

Module-3

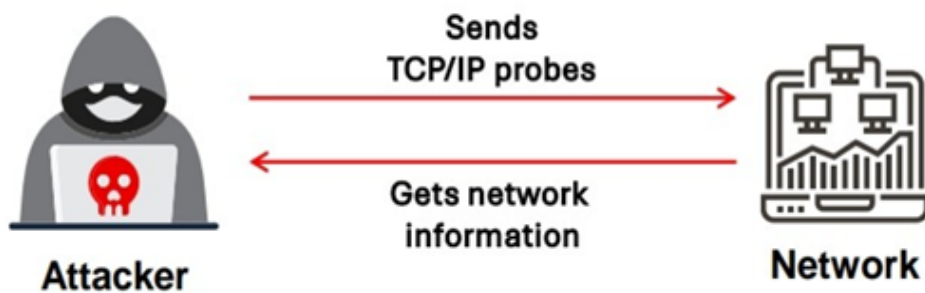
Scanning Network

What is network Scanning

- Network scanning is the process of troubleshooting the active devices on your system for vulnerabilities. It identifies and examines the connected devices by deploying one or more features in the network protocol.

How to work Network Scanning process

Network Scanning Process



Types of Scanning

Port Scan

- **Purpose:** Identifies open ports on a target system.
- **How it works:** Scans a range of ports (TCP or UDP) on a device to determine which are open and which services are running.
- **Common tools:**
- **Used for:** Mapping out services running on a device to assess vulnerabilities.

Vulnerability Scan

- **Purpose:** Identifies known vulnerabilities in a system.
- **How it works:** Scans for outdated software, unpatched systems, and security weaknesses based on vulnerability databases.
- **Common tools:** Nmap, Hping3
- **Used for:** Assessing security flaws and risks in a network or system.

Network Scanning

- **Purpose:** To identify devices and resources on a network
- **How it Work:** Network scanning tools help map out the network by discovering active devices, their IP addresses, and other characteristics (e.g., device type, operating system).
- **Common tools** namp

Used for **Network Device Scanner**. Ensure **network** visibility **using** Lansweeper's IP **scanning** tool. Fast & Reliable IP **scanner** that discovers all devices on your **network** by **scanning** IP range [Manage Asset Lifecycle](#)

Exercise 1

Scanning tools using

1 nmap

2 zenmap

3 hping3

1 nmap: Nmap is an open-source network scanning and host discovery tool, which was created by Gordon Lyon and has been actively developed and maintained over two decades.

2 Zenmap: is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners

3hping3: hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size.

What is Host Discover

This host discovery method

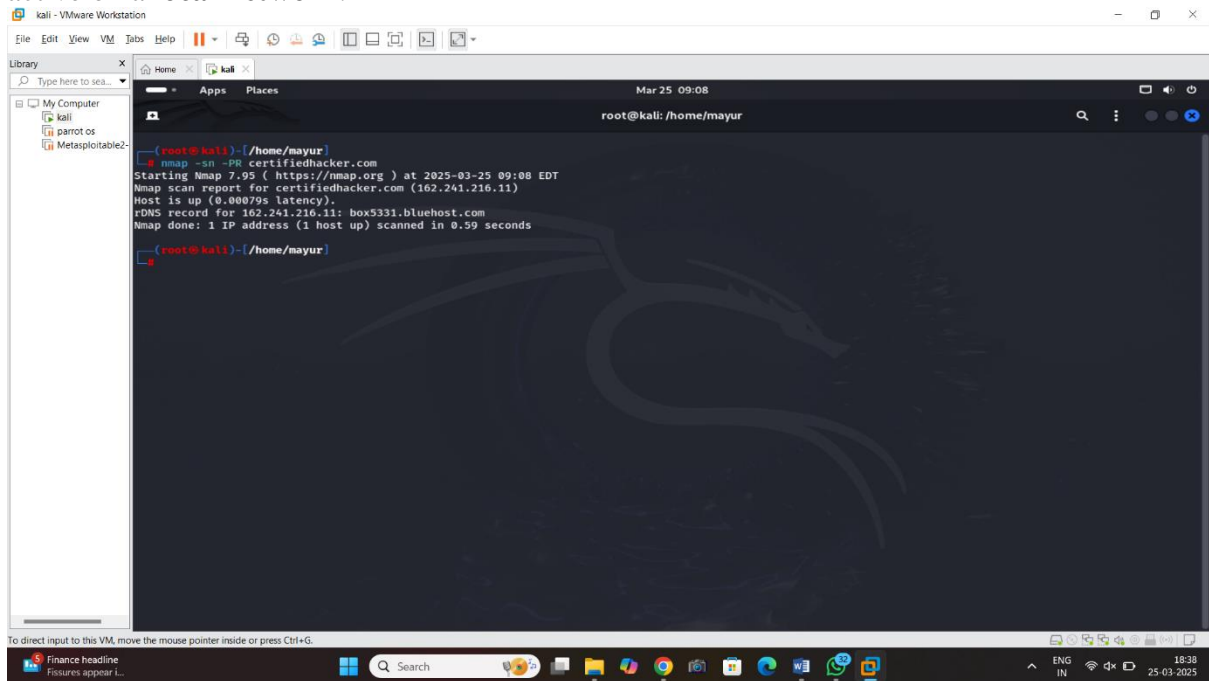
looks for either responses using the same protocol as a probe, or ICMP protocol unreachable messages which signify that the given protocol isn't supported using

PING Scanning Using nmap

1 ARP Ping Scan (-PR)

Command use: `nmap -sn -PR certifiedhacker.com`

Explanation: An **ARP Ping Scan** is a technique used to find out which devices are currently active on a **local network**.



The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the execution of the command `nmap -sn -PR certifiedhacker.com`. The output indicates that Nmap 7.95 is starting at 2025-03-25 09:08 EDT. It reports that the host is up with a latency of 0.00079s. A DNS record for 162.241.216.11 is shown as box5331.bluehost.com. The scan is completed in 0.59 seconds, identifying 1 IP address (1 host up).

```
(root@kali) ~/home/mayur
nmap -sn -PR certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 09:08 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.00079s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds

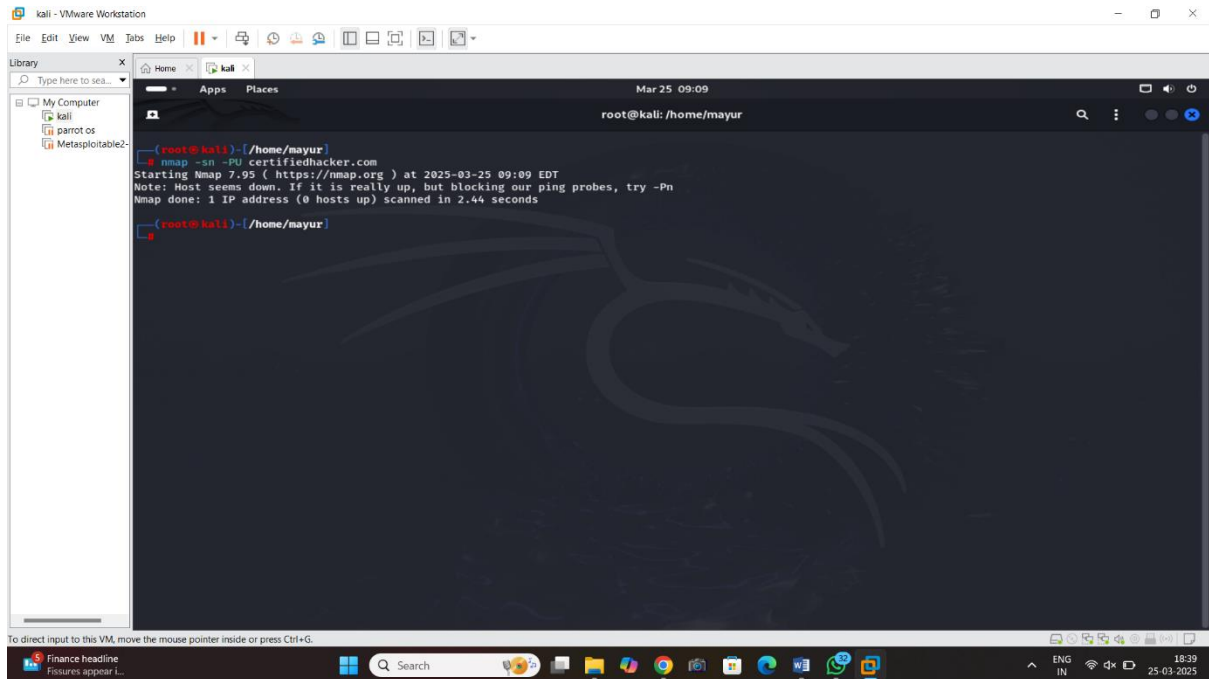
(root@kali)~/home/mayur
```

- **Description:**
 - Network inventory discovery
 - Checking live hosts when ICMP is blocked
 - Mapping IP-to-MAC addresses for security auditing

UDP Ping Scan

Command: `nmap -sn -PU certifiedhacker.com`

Explanation: A **UDP Ping Scan** is a network scanning technique used to discover active hosts by sending **UDP packets** to specific ports and waiting for a response



The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the execution of the command `nmap -sn -PU certifiedhacker.com`. The output indicates that Nmap 7.95 is starting at 2025-03-25 09:09 EDT. It notes that the host seems down but suggests trying `-Pn` if it's really up but blocking ping probes. The scan is completed, showing 1 IP address scanned in 2.44 seconds.

```
(root@kali)~/home/mayur
# nmap -sn -PU certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 09:09 EDT
Notes: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.44 seconds

(root@kali)~/home/mayur
#
```

Description:

Protocol: UDP (User Datagram Protocol)

