Module 3
Network Scanning

25.11.25

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

INDEX:

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 generate a virtual circuit between sender and receiver for the duration of transmission.**
- **stram and dat transfer,multi routing,logical connection,full duplex.**

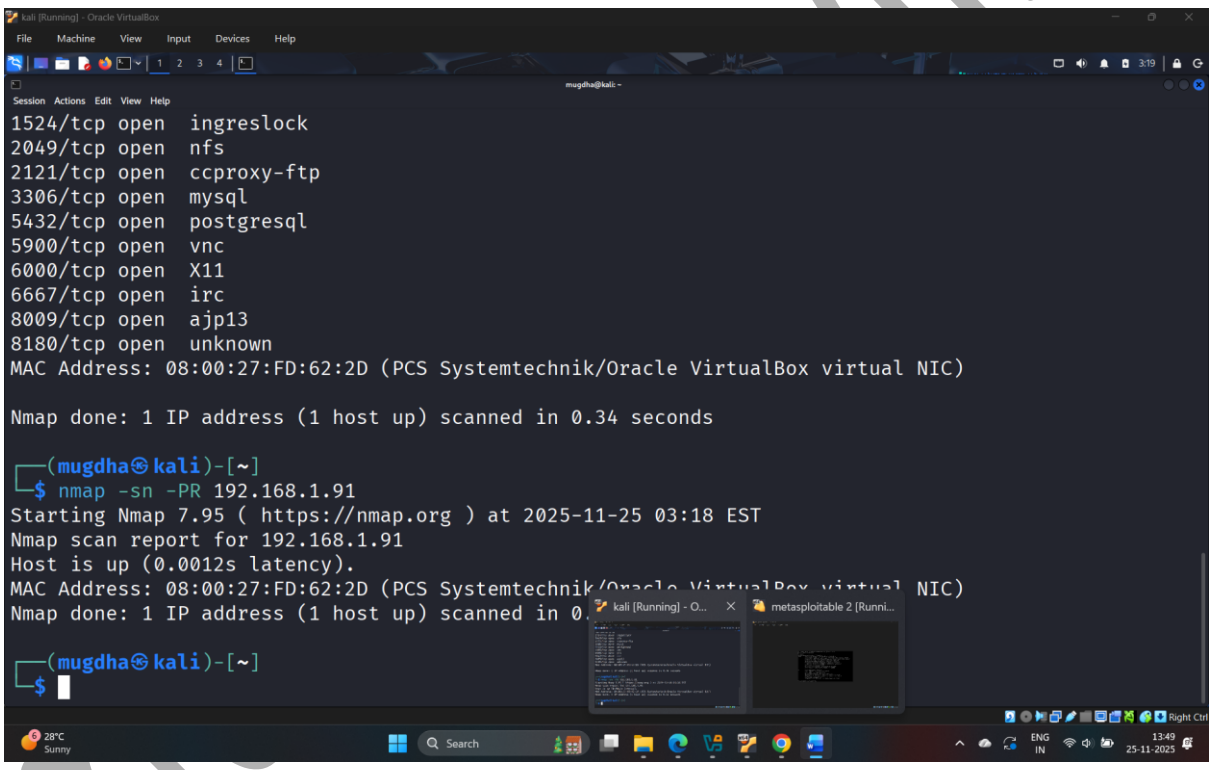
III. UDP :

- **UDP stand for user datagram protocol**
- **UDP isa 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:

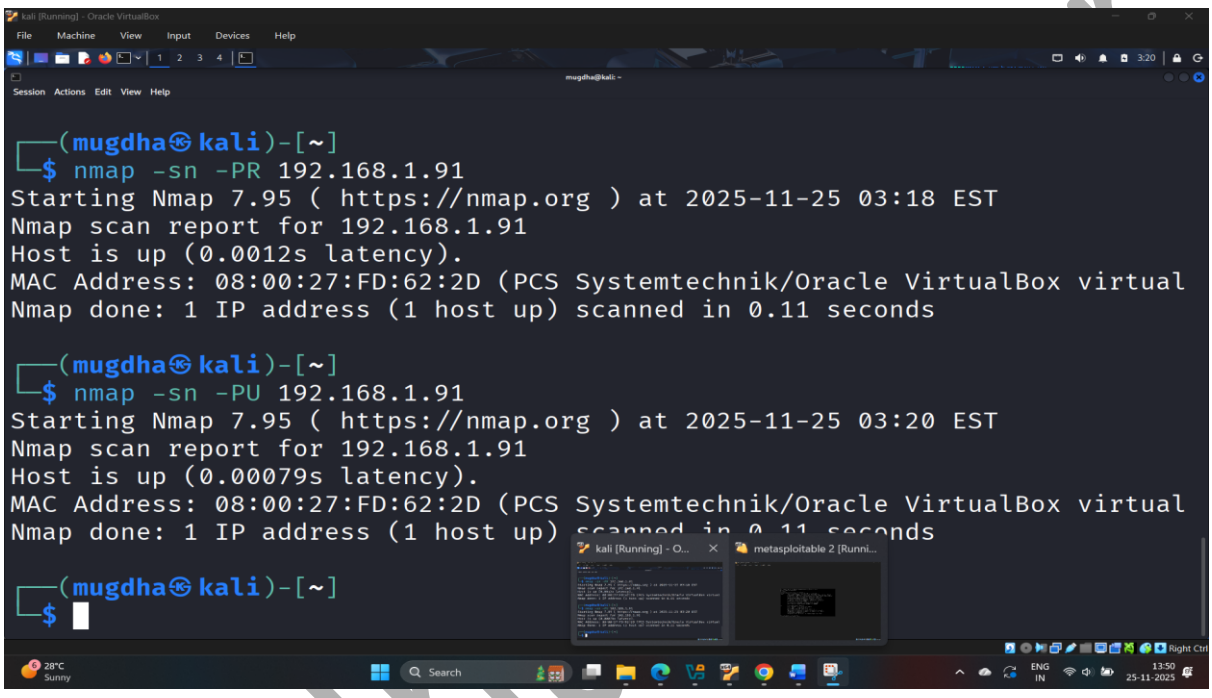
Host discovery using Nmap means finding which devices (hosts) are active/alive on a network without doing a full port scan.It is the first step in network scanning & penetration testing.

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**



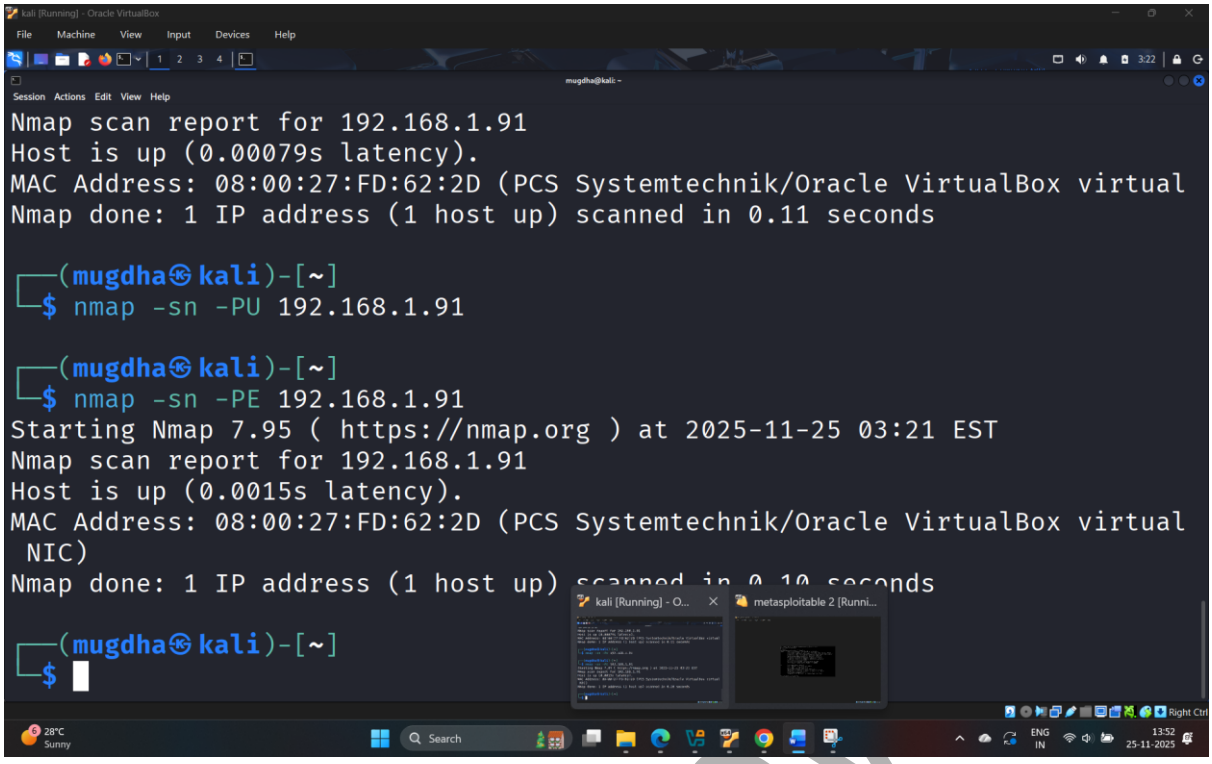
1.2.1

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**



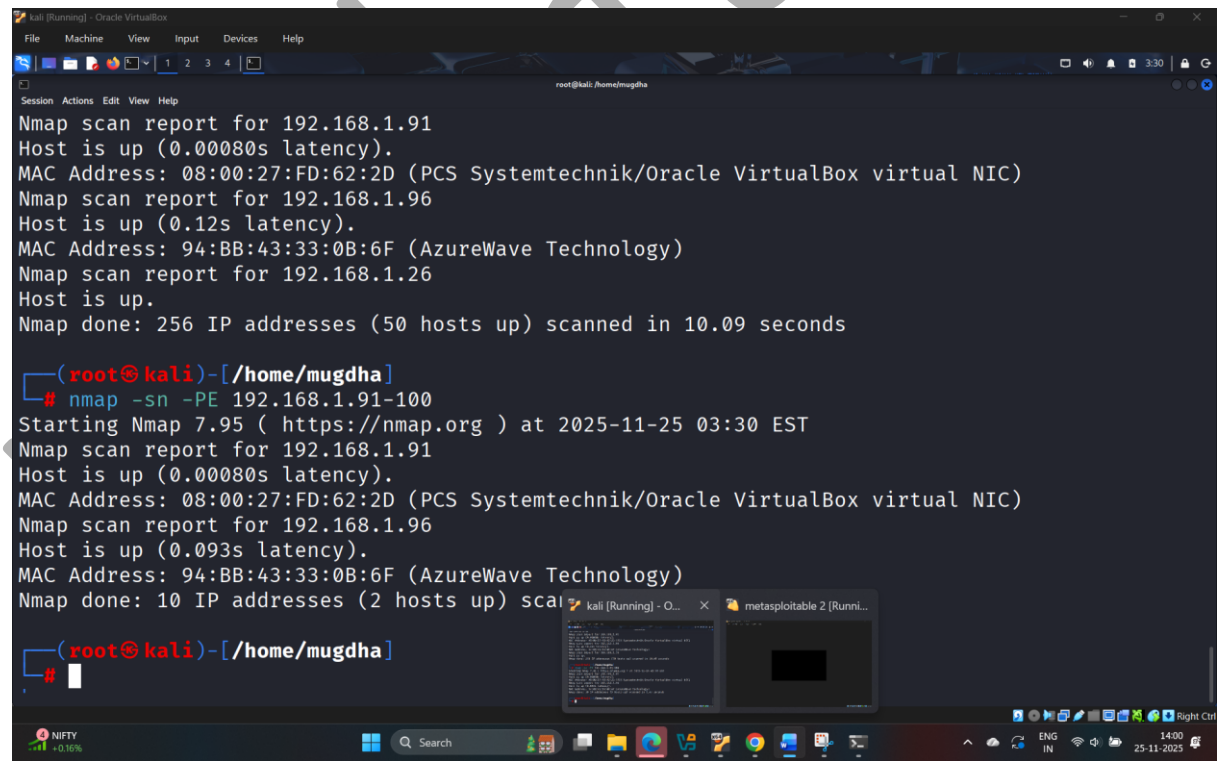
1.3.1

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**

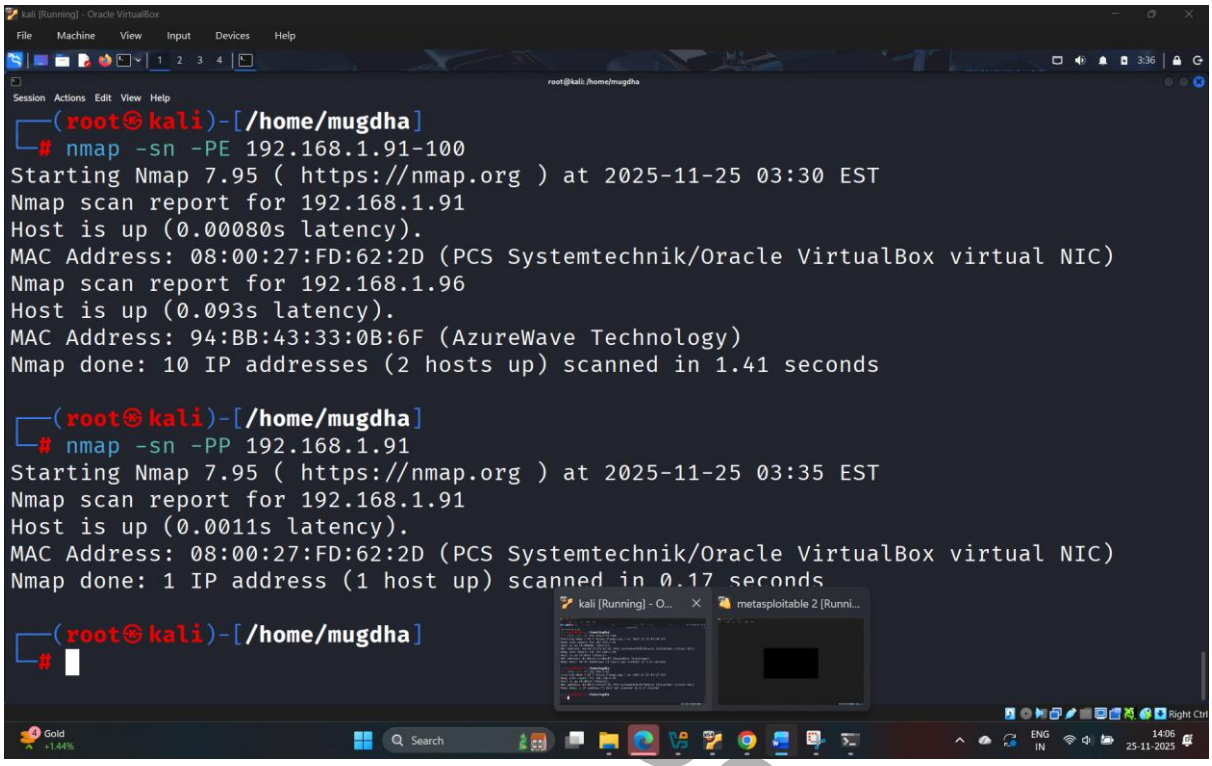


1.4.1

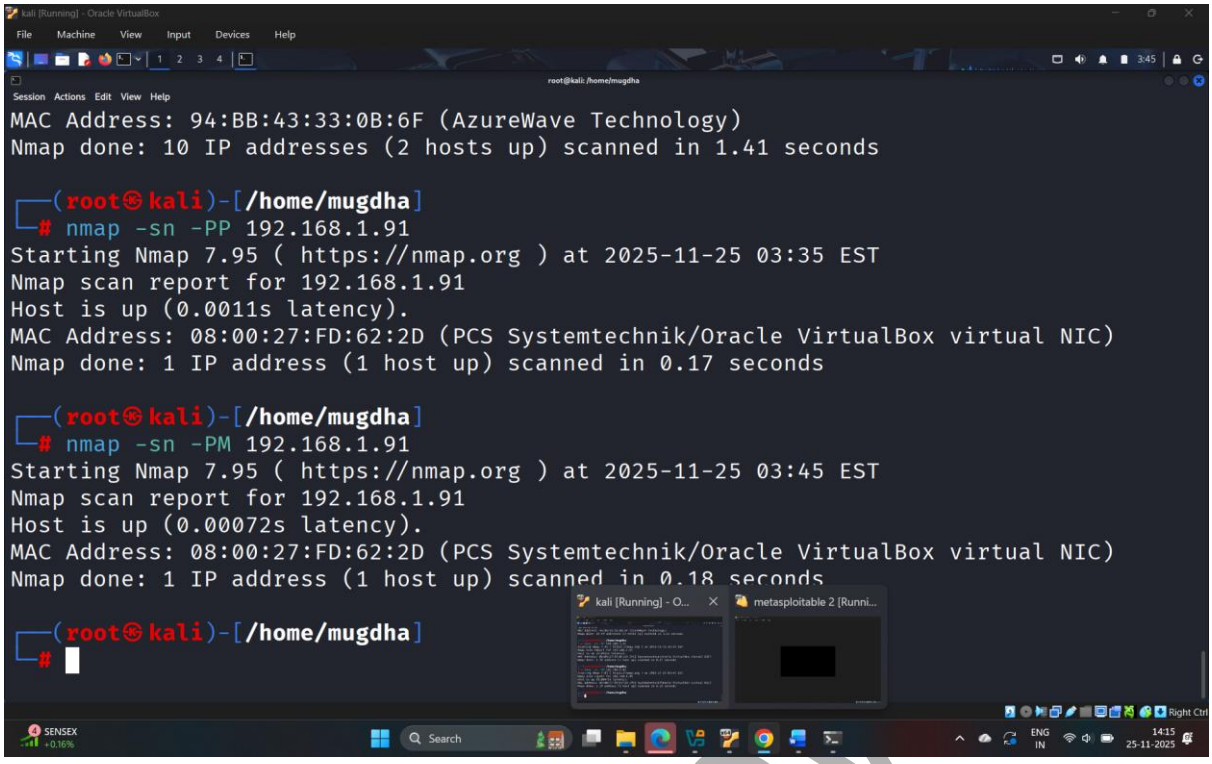
5. **-PE : ICMP echo ping sweep to discover live hosts from a range of target IP addresses by sending ICMP echo requests to multiple hosts if a host is alive it will return an ICMP echo reply .Here we are setting the range of 100**



