

# **Module 3**

# **Network Scanning**

**25.11.25**

**Name : Mugdha Makarand Govilkar**

**Instructor : Satish Singh**

## INDEX:

1. perform host discovery using nmap:
2. explore zenmap using nmap:
3. perform stealth scan/TCP half open scan :
4. perform Xmas scan :
5. TCP Maimon scan :
6. perform ACK flag probe :
7. perform UDP scan :
8. perform Null Scan :
9. perform service version scan:
10. perform aggressive scan :
11. Perform OS discovery :
12. perform script:
13. Evasion of firewall :
14. scan a target network using Metasploit :

# **Concepts :**

## **I. Scanning :**

- Scanning is a set of procedures for identifying live hosts, ports, services, discovering operating system and architecture of target system, identifying vulnerabilities and threats in the network.
- Networking scanning is used to identify active devices on a network by employing features in the network protocol.

## **II. TCP :**

- TCP stands for transmission control protocol.
- It is a connection oriented protocol means the connection established between both the ends of the transmission.
- For creating connection TCP generates a virtual circuit between sender and receiver for the duration of transmission.
- Stream and dat transfer, multi routing, logical connection, full duplex.

## **III. UDP :**

- UDP stands for user datagram protocol
- UDP is a connectionless protocol.
- UDP is a simple protocol and it provides non-sequenced transport functionality.
- This type of protocol is used when reliability and security are less important than speed and size
- Multicast and broadcast. fast delivery of message, small transition such as DNS lookup.

# 1. perform host discovery using nmap:

Host discovery using Nmap means finding which devices (hosts) are active/alive on a network without doing a full port scan. It is the first step in network scanning & penetration testing.

1. -sn : disables port scan

2. -PR : The ARP ping scan probes ARP request to target host an ARP response means that the host is active

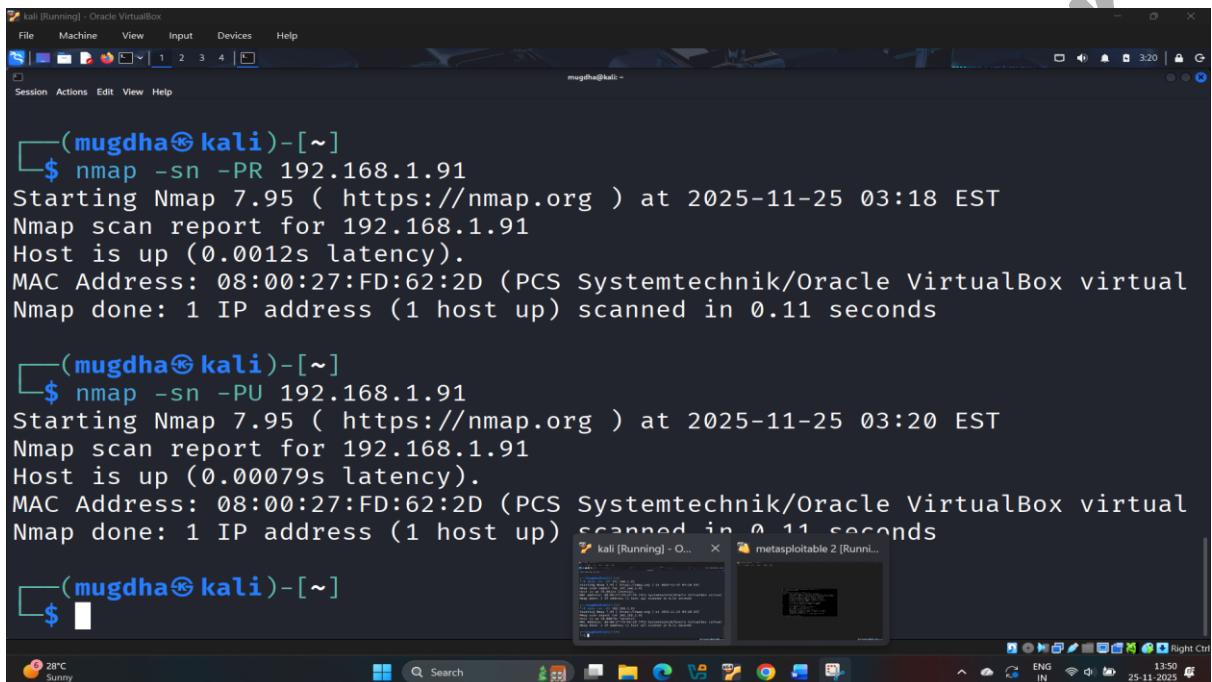
```
mugdha@kali:~$ nmap -sn -PR 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:18 EST
Nmap scan report for 192.168.1.91
Host is up (0.0012s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

(mugdha@kali):~$
```

1.2.1

**3. -PU : the UDP ping scan sends UDP packets to the target host a UDP response means that the host is active and if the target host is offline or unreachable various error messages such as host/network unreachable or TTL exceeded could be returned**



```
(mugdha㉿kali)-[~]
$ nmap -sn -PR 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:18 EST
Nmap scan report for 192.168.1.91
Host is up (0.0012s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

(mugdha㉿kali)-[~]
$ nmap -sn -PU 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:20 EST
Nmap scan report for 192.168.1.91
Host is up (0.00079s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

### 1.3.1

**4. -PE : The ICMP echo ping scan involves sending ICMP echo requests to a host if the target host is alive it will return an ICMP echo reply this scan is useful for locating active devices or determining if the ICMP is passing through a firewall**

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
mugdha@kali: ~
Nmap scan report for 192.168.1.91
Host is up (0.00079s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

└──(mugdha㉿kali)-[~]
$ nmap -sn -PU 192.168.1.91

└──(mugdha㉿kali)-[~]
$ nmap -sn -PE 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:21 EST
Nmap scan report for 192.168.1.91
Host is up (0.0015s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds

└──(mugdha㉿kali)-[~]
$ 

```

#### 1.4.1

**5. -PE : ICMP echo ping sweep to discover live hosts from a range of target IP addresses by sending ICMP echo requests to multiple hosts if a host is alive it will return an ICMP echo reply .Here we are setting the range of 100**

```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali: /home/mugdha
Nmap scan report for 192.168.1.91
Host is up (0.00080s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.96
Host is up (0.12s latency).
MAC Address: 94:BB:43:33:0B:6F (AzureWave Technology)
Nmap scan report for 192.168.1.26
Host is up.
Nmap done: 256 IP addresses (50 hosts up) scanned in 10.09 seconds

└──(root㉿kali)-[/home/mugdha]
# nmap -sn -PE 192.168.1.91-100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:30 EST
Nmap scan report for 192.168.1.91
Host is up (0.00080s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.96
Host is up (0.093s latency).
MAC Address: 94:BB:43:33:0B:6F (AzureWave Technology)
Nmap done: 10 IP addresses (2 hosts up) scanned in 10.09 seconds

└──(root㉿kali)-[/home/mugdha]
# 

```

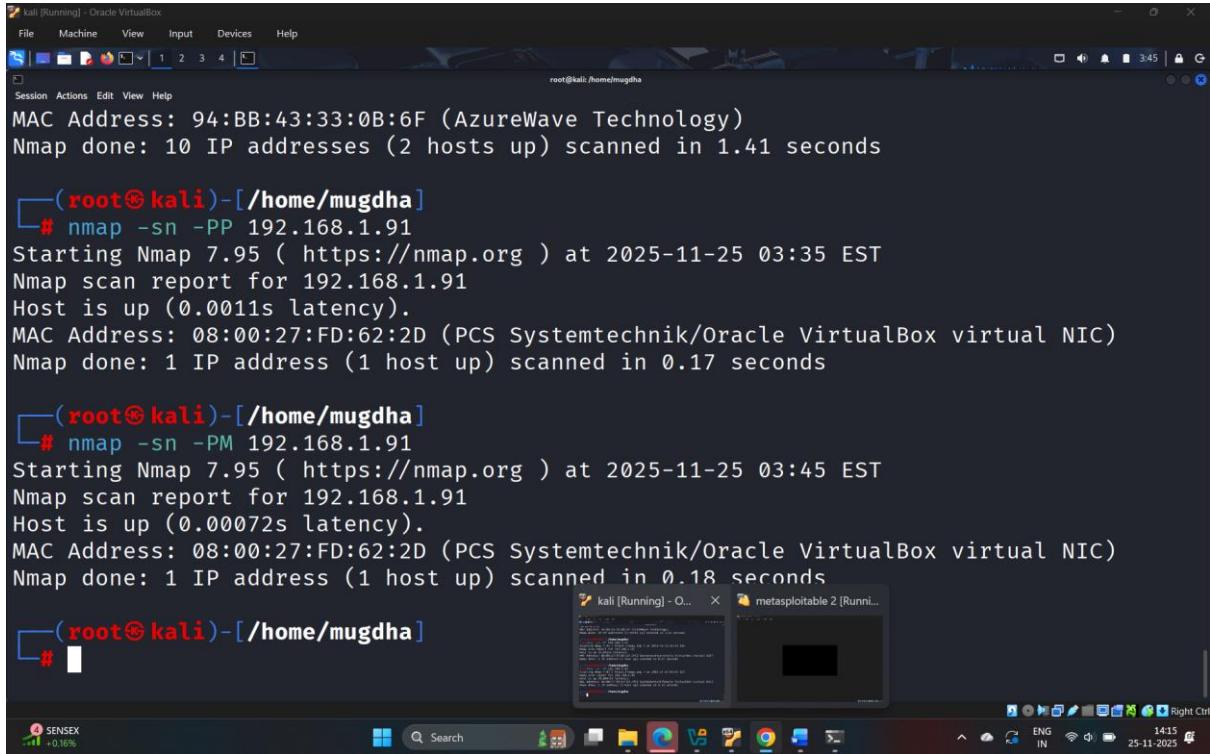
**6. -PP : ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine**

```
(root㉿kali)-[~/home/mugdha]
└─# nmap -sn -PE 192.168.1.91-100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:30 EST
Nmap scan report for 192.168.1.91
Host is up (0.00080s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.96
Host is up (0.093s latency).
MAC Address: 94:BB:43:33:0B:6F (AzureWave Technology)
Nmap done: 10 IP addresses (2 hosts up) scanned in 1.41 seconds

(roots㉿kali)-[~/home/mugdha]
└─# nmap -sn -PP 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:35 EST
Nmap scan report for 192.168.1.91
Host is up (0.0011s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

(roots㉿kali)-[~/home/mugdha]
└─#
```

**7. -PM : this technique is an alternative for the traditional ICMP echo ping scan which are used to determine whether the target host is alive specifically when administrators block the ICMP echo pings**

