

# MODULE: 3

## Report on: Scanning Networks

-ATHARVA KATKAR

Sr no.	Contents	Fig no.
01.	Introduction to Network Scanning	0
02.	Host Discovery <ul style="list-style-type: none"> <li>• Tool used: Nmap               <ul style="list-style-type: none"> <li>➢ ARP ping scan</li> <li>➢ UDP ping scan</li> <li>➢ ICMP echo ping</li> <li>➢ SYN</li> <li>➢ ACK</li> </ul> </li> </ul>	1-6
03.	Port & Service Discovery <ul style="list-style-type: none"> <li>• Tool used: Zenmap               <ul style="list-style-type: none"> <li>➢ TCP full open scan</li> <li>➢ Stealth Scan</li> <li>➢ Xmas scan</li> <li>➢ Maimon scan</li> <li>➢ ACK</li> <li>➢ UDP</li> </ul> </li> </ul>	7-22
04.	OS Discovery <ul style="list-style-type: none"> <li>• Tool used: Nmap               <ul style="list-style-type: none"> <li>➢ Aggressive scan</li> <li>➢ OS detection scan</li> </ul> </li> </ul>	23-25
05.	IDS and Firewall <ul style="list-style-type: none"> <li>• Tool used: Nmap &amp; Wireshark</li> </ul>	26-34
06.	Additional tools: <ul style="list-style-type: none"> <li>• Hping3               <ul style="list-style-type: none"> <li>➢ ICMP</li> <li>➢ UDP</li> <li>➢ ACK</li> <li>➢ SYN</li> </ul> </li> <li>• Metasploit</li> </ul>	35-50

# NETWORK SCANNING

Network scanning is a process used in computer networks to identify active devices, services, and potential vulnerabilities within a network. It involves sending data packets to target systems and analyzing their responses to gather information such as IP addresses, open ports, running services, and security risks.

Objectives –

- Discovery
- Security assessment
- Vulnerability detection
- Network mapping
- Performance analysis

## Types of Network Scanning:

### 1. Port Scanning

Used to find:

- Open ports
- Closed ports
- Filtered (firewalled) ports

Tools: Nmap, Masscan

Examples:

- nmap -sS → SYN Stealth scan
- nmap -sU → UDP scan
- nmap -sV → Service version detection

## **2. Host Scanning (Ping Scanning)**

Finds live hosts in a network.

Tools: Nmap, Angry IP Scanner

Examples:

- nmap -sn 192.168.1.0/24
- nmap -PR → ARP ping on LAN
- nmap -PE → ICMP ping

## **3. Vulnerability Scanning**

Identifies weaknesses or CVEs.

Tools: Nessus, OpenVAS, Qualys

Finds:

- Missing patches
- Weak configurations
- Known vulnerabilities

## **4. Network Mapping (Topology Discovery)**

Discovers network structure, routers, paths.

Tools: Nmap, traceroute

### **Why Network Scanning Is Important:**

- Identify live hosts
- Identify open ports
- Identify services and versions
- Detect misconfigurations
- Prepare for exploitation

# HOST DISCOVERY

Host Discovery is the process of identifying which systems (hosts) are alive and reachable on a network.

## What Is Host Discovery?

Host Discovery (also called ping scanning) is the process of checking: Which devices are up and reachable on a network. It does not scan ports or services.

**It only answers the question:**

- ✓ Is the host alive?
- ✓ Is it reachable across the network?
- ✓ Does it respond to basic network probes?

The following are examples of host discovery techniques:

- . ARP ping scan
- . UDP ping scan
- . ICMP ping scan (ICMP ECHO ping, ICMP timestamp, ping ICMP, and address mask ping)
- TCP ping scan (TCP SYN ping and TCP ACK ping)
- IP protocol ping scan

# Host Discovery using Nmap:

## Test/Tool Shown:

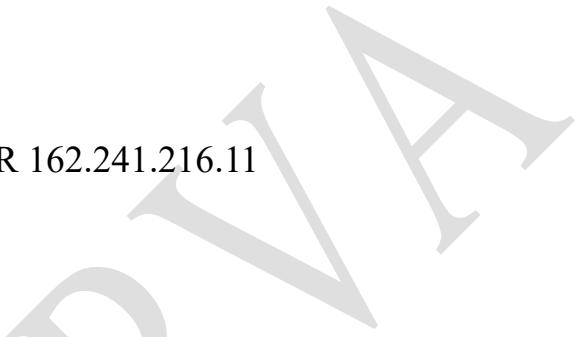
Nmap (nmap -sn -PR) on Kali Linux terminal

-sn: disables port scan an -PR: performs ARP ping scan.

## Step Performed:

Executed the command: nmap -sn -PR 162.241.216.11

## Output:



```
Atharva1 [Running] - Oracle VirtualBox
Nov 27 19:33
root@kali:/home/atharva
(atlarva㉿kali)-[~]
$ sudo su
[sudo] password for atharva:
(root㉿kali)-[/home/atharva]
# nmap -sn -PR 162.241.216.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 19:32 IST
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.021s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
(root㉿kali)-[/home/atharva]
#
```

Fig(1)

- Nmap started normally.
- It resolved the IP address to a hostname: box5331.bluehost.com
- It detected: Host is up (0.021s latency)

## **Test/Tool Shown:**

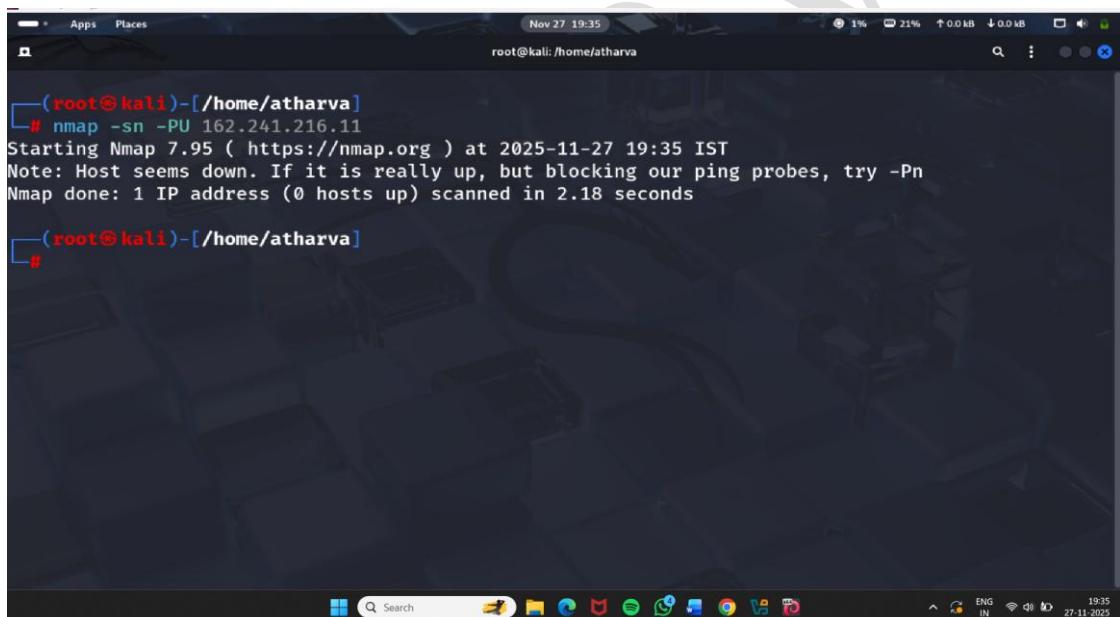
Nmap (nmap -sn -PU) on Kali Linux terminal

-PU: performs UDP ping scan

## **Step Performed:**

Executed the command: nmap -sn -PU 162.241.216.11

## **Output:**



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '(root㉿kali)-[~/home/atharva]'. The command entered is '# nmap -sn -PU 162.241.216.11'. The output message indicates that the host seems down, suggesting it might be a firewall or a host that does not respond to ping probes. The scan results show 0 hosts up.

```
(root㉿kali)-[~/home/atharva]
# nmap -sn -PU 162.241.216.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 19:35 IST
Note: 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 2.18 seconds
```

Fig(2)

- Nmap attempted UDP ping packets.
- It returned the message:  
“Host seems down. If it is really up, but blocking our ping probes, try -Pn”
- Scan result: 0 hosts up

## **Test/Tool Shown:**

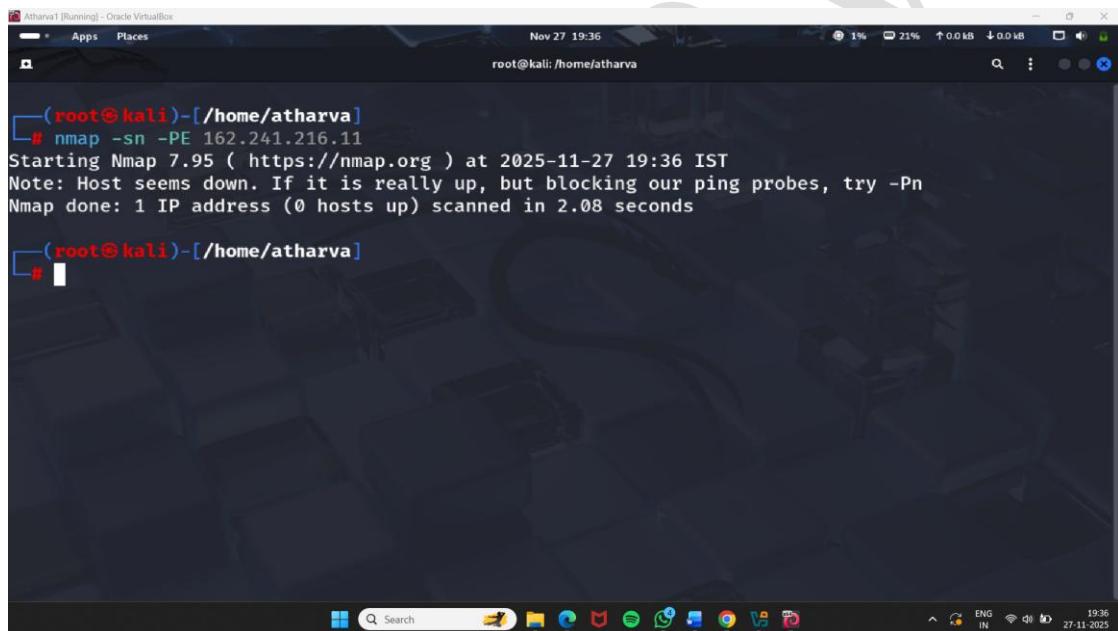
Nmap (nmap -sn -PE) – on Kali Linux terminal.

-PE : ICMP Echo ping (normal ping)

## **Step Performed:**

Executed the command: nmap -sn -PE 162.241.216.11

## **Output:**



The screenshot shows a terminal window titled "Atharva1 [Running] - Oracle VirtualBox". The terminal is running as root, indicated by the prompt "(root@kali)-[~/home/atharva]". The user has run the command "nmap -sn -PE 162.241.216.11". The output indicates that the host seems down, suggesting it might be blocking ping probes. The final result shows 0 hosts up.

```
(root@kali)-[~/home/atharva]
# nmap -sn -PE 162.241.216.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 19:36 IST
Note: 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 2.08 seconds
#
```

Fig(3)

- Nmap attempted ICMP echo requests.
- Output displayed:
- “Host seems down. If it is really up, but blocking our ping probes, try -Pn”
- Final result: 0 hosts up

## Test/Tool Shown:

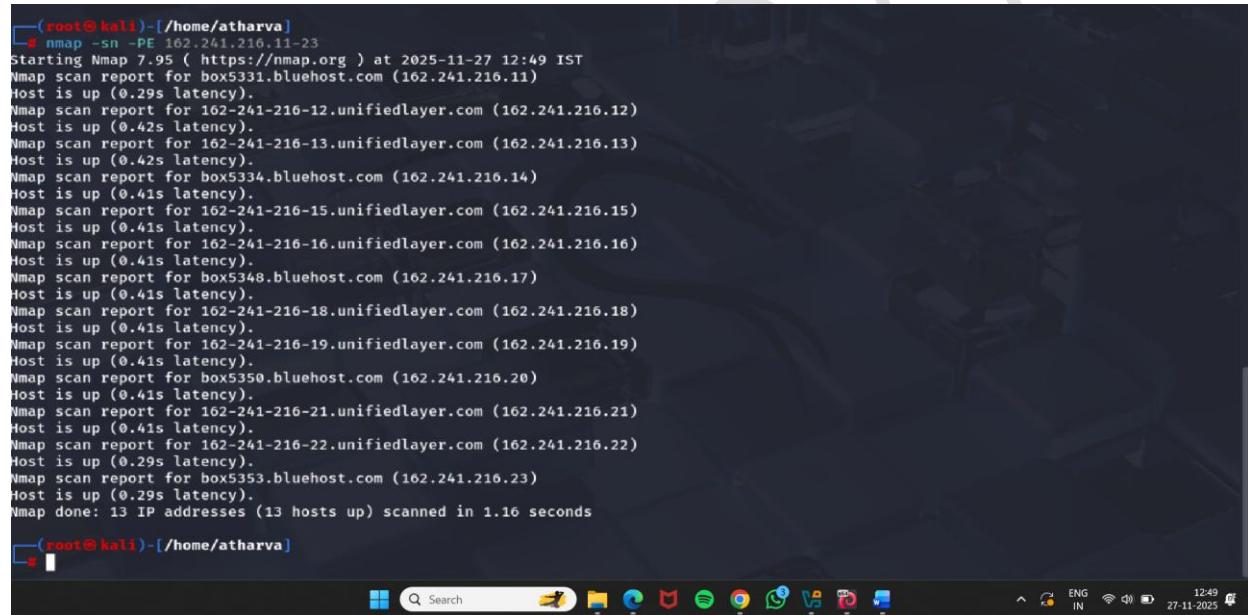
Nmap (nmap -sn -PE.....-23) – on Kali Linux terminal.

-PE: ICMP Echo ping

## Step Performed:

Executed the command: nmap -sn -PE 162.241.216.11-23

## Output:



```
(root@kali)-[~/home/atharva]
# nmap -sn -PE 162.241.216.11-23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 12:49 IST
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.29s latency).
Nmap scan report for 162-241-216-12.unifiedlayer.com (162.241.216.12)
Host is up (0.42s latency).
Nmap scan report for 162-241-216-13.unifiedlayer.com (162.241.216.13)
Host is up (0.42s latency).
Nmap scan report for box5334.bluehost.com (162.241.216.14)
Host is up (0.41s latency).
Nmap scan report for 162-241-216-15.unifiedlayer.com (162.241.216.15)
Host is up (0.41s latency).
Nmap scan report for 162-241-216-16.unifiedlayer.com (162.241.216.16)
Host is up (0.41s latency).
Nmap scan report for box5348.bluehost.com (162.241.216.17)
Host is up (0.41s latency).
Nmap scan report for 162-241-216-18.unifiedlayer.com (162.241.216.18)
Host is up (0.41s latency).
Nmap scan report for 162-241-216-19.unifiedlayer.com (162.241.216.19)
Host is up (0.41s latency).
Nmap scan report for box5350.bluehost.com (162.241.216.20)
Host is up (0.41s latency).
Nmap scan report for 162-241-216-21.unifiedlayer.com (162.241.216.21)
Host is up (0.41s latency).
Nmap scan report for 162-241-216-22.unifiedlayer.com (162.241.216.22)
Host is up (0.29s latency).
Nmap scan report for box5353.bluehost.com (162.241.216.23)
Host is up (0.29s latency).
Nmap done: 13 IP addresses (13 hosts up) scanned in 1.16 seconds

```

Fig(4)

- Total Hosts Scanned: 13 IP addresses (the range .11 to .23 inclusive).
- Hosts Identified as Up: 13 hosts were found to be up.
- Scan Reports: Nmap successfully received ICMP Echo Replies from all 13 addresses.

## **Test/Tool Shown:**

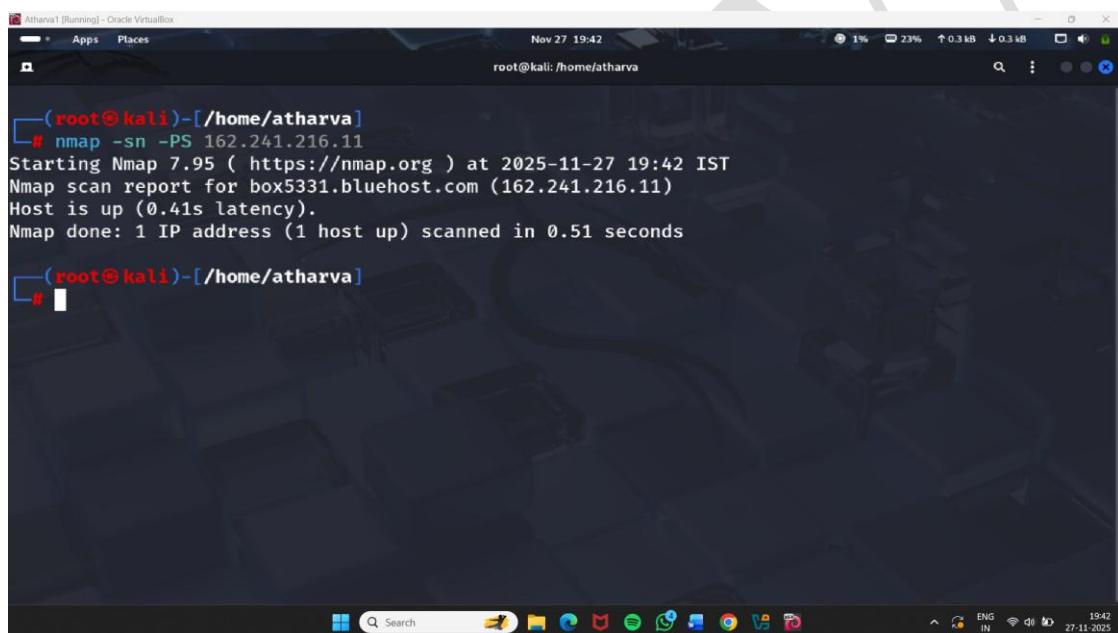
Nmap (nmap -sn -PS) – on Kali Linux terminal.

-PS: performs a TCP SYN Ping Scan

## **Step Performed:**

Executed the command: nmap -sn -PS 162.241.216.

## **Output:**



The screenshot shows a terminal window titled "Atharva1 [Running] - Oracle VirtualBox". The terminal is running as root on a Kali Linux system. The command entered is "nmap -sn -PS 162.241.216.11". The output shows the Nmap version (7.95), the start time (Nov 27 19:42 IST), the target host (box5331.bluehost.com at 162.241.216.11), and the fact that the host is up (0.41s latency). It also indicates that the scan took 0.51 seconds. The terminal prompt ends with a "#".

Fig(5)

- Nmap Scan Report: Nmap scan report for box5331.bluehost.com (162.241.216.11)
- Host Status: Host is up
  - ❖ Mechanism: Nmap sent a TCP SYN probe to the host and received a response (likely a SYN/ACK), indicating the host is alive and a port (or the firewall) is responding to TCP requests.
- Final Result: Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds.

