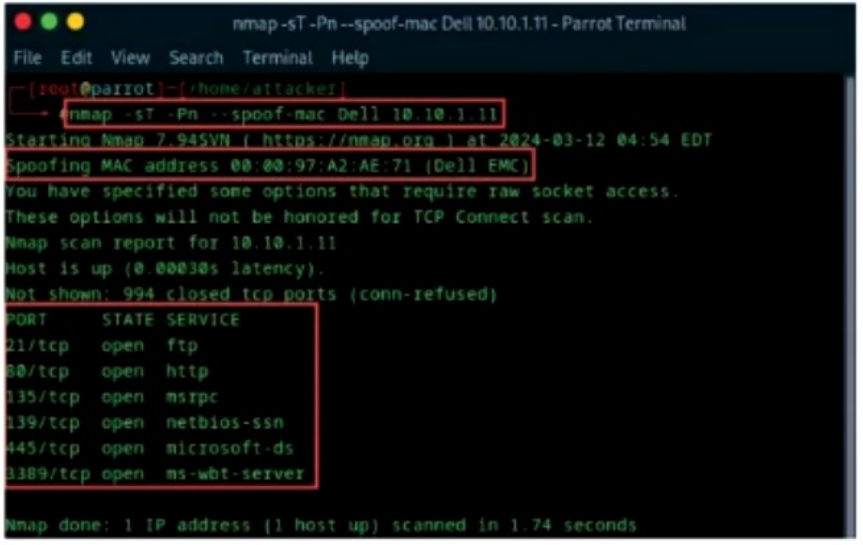
```
Hping3 www.certifiedhacker.com -a 7.7.7.7
```

Note: You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses

MAC Address Spoofing

- The MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network
- Attackers use the **--spoof-mac** Nmap option to set a specific MAC address for the packets to evade firewalls

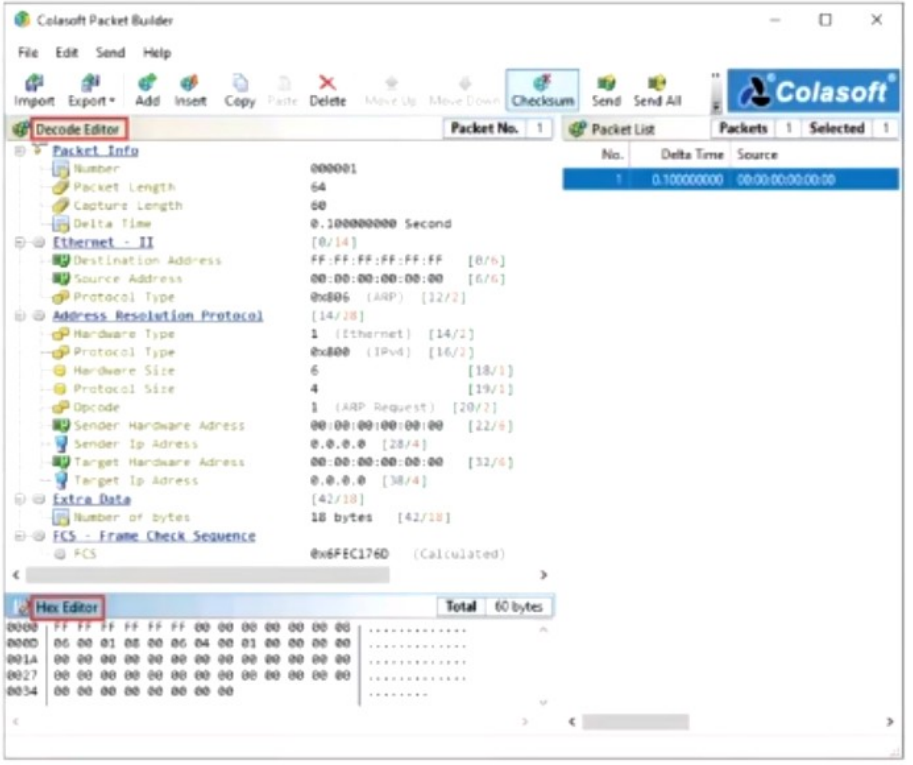




Creating Custom Packets

Creating Custom Packets by using Packet Crafting Tools

- Attackers **create custom TCP packets** using various packet crafting tools like **Colasoft Packet Builder**, **NetScanTools Pro**, etc. to scan a target beyond a firewall