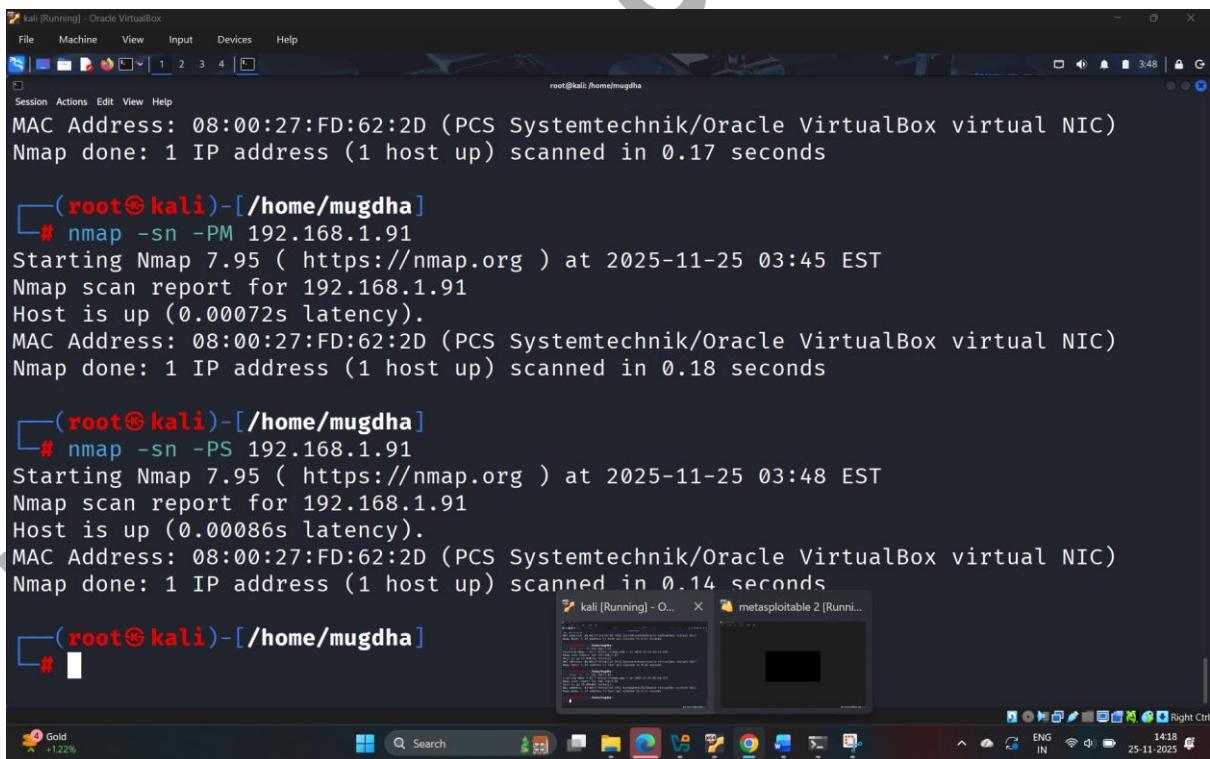


```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~# nmap -sn 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:35 EST
Nmap scan report for 192.168.1.91
Host is up (0.0011s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

(root@kali)-[~/home/mugdha]
# nmap -sn 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:45 EST
Nmap scan report for 192.168.1.91
Host is up (0.00072s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

(root@kali)-[~/home/mugdha]
#
```

## 8. -PS : TCP SYN ping scan is the technique that sends empty TCP SYN packets to the target hosts ACK response means that the host is active

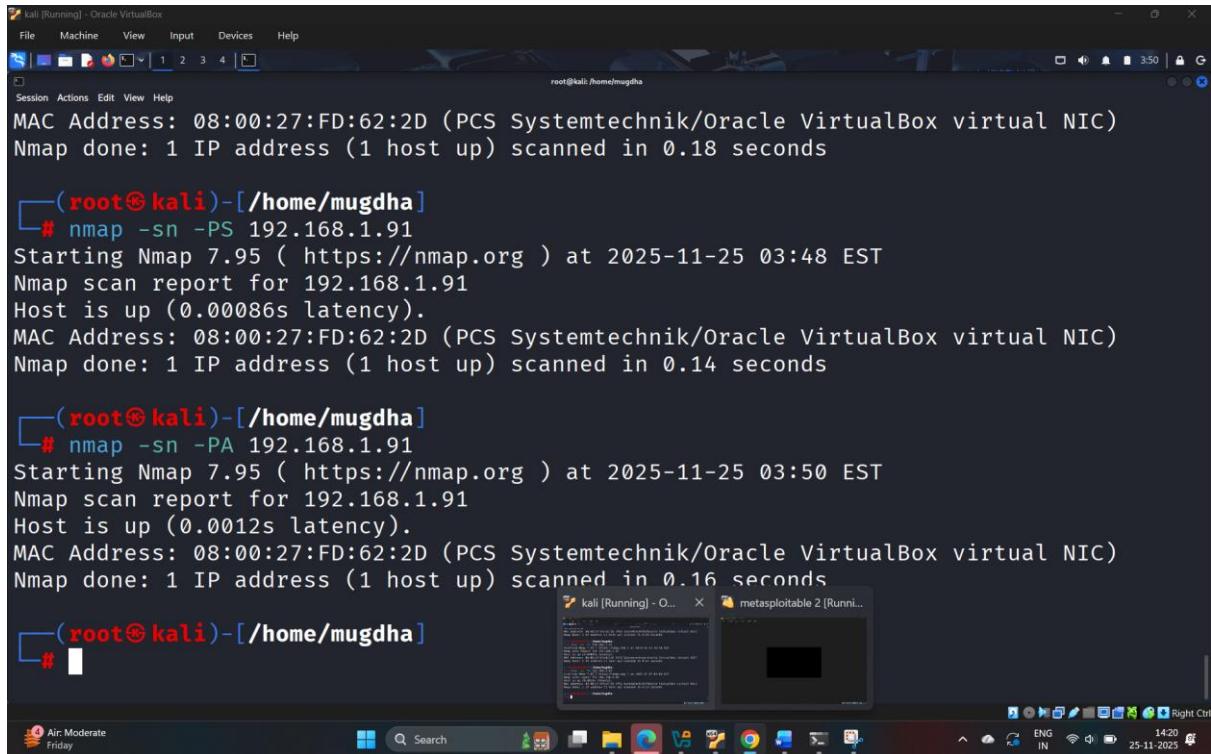


```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
root@kali:~# nmap -sn 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:45 EST
Nmap scan report for 192.168.1.91
Host is up (0.00072s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

(root@kali)-[~/home/mugdha]
# nmap -sn 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:48 EST
Nmap scan report for 192.168.1.91
Host is up (0.00086s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(root@kali)-[~/home/mugdha]
#
```

## 9. -PA : TCP ACK ping scan is the technique that sends empty TCP ACK packets to the target host. An ACK response means that the host is active



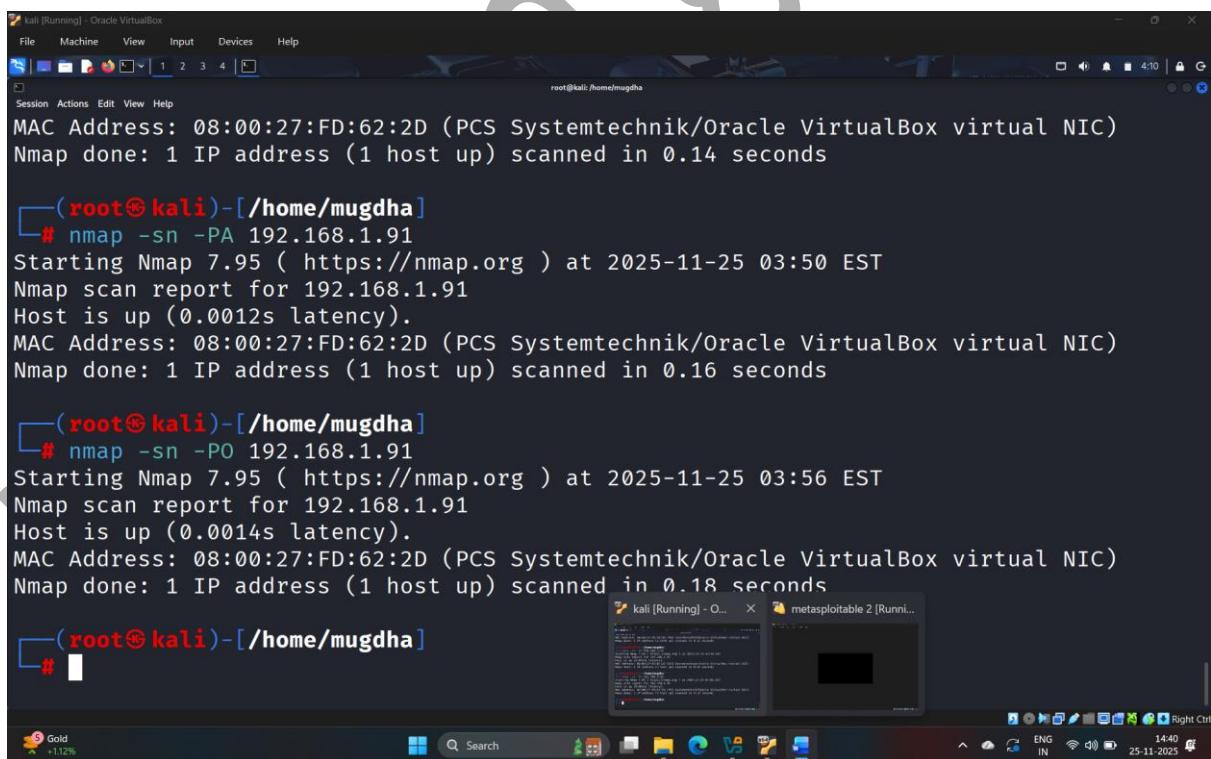
```
root@kali:[/home/mugdha]
# nmap -sn 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:48 EST
Nmap scan report for 192.168.1.91
Host is up (0.00086s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

root@kali:[/home/mugdha]
# nmap -sn -PA 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:50 EST
Nmap scan report for 192.168.1.91
Host is up (0.0012s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

root@kali:[/home/mugdha]
#
```

1.9.1

## 10. -PO : IP protocol ping scan is the technique that sends different probe packets of different IP protocols to the target host any response from any pobe indicates that a host is active



```
root@kali:[/home/mugdha]
# nmap -sn 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:50 EST
Nmap scan report for 192.168.1.91
Host is up (0.0012s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

root@kali:[/home/mugdha]
# nmap -sn -PA 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:56 EST
Nmap scan report for 192.168.1.91
Host is up (0.0014s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

root@kali:[/home/mugdha]
# nmap -sn -PO 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 03:56 EST
Nmap scan report for 192.168.1.91
Host is up (0.0014s latency).
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

root@kali:[/home/mugdha]
#
```