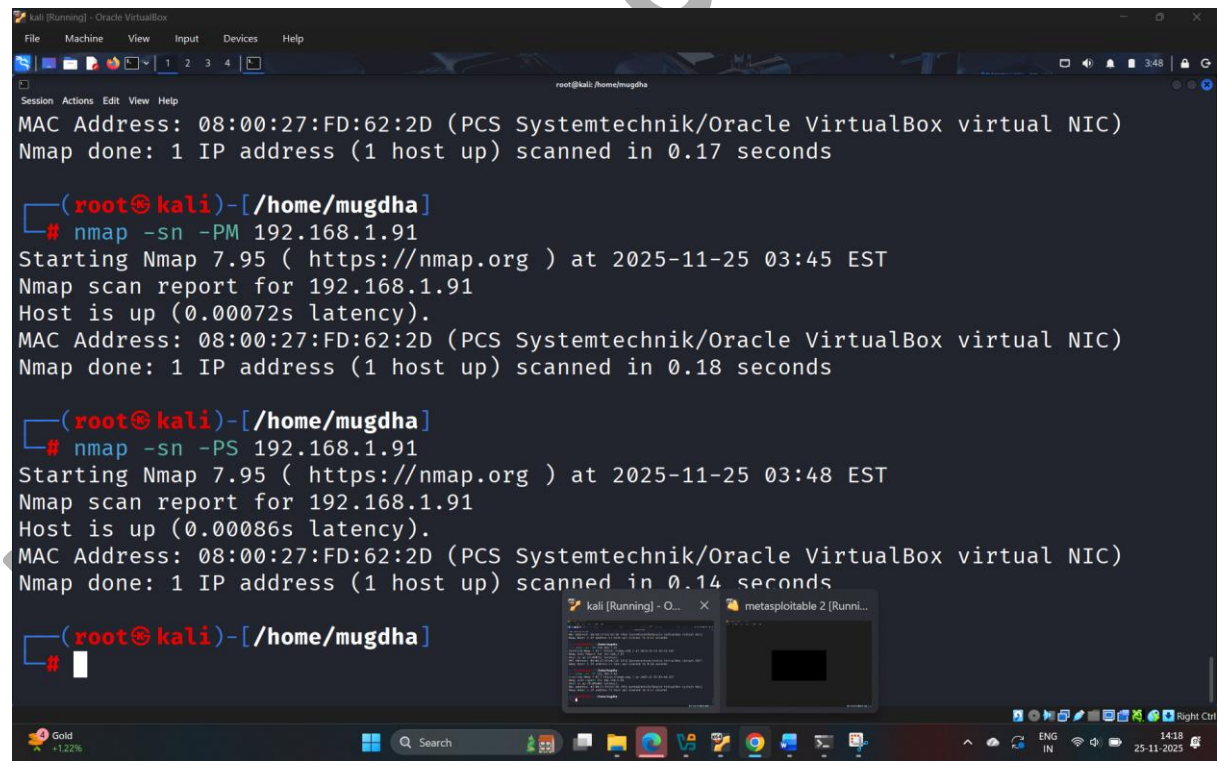
6. **-PP : ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine**



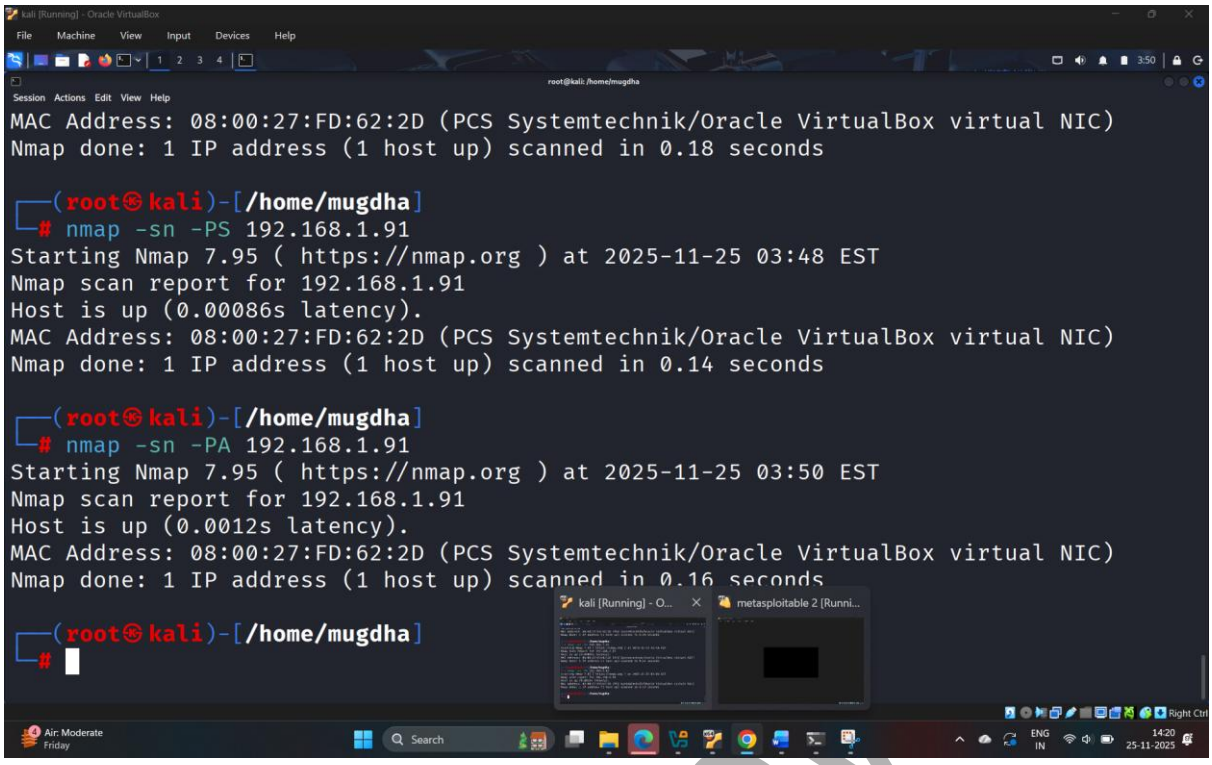
7. **-PM : this technique is an alternative for the traditional ICMP echo ping scan which are used to determine whether the target host is alive specifically when administrators block the ICMP echo pings**



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**

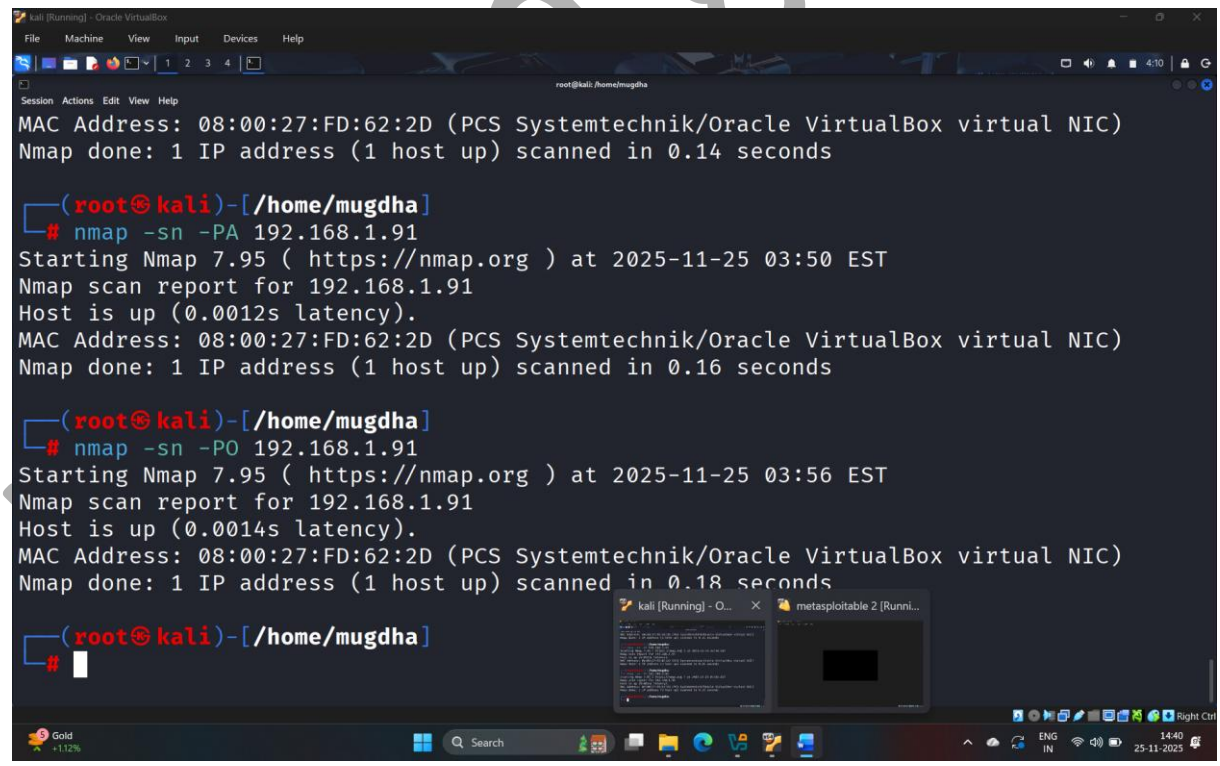


9. **-PA : TCP ACK ping scan is the technique that sends empty TCP ACK packets to the target host.An ACK response means that the host is active**



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



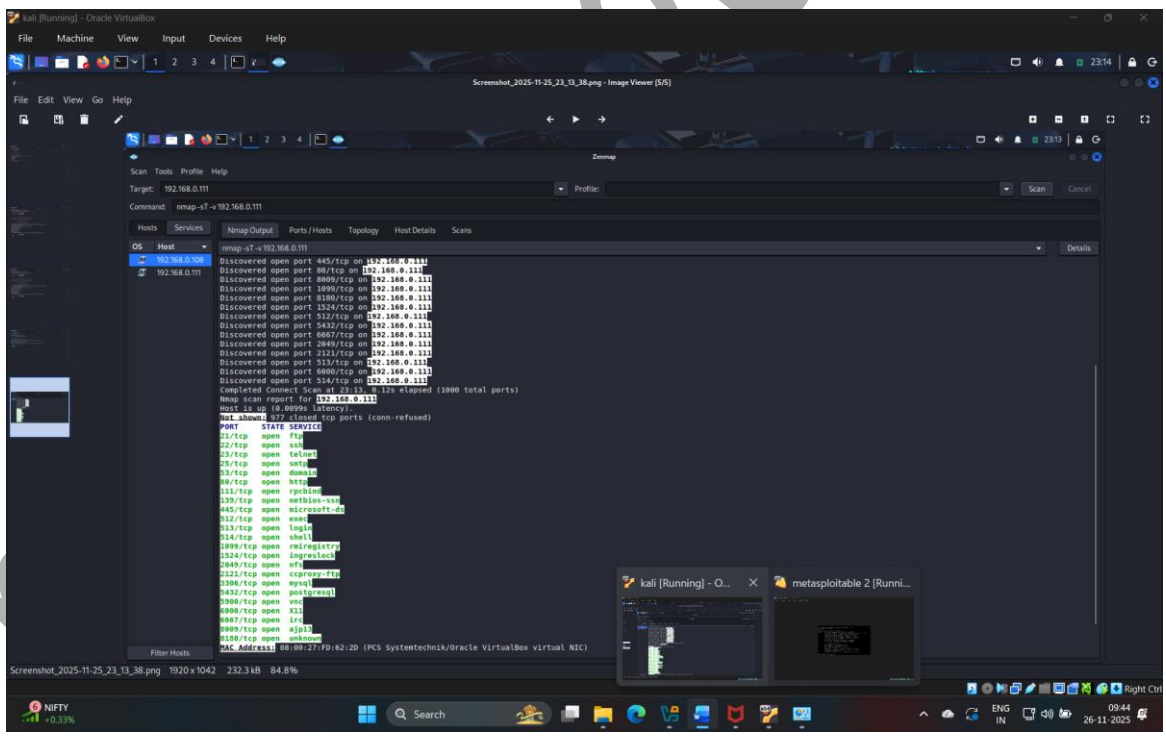
1.10.1

2.explore zenmap using nmap:

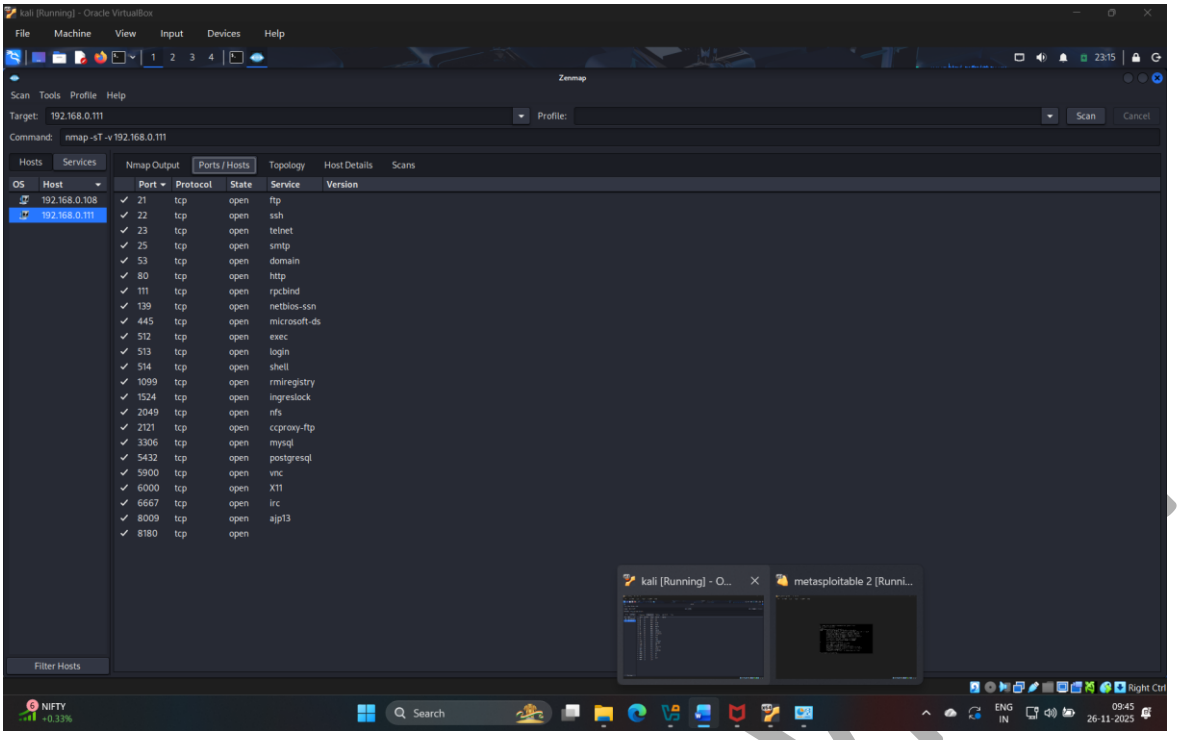
Zenmap is the official GUI (Graphical User Interface) for Nmap.It makes network scanning easier for beginners and faster for professionals. Instead of typing commands in terminal, Zenmap allows you to run scans with buttons and menus. Zenmap includes ready-made scan templates like:

- **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 displayes :port,protocol,state,service, version,scan**