Detection method: Waits for ICMP "port unreachable" or no response

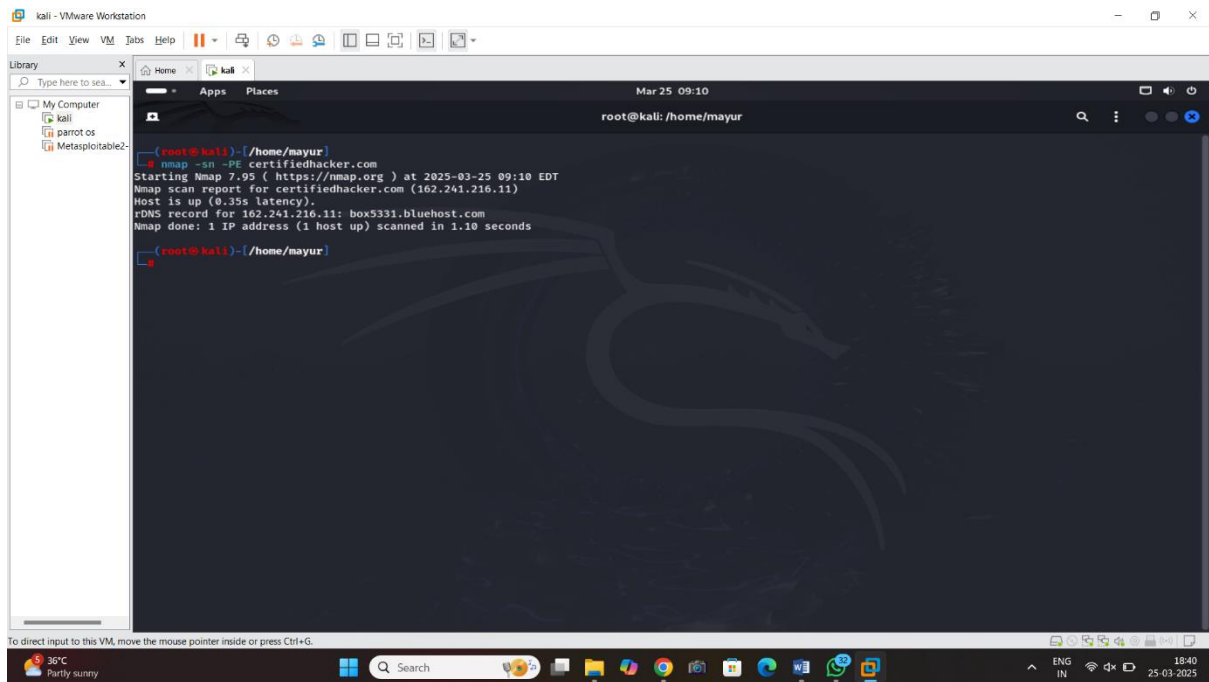
Speed: Slower than ARP or ICMP scans, due to wait times and lack of responses

Accuracy: Less accurate (UDP may not reply at all), more guesswork involved

3 Icmp Ping Scan

Command : `nmap -sn -PE certifiedhacker.com`

Explaination: An **ICMP Ping Scan** is a common network scanning method used to find live hosts by sending **ICMP Echo Request** packets (like the `ping` command) and waiting for **ICMP Echo Replies**.



The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the output of the command `nmap -sn -PE certifiedhacker.com`. The output indicates that the scan was successful, identifying the host as `162.241.216.11` and `box5331.bluehost.com`. The terminal also shows the nmap version (7.95) and the scan time (2025-03-25 09:10 EDT). The terminal window is titled `root@kali: /home/mayur` and the date/time is `Mar 25 09:10`. The terminal background features a Kali Linux dragon logo.

```
root@kali: /home/mayur
nmap -sn -PE certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 09:10 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.35s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
root@kali: /home/mayur
```

Discription:

Protocol: ICMP (Internet Control Message Protocol)

Purpose: To check if a host is up and reachable

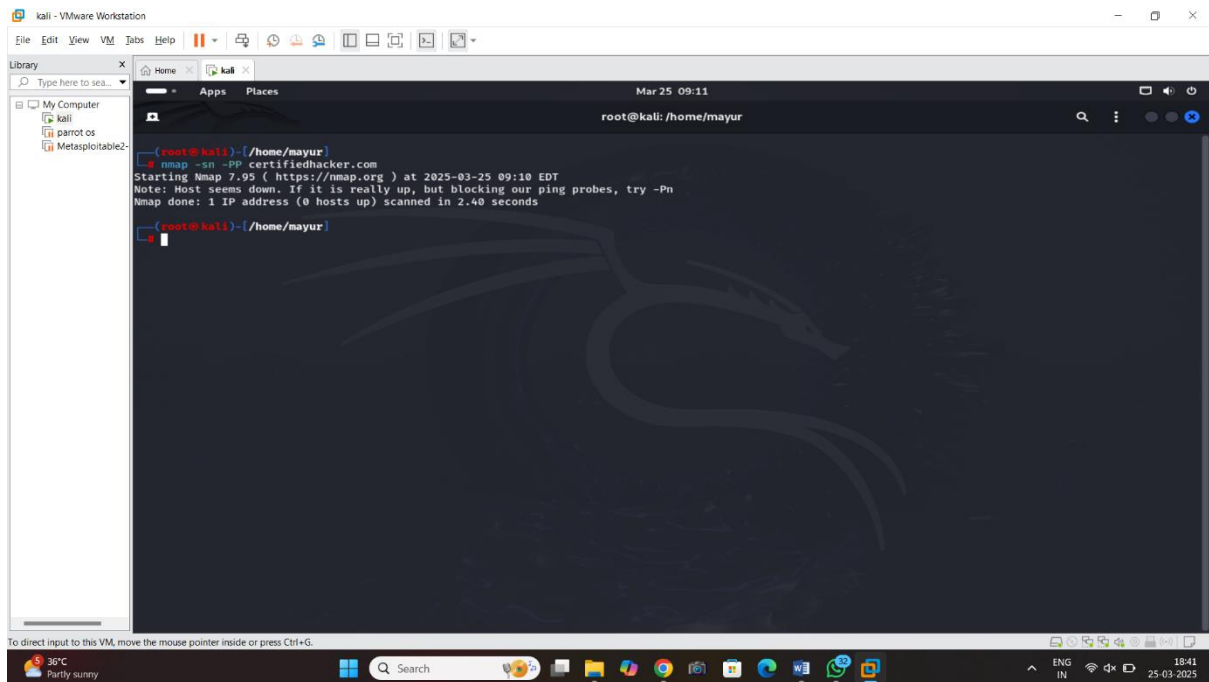
Speed: Fast and efficient for large networks

Detection method: Direct Echo Reply from the target host

4 Icmp Time Stamp Ping scan

Command: `nmap -sn -PP certifiedhacker.com`

Explanation: **ICMP Timestamp Ping** — sends ICMP Timestamp Requests to check if hosts are alive.



Discription:

Can bypass situations where standard ICMP Echo Requests are blocked.

To check if a host is up and responding.

Sometimes used for operating system fingerprinting or timing analysis.

5ICMP Address Mask Ping Scan

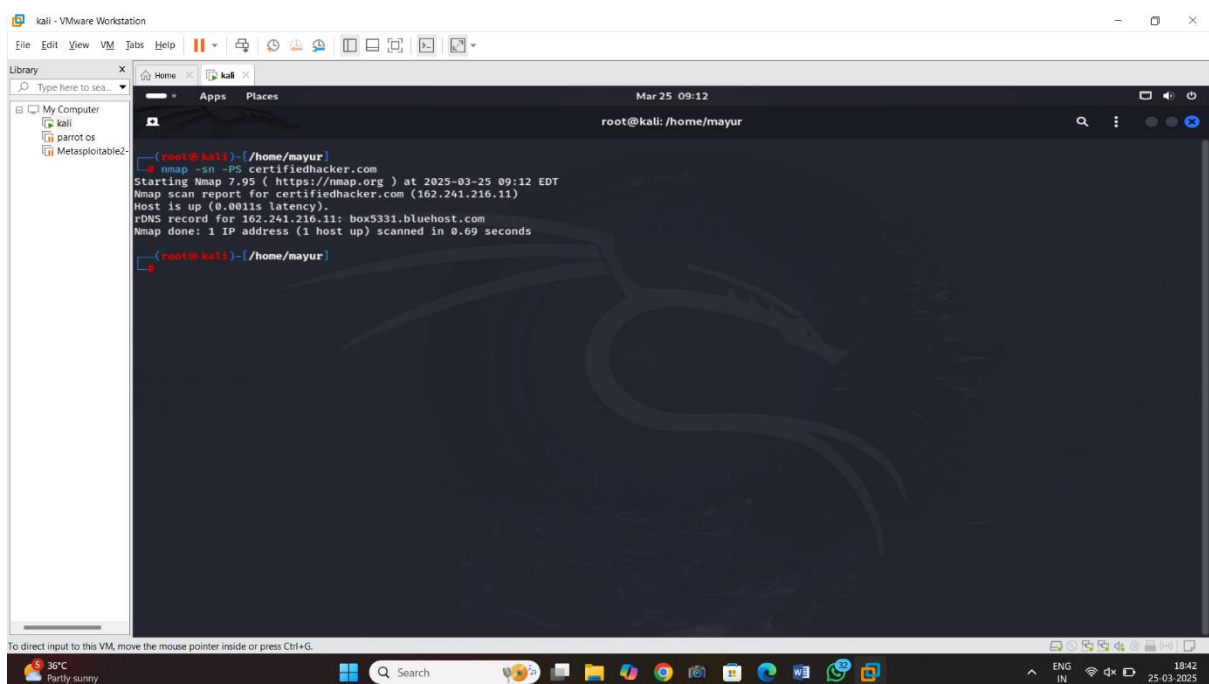
Cammand: `nmap -sn -PM certifiedhacker.com`