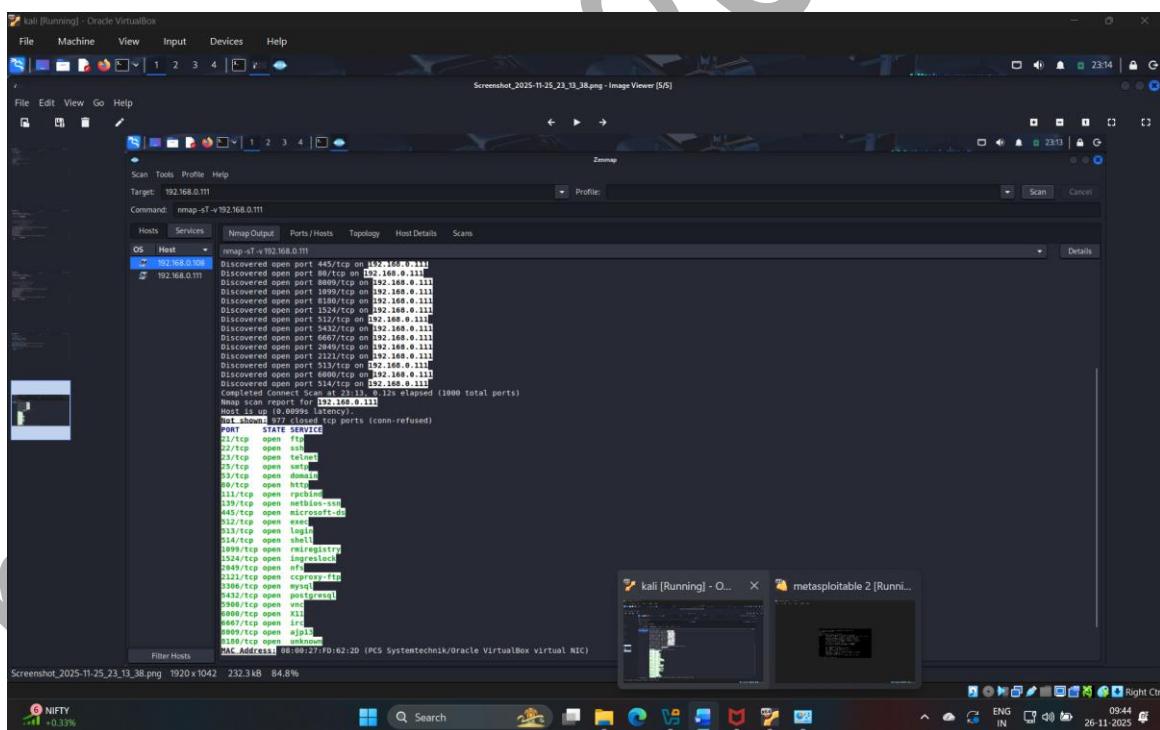
1.10.1

## 2.explore zenmap using nmap:

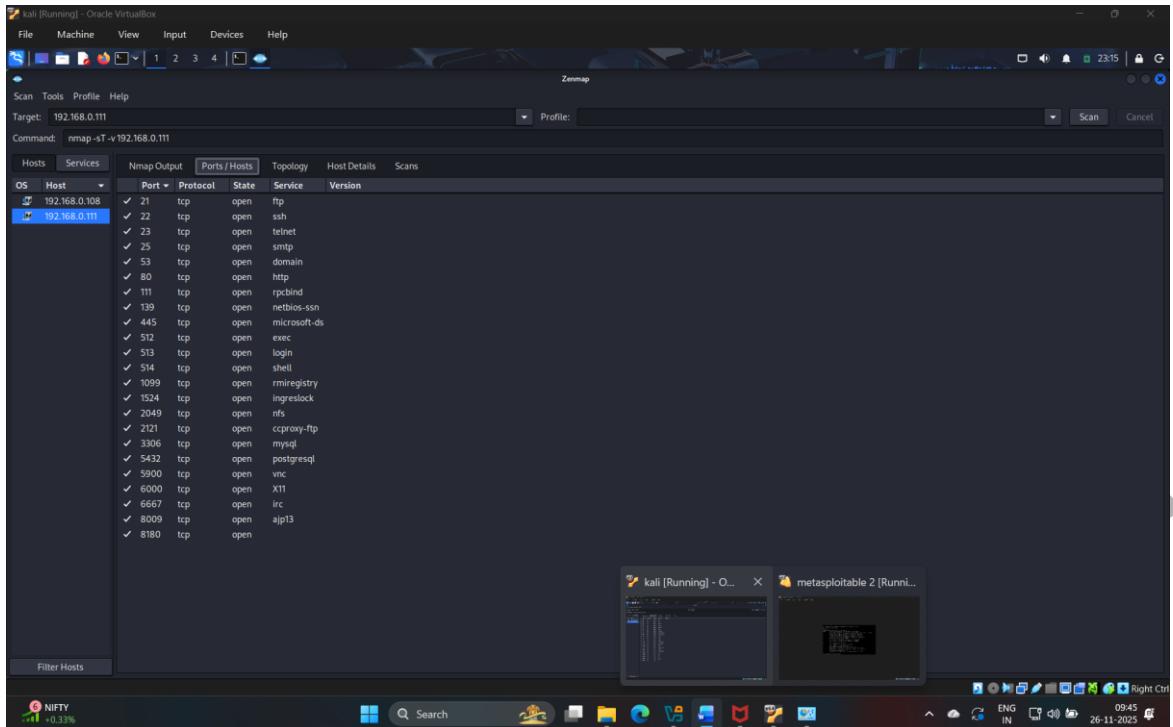
**Zenmap is the official GUI (Graphical User Interface) for Nmap. It makes network scanning easier for beginners and faster for professionals. Instead of typing commands in terminal, Zenmap allows you to run scans with buttons and menus. Zenmap includes ready-made scan templates like:**

- Intense Scan
- Quick Scan
- Ping Scan
- OS Detection Scan
- Aggressive Scan

1. **-sT : performs tcp connection/full open scan**
2. **-v : enables verbose output. In cybersecurity and Linux tools, verbose mode is used to display extra information, such as progress, errors, internal processes, and debugging details. Nmap displays :port, protocol, state, service, version, scan**

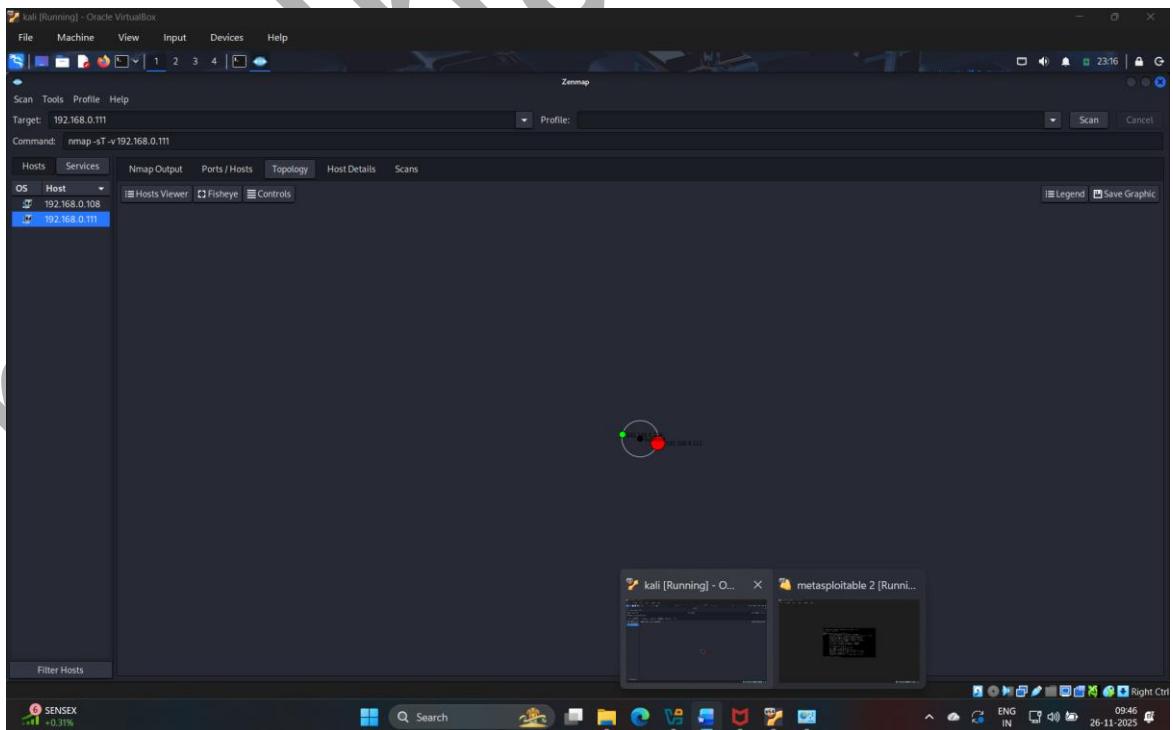


**2.1**



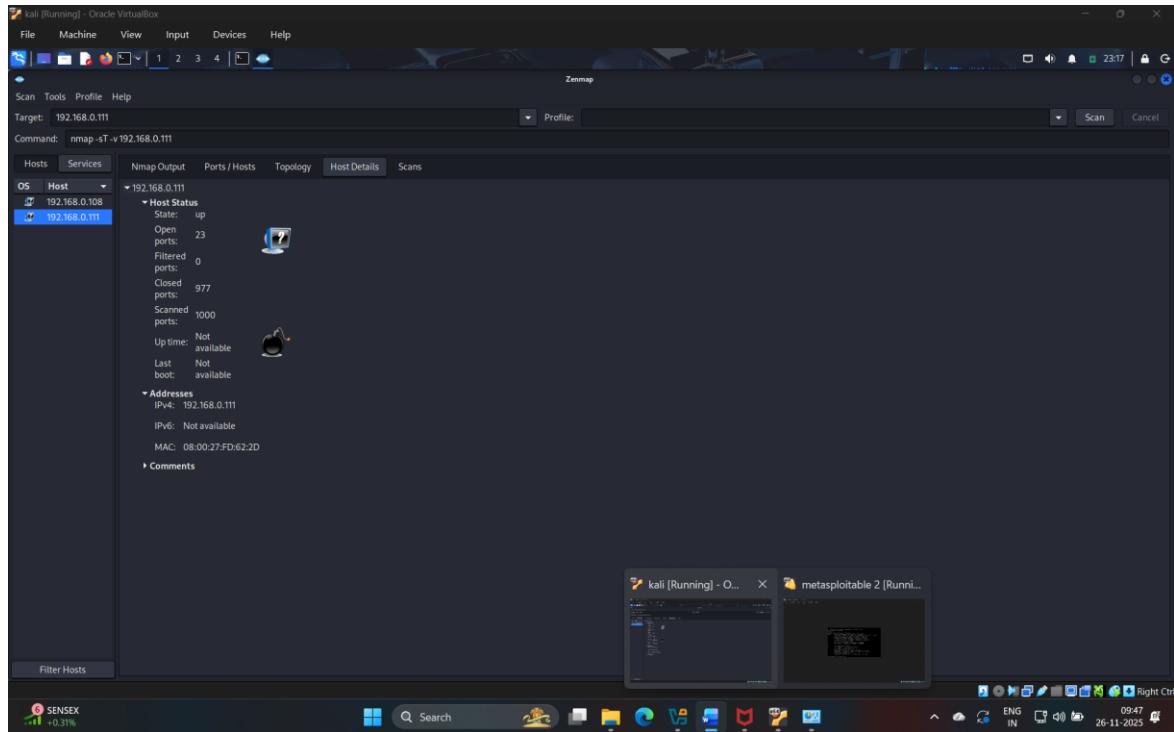
## 2.2

3. Click on the topology that shows provided ip :



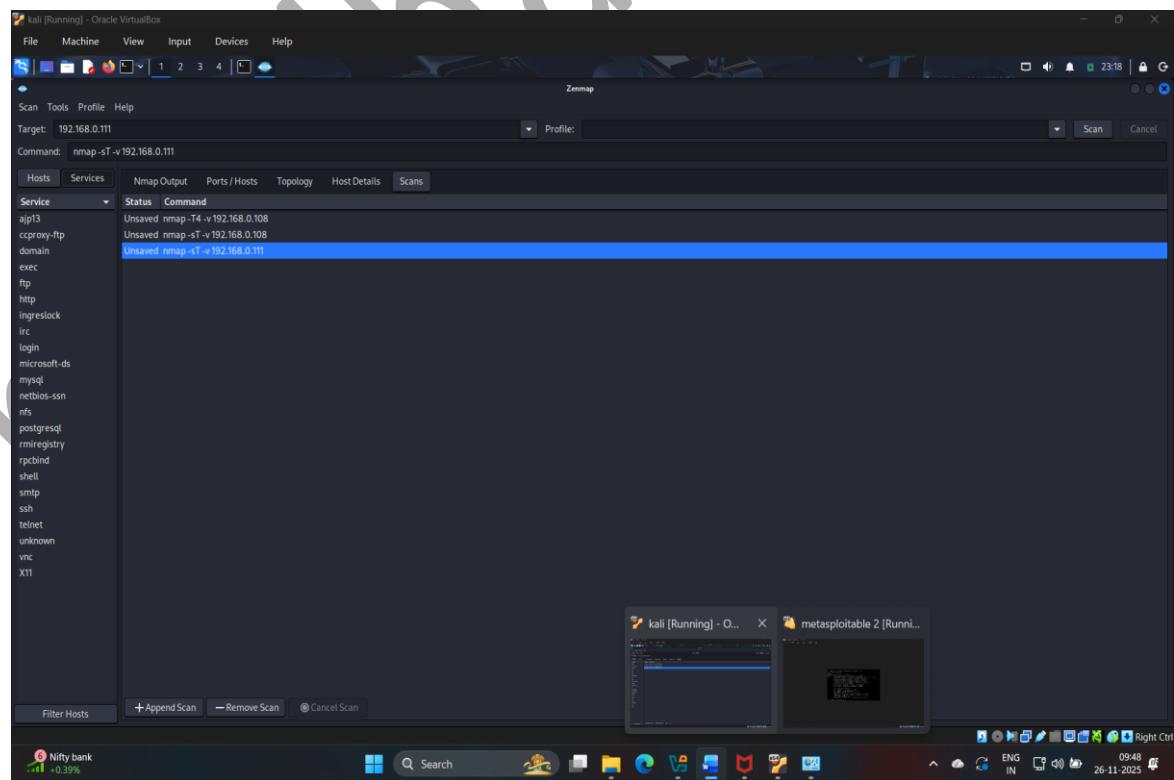
## 2.3

**4. Click on host details to view the details of tcp connection scan :**



2.4

**5. Then click on the services running you can use any of these services and their open ports to enter into target network/host and establish a connection :**