## **Test/Tool Shown:**

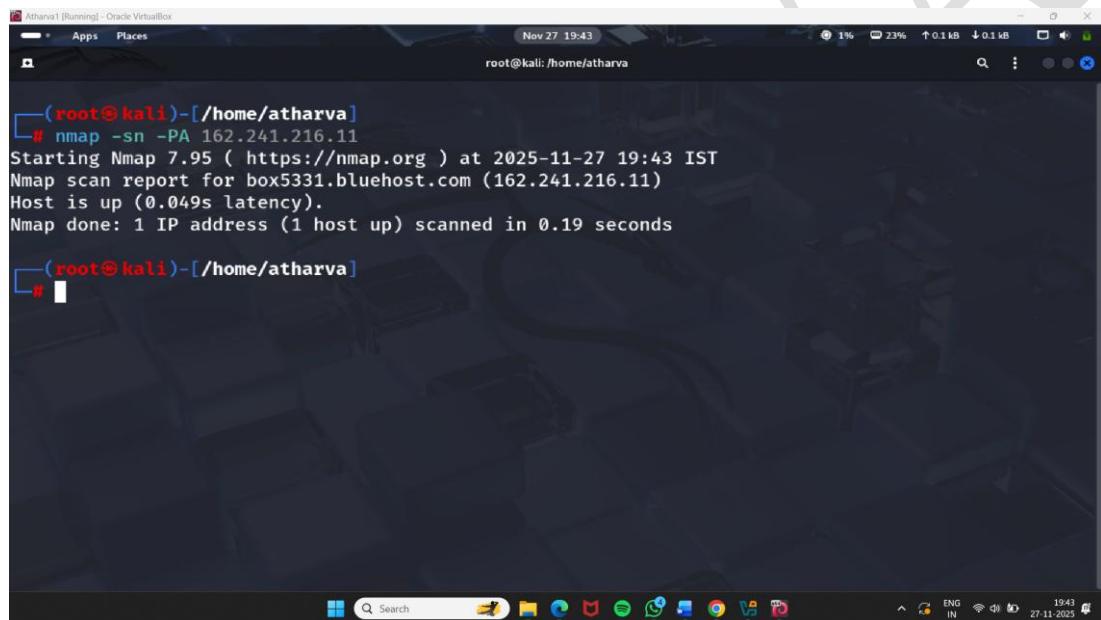
Nmap (nmap -sn -PA) – on Kali Linux terminal.

-PA: acknowledgement

## **Step Performed:**

Executed the command: nmap -sn -PA 162.241.216.11

## **Output:**



The screenshot shows a terminal window titled "Atharva1 [Running] - Oracle VM VirtualBox". The terminal is running as root, indicated by the red "(root@kali)". The command entered is "# nmap -sn -PA 162.241.216.11". The output shows the Nmap version (7.95), the start time (Nov 27 19:43 IST), the target host (box5331.bluehost.com, 162.241.216.11), and its status (Host is up). It also indicates the latency (0.049s) and the total scan time (0.19 seconds). The terminal prompt "# " is visible at the bottom.

Fig(6)

- Nmap Scan Report: Nmap scan report for box5331.bluehost.com (162.241.216.11)
- Host Status: Host is up
- Mechanism: Nmap sent a TCP ACK probe to the target host. A responsive RST (Reset) packet indicates the host is alive, even if it's firewalled, as the packet successfully traversed the network stack. This is often used to bypass firewalls that block ICMP Echo requests (like the scenario described in your original "Observed Output").
- Final Result: Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds.

# PORT & SERVICE DISCOVERY

Port and service discovery is the process of identifying open ports and services running on the target IP addresses/active

When analyzing a network, security professionals need to know:

- Which ports are open
- Which services are running
- Which versions or applications are active
- Which ports are filtered or blocked by firewalls

Port scanning techniques are categorized according to the type of protocol used for communication within the network:

- TCP Scanning
  - Open TCP scanning methods (TCP connect/full open scan)
  - Stealth TCP scanning methods (Half-open Scan, Inverse TCP Flag Scan, ACK flag probe scan, third party and spoofed TCP scanning methods)
- UDP Scanning
- SCTP Scanning
  - SCTP INIT Scanning
  - SCTP COOKIE/ECHO Scanning
- SSDP and List Scanning
- IPv6 Scanning

## **Test/Tool Shown:**

- Zenmap (nmap -sT -v ) on zenmap terminal.

## **Step Performed:**

- A single target host 162.241.216.11 (box5331.bluehost.com) was scanned with Nmap from Zenmap using a TCP connect scan over the first 1000 TCP ports with DNS resolution and verbosity enabled.

## Output:

Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-27 19:46 +0530

Initiating Ping Scan at 19:46

Scanning 162.241.216.11 [1000 ports]

Completed Ping Scan at 19:46

0.03s elapsed [1 total hosts]

Initiating Parallel DNS resolution of 1 host. at 19:46

Completed Parallel DNS resolution of 1 host. at 19:46, 0.01s elapsed

Initiating Connect Scan at 19:46

Scanning box331.bluehost.com [162.241.216.11] [1000 ports]

Completed Connect Scan at 19:46, 6.61s elapsed (1000 total ports)

Hosts reported as up: box331.bluehost.com (162.241.216.11)

Host is up (0.31s latency).

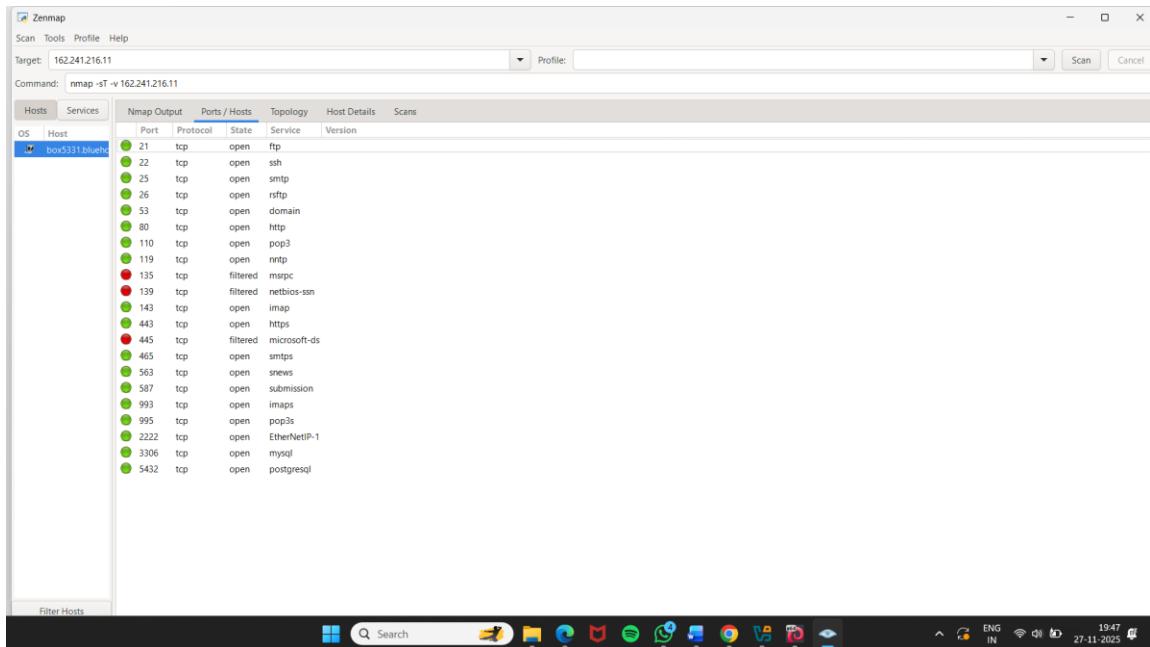
Not shown: 979 closed tcp ports (conn-refused)

PORT	STATE	SERVICE
21/tcp	open	ftp
25/tcp	open	smtp
25/tcp	open	smtp
26/tcp	open	rfttp
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop3
119/tcp	open	nntp
139/tcp	filtered	netbios-ssn
139/tcp	open	netbios-ssn
443/tcp	open	https

Filter Hosts

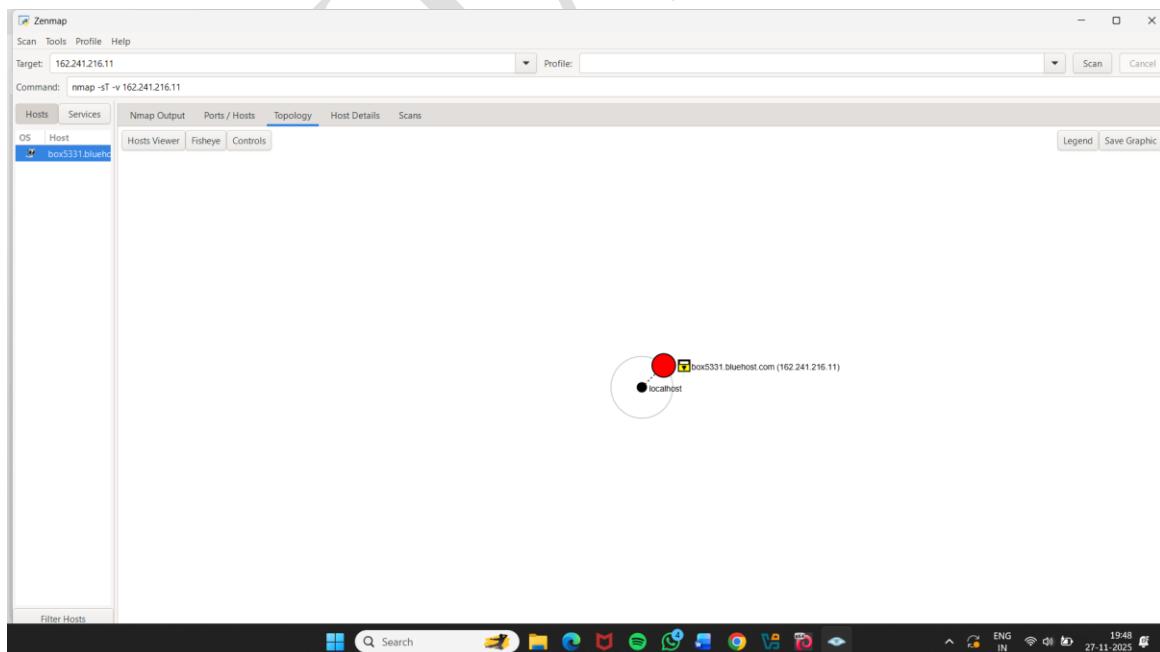
Fig(7)

- Host is up with low latency and resolves to hostname box5331.bluehost.com (an IP in a hosted/server network range).
  - 16 TCP ports are reported open: 21, 22, 25, 53, 80, 110, 143, 443, 465, 587, 993, 995, 2222, 3306, 5432 plus 993/995 already counted, with services identified as ftp, ssh, smtp, domain (DNS over TCP), http, pop3, imap, https, smtps, submission, imaps, pop3s, EtherNetIP-1 (on 2222), mysql, and postgresql.
  - Remaining scanned TCP ports (up to 1000) are shown as closed/filtered and not listed individually.



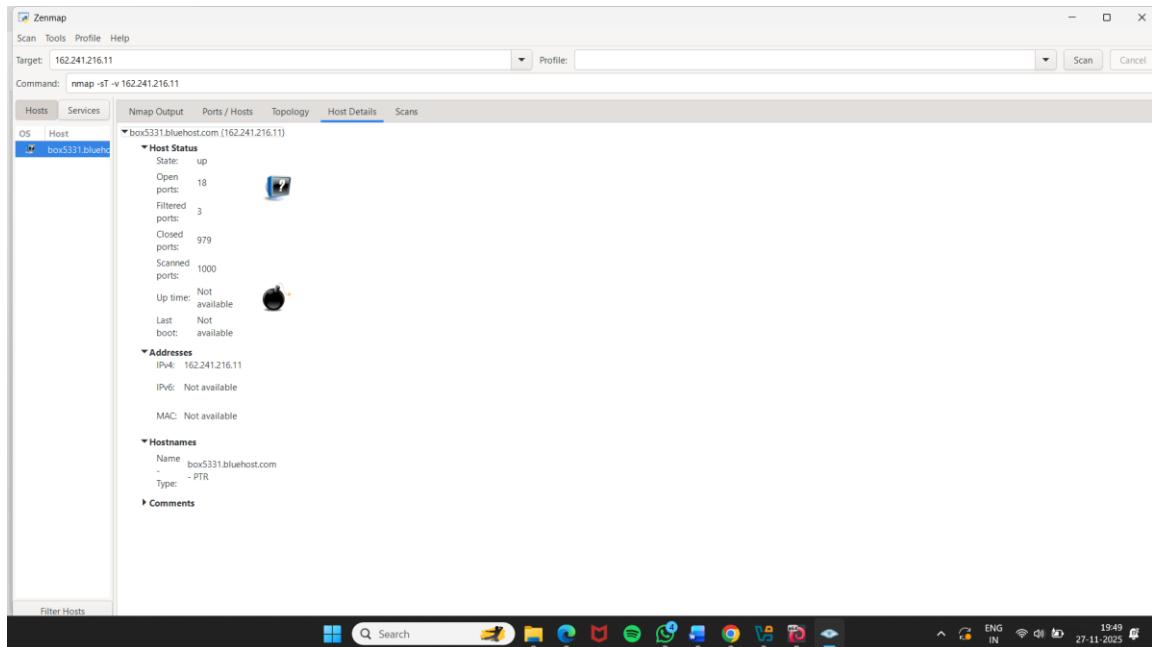
Fig(8)

The image shows the Ports / Hosts tab of the Zenmap graphical user interface, which is displaying the results of a successful Nmap port scan executed against the target IP address 162.241.216.11.

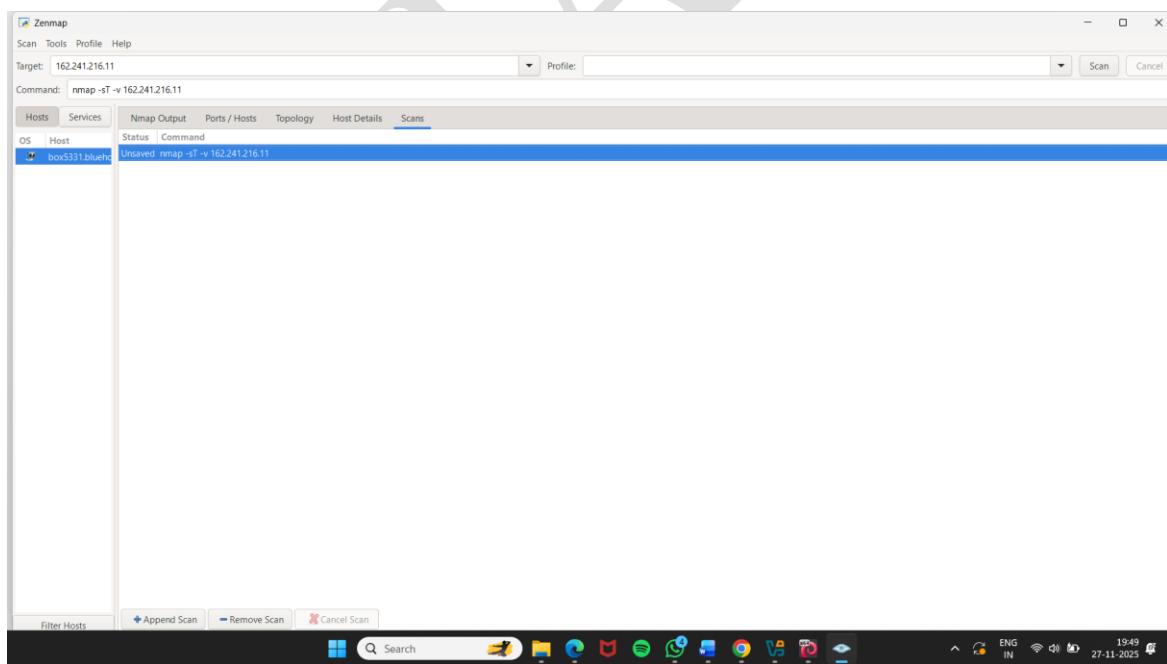


Fig(9)

The image displays the Topology tab within the Zenmap graphical user interface, showing a network visualization of the scan results.



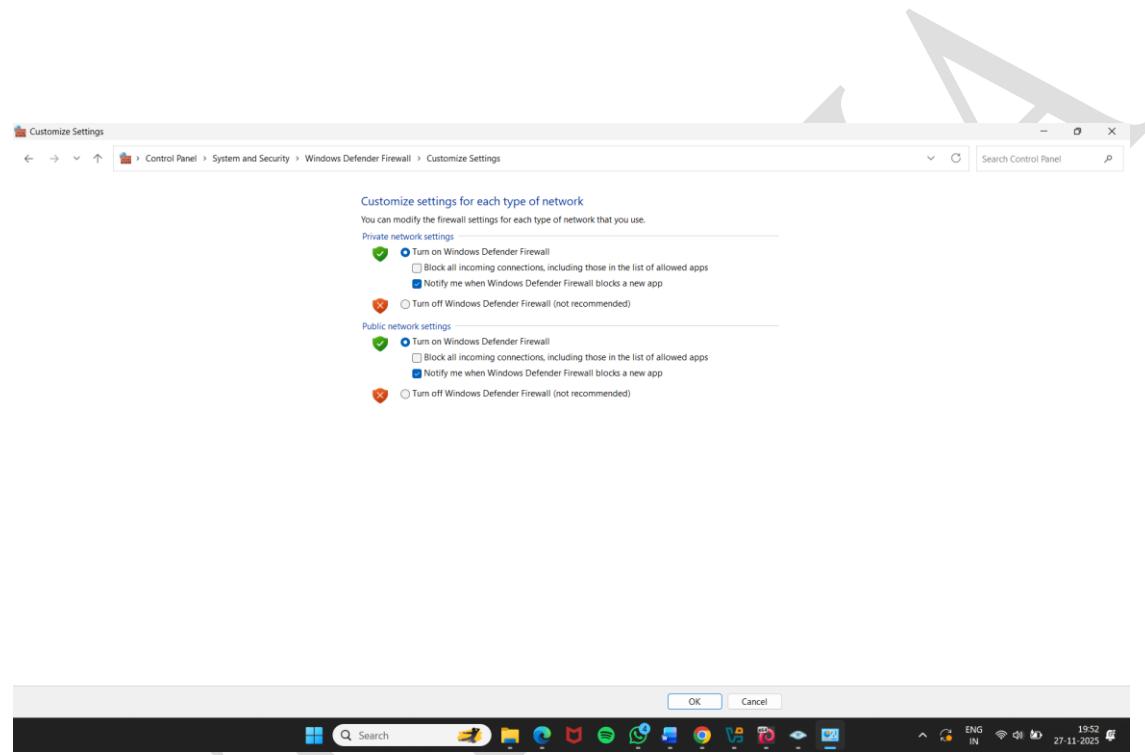
Fig(10)



Fig(11)

In this sub-task, we have performed a **Stealth scan/TCP half-open scan**, **Xmas scan**, **TCP Maimon scan**, and **ACK flag probe scan** on a firewall-enabled machine.

Step: Navigate to Control Panel System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off, enable Windows Firewall and click OK, as shown.



Fig(12)

## Test/Tool Shown:

Zmap (Zenmap GUI) – Nmap Stealth SYN Scan (-sS).