Exercise 2

TCP SYN Ping

Command: `nmap -sn -PY certifiedhacker.com`

Explanation: is a type of host discovery technique where the scanner sends **TCP SYN packets** (the first packet in a TCP handshake) to specific ports and waits for a response to determine if the host is alive.



```
(root@kali)~/home/mayur
$ nmap -sn -PY certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 09:12 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.0011s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
(root@kali)~/home/mayur
```

Description:

Protocol TCP (Transmission Control Protocol)

Packet sent: TCP SYN packets

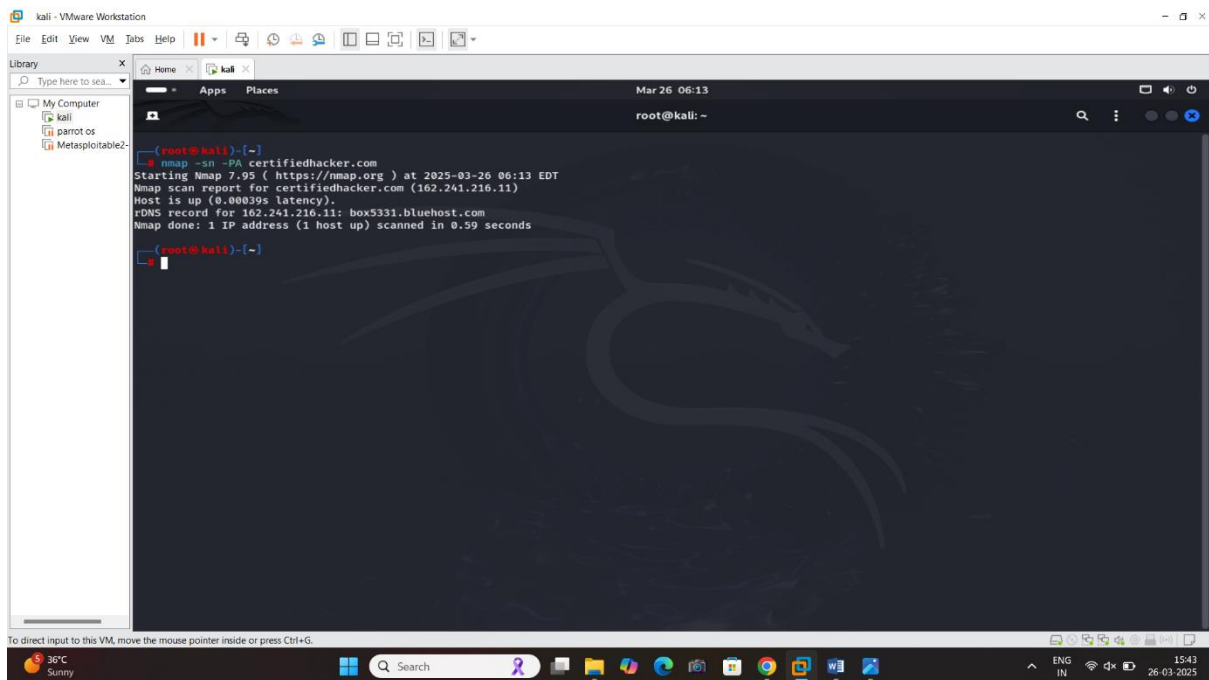
Purpose: Discover live hosts by checking TCP responsiveness

Useful for firewalled environments that only allow certain TCP ports.

TCP ACK ping Scan

Command: `nmap -sn -PA certifiedhacker.com`

Explanation: A **TCP ACK Ping Scan** is a network scanning technique used to determine whether a host is up by sending TCP packets with the ACK flag set and analyzing the responses.



```
root@kali:~# nmap -sn -PA certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 06:13 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.00039s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

Description:

A TCP packet with the ACK flag is sent to a target host on a specified port.

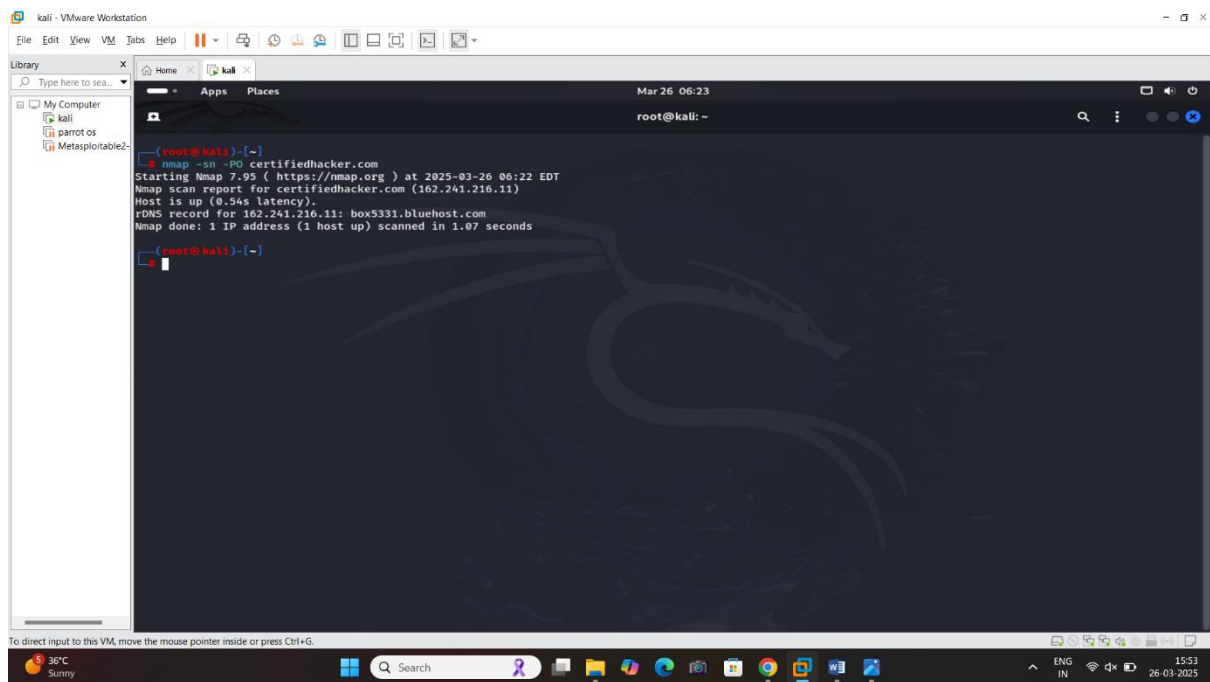
If the host is up and the port is closed, the host will typically respond with a **RST (reset)** packet.

If there is no response, or if an ICMP unreachable message is received, it might indicate that the host is down or that a firewall is blocking the packet.

IP protocol ping Scan

Command: `nmap -sn -PO certifiedhacker.com`

Explanation: An **IP Protocol Ping Scan** is a scanning method used to determine if a host is up by sending packets with various **IP protocol numbers** (instead of TCP, UDP, or ICMP) and observing responses.



The screenshot shows a Kali Linux terminal window within a VMware Workstation environment. The terminal displays the output of the command `nmap -sn -PO certifiedhacker.com`. The output indicates that Nmap 7.95 is running at 2025-03-26 06:22 EDT. It reports that the host is up with a latency of 0.34s. The rDNS record for the IP address 162.241.216.11 is identified as box5331.bluehost.com. The scan was completed in 1.07 seconds, identifying 1 IP address as up.