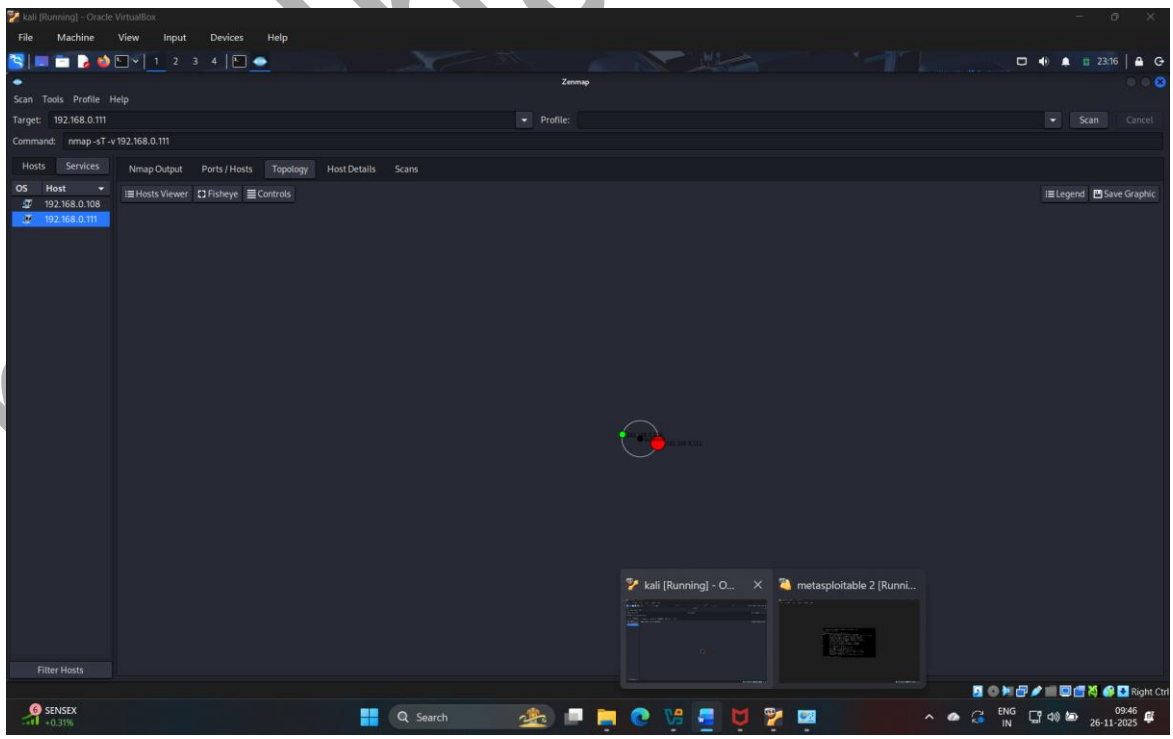


2.1



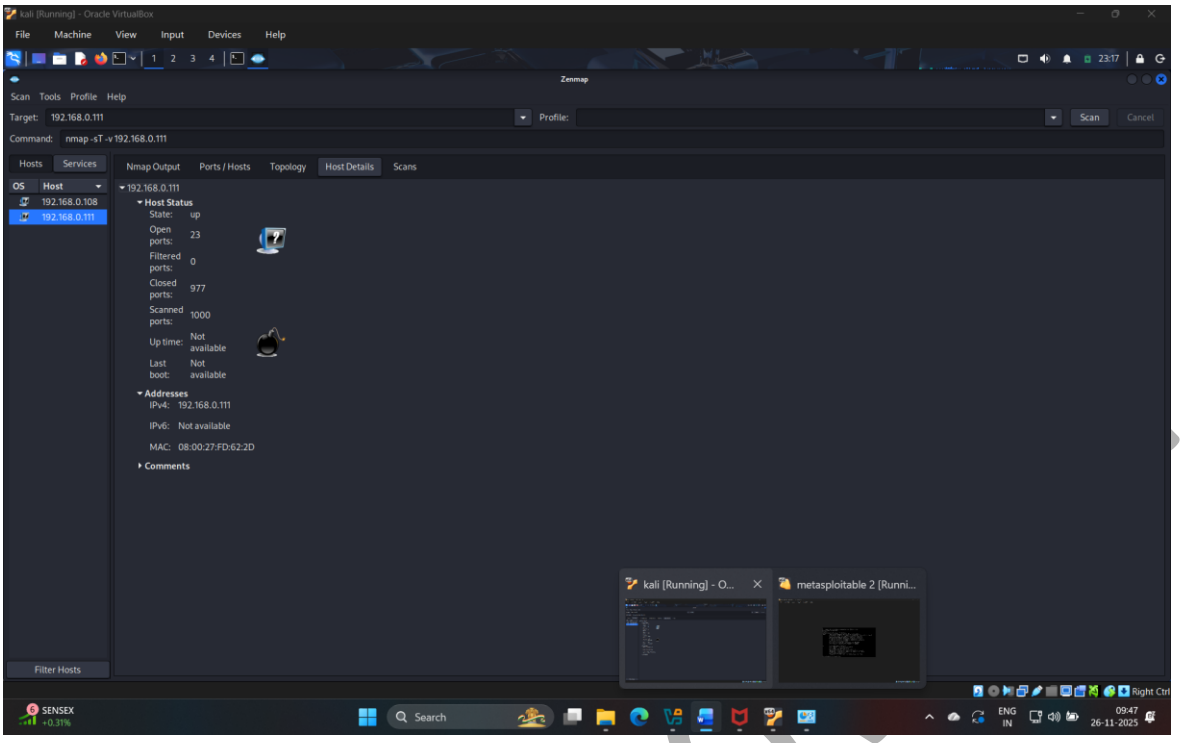
2.2

3. **Click on the topology that shows provided ip :**



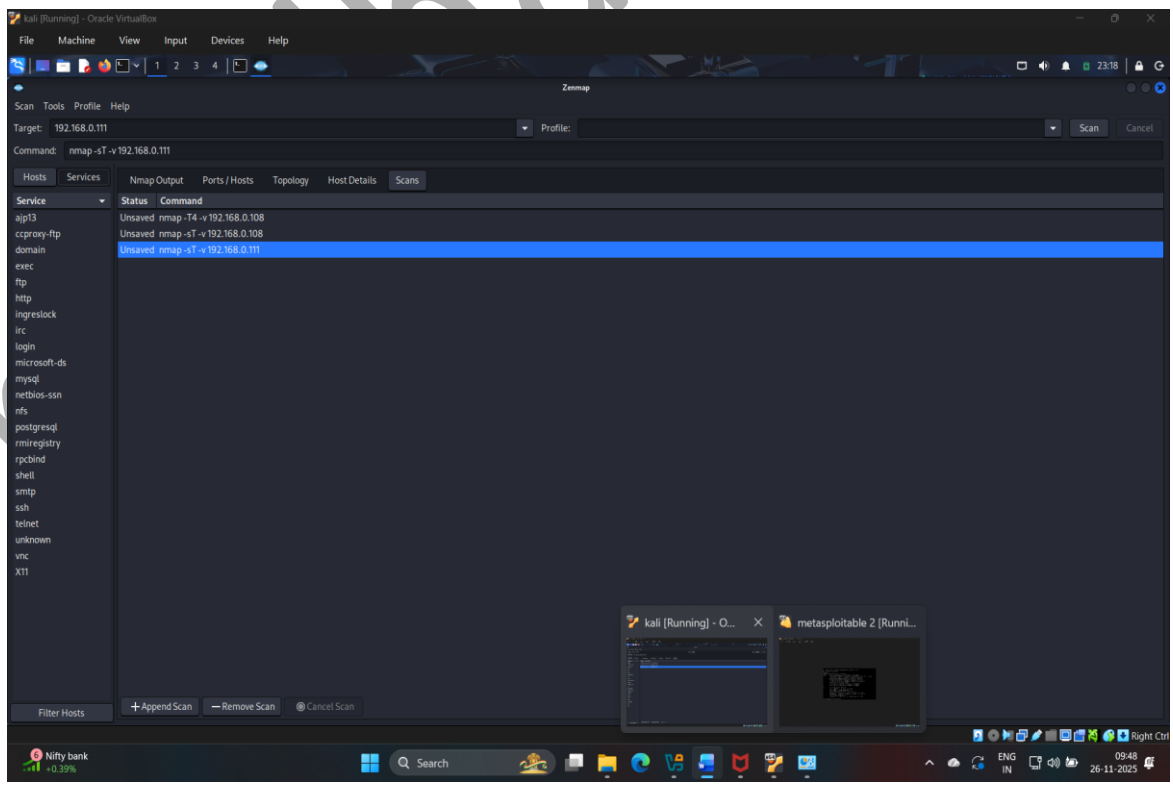
2.3

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



2.4

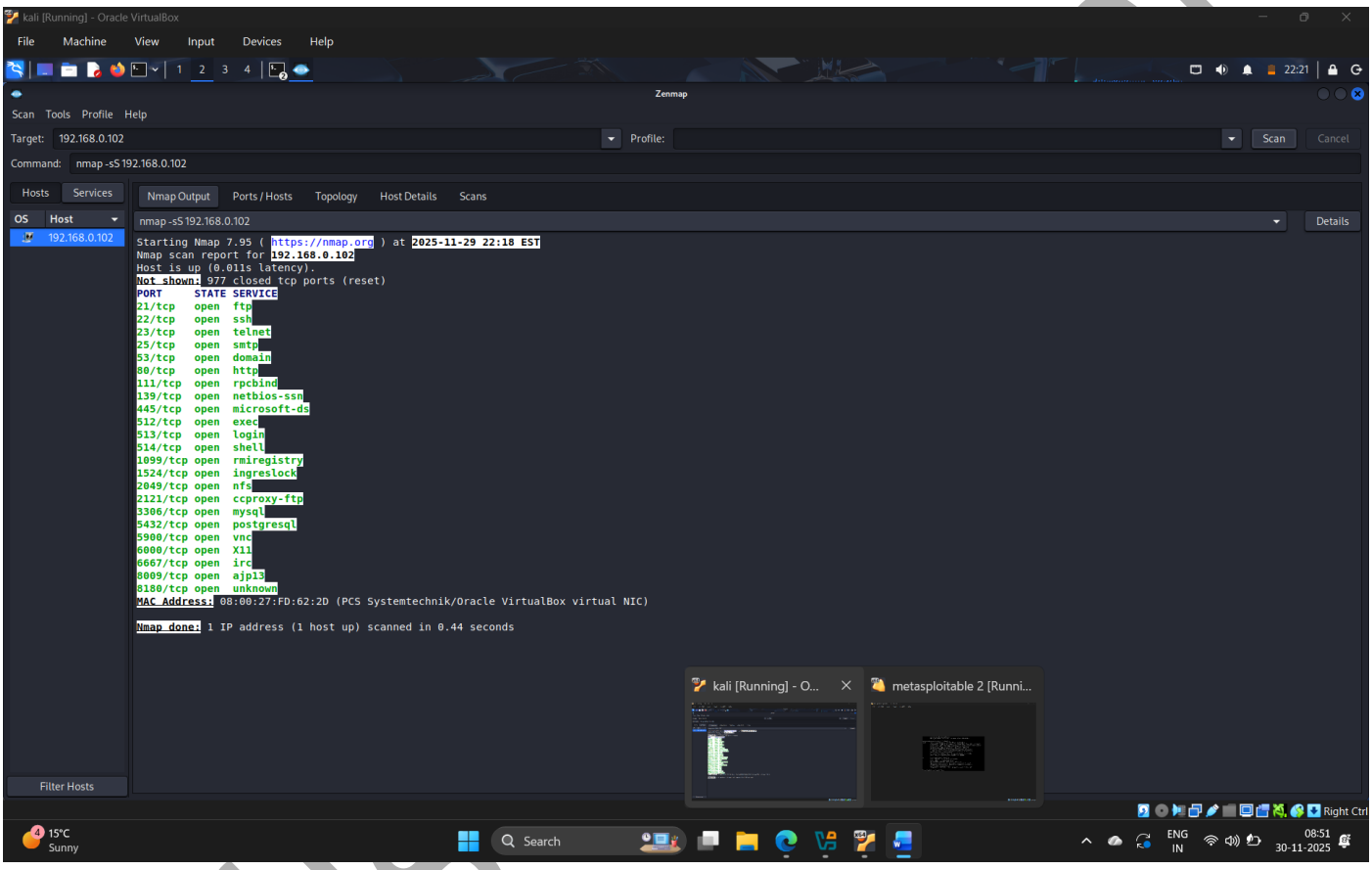
5. **Then click on the services running you can use any of these services and their open ports to enter into target network/host and establish a connection :**



2.5

3.perform stealth scan/TCP half open scan :

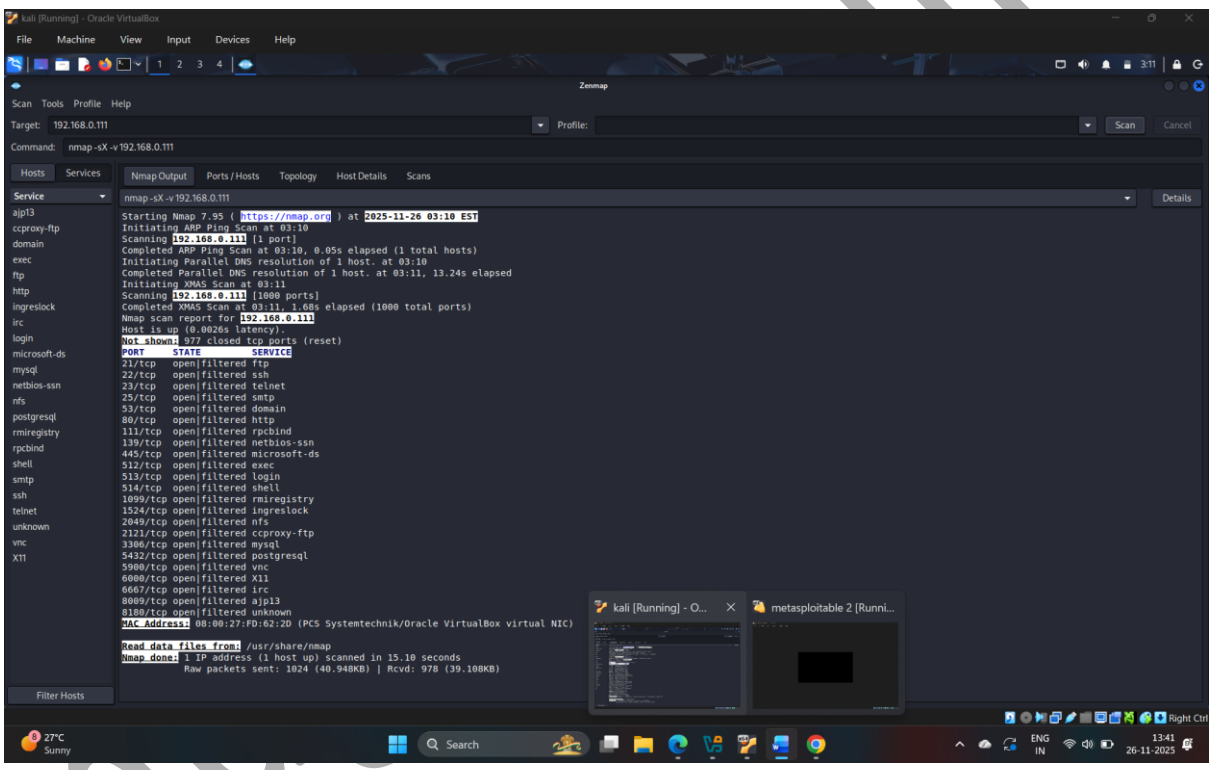
- **-sS : the stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three way handshake signals and hence leaving the connection half open this scanning technique can be used to bypass firewall rules. logging mechanism,and hide under network traffic**



3.1

4.perform Xmas scan :

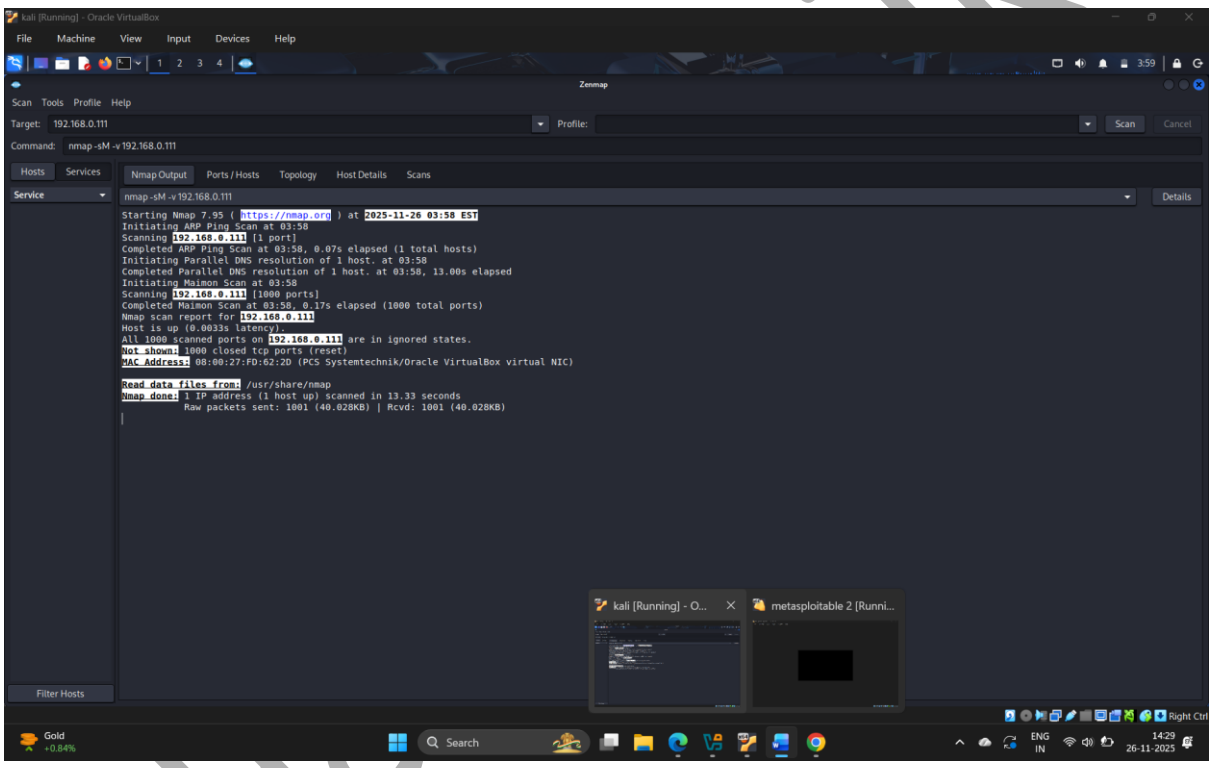
- **-sX : xmas scan sends a TCP frame to a target system with FIN<URG and PUSH flags set. If the target has opened the port then you will receive no response from the target system .If the target has closed the port then you will receive a target system reply with an RST. The scan result appear displaying 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**