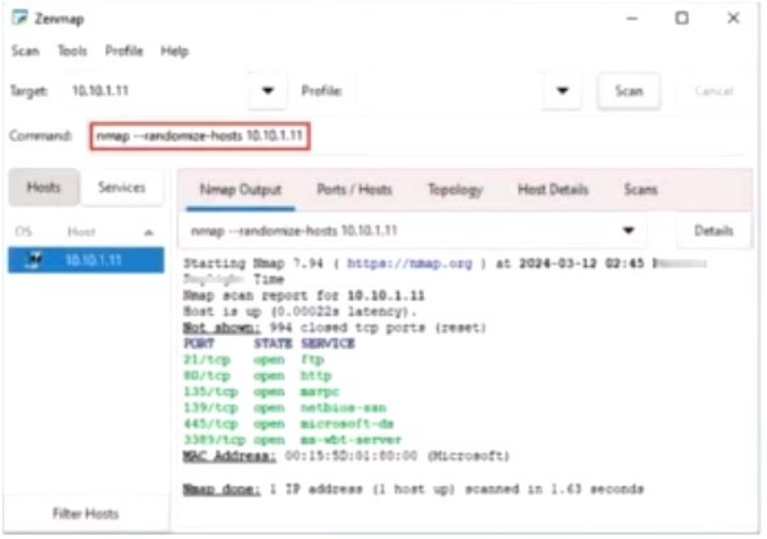


https://www.colasoft.com

Randomizing Host Order and Sending Bad Checksums

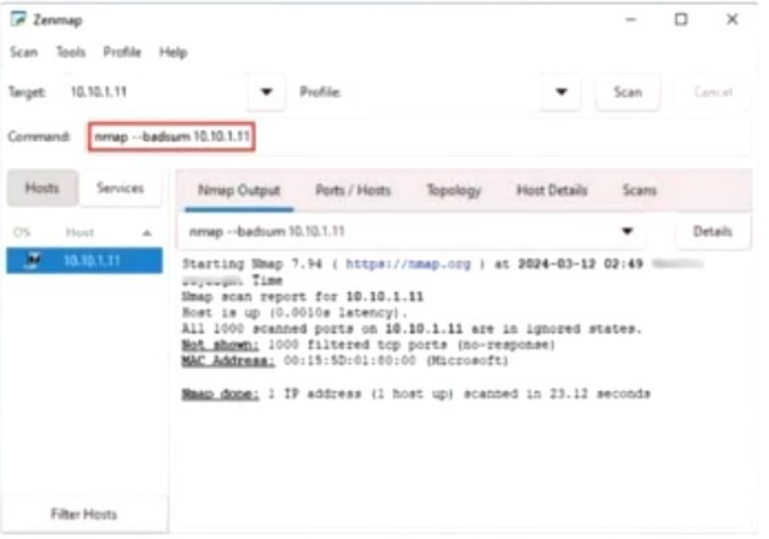
Randomizing Host Order

Attackers **scan the number of hosts** in the target network **in random order** to scan an intended target that is behind a firewall



Sending Bad Checksums

Attackers send packets with bad or bogus **TCP/UPD checksums** to the intended target to avoid certain firewall rulesets



https://nmap.org

Proxy Servers

A proxy server is an application that can serve as an intermediary for connecting with other computers

Why Attackers Use Proxy Servers?

1. To hide the actual source of a scan and **evade certain IDS/firewall restrictions**
2. To **mask the actual source** of an attack by impersonating the fake source address of the proxy
3. To **remotely access intranets** and other **website resources** that are normally restricted
4. To **interrupt all requests** sent by a user and transmit them to a third destination such that victims can only identify the proxy server address
5. To chain **multiple proxy servers** to avoid detection

Note: A search in **Google** will list thousands of **free proxy servers**

Objective 06

Explain Network Scanning Countermeasures

Ping Sweep Countermeasures

1. Configure firewalls to **block incoming ICMP echo requests** from unknown or untrusted sources
2. Use **intrusion detection systems** (IDSes) and **intrusion prevention systems** (IPSes), such as **Snort** to detect and prevent ping sweep attempts
3. Carefully evaluate the **type of ICMP traffic** flowing through enterprise networks
4. **Terminate** the connection with any host sending **more than 10 ICMP ECHO requests**
5. Use a DMZ and allow only commands such as **ICMP ECHO_REPLY**, **HOST UNREACHABLE**, and **TIME EXCEEDED** in the DMZ
6. **Limit ICMP traffic** with **access-control lists** (ACLs) to the ISP's specific IP addresses

Port Scanning Countermeasures

1. Configure **firewall** and **IDS rules** to detect and block probes
2. Run **port scanning tools** against hosts on the network to determine whether the firewall properly **detects port scanning activity**
3. Ensure that the mechanisms used for **routing** and **filtering** at the routers and firewalls, respectively, **cannot be bypassed** using a particular source port or source routing methods
4. Ensure that the **router**, **IDS**, and **firewall firmware** are updated to their latest releases/versions
5. Use a **custom rule set** to lock down the network and block **unwanted ports** at the firewall
6. Filter all **ICMP messages** (i.e., inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the **firewalls and routers**
7. Perform **TCP and UDP scanning** along with ICMP probes against your organization's IP address space to **check the network configuration and its available ports**
8. Ensure that **anti-scanning** and **anti-spoofing** rules are properly configured