```
(root@kali)~# nmap -sn -PO certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 06:22 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.34s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
(root@kali)~#
```

Description:

An **IP Protocol Ping Scan** is a scanning method used to determine if a host is up by sending packets with various **IP protocol numbers** (instead of TCP, UDP, or ICMP) and observing responses.

Port and Service Discovery

What is port Discovery

Port Discovery refers to the process of finding **open, closed, or filtered ports** on a target system. It's a key part of network reconnaissance and vulnerability assessment, helping you understand which services are running and potentially exploitable.

Types of ports Scanning

1 TCP Port Scanning

2 NON TCP AND UDP Port Scanning

TCP Port Scanning

1 TCP Scan (full Scan)

Cammand: nmap -v -sT certifiedhacker.com

Explanation: TCP Full Scan, also known as a **TCP Connect Scan**, is a scanning technique where the scanner attempts to **fully establish a TCP connection (three-way handshake)** with the target port to check whether it's open, closed, or filtered

The image shows a VMware Workstation window titled "kali - VMware Workstation". Inside the VM, a terminal window is open with the prompt "root@kali: ~". The terminal displays the output of an nmap scan: "nmap -v -sT certifiedhacker.com", "Starting Nmap 7.95 (https://nmap.org) at 2025-03-26 06:53 EDT", "Initiating Ping Scan at 06:53", "Scanning certifiedhacker.com (162.241.216.11) [4 ports]", "Completed Ping Scan at 06:53, 0.89s elapsed (1 total hosts)", "Initiating Parallel DNS resolution of 1 host. at 06:53", "Completed Parallel DNS resolution of 1 host. at 06:53, 0.06s elapsed", "Initiating Connect Scan at 06:53", "Scanning certifiedhacker.com (162.241.216.11) [1000 ports]", "Completed Connect Scan at 06:53, 22.82s elapsed (1000 total ports)", "Nmap scan report for certifiedhacker.com (162.241.216.11)", "Host is up (0.0011s latency).", "RDNS record for 162.241.216.11: box533i-bluehost.com", "All 1000 scanned ports on certifiedhacker.com (162.241.216.11) are in ignored states.", "Not shown: 1000 filtered tcp ports (no-response)", "Read data files from: /usr/share/nmap", "Nmap done: 1 IP address (1 host up) scanned in 23.14 seconds", "Raw packets sent: 4 (152B) | Rcvd: 1 (40B)". The terminal also shows several prompt changes: "(root@kali).-[-]", "(root@kali).-[-]", "(root@kali).-[-]", "(root@kali).-[-]", "(root@kali).-[-]", "(root@kali).-[-]", "(root@kali).-[-]". The VMware interface includes a "Library" pane on the left showing "My Computer" with icons for "kali", "parrot os", and "Metasploitable2". The top of the terminal window shows "Mar 26 06:54" and "root@kali: ~". The bottom of the image shows the Windows taskbar with a search bar, task view button, and various application icons, along with system tray icons for temperature (37°C), weather (Sunny), and time (16:24, 26.03.2022).

Description:

SYN (Synchronize): The scanner sends a SYN packet to a target port.

SYN-ACK (Synchronize-Acknowledge): If the port is open, the target replies with a SYN-ACK.

ACK (Acknowledge): The scanner responds with an ACK, completing the handshake.

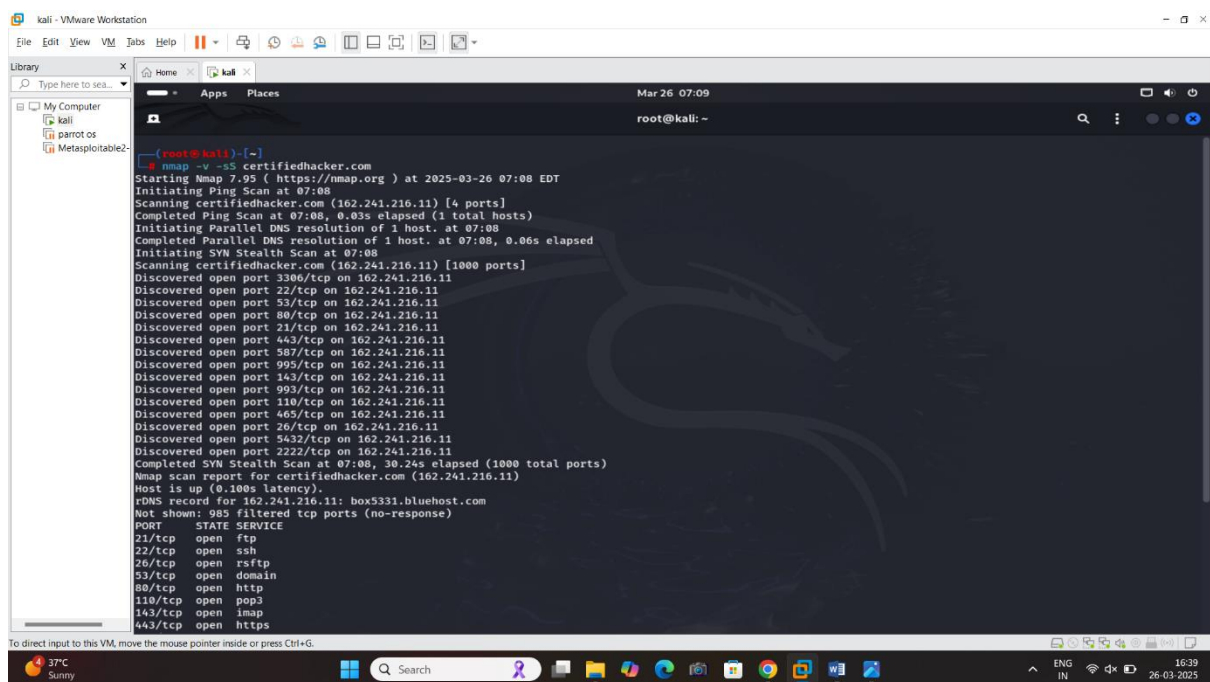
Connection Closure: The scanner may send a FIN or RST to terminate the connection.

2 Half Scan (s-S)

(Steath Scan , Half Scan , Hidden Scan)

Cammand: `nmap -v -sS certifiedhacker.com`

Explination: The **TCP Half Scan**, also called a **SYN scan**, is one of the most popular and efficient scanning methods. It's often referred to as a **stealth scan** because it never fully completes the TCP handshake — it stops after the SYN-ACK response



```
root@kali: ~# nmap -v -sS certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 07:08 EDT
Initiating Ping Scan at 07:08
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 07:08, 0.035s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:08
Completed Parallel DNS resolution of 1 host. at 07:08, 0.00s elapsed
Initiating SYN Stealth Scan at 07:08
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Discovered open port 3306/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 21/tcp on 162.241.216.11
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 587/tcp on 162.241.216.11
Discovered open port 993/tcp on 162.241.216.11
Discovered open port 143/tcp on 162.241.216.11
Discovered open port 993/tcp on 162.241.216.11
Discovered open port 110/tcp on 162.241.216.11
Discovered open port 465/tcp on 162.241.216.11
Discovered open port 26/tcp on 162.241.216.11
Discovered open port 5632/tcp on 162.241.216.11
Discovered open port 2222/tcp on 162.241.216.11
Completed SYN Stealth Scan at 07:08, 30.24s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.100s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 985 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
```

Discription:

SYN (Synchronize): The scanner sends a SYN packet to the target port.

Response from Target:

If the port is open: The target replies with a SYN-ACK.

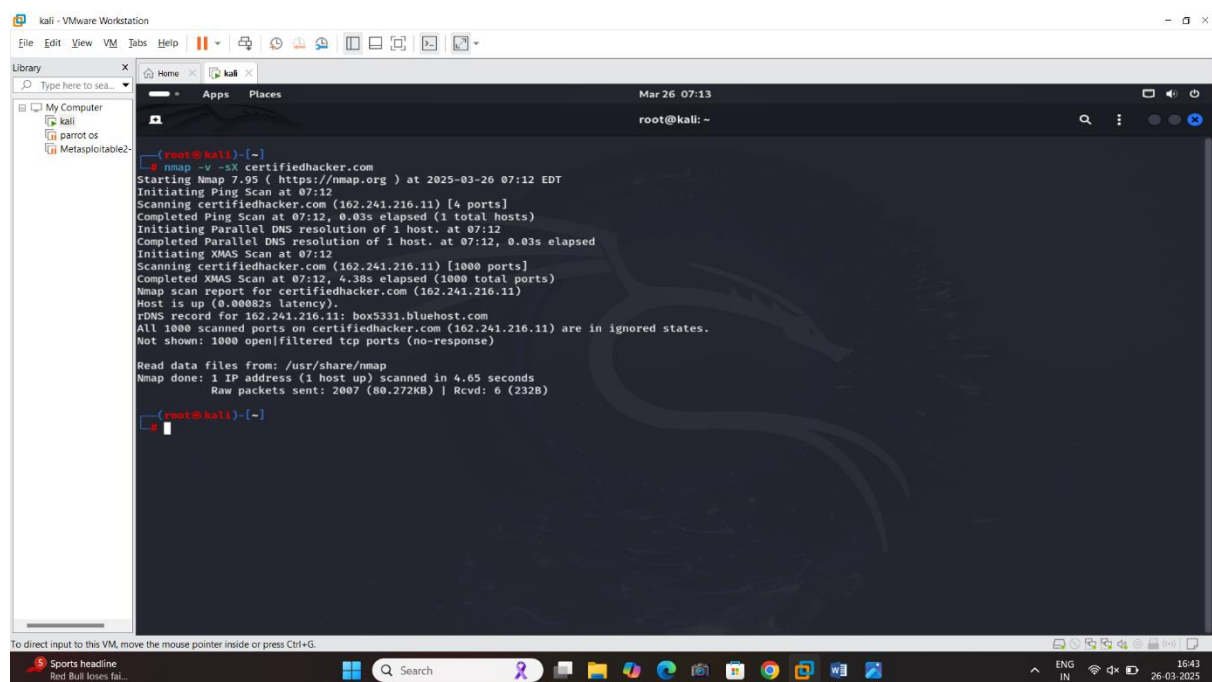
If the port is closed: The target responds with an RST (Reset) packet. No Completion of Handshake:

Instead of sending an ACK (which would complete the handshake), the scanner sends an RST to terminate the connection

3 Xmas Scan (-sX)

Command: `nmap -v -sX Certifiedhacker.com`

Explanation: The **Xmas Scan** is a TCP scanning technique that sends packets with **FIN**, **PSH**, and **URG** flags set — lighting up the packet "like a Christmas tree," hence the name **Xmas scan**.



```
(root@kali)~# nmap -v -sX certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 07:12 EDT
Initiating Ping Scan at 07:12
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 07:12, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:12
Completed Parallel DNS resolution of 1 host. at 07:12, 0.03s elapsed
Initiating XMAS Scan at 07:12
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Completed XMAS Scan at 07:12, 4.38s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.00082s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
All 1000 scanned ports on certifiedhacker.com (162.241.216.11) are in ignored states.
Not shown: 1000 open/filtered tcp ports (no-response)

