

Mini project -2

Network scanning

Submitted by - Aditi Devi Prasad

Batch - August 2024

Date – 02/12/2024

Network scanning is a process of scanning the targeted network to find the active devices and IP address associated with these active devices, port numbers, and services on those port numbers so that we can define the loopholes across the particular network. This process is malicious.

Methodology:

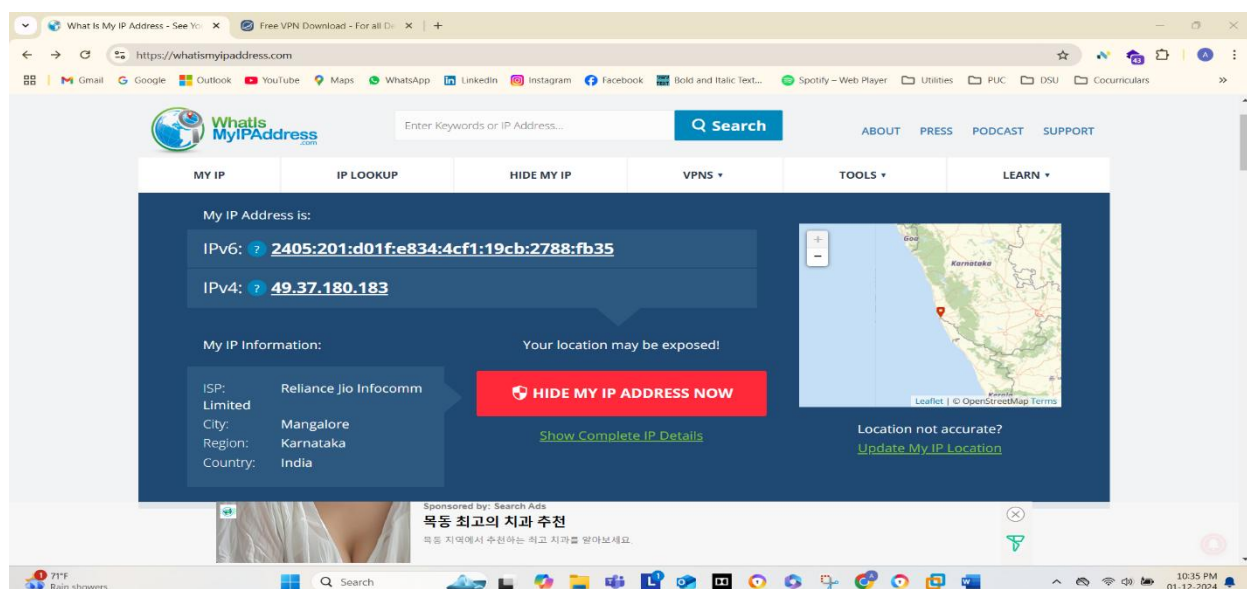
- Aiming the target.
- Scan their IP range of addresses.
- Scan their Open ports.
- Check the services running on open ports.
- Find the service versions of open ports.
- Check the operating system of the target.
- Bypass the security devices.
- Choose the right type of scan.

Types of network scan:

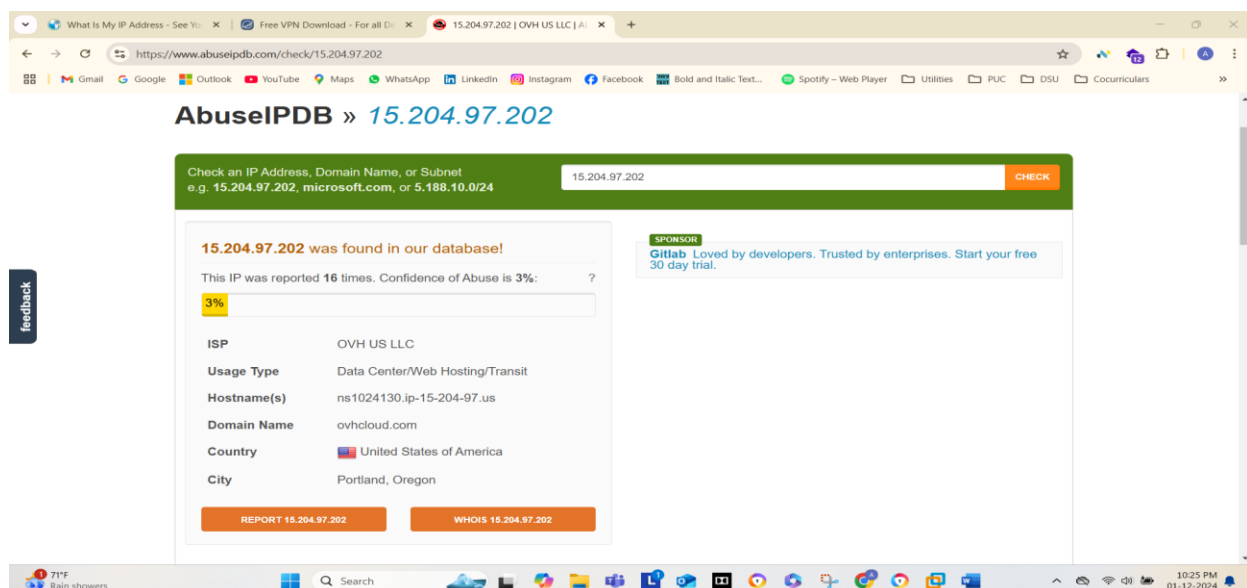
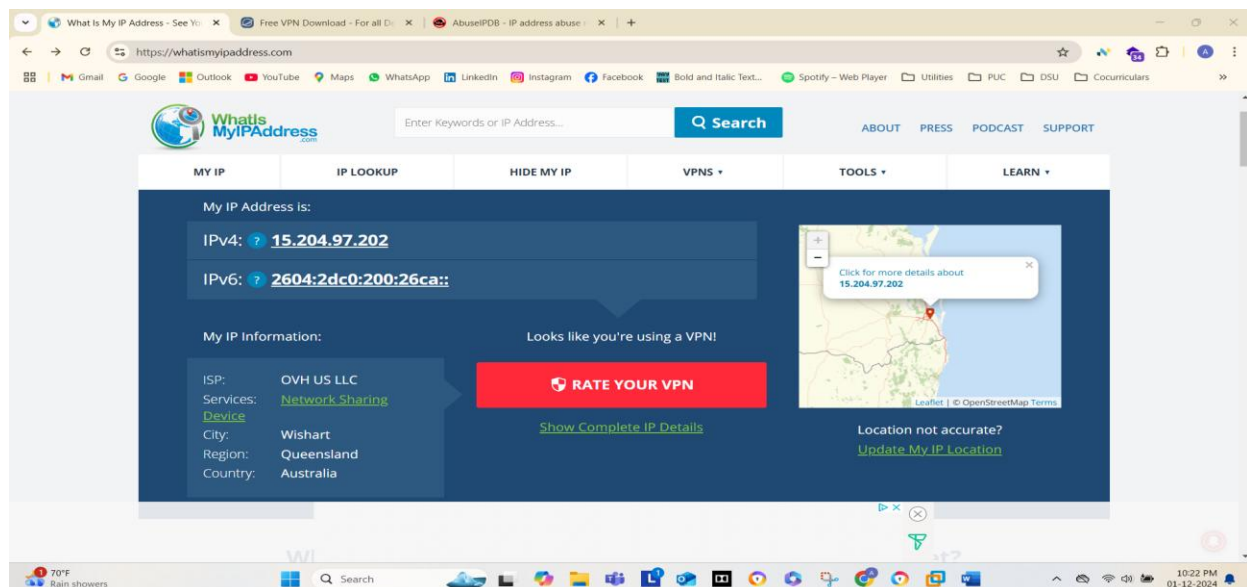
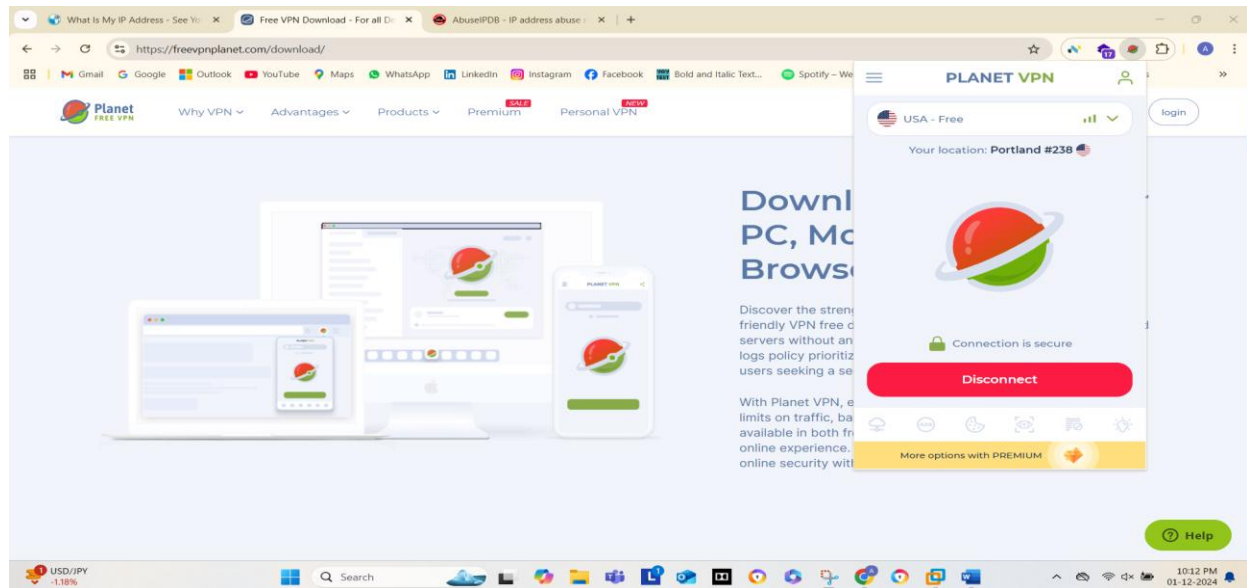
- TCP scan – by ‘-sT’
- UDP scan – by ‘-sU’
- Syn scan (stealth scan) – by ‘-sS’
- XMas and IDLE scan – by ‘-SX’ and ‘-SI’