## Step Performed:

A verbose SYN scan was executed to discover open TCP ports without completing full connections. (nmap -sS -v 162.241.216.11)

## Output:

The screenshot shows the Zenmap interface with the target set to 162.241.216.11. The 'Nmap Output' tab is selected, displaying a detailed list of open ports and services. The output text is as follows:

```
Scanning: box5331.bluehost.com (162.241.216.11)
Completed: 1 IP address (1 host up) scanned in 13.89 seconds
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.31s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    filtered  nntp
25/tcp    open     smtp
26/tcp    open     rsmtp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
1433/tcp  open     microsoft-ds
443/tcp   open     https
445/tcp   filtered  microsoft-ds
465/tcp   open     smtps
587/tcp   open     submission
993/tcp   open     imaps
995/tcp   open     pop3s
2222/tcp  open     EtherNetIP-1
3306/tcp  open     mysql
5432/tcp  open     postgresql

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 13.89 seconds
Raw packets sent: 1067 (46.924KB) | Rcvd: 1084 (43.552KB)
```

Fig(13)

## Output:

The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

**Note:** The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.

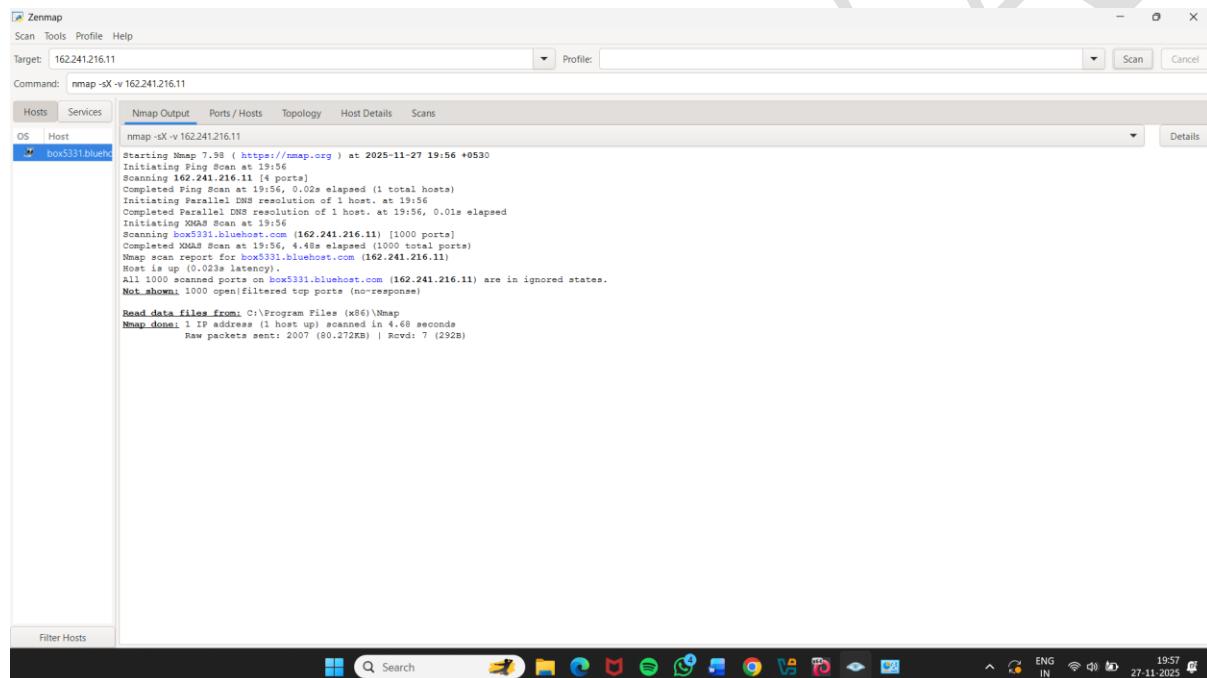
## Test/Tool Shown:

Zenmap – XMAS scan (-sX).

## Step Performed:

An XMAS scan was run to probe firewall behavior using FIN, URG, PSH flags.  
(nmap -sX -v 162.241.216.11)

## Output:



The screenshot shows the Zenmap interface with the following details:

- Target:** 162.241.216.11
- Command:** nmap -sX -v 162.241.216.11
- Host:** box331.bluehost.com
- OS:** Linux
- Nmap Output:**

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-27 19:56 +0530
Initiating Ping Scan at 19:56
Scanning 162.241.216.11 (1 host)
Completed Parallel DNS resolution of 1 host. at 19:56
Initiating XMAS Scan at 19:56
Scanning box331.bluehost.com (162.241.216.11) [1000 ports]
Completed Parallel DNS resolution of 1 host. at 19:56, 0.01s elapsed
Initiating Nmap report at 19:56
Scanning box331.bluehost.com (162.241.216.11) [1000 ports]
Completed Parallel DNS resolution of 1 host. at 19:56, 4.48s elapsed (1000 total ports)
Nmap scan report for box331.bluehost.com (162.241.216.11)
Host is up (0.023s latency).
All 1000 scanned ports on box331.bluehost.com (162.241.216.11) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds
Raw packets sent: 2007 (80.272KB) | Rcvd: 7 (292B)
```

Fig(14)

- All 1000 ports are in ignored states
- Not shown: 1000 open|filtered tcp ports (no-response)

**Note:** Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

## Test/Tool Shown:

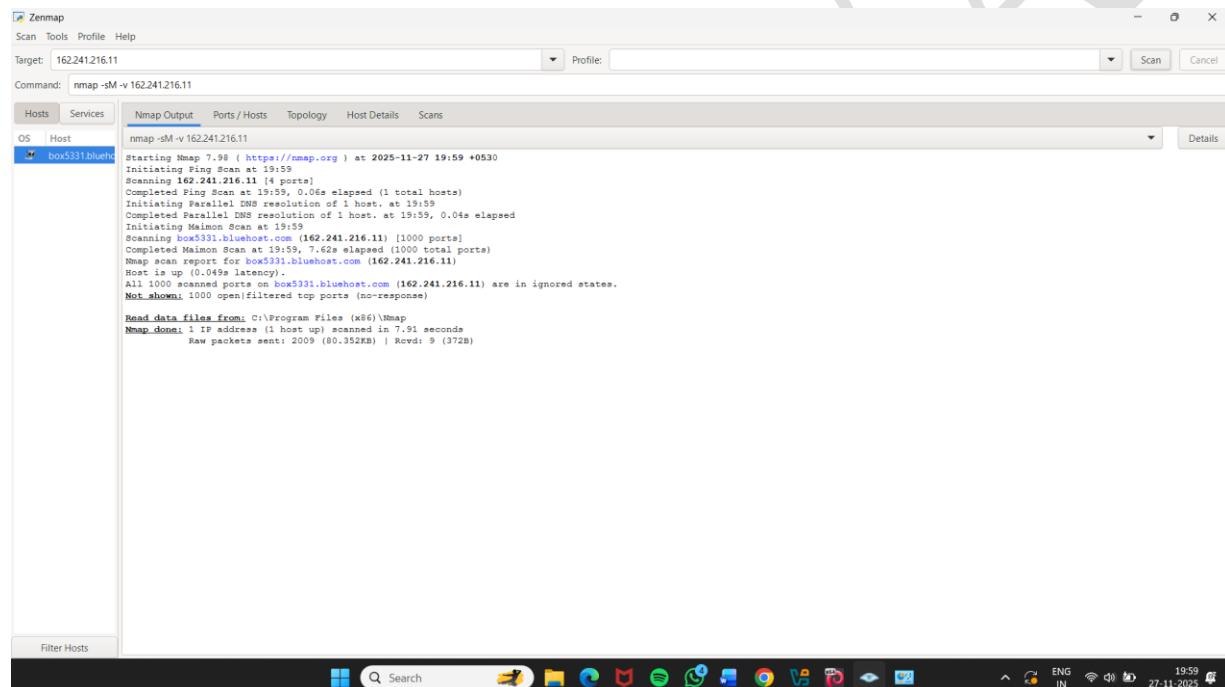
Zenmap – Maimon Scan (-sM).

## Step Performed:

Executed a Maimon TCP FIN/ACK probe to detect filtering anomalies.

(nmap -sM -v 162.241.216.11)

## Output:



```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-27 19:59 +0530
Initiating Ping Scan at 19:59
Scanning 162.241.216.11 [4 ports]
Completed Ping Scan at 19:59, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:59
Completed Parallel DNS resolution of 1 host. at 19:59, 0.04s elapsed
Initiating Maimon Scan at 19:59
Scanning box5331.bluehost.com (162.241.216.11) [1000 ports]
Completed Maimon Scan at 19:59, 7.62s elapsed (1000 total ports)
Nmap done: 1 IP address (1 host up) scanned in 7.91 seconds
Host is up (0.049s latency).
All 1000 scanned ports on box5331.bluehost.com (162.241.216.11) are in ignored states.
Not shown: 1000 open|filtered ports (no-response)

Read data files from: C:\Program Files (x86)\Nmap
Nmap.done: 1 IP address (1 host up) scanned in 7.91 seconds
Raw packets sent: 2009 (80.352KB) | Rcvd: 9 (372B)
```

Fig(15)

- All 1000 ports are in ignored states
- Server gave no responses.

**Note:** In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open | Filtered, but if the RST packet is sent as a response, then the port is closed.

## Test/Tool Shown:

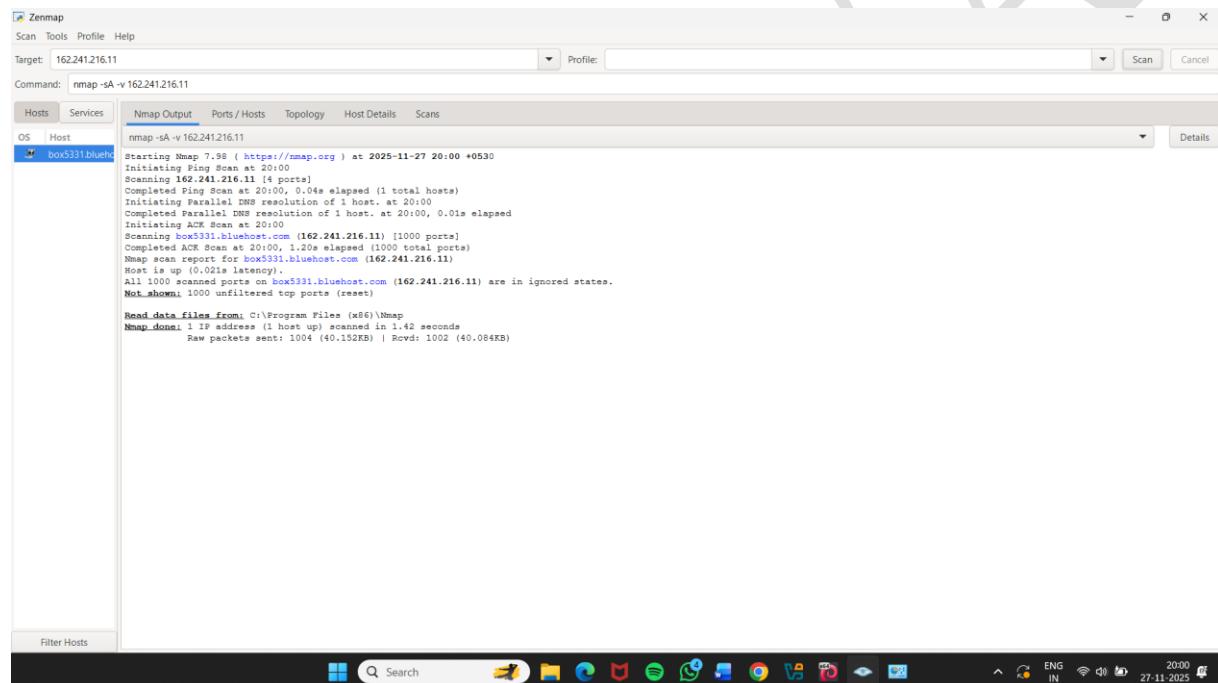
Zenmap – ACK scan (-sA).

## Step Performed:

An ACK scan was run to detect firewall rules, not open ports.

(nmap -sA -v 162.241.216.11)

## Output:



The screenshot shows the Zenmap interface with the following details:

- Scan Tab:** Selected.
- Target:** 162.241.216.11
- Command:** nmap -sA -v 162.241.216.11
- Host:** box331.bluehost.com (162.241.216.11)
- OS:** Not shown
- Services:** Nmap Output tab selected. The output shows:
  - Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-27 20:00 +0530
  - Initiating Ping Scan at 20:00
  - Scanning 162.241.216.11 [4 ports]
  - Completed Ping Scan at 20:00, 0.04s elapsed (1 total hosts)
  - Initiating Parallel DNS resolution of 1 host at 20:00
  - Completed Parallel DNS resolution of 1 host at 20:00, 0.01s elapsed
  - Initiating ACK Scan at 20:00
  - Scanning box331.bluehost.com (162.241.216.11) [1000 ports]
  - Completed ACK Scan at 20:00, 1.20s elapsed (1000 total ports)
  - Raw packets sent: 1004 (40.152KB) | Rcvd: 1002 (40.084KB)
  - Host is up (0.021s latency).
  - All 1000 scanned ports on box331.bluehost.com (162.241.216.11) are in ignored states.
  - Not shown: 1000 unfiltered top ports (reset)
- Ports / Hosts:** Shows 1 IP address (1 host up) scanned in 1.42 seconds.
- Topology:** Not applicable for this scan type.
- Host Details:** Not applicable for this scan type.
- Scans:** Not applicable for this scan type.

Fig(16)

- **All 1000 ports: unfiltered**
- Host responds with RST to ACK probes.

**Note:** The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.

## Test/Tool Shown:

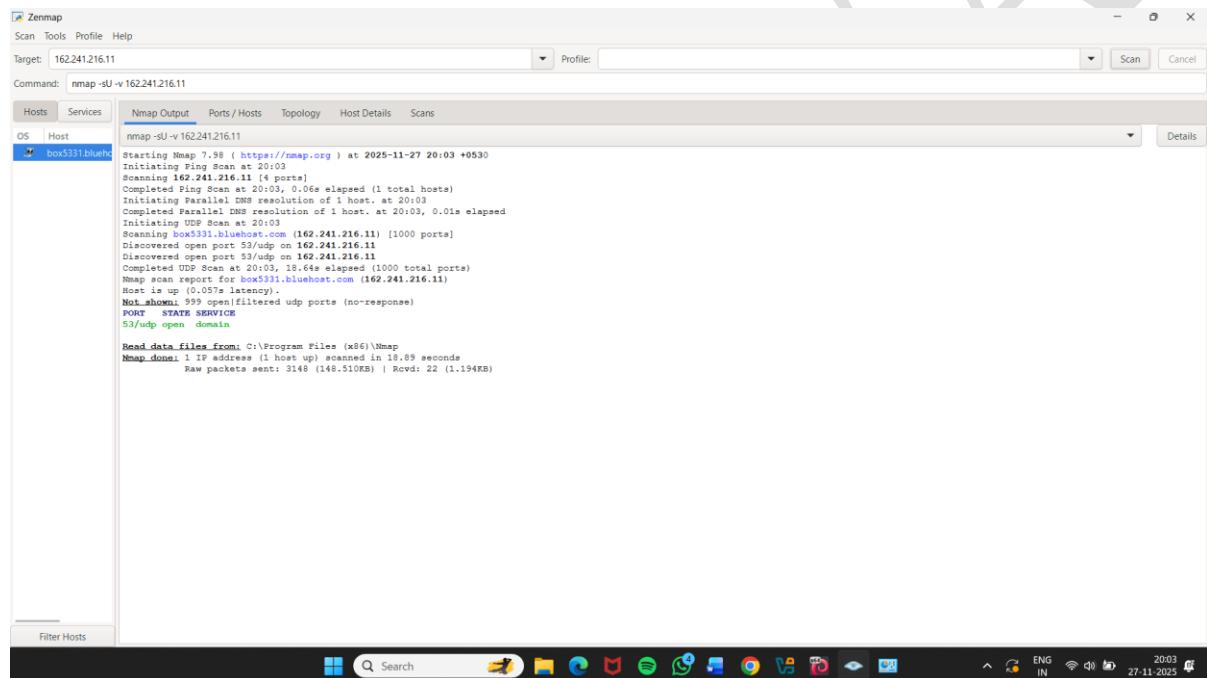
Zenmap – UDP scan (-sU).

## Step Performed:

A verbose UDP scan was executed on all 1000 UDP ports.

(nmap -sU -v 162.241.216.11)

## Output:



```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-27 20:03 +0530
Initiating Ping Scan at 20:03
Scanning 162.241.216.11 (4 ports)
Completed Parallel DNS resolution of 1 host. at 20:03
Completed Parallel Nmap resolution of 1 host. at 20:03, 0.01ms elapsed
Initiating UDP Scan at 20:03
Scanning box331.bluehost.com (162.241.216.11) [1000 ports]
Completed UDP Scan at 20:03, 18.64s elapsed (1000 total ports)
Nmap scan report for box331.bluehost.com (162.241.216.11)
Host is up (0.057s latency).
Not shown: 995 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 18.89 seconds
Raw packets sent: 3140 (146.510KB) | Rcvd: 22 (1.194KB)
```

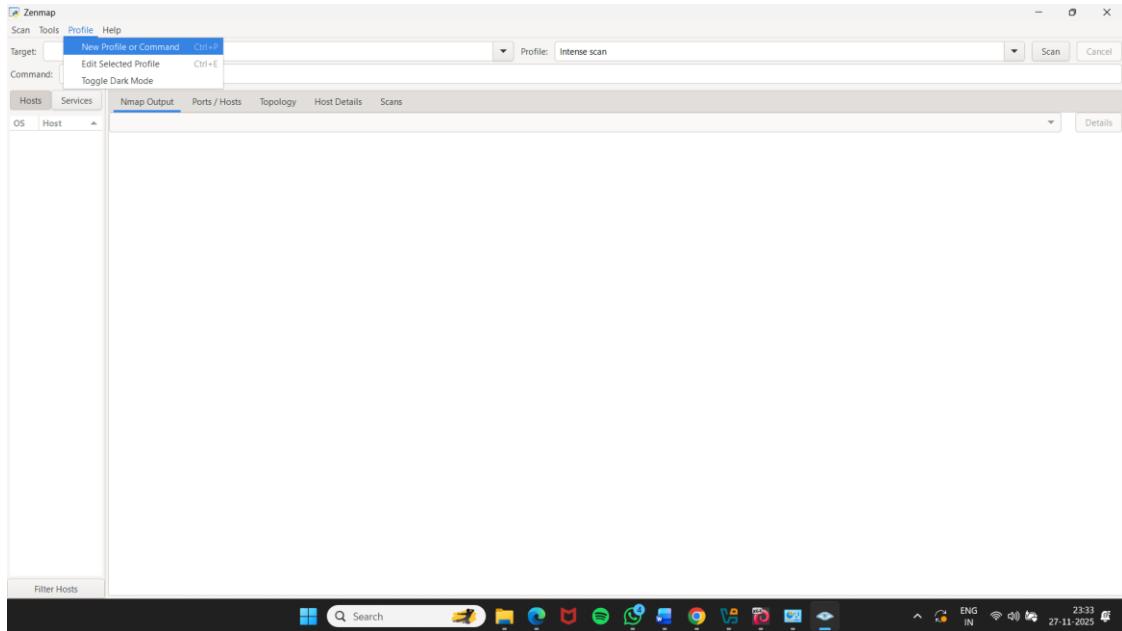
Fig(17)

- Only **port 53/udp (DNS)** is open.
- All others are **open|filtered** (typical for UDP).
- “No response” means UDP packets are dropped silently.

**Note:** The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.

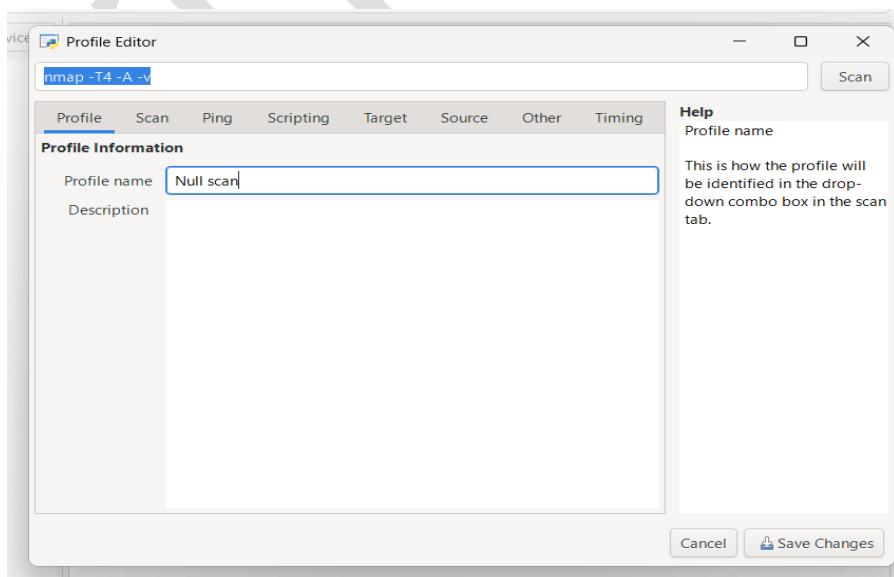
## Creating a Scan Profile:

- Open Nmap - Zenmap GUI app.
- To create a scan profile; click Profile → New Profile or Command.



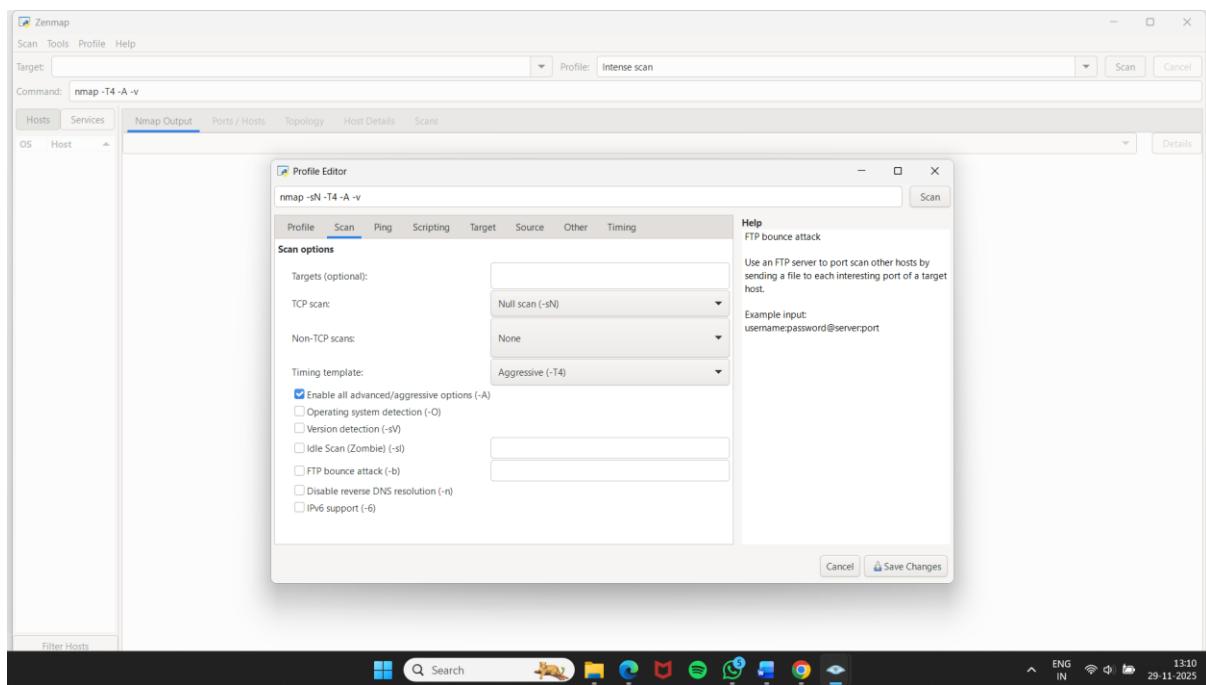
Fig(18)

- The Profile Editor window appears. In the Profile tab, under the Profile Information section, input a profile name (Null Scan) into the Profile name field.



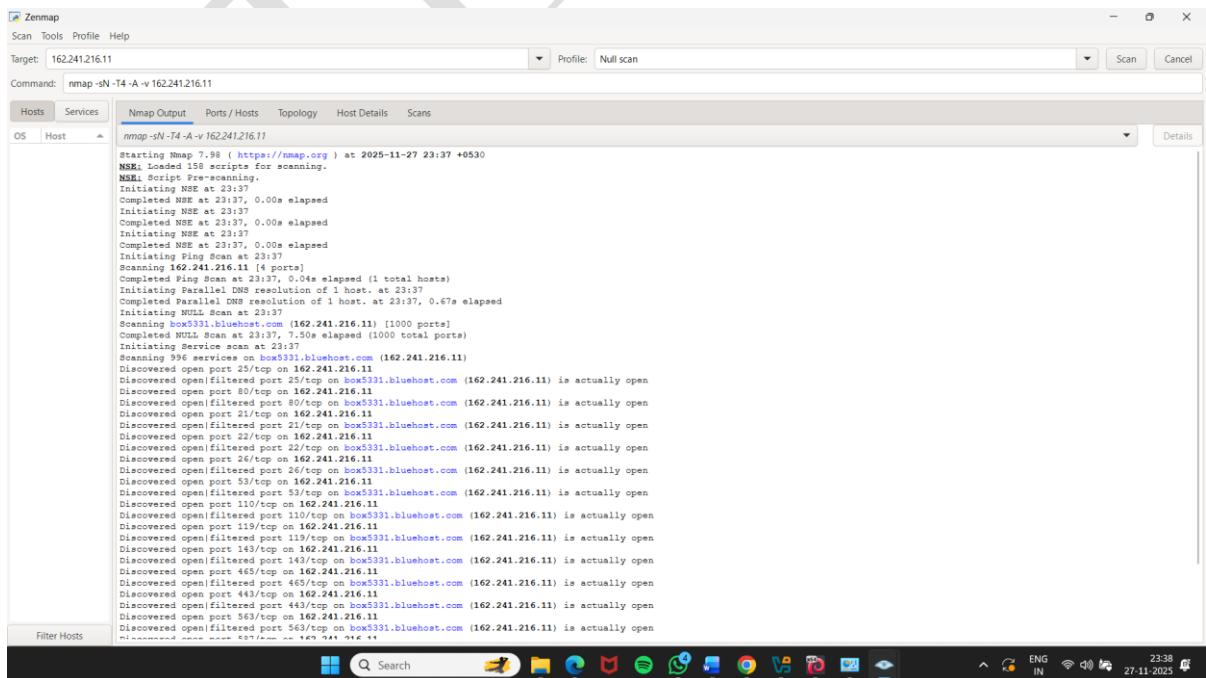
Fig(19)

- click the Scan tab and select the scan option (here, Null scan (-sN)) from the TCP scan drop-down list.



Fig(20)

- This will create a new profile and will thus be added to the profile list.
- In the main window of Zenmap, enter the target IP address (162.241.216.11) in the Target field to scan. Select the Null Scan profile, which you created from the Profile drop-down list, and then click Scan.



Fig(21)

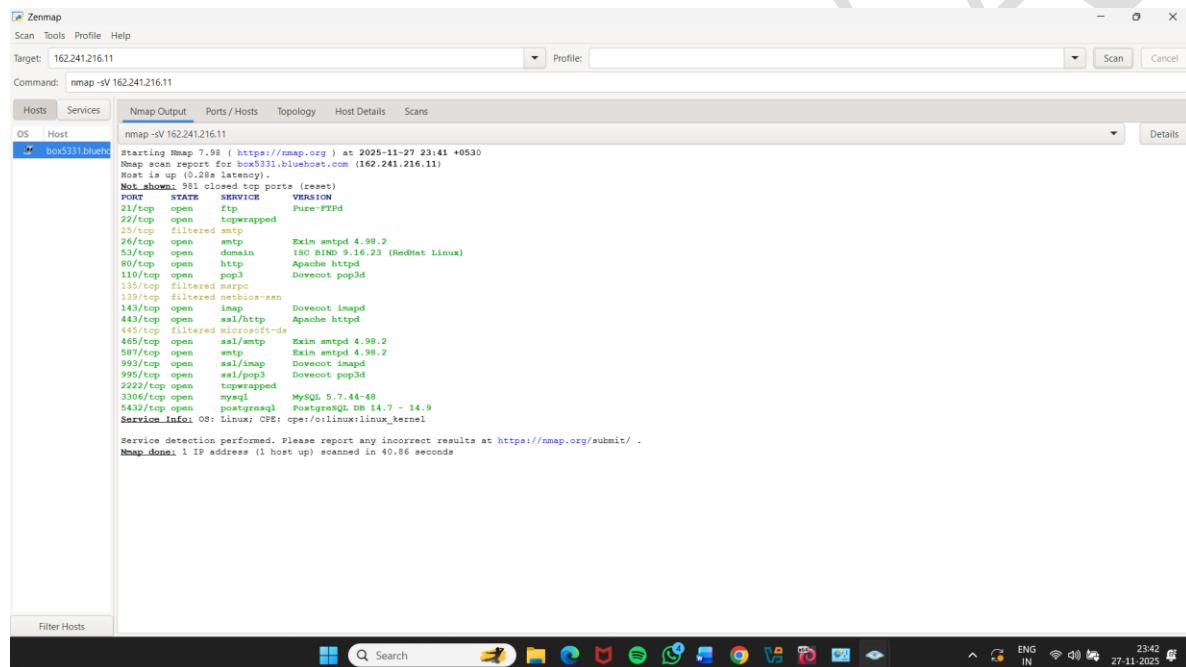
## Test/Tool Shown:

Zenmap (Nmap GUI) — Version Detection Scan (-sV).

## Step Performed:

A service/version detection scan was run on the target host:  
(nmap -sV 162.241.216.11)

## Output:



The screenshot shows the Zenmap interface with the target set to 162.241.216.11 and the command set to nmap -sV 162.241.216.11. The Services tab is selected, displaying a table of open ports and their corresponding services and versions. The table includes columns for PORT, STATE, SERVICE, and VERSION. Key findings include port 21/tcp (FTP) running Pure-FTPD, port 80/tcp (HTTP) running Apache httpd, and port 443/tcp (SSL/TLS) running Apache httpd. Other ports listed include 22/tcp (SSH), 25/tcp (SMTP), 465/tcp (SMTPS), 53/tcp (DNS), 110/tcp (POP3), 139/tcp (NetBIOS-SSN), 143/tcp (IMAP), 587/tcp (SMTP), 993/tcp (IMAPS), and 995/tcp (POP3S). The output also indicates 991 closed TCP ports. A note at the bottom states "Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>. Nmap done: 1 IP address (1 host up) scanned in 40.86 seconds".

Fig(22)

- Open Ports & Services Identified.
- 991 TCP ports were closed.
- Version detection succeeded on most open ports.
- Host appears to be a Bluehost shared hosting server.

**Note:** -A: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

# OS DISCOVERY

OS discovery (or OS fingerprinting) is the process of finding out which operating system a remote machine is running — for example:

- Windows 10
- Windows Server
- Linux (Ubuntu, CentOS, Debian, etc.)
- macOS
- Network OS (Cisco, Juniper, MikroTik)

OR

Banner grabbing, or OS fingerprinting, is a method used to determine the OS that is running on a remote target system.

Kali Linux uses tools like Nmap, Netcat, and TTL analysis to make an educated guess about the OS based on how the target responds to network packets.

There are two types of OS discovery or banner grabbing techniques:

**Active Banner Grabbing** Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.

**Passive Banner Grabbing** This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

## Test/Tool Shown:

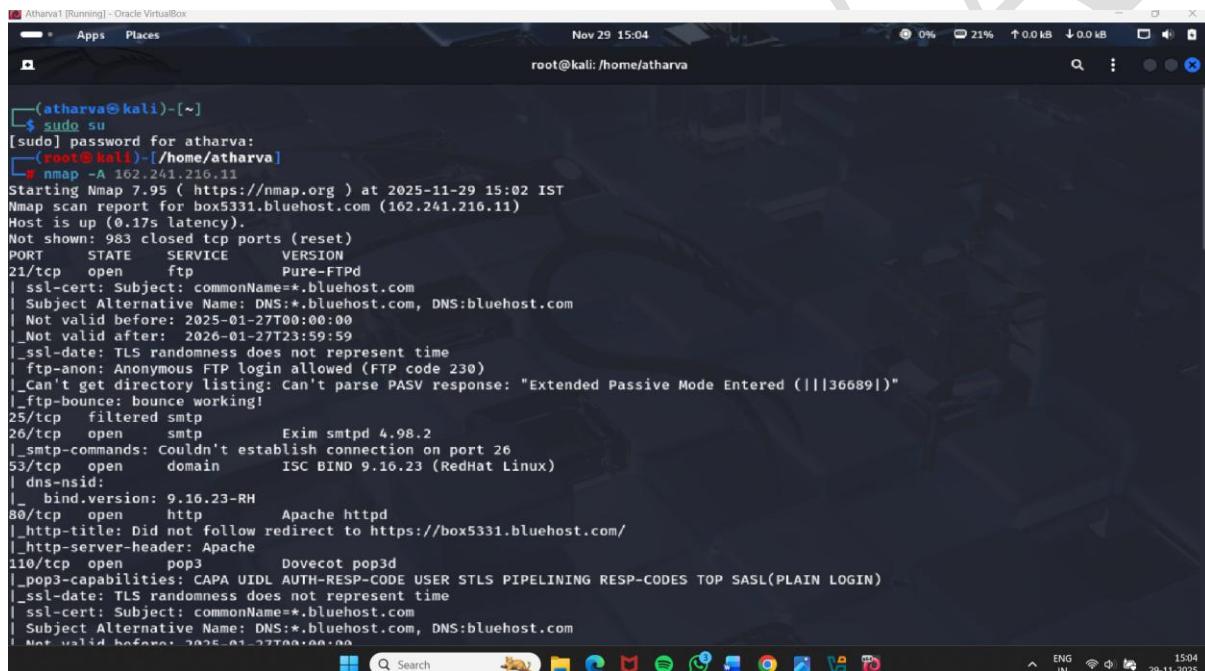
Nmap (Aggressive Scan -A)

## Step Performed:

Executed: nmap -A 162.241.216.11

This performs: OS detection, Version detection, Script scanning, Traceroute.

## Output:



```
(atharva㉿kali)-[~]
$ sudo su
[sudo] password for atharva:
[root@kali]-[~/home/atharva]
# nmap -A 162.241.216.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 15:02 IST
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.17s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp          Pure-FTPD
|_ssl-cert: Subject: commonName=*.bluehost.com
| Subject Alternative Name: DNS:*.bluehost.com, DNS:bluehost.com
| Not valid before: 2025-01-27T00:00:00
| Not valid after: 2026-01-27T23:59:59
|_ssl-date: TLS randomness does not represent time
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: Can't parse PASV response: "Extended Passive Mode Entered (|||36689|)"
|_ftp-bounce: bounce working!
25/tcp    filtered smtp
26/tcp    open      smtp        Exim smtpd 4.98.2
|_smtp-commands: Couldn't establish connection on port 26
53/tcp    open      domain      ISC BIND 9.16.23 (RedHat Linux)
| dns-nsid:
|_ bind.version: 9.16.23-RH
80/tcp    open      http        Apache httpd
|_http-title: Did not follow redirect to https://box5331.bluehost.com/
|_http-server-header: Apache
110/tcp   open      pop3       Dovecot pop3d
|_pop3-capabilities: CAPA UIDL AUTH-RESP-CODE USER STLS PIPELINING RESP-CODES TOP SASL(PLAIN LOGIN)
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=*.bluehost.com
| Subject Alternative Name: DNS:*.bluehost.com, DNS:bluehost.com
| Not valid before: 2025-01-27T00:00:00
```

Fig(23)

- Open ports & Services Detected
- The server is a Bluehost shared hosting machine.
- Many mail services (POP/IMAP/SMTP) are running.
- Both MySQL and PostgreSQL are publicly accessible, which is unsafe.
- FTP is active.

## Test/Tool Shown:

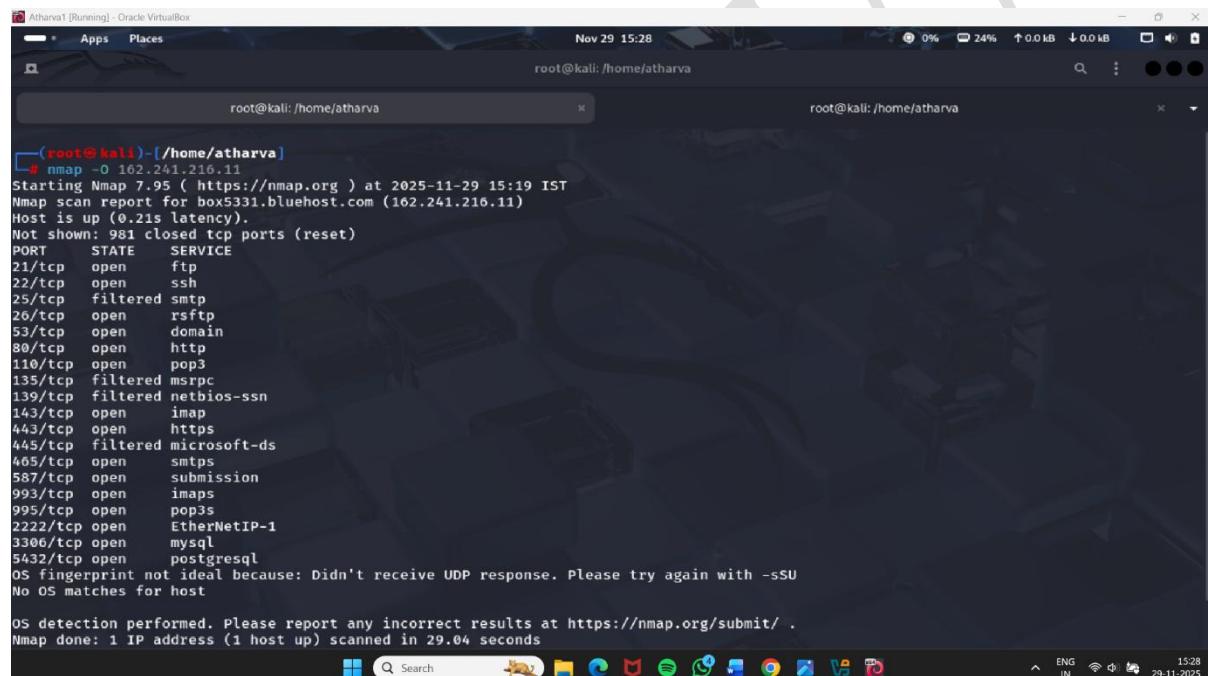
Nmap OS Detection Scan (-O)

## Step Performed:

Executed: nmap -O 162.241.216.11

This attempts to identify the OS via network fingerprinting

## Output:



The screenshot shows a terminal window titled 'Atharva1 [Running] - Oracle VirtualBox' with two tabs open. The left tab shows the command: 'root@kali: /home/atharva# nmap -O 162.241.216.11'. The right tab shows the results of the scan. The results output is as follows:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 15:19 IST
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.21s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    filtered  smtp
26/tcp    open      rsftp
53/tcp    open      domain
80/tcp    open      http
110/tcp   open      pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open      imap
443/tcp   open      https
445/tcp   filtered microsoft-ds
465/tcp   open      smtps
587/tcp   open      submission
993/tcp   open      imaps
995/tcp   open      pop3s
2222/tcp  open      EtherNetIP-1
3306/tcp  open      mysql
5432/tcp  open      postgresql
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.04 seconds
```

Fig(24)

- Open Ports Detected (same as aggressive scan, but without version banners)
- OS detection failed because the host's firewall blocks UDP probes.
- Filtered ports (25,135,139,445) indicate firewall protection is active.