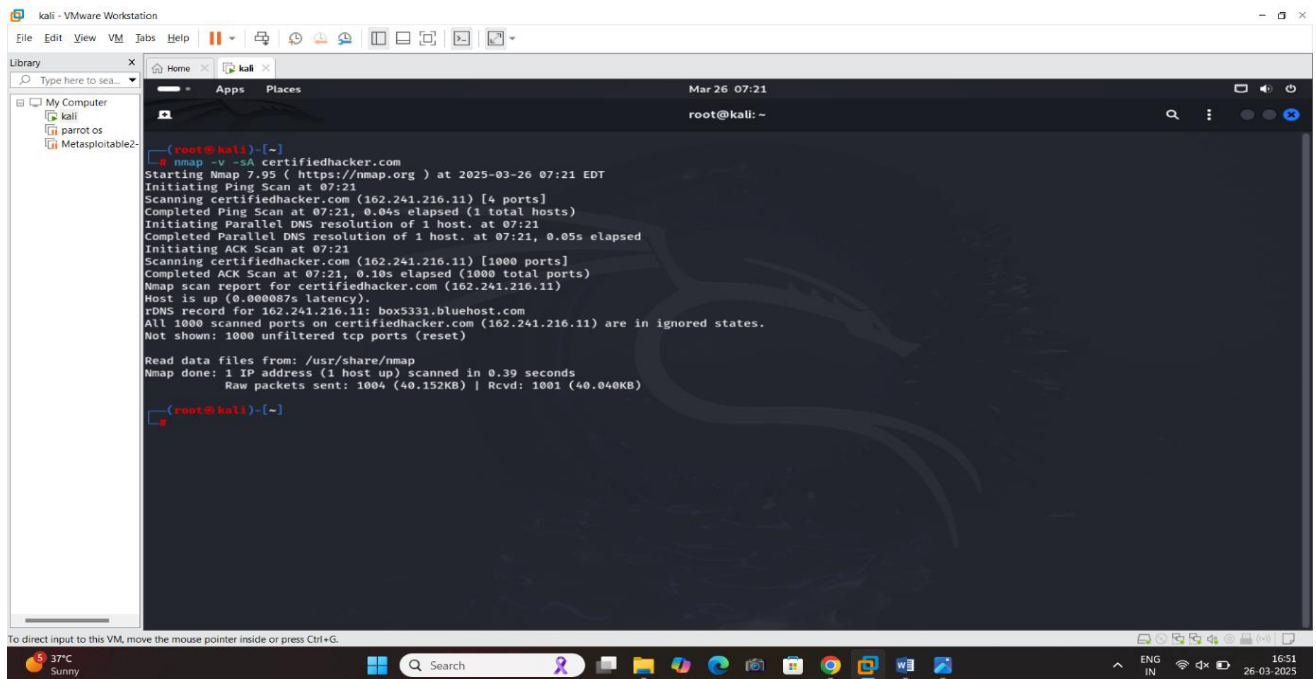
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.65 seconds
Raw packets sent: 2007 (80.272KB) | Rcvd: 6 (232B)

(root@kali)~#
```

4 ACK Scan (-sA)

Command: `nmap -v -sA certifiedhacker.com`

Explanation: The **ACK Scan** is a special type of TCP scan used to **map firewall rules** and determine if ports are **filtered** or **unfiltered** — it does **not** determine if the port is open or closed.



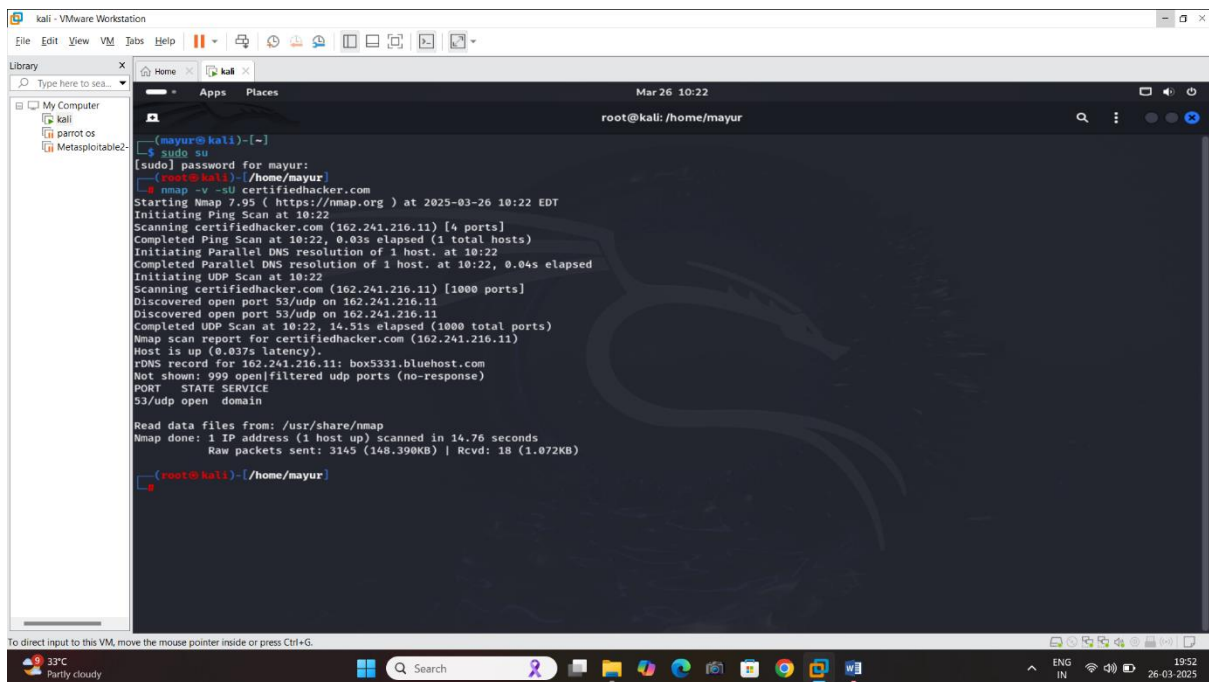
Discription: The scanner sends a TCP packet with only the ACK flag set (as if it were part of an ongoing connection).

2 NON TCP AND UDP Port Scanning

1 UDP Port Sacnning

Command: `nmap -v -sU certifiedhacker.com`

Explination: **UDP Port Scanning** is used to identify open UDP ports on a target host. Unlike TCP, UDP is a connectionless protocol — there's no handshake — so scanning UDP ports is more challenging and slower.



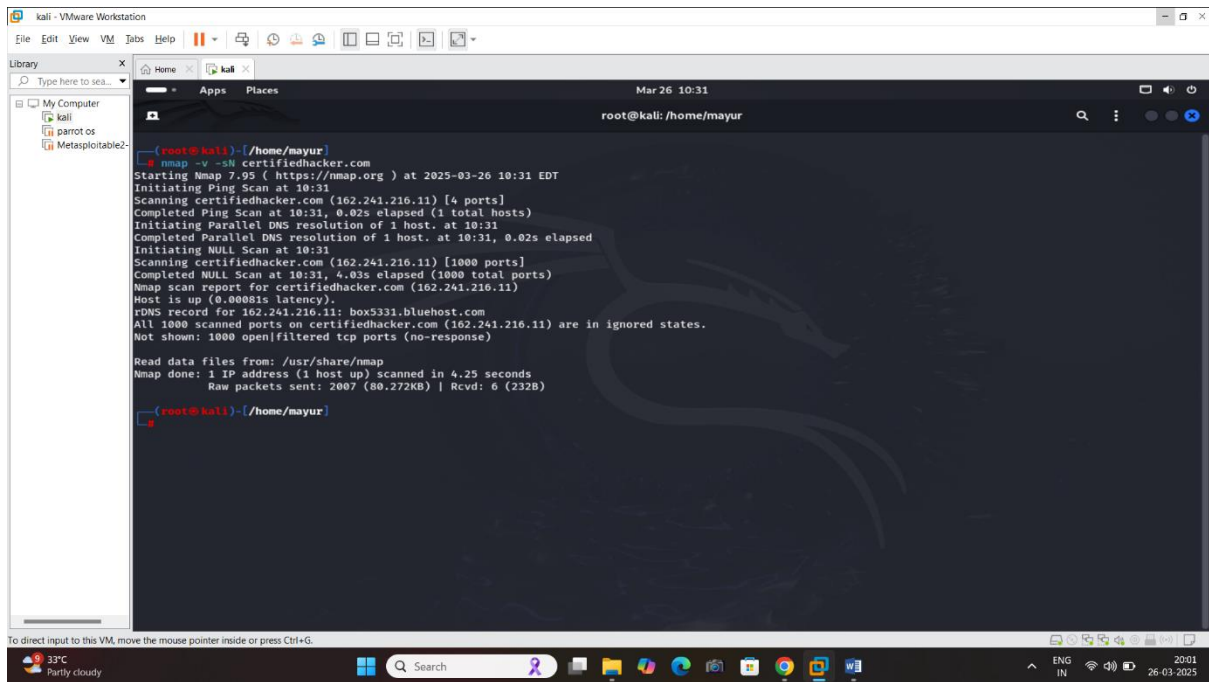
• Discription:

- Slower than TCP scans (due to lack of response).
- Often rate-limited by firewalls/IDS.
- Easy to trigger alerts.

Null Scan(-sN)

Command: `nmap -v -sN certifiedhacker.com`

Explination: A **Null Scan** is a type of TCP scan where **no flags are set** in the TCP packet header (all bits are zero).



The screenshot shows a Kali Linux virtual machine window. The terminal is running the command `nmap -v -sN certifiedhacker.com`. The output shows the scan progress, including ping scan, DNS resolution, and a null scan. The scan results indicate that the host is up and that all 1000 scanned ports are in ignored states. The terminal window has a dark background with a Kali Linux logo watermark. The window title is "kali - VMware Workstation". The bottom status bar shows the date and time as "Mar 26 10:31" and "2021 26-03-2025".