Firstly, we have to become anonymous before performing all these. This can be achieved by two methods for wireless networks.

1. By VPN – not the best way as there is a chance of DNS data leakage.
My IP address:



My IP after using VPN:



2. By Proxychains: This is the safest method as it uses proxy DNS servers itself. We are using only one proxy here and activate the TOR.

Free Proxy List [1000+ IPs] X

https://geonode.com/free-proxy-list

Black Friday offer: Get 10 GB Premium Proxies for \$1

Filters

Country: Germany X

Port: 159.69.43.215 22139 75.119.150.125 13096 91198.137.31 3587 144.91.89.245 1981 139.162.182.54 11127 138.201.248.43 31043 46.4.73.88 80

Anonymity

☐ Elite (HIA)

☐ Anonymous (ANM)

☐ Transparent (NOA)

Proxy protocol

☐ HTTP

☐ HTTPS

☐ SOCKS4

☒ SOCKS5

Speed

☐ Fast

☐ Medium

IP ADDRESS	PORT	COUNTRY	PROTOCOLS	ANONYMITY	ORG & ASN	SPEED	UPTIME	RESPONSE	GOOGLE	LI
159.69.43.215	22139	DE	SOCKS5	Elite (HIA)	AS24940 Hetzner	1ms	100%	1506ms	X	11
75.119.150.125	13096	DE	SOCKS5	Elite (HIA)	AS51167 Contabo	1ms	99%	1067ms	X	11
91198.137.31	3587	DE	SOCKS5	Elite (HIA)	AS42927 Adrian Andreas Z	1ms	100%	1305ms	X	2
144.91.89.245	1981	DE	SOCKS5	Elite (HIA)	AS51167 Contabo GmbH	1ms	87%	484ms	X	9
139.162.182.54	11127	DE	SOCKS5	Elite (HIA)	AS63949 Linode, LLC	1ms	99%	5392ms	X	11
138.201.248.43	31043	DE	SOCKS5	Elite (HIA)	AS24940 Hetzner	1ms	95%	806ms	X	11
46.4.73.88	80	DE	SOCKS5	Elite (HIA)	AS24940 Hetzner	1ms	85%	5094ms	X	2

Kali 2024 x64 Customized by zSecurity v1.3 - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