4.1

5.TCP Maimon scan :

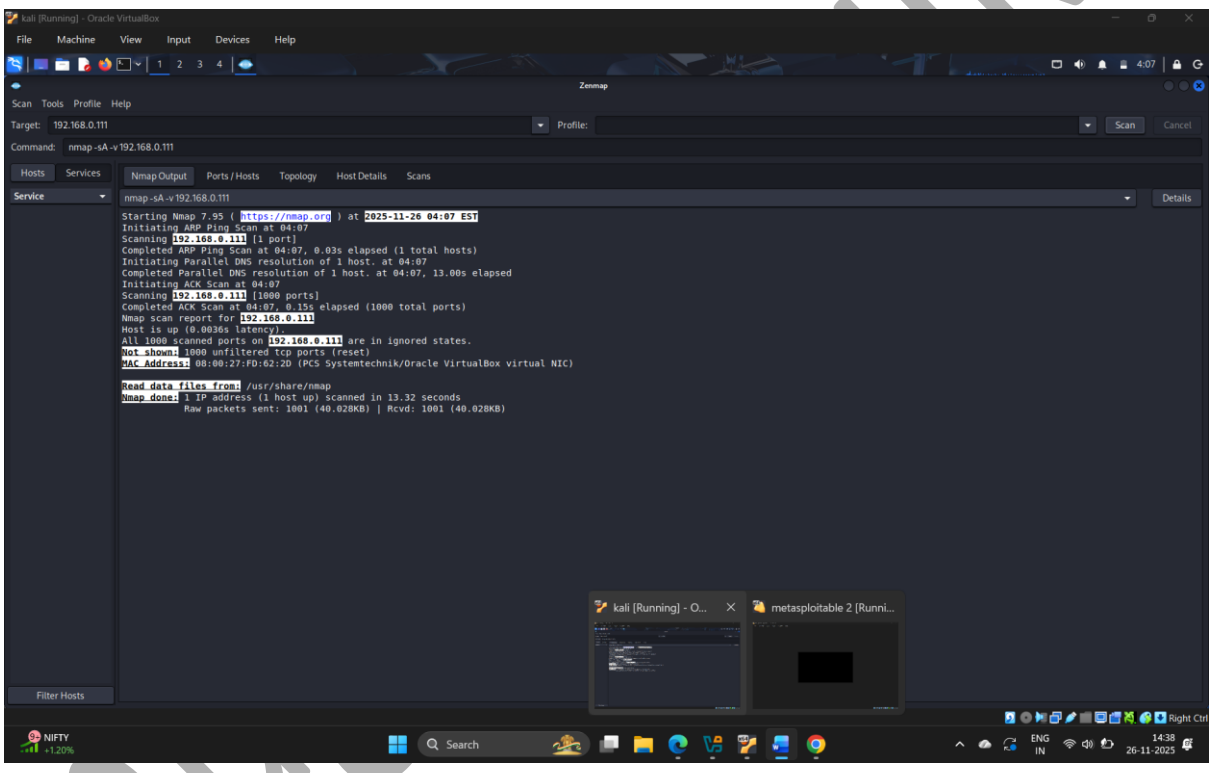
- **-sM : In the TCP mainon scan a FIN/ACK probe is sent to the target if there is no response then the port is open/filtered but if the RST packet is sent as a response then the port is closed it displays either the ports are open/filtered on the target machine which means a firewall has been configured on the target machine. In this result we get RST flag which means all ports are closed**



5.1

6.perform ACK flag probe :

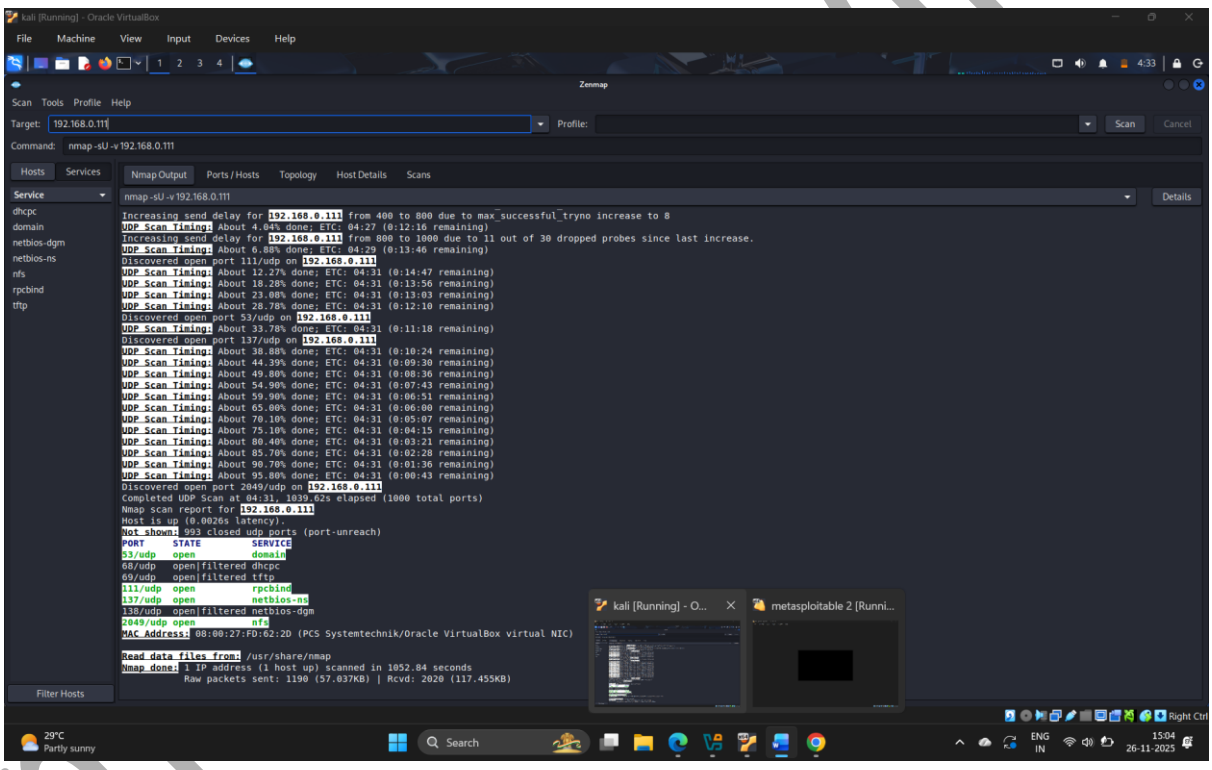
- **-sA : The ACK flag probe scan send ACK probe packet with a random sequence number no response implies that the port is filtered(stateful firewall is present)and an RST response means that the port is not filtered.This scan displays that the ports are filtered on the target machine as shown in the screenshot.In this result we gt RST flag which means port id not filtered**



6.1

7.perform UDP scan :

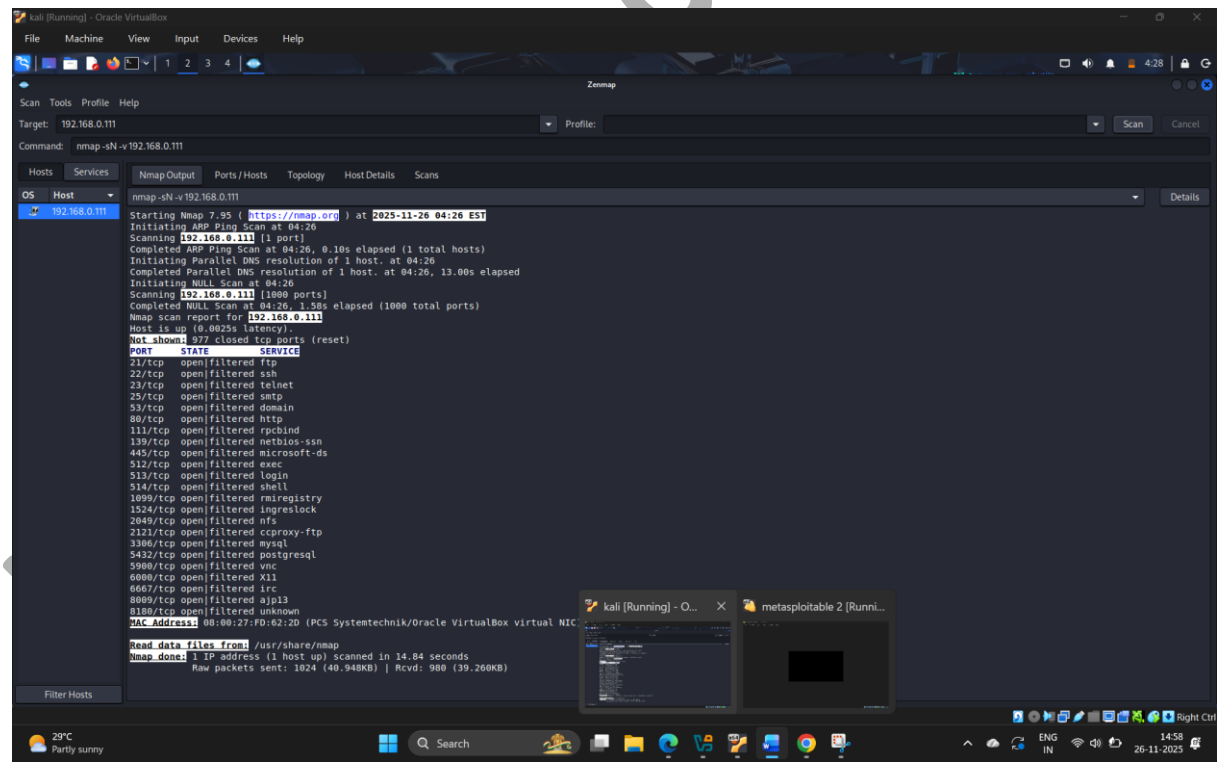
- **-sU : The UDP scan uses UDP protocol instead of the TCP.There is no three way handshake for the UDP scan.it sends UDP packets to the target host no response means that that thr port is open.If the port is closed and ICMP port unreachable message is received.Here we get the result as port unreachable means port is closed.**



7.1

8.perform Null Scan :

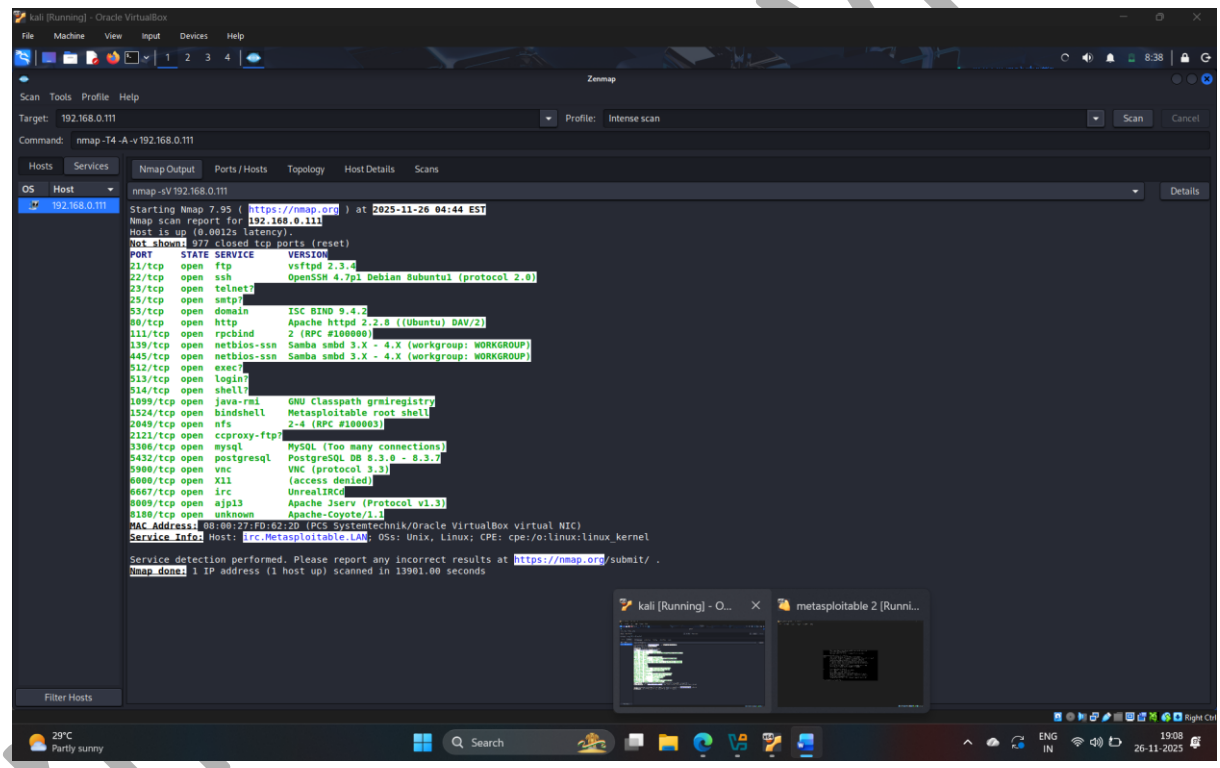
- **-sN : A NULL scan in Zenmap/Nmap is a special type of TCP scan used mainly in ethical hacking and penetration testing to bypass firewalls or IDS and to map open/closed ports without sending normal TCP flags.**
- **If the port is closed → target replies with RST**
- **If the port is open → no response**
- **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**



8.1

9.perform service version scan:

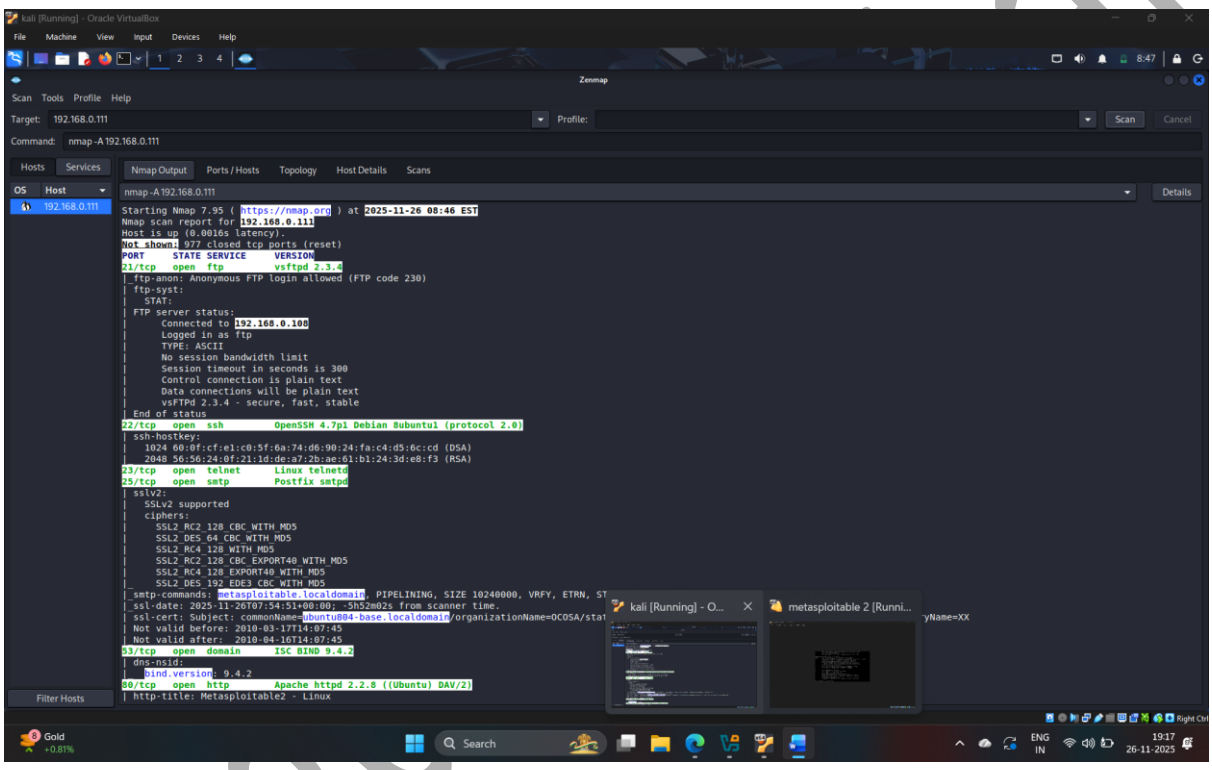
- **-sV : service version detection helps you to obtain information about the running services and their versions on a target system.obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.The scan result displays that the open ports and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