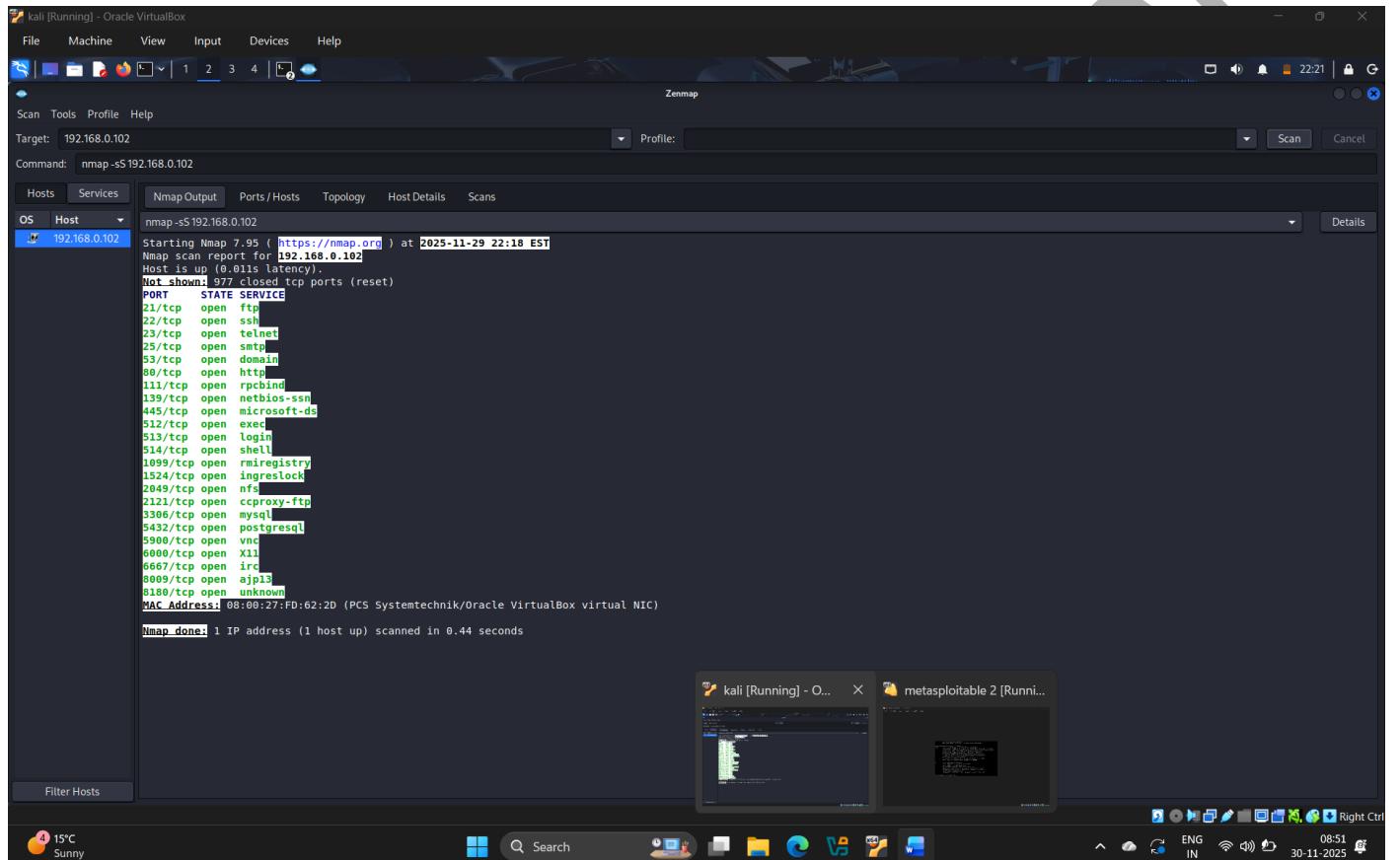


2.5

### 3.perform stealth scan/TCP half open scan :

- -sS : 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 mechanism, and hide under network traffic



```
nmap -sS 192.168.0.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 22:18 EST
Host scan report for 192.168.0.102
Host is up (0.011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

3.1

## 4.perform Xmas scan :

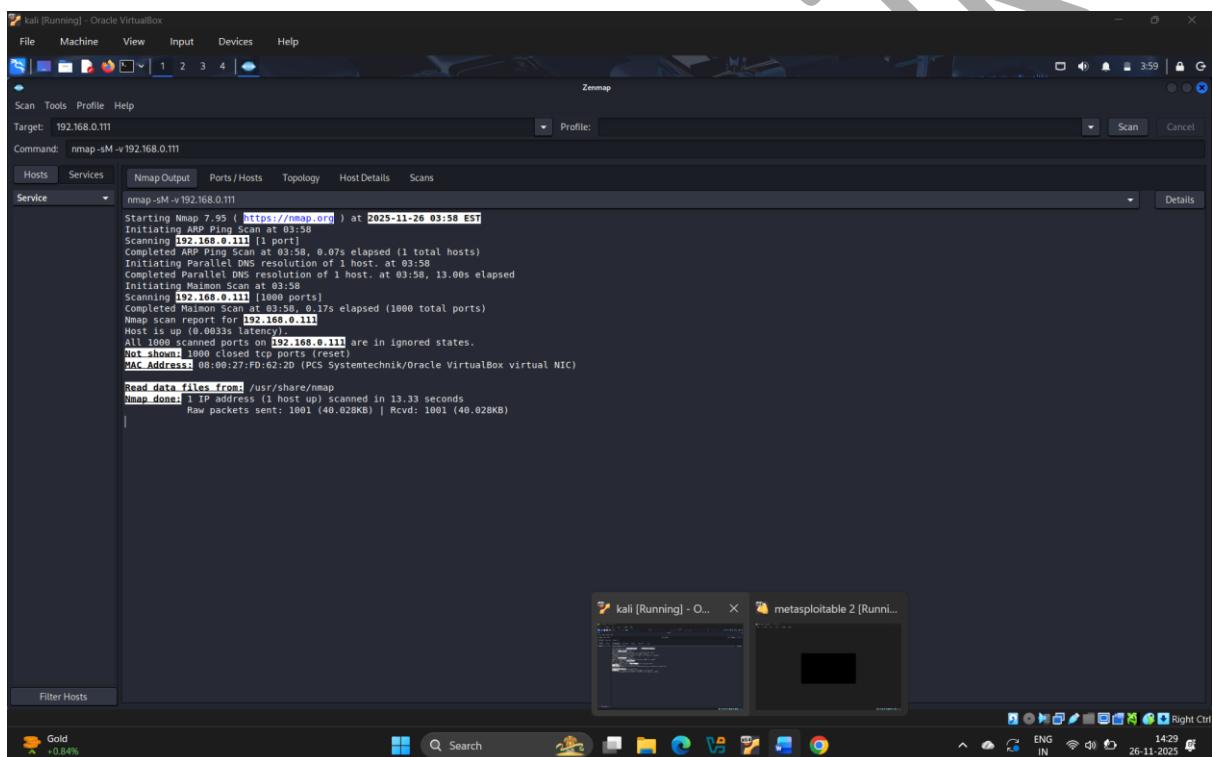
- sX : xmas scan sends a TCP frame to a target system with FIN<URG and PUSH flags set. If the target has opened the port then you will receive no response from the target system .If the target has closed the port then you will receive a target system reply with an RST. The scan result appear displaying that the ports are either open or filtered on the target machine which means a firewall has been configured on the target machine. Here we got RST flag for 977 port out of 1000 poers which means these 977 ports are closed and remaining 23 ports are filtered which means there is firewall on the target machine

Service	Port	State	Service
ajp13	21/tcp	open filtered	ftp
ccproxy-ftp	22/tcp	open filtered	ssh
domain	23/tcp	open filtered	telnet
exec	25/tcp	open filtered	smtp
ftp	53/tcp	open filtered	domain
http	80/tcp	open filtered	http
ingreslock	111/tcp	open filtered	rpcbind
irc	139/tcp	open filtered	netbios-ssn
login	445/tcp	open filtered	microsoft-ds
microsoft-ds	512/tcp	open filtered	exec
mysql	513/tcp	open filtered	login
netbios-ssn	514/tcp	open filtered	shell
nfs	1099/tcp	open filtered	rmiregistry
postgresql	135/tcp	open filtered	ingreslock
rmiregistry	2049/tcp	open filtered	nfs
rpcbind	2121/tcp	open filtered	ccproxy-ftp
shell	3306/tcp	open filtered	mysql
smtp	5432/tcp	open filtered	postgresql
ssh	5500/tcp	open filtered	pgsql
telnet	6000/tcp	open filtered	X11
unknown	6667/tcp	open filtered	irc
vnc	8009/tcp	open filtered	ajp13
X11	8180/tcp	open filtered	unknown

4.1

## 5.TCP Maimon scan :

- sM : In the TCP mainon 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 it displays either the ports are open/filtered on the target machine which means a firewall has been configured on the target machine. In this result we get RST flag which means all ports are closed



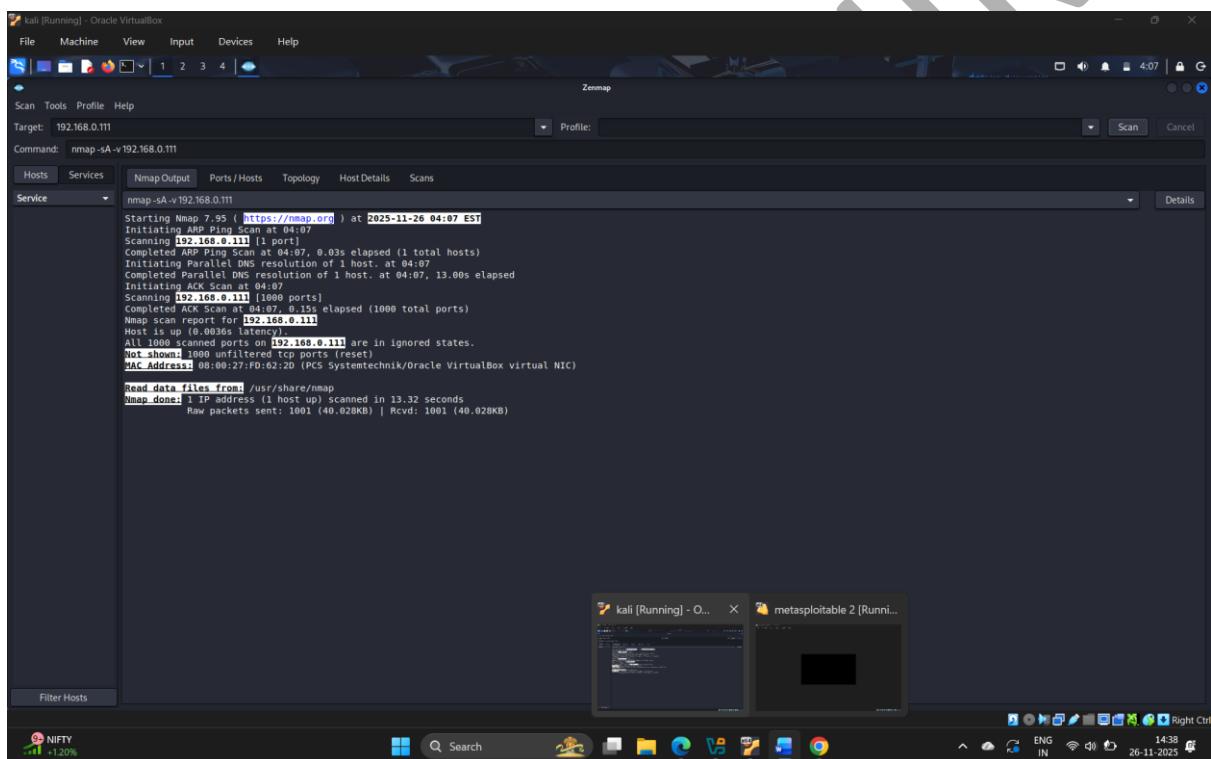
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 03:58 EST
Initiating Ping Scan at 03:58
Scanning 192.168.0.111 [1 port]
Completed ARP Ping Scan at 03:58, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 03:58
Completed Parallel DNS resolution of 1 host at 03:58, 13.00s elapsed
Initiating Maimon Scan at 03:58
Scanning 192.168.0.111 [1000 ports]
Completed Maimon Scan at 03:58, 0.17s elapsed (1000 total ports)
Nmap scan report for 192.168.0.111
Host is up (0.003s latency).
All 1000 scanned ports on 192.168.0.111 are in ignored states.
Note: showme[1000] closed tcp ports (reset)
MAC Address: 0B:00:27:F0:62:20 (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
          Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)
```