Metasploit2-Linux

Kali 2024 x64 Customized by zSecurity v1.3

Dec 1 11:18

root@kali: /etc

```
GNU nano 0.1
# Whenever I connect to the new given destinations.
# Whenever I connect to 1.1.1.1 on port 1234 actually connect to 1.1.1.2 on port 443
# dnat 1.1.1.1:1234 1.1.1.2:443
# Whenever I connect to 1.1.1.1 on port 443 actually connect to 1.1.1.2 on port 443
# dnat 1.1.1.1:443 1.1.1.2:443
# No matter what port I connect to on 1.1.1.1 port actually connect to 1.1.1.2 on port 443
# dnat 1.1.1.1 1.1.1.2:443
# Always, instead of connecting to 1.1.1.1, connect to 1.1.1.2
# dnat 1.1.1.1 1.1.1.2

# Proxylist format
# type ip port [user pass]
# (values separated by 'tab' or 'blank')
# only numeric ipv4 addresses are valid

# Examples:
# socks5 192.168.87.78 1880 lamer secret
# http 192.168.89.3 8080 justu hidden
# socks4 192.168.2.49 1880
# http 192.168.39.93 8080

# proxy types: http, socks4, socks5, raw
# raw: The traffic is simply forwarded to the proxy without modification.
# (multitypes supported: "basic"-http "user/pass"-socks)

[proxylist]
# add proxy here ...
# example
# defaults set to "tor"
socks5 75.119.150.125 13096
```

Kali 2024 x64 Customized by zSecurity v1.3 - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

Metasploit2-Linux

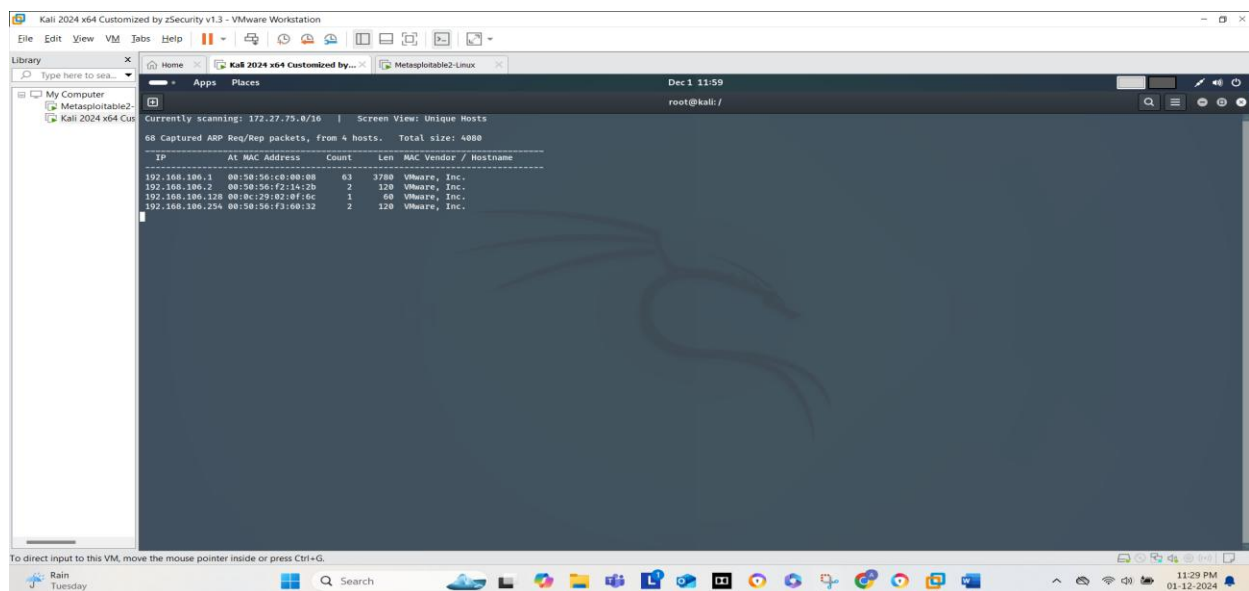
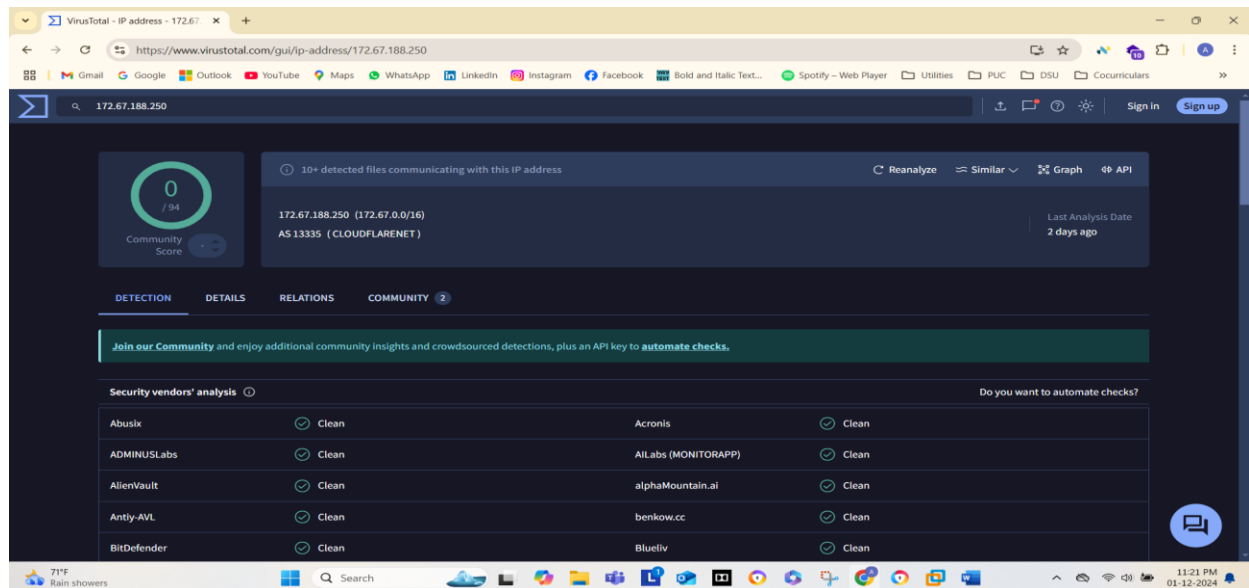
Kali 2024 x64 Customized by zSecurity v1.3