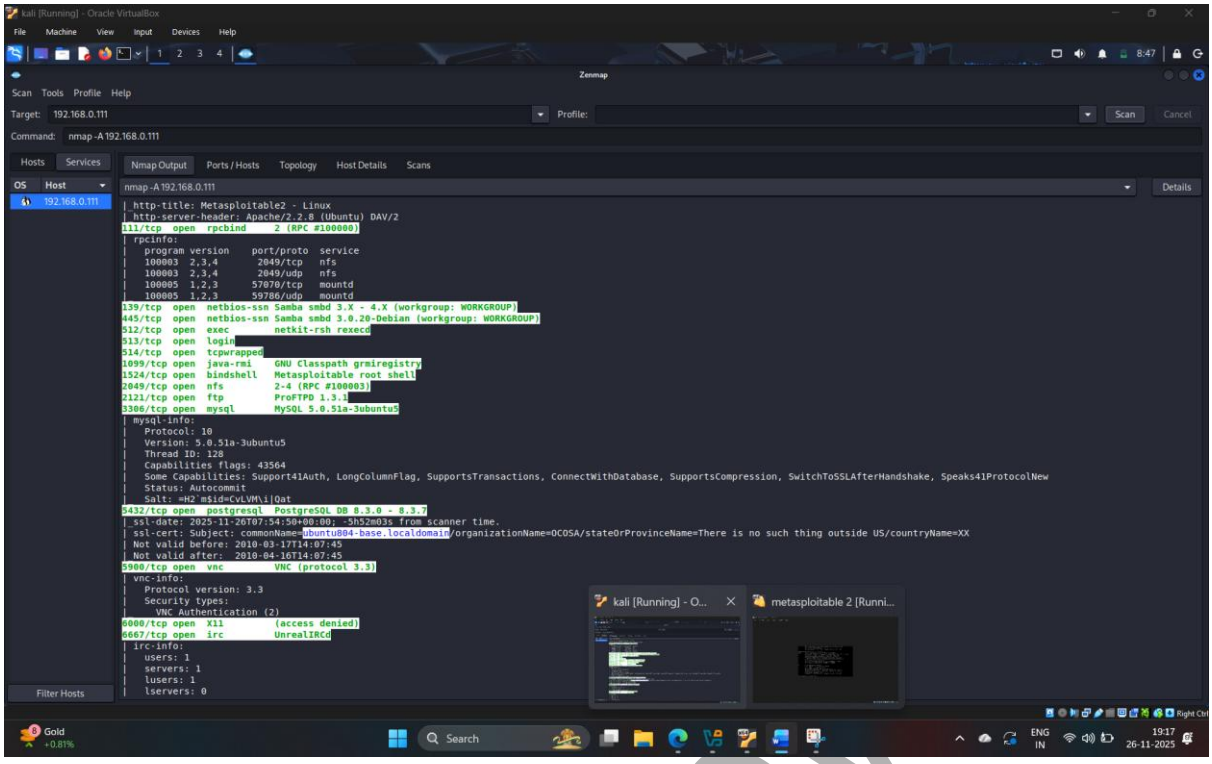
9.1

10.perform aggressive scan :

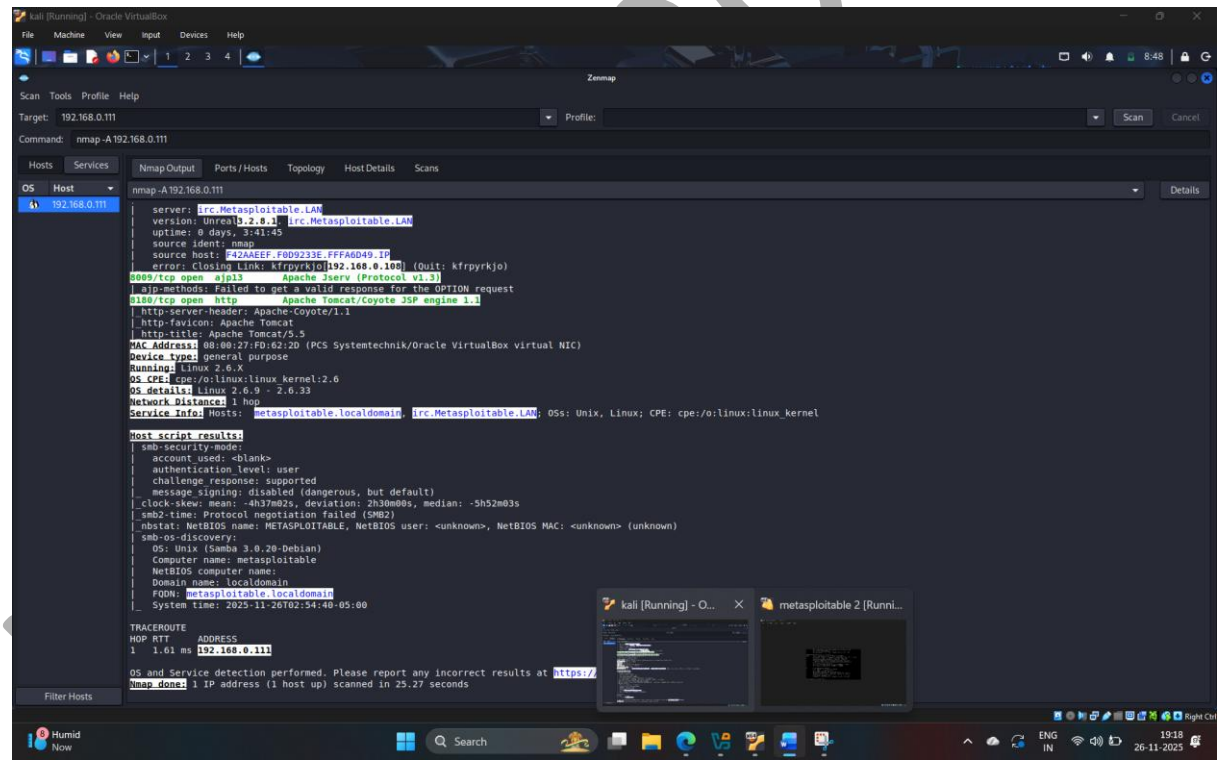
- **-A : It supports os detection,version scanning,script scanning,traceroute**



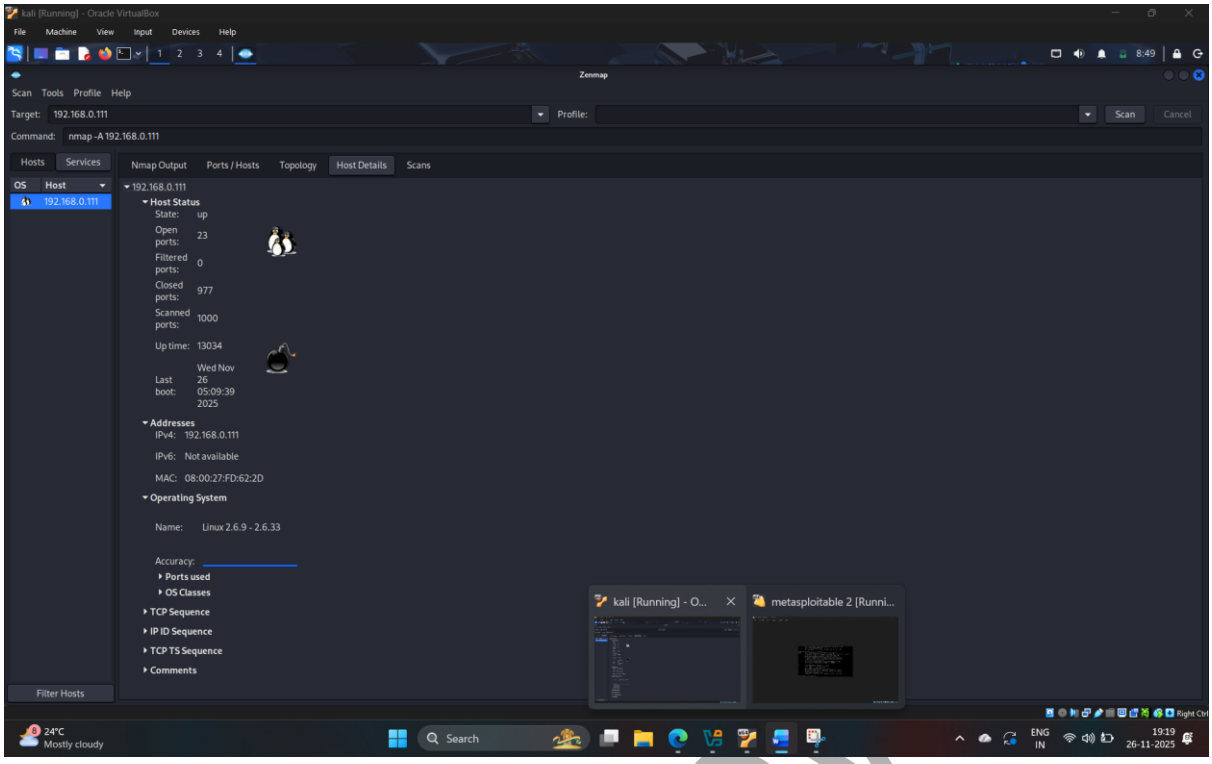
10.1


kali [Running] - Oracle VirtualBox
Zenmap
Target: 192.168.0.111
Command: nmap -A 192.168.0.111
Nmap Output
nmap -A 192.168.0.111
| http-title: Metasploitable2 - Linux
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 57070/tcp mountd
| 100005 1,2,3 59786/udp mountd
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell 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 ID: 128
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41ProtocolNew
| Status: Autocommit
| Salt: =H2`#5id<CvLVM\i]Qat
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-date: 2025-11-26T07:54:50+00:00; -5h52m03s from scanner time.
| 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
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)
6667/tcp open irc UnrealIRCd
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
Filter Hosts
kali [Running] - O...
metasploitable 2 [Runni...
Gold +0.81%
Search
ENG IN
19:17 26-11-2025

10.2


kali [Running] - Oracle VirtualBox
Zenmap
Target: 192.168.0.111
Command: nmap -A 192.168.0.111
Nmap Output
nmap -A 192.168.0.111
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 3:41:45
| source ident: nmap
| source host: F42AAEEF.F0D9233E.FFFA6D49.IP
| error: Closing Link: kfrpyrkjo[192.168.0.108] (Quit: kfrpyrkjo)
8009/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-server-header: Apache-Coyote/1.1
| http-favicon: Apache Tomcat
| http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:FD:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -4h37m02s, deviation: 2h30m00s, median: -5h52m03s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-11-26T02:54:40-05:00
TRACEROUTE
HOP RTT ADDRESS
1 1.61 ms 192.168.0.111
OS and Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 25.27 seconds
Filter Hosts
kali [Running] - O...
metasploitable 2 [Runni...
Humid Now
Search
ENG IN
19:18 26-11-2025

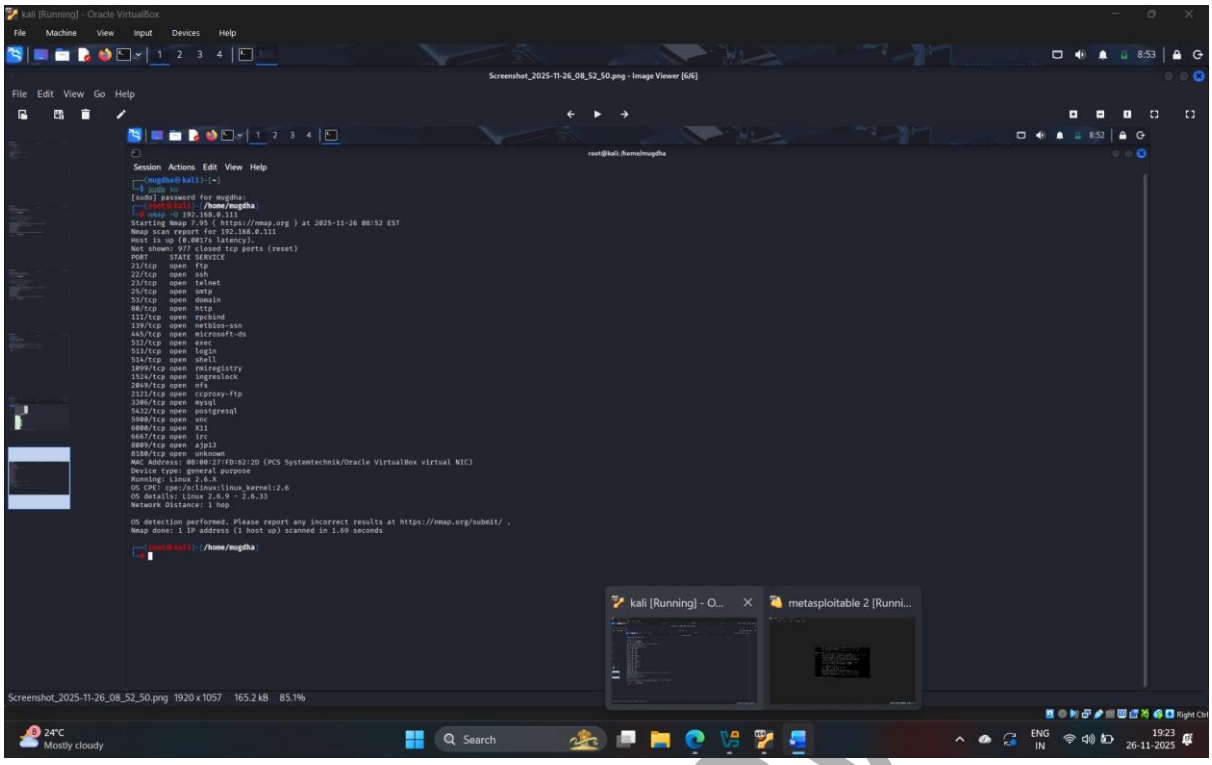
10.3



10.4

11 . Perform OS discovery :

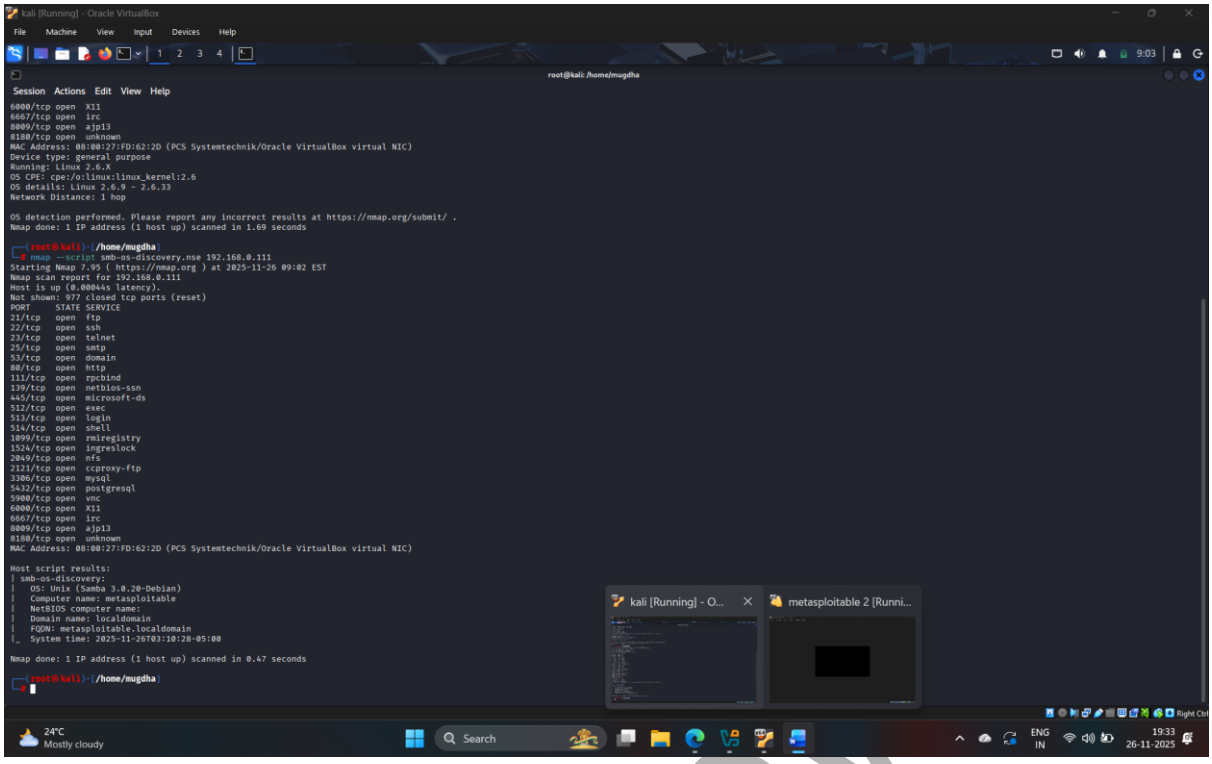
- **-O : Scan result displays information about open ports and services running on those ports,operating system of target machine**



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)**



12.1

13.Evasion of firewall :