5.1

## 6.perform ACK flag probe :

- **-sA** : The ACK flag probe scan send 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.This scan displays that the ports are filtered on the target machine as shown in the screenshot.In this result we gt RST flag which means port id not filtered



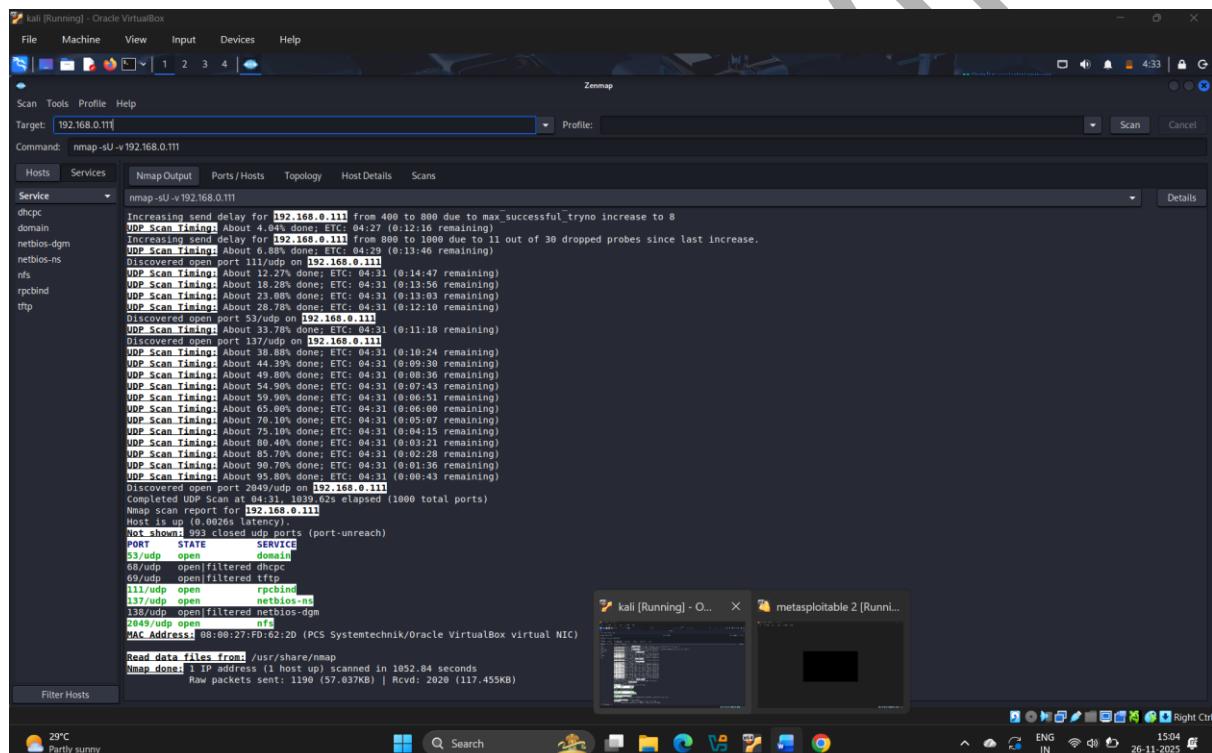
```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Scan Tools Profile Help
Target: 192.168.0.111 Profile: Scan Cancel
Command: nmap -sA -v 192.168.0.111
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
Service
nmap -sA -v 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 04:07 EST
Initiating ARP Ping Scan at 04:07
Scanning 192.168.0.111 [1 port]
Completed ARP Ping Scan at 04:07, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 04:07
Completed Parallel DNS resolution of 1 host at 04:07, 13.00s elapsed
Initiating ACK Scan at 04:07
Scanning 192.168.0.111 [1000 ports]
Completed ACK Scan at 04:07, 0.35s elapsed (1000 total ports)
Nmap scan report for 192.168.0.111
Host is up (0.038s latency).
All 1000 scanned ports on 192.168.0.111 are in ignored states.
Not shown: 3000 unfiltered TCP ports (reset)
MAC Address: 00:00:27:FD:02:20 (PC Systemtechnik/Oracle VM virtual NIC)

Read data files from: /usr/share/nmap
nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)
```

6.1

## 7.perform UDP scan :

- **-sU** : 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 that the port is open. If the port is closed and ICMP port unreachable message is received. Here we get the result as port unreachable means port is closed.



```
Zmap [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Scan Tools Profile Help
Target: 192.168.0.111 Profile: Scan Cancel
Command: nmap -sU -v 192.168.0.111
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
Service Details
Targets: 192.168.0.111
Nmap version 7.00 ( https://nmap.org ) starting at 2023-11-26 15:04
[+] Nmap done: 1 IP address (0 hosts up) scanned in 10.00 seconds
[+] Nmap done: 1 IP address (1 host up) scanned in 1059.002 seconds (1000 total ports)
Completed UDP Scan at 04:31 | 1059.002s elapsed (1000 total ports)
Nmap report for 192.168.0.111
Host is up (0.0026s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE      SERVICE
53/udp    open       dns
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind
139/udp   open       netbios-ssn
138/udp   open|filtered netbios-dgm
2049/udp  open       ntp
MAC Address: 08:00:27:F0:02:20 (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1052.04 seconds
Raw packets sent: 1190 (57.037KB) | Rcvd: 2020 (117.455KB)
```

7.1

# 8.perform Null Scan :

- **-sN** : A NULL scan in Zenmap/Nmap is a special type of TCP scan used mainly in ethical hacking and penetration testing to bypass firewalls or IDS and to map open/closed ports without sending normal TCP flags.
- If the port is closed → target replies with RST
- If the port is open → no response
- If the port is filtered → no response or ICMP unreachable
- Here we get RST response it means 977 ports are in closed state and remaining 23 are in open state

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 04:26 EST
Initiating ARP Ping Scan at 04:26
Scanning 192.168.0.111 [1 port]
Completed ARP Ping Scan at 04:26, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:26
Completed parallel DNS resolution of 1 host. at 04:26, 13.00s elapsed
Initiating NULL Scan at 04:26
Scanning 192.168.0.111 [1000 ports]
Completed NULL Scan at 04:26, 1.58s elapsed (1000 total ports)
Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
3333/tcp  open|filtered  netm
25/tcp    open|filtered  smtp
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
113/tcp   open|filtered  radmin
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
512/tcp   open|filtered  exec
513/tcp   open|filtered  login
514/tcp   open|filtered  shell
1093/tcp  open|filtered  registry
1524/tcp  open|filtered  ingreslock
2049/tcp  open|filtered  nefs
2121/tcp  open|filtered  cproxxy-ftp
3306/tcp  open|filtered  mysql
5432/tcp  open|filtered  postgresql
5900/tcp  open|filtered  vnc
6000/tcp  open|filtered  X11
6667/tcp  open|filtered  irc
8009/tcp  open|filtered  ajp13
8180/tcp  open|filtered  unknown
MAC Address: 00:0C:27:F0:62:20 (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
Raw packets sent: 1024 (40.940KB) | Rxvd: 980 (39.260KB)
```

8.1

# 9.perform service version scan:

- **-sV : service version detection** helps you to obtain information about the running services and their versions on a target system. obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to. The scan result displays that the open ports and version of services running on the ports.

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Scan Tools Profile Help
Target: 192.168.0.111 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v 192.168.0.111
Hosts Services Nmap Output Ports/Hosts Topology HostDetails Scans
OS Host
192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 04:44 EST
Nmap scan report for 192.168.0.111
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain      IEC 61850 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
535/tcp   open  logon?
514/tcp   open  mail??
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs        2-4 (RPC #100003)
2232/tcp  open  http-proxy-ftp?
3306/tcp  open  mysql      MySQL [Too many connections]
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc        VNC (protocol 3.3)
6000/tcp  open  x11        (access denied)
6667/tcp  open  irc        Unredacted
8089/tcp  open  http-alt   Apache JBoss (Protocol v1.3)
9199/tcp  open  unknown    Apache-Coyote/1.1
MAC Address: 00:00:27:FD:62:2D (PC5 Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13901.00 seconds

Filter Hosts
```

9.1

## **10.perform aggressive scan :**

- -A : It supports os detection,version scanning,script scanning,traceroute

The screenshot shows a Kali Linux desktop environment with several windows open:

- Zenmap**: The primary application window showing an Nmap scan report for target 192.168.0.111. The report details various ports and services, including an anonymous FTP login allowed on port 21.
- kali [Running] - Oracle VirtualBox**: A terminal window showing a root shell session on the target machine.
- metasploitable 2 [Running]**: Another terminal window showing a root shell session on the Metasploitable 2 host.
- File Browser**: A window showing the contents of the /var/www/html directory, which contains files for Apache and Metasploitable 2.

The desktop interface includes a top bar with File, Machine, View, Input, Devices, Help menus, and system status icons. The taskbar at the bottom shows various application icons and the current date and time (19:17, 26-11-2025).

10.1

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Scan Tools Profile Help

Target: 192.168.0.11 Profile: Scan Cancel

Command: nmap -A 192.168.0.11

Hosts Services NmapOutput Ports/Hosts Topology Host Details Scans

OS Host

192.168.0.11

nmap -A 192.168.0.11

| http-title: Metasploitable2 - Linux  
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  
113/tcp open rpcbind 2 (RPC #100000)  
| rpcinfo:  
| portnum version port/proto service  
| 100003 2,3,4 2049/tcp nfs  
| 100003 2,3,4 2049/udp nfs  
| 100005 1,2,3 5707/tcp mounted  
| 100005 1,2,3 5978/udp mounted  
139/tcp open netbios-ssn Samba smbd 3.6.0-4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.6.0-20-Debian (workgroup: WORKGROUP)  
512/tcp open exec netkit-ssh reexec  
513/tcp open login  
514/tcp open tcptrapped  
109/tcp open java-remnux GNU Classpath glibc registry  
1254/tcp open ashell Metasploitable root shell  
2049/tcp open nfs 2-4 (RPC #100003)  
2121/tcp open ftp ProFTPD 1.3.5.l  
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5  
| mysql-info:  
| protocol: 10  
| Version: 5.0.51a-3ubuntu5  
| Thread ID: 128  
| Capabilities Flags: 4364  
| Some Capabilities: Support4IAuth, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SupportsCompression, SwitchToSSLAfterHandshake, Speaks4IProtocolNew  
| Statistics:  
| calls: 401 msIndex:1mVMI:10t  
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
| ssl-date: 2025-11-26T07:54:59+00:00 -5H52m03s from scanner time.  
| ssl-cert: Subject: commonName=ubuntu4-base.localdomain/organizationName=OCDSA/stateOrProvinceName=There is no such thing outside US/countryName=XX  
| Not valid after: 2016-03-17T07:54:59Z  
| Not valid before: 2016-03-17T07:54:45Z  
5980/tcp open vnc VNC (protocol 3.3)  
| vnc-info:  
| Protocol version: 3.3  
| Security types:  
| VNC Authentication (2)  
6000/tcp open x11 (access denied)  
6667/tcp open irc UnrealIRCd  
| irc-info:  
| users: 1  
| lines: 1  
| lusers: 1  
| lservers: 0