Banner Grabbing Countermeasures

Disabling or Changing Banner

- Display **false banners** to mislead or deceive attackers
- **Turn off unnecessary services** on the network host to limit the disclosure of information
- Use server masking tools to disable or change banner information
- For Apache 2.x with the `mod_headers` module, use a directive in the `httpd.conf` file to change the banner information header and set the server as `New Server Name`
- Alternatively, change the `ServerSignature` line to `ServerSignature Off` in the `httpd.conf` file

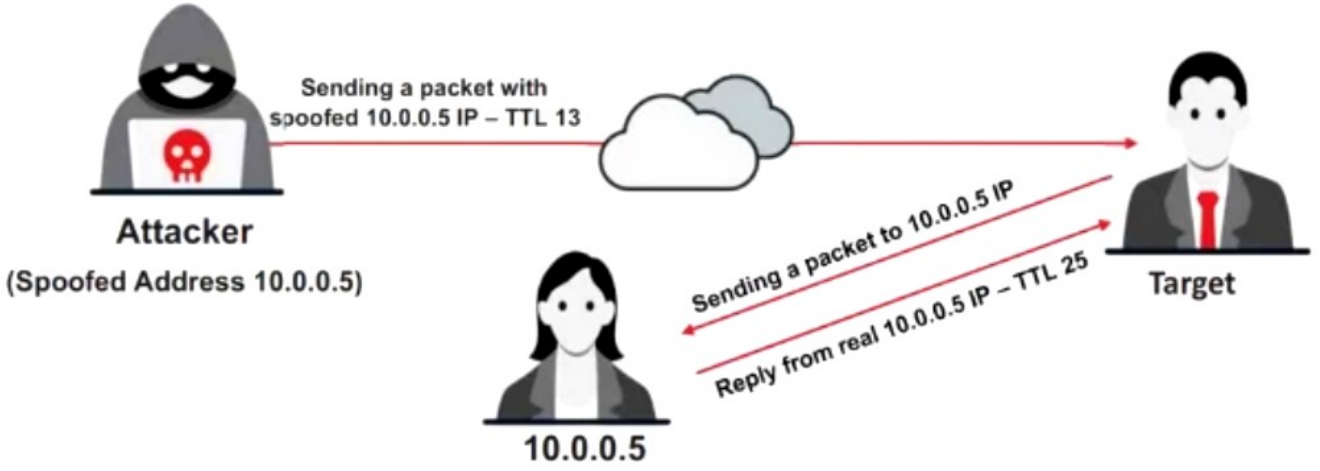
Hiding File Extensions from Web Pages

- File extensions reveal information about the **underlying server technology** that an attacker can utilize to launch attacks
- Hide file extensions to **mask the web technologies**
- Replace **application mappings** such as .asp with .htm or .foo, etc. to disguise the identities of servers
- Apache users can use `mod_negotiation` directives

✓ **It is preferable to not use file extensions at all**

IP Spoofing Detection Techniques: Direct TTL Probes

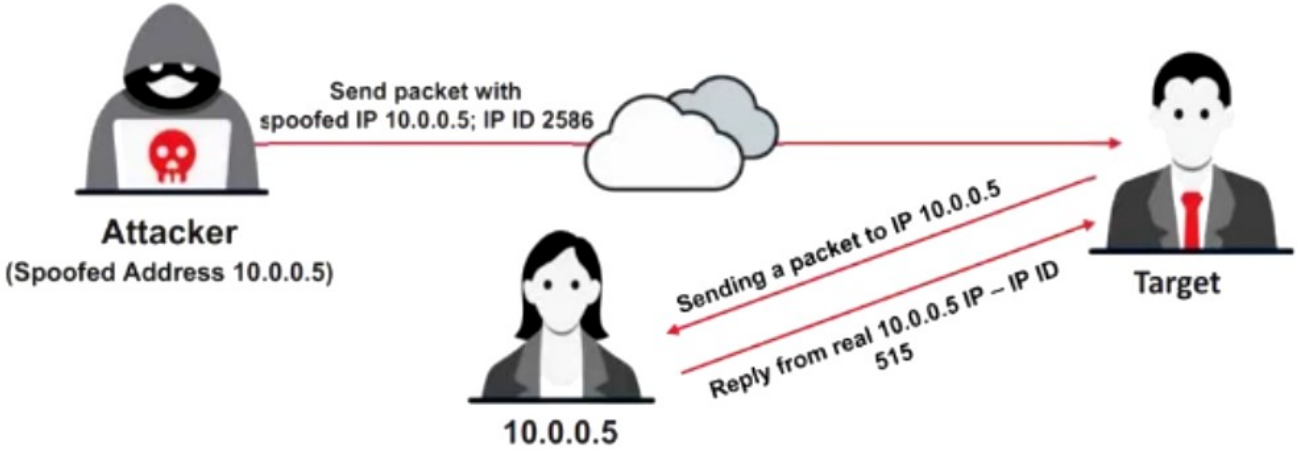
- Send a packet to the host of a suspected spoofed packet that triggers a reply and compare the TTL with that of the suspected packet; if the **TTL in the reply is not the same** as the packet being checked, this implies that it is a spoofed packet
- This technique is successful when the attacker is in a **different subnet** from that of the victim