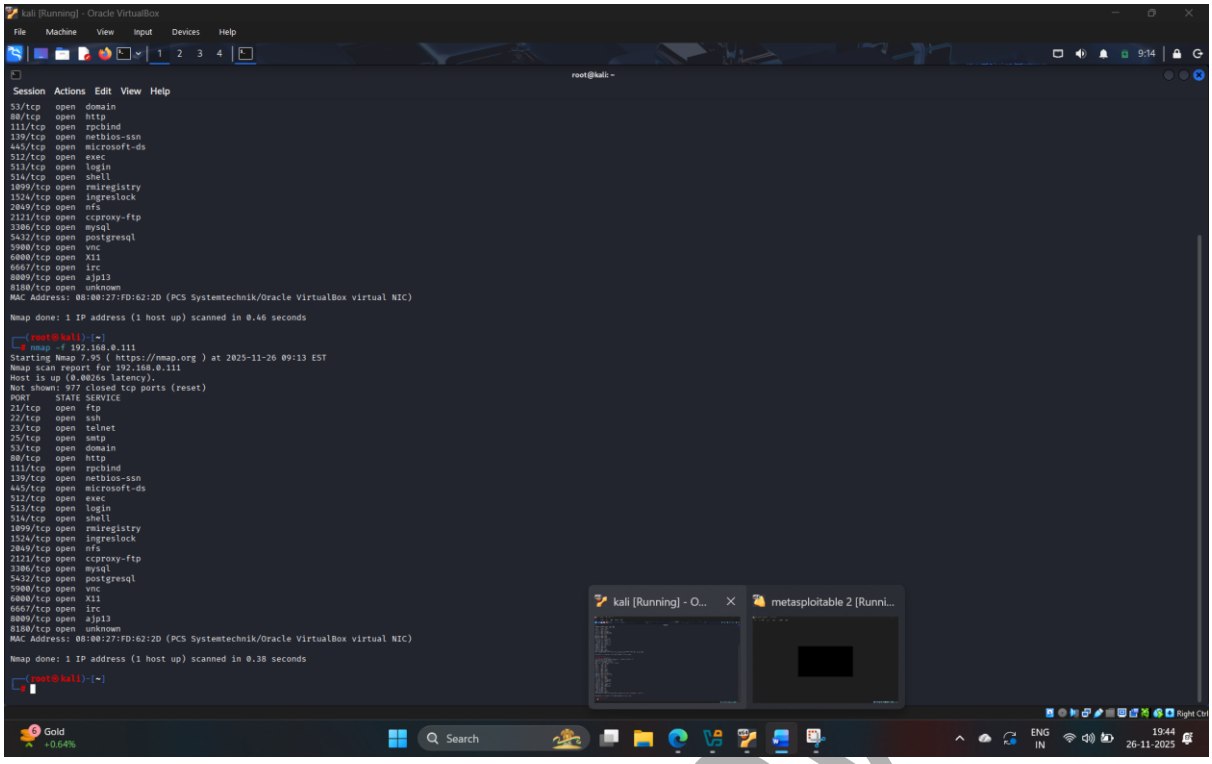
- **Nmap offersmany features to help understand complex networks with enabled securityand supports mechanisms for bypassing poorly implemented defenses.using nmap**

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

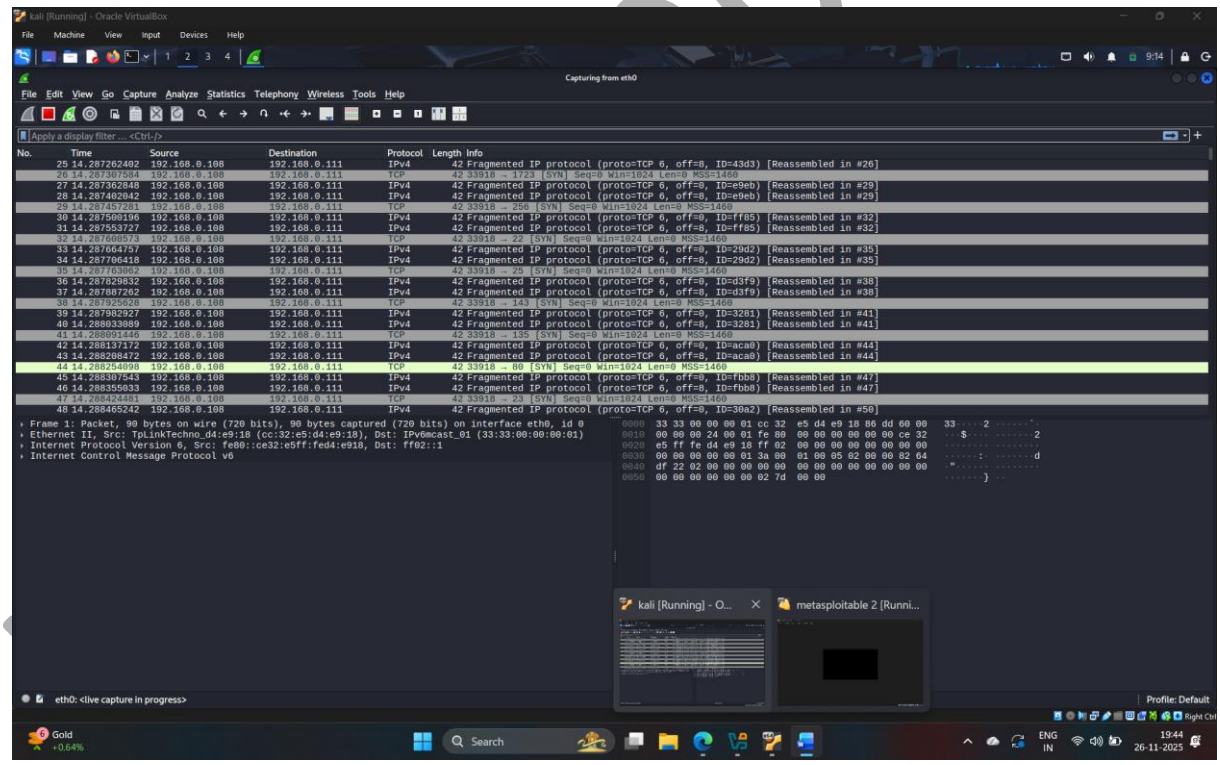
- **Here are some techniques :**

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.**


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: ~
Session Actions Edit View Help
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 0.46 seconds
(root@kali)-[~]
nmap -A 192.168.0.111
Starting Nmap 7.95 (https://nmap.org) at 2025-11-26 09:13 EST
Nmap scan report for 192.168.0.111
Host is up (0.0026s 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 0.38 seconds
(root@kali)-[~]
kali [Running] - O...
metasploitable 2 [Runni...
Gold +0.64%
Search
ENG IN
19:44 26-11-2025

13.1.1

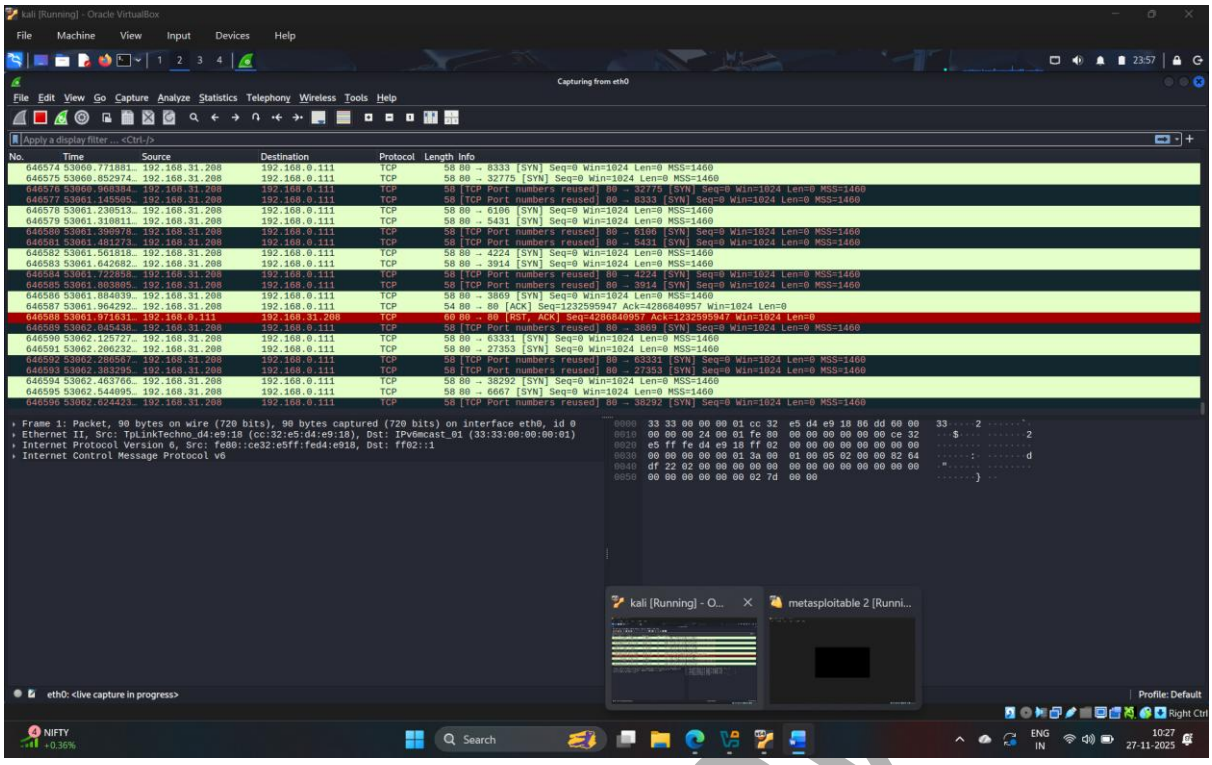

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
25 14.287262402 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=43d3) [Reassembled in #26]
26 14.287303214 192.168.0.108 192.168.0.111 TCP 42 33911 → 1024 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27 14.287362848 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=e9eb) [Reassembled in #29]
28 14.287402042 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=e9eb) [Reassembled in #29]
29 14.287457281 192.168.0.108 192.168.0.111 TCP 42 33918 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30 14.287500196 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=ff05) [Reassembled in #32]
31 14.287553727 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=ff05) [Reassembled in #32]
32 14.287608573 192.168.0.108 192.168.0.111 TCP 42 33918 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33 14.287664757 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=29d2) [Reassembled in #35]
34 14.287706418 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=29d2) [Reassembled in #35]
35 14.287761019 192.168.0.108 192.168.0.111 TCP 42 33911 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36 14.287829832 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=d3f9) [Reassembled in #38]
37 14.287887262 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=d3f9) [Reassembled in #38]
38 14.287925928 192.168.0.108 192.168.0.111 TCP 42 33918 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39 14.287982927 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=3281) [Reassembled in #41]
40 14.288033089 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=3281) [Reassembled in #41]
41 14.288091446 192.168.0.108 192.168.0.111 TCP 42 33918 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42 14.288137172 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=aca0) [Reassembled in #44]
43 14.288208472 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=aca0) [Reassembled in #44]
44 14.288254098 192.168.0.108 192.168.0.111 TCP 42 33918 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45 14.288307543 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=fbb8) [Reassembled in #47]
46 14.288355033 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=fbb8) [Reassembled in #47]
47 14.288407411 192.168.0.108 192.168.0.111 TCP 42 33911 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48 14.288465242 192.168.0.108 192.168.0.111 IPv4 42 Fragmented IP protocol (proto=TCP 6, off=8, ID=30a2) [Reassembled in #50]
Frame 1: Packet, 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
Ethernet II, Src: TpLinkTechno_d4:e9:18 (cc:32:e5:d4:e9:18), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::ce32:e5ff:fed4:e918, Dst: ff02::1
Internet Control Message Protocol v6
0000 33 33 00 00 00 01 cc 32 e5 d4 e9 18 86 dd 60 00
0010 00 00 00 24 00 01 fe 80 00 00 00 00 00 00 ce 32
0020 e5 ff fe d4 e9 18 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 01 3a 00 01 00 05 02 00 00 82 64
0040 df 22 02 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 02 7d 00 00
kali [Running] - O...
metasploitable 2 [Runni...
eth0: <live capture in progress>
Profile: Default
Gold +0.64%
Search
ENG IN
19:44 26-11-2025

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.**

13.2.1



13.2.2

3.maximum transmission unit:

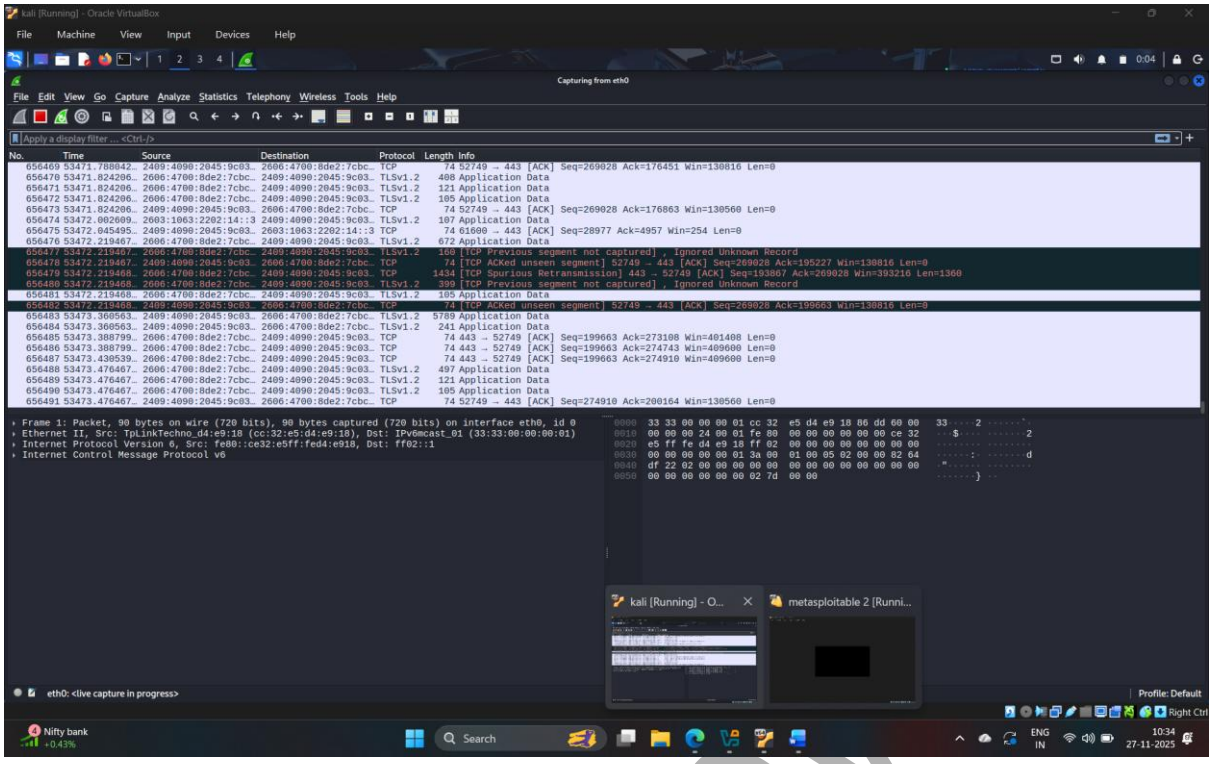
- **Using mtu smaller packets are transmitted instead of sending one complete packet at a time this technique evades the filtering and detection mechanism enables in the target machine**
- **-mtu : this specifies the numner of maximum transmission unit here 8 bytes of packet.**

```
┌──(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 :

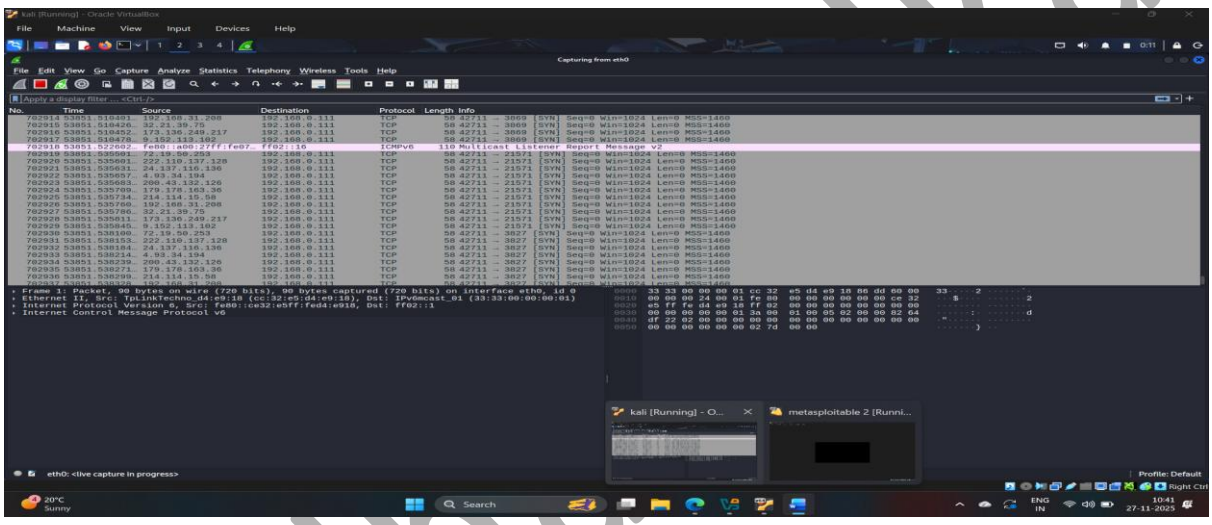
- **The ip address decoy techniquenreferss ti generating or manually specifying ip addresses of the decoys to evade IDS/firewall.**
- **This technique makes it difficult for the IDS/firewall to determine which ip address was actually scanning the network and which ip address were decoys**
- **By using 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(here10).**