```
(root@kali)~/home/mayur
nmap -v -sN certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 10:31 EDT
Initiating Ping Scan at 10:31
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 10:31, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:31
Completed Parallel DNS resolution of 1 host. at 10:31, 0.02s elapsed
Initiating NULL Scan at 10:31
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Completed NULL Scan at 10:31, 4.03s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.00081s latency).
DNS record for 162.241.216.11: box5331.bluehost.com
All 1000 scanned ports on certifiedhacker.com (162.241.216.11) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds
Raw packets sent: 2007 (80.272KB) | Rcvd: 6 (232B)

(root@kali)~/home/mayur
```

“All information collect the one command “

For example: service port on and down, host up and down,

Command : `nmap -v -A -T4 certifiedhacker.com`

Explanation

1 -v (verbo)

2 -A (for Advance)

3-T4 (Aggressive)

Exercise 3

OS Discovery Using (NSE) Nmap Scripting engine

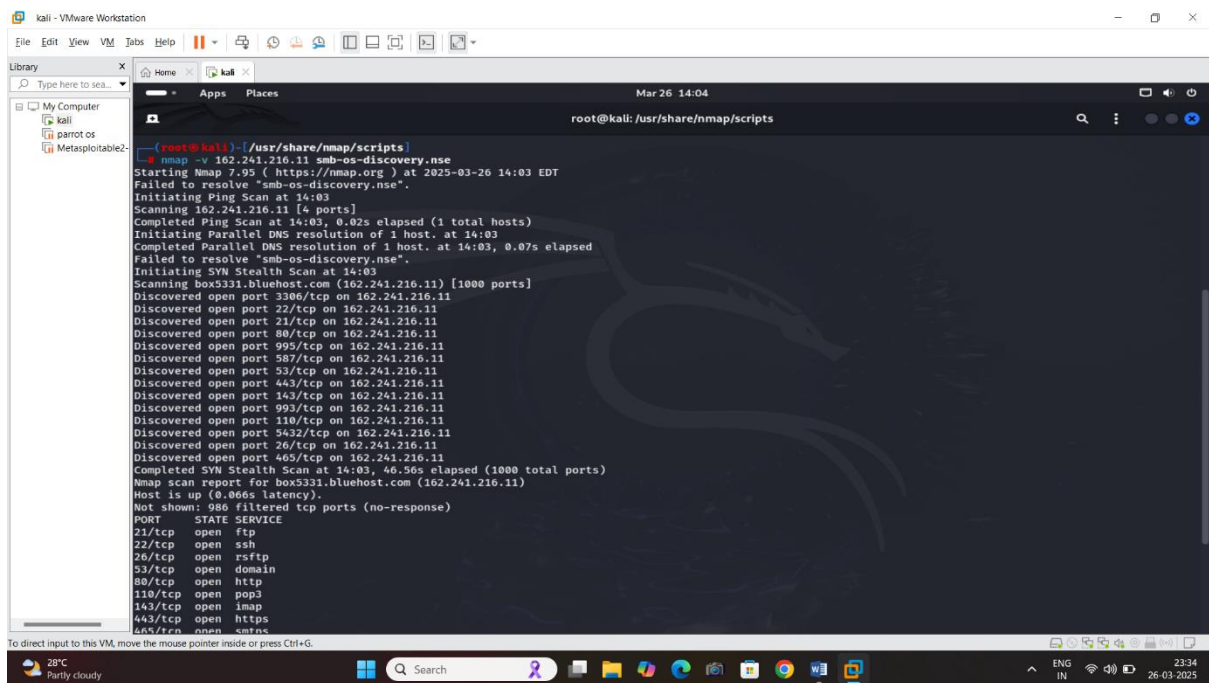
This command are use OS information

Script Location

/usr/share/nmap/scripts/

Command: `nmap -v -i 192.168.1.1 --os-discovery.nse`

Explanation: The script is a part of the **Nmap Scripting Engine (NSE)** and is used to discover the operating system information of a target system by querying the SMB (Server Message Block) service.



```
root@kali: /usr/share/nmap/scripts
nmap -v 192.241.216.11 --os-discovery.nse
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 14:03 EDT
Failed to resolve "smb-os-discovery.nse".
Initiating Ping Scan at 14:03
Scanning 192.241.216.11 [4 ports]
Completed Ping Scan at 14:03, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:03
Completed Parallel DNS resolution of 1 host. at 14:03, 0.07s elapsed
Failed to resolve "smb-os-discovery.nse".
Initiating SYN Stealth Scan at 14:03
Scanning box5331.bluehost.com (192.241.216.11) [1000 ports]
Discovered open port 3306/tcp on 192.241.216.11
Discovered open port 22/tcp on 192.241.216.11
Discovered open port 21/tcp on 192.241.216.11
Discovered open port 80/tcp on 192.241.216.11
Discovered open port 995/tcp on 192.241.216.11
Discovered open port 587/tcp on 192.241.216.11
Discovered open port 33/tcp on 192.241.216.11
Discovered open port 443/tcp on 192.241.216.11
Discovered open port 143/tcp on 192.241.216.11
Discovered open port 993/tcp on 192.241.216.11
Discovered open port 110/tcp on 192.241.216.11
Discovered open port 5432/tcp on 192.241.216.11
Discovered open port 26/tcp on 192.241.216.11
Discovered open port 465/tcp on 192.241.216.11
Completed SYN Stealth Scan at 14:03, 46.56s elapsed (1000 total ports)
Nmap scan report for box5331.bluehost.com (192.241.216.11)
Host is up (0.066s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
```

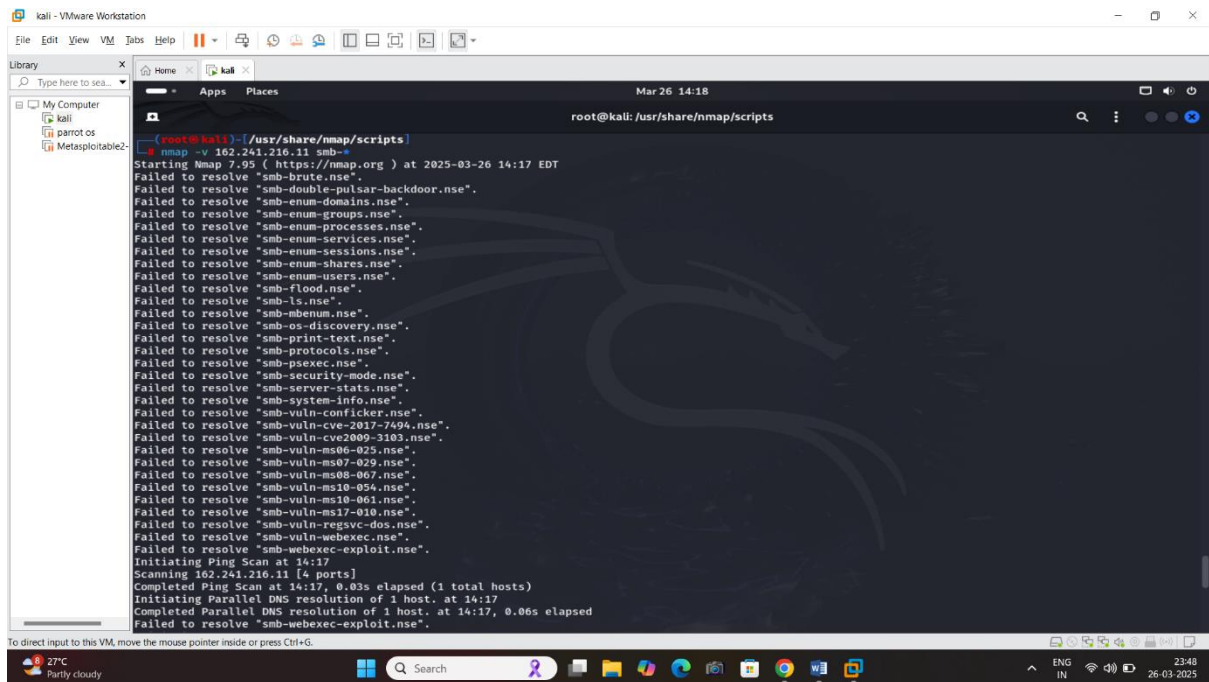
Discription:

Helps **identify operating systems** running on SMB-enabled hosts.

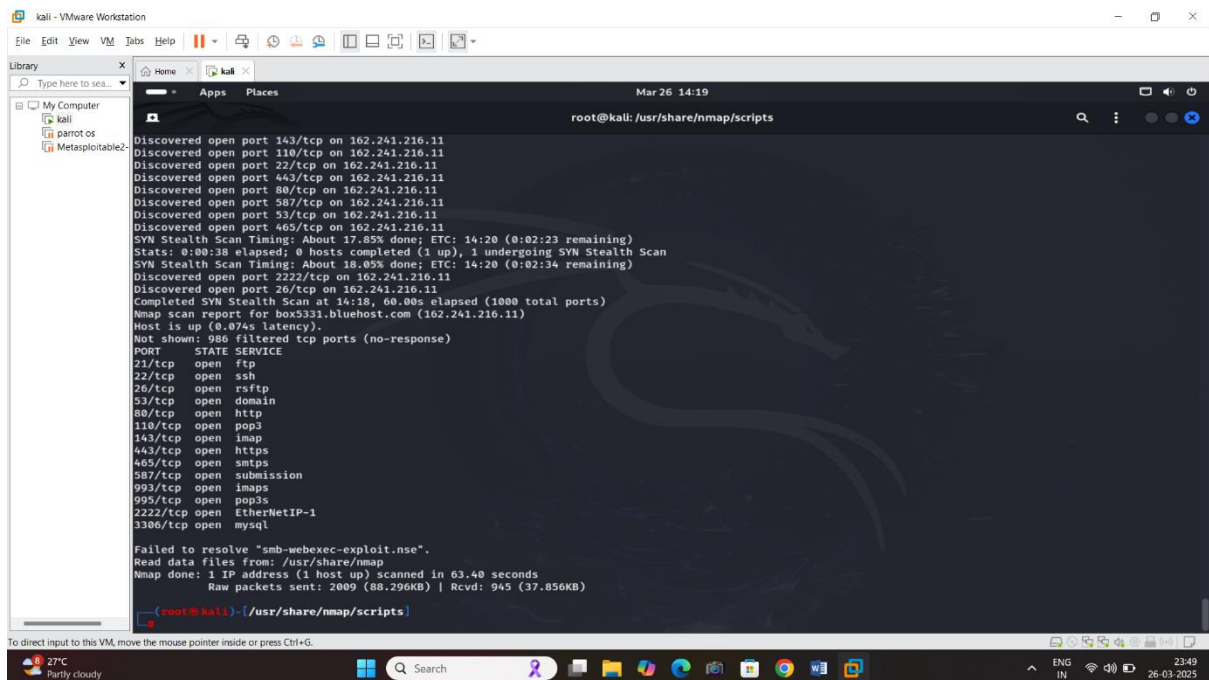
Provides **OS details, system time, and workgroup/domain**, which can be used for further exploitation.

2 this command are use multiple OS filter (NSE)

Command : Nmap -v 162.241.216.11 -os smb-*