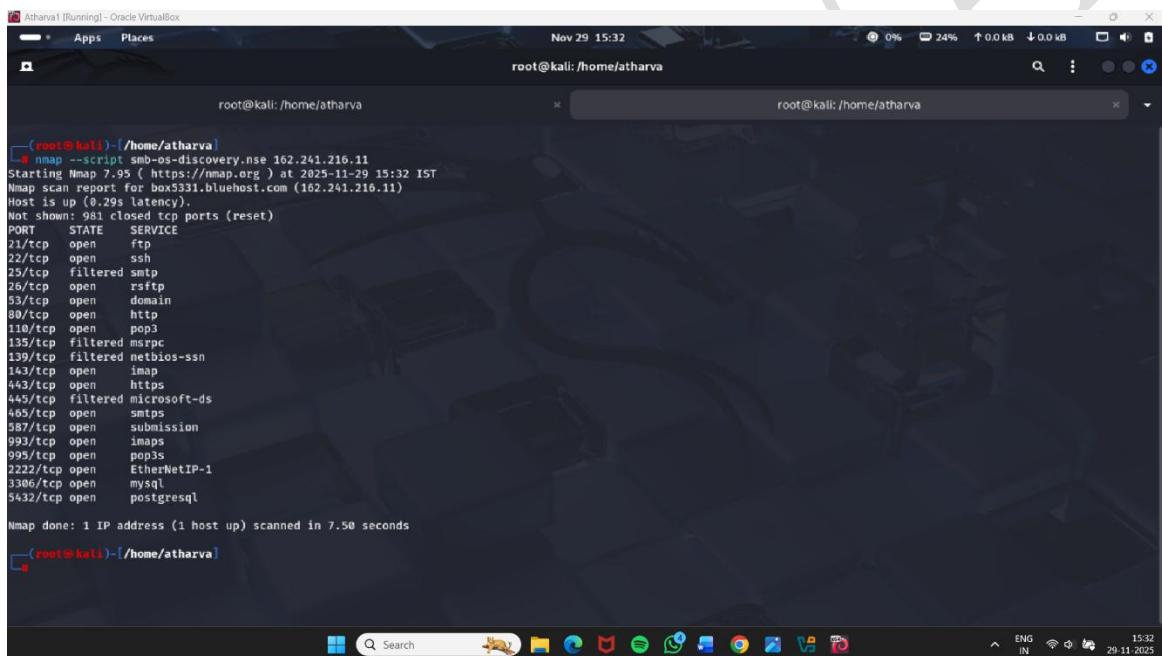
## **Test/Tool Shown:**

nmap --script smb-os-discovery.nse

## **Step Performed:**

Executed the command to detect SMB-related OS information, to enumerate Windows-style SMB shares or metadata, to check SMB version or domain/workgroup details.

## **Output:**



```
root@kali:~/home/atharva
nmap --script smb-os-discovery.nse 162.241.216.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 15:32 IST
Nmap scan report for box5331.bluehost.com (162.241.216.11)
Host is up (0.29s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    filtered  smtp
26/tcp    open      rsftp
53/tcp    open      domain
80/tcp    open      http
110/tcp   open      pop3
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
143/tcp   open      imap
443/tcp   open      https
445/tcp   filtered  microsoft-ds
465/tcp   open      smtps
587/tcp   open      submission
993/tcp   open      imaps
995/tcp   open      pop3s
2222/tcp  open      EtherNetIP-1
3306/tcp  open      mysql
5432/tcp  open      postgresql

Nmap done: 1 IP address (1 host up) scanned in 7.50 seconds
```

Fig(25)

- Ports Detected.
- The script returned NO SMB information because port 445 (SMB) is filtered, not open.

## Scan Beyond IDS and Firewall

Scanning beyond IDS and firewall is a process of sending intended packets to the target system in order to exploit IDS/firewall limitations.

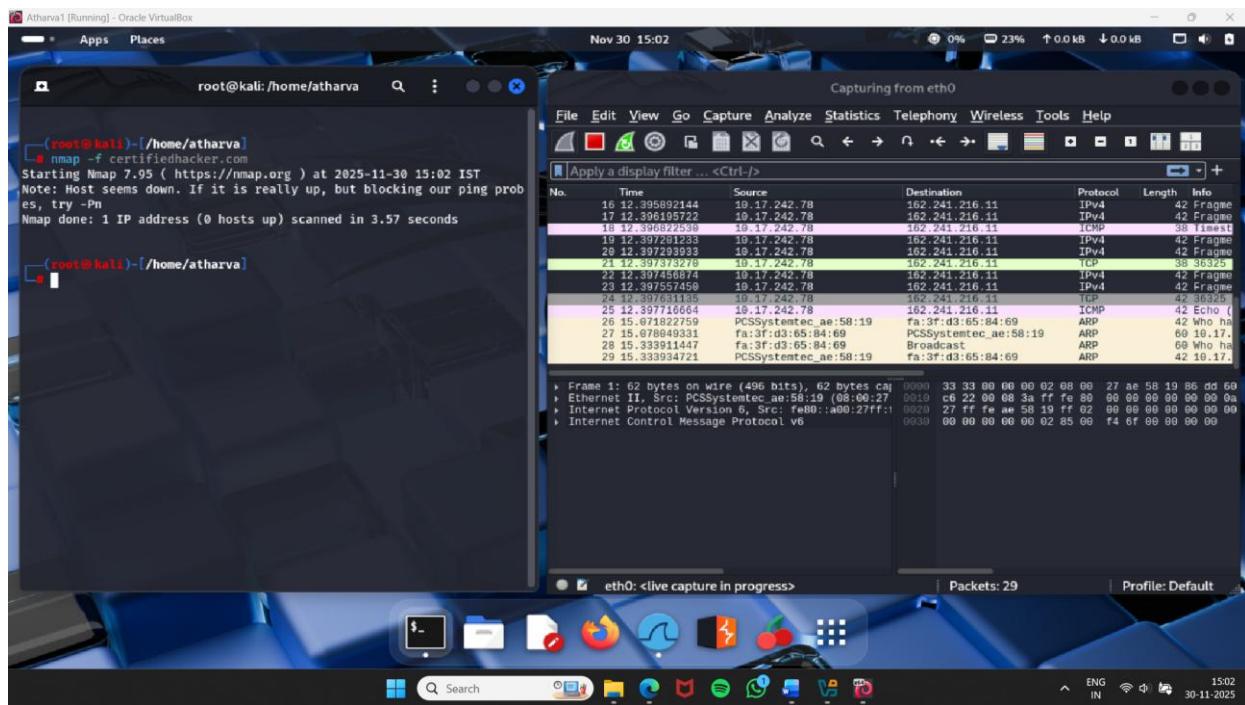
An Intrusion Detection System (IDS) and firewall are the security mechanisms intended to prevent an unauthorized person from accessing a network. However, even IDSs and firewalls have some security limitations. Firewalls and IDSs intend to avoid malicious traffic (packets) from entering into a network, but certain techniques can be used to send intended packets to the target and evade IDSs/firewalls.

### Techniques to evade IDS/firewall:

- Packet Fragmentation
- Source Routing
- Source Port Manipulation
- IP Address Decoy
- IP Address Spoofing
- Creating Custom Packets
- Sending Bad Checksums
- Proxy Servers
- Randomizing Host Order

## Test/Tool Shown:

### 1)Nmap (normal scan) + Wireshark packet capture



Fig(26)

## Step Performed:

Command executed: nmap -f certifiedhacker.com  
Fragmentation scan attempted.

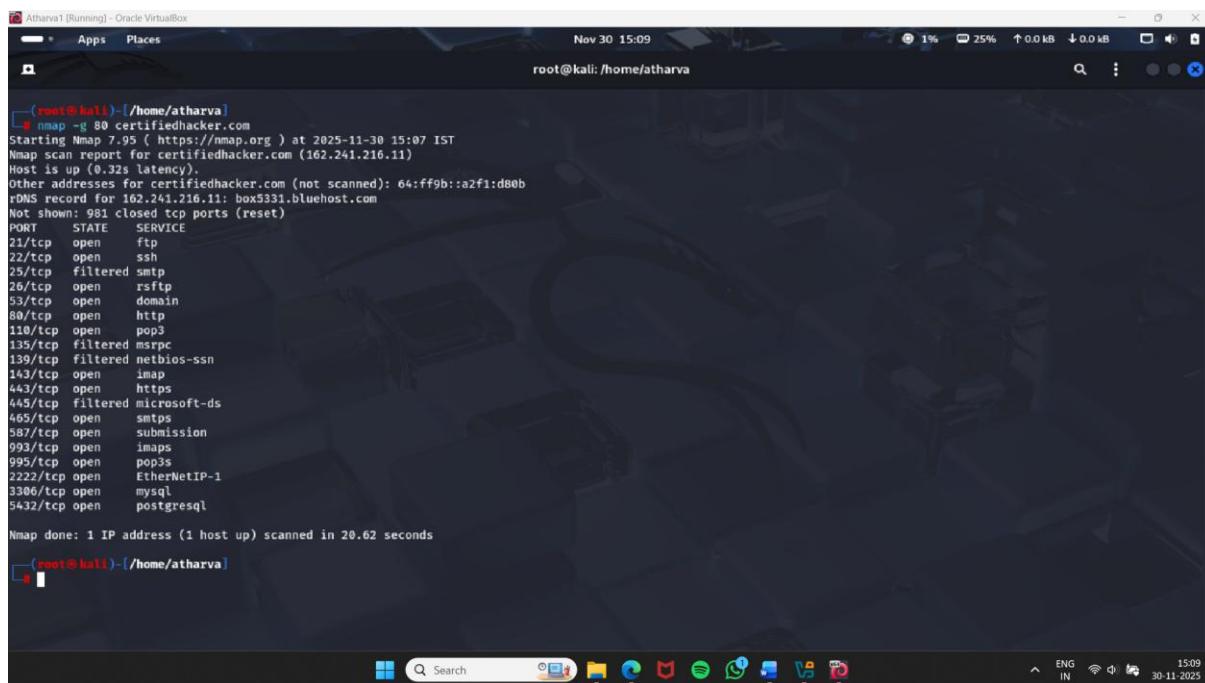
## Output:

- Wireshark shows outbound packets from 10.17.242.78 → 162.241.216.11, but no meaningful replies.
- The target host blocked fragmented packets (-f) or ICMP echo requests.
- Host is alive, but firewall rejects Nmap's discovery probes.

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

## Test/Tool Shown:

2)Nmap verbose + packet tracing.



```
(root㉿kali)-[~/home/atharva]
└─# nmap -v -g 80 certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 15:07 IST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.32s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff9b:a2f1:d8eb
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    filtered smtp
26/tcp    open     rsftp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
445/tcp   filtered microsoft-ds
465/tcp   open     smtps
587/tcp   open     submission
993/tcp   open     imaps
995/tcp   open     pop3s
2222/tcp  open     EtherNetIP-1
3306/tcp  open     mysql
5432/tcp  open     postgresql

Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds
└─#
```

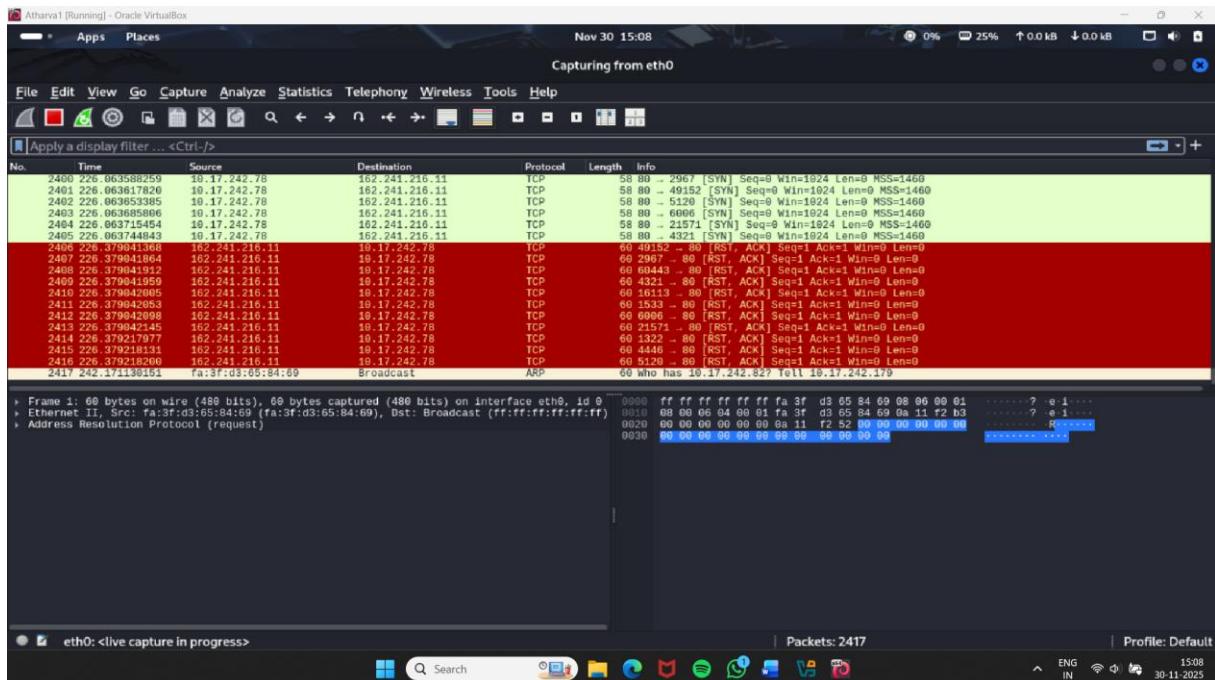
Fig(27)

## Step Performed:

Command executed: nmap -v -g 80 certifiedhacker.com  
(Source port spoofed as port 80)

## Output:

- Nmap discovered multiple open ports:
- 80, 993, 110, 21, 995, 443, 587, 143, 3306, 26, 2222, 5432 etc.
- Many shared hosting servers allow traffic from port 80 due to “firewall trust” policy.



Fig(28)

**Note:** Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.

## Test/Tool Shown:

### 3)Nmap with fragmentation MTU

```
(root@kali)-[~]
# nmap -mtu 96 certifiedhacker.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 19:53 IST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.27s latency).
Other addresses for certifiedhacker.com (not scanned): 64:ff:9b:a2:f1:d8eb
rDNS record for 162.241.216.11: box331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filtered smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   filtered microsoft-ds
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2222/tcp  open  EtherNetIP-1
3306/tcp  open  mysql
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 46.05 seconds

```

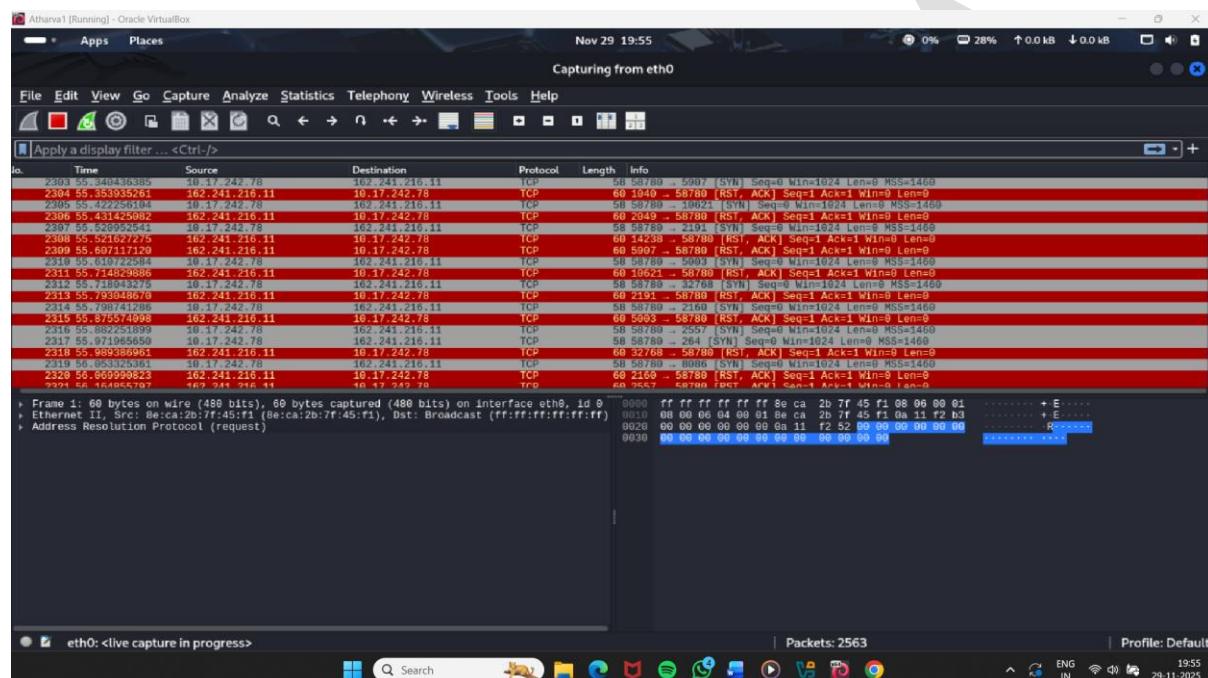
Fig(29)

## Step Performed:

Command executed: nmap --mtu 96 certifiedhacker.com

## Output:

- Host responded normally.
- Same ports open as previous scan.
- Smaller packets are transmitted instead of sending one complete packet at a time.