Note: Normal traffic from one host can contrast TTLs depending on traffic patterns

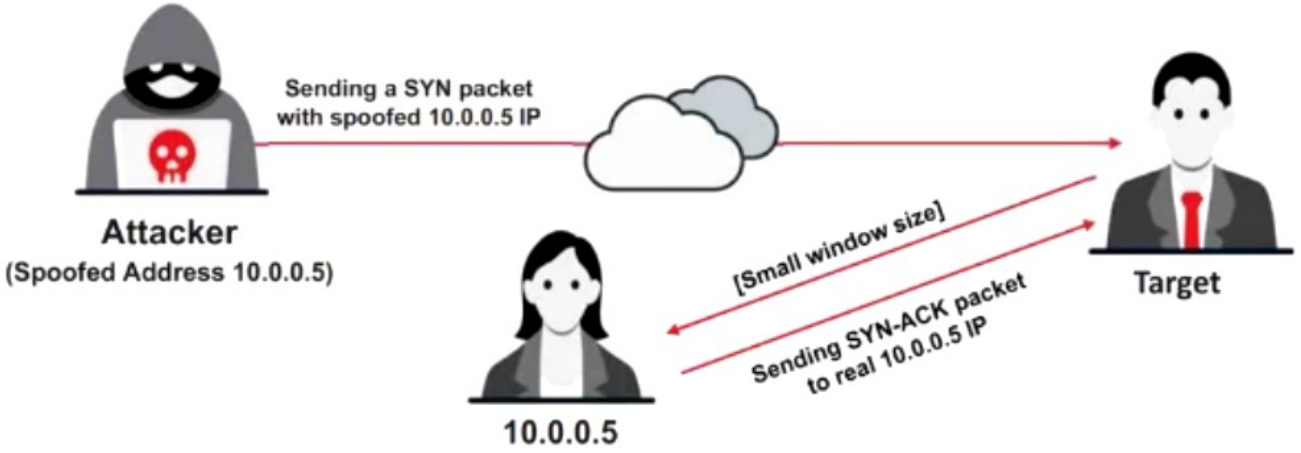
IP Spoofing Detection Techniques: IP Identification Number

1. Send a probe to the host of a suspected spoofed traffic that triggers a reply and **compare the IPID** with the suspected traffic
2. If the IPIDs are **not close in value** to the packet being checked, then the suspected traffic is spoofed
3. This technique is considered reliable even if the attacker is in the **same subnet**



IP Spoofing Detection Techniques: TCP Flow Control Method

1. Attackers sending spoofed TCP packets will not receive the **target's SYN-ACK packets**
2. Therefore, attackers cannot respond to a change in the congestion window size
3. When received traffic continues after a window size is exhausted, the **packets are most likely spoofed**



IP Spoofing Countermeasures

1. **Encrypt all the network traffic** using cryptographic network protocols such as IPsec, TLS, SSH, and HTTPS
2. **Use multiple firewalls** to provide a multi-layered depth of protection
3. Do not rely on **IP-based authentication**
4. **Use a random initial sequence number** to prevent IP spoofing attacks based on sequence number spoofing
5. **Ingress Filtering**: Use routers and firewalls at your network perimeter to filter incoming packets that appear to come from an internal IP address
6. **Egress Filtering**: Filter all outgoing packets with an invalid local IP address as the source address

Module Summary

- In this module, we have discussed the following:
  - How attackers discover live hosts from a range of IP addresses by sending various ping scan requests to multiple hosts
  - How attackers perform different scanning techniques to determine open ports, services, service versions, etc. on the target system
  - How attackers perform banner grabbing or OS fingerprinting to determine the operating system running on a remote target system
  - Various scanning techniques that attackers can employ to bypass IDS/firewall rules and logging mechanisms, and disguise themselves as regular network traffic
  - Network scanning countermeasures to defend against network scanning attacks
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform enumeration to collect information about a target before an attack or audit