Filter Hosts

Zmap

Scan

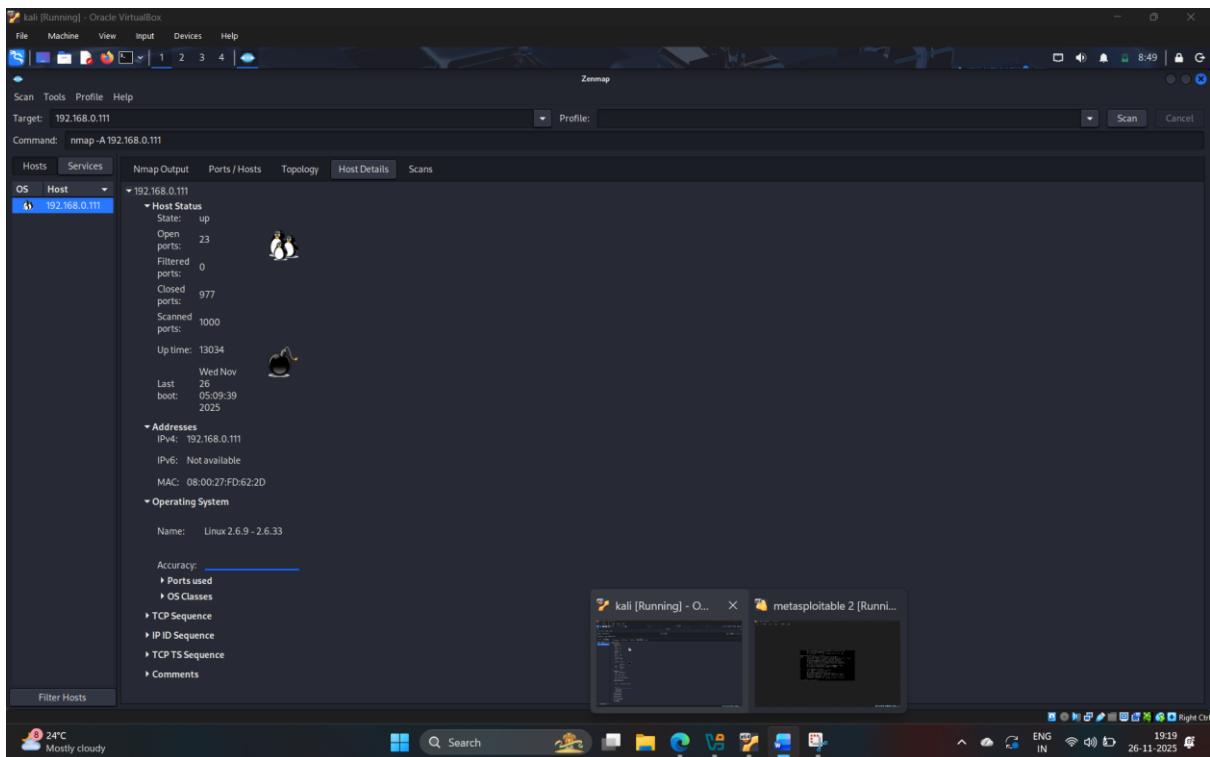
Details

19:17 26-11-2025

10.2

The screenshot shows a Kali Linux desktop environment. A terminal window titled "metasploitable 2 [Running]" is open, showing a shell session with the command "id" and its output. In the background, the ZMap application is running, scanning the IP address 192.168.0.111. The ZMap interface displays detailed information about the host, including OS detection (Ubuntu 20.04), ports open (80, 443, 8080, 8089), and service details like Apache Tomcat and MySQL. The terminal also shows the results of a "nmap -A" scan, which includes a full port scan, script execution, and traceroute information. The desktop taskbar at the bottom shows various icons for file management, browser, and system tools.

10.3



10.4

## 11 . Perform OS discovery :

- **-O : Scan result displays information about open ports and services running on those ports, operating system of target machine**

```
[root@kali:~]# nmap -sS 192.168.0.111
[+] Starting Nmap 7.91 ( https://nmap.org ) at 2025-11-26 08:52 EST
Nmap scan report for 192.168.0.111
Host is up (0.0017s latency).
Not shown: 973 closed ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  rbcbind
139/tcp   open  netbios-ssn
445/tcp   open  smb
512/tcp   open  exec
513/tcp   open  shell
1090/tcp  open  rmiregistry
1234/tcp  open  freeradius
2847/tcp  open  nfs
2312/tcp  open  cups-ppd
5432/tcp  open  postgresql
3939/tcp  open  cvs
6000/tcp  open  x11
645/tcp   open  smb
4191/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Map done: 1 IP address (1 host up) scanned in 1.46 seconds
[root@kali:~]
```

11.1

## 12.perform script :

- **--script : specifies the customize script and smb-os-discovery.nse determine os,computer name,workgroup and current time over smb protocol(port 445 and 139)**

```

root@kali:~/home/mugdha
File Machine View Input Devices Help
Session Actions Edit View Help
6000/tcp open X11
6667/tcp open irc
8089/tcp open ajp13
8333/tcp open unknown
MAC Address: 08:00:27:FD:62:2D (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Network card: Intel PRO/100 MT Desktop
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds
[+] nmap --script smb-os-discovery.nse 192.168.0.111
Starting nmap 7.95 ( https://nmap.org ) at 2025-11-26 09:02 EST
Nmap scan report for 192.168.0.111
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  vsftpd
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
330/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
535/tcp   open  vnc
514/tcp   open  shell
1099/tcp  open  rmiregistry
1234/tcp  open  ingreslock
2049/tcp  open  nmb
2111/tcp  open  cccproxy-ftp
3389/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  nc
6000/tcp  open  X11
6667/tcp  open  irc
8089/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:FD:62:2D (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|_ OS: Linux (Samba 3.0.29-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-11-26T03:10:28+05:00

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
[+] root@kali:~/home/mugdha

```

12.1

## 13. Evasion of firewall :

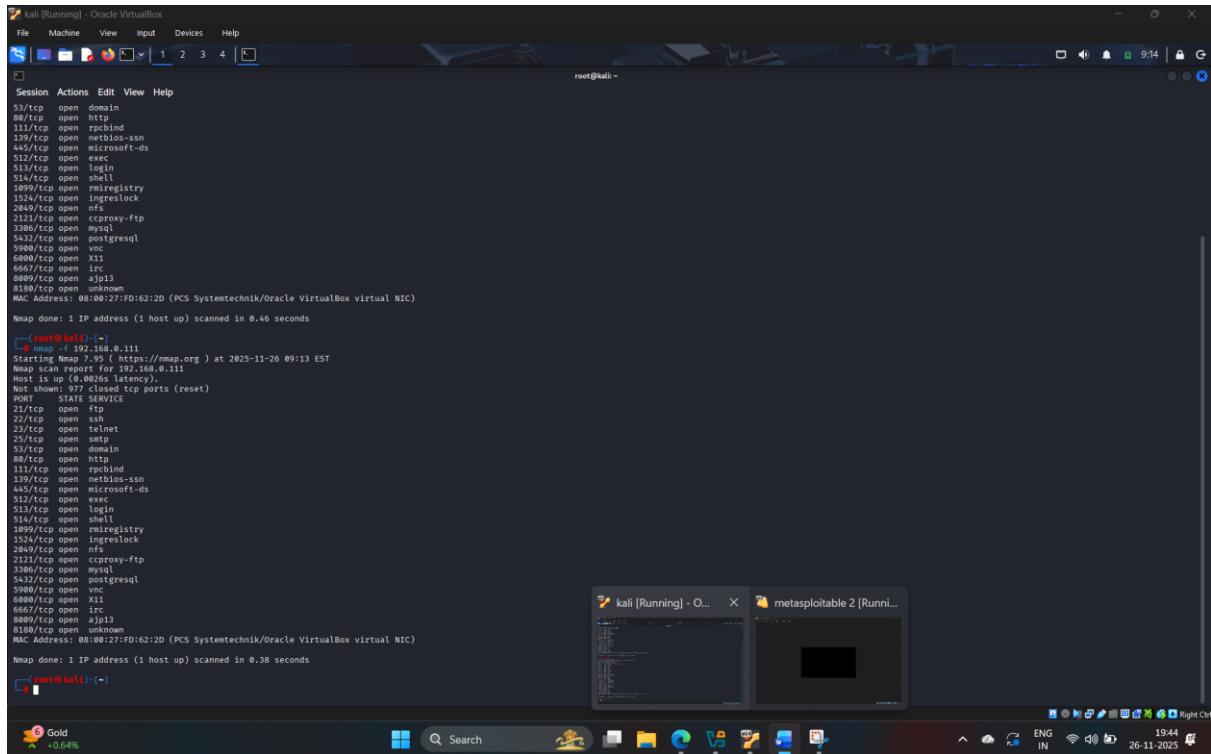
- Nmap offers many features to help understand complex networks with enabled security and supports mechanisms for bypassing poorly implemented defenses using nmap**

**various techniques can be implemented which can bypass the IDS/firewall security mechanism.**

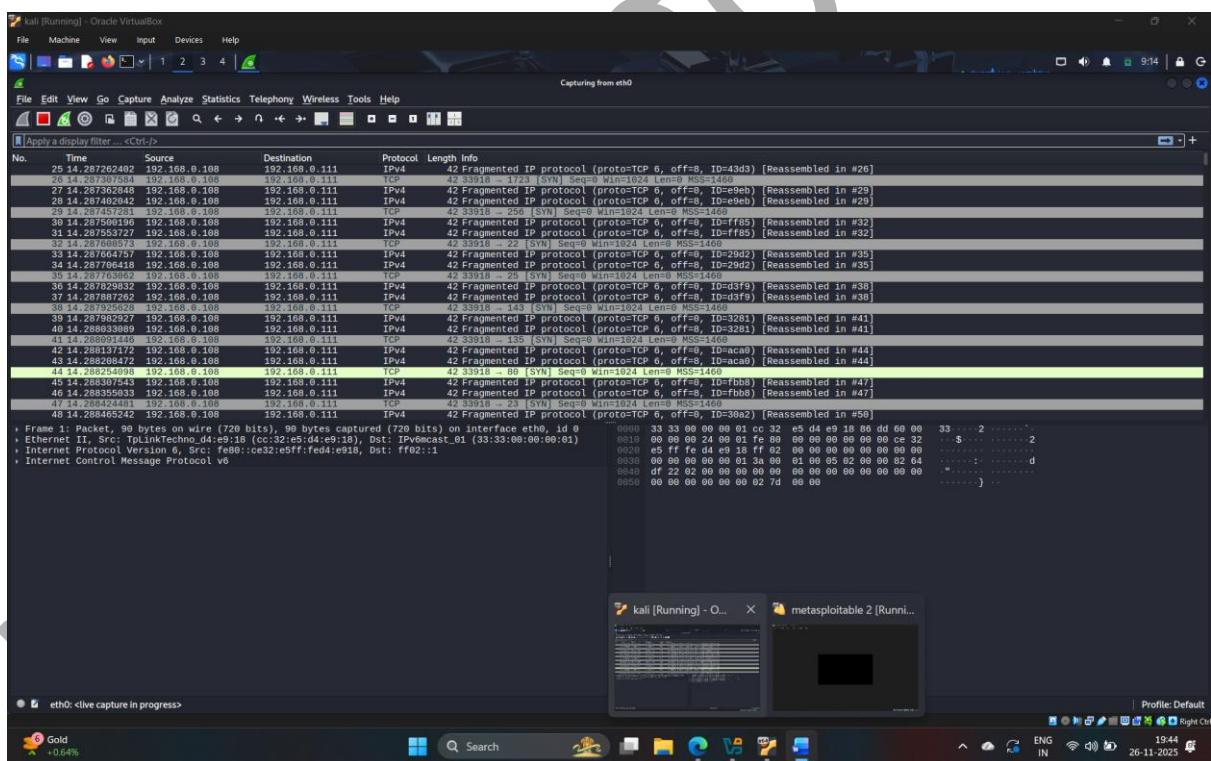
- **Here are some techniques :**

#### **1.fragmentation :**

- **Packet fragmentation refers to the splitting of a probe packet into several smaller packlets(fragments) while sending it to a network.**
- **When these packets reach a host,IDS and firewall behind the host generally queue all of them and process them one by one.**
- **However since this method of processing involves greater CPU consumption as well as mnetwork resources,the configuration of most of IDS's makes it skip fragmented packets during port scans.**
- **-f : whitch is used to split the ip packet into tiny gragment packets.**