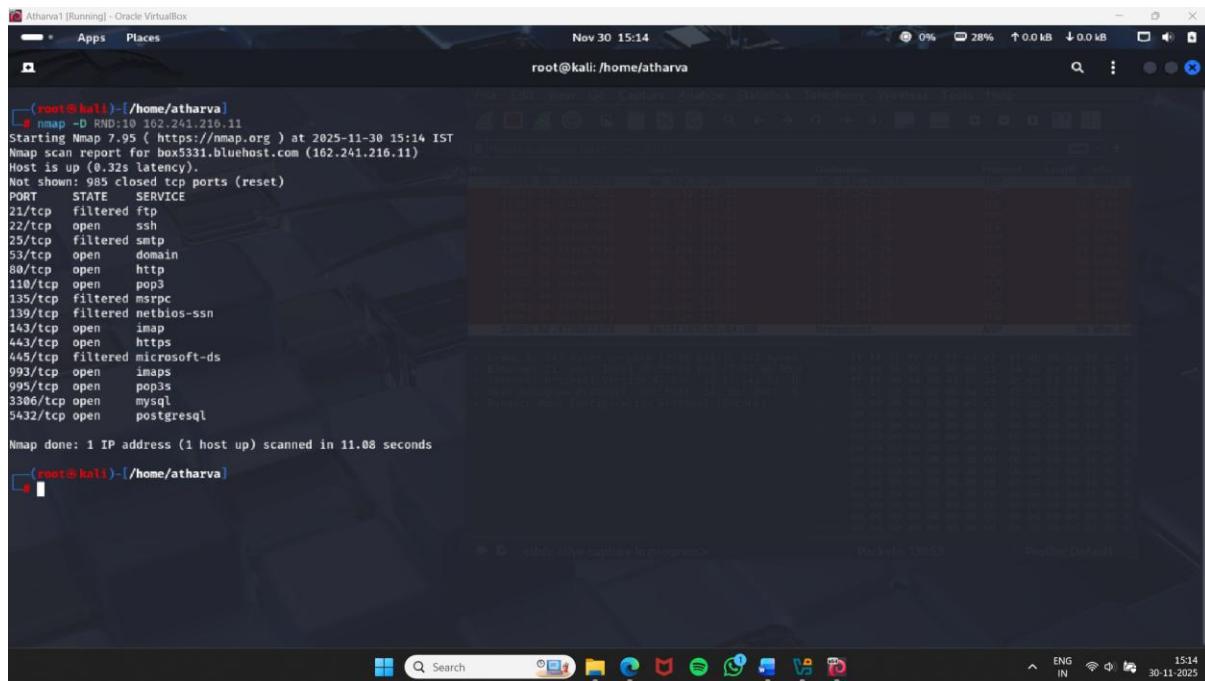


Fig(30)

**Note:** Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.

## Test/Tool Shown:

### 4)Nmap decoy scan



The screenshot shows a terminal window titled "Atharva1 [Running] - Oracle VirtualBox". The command entered was "nmap -D RND:10 162.241.216.11". The output shows a scan report for the host 162.241.216.11, which is up with 0.32s latency. The scan found 985 closed TCP ports (reset). It lists various open and filtered ports, including 22/tcp (ssh), 25/tcp (smtp), 80/tcp (http), 110/tcp (pop3), 135/tcp (msrpc), 139/tcp (netbios-ssn), 143/tcp (imap), 443/tcp (https), 445/tcp (microsoft-ds), 993/tcp (imaps), 995/tcp (pop3s), 3306/tcp (mysql), and 5432/tcp (postgresql). The scan took 11.08 seconds. The terminal prompt "(root㉿kali)-[~/home/atharva]" is visible at the bottom.

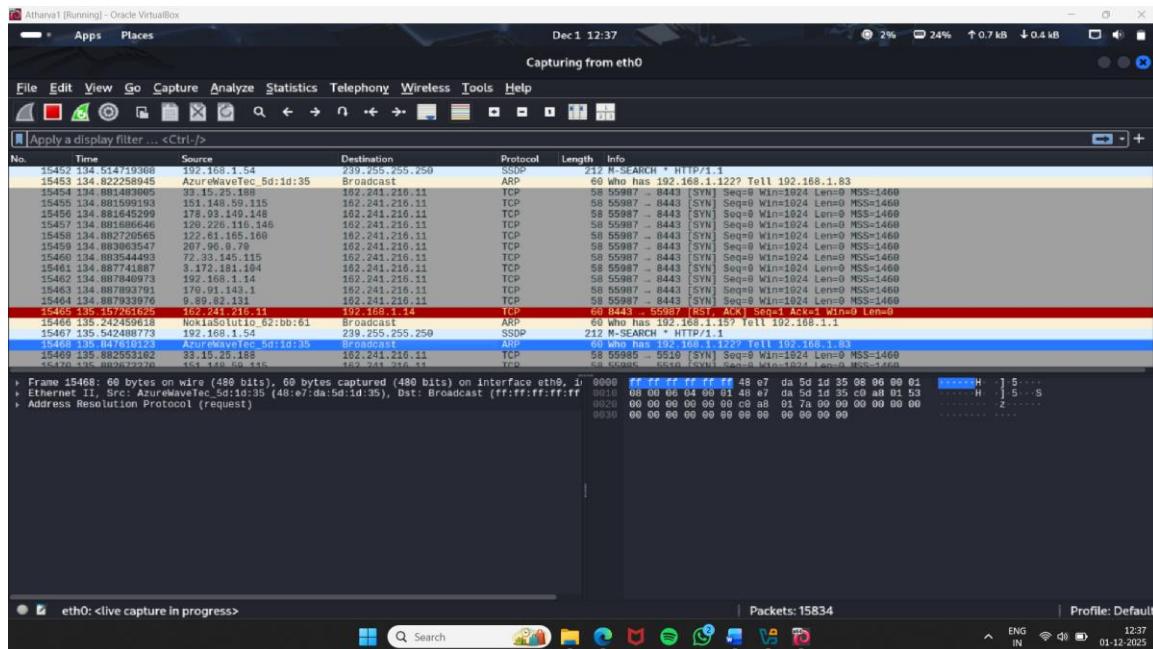
Fig(31)

## Step Performed:

```
nmap -D RND:10 162.241.216.11
```

## Output:

- Decoy scan completed.
- Same ports appear open.
- Nmap automatically generated a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.



Fig(32)

**Note:** This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys and you can observe the packets displaying the multiple IP addresses in the source section, as shown in the screenshot.

## 5) Test/Tool Shown:

Nmap 7.95 – TCP Connect Scan (-sT), no ping (-Pn), random MAC address spoofing.

```
(root@kali:~) [~]
nmap -sT -Pn --spoof-mac 0 162.241.216.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 12:50 IST
Spoofing MAC address 00:0B:02:E9:D1:05 (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for box331.bluehost.com (162.241.216.11)
Host is up (0.31s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    open     smtp
26/tcp    open     rsftp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered rpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
445/tcp   filtered microsoft-ds
465/tcp   open     smtps
587/tcp   open     submission
993/tcp   open     imaps
995/tcp   open     pop3s
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1094/tcp  filtered LSA-or-nterm
2227/tcp  open     EthNetIP-1
3386/tcp  open     mysql
5432/tcp  open     postgresql
9898/tcp  filtered monkeycom

Nmap done: 1 IP address (1 host up) scanned in 40.32 seconds
(root@kali:~) [~]
```

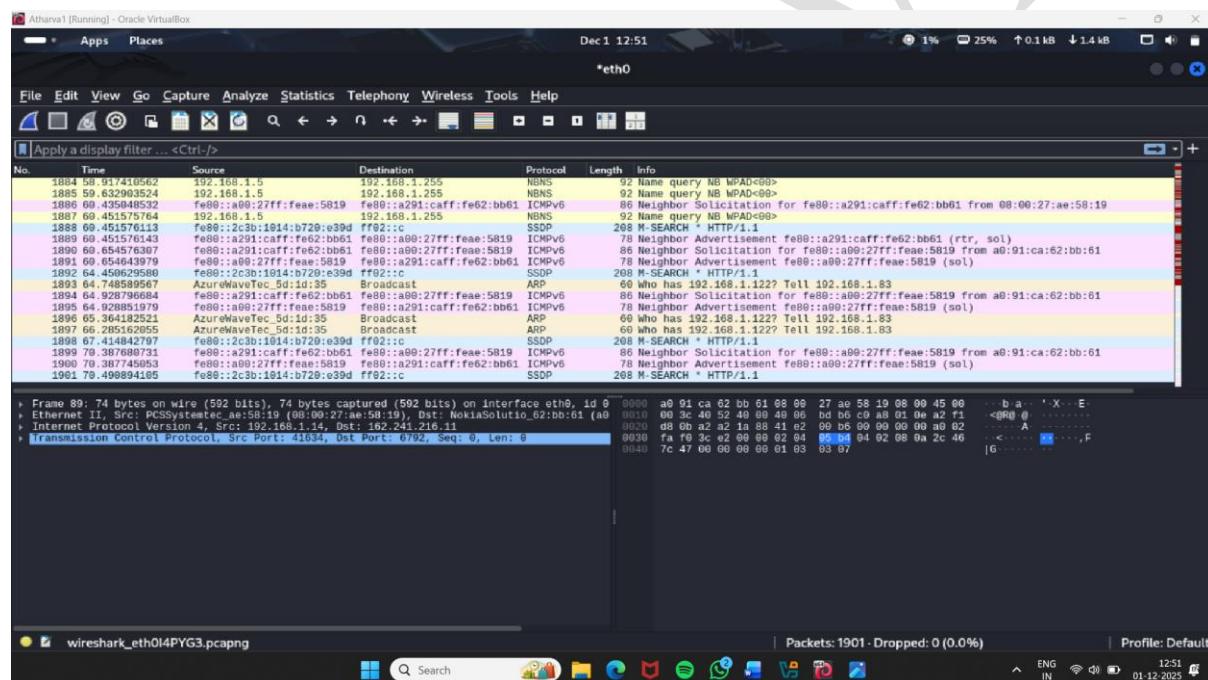
Fig(33)

## Step Performed:

Executed a full TCP Connect scan on target **162.241.216.11**, attempting to spoof MAC.

## Output:

- Multiple ports shown open:  
21,22,25,53,80,110,135,143,443,445,587,993,995,2082,2222,3306,..
- Some ports filtered: 1022,1023,1026,1433,9898...
- Spoofing a MAC address with the MAC address of a legitimate user on the network.



Fig(34)

**Note:** MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network. This technique allows you to send request packets to the targeted machine/network pretending to be a legitimate host.

## Additional Tools

### hping3

hping3 is a network tool that's able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies .

#### What is hping3?

hping3 is an advanced network packet crafting tool that allows you to generate and manipulate packets for various network protocols, including TCP, UDP, ICMP, and RAW-IP. It is primarily used for network security testing, firewall testing, advanced network diagnostics, and even penetration testing. Think of it as a more powerful version of the traditional ping command, but with much more control over the packets being sent.

#### Main Features of hping3:

- TCP/IP Packet Manipulation: You can craft and send custom TCP, UDP, ICMP, and RAW-IP packets.
- Port Scanning: hping3 can perform basic to advanced port scanning.
- Firewall Testing: Test firewall rules by crafting specific packets and analyzing the responses.
- Network Trace Routing: Similar to traceroute, you can track the path packets take across the network.
- Advanced Packet Crafting: You have control over packet headers, flags (SYN, ACK, FIN), TTL, window size, and more.
- Flooding and DoS Simulation: Simulate high packet loads to test the resilience of servers.
- Data Transfer Testing: Send raw data over different protocols to test throughput and reliability.
- OS Fingerprinting: Infer the operating system of a remote host by analyzing packet responses.

#### Basic Syntax of hping3: hping3 [options] [host]

#### Legal and Ethical Considerations:

- hping3 is a powerful tool often used in network testing and security auditing.
- Unauthorized usage on networks you do not own or have permission to test is illegal and violates cybersecurity laws.

## Test/Tool Shown:

1)hping3 in ICMP mode (-1) with random source addresses.

```
(root@kali)-[~]
# hping3 -1 --rand-source -p 80 162.241.216.11 --flood
PING 162.241.216.11 (eth0 162.241.216.11): icmp mode set, 28 headers + 0 data bytes
ping in flood mode, no replies will be shown
C
-- 162.241.216.11 hping statistic ---
616839 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(root@kali)-[~]
#
```

Fig(35)

## Step Performed:

Command used: hping3 -1 --rand-source -p 80 162.241.216.11 --flood

## Output:

- ICMP mode initialized.
- No replies shown (expected in flood mode).
- Summary: **4616839 packets transmitted, 0 received, 100% loss.**
- Sent a massive, high-speed volume of ICMP Echo Requests (-1) to the target (162.241.216.11) while masking the true source by using randomly spoofed IP addresses (--rand-source).

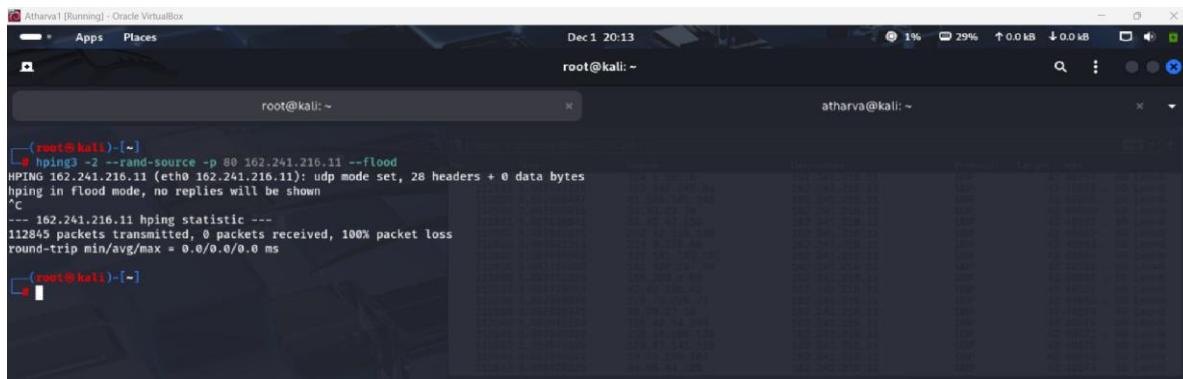
```
Athava1 [Running] - Oracle VM VirtualBox
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Dec 1 20:10 1% 27% ↑ 0.0 kB ↓ 0.0 kB
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter... <Ctrl-/>
No. Time Source Destination Protocol Length Info
81660 2.699264059 7.0.0.41.38 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=46342/50869, ttl=64 (no response found!)
81663 2.699264059 103.38.172.111 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=46799/50870, ttl=64 (no response found!)
81664 2.699264059 144.289.158.93 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=47046/50871, ttl=64 (no response found!)
81668 2.699318273 58.72.27.39 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=47392/50872, ttl=64 (no response found!)
81669 2.699344666 138.66.5.114 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=47558/50873, ttl=64 (no response found!)
81670 2.699344666 213.97.197.46 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=47814/50874, ttl=64 (no response found!)
81671 2.699344666 109.230.178.78 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=48070/50875, ttl=64 (no response found!)
81672 2.699434376 171.245.81.213 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=48326/50876, ttl=64 (no response found!)
81673 2.699434376 8.69.204.192 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=48582/50877, ttl=64 (no response found!)
81674 2.699434376 194.172.73.144 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=48838/50878, ttl=64 (no response found!)
81675 2.699434376 58.117.34.183 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=49094/50879, ttl=64 (no response found!)
81676 2.699545591 196.88.128.92 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=49250/50880, ttl=64 (no response found!)
81677 2.699571319 82.125.194.98 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=49606/50881, ttl=64 (no response found!)
81678 2.699601027 122.213.38.292 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=49862/50882, ttl=64 (no response found!)
81679 2.699628562 144.124.45.111 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=50118/50883, ttl=64 (no response found!)
81680 2.699628562 122.85.162.291 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=50374/50884, ttl=64 (no response found!)
81681 2.699682323 192.168.1.97 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=50530/50885, ttl=64 (no response found!)
81682 2.699789543 194.259.41.238 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=50886/50886, ttl=64 (no response found!)
81683 2.699789543 7.203.122.58 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=51142/50887, ttl=64 (no response found!)
81684 2.699789543 7.203.122.58 162.241.216.11 ICMP 42 Echo (ping) request id=0x912b, seq=51143/50887, ttl=64 (no response found!)

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0 0000 0a f8 cb 39 f2 d2 68 00 27 ae 58 19 08 09 45 00 ... X E
Ethernet II, Src: PCSSystemtec ae:58:19 (08:00:27:ae:58:19), Dst: 0a:f8:cb:39:f2:d2 (0a:f8:cb:39:f2:d2)
Internet Protocol Version 4, Src: 95.250.88.170, Dst: 162.241.216.11
Internet Control Message Protocol
```

Fig(36)

## Test/Tool Shown:

2)hping3 – UDP mode (-2).



```
root@kali:~
```

```
hping3 -2 --rand-source -p 80 162.241.216.11 --Flood
HPING 162.241.216.11 (eth0 162.241.216.11): udp mode set, 28 headers + 0 data bytes
hpings in Flood mode, no replies will be shown
^C
--- 162.241.216.11 hping statistic ---
112845 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

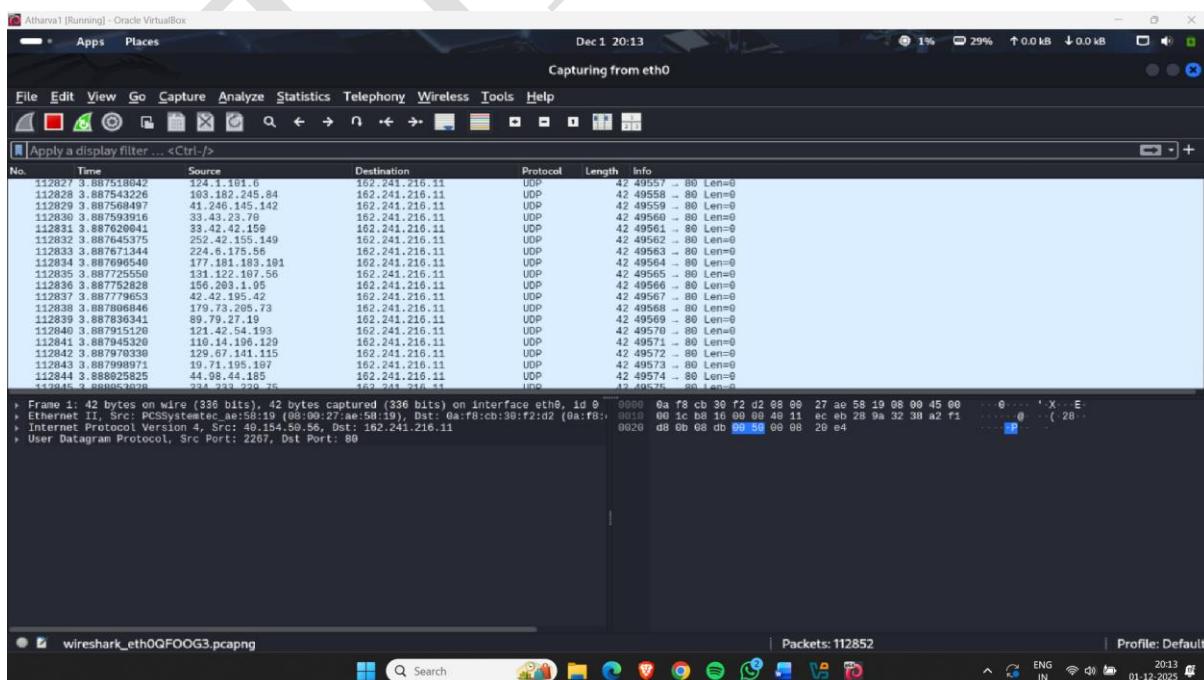
Fig(37)

## Step Performed:

Command used: hping3 -2 --rand-source -p 80 162.241.216.11 –flood

## Output:

- UDP mode activated.
- 112845 packets transmitted.
- The terminal confirms it's sending packets in "udp mode" and "pinging in flood mode."



Capturing from eth0

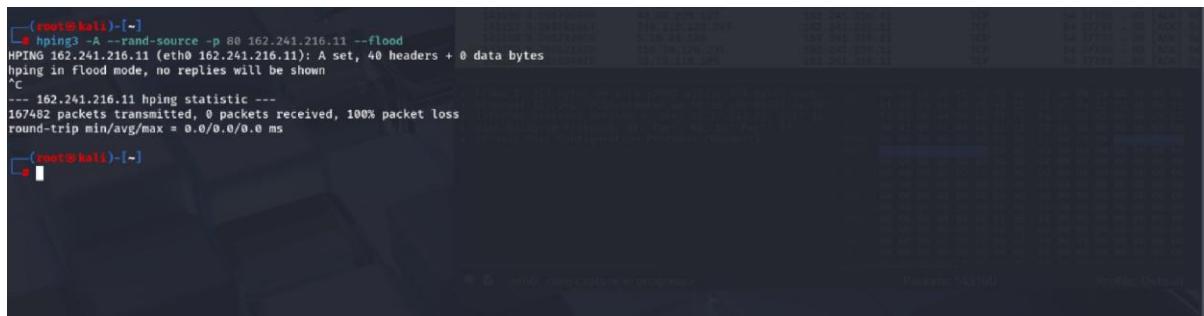
No.	Time	Source	Destination	Protocol	Length	Info
112827	3.887518642	124.1.181.6	162.241.216.11	UDP	42	49557 - 80 Len=0
112828	3.887543226	103.182.245.84	162.241.216.11	UDP	42	49558 - 80 Len=0
112829	3.887568494	41.246.145.142	162.241.216.11	UDP	42	49559 - 80 Len=0
112830	3.887601516	150.23.12.70	162.241.216.11	UDP	42	49560 - 80 Len=0
112831	3.887629841	33.42.42.158	162.241.216.11	UDP	42	49561 - 80 Len=0
112832	3.887645375	252.42.155.149	162.241.216.11	UDP	42	49562 - 80 Len=0
112833	3.887671344	224.6.175.56	162.241.216.11	UDP	42	49563 - 80 Len=0
112834	3.887690540	177.181.183.101	162.241.216.11	UDP	42	49564 - 80 Len=0
112835	3.887700556	156.203.1.95	162.241.216.11	UDP	42	49565 - 80 Len=0
112836	3.887752828	156.203.1.95	162.241.216.11	UDP	42	49566 - 80 Len=0
112837	3.887779653	42.42.195.42	162.241.216.11	UDP	42	49567 - 80 Len=0
112838	3.887806646	179.73.205.73	162.241.216.11	UDP	42	49568 - 80 Len=0
112839	3.887836341	89.79.27.19	162.241.216.11	UDP	42	49569 - 80 Len=0
112840	3.887860393	127.13.10.93	162.241.216.11	UDP	42	49570 - 80 Len=0
112841	3.887945320	110.14.106.129	162.241.216.11	UDP	42	49571 - 80 Len=0
112842	3.887970330	129.67.141.115	162.241.216.11	UDP	42	49572 - 80 Len=0
112843	3.887998971	19.71.195.107	162.241.216.11	UDP	42	49573 - 80 Len=0
112844	3.888025825	44.98.44.185	162.241.216.11	UDP	42	49574 - 80 Len=0
112845	3.888049059	107.711.517.1	162.241.216.11	UDP	42	49575 - 80 Len=0

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0x0000 0a:f8:cb:30:f2:d2 08:00 27:ae:58:19:08:00 45:00 ... 0:... 'X..E-  
Ethernet II, Src: PCSystem tec\_8e:58:19 (08:00:27:ae:58:19), Dst: 162.241.216.11 (0a:f8:cb:30:f2:d2)  
Internet Protocol Version 4, Src: 49.154.50.56, Dst: 162.241.216.11 (0a:f8:cb:30:f2:d2)  
User Datagram Protocol, Src Port: 2267, Dst Port: 80

Fig(38)

## Test/Tool Shown:

3)hping3 – TCP ACK mode (-A)