```
(root@kali)~# nmap -v 162.241.216.11 smb-*
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 14:17 EDT
Failed to resolve "smb-brute.nse".
Failed to resolve "smb-double-pulsar-backdoor.nse".
Failed to resolve "smb-enum-domains.nse".
Failed to resolve "smb-enum-groups.nse".
Failed to resolve "smb-enum-processes.nse".
Failed to resolve "smb-enum-services.nse".
Failed to resolve "smb-enum-sessions.nse".
Failed to resolve "smb-enum-shares.nse".
Failed to resolve "smb-enum-users.nse".
Failed to resolve "smb-flood.nse".
Failed to resolve "smb-ls.nse".
Failed to resolve "smb-menum.nse".
Failed to resolve "smb-os-discovery.nse".
Failed to resolve "smb-print-text.nse".
Failed to resolve "smb-protocols.nse".
Failed to resolve "smb-psexec.nse".
Failed to resolve "smb-security-mode.nse".
Failed to resolve "smb-server-stats.nse".
Failed to resolve "smb-system-info.nse".
Failed to resolve "smb-vuln-conficker.nse".
Failed to resolve "smb-vuln-cve-2017-7494.nse".
Failed to resolve "smb-vuln-cve-2009-3103.nse".
Failed to resolve "smb-vuln-ms06-025.nse".
Failed to resolve "smb-vuln-ms07-029.nse".
Failed to resolve "smb-vuln-ms08-067.nse".
Failed to resolve "smb-vuln-ms10-054.nse".
Failed to resolve "smb-vuln-ms10-061.nse".
Failed to resolve "smb-vuln-ms17-010.nse".
Failed to resolve "smb-vuln-regsvcs-dos.nse".
Failed to resolve "smb-vuln-webexec.nse".
Failed to resolve "smb-webexec-exploit.nse".
Initiating Ping Scan at 14:17
Scanning 162.241.216.11 [4 ports]
Completed Ping Scan at 14:17, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:17
Completed Parallel DNS resolution of 1 host. at 14:17, 0.06s elapsed
Failed to resolve "smb-webexec-exploit.nse".
```



```
Discovered open port 143/tcp on 162.241.216.11
Discovered open port 110/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 987/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 465/tcp on 162.241.216.11
SYN Stealth Scan Timing: About 17.85% done; ETC: 14:20 (0:02:23 remaining)
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.05% done; ETC: 14:20 (0:02:34 remaining)
Discovered open port 2222/tcp on 162.241.216.11
Discovered open port 26/tcp on 162.241.216.11
Completed SYN Stealth Scan at 14:19, 60.00s elapsed (1000 total ports)
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.074s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
987/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2222/tcp  open  EtherNetIP-1
3306/tcp  open  mysql

Failed to resolve "smb-webexec-exploit.nse".
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 63.40 seconds
Raw packets sent: 2009 (88.296KB) | Rcvd: 945 (37.856KB)

(root@kali)~#
```

Exercise 4

First Technique of IDS Firewall by pass

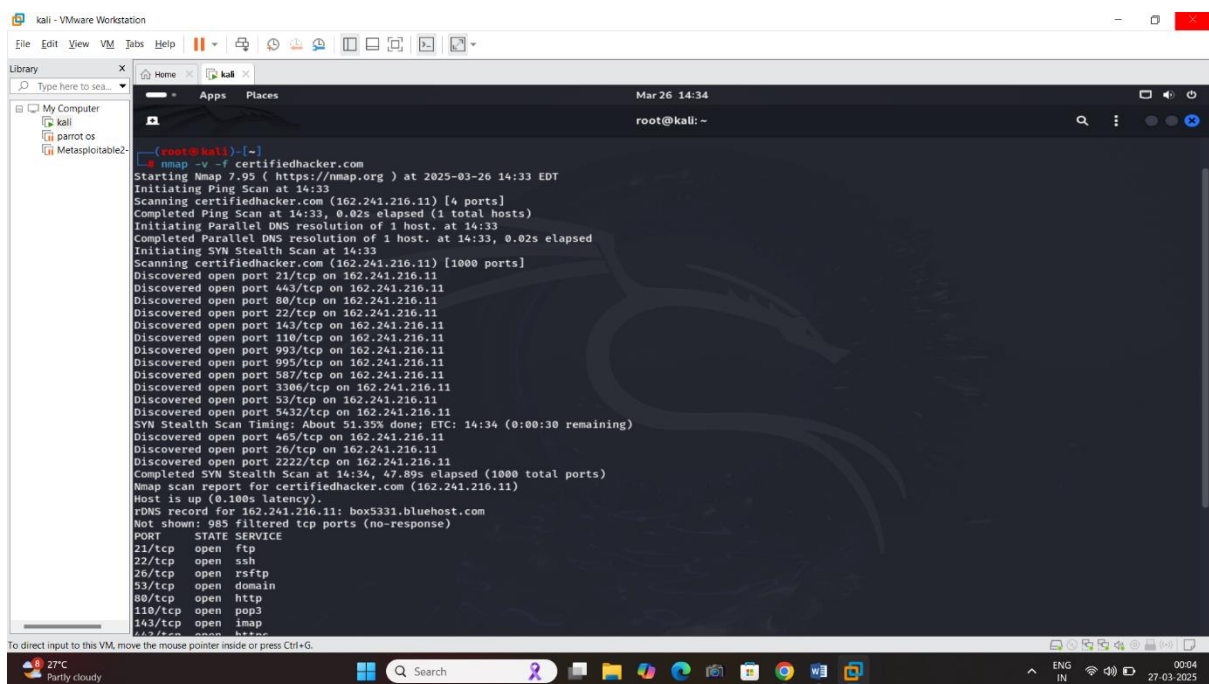
1 Packet Fragmentation

Command: Nmap -f certifiedhacker.com

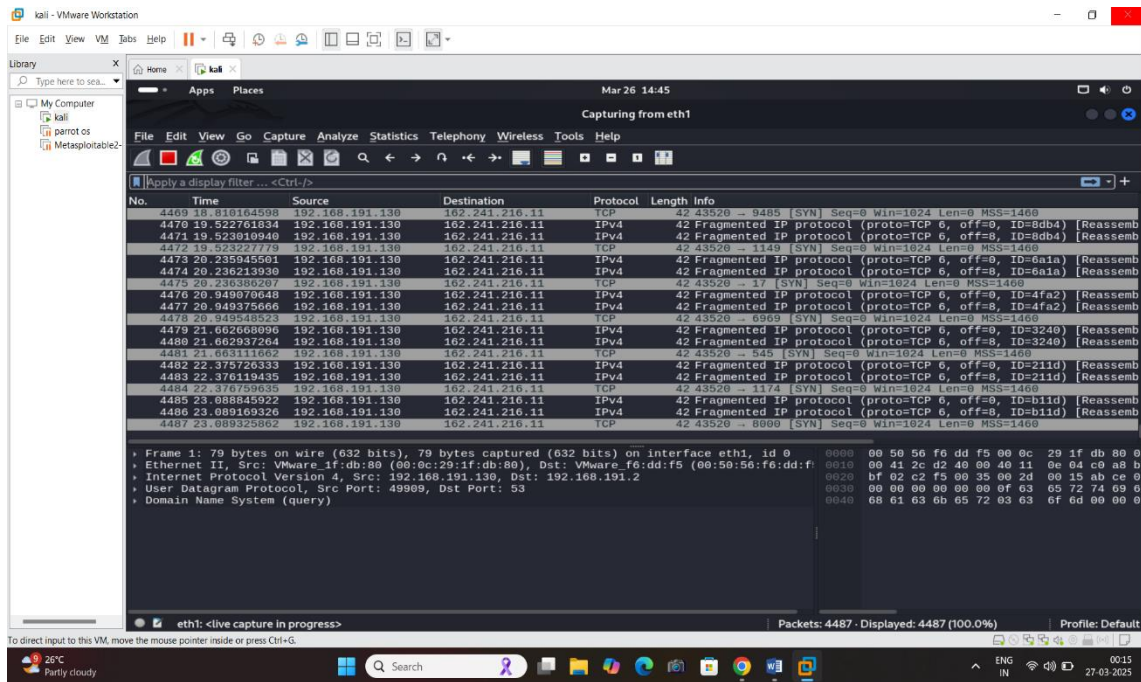
Explaniation:

Packet fragmentation is the process of **breaking a large network packet into smaller pieces**

Security testers use **fragmentation** to **bypass firewall rules** that inspect full packets