```
┌──(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



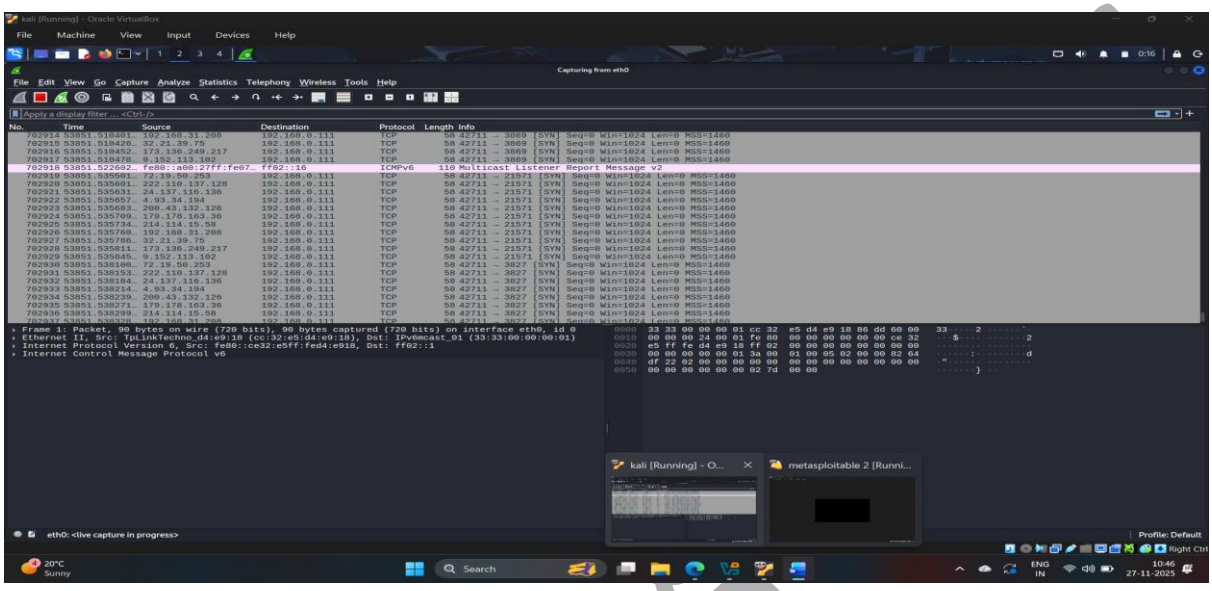
13.4.2

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.
```

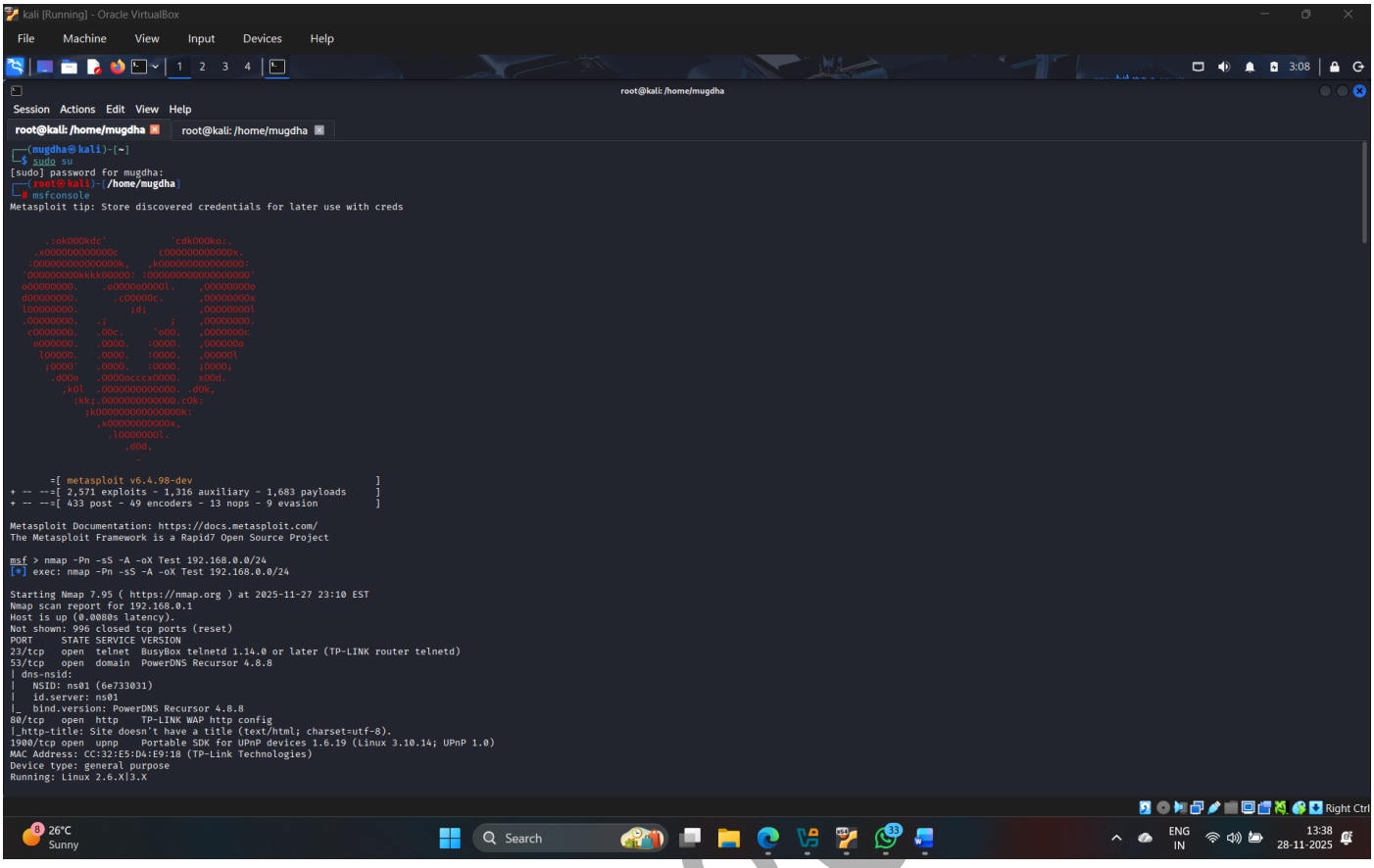
13.5.1



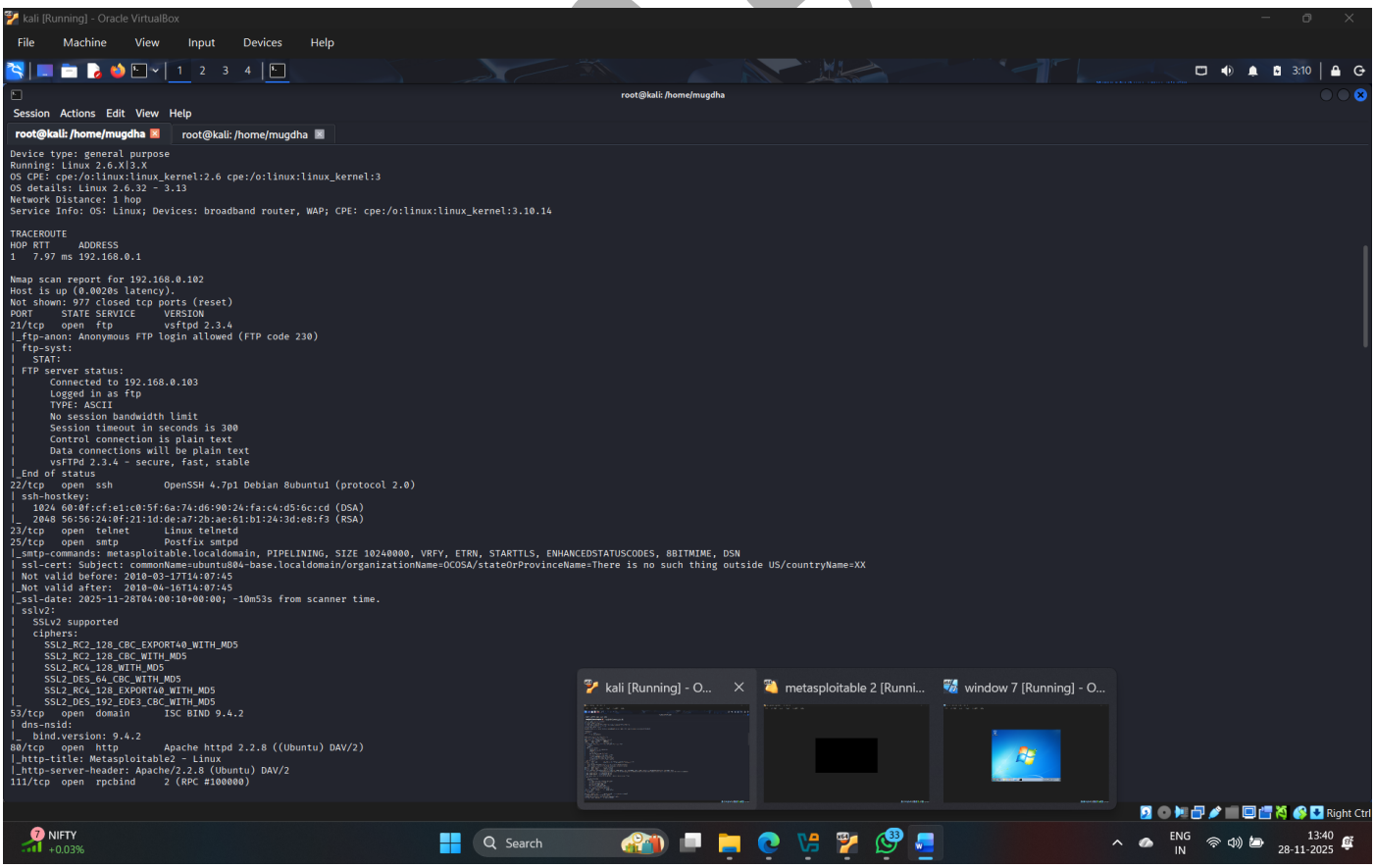
13.5.2

14.scan a target network using Metasploit :

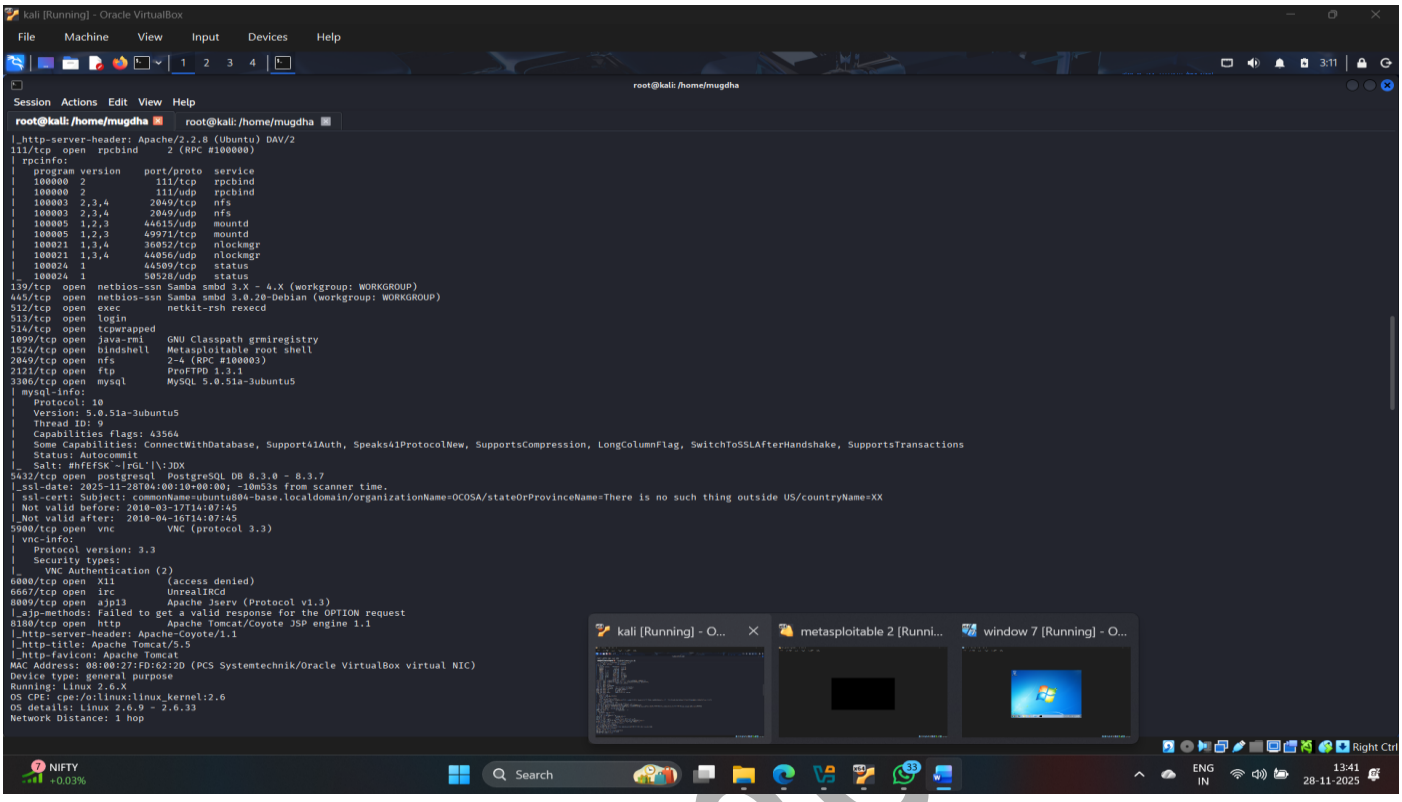
- **Metasploit framework is a tool that provides information about security vulnerabilities in the target organization system and aids in penetration testing and IDS signature development**
- **It facilitates the tasks of attackers exploit writers and payload writers**
- **A major advantage of the fra,ework 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, an 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
root@kali: /home/mugdha
Session Actions Edit View Help
root@kali: /home/mugdha
root@kali: /home/mugdha
(mugdha㉿kali)-[~]
$ sudo su
[sudo] password for mugdha:
(root㉿kali)-[/home/mugdha]
msfconsole
Metasploit tip: Store discovered credentials for later use with creds
=[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 -sS -A -oX Test 192.168.0.0/24
[*] 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 (0.0080s 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-nsid:
| NSID: ns01 (6e733031)
| id.server: ns01
|_ 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).
1900/tcp open upnp Portable SDK for UPnP devices 1.6.19 (Linux 3.10.14; UPnP 1.0)
MAC Address: CC:32:E5:D4:E9:18 (TP-Link Technologies)
Device type: general purpose
Running: Linux 2.6.X|3.X
26°C Sunny
Search
ENG IN
13:38 28-11-2025

14.1

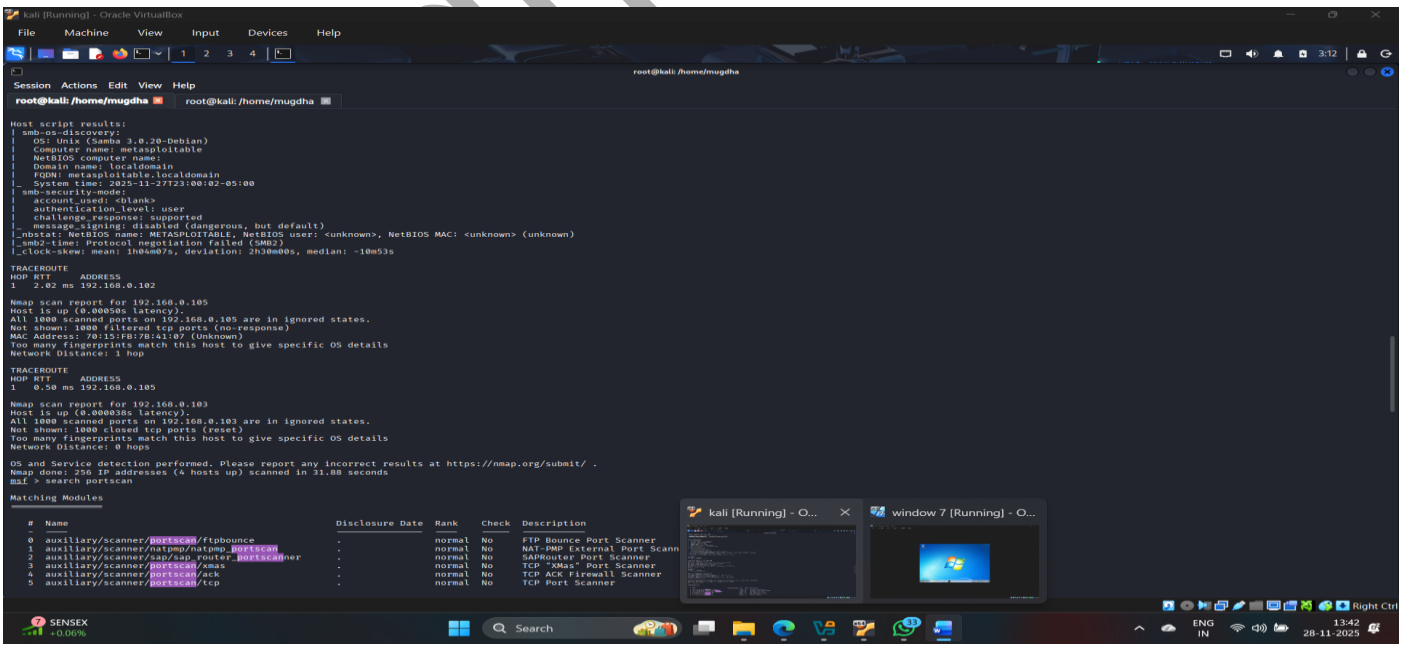

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/mugdha
Session Actions Edit View Help
root@kali: /home/mugdha
root@kali: /home/mugdha
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: 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 (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.0.103
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_smtp-commands: metasploitable.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: 2025-11-28T04:00:10+00:00; -10m53s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ 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)
kali [Running] - O...
metasploitable 2 [Runni...
window 7 [Running] - O...
NIFTY +0.03%
Search
ENG IN
13:40 28-11-2025

14.2



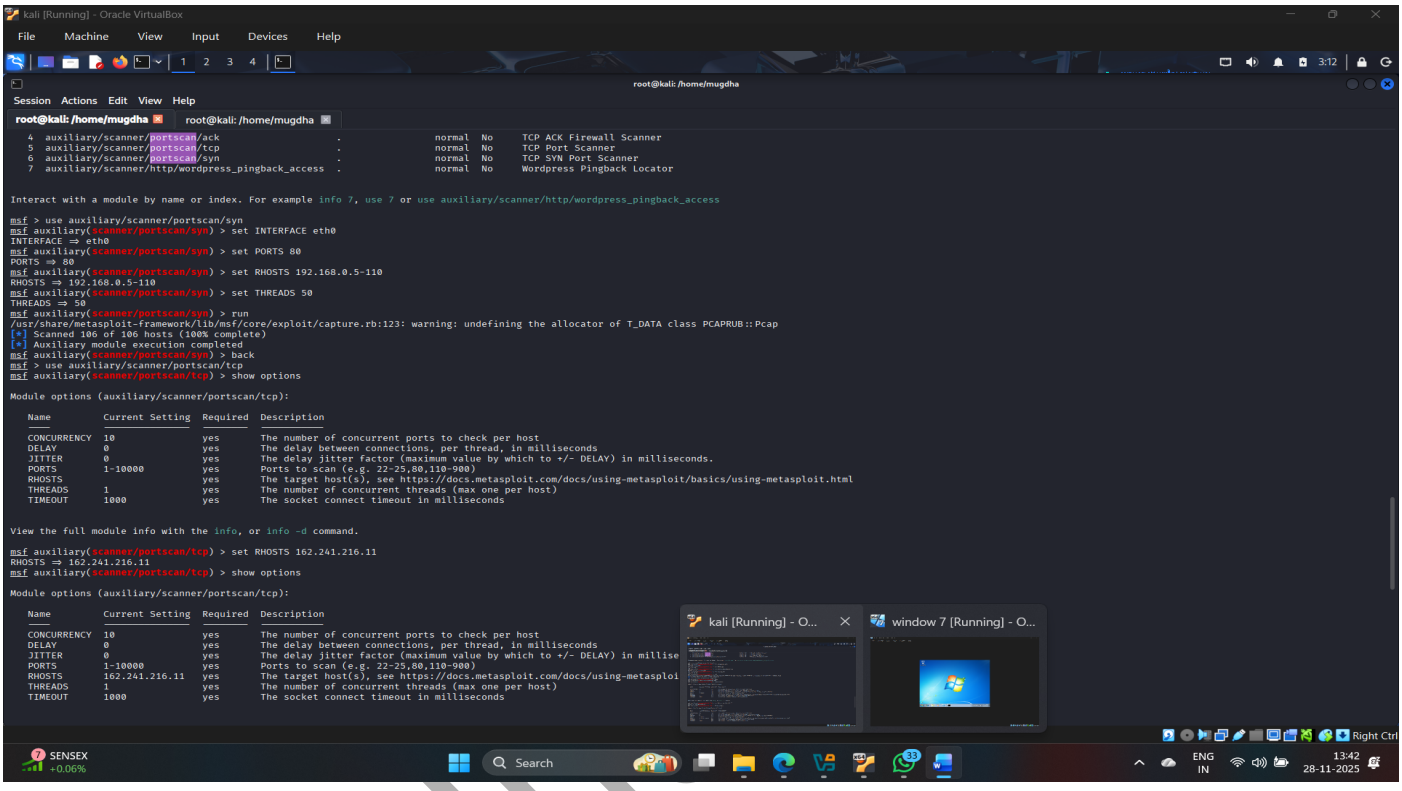
14.3

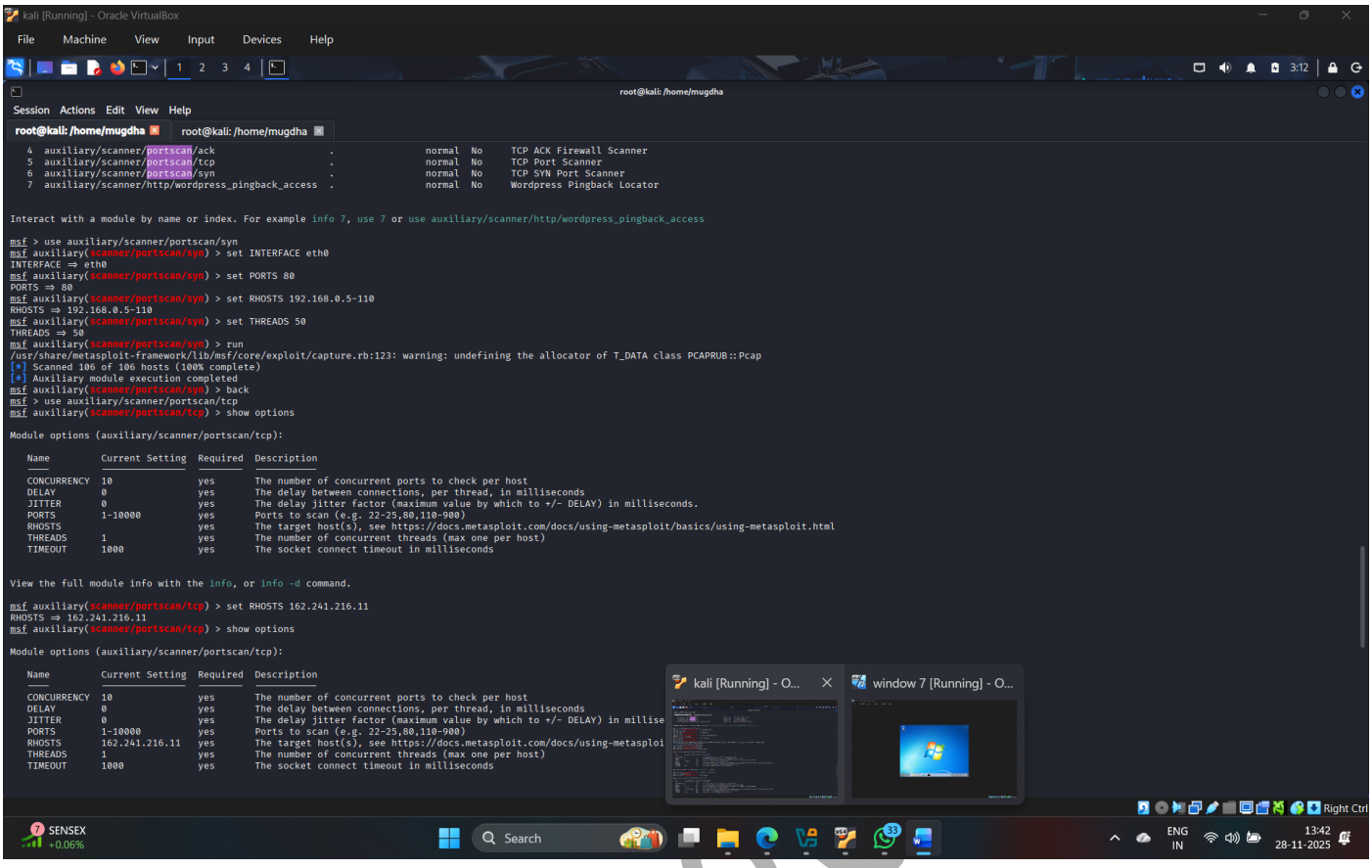
- **Type search portscan and press enter the etasploit port scanning modules apper as shown in the screenshot**



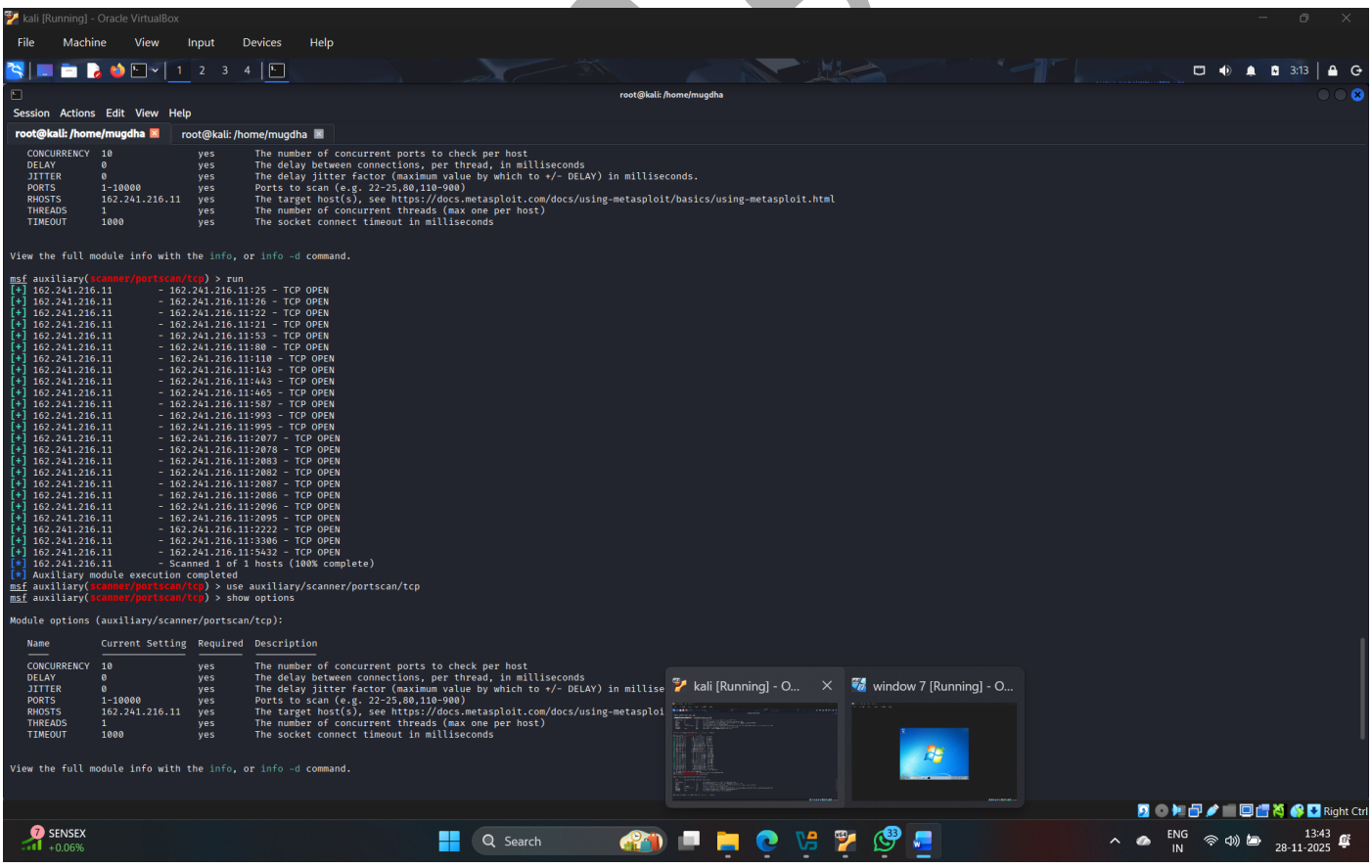
14.4

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

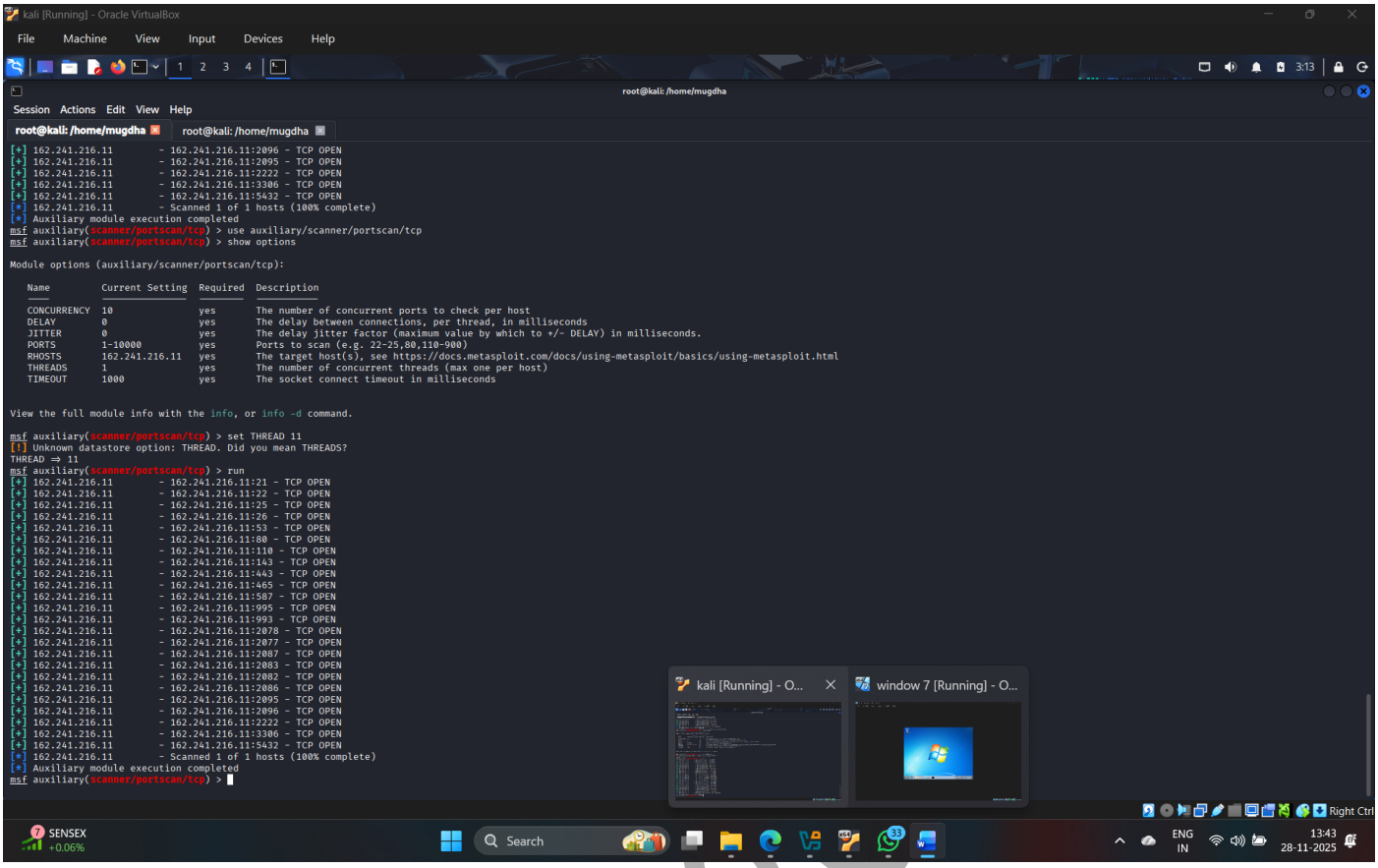



kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/mugdha
Session Actions Edit View Help
root@kali: /home/mugdha
root@kali: /home/mugdha