```
(root@kali:~]# hping3 -A --rand-source -p 80 162.241.216.11 --flood
HPING 162.241.216.11 (eth0 162.241.216.11): A set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 162.241.216.11 hping statistic ---
167482 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@kali:~]
```

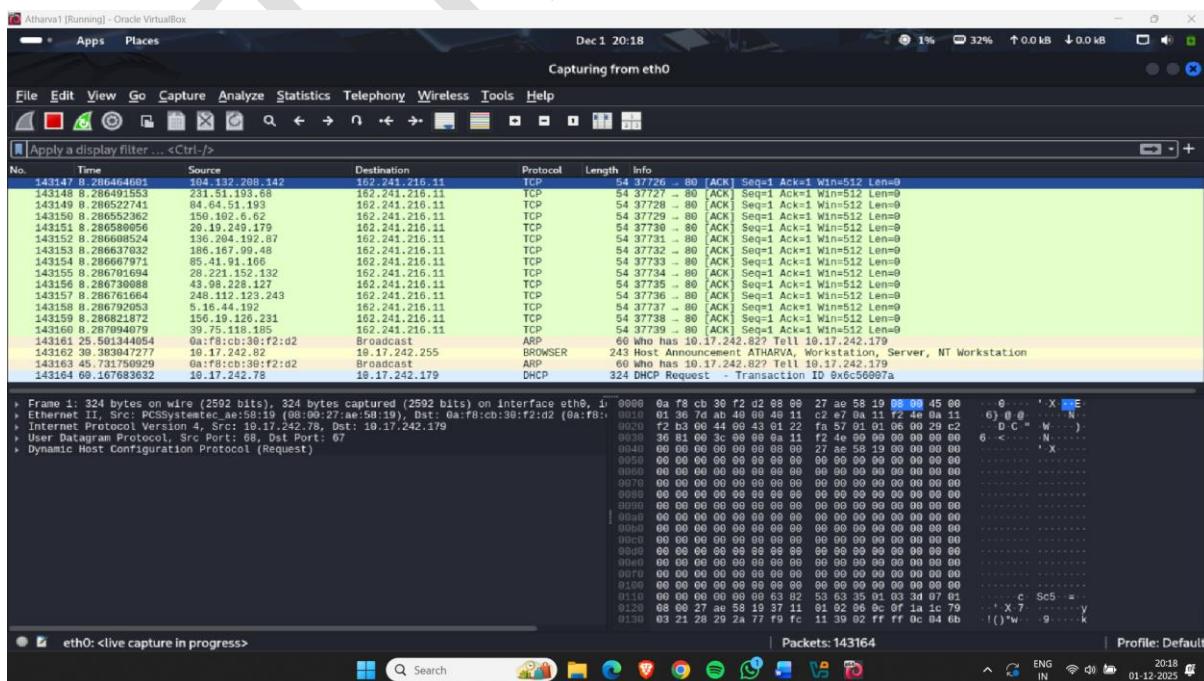
Fig(39)

## Step Performed:

Command used: hping3 -A --rand-source -p 80 162.241.216.11 --flood

## Output:

- TCP ACK packets sent.
- 167482 packets transmitted, 0 received
- Massive stream of TCP packets with the ACK flag set to the target on a specific port (like port 80).



Wireshark (Capturing from eth0)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display Filter... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
43147	8.286464601	104.132.208.142	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43148	8.286464602	231.132.192.68	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43149	8.286522741	84.64.51.193	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43150	8.286552362	150.192.6.62	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43151	8.286590056	20.19.249.179	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43152	8.286608524	136.204.192.87	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43153	8.286637932	186.167.98.48	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43154	8.286647165	84.51.102.105	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43155	8.286701694	28.221.152.132	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43156	8.286730088	43.98.228.127	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43157	8.286761664	248.112.123.243	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43158	8.286793595	5.16.44.192	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43159	8.2868118172	150.192.104.231	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43160	8.287894079	39.75.118.185	162.241.216.11	TCP	54	37726 - 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
43161	25.501344054	0:a:f0:cb:30:f2:d2	Broadcast	ARP	60	who has 10.17.242.82? Tell 10.17.242.179
43162	39.383847277	10.17.242.82	10.17.242.255	BROWSER	243	Host Announcement ATHARVA Workstation, Server, NT Workstation
43163	45.731750929	0:a:f0:cb:30:f2:d2	Broadcast	ARP	60	who has 10.17.242.82? Tell 10.17.242.179
43164	69.167683032	10.17.242.78	10.17.242.179	DHCP	324	DHCP Request - Transaction ID 0x9c56697a

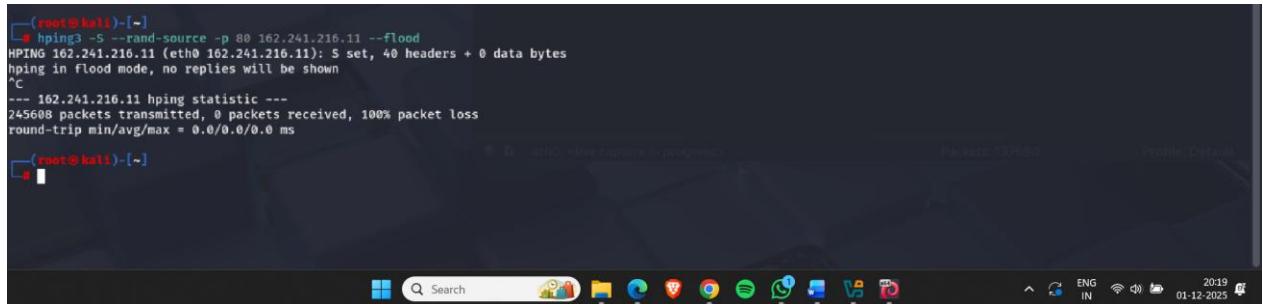
Frame 1: 324 bytes on wire (2592 bits), 324 bytes captured (2592 bits) on interface eth0, id 1
Ethernet II, Src: PCSystemtec ae:58:19 (00:00:27:ae:58:19), Dst: 0:a:f0:cb:30:f2:d2 (0:a:f0:cb:30:f2:d2)
Internet Protocol Version 4, Src: 10.17.242.78, Dst: 10.17.242.179
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)

Packets: 143164 | Profile: Default

Fig(40)

## Test/Tool Shown:

### 4)hping3 – TCP SYN mode (-S)



```
(root@kali:[~]
└─# hping3 -S --rand-source -p 80 162.241.216.11 --flood
HPING 162.241.216.11 (eth0 162.241.216.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 162.241.216.11 hping statistic ---
245608 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
└─#
```

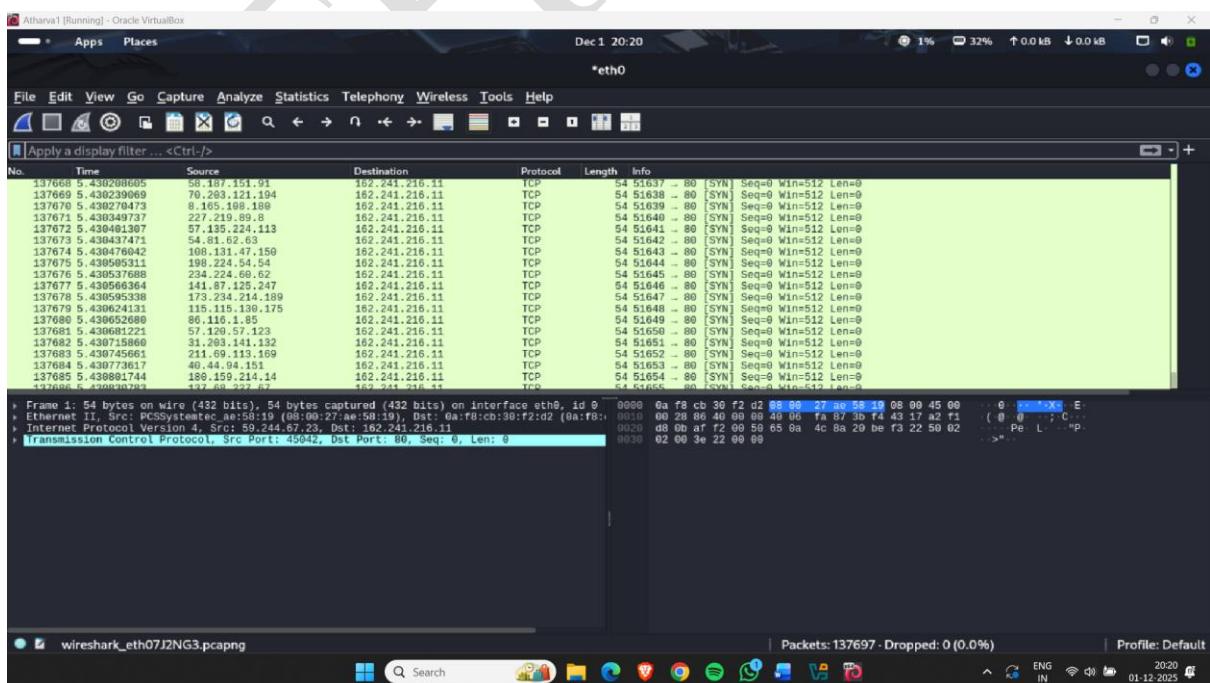
Fig(41)

## Step Performed:

Command used: hping3 -S --rand-source -p 80 162.241.216.11 –flood

## Output:

- SYN packets sent in flood mode.
- 245608 transmitted, 100% loss.
- [SYN] flag set, directed at port 80 on the target.



Fig(42)

## **Test/Tool Shown:**

5) hping3 – ICMP + spoofed source (-a)

```
[root@kali:~]# hping3 -1 -a 162.241.216.11 -S 162.241.216.11 -p 80 --flood
HPING 162.241.216.11 (eth0 162.241.216.11): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
*C
--- 162.241.216.11 hping statistic ---
165642 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

[root@kali:~]#
```

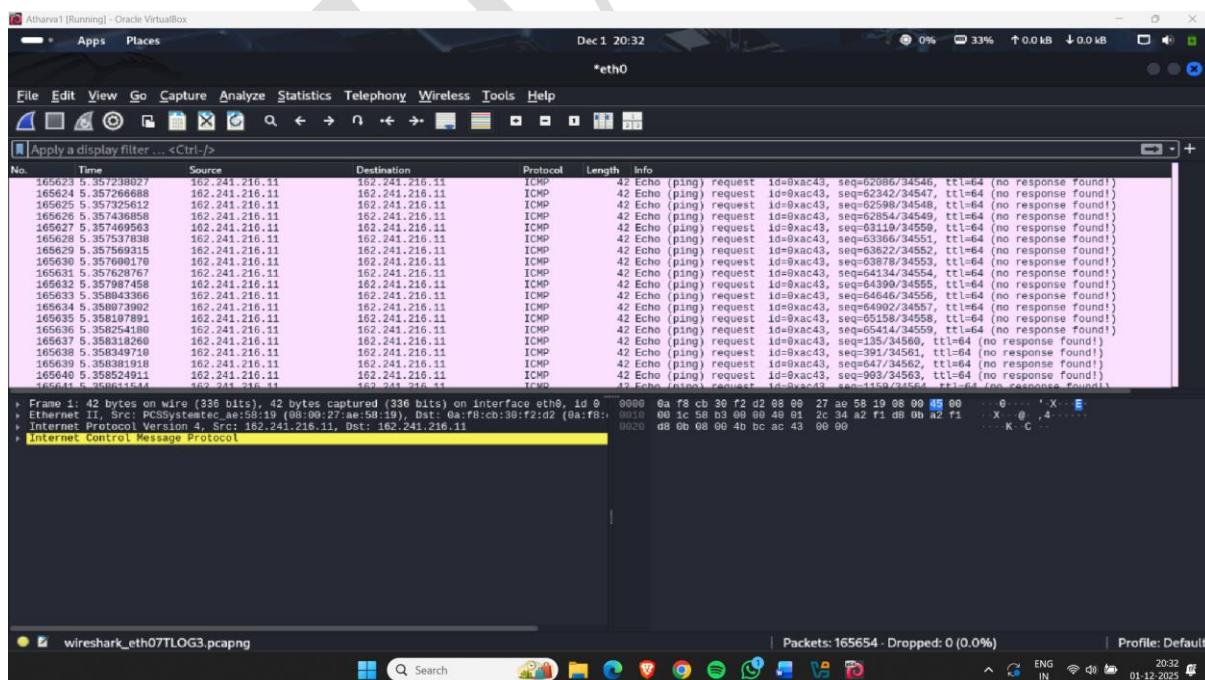
Fig(43)

### **Step Performed:**

Command used: hping3 -1 -a 162.241.216.11 -S 162.241.216.11 -p 80 -flood

## **Observed Output:**

- ICMP packets being sent.
  - 165642 packets transmitted.
  - -a 162.241.216.11 → Spoofed source IP
  - -S 162.241.216.11 → Target IP (packets sent to own machine)



Fig(43)

## **Metasploit:**

Metasploit is one of the most important and powerful tools in cybersecurity. It is used for penetration testing, exploit development, vulnerability assessment, and security research. Below is a clear, structured explanation that helps beginners and intermediate learners.

### **What is Metasploit?**

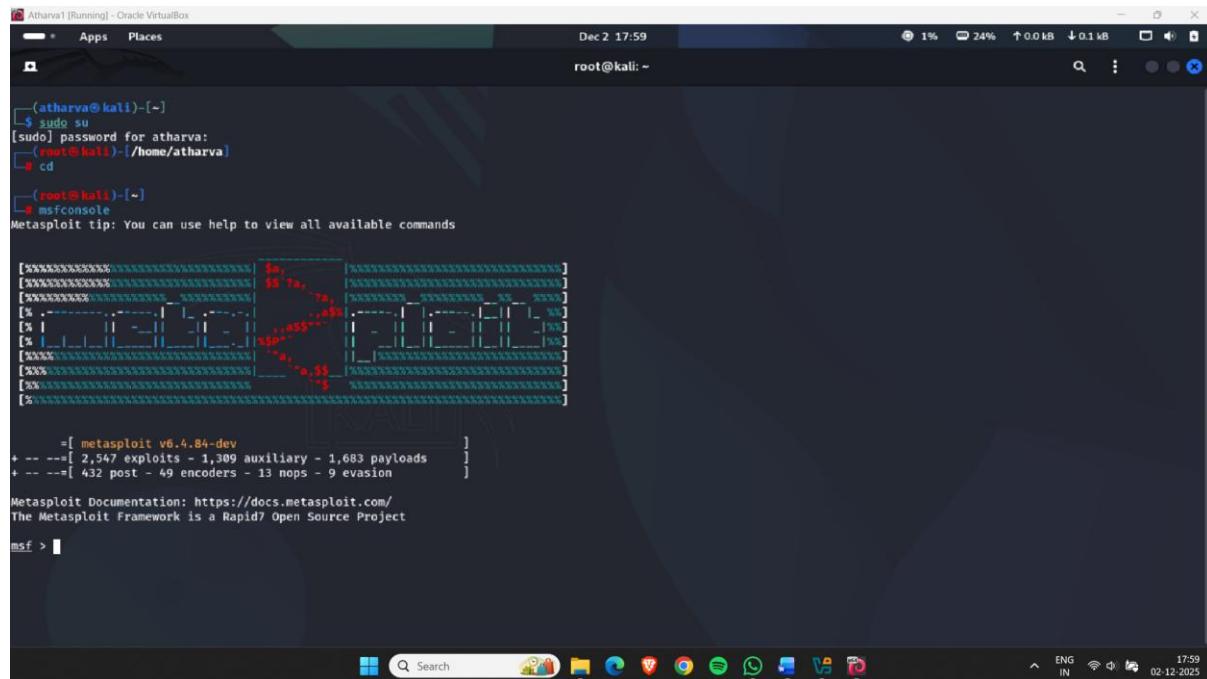
Metasploit is an open-source penetration testing framework used to:

- Find vulnerabilities
- Exploit vulnerabilities
- Test security defenses
- Create payloads
- Run post-exploitation modules
- Perform red-team assessments

### **Why Metasploit Is Important in Cybersecurity?**

- Automates exploitation
- Contains huge exploit and payload library
- Helps professionals learn real-world attack techniques
- Supports post-exploitation and pivoting
- Useful for practical cybersecurity training

## Step1: Execute command msfconsole to launch Metasploit.

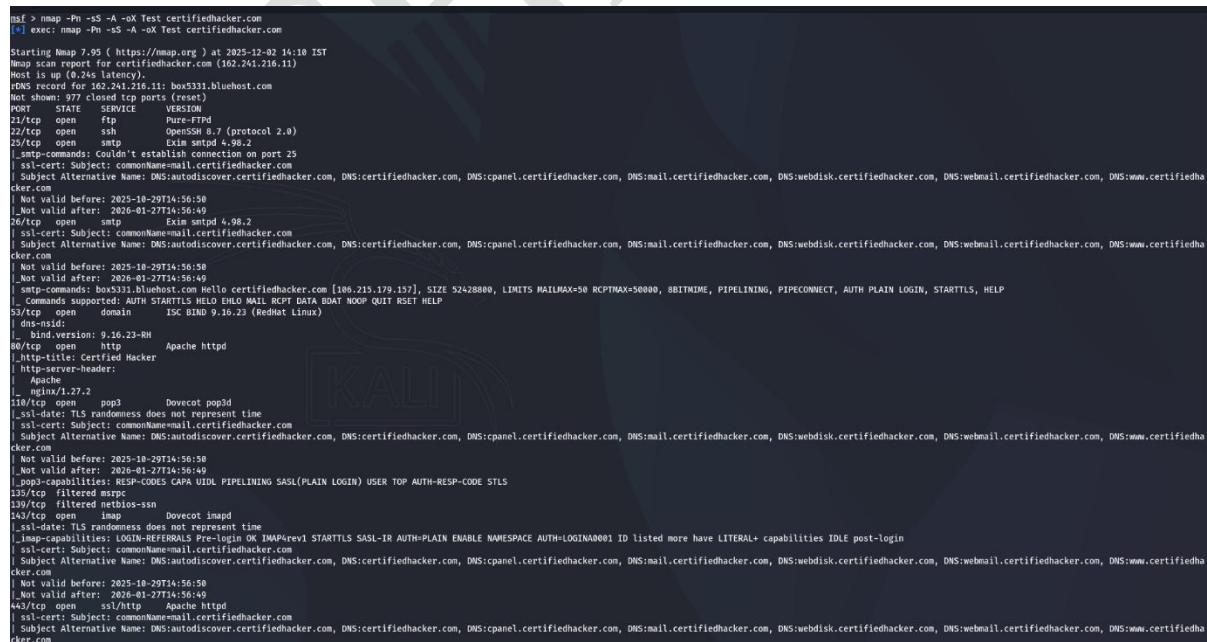


The screenshot shows a terminal window titled "Atharva1 [Running] - Oracle VirtualBox". The terminal is running as root on a Kali Linux system. The user has entered the command "msfconsole" to start the Metasploit framework. The Metasploit interface displays various exploit modules, auxiliary tools, and payloads available. The terminal also shows the Metasploit documentation URL and a note about the framework being a Rapid7 Open Source Project. The desktop environment includes a taskbar with icons for various applications like a browser, file manager, and terminal.

Fig(44)

Step2: An msf command line appears. Type nmap -Pn -sS -A -oX Test (target) and press Enter to scan .

After the scan completes, Nmap displays the host information in the target network along with open ports, service and OS enumeration.



The screenshot shows the terminal output of an Nmap scan. The user has run the command "nmap -Pn -sS -A -oX Test" against a target host. The output provides detailed information about the target's ports, services, and operating system. Key findings include port 80/tcp listening on Apache httpd, port 25/tcp listening on Exim smtpd, and port 443/tcp listening on OpenSSL. The output also lists various OS fingerprints and service details for the target host.

Fig(45)