```
(root@kali)~# nmap -v -f certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 14:33 EDT
Initiating Ping Scan at 14:33
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 14:33, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:33
Completed Parallel DNS resolution of 1 host. at 14:33, 0.02s elapsed
Initiating SYN Stealth Scan at 14:33
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Discovered open port 21/tcp on 162.241.216.11
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 143/tcp on 162.241.216.11
Discovered open port 110/tcp on 162.241.216.11
Discovered open port 993/tcp on 162.241.216.11
Discovered open port 995/tcp on 162.241.216.11
Discovered open port 587/tcp on 162.241.216.11
Discovered open port 3306/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 5432/tcp on 162.241.216.11
SYN Stealth Scan Timing: About 51.35% done; ETC: 14:34 (0:00:30 remaining)
Discovered open port 465/tcp on 162.241.216.11
Discovered open port 26/tcp on 162.241.216.11
Discovered open port 2222/tcp on 162.241.216.11
Completed SYN Stealth Scan at 14:34, 47.89s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.100s latency).
DNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 985 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
144/tcp   open  kpop
145/tcp   open  kpop
146/tcp   open  kpop
147/tcp   open  kpop
```



Second Technique of IDS Firewall by pass

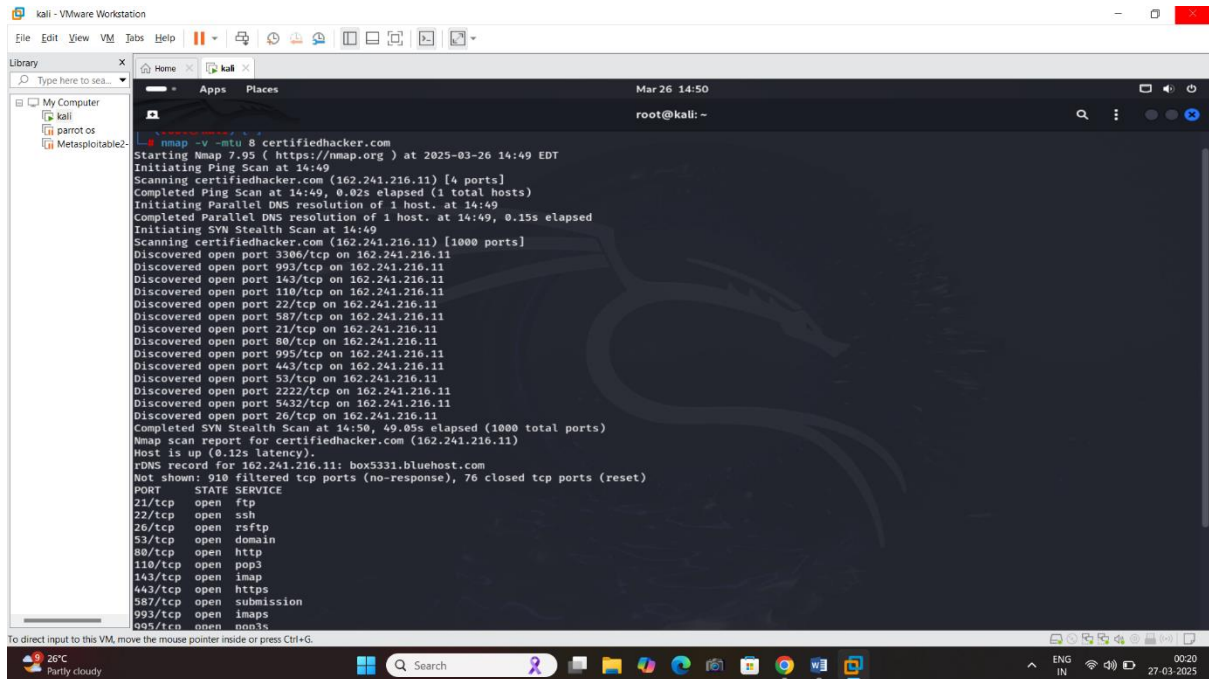
Command: Nmap -v -mtu 8 certifiedhacker.com

MTU(maximum , transmission , unit)

Explanation:

option forces **fragmentation** by setting the packet MTU to **8 bytes**.

This is a **stealth technique** to bypass firewalls and intrusion detection systems (IDS).



```
nmap -v -mtu 8 certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 14:49 EDT
Initiating Ping Scan at 14:49
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 14:49, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:49
Completed Parallel DNS resolution of 1 host. at 14:49, 0.15s elapsed
Initiating SYN Stealth Scan at 14:49
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Discovered open port 3306/tcp on 162.241.216.11
Discovered open port 993/tcp on 162.241.216.11
Discovered open port 143/tcp on 162.241.216.11
Discovered open port 110/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 587/tcp on 162.241.216.11
Discovered open port 21/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 995/tcp on 162.241.216.11
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 2222/tcp on 162.241.216.11
Discovered open port 5432/tcp on 162.241.216.11
Discovered open port 26/tcp on 162.241.216.11
Completed SYN Stealth Scan at 14:50, 49.05s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.12s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 910 filtered tcp ports (no-response), 76 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imap
995/tcp   open  nntp
```

Description:

This command runs an **Nmap scan** using **two fragmentation techniques** to evade firewalls and Intrusion Detection Systems (IDS)

Command: `Nmap -v -g 80 certifiedhacker.com`

Explanation: (-g) Source port target set 80 port

(-g) use the spoofing are use this technique are by pass firewall technique

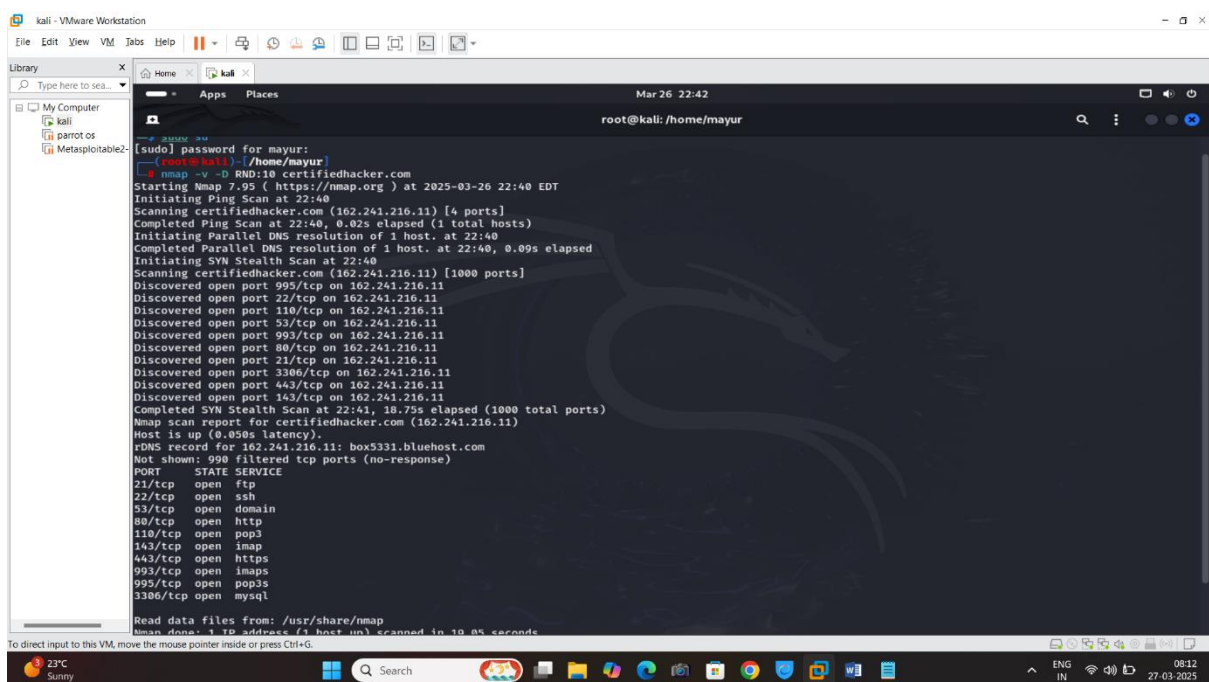
Exercise 5

3rd Technique of IDS Firewall by pass

Decoy Technique

Command: `nmap -v -D RND:10 certifiedhacker.com`

Explanation: The **decoy technique** in Nmap is used to **mask the real attacker's IP address** by generating fake (decoy) IP addresses during a scan. This confuses firewalls and Intrusion Detection Systems (IDS) by making it difficult to identify the real scanner.



```
[sudo] password for mayur:
root@kali: /home/mayur
nmap -v -D RND:10 certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 22:40 EDT
Initiating Ping Scan at 22:40
Scanning certifiedhacker.com (162.241.216.11) [4 ports]
Completed Ping Scan at 22:40, 0.025s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:40
Completed Parallel DNS resolution of 1 host. at 22:40, 0.09s elapsed
Initiating SYN Stealth Scan at 22:40
Scanning certifiedhacker.com (162.241.216.11) [1000 ports]
Discovered open port 995/tcp on 162.241.216.11
Discovered open port 22/tcp on 162.241.216.11
Discovered open port 110/tcp on 162.241.216.11
Discovered open port 53/tcp on 162.241.216.11
Discovered open port 993/tcp on 162.241.216.11
Discovered open port 80/tcp on 162.241.216.11
Discovered open port 21/tcp on 162.241.216.11
Discovered open port 3306/tcp on 162.241.216.11
Discovered open port 443/tcp on 162.241.216.11
Discovered open port 143/tcp on 162.241.216.11
Completed SYN Stealth Scan at 22:41, 18.75s elapsed (1000 total ports)
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.050s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp   open  mysql

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 19.05 seconds
```

Discription:

-D RND:10 → **Decoy Scanning Mode** with **10 random spoofed IP addresses**

where 10 random IP addresses are used as **fake sources** to **mask the real attacker's IP**. This technique makes it harder for the target to detect the actual scanning source.

Hping3

Hping3 is a powerful **command-line tool** used for network security auditing, advanced packet manipulation, and **TCP/IP scanning**. It allows users to **craft and send custom packets**, making it a valuable tool for penetration testing, firewall testing, and DoS attack simulations.

Command : `hping3 -1 162.241.216.11 -a 162.241.216.11 -p 80 --faster`

Explination: • `hping3` → Calls the Hping3 tool.

- `-1` → Uses **ICMP Echo Request** (like a standard ping).
- `162.241.216.11` → **Target IP address** to be scanned.
- `-a 162.241.216.11` → **Spoofs the source IP**, making it look like the packets are coming from the target itself (**IP spoofing**).
- `-p 80` → Targets **port 80** (HTTP).
- `--faster` → Increases packet sending speed.