4 auxiliary/scanner/portscan/ack . normal No TCP ACK Firewall Scanner
5 auxiliary/scanner/portscan/tcp . normal No TCP Port Scanner
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 module execution completed
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 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 millise
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-metasploi
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 1000 yes The socket connect timeout in milliseconds
kali [Running] - O...
window 7 [Running] - O...
Right Ctrl
SENSEX +0.06%
Search
ENG IN
13:42 28-11-2025

14.5


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/mugdha
Session Actions Edit View Help
root@kali: /home/mugdha
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 - 162.241.216.11:53 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:80 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:110 - 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 - 162.241.216.11:995 - 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 - 162.241.216.11:2082 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:2087 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:2086 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:2096 - 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 - 162.241.216.11:3306 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:5432 - TCP OPEN
[*] 162.241.216.11 - Scanned 1 of 1 hosts (100% complete)
[*] 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 millise
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-metasploi
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.
kali [Running] - O...
window 7 [Running] - O...
Right Ctrl
SENSEX +0.06%
Search
ENG IN
13:43 28-11-2025

14.6


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/mugdha
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 - 162.241.216.11:2095 - 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)
[*] 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.
msf auxiliary(scanner/portscan/tcp) > set THREAD 11
[!] Unknown datastore option: THREAD. Did you mean THREADS?
THREAD => 11
msf auxiliary(scanner/portscan/tcp) > run
[+] 162.241.216.11 - 162.241.216.11:21 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:22 - 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 - 162.241.216.11:110 - 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 - 162.241.216.11:995 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:993 - 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 - 162.241.216.11:2082 - TCP OPEN
[+] 162.241.216.11 - 162.241.216.11:2086 - 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)
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) >
kali [Running] - O...
window 7 [Running] - O...
Right Ctrl
SENSEX +0.06%
Search
ENG IN
13:43 28-11-2025

14.6