```

[ Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
  _Not valid before: 2025-10-29T14:56:59
  _Not valid after: 2026-01-27T14:56:49
  _http-title: Certified Hacker
  _http-server-header:
  _App: Apache
  _nginx/1.27.2
  _ssl-date: TLS randomness does not represent time
443/tcp filtered microsoft-uds
465/tcp open   ssl      Exim smtpd 4.98.2
  _smtp-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP
  _Commands supported: AUTH HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
  _ssl-cert: Subject: commonName@mail.certifiedhacker.com
  _Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
  _Not valid before: 2025-10-29T14:56:59
  _Not valid after: 2026-01-27T14:56:49
587/tcp open   smtp    Exim smtpd 4.98.2
  _smtp-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
  _Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
  _ssl-cert: Subject: commonName@mail.certifiedhacker.com
  _Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
  _Not valid before: 2025-10-29T14:56:59
  _Not valid after: 2026-01-27T14:56:49
993/tcp open   ssl      Dovecot pop3d
  _ssl-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
  _Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
  _ssl-cert: Subject: commonName@mail.certifiedhacker.com
  _Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
  _Not valid before: 2025-10-29T14:56:59
  _Not valid after: 2026-01-27T14:56:49
1093/tcp open  imap   Dovecot imapd
  _ssl-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
  _imap-capabilities: LOGIN-REFERRALS Pre-Login OK IMAP4rev1 SASL-IR AUTH=PLAIN ENABLE NAMESPACE AUTH=LOGIN@0001 ID listed more IDLE LITERAL+ capabilities post-login have
  _ssl-date: TLS randomness does not represent time
995/tcp open   ssl      Dovecot pop3d
  _ssl-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
  _Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
  _ssl-cert: Subject: commonName@mail.certifiedhacker.com
  _Subject Alternative Name: DNS:autodiscover.certifiedhacker.com, DNS:cpanel.certifiedhacker.com, DNS:mail.certifiedhacker.com, DNS:webdisk.certifiedhacker.com, DNS:webmail.certifiedhacker.com, DNS:www.certifiedhacker.com
  _Not valid before: 2025-10-29T14:56:59
  _Not valid after: 2026-01-27T14:56:49
3308/tcp open  mysql  MySQL 5.7.44-48
  _ssl-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
  _ssl-date: TLS randomness does not represent time
  _ssl-cert: Subject: commonName+=bluehost.com
  _Subject Alternative Name: DNS+=bluehost.com, DNS:bluehost.com
  _Not valid before: 2025-01-27T00:00:00
  _Not valid after: 2026-01-27T23:59:59
  _mysql-info:
    Protocol: 10
    Version: 5.7.44-48
    Thread ID: 10137403

```

Fig(46)

```

[ _Not valid after: 2026-01-27T14:56:49
  _pop-capabilities: RESP-CODES SASL(PLAIN LOGIN) USER CAPA TOP AUTH-RESP-CODE UIDL PIPELINING
  _ssl-date: TLS randomness does not represent time
1022/tcp filtered exp2
1023/tcp filtered netvenuechat
1024/tcp filtered netvenueitem
2222/tcp open   ssh    OpenSSH 8.7 (protocol 2.0)
3308/tcp open  mysql  MySQL 5.7.44-48
  _ssl-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
  _ssl-date: TLS randomness does not represent time
  _ssl-cert: Subject: commonName+=bluehost.com
  _Subject Alternative Name: DNS+=bluehost.com, DNS:bluehost.com
  _Not valid before: 2025-01-27T00:00:00
  _Not valid after: 2026-01-27T23:59:59
  _mysql-info:
    Protocol: 10
    Version: 5.7.44-48
    Thread ID: 10137403
    Capabilities flags: 05535
    Some Capabilities: DontAllowDatabaseTableColumn, SupportsLoadDataLocal, Speaks4ProtocolOld, SupportsTransactions, InteractiveClient, SwitchToSSLAfterHandshake, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, ConnectWithDatabase, SupportsCompression, Supports4Auth, FoundRows, Speaks4ProtocolNew, LongColumnFlag, ODBCClient, LongPassword, SupportsAuthPlugins, SupportsMultipleStatements, SupportsMultipleResults
    SSL: 0
    SSL Commit: 0
    SSL DEJ: 0
    DTC:AN:90\x1f\x7f\x10
    _Auth Plugin Name: mysql_native_password
5432/tcp open  postgresql PostgreSQL 14.7 - 14.9
  _ssl-commands: box5331.bluehost.com Hello certifiedhacker.com [106.215.179.157], SIZE 52428800, LIMITS MAILMAX=50 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
  Aggressive OS guesses: D-Link DIR-825 WAP (9%), D-Link DIR-615, Encore 3G, or Engenius ESR-0752 WAP (89%), Linux 2.4.21 - 2.4.25 (embedded) (89%), OpenWrt Kamikaze 8.09 (Linux 2.6.25 - 2.6.26) (89%), Linux 2.6.18 (89%), Linux 2.6.19 - 2.6.32 (89%), Linux 2.6.32 (89%), Linux 2.6.38 (89%)
  No exact OS matches for host (test conditions non-ideal).
  Network Distance: 17 hops
  Service Info: OS: Linux; CPE: cpe:0:linux:linux_kernel
  TRACEROUTE (using port 554/tcp)
  HOP RTT           ADDRESS
  1  5.21 ms        Unit (192.168.1.1)
  2  52.67 ms       10.248.8.56
  ...
  4  60.28 ms       dsl-del-129.25.246.61.airtelbroadband.in (61.246.25.129)
  5  141.54 ms      116.119.61.232
  6  143.84 ms      mei-b5-link.ip.twelve99.net (62.115.42.118)
  7  172.42 ms      prs-b5-link.ip.twelve99.net (62.115.124.54)
  8  133.46 ms      ats-b5-link.ip.twelve99.net (62.115.130.103)
  9  323.05 ms      ats-bb1-link.ip.twelve99.net (62.115.138.71)
  10 325.54 ms      nash-bb1-link.ip.twelve99.net (62.115.137.55)
  11 325.89 ms      dls-bb1-link.ip.twelve99.net (62.115.137.45)
  12 340.39 ms      dls-b5-link.ip.twelve99.net (62.115.136.119)
  13 328.54 ms      dls-b5-link.ip.twelve99.net (62.115.139.150)
  14 334.54 ms      phx-b6-link.ip.twelve99.net (62.115.122.59)
  15 329.99 ms      213.248.67.33
  16 328.76 ms      140.91.195.7
  17 323.48 ms      box5331.bluehost.com (106.241.216.11)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done : IP address (1 host up) scanned in 116.10 seconds
nse > ]

```

Fig(46)

Step4: Type search portscan and press Enter. The Metasploit Metasploit port scanning modules appear, as shown in the screenshot

```

| Status: Autocommit
| Salt: ?7DeJ
| DFCAN-904x1xFx7Fx10
| Adapter Plugin Name: postgresql_native_password
5432/tcp open  postgresql PostgreSQL DB 14.7 - 14.9
9893/tcp filtered monkeycom
Aggressive OS guesses: D-link DIR-635 WAP (93%), Compaq C66640 cable modem (90%), D-Link DIR-615, Encore 36, or EnGenius ESR-0752 WAP (89%), Linux 2.4.21 - 2.4.25 (embedded) (89%), OpenWrt Kamikaze 8.09 (Linux 2.6.25 - 2.6.26) (89%), Linux 2.6.18 (89%), Linux 2.6.19 - 2.6.32 (89%), Linux 2.6.32 (89%), Linux 2.6.38 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT ADDRESS
1 2.21 ms Unit (192.168.1.1)
2 52.07 ms 10.246.0.56
3 ...
4 60.28 ms dsl-del-129.25.246.61.airtelbroadband.in (61.246.25.129)
5 147.94 ms 10.246.0.53
6 134.82 ms 10.246.0.53-1nm.ip.twelve99.net (62.115.42.118)
7 172.62 ms prs-bb1-link.ip.twelve99.net (62.115.124.24)
8 314.86 ms rest-bb1-link.ip.twelve99.net (62.115.148.105)
9 325.05 ms at1-bb1-link.ip.twelve99.net (62.115.138.71)
10 325.05 ms at1-bb1-link.ip.twelve99.net (62.115.137.159)
11 325.09 ms at1-bb1-link.ip.twelve99.net (62.115.137.152)
12 340.39 ms dls-b2-1-link.ip.twelve99.net (62.115.136.119)
13 328.32 ms dls-b7-link.ip.twelve99.net (62.115.139.130)
14 334.54 ms phx-b6-link.ip.twelve99.net (62.115.125.95)
15 329.99 ms 213.248.107.53
16 328.76 ms 148.91.195.7
17 323.48 ms box5331.bluehost.com (162.241.216.11)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.10 seconds
msf > search portscan
Matching Modules
=====
# Name           Disclosure Date Rank Check Description
----- 
0 auxiliary/scanner/portscan/ftpbounce          .      normal No   FTP Bounce Port Scanner
1 auxiliary/scanner/natpmp/natpmp_portscan       .      normal No   NAT-PMP External Port Scanner
2 auxiliary/scanner/sap/sap_router_portscanner    .      normal No   SAPRouter Port Scanner
3 auxiliary/scanner/portscan/naas                .      normal No   TCP ACK Firewall Scanner
4 auxiliary/scanner/portscan/nc                  .      normal No   TCP NC Port Scanner
5 auxiliary/scanner/portscan/tcp                 .      normal No   TCP Port Scanner
6 auxiliary/scanner/portscan/syn                .      normal No   TCP SYN Port Scanner
7 auxiliary/scanner/http/wordpress_pingback_access .      normal No   Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(scanner/portscan/tcp) > 

```

Fig(47)

Step5: Issue command: set RHOSTS 192.168.1.12

```

Dec 2 15:35
root@kali:~/home/pratik
5 auxiliary/scanner/portscan/tcp      .      normal No   TCP Port Scanner
6 auxiliary/scanner/portscan/syn     .      normal No   TCP SYN Port Scanner
7 auxiliary/scanner/http/wordpress_pingback_access .      normal No   Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf > use auxiliary/scanner/portscan/syn
msf auxiliary(scanner/portscan/syn) > show poisons
[-] Invalid parameter "poisons", use "show -h" for more information
msf auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):
Name  Current Setting Required Description
----- 
BATCHSIZE 256      yes   The number of hosts to scan per set
DELAY 0          yes   The delay between connections, per thread, in milliseconds
INTERFACE no        yes   The name of the interface
JITTER 0          yes   The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000    yes   Ports to scan (e.g. 22-25,80,116-980)
RHOSTS 192.168.1.12 yes   The target host(s). See https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN 65535    yes   The maximum number of bytes to capture
THREADS 1          yes   The number of concurrent threads (max one per host)
TIMEOUT 500        yes   The reply read timeout in milliseconds

View the full module info with the info, or info -d command.
msf auxiliary(scanner/portscan/syn) > set RHOSTS 192.168.1.12
RHOSTS => 192.168.1.12
msf auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):
Name  Current Setting Required Description
----- 
BATCHSIZE 256      yes   The number of hosts to scan per set
DELAY 0          yes   The delay between connections, per thread, in milliseconds
INTERFACE no        yes   The name of the interface
JITTER 0          yes   The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000    yes   Ports to scan (e.g. 22-25,80,116-980)
RHOSTS 192.168.1.12 yes   The target host(s). See https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN 65535    yes   The maximum number of bytes to capture
THREADS 1          yes   The number of concurrent threads (max one per host)
TIMEOUT 500        yes   The reply read timeout in milliseconds

```

Fig(48)

**Step6:**Issue the below commands:

- set INTERFACE eth0
  - set THREADS 50
  - show options

```

msf auxiliary(scanner/portscan/syn) > set RHOSTS 192.168.1.12
RHOSTS => 192.168.1.12
msf auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):
Name  Current Setting  Required  Description
----  -----  -----  -----
BATCHSIZE  256  yes  The number of hosts to scan per set
DELAY  0  yes  The delay between connections, per thread, in milliseconds
INTERFACE  eth0  no  The name of the interface
JITTER  0  yes  The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS  1-10000  yes  Ports to scan (e.g. 22-25,80,110-980)
RHOSTS  192.168.1.12  yes  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN  65535  yes  The number of bytes to capture
THREADS  1  yes  The number of concurrent threads (max one per host)
TIMEOUT  500  yes  The reply read timeout in milliseconds

View the full module info with the info, or info -d command.

msf auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):
Name  Current Setting  Required  Description
----  -----  -----  -----
BATCHSIZE  256  yes  The number of hosts to scan per set
DELAY  0  yes  The delay between connections, per thread, in milliseconds
INTERFACE  eth0  no  The name of the interface
JITTER  0  yes  The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS  1-10000  yes  Ports to scan (e.g. 22-25,80,110-980)
RHOSTS  192.168.1.12  yes  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN  65535  yes  The number of bytes to capture
THREADS  50  yes  The number of concurrent threads (max one per host)
TIMEOUT  500  yes  The reply read timeout in milliseconds

View the full module info with the info, or info -d command.

msf auxiliary(scanner/portscan/syn) > run
[*] /usr/share/metasploit-framework/lib/core/exploit/capture.rb:123: warning: undefining the allocator of T_DATA class PCAPRUB::Pcap
[*] TCP OPEN 192.168.1.12:22
[+] TCP OPEN 192.168.1.12:22
[*] TCP OPEN 192.168.1.12:23
[+] TCP OPEN 192.168.1.12:23
[*] TCP OPEN 192.168.1.12:53
[+] TCP OPEN 192.168.1.12:53
[*] TCP OPEN 192.168.1.12:80
[+] TCP OPEN 192.168.1.12:80
[*] TCP OPEN 192.168.1.12:139
[+] TCP OPEN 192.168.1.12:139
[*] TCP OPEN 192.168.1.12:512
[+] TCP OPEN 192.168.1.12:512
[*] TCP OPEN 192.168.1.12:513
[+] TCP OPEN 192.168.1.12:513
[*] TCP OPEN 192.168.1.12:514
[+] TCP OPEN 192.168.1.12:514

```

Fig(49)

Step7: Issue command : set RHOSTS 162.241.216.11

```
• Apps Places Dec 2 16:48
root@kali:~/home/pratik 26% 53% ↑0.00 kB 0.00 kB

[!] Unknown datastore option: INTERFACE.
INTERFACE => eth0
msf auxiliary(scanner/portscan/tcp) > back
msf > use 5
msf auxiliary(scanner/portscan/tcp) > set RHOSTS 162.241.216.11
msf auxiliary(scanner/portscan/tcp) >
msf auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

Name Current Setting Required Description
----- -----
CONCURRENCY 10 yes The number of concurrent ports to check per host
DELAY 0 yes The delay between connections, per thread, in milliseconds
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan, separated by commas
RHOSTS 162.241.216.11 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 1000 yes The socket connect timeout in milliseconds

View the full module info with the info, or info -d command.

msf auxiliary(scanner/portscan/tcp) > run
[*] 162.241.216.11 - 162.241.216.11:22 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:23 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:25 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:26 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:37 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:80 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:10 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:143 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:199 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:445 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:587 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:993 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2000 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2077 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2078 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2082 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2083 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2086 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2087 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2095 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2096 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2222 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:3306 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:5432 - TCP OPEN
[*] 162.241.216.11 - Scanned 1 of 1 hosts (100% complete)

msf auxiliary(scanner/portscan/tcp) > Intropurt: use the 'exit' command to quit
msf auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/portscan/tcp
msf auxiliary(scanner/portscan/tcp) > 
```

Fig(50)