### 13.1.1



### 13.1.2

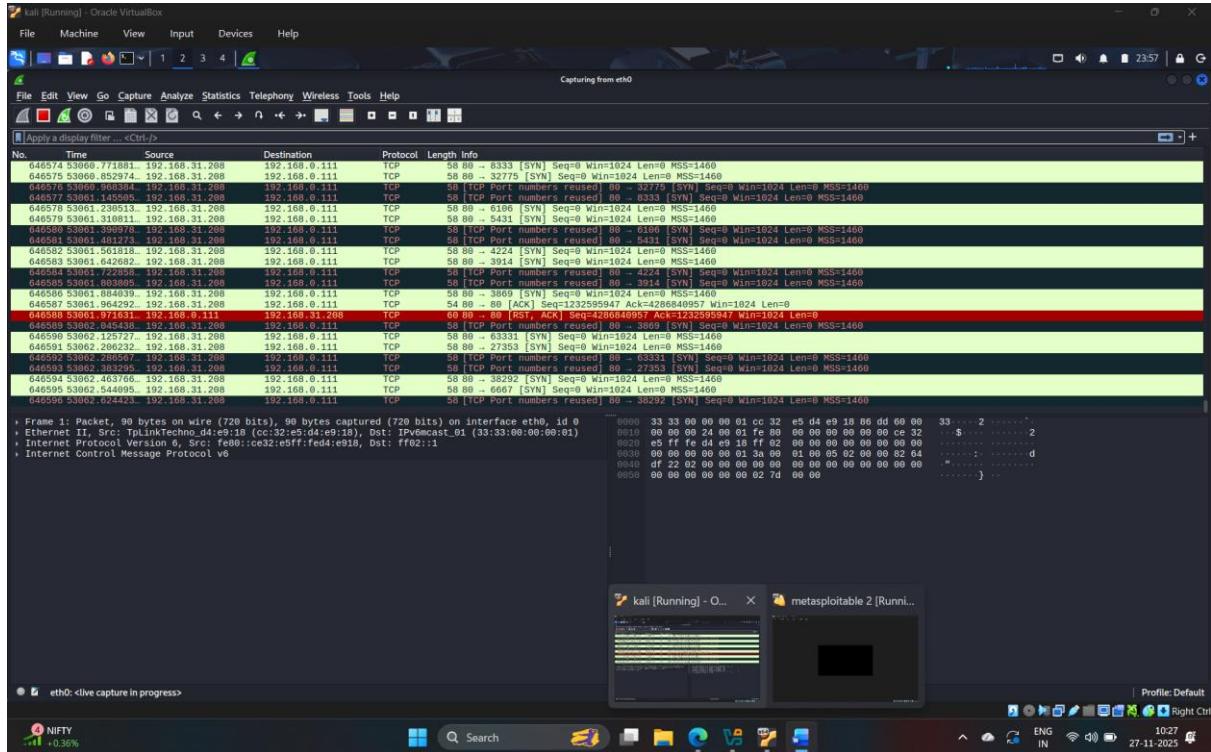
## 2.source port :

- 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.
- -g : this is the command used to perform source port manipulation.

```
[root@kali]# nmap -g 80 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 09:33 EST
Nmap scan report for 192.168.0.111
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
[root@kali]# nmap -g 80 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 23:54 EST
■
```

13.2.1



### 13.2.2

## 3.maximum transmission unit:

- Using mtu smaller packets are transmitted instead of sending one complete packet at a time this technique evades the filtering and detection mechanism enables in the target machine**
- mtu : this specifies the number of maximum transmission unit here 8 bytes of packet.**

```

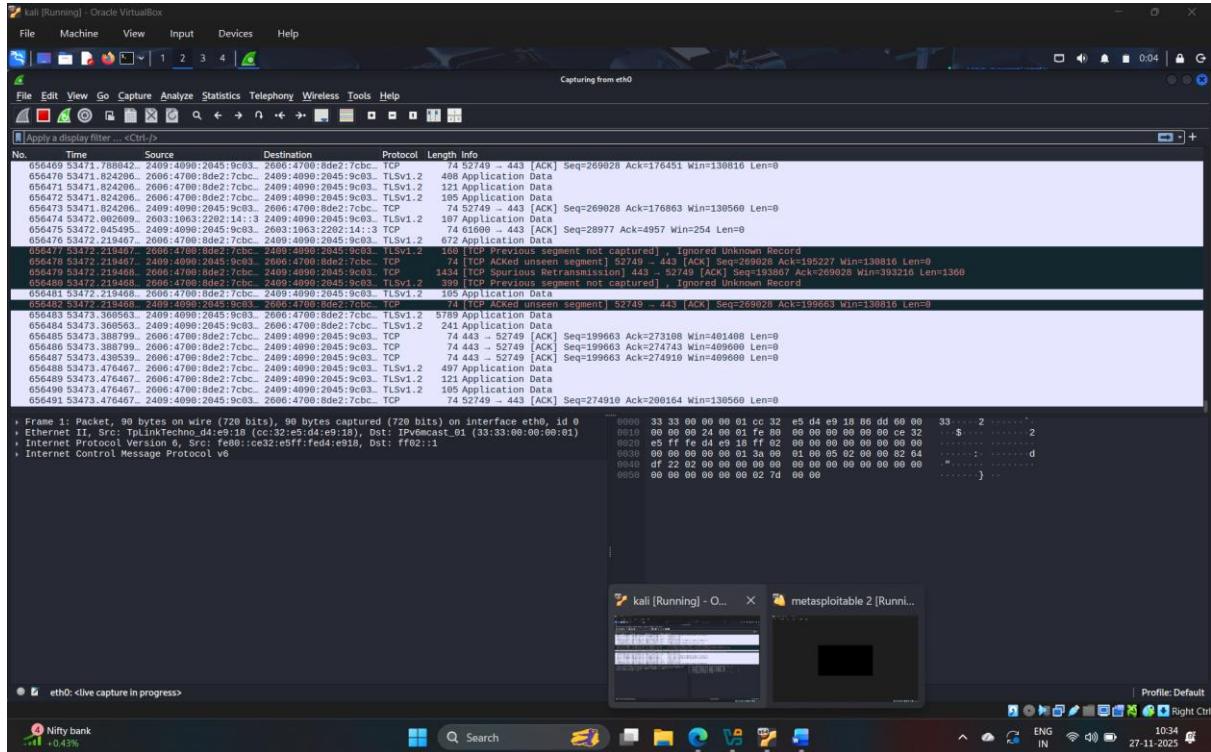
[root@kali]-[~]
# nmap -mtu 8 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 00:00 EST
Nmap scan report for 192.168.0.111
Host is up (0.0091s latency).
All 1000 scanned ports on 192.168.0.111 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds

[root@kali]-[~]
# 

```

### 13.3.1



### 13.3.2

## 4.decoy :

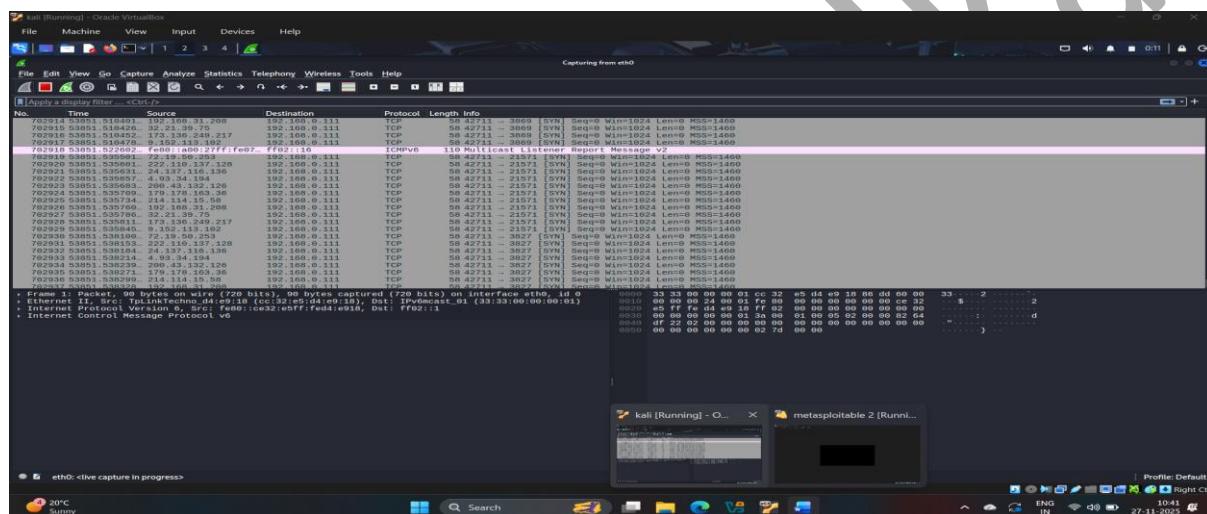
- The ip address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall.
- This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP address were decoys.
- By using this command nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.
- -D : performs decoy scan
- -RND : generates a random and non reserved IP addresses (here 10).

```
(root㉿kali)-[~]
# nmap -D RND:10 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 00:10 EST
Nmap scan report for 192.168.0.111
Host is up (0.059s latency).
All 1000 scanned ports on 192.168.0.111 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds

(root㉿kali)-[~]
#
```

### 13.4.1



### 13.4.2

## 5.mac spoof :

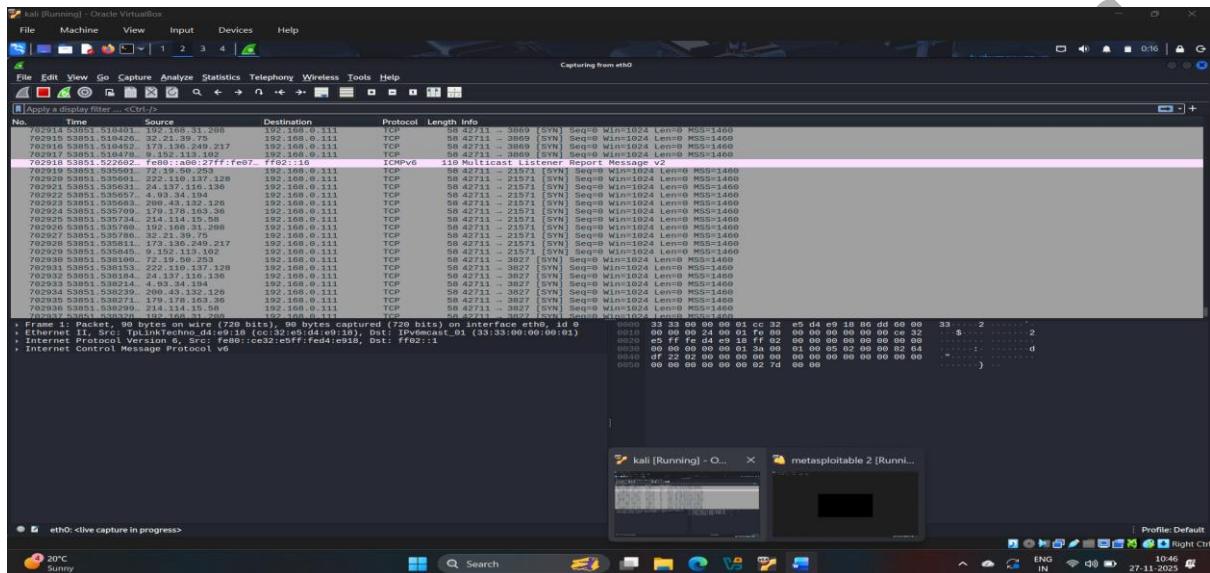
- MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network**
- This technique allows you to send request packets to the targeted machine/network pretending to be a legitimate host**
- spoof-mac 0 : this represent randomizing the MAC address**
- sT : performs the TCP connect?full open scan**
- Pn : is used to skip the host discovery**

```

└─[root@kali]─[~]
# nmap -sT -Pn --spoof-mac 0 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 00:15 EST
Spoofing MAC address 43:57:51:2D:49:AD (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.

```

### 13.5.1



### 13.5.2

# **14.scan a target network using Metasploit :**

- Metasploit framework is a tool that provides information about security vulnerabilities in the target organization system and aids in penetration testing and IDS signature development
- It facilitates the tasks of attackers exploit writers and payload writers
- A major advantage of the framework is the modular approach that is allowing the combination of any exploit with any payload
- Here we will use Metasploit to discover active hosts, open ports, services running, and os details of systems present in the target network
- Execute command msfconsole to launch Metasploit.
- An msf command line appears type nmap -Pn -sS -A -oX Test 192.168.0.0/24 and press enter to scan the subnet as shown in the screenshot. Here we are scanning the whole subnet for active hosts
- After scanning completes nmap displays the host information in the target network along with open ports, service and os enumeration

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

root@kali:/home/mugdha root@kali:/home/mugdha

```
[mugdha@kali:~]# sudo su
[sudo] password for mugdha:
[root@kali:~]# msfconsole
Metasploit tip: Store discovered credentials for later use with creds

... (Metasploit command history and exploit details)
```

+ --=[ metasploit v6.4.98-dev ]  
+ --=[ 2,571 exploits + 1,316 auxiliary - 1,683 payloads ]  
+ --=[ 433 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

```
[msf] > nmap -Pn -sB -A -oX Test 192.168.0.0/24
[msf] exec: nmap -Pn -sS -A -oX Test 192.168.0.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 23:10 EST
Nmap scan report for 192.168.0.1
Host is up (0.020s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  BusyBox telnetd 1.14.0 or later (TP-LINK router telnetd)
53/tcp    open  domain  PowerDNS Recursor 4.8.8
| dns-nse:
|_ id.nse: ns81 {6e733031}
| id.server: ns81
|_ bind.version: PowerDNS Recursor 4.8.8
80/tcp    open  http   TP-LINK WAP http config
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
1980/tcp   open  ssh   Unprivileged SSH for UPnP devices 1.6.19 (Linux 3.10.14; UPnP 1.0)
|_http-title: C2523:EB:D4:E9:18 (TP-Link Technologies)
Device type: general purpose
Running: Linux 2.6.X!#X
```

26°C Sunny

13:38 28-11-2025

14.1

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

root@kali:/home/mugdha root@kali:/home/mugdha

```
Device type: general purpose
Running: Linux 2.6.X!#X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.13
Network Distance: 1 hop
Service Info: OS: linux; Devices: broadband router, WAP; CPE: cpe:/o:linux:linux_kernel:3.10.14

TRACEROUTE
HOP RTT ADDRESS
1 7.97 ms 192.168.0.1

Nmap scan report for 192.168.0.102
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
| 1024 60:0f:cfe:1c:05:f6:a7:74:d6:90:24:fac:c4:dd:56:cc (DSA)
| 2048 56:56:24:0f:21:1d:de:a7:2b:ae:01:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp  Postfix smtpd
|_smtp-commands: netcatutable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-11-28T04:00:00+00:00; -10m53s from scanner time.
|_ssl-v3: 
|_ssl-tls: 
|_ssl-sslv2 supported
|_ciphers:
|  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|  SSL2_RC2_128_CBC_WITH_MD5
|  SSL2_RC4_128_WITH_MD5
|  SSL2_RC4_40_WITH_MD5
|  SSL2_RC4_128_EXPORT40_WITH_MD5
|  SSL2_RC4_128_EXPORT40_WITH_MD5
|  SSL2_DES_40_EDE3_CBC_WITH_MD5
53/tcp    open  domain  ISC BIND 9.4.2
| dns-nse:
| bind.version: 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind 2 (RPC #100000)
```

NIFTY +0.03%

metasploitable 2 [Running] - O... window 7 [Running] - O...

13:40 28-11-2025

14.2

```

root@kali:~/home/mugdha root@kali:~/home/mugdha
[+] http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
|_ service version port/proto service
|   100000 2      111/tcp rpcbind
|   100000 2      111/udp rpcbind
|   100003 2,3,4  2049/tcp nfs
|   100004 2,3,4  2049/udp nfs
|   100005 1,2,3  4415/udp mountd
|   100005 1,2,3  49971/tcp mountd
|   100021 1,3,4  36852/tcp lockmgr
|   100024 1,3,4  44509/tcp status
|   100024 1      50528/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp open exec netkit-ssh reexec
513/tcp open login
514/tcp open tcptrapped
1433/tcp open jdbc-mlm GNU Classpath gmiregistry
524/tcp open metasploit Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread: 1
|_ Capabilities Flags: 43564
|_ Some Capabilities: ConnectWithDatabase, Support41Auth, Speaks41ProtocolNew, SupportsCompression, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions
|_ Status: Autocommit
|_ Sockets: AutoCommit
5800/tcp open postgres PostgreSQL DB 8.3.0 - 8.3.7
| ssl-date: 2025-11-28T04:00:00+00:00; -10m53s from scanner time.
| ssl-cert: Subject: commonName=metasploitable4-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Valid Until: 2010-03-16T14:07:45
|_ Not valid after: 2010-03-16T14:07:45
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|_ protocol version: 3.3
|_ security types:
|_ VNC Authentication (2)
6000/tcp open x11 (access denied)
6001/tcp open x11 Unspecified
6009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_ http-title: Apache Tomcat/5.5.24
|_ http-favicon: Apache Tomcat
Mac Address: 08:00:27:F0:D6:2D (RCS Systemtechnik/Oracle VirtualBox virtual NIC)
OS: Windows 7 Home Premium
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

```

14.3

- Type search portscan and press enter the etasploit port scanning modules appear as shown in the screenshot

```

Host script results:
|_ smbd - discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   SMB3 support: yes
|   NetBIOS computer name: 
|   Domain name: localdomain
|   FQDN: metasploitable4-base.localdomain
|   System time: 2025-11-27T23:00:02-05:00
|   SMB2 support: yes
|   account_used: cbtlan_
|   authentication_level: user
|   challenge_response_supported: yes
|   message_signing: disabled (dangerous, but default)
|   _obbies: NetBIOS: METABACONNECT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|   _obbies: Protocol: SMB2 (SMB2)
|   _obbies: Connection failed (SMB2)
|   _obbies: Clock skew: mean: 1nb4m07s, deviation: 2h30m00s, median: -10m53s
|_ clock-skew: mean: 1nb4m07s, deviation: 2h30m00s, median: -10m53s

TRACEROUTE
HOP RTT ADDRESS
1  2.02 ms 192.168.0.105

Nmap scan report for 192.168.0.105
Host is up (0.0005s latency).
All 1000 scanned ports on 192.168.0.105 are in ignored states.
Not shown: 296 IP addresses (4 hosts up) scanned in 31.88 seconds
MAC Address: 70:15:FB:7B:41:07 (Unknown)
TCP port 22: Service fingerprinting failed this host to give specific OS details
Network Distance: 1 hop

NMAP OUTPUT
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 296 IP addresses (4 hosts up) scanned in 31.88 seconds
Nmap search: portscan

Matching Modules
# Name                                Disclosure Date  Rank    Check  Description
0 auxiliary/scanner/portscan/ftpbounce  normal        No     ETP Bounce Port Scanner
1 auxiliary/scanner/natpmp/natpmp_portscan  normal        No     NAT-PMP External Port Scann
2 auxiliary/scanner/nmap/nmap_portscanner  normal        No     Nmap Port Scanner
3 auxiliary/scanner/portscan/xmas        normal        No     TCP XMAS Port Scanner
4 auxiliary/scanner/portscan/ack          normal        No     TCP ACK Firewall Scanner
5 auxiliary/scanner/portscan/tcp          normal        No     TCP Port scanner

```

14.4

- Here we use auxillary/scanner/portscanner/tcp
- Set RHOST
- Set thread
- Run

```

root@kali:~/home/mugdha# msf auxiliary(scanner/portscan/syn) > use auxiliary/scanner/portscan/tcp
[!] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) > set INTERFACE eth0
INTERFACE => eth0
msf auxiliary(scanner/portscan/tcp) > set PORTS 80
PORTS => 80
msf auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.0.5-110
RHOSTS => 192.168.0.5-110
msf auxiliary(scanner/portscan/tcp) > set THREADS 50
THREADS => 50
msf auxiliary(scanner/portscan/tcp) > run
[*] /share/metasploit-framework/msfvenom/exploit/capture.rb:123: warning: undefining the allocator of T_DATA class PCAPRUB::Pcap
[*] Exploit running: [none] (100% done)
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) > back
msf > use 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 host, in milliseconds
JITTER 0  yes  The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000  yes  Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 192.168.0.5-110  yes  The target hosts(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) > set RHOSTS 162.241.216.11
RHOSTS => 162.241.216.11
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 (e.g. 22-25,80,110-900)
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

```

The terminal window is running on a Kali Linux system, with a watermark 'mugdah' diagonally across the screen. In the background, there is another window titled 'window 7 [Running] - O...' showing a Windows 7 desktop environment.

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

root@kali:/home/mugdha

```
4 auxiliary/scanner/portscan/ack . normal No TCP ACK Firewall 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/syn
msf auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf auxiliary(scanner/portscan/syn) > set RHOSTS 192.168.0.5-110
RHOSTS => 192.168.0.5-110
msf auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf auxiliary(scanner/portscan/syn) > run
/usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123: warning: undefining the allocator of T_DATA class PCAPRUB::Pcap
[*] Scanned 106 of 106 hosts (100% complete)
[*] Auxiliary exploit module successfully loaded
msf auxiliary(scanner/portscan/syn) > back
msf > use 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 (e.g. 22-25,80,110-900)                                                                  |
| RHOSTS      | yes             | 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) > set RHOSTS 162.241.216.11
RHOSTS => 162.241.216.11
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 (e.g. 22-25,80,110-900)                                                                  |
| 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                                                             |


```

14.5

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

root@kali:~/home/mugdha

```
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 (e.g. 22-25,80,110-900)
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 - 162.241.216.11:25 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:26 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:22 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:21 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:19 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:180 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:143 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:143 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:1465 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:89 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:19 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:995 - 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 - 162.241.216.11:2083 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:10480 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:12077 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2086 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2090 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2095 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2222 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:13300 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:1432 - TCP OPEN
[*] 162.241.216.11 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf auxiliary(scanner/portscan/tcp) > use 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 (e.g. 22-25,80,110-900)
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.
```

14.6

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Session Actions Edit View Help

```
root@kali:~/home/mugdha root@kali:~/home/mugdha
[+] 162.241.216.11 - 162.241.216.11:2096 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:2895 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:2222 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:3386 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:5432 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:22 - TCP OPEN
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) > use 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 (e.g. 22-25,80,113,443)
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.

[*] Unknown datastore option THREAD. Did you mean THREAD?
THREAD => 11
msf auxiliary(scanner/portscan/tcp) > run
[*] Starting port scan on 162.241.216.11 (TCP)
[*] 162.241.216.11 - 162.241.216.11:21 - 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 - 162.241.216.11:53 - 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 - 162.241.216.11:443 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:465 - 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 - 162.241.216.11:1093 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2078 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2077 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2087 - 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 - 162.241.216.11:2896 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2895 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:2222 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:3386 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:5432 - TCP OPEN
[*] 162.241.216.11 - 162.241.216.11:22 - TCP OPEN
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) >
```

14.6