Dec 1 11:19

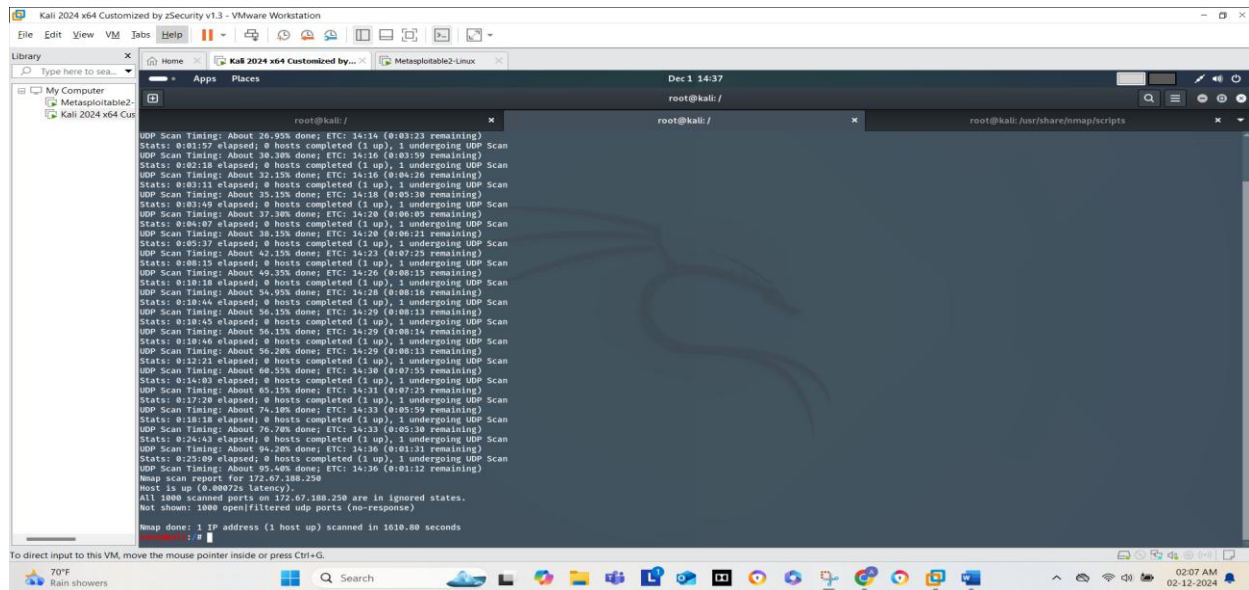
root@kali: /etc

```
After this operation, 26.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://zsecurity.org/custom-kali-sources kali-last-snapshot/main amd64 0.4.8.12-1 [2049 kB]
Get:2 https://zsecurity.org/custom-kali-sources kali-last-snapshot/main amd64 tor-geonode all 0.4.8.12-1 [2318 kB]
Get:3 https://zsecurity.org/custom-kali-sources kali-last-snapshot/main amd64 torsocks amd64 2.4.8-2 [74.4 kB]
Get:4 https://zsecurity.org/custom-kali-sources kali-last-snapshot/main amd64 torsocks amd64 2.4.8-2 [74.4 kB]
Selecting previously unselected package tor.
(Reading database ... 435596 files and directories currently installed.)
Preparing to unpack .../tor-geonode_0.4.8.12-1_all.deb ...
Unpacking tor-geonode (0.4.8.12-1) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.4.8-2_amd64.deb ...
Unpacking torsocks (2.4.8-2) ...
Setting up tor (0.4.8.12-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.4.8-2) ...
Setting up tor-geonode (0.4.8.12-1) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...
# tor.service - Anonymizing overlay network for TCP (multi-instance-master)
Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
Active: inactive (dead)
# tor.service - Anonymizing overlay network for TCP (multi-instance-master)
Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
Active: active (exited) since Sun 2024-12-01 11:17:08 CST; 9s ago
Invocation: a582a8f0d8a419e4e4b12edc18
Process: 3436 ExecStart=/bin/true (Code=exited, status=0/SUCCESS)
Main PID: 3436 (code=exited, status=0/SUCCESS)

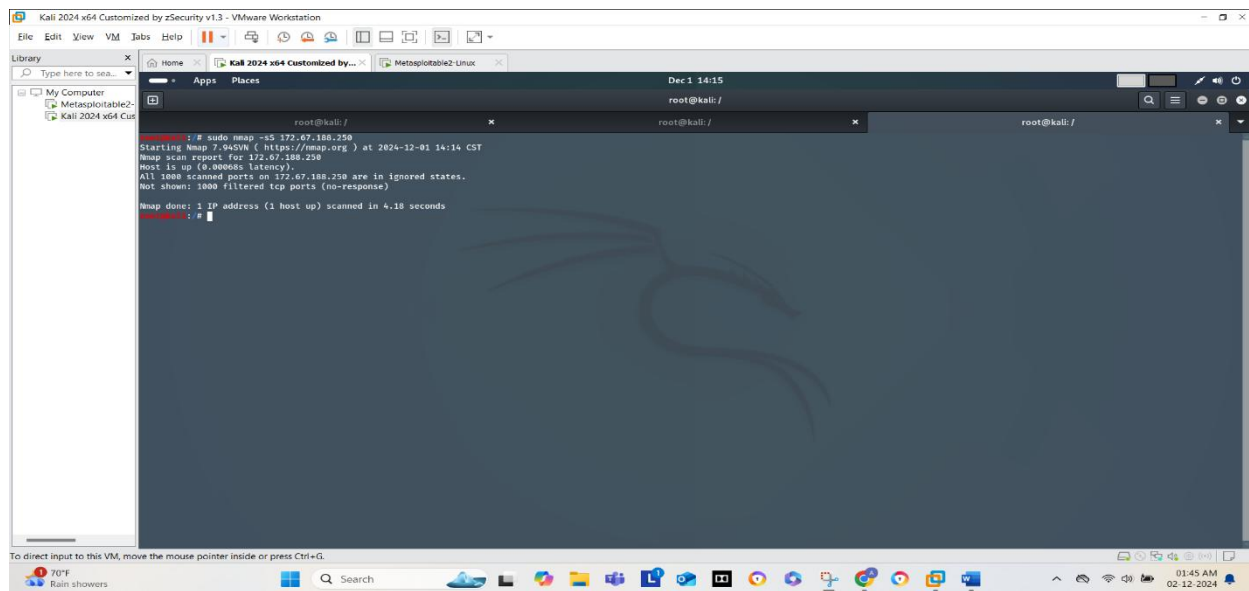
Dec 01 11:17:08 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
Dec 01 11:17:08 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).
# nano proxychains4.conf
```

2. We perform TCP scanning:
 - It is useful in finding the security devices and it is the best to use when there are no security devices.
 - It is connection-establishment protocol.
 - The Nmap for it is '-sT'.



4. We perform synchronous/stealth scanning:
 - This is also a type of TCP scan.
 - These type of scans uses the bypass security devices.
 - It doesn't establish the communication.



5. We find the vulnerability:

