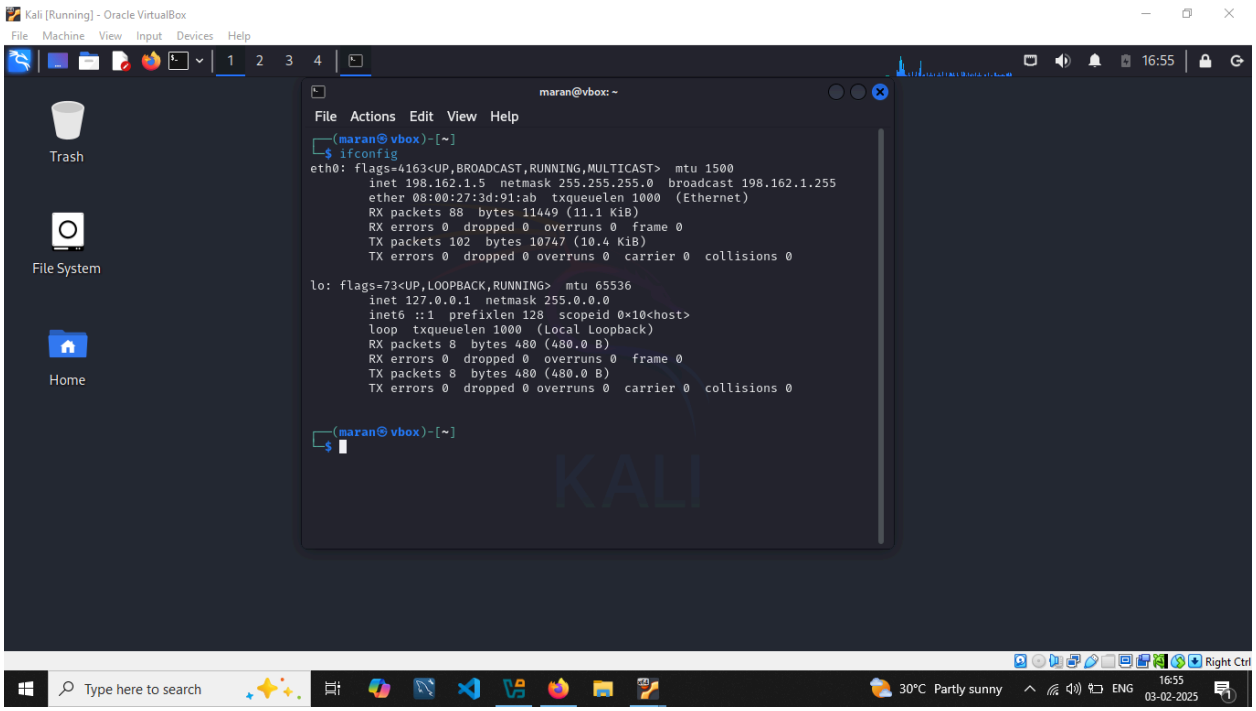
Week 3: Network scanning, Footprinting and Enumeration.

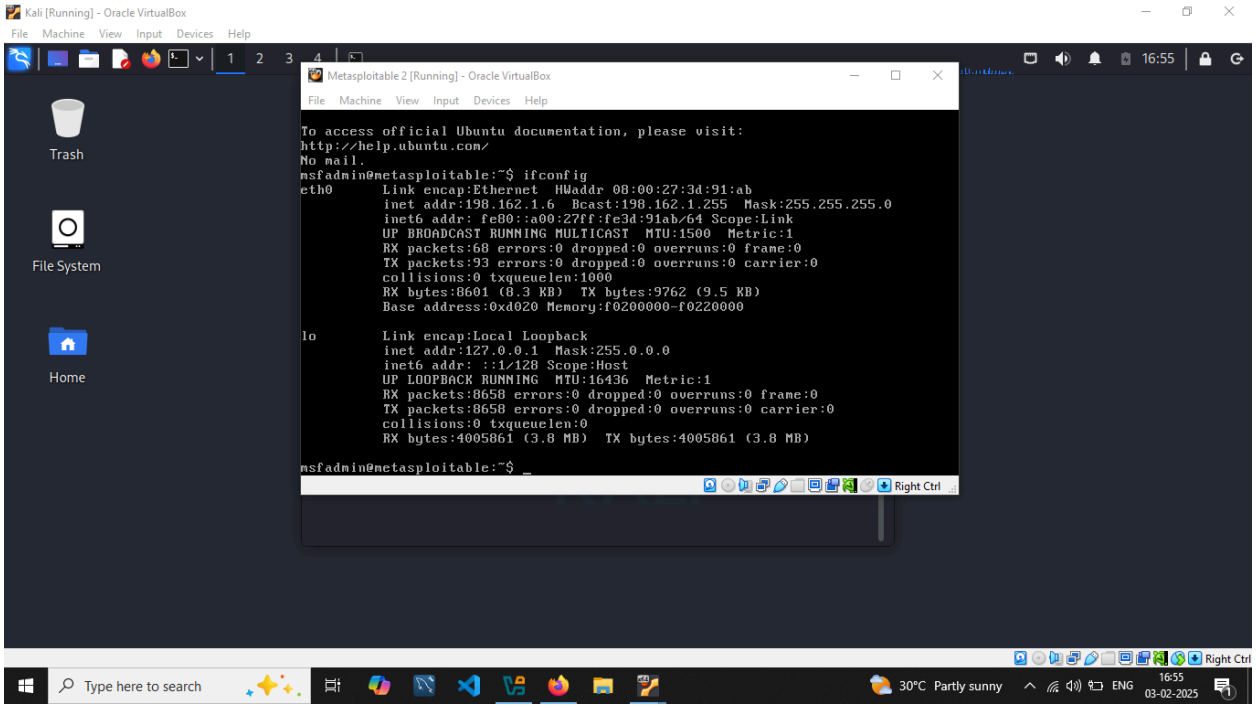
Name: Mathimaran M.S
Email: mathimaranms0@gmail.com

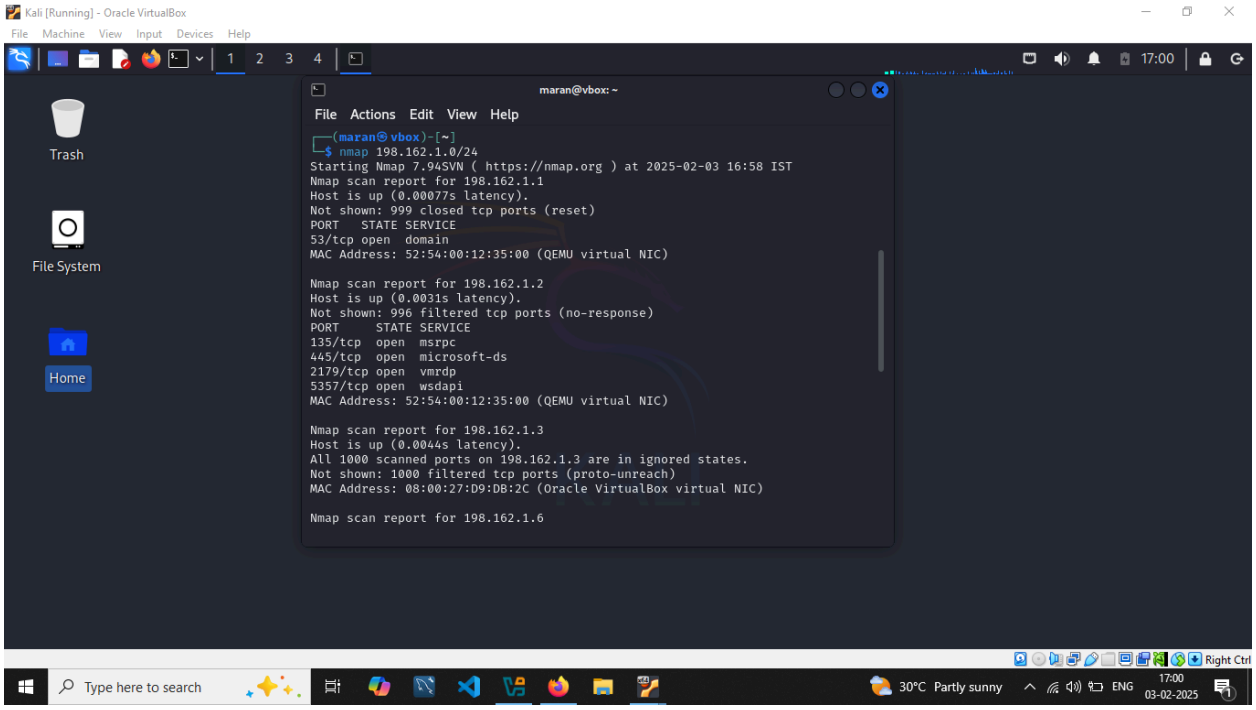
1. Identify Target IP Range:

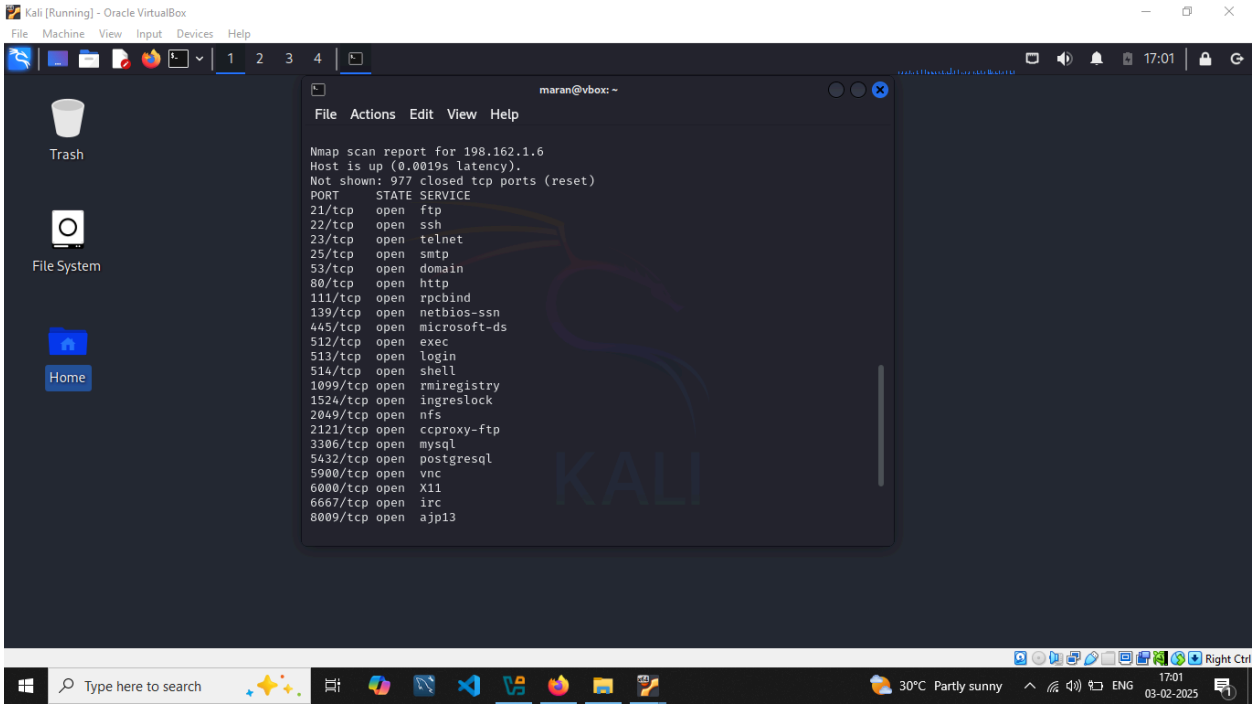
- Opening the terminal of kali linux and checking the ip address of the kali linux with the command `ifconfig`.
- Identified the ip address `198.162.1.5` of the kali linux which is the target ip range `198.162.1.0` to attack.
- The available 5 ip addresses from the target ip range are `198.162.1.1`, `198.162.1.2`, `198.162.1.3`, `198.162.1.6` and `198.162.1.5` (kali linux own ip address).

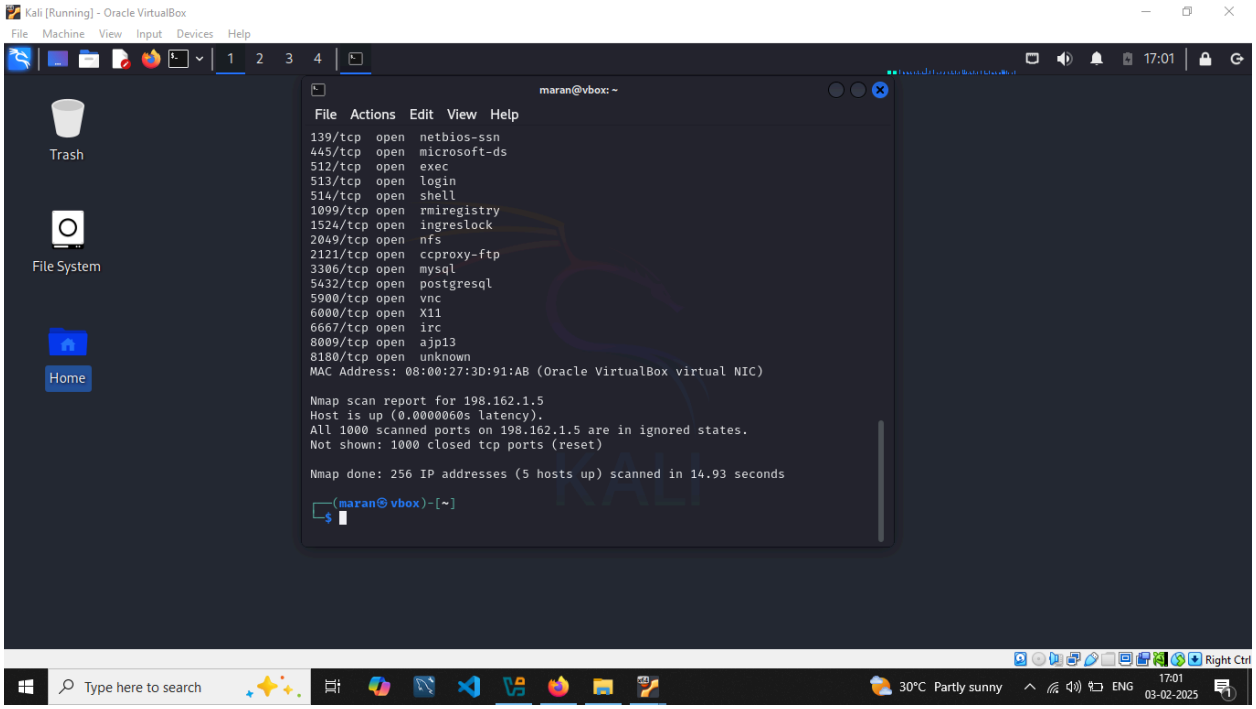
Screenshots:




Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:3d:91:ab
inet addr:198.162.1.6 Bcast:198.162.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe3d:91ab/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:68 errors:0 dropped:0 overruns:0 frame:0
TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:8601 (8.3 KB) TX bytes:9762 (9.5 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:8658 errors:0 dropped:0 overruns:0 frame:0
TX packets:8658 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:4005861 (3.8 MB) TX bytes:4005861 (3.8 MB)
msfadmin@metasploitable:~$ _
Right Ctrl
16:55
Type here to search
30°C Partly sunny
ENG
16:55
03-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ nmap 198.162.1.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 16:58 IST
Nmap scan report for 198.162.1.1
Host is up (0.00077s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 198.162.1.2
Host is up (0.0031s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
445/tcp open microsoft-ds
2179/tcp open vmrdp
5357/tcp open wsdapi
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 198.162.1.3
Host is up (0.0044s latency).
All 1000 scanned ports on 198.162.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D9:DB:2C (Oracle VirtualBox virtual NIC)
Nmap scan report for 198.162.1.6
Right Ctrl
17:00
Type here to search
30°C Partly sunny
ENG
17:00
03-02-2025

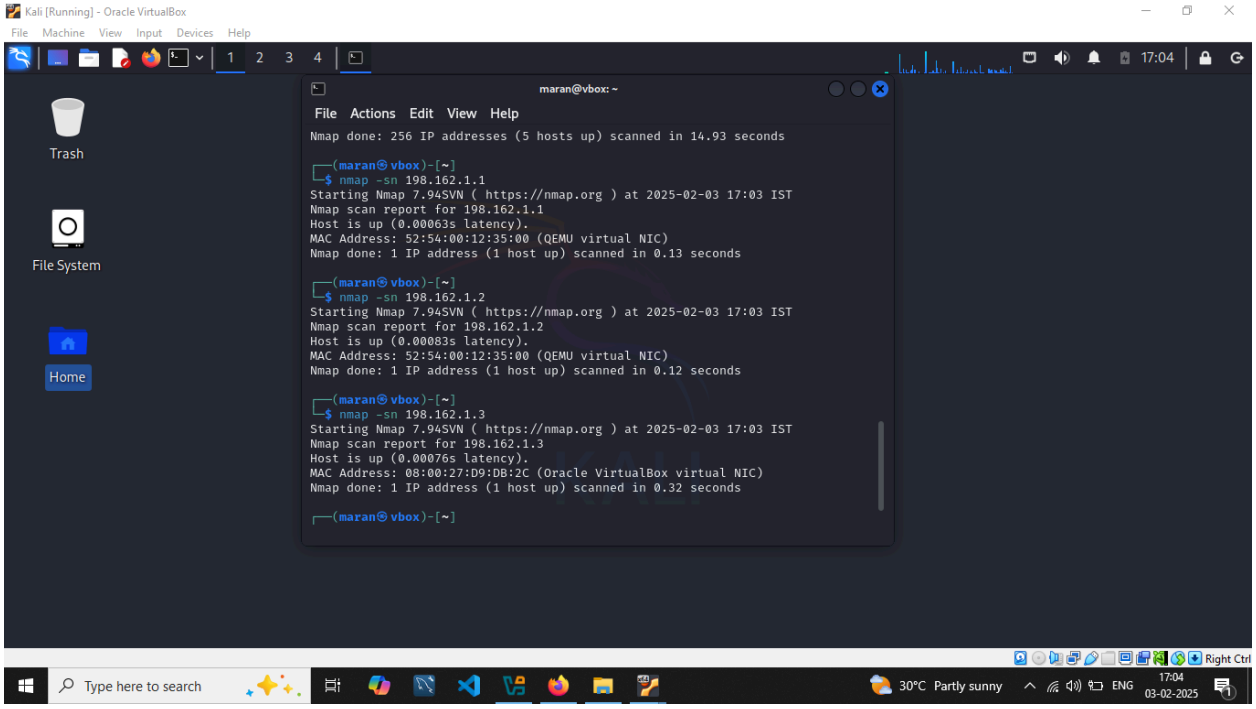

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
Nmap scan report for 198.162.1.6
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
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
Trash
File System
Home
Type here to search
30°C Partly sunny
ENG
17:01
03-02-2025

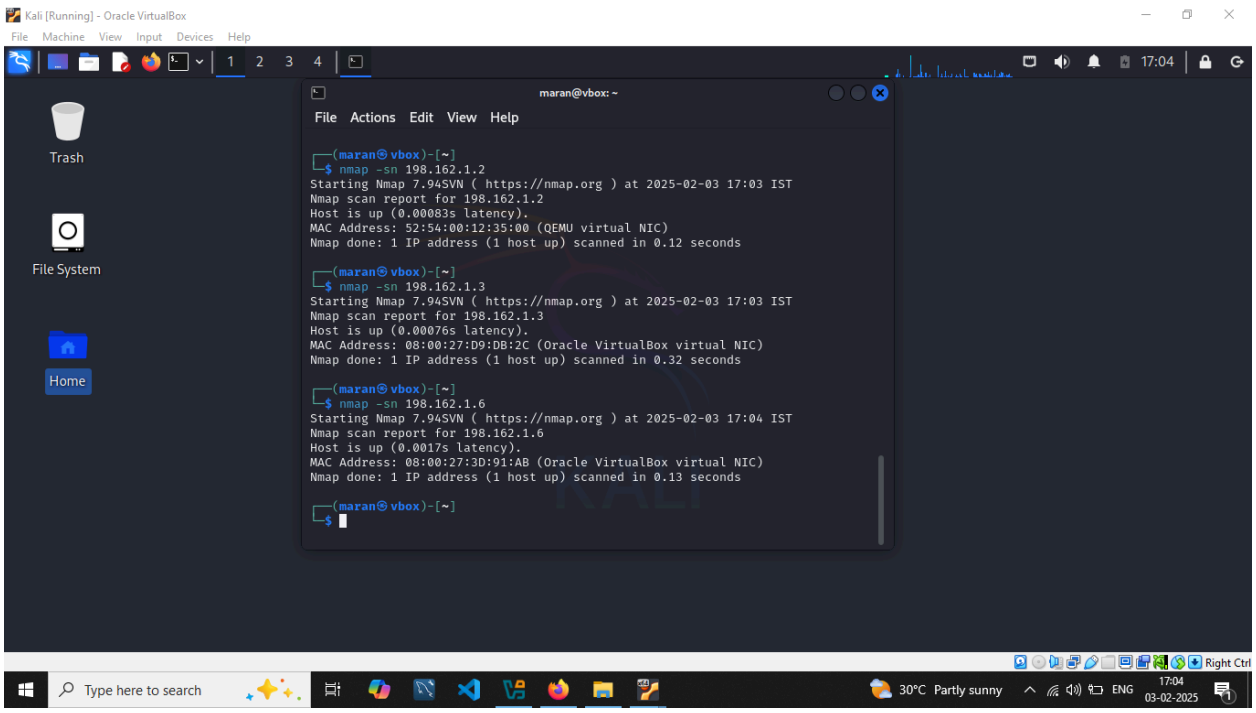

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open 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: 08:00:27:3D:91:AB (Oracle VirtualBox virtual NIC)
Nmap scan report for 198.162.1.5
Host is up (0.0000060s latency).
All 1000 scanned ports on 198.162.1.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 256 IP addresses (5 hosts up) scanned in 14.93 seconds
(maran㉿vbox)-[~]
$
Trash
File System
Home
Type here to search
30°C Partly sunny
ENG
17:01
03-02-2025

2. Perform Ping Scan:

- To perform a ping scan the `nmap -sn <ip address>` command is used.
- Performed ping scan using the command `nmap -sn 198.162.1.1` for the first available ip address and did the same for other available ip addresses.
- Found out all hosts are active within the target ip range.

Screenshots:

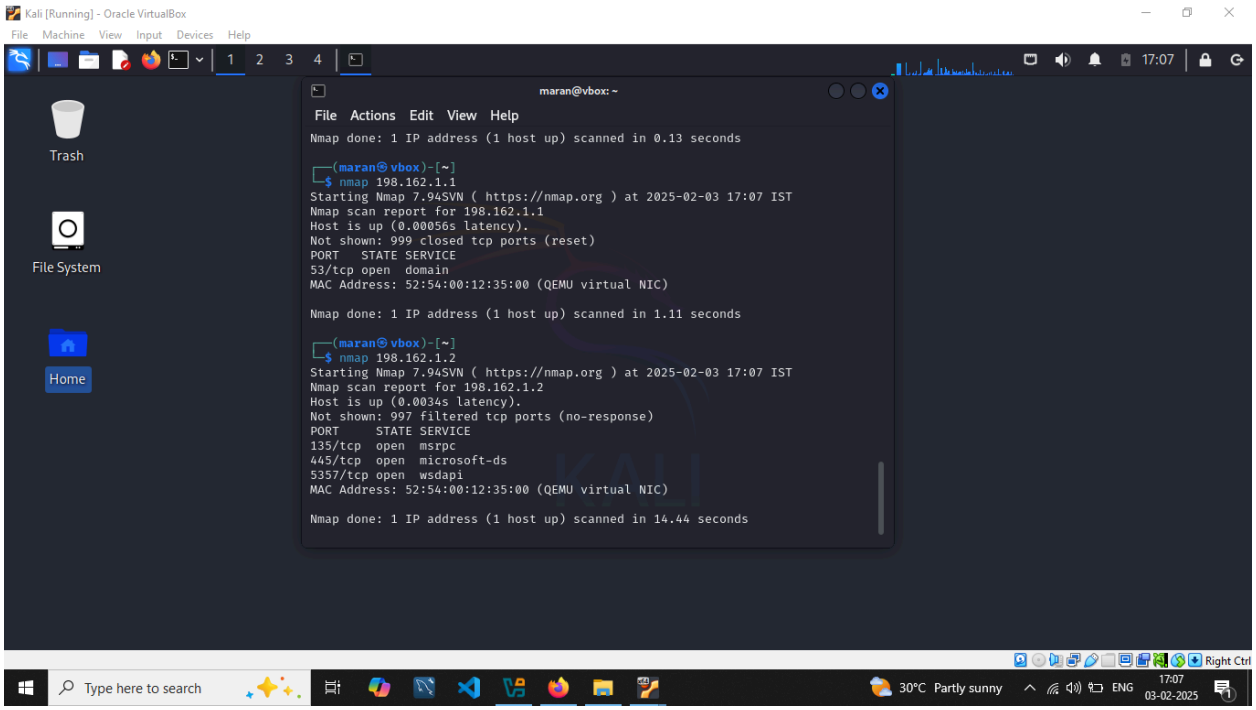


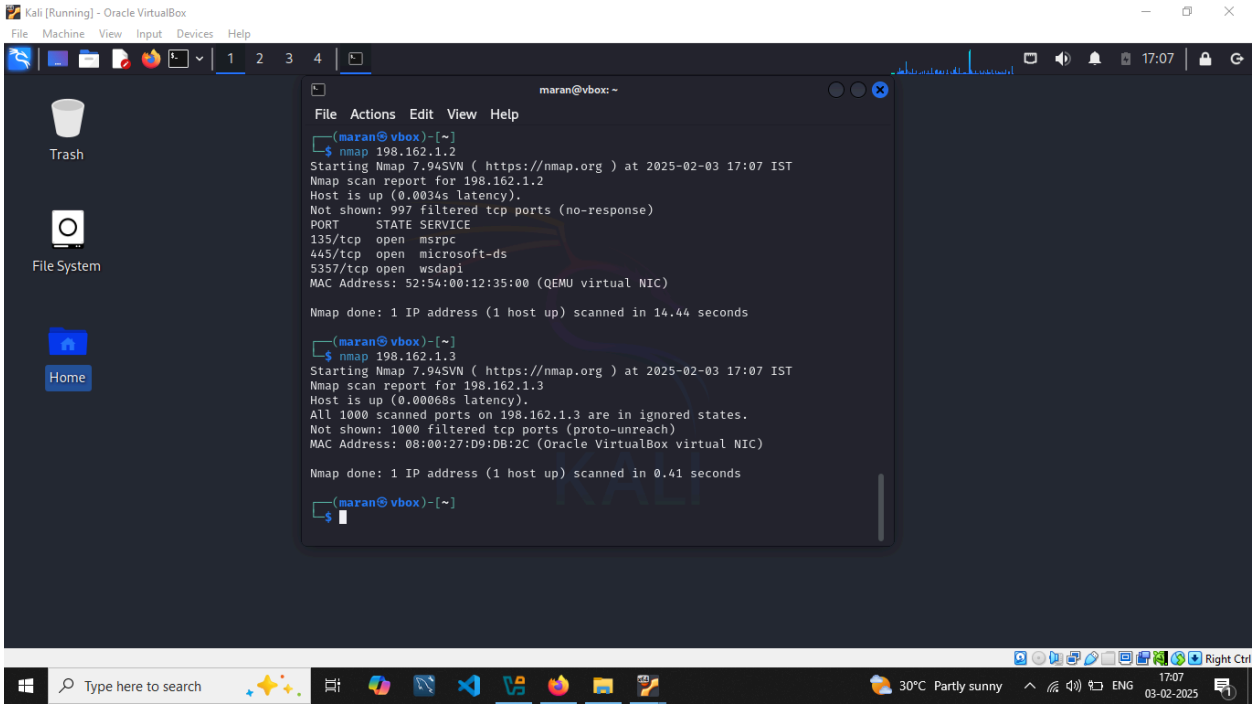


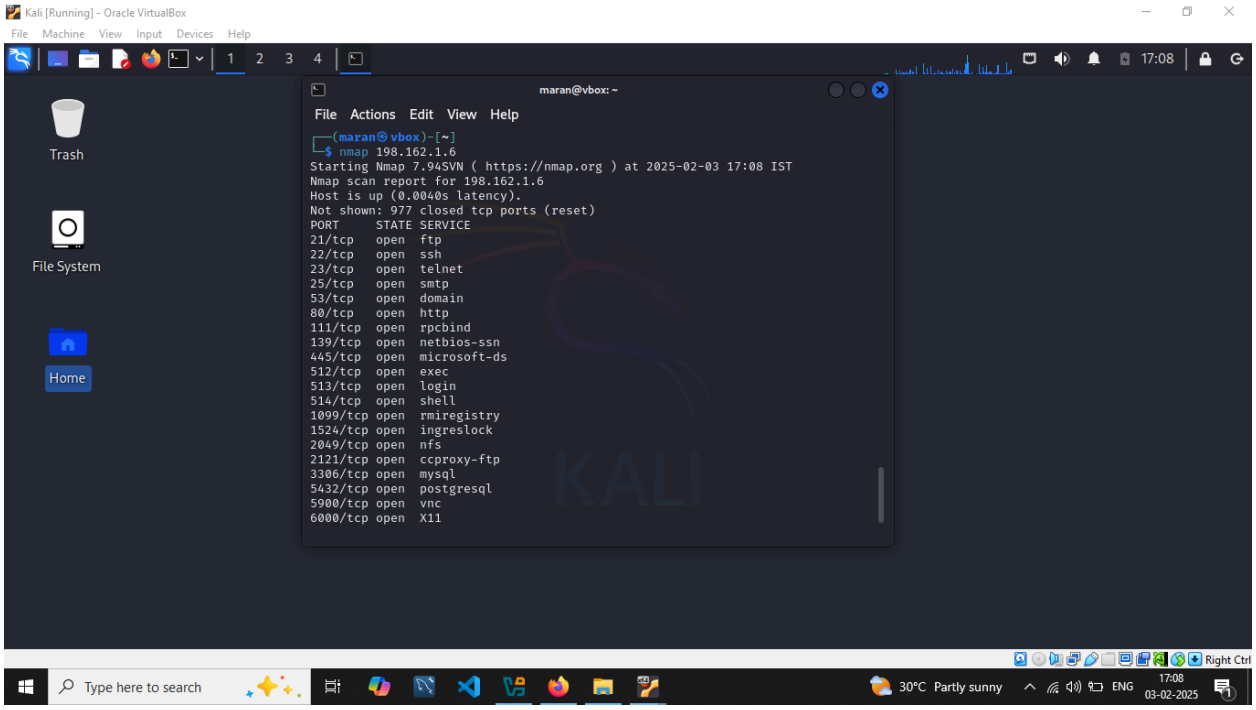
3. Port Scanning/Service Enumeration:

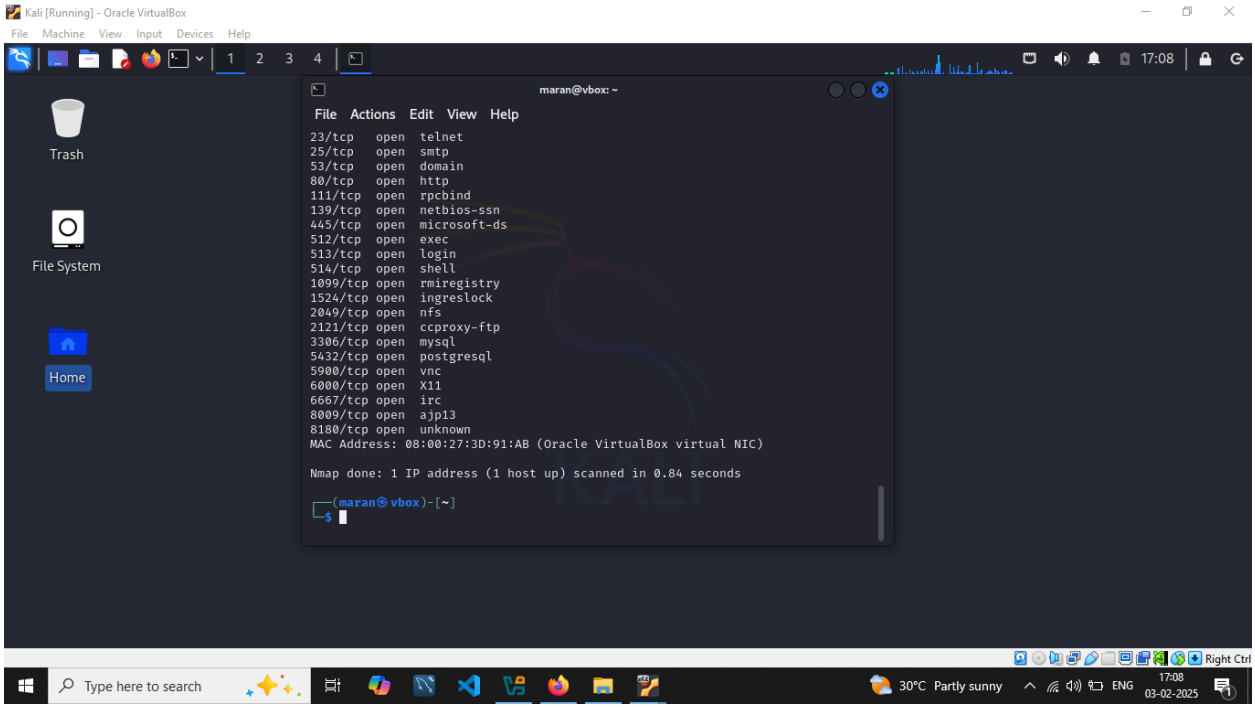
- To scan open ports and identify the service running in the active hosts just by the command `nmap <ip address>`.
- Performed the port scanning to identify the open ports and identify the service running in the active hosts by using commands `nmap 198.162.1.1`, `nmap 198.162.1.2`, `nmap 198.162.1.3`, `nmap 198.162.1.6` in the output of this shows the open ports and services.

Screenshots:




Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:07
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ nmap 198.162.1.2
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:07 IST
Nmap scan report for 198.162.1.2
Host is up (0.0034s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
445/tcp open microsoft-ds
5357/tcp open wsdapi
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.44 seconds
(maran㉿vbox)-[~]
$ nmap 198.162.1.3
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:07 IST
Nmap scan report for 198.162.1.3
Host is up (0.00068s latency).
All 1000 scanned ports on 198.162.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D9:DB:2C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:07
03-02-2025

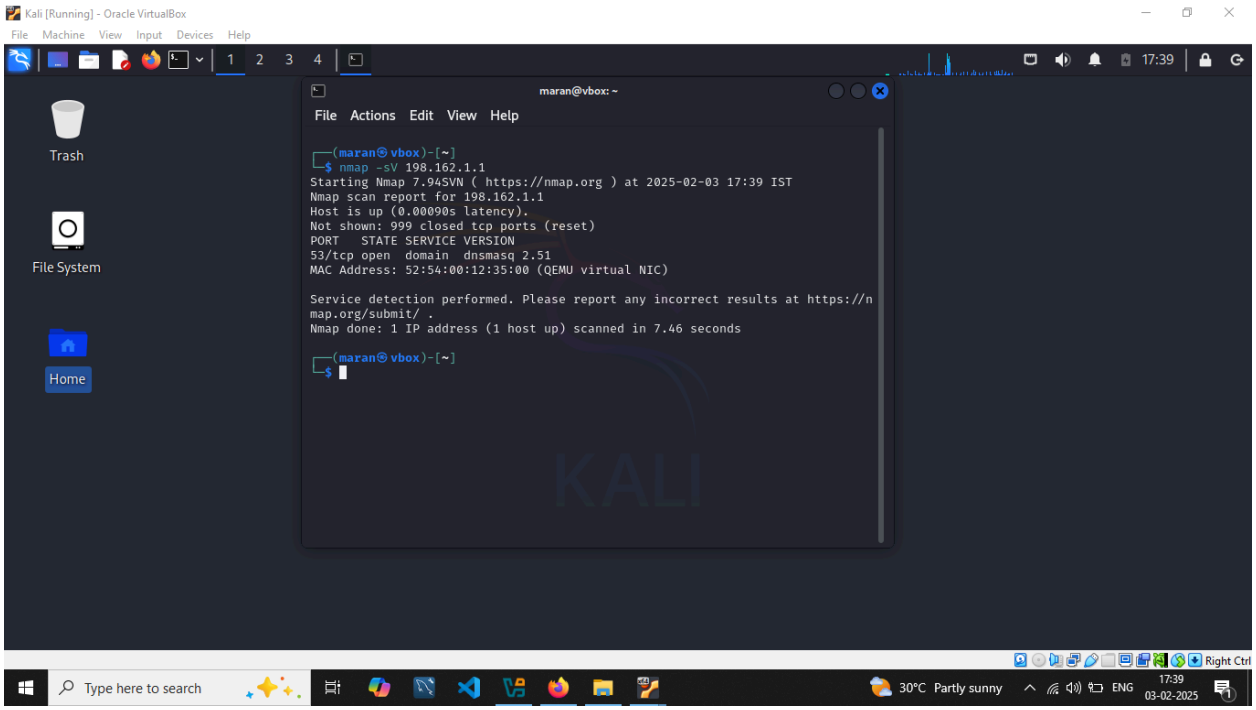

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:08
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ nmap 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:08 IST
Nmap scan report for 198.162.1.6
Host is up (0.0040s latency).
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
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:08
03-02-2025

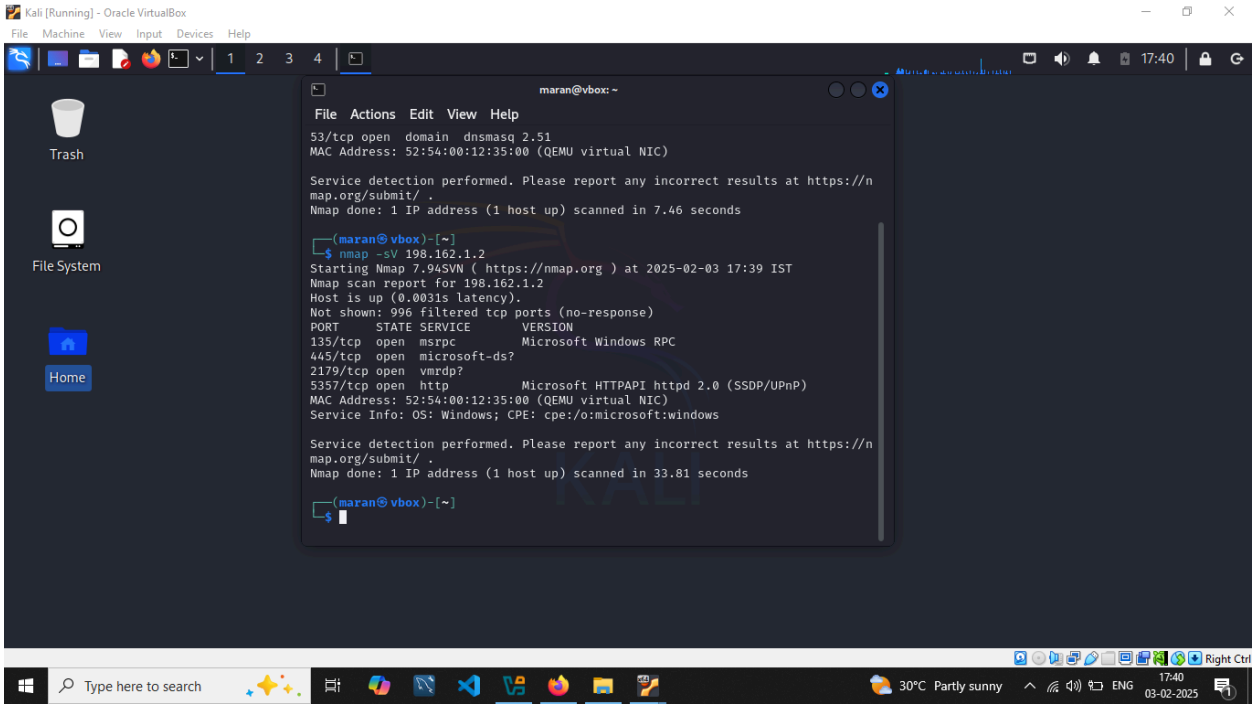

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:08
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp 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: 08:00:27:3D:91:AB (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:08
03-02-2025

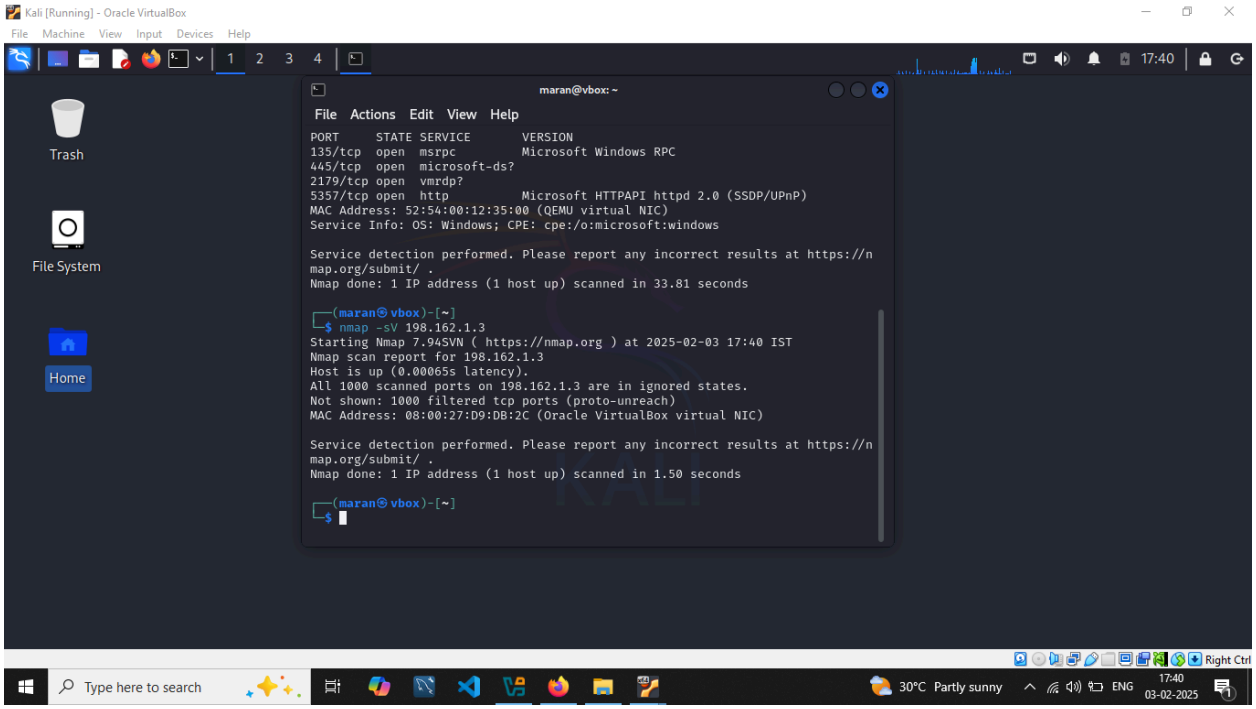
4. Banner Grabbing:

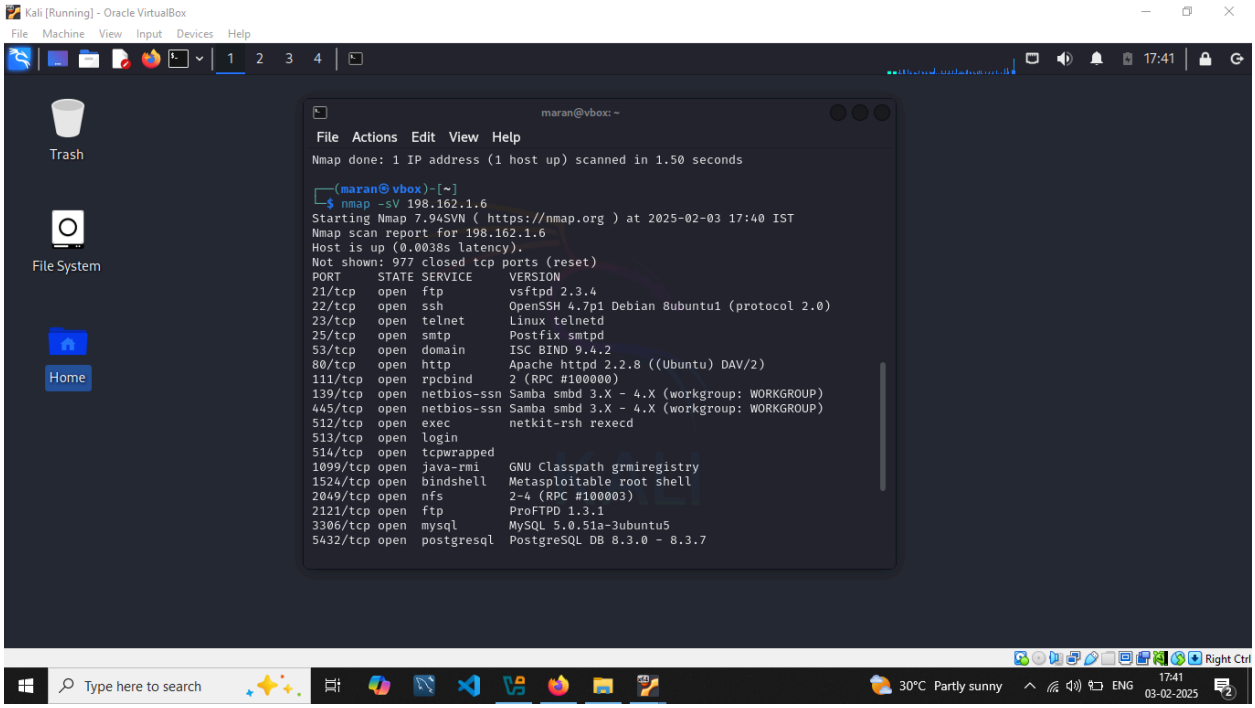
- Banner grabbing is one of the information gathering techniques which is collecting the information from the host by open ports and services running on the open port with their version.
- To perform banner grabbing in nmap the `nmap -sV <ip address>` command is used.
- There are a lot of commands to perform banner grabbing like `telnet`, `cURL`, `Wget`.
- Performed the banner grabbing using command `nmap -sV 198.162.1.1`, `nmap -sV 198.162.1.2`, `nmap -sV 198.162.1.3`, `nmap -sV 198.162.1.6` in the output of this shows the open ports and services running on the open port with their version.

Screenshots:




Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:40
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
53/tcp open domain dnsmasq 2.51
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.46 seconds
(maran㉿vbox)-[~]
$ nmap -sV 198.162.1.2
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:39 IST
Nmap scan report for 198.162.1.2
Host is up (0.0031s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
2179/tcp open vmrdp?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.81 seconds
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:40
03-02-2025

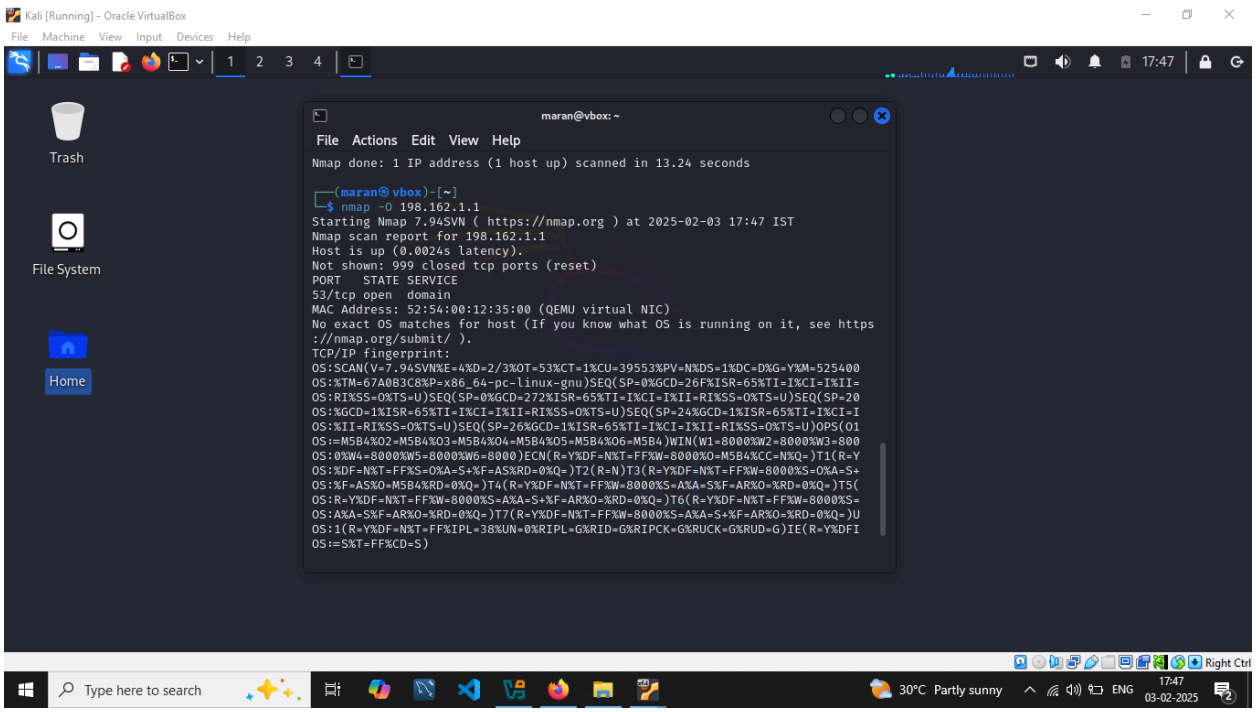

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:40
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
2179/tcp open vmrdp?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.81 seconds
(maran㉿vbox)-[~]
$ nmap -sV 198.162.1.3
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:40 IST
Nmap scan report for 198.162.1.3
Host is up (0.00065s latency).
All 1000 scanned ports on 198.162.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D9:DB:2C (Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:40
03-02-2025

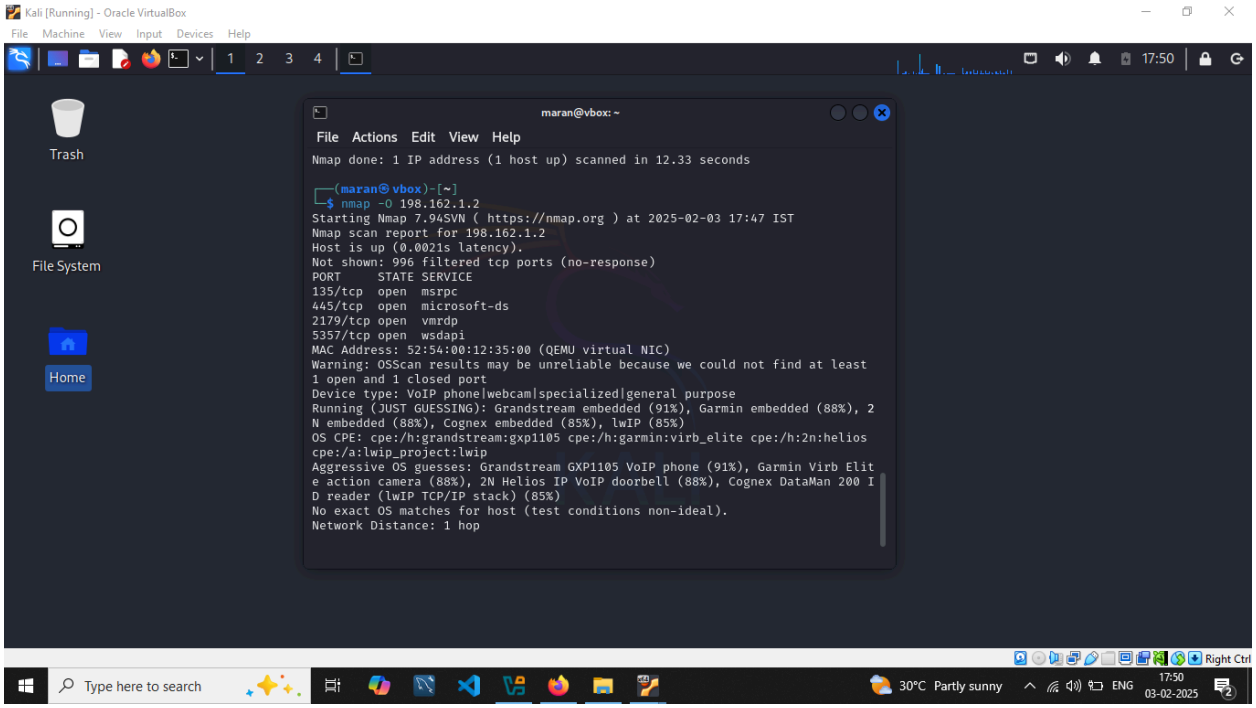

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:41
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
┌──(maran㉿vbox)-[~]
└─$ nmap -sV 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:40 IST
Nmap scan report for 198.162.1.6
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 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 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
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:41
03-02-2025

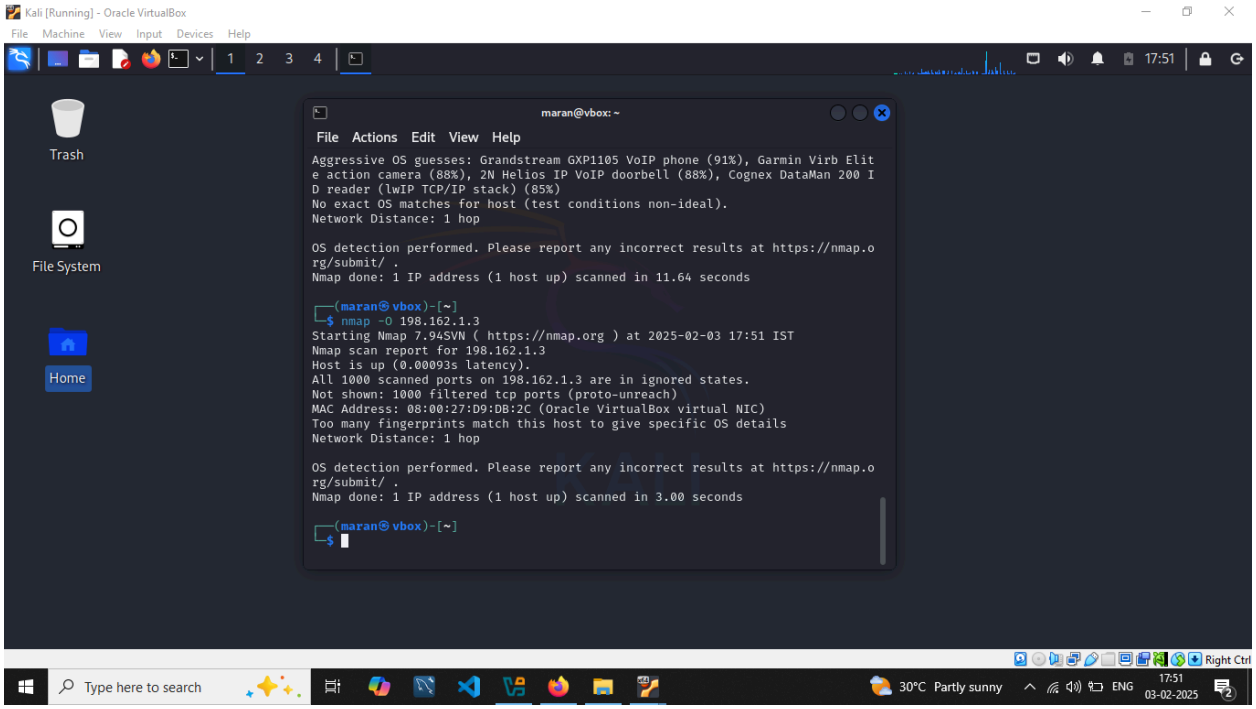
5.OS Fingerprinting:

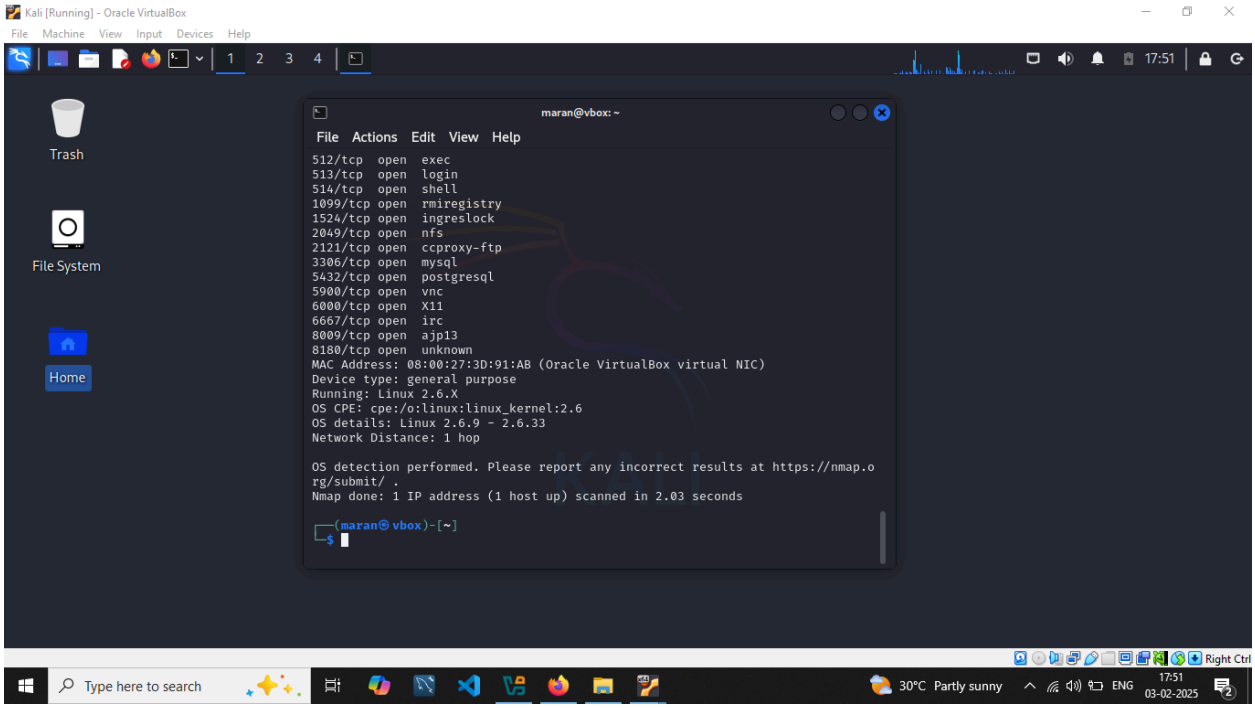
- OS fingerprinting is one of the information gathering techniques which collects the information about Operating systems and their versions.
- To perform OS fingerprinting in nmap the `nmap -O <ip address>` command is used.
- Performed the OS fingerprinting using command `nmap -O 198.162.1.1`, `nmap -O 198.162.1.2`, `nmap -O 198.162.1.3`, `nmap -O 198.162.1.6` in the output of this shows the information about Operating systems and their versions.

Screenshots:




Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:50
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 12.33 seconds
(maran㉿vbox)-[~]
$ nmap -O 198.162.1.2
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:47 IST
Nmap scan report for 198.162.1.2
Host is up (0.0021s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
445/tcp open microsoft-ds
2179/tcp open vmrdp
5357/tcp open wsdapi
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|webcam|specialized|general purpose
Running (JUST GUESSING): Grandstream embedded (91%), Garmin embedded (88%), 2N embedded (88%), Cognex embedded (85%), lwIP (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios cpe:/a:lwip_project:lwip
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), Garmin Virb Elite action camera (88%), 2N Helios IP VoIP doorbell (88%), Cognex DataMan 200 ID reader (lwIP TCP/IP stack) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:50
03-02-2025

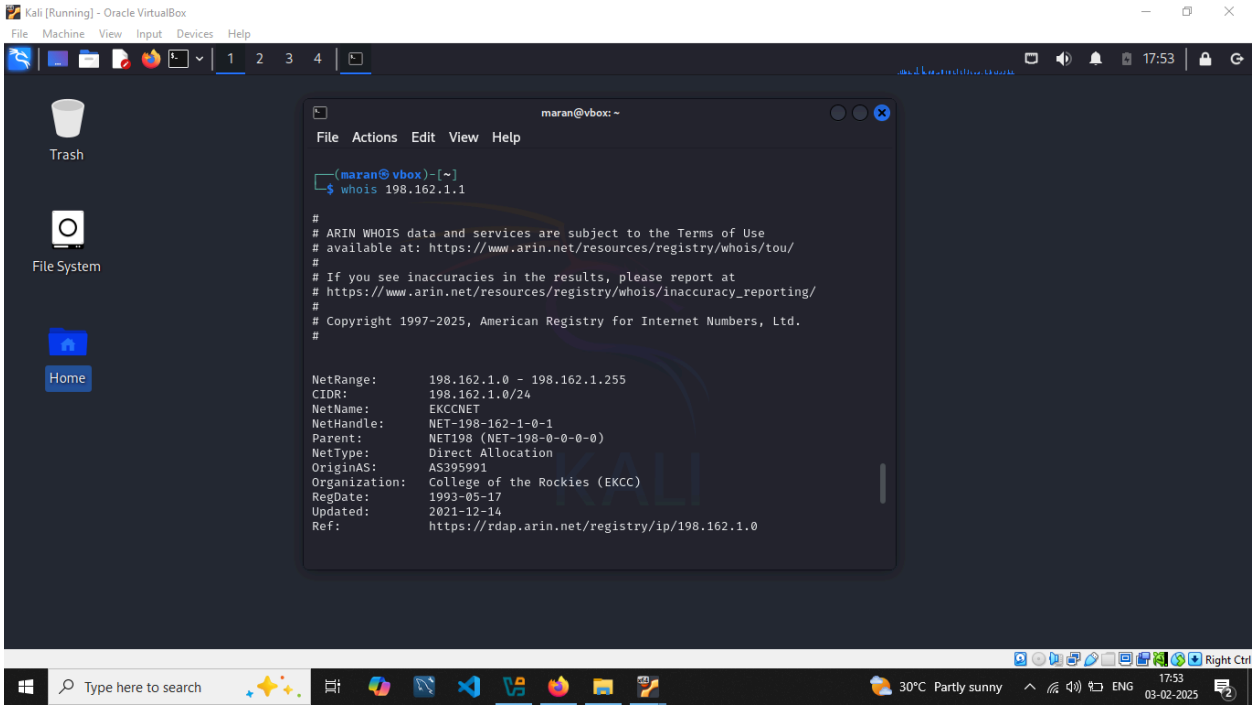

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:51
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), Garmin Virb Elite action camera (88%), 2N Helios IP VoIP doorbell (88%), Cognex DataMan 200 ID reader (lwIP TCP/IP stack) (85%)
No exact OS matches for host (test conditions non-ideal).
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 11.64 seconds
(maran㉿vbox)-[~]
$ nmap -O 198.162.1.3
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 17:51 IST
Nmap scan report for 198.162.1.3
Host is up (0.00093s latency).
All 1000 scanned ports on 198.162.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D9:DB:2C (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 3.00 seconds
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:51
03-02-2025

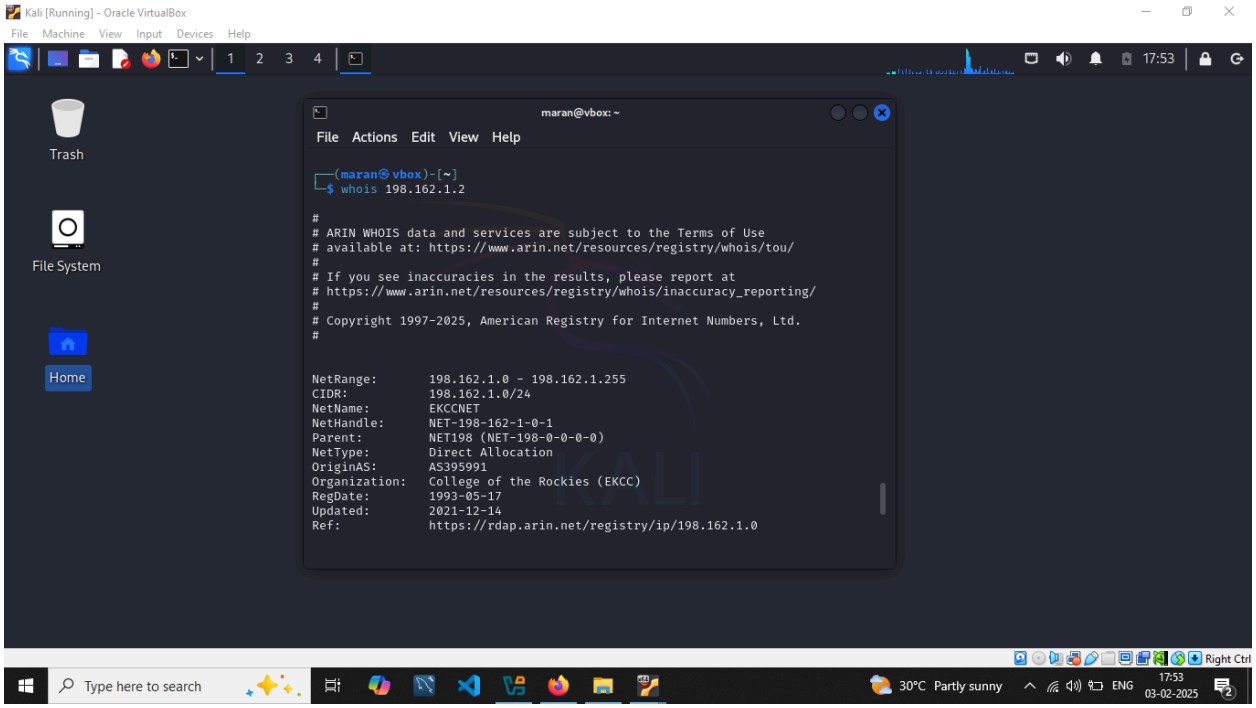

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:51
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp 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: 08:00:27:3D:91:AB (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
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:51
03-02-2025

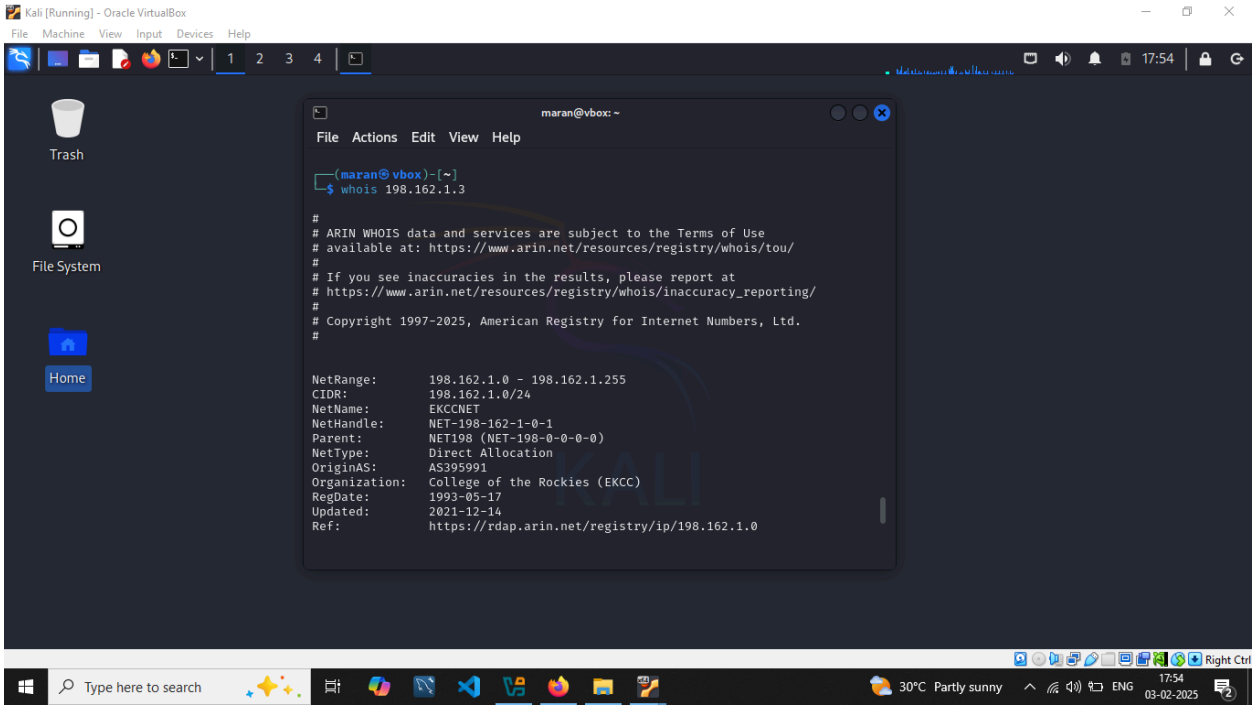
6.Footprinting:

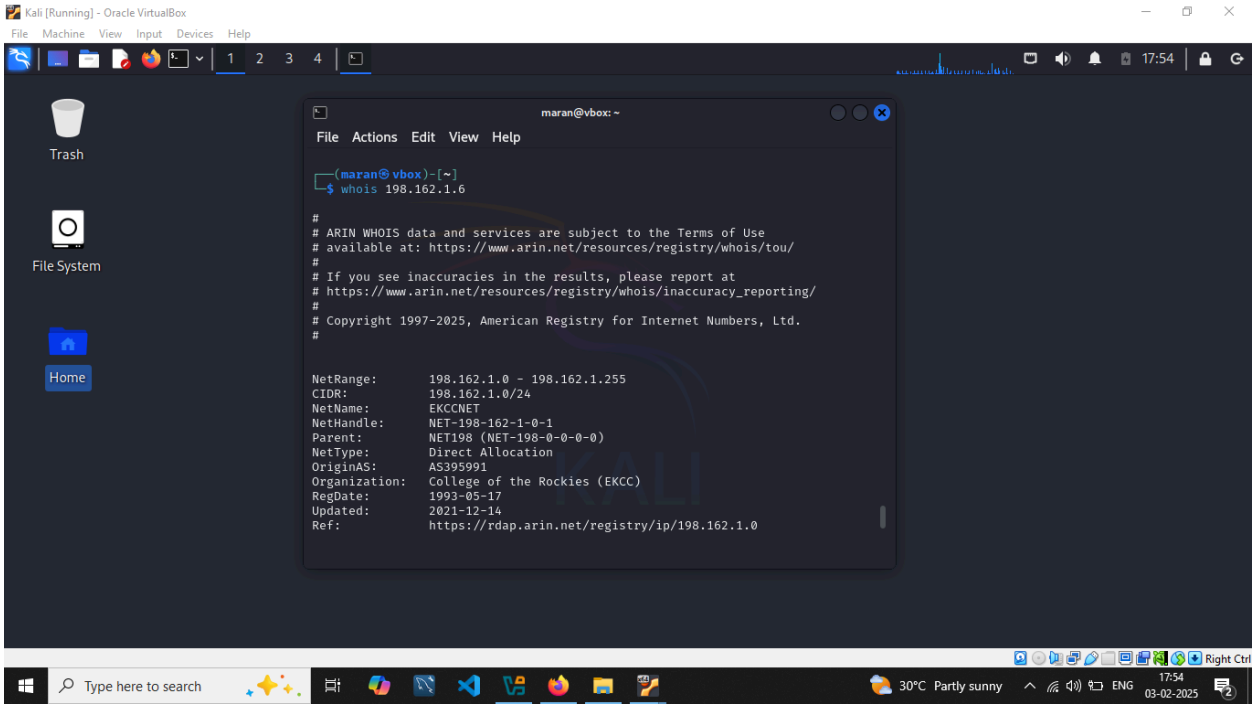
- Footprinting is a process of gathering information about a target organization or network to identify vulnerabilities.
- Using tools like `whois`, `dig`, and `nslookup` to gather additional information about the target network and domain.
- Using `whois` tool first, using command `whois 198.162.1.1`, `whois 198.162.1.2`, `whois 198.162.1.3`, `whois 198.162.1.6` to collect information about the active hosts in the target ip address range.
- Using `dig` tool next, using command `dig 198.162.1.1`, `dig 198.162.1.2`, `dig 198.162.1.3`, `dig 198.162.1.6` to collect information about the active hosts in the target ip address range.
- Using `nslookup` tool, using command `nslookup 198.162.1.1`, `nslookup 198.162.1.2`, `nslookup 198.162.1.3`, `nslookup 198.162.1.6` to collect information about the active hosts in the target ip address range.

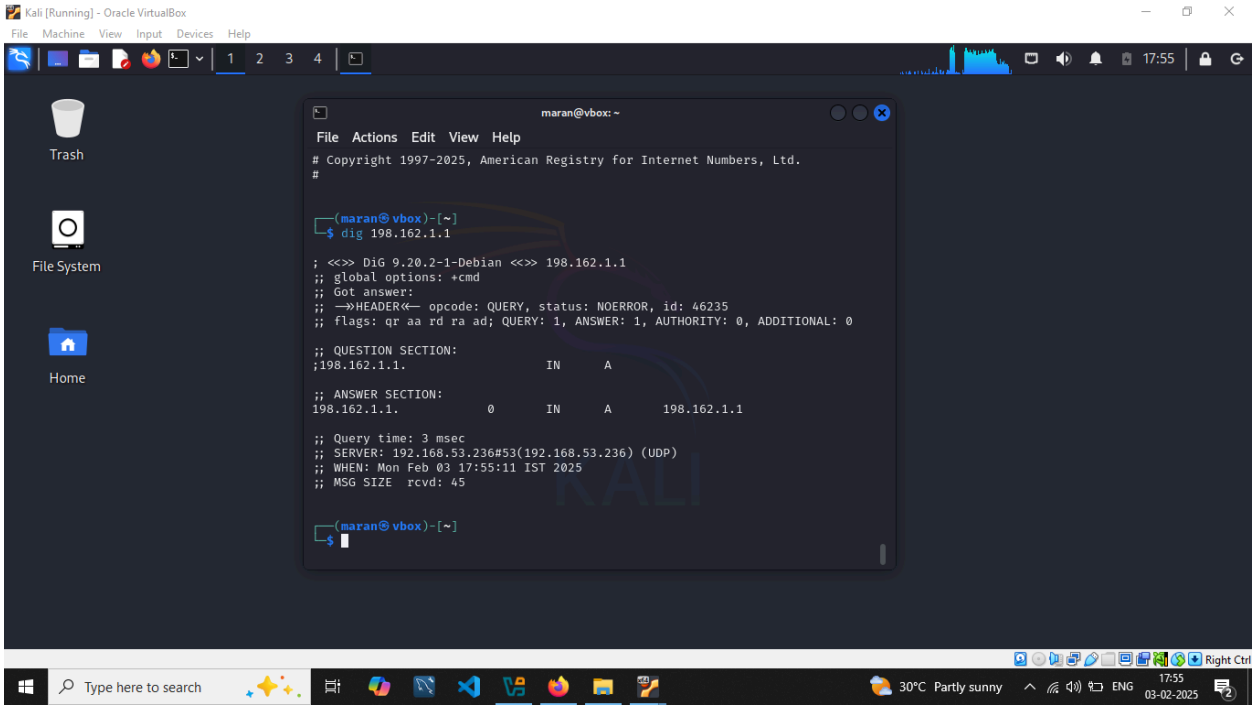
Screenshots:

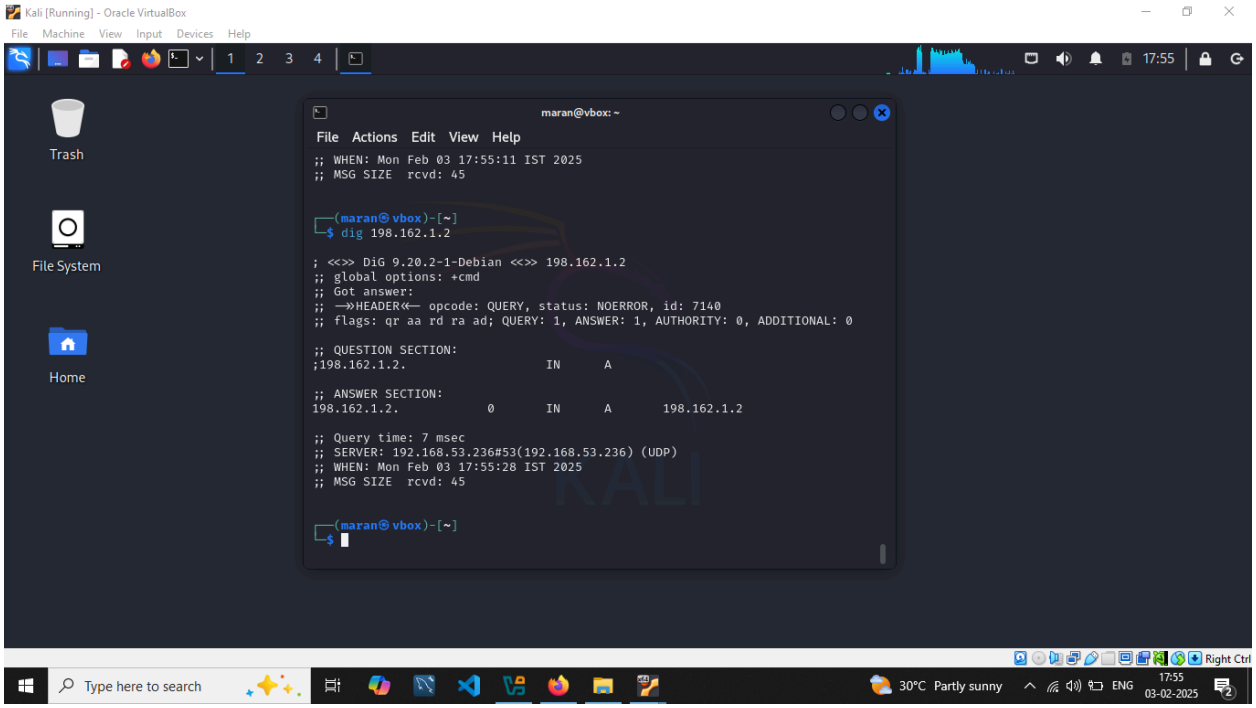


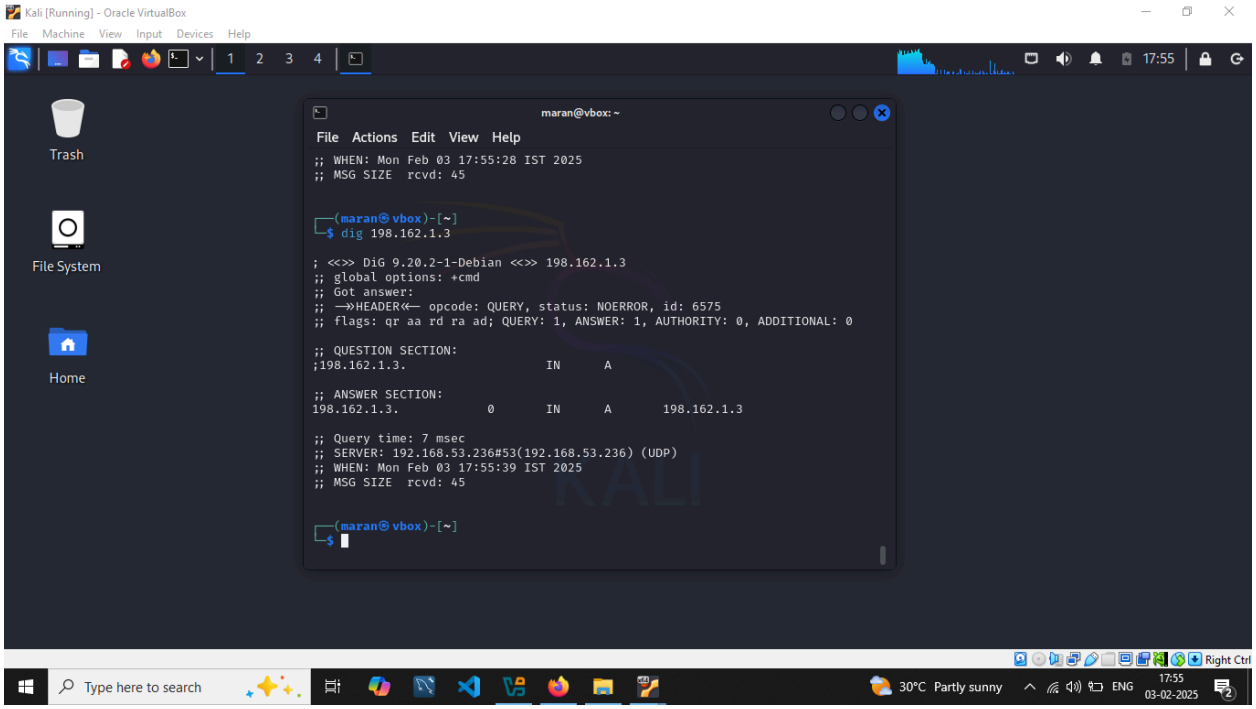

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:53
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ whois 198.162.1.2
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
NetRange: 198.162.1.0 - 198.162.1.255
CIDR: 198.162.1.0/24
NetName: EKCCNET
NetHandle: NET-198-162-1-0-1
Parent: NET198 (NET-198-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS395991
Organization: College of the Rockies (EKCC)
RegDate: 1993-05-17
Updated: 2021-12-14
Ref: https://rdap.arin.net/registry/ip/198.162.1.0
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:53
03-02-2025

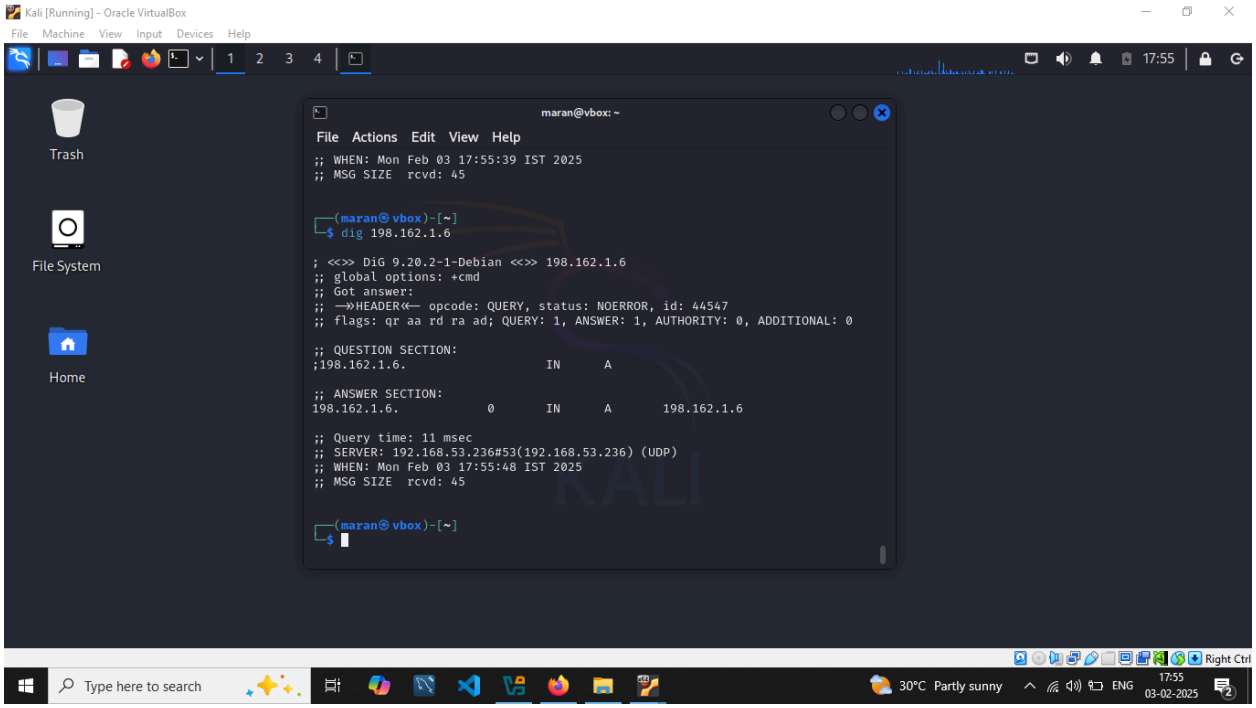

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:54
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ whois 198.162.1.3
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
NetRange: 198.162.1.0 - 198.162.1.255
CIDR: 198.162.1.0/24
NetName: EKCCNET
NetHandle: NET-198-162-1-0-1
Parent: NET198 (NET-198-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS395991
Organization: College of the Rockies (EKCC)
RegDate: 1993-05-17
Updated: 2021-12-14
Ref: https://rdap.arin.net/registry/ip/198.162.1.0
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:54
03-02-2025

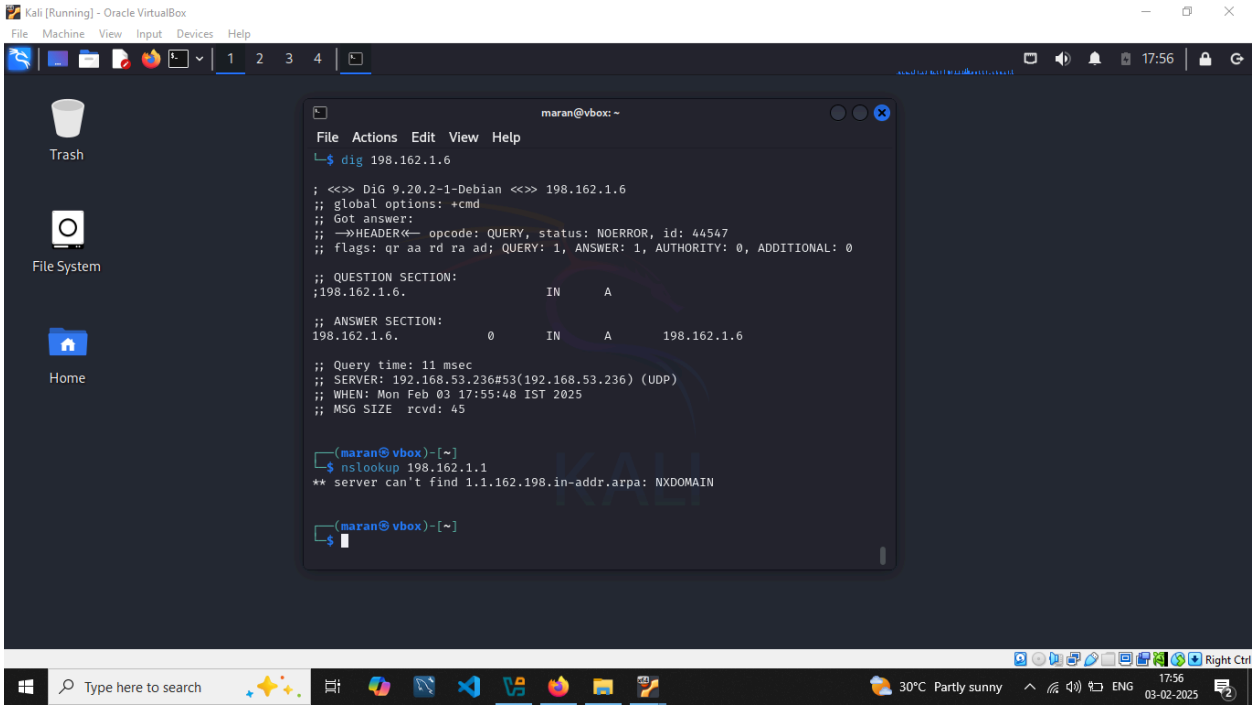

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:54
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ whois 198.162.1.6
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
NetRange: 198.162.1.0 - 198.162.1.255
CIDR: 198.162.1.0/24
NetName: EKCCNET
NetHandle: NET-198-162-1-0-1
Parent: NET198 (NET-198-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS395991
Organization: College of the Rockies (EKCC)
RegDate: 1993-05-17
Updated: 2021-12-14
Ref: https://rdap.arin.net/registry/ip/198.162.1.0
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:54
03-02-2025

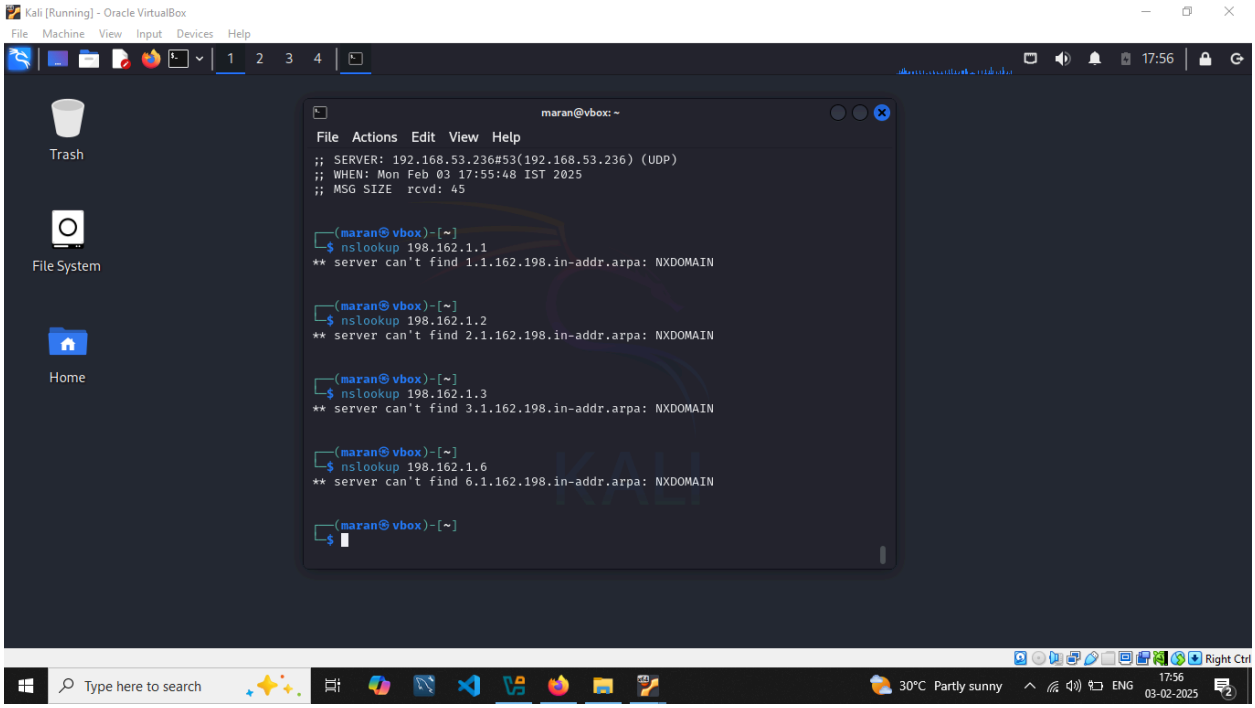

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:55
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
(maran㉿vbox)-[~]
$ dig 198.162.1.1
; <<>> DiG 9.20.2-1-Debian <<>> 198.162.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46235
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;198.162.1.1. IN A
;; ANSWER SECTION:
198.162.1.1. 0 IN A 198.162.1.1
;; Query time: 3 msec
;; SERVER: 192.168.53.236#53(192.168.53.236) (UDP)
;; WHEN: Mon Feb 03 17:55:11 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:55
03-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:55
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
;; WHEN: Mon Feb 03 17:55:11 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$ dig 198.162.1.2
; <<>> DiG 9.20.2-1-Debian <<>> 198.162.1.2
;; global options: +cmd
;; Got answer:
;; →→HEADER←← opcode: QUERY, status: NOERROR, id: 7140
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;198.162.1.2. IN A
;; ANSWER SECTION:
198.162.1.2. 0 IN A 198.162.1.2
;; Query time: 7 msec
;; SERVER: 192.168.53.236#53(192.168.53.236) (UDP)
;; WHEN: Mon Feb 03 17:55:28 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:55
03-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:55
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
;; WHEN: Mon Feb 03 17:55:28 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$ dig 198.162.1.3
; <<>> DiG 9.20.2-1-Debian <<>> 198.162.1.3
;; global options: +cmd
;; Got answer:
;; →→HEADER←← opcode: QUERY, status: NOERROR, id: 6575
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;198.162.1.3. IN A
;; ANSWER SECTION:
198.162.1.3. 0 IN A 198.162.1.3
;; Query time: 7 msec
;; SERVER: 192.168.53.236#53(192.168.53.236) (UDP)
;; WHEN: Mon Feb 03 17:55:39 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:55
03-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:55
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
;; WHEN: Mon Feb 03 17:55:39 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$ dig 198.162.1.6
; <<>> DiG 9.20.2-1-Debian <<>> 198.162.1.6
;; global options: +cmd
;; Got answer:
;; →→HEADER←← opcode: QUERY, status: NOERROR, id: 44547
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;198.162.1.6. IN A
;; ANSWER SECTION:
198.162.1.6. 0 IN A 198.162.1.6
;; Query time: 11 msec
;; SERVER: 192.168.53.236#53(192.168.53.236) (UDP)
;; WHEN: Mon Feb 03 17:55:48 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:55
03-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:56
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
$ dig 198.162.1.6
; <<>> DiG 9.20.2-1-Debian <<>> 198.162.1.6
;; global options: +cmd
;; Got answer:
;; →→HEADER←← opcode: QUERY, status: NOERROR, id: 44547
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;198.162.1.6. IN A
;; ANSWER SECTION:
198.162.1.6. 0 IN A 198.162.1.6
;; Query time: 11 msec
;; SERVER: 192.168.53.236#53(192.168.53.236) (UDP)
;; WHEN: Mon Feb 03 17:55:48 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$ nslookup 198.162.1.1
** server can't find 1.1.162.198.in-addr.arpa: NXDOMAIN
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:56
03-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:56
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
;; SERVER: 192.168.53.236#53(192.168.53.236) (UDP)
;; WHEN: Mon Feb 03 17:55:48 IST 2025
;; MSG SIZE rcvd: 45
(maran㉿vbox)-[~]
$ nslookup 198.162.1.1
** server can't find 1.1.162.198.in-addr.arpa: NXDOMAIN
(maran㉿vbox)-[~]
$ nslookup 198.162.1.2
** server can't find 2.1.162.198.in-addr.arpa: NXDOMAIN
(maran㉿vbox)-[~]
$ nslookup 198.162.1.3
** server can't find 3.1.162.198.in-addr.arpa: NXDOMAIN
(maran㉿vbox)-[~]
$ nslookup 198.162.1.6
** server can't find 6.1.162.198.in-addr.arpa: NXDOMAIN
(maran㉿vbox)-[~]
$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
17:56
03-02-2025

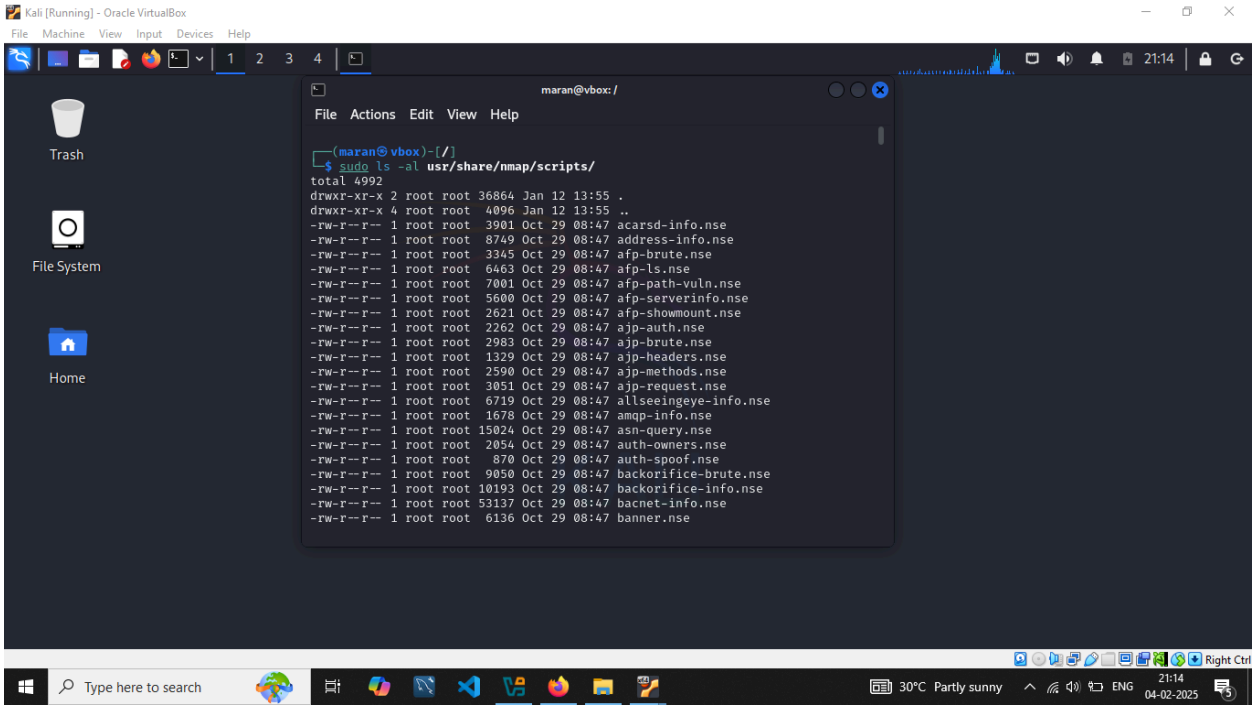
7.Vulnerability assessment:

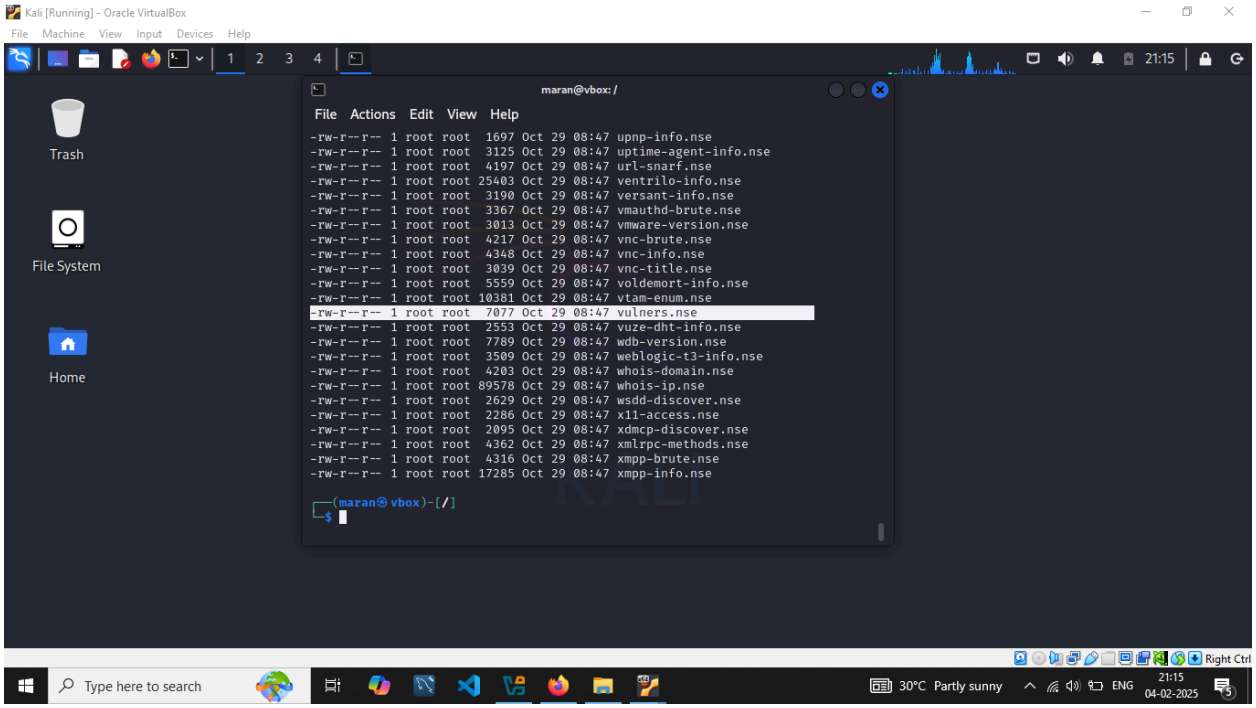
- To perform vulnerability assessment using nmap there are pre-installed scripts available.
- Vulners.nse is the file which is used to do vulnerability assessment in nmap.
- Using command `sudo ls -al usr/share/nmap/scripts/` to locate the pre-installed scripts of nmap, locating the `vulners.nse` script.
- Using this script for vulnerability assessment by the command

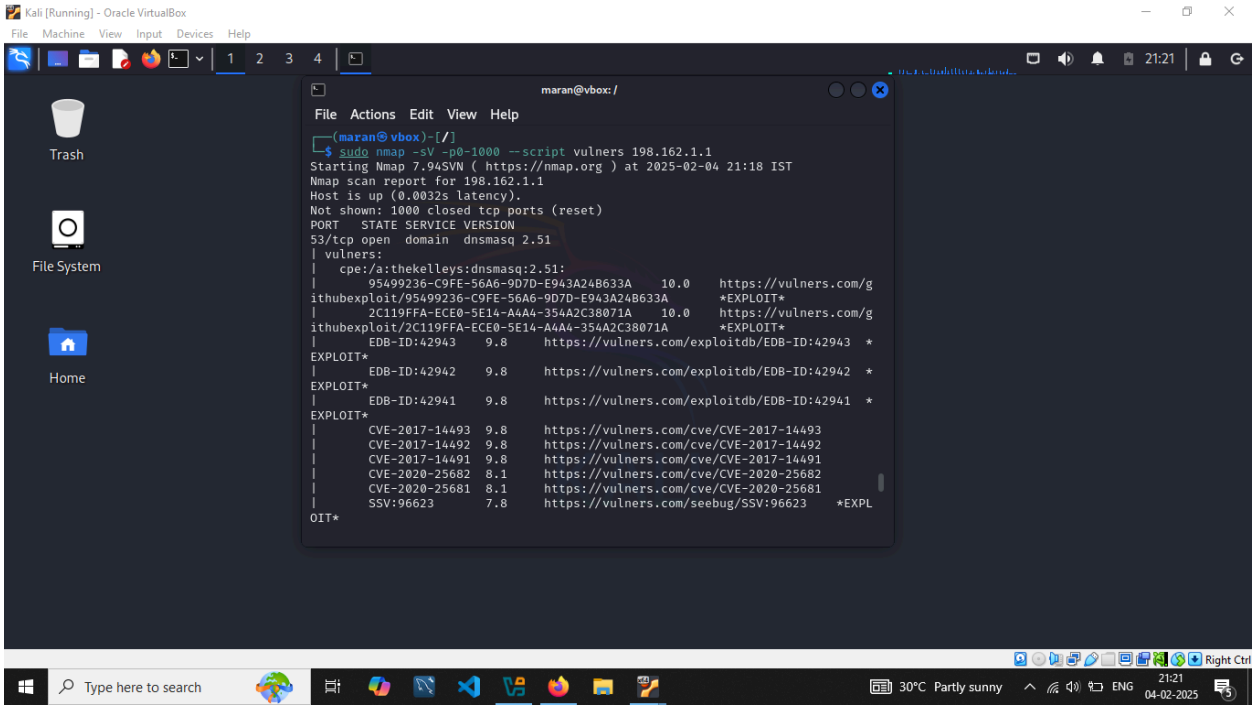
  ```
  sudo nmap -sV -p0-1000 -script vulners 198.162.1.1
  sudo nmap -sV -p0-1000 -script vulners 198.162.1.2
  sudo nmap -sV -p0-1000 -script vulners 198.162.1.3
  sudo nmap -sV -p0-1000 -script vulners 198.162.1.6
  ```

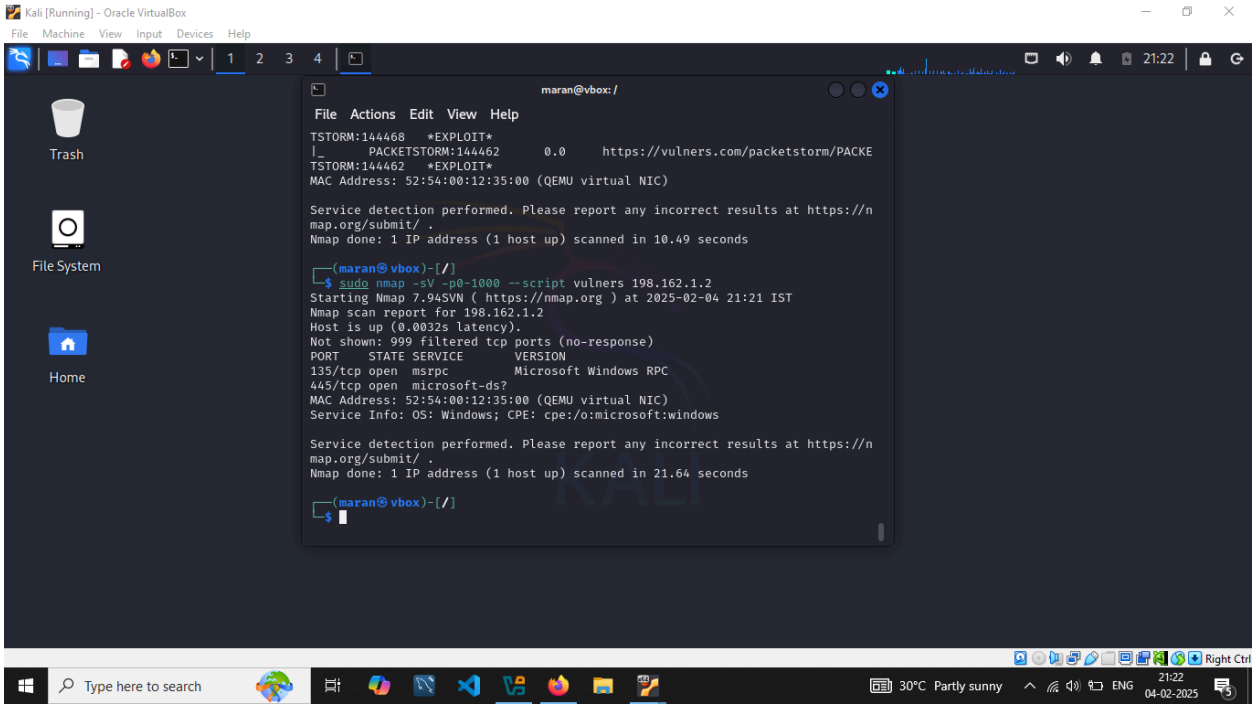
  to do the vulnerability assessment for all the active hosts in the target ip address range.
- In the output of active hosts have the vulnerabilities with the cvss (common vulnerability scoring system)with a link to its website there is all the information about the vulnerability, exploits and disclosed date.

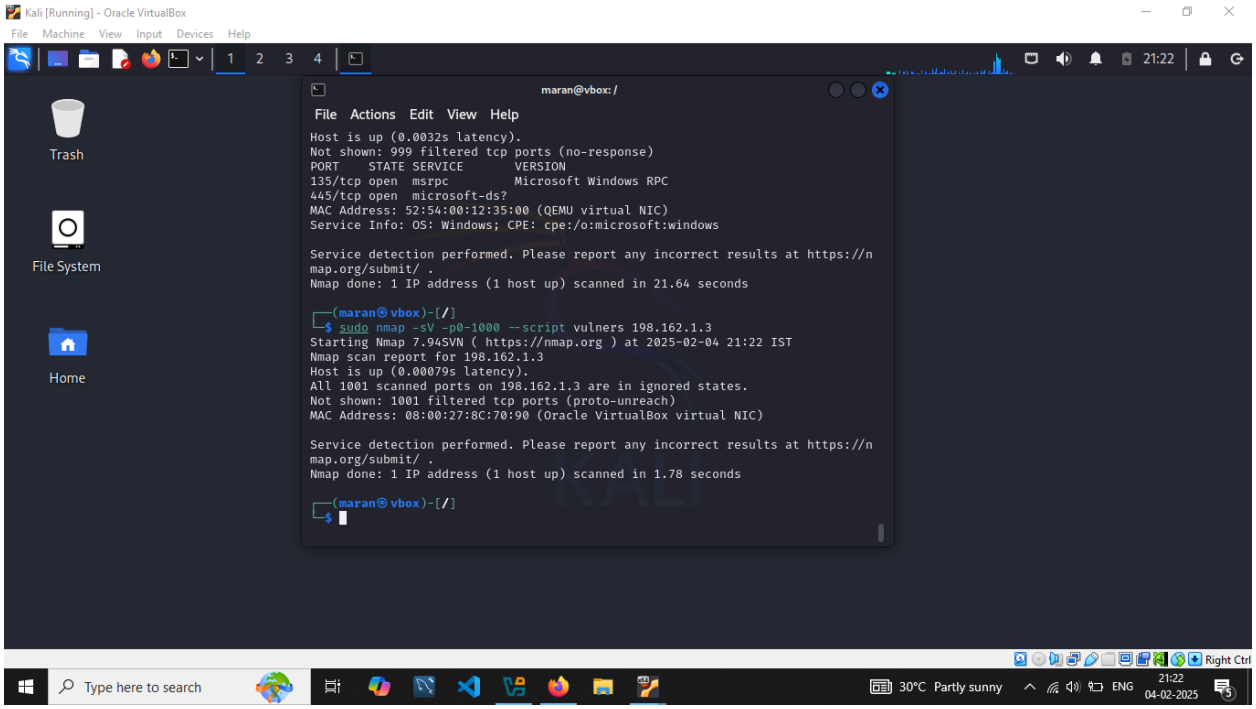
Screenshots:

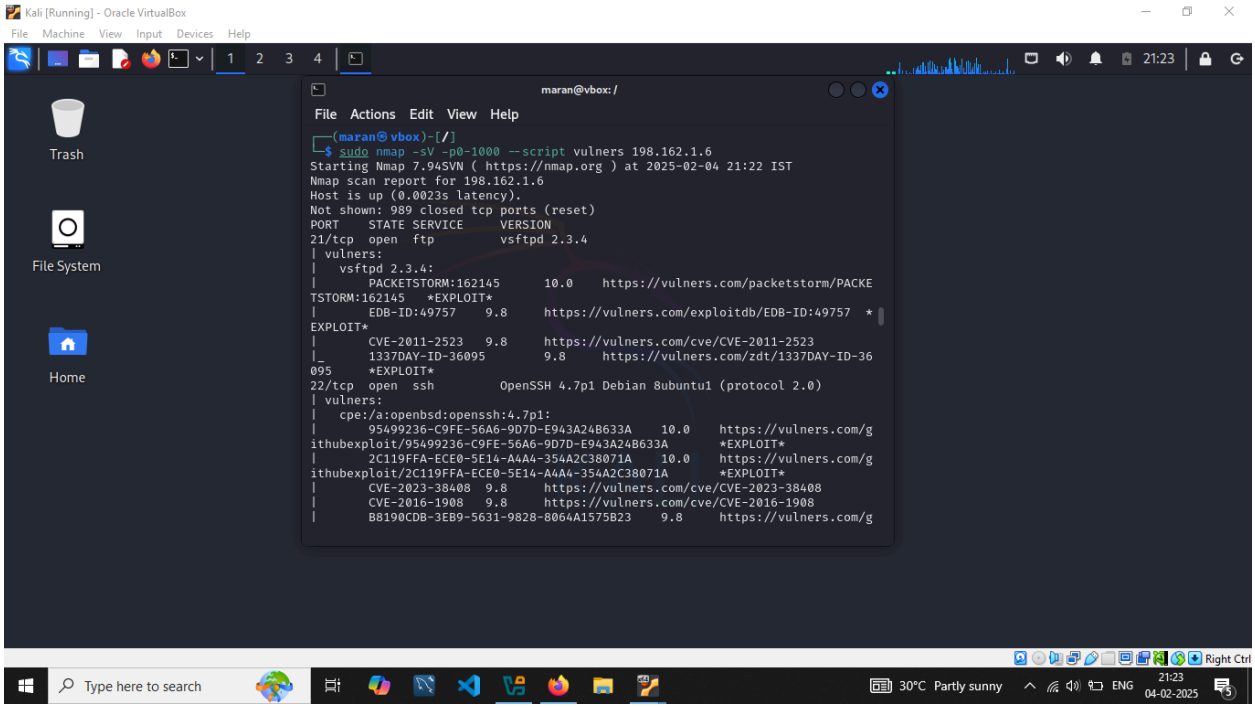



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: /
File Actions Edit View Help
-rw-r--r-- 1 root root 1697 Oct 29 08:47 upnp-info.nse
-rw-r--r-- 1 root root 3125 Oct 29 08:47 uptime-agent-info.nse
-rw-r--r-- 1 root root 4197 Oct 29 08:47 url-snarf.nse
-rw-r--r-- 1 root root 25403 Oct 29 08:47 ventrilo-info.nse
-rw-r--r-- 1 root root 3190 Oct 29 08:47 versant-info.nse
-rw-r--r-- 1 root root 3367 Oct 29 08:47 vmauthd-brute.nse
-rw-r--r-- 1 root root 3013 Oct 29 08:47 vmware-version.nse
-rw-r--r-- 1 root root 4217 Oct 29 08:47 vnc-brute.nse
-rw-r--r-- 1 root root 4348 Oct 29 08:47 vnc-info.nse
-rw-r--r-- 1 root root 3039 Oct 29 08:47 vnc-title.nse
-rw-r--r-- 1 root root 5559 Oct 29 08:47 voldemort-info.nse
-rw-r--r-- 1 root root 10381 Oct 29 08:47 vtam-enum.nse
-rw-r--r-- 1 root root 7077 Oct 29 08:47 vulners.nse
-rw-r--r-- 1 root root 2553 Oct 29 08:47 vuze-dht-info.nse
-rw-r--r-- 1 root root 7789 Oct 29 08:47 wdb-version.nse
-rw-r--r-- 1 root root 3509 Oct 29 08:47 weblogic-t3-info.nse
-rw-r--r-- 1 root root 4203 Oct 29 08:47 whois-domain.nse
-rw-r--r-- 1 root root 89578 Oct 29 08:47 whois-ip.nse
-rw-r--r-- 1 root root 2629 Oct 29 08:47 wsdd-discover.nse
-rw-r--r-- 1 root root 2286 Oct 29 08:47 x11-access.nse
-rw-r--r-- 1 root root 2095 Oct 29 08:47 xdmcp-discover.nse
-rw-r--r-- 1 root root 4362 Oct 29 08:47 xmlrpc-methods.nse
-rw-r--r-- 1 root root 4316 Oct 29 08:47 xmpp-brute.nse
-rw-r--r-- 1 root root 17285 Oct 29 08:47 xmpp-info.nse
(maran㉿vbox)-[/]
$
Trash
File System
Home
21:15
Type here to search
30°C Partly sunny
ENG
21:15
04-02-2025
Right Ctrl


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: /
File Actions Edit View Help
(maran㉿vbox)-[/]
$ sudo nmap -sV -p0-1000 --script vulners 198.162.1.1
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 21:18 IST
Nmap scan report for 198.162.1.1
Host is up (0.0032s latency).
Not shown: 1000 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.51
| vulners:
| cpe:/a:thekelleys:dnsmasq:2.51:
| 95499236-C9FE-56A6-9D7D-E943A24B633A 10.0 https://vulners.com/github/exploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
| 2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/github/exploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
| EDB-ID:42943 9.8 https://vulners.com/exploitdb/EDB-ID:42943 *EXPLOIT*
| EDB-ID:42942 9.8 https://vulners.com/exploitdb/EDB-ID:42942 *EXPLOIT*
| EDB-ID:42941 9.8 https://vulners.com/exploitdb/EDB-ID:42941 *EXPLOIT*
| CVE-2017-14493 9.8 https://vulners.com/cve/CVE-2017-14493
| CVE-2017-14492 9.8 https://vulners.com/cve/CVE-2017-14492
| CVE-2017-14491 9.8 https://vulners.com/cve/CVE-2017-14491
| CVE-2020-25682 8.1 https://vulners.com/cve/CVE-2020-25682
| CVE-2020-25681 8.1 https://vulners.com/cve/CVE-2020-25681
| SSV:96623 7.8 https://vulners.com/seebug/SSV:96623 *EXPLOIT*
Trash
File System
Home
21:21
Type here to search
30°C Partly sunny
ENG
21:21
04-02-2025
Right Ctrl


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: /
File Actions Edit View Help
TSTORM:144468 *EXPLOIT*
|_ PACKETSTORM:144462 0.0 https://vulners.com/packetstorm/PACKE
TSTORM:144462 *EXPLOIT*
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.49 seconds
(maran㉿vbox)-[/]
$ sudo nmap -sV -p0-1000 --script vulners 198.162.1.2
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 21:21 IST
Nmap scan report for 198.162.1.2
Host is up (0.0032s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
(maran㉿vbox)-[/]
$
Trash
File System
Home
21:22
Type here to search
30°C Partly sunny
ENG
21:22
04-02-2025
Right Ctrl

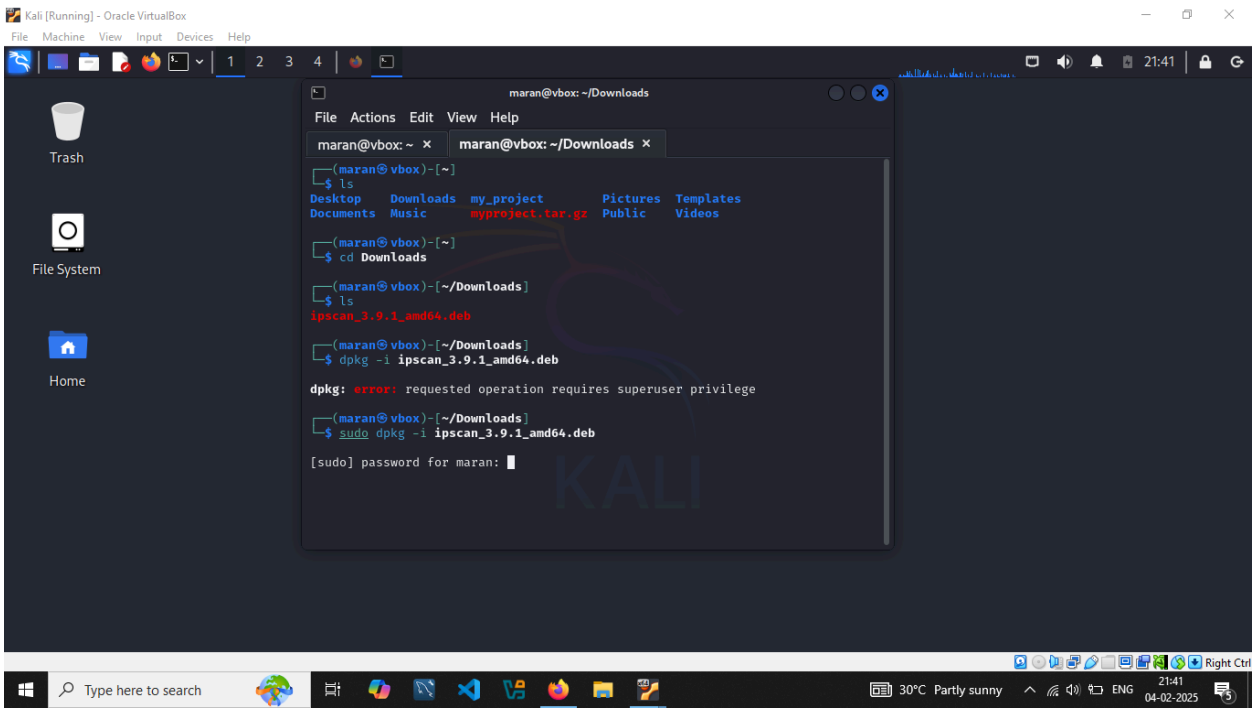

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: /
File Actions Edit View Help
Host is up (0.0032s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
(maran㉿vbox)-[/]
$ sudo nmap -sV -p0-1000 --script vulners 198.162.1.3
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 21:22 IST
Nmap scan report for 198.162.1.3
Host is up (0.00079s latency).
All 1001 scanned ports on 198.162.1.3 are in ignored states.
Not shown: 1001 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:8C:70:90 (Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
(maran㉿vbox)-[/]
$
Trash
File System
Home
21:22
Type here to search
30°C Partly sunny
ENG
21:22
04-02-2025
Right Ctrl

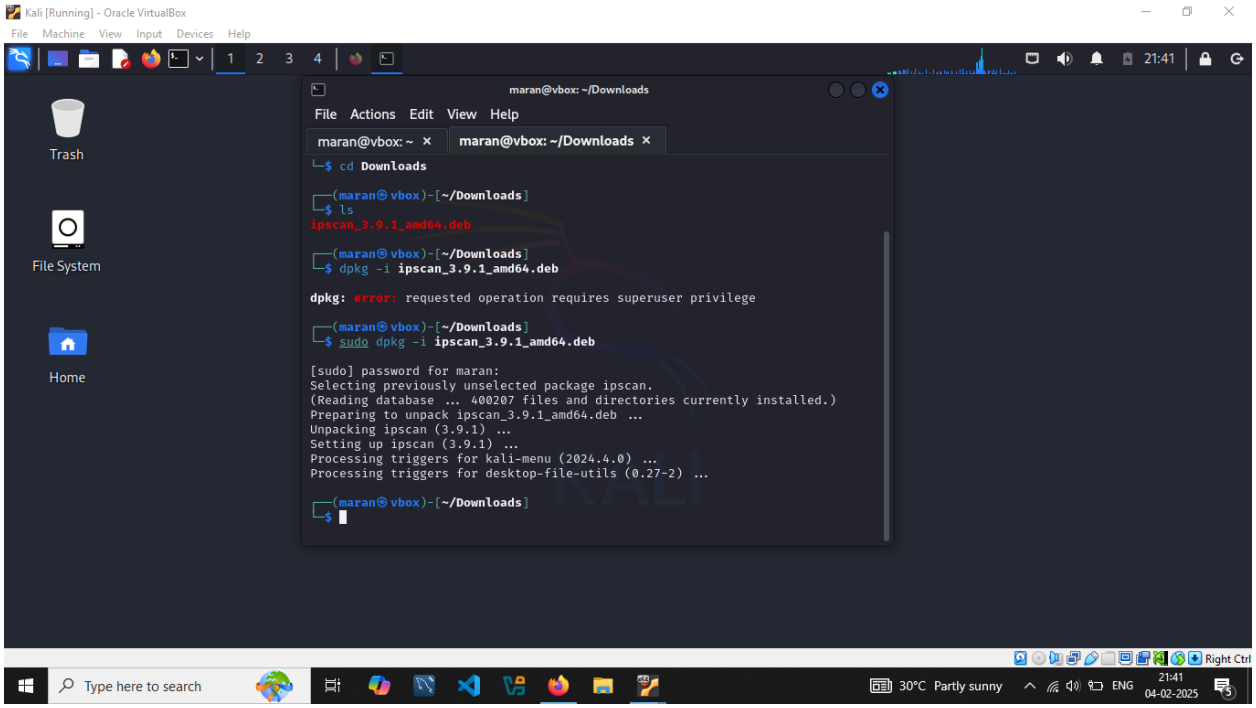

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:23
Trash
File System
Home
maran@vbox: /
File Actions Edit View Help
┌──(maran㉿vbox)-[/]
└─$ sudo nmap -sV -p0-1000 --script vulners 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 21:22 IST
Nmap scan report for 198.162.1.6
Host is up (0.0023s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| vulners:
| vsftpd 2.3.4:
| PACKETSTORM:162145 10.0 https://vulners.com/packetstorm/PACKETSTORM:162145 *EXPLOIT*
| EDB-ID:49757 9.8 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
| CVE-2011-2523 9.8 https://vulners.com/cve/CVE-2011-2523
|_ 1337DAY-ID-36095 9.8 https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:4.7p1:
| 95499236-C9FE-56A6-9D7D-E943A24B633A 10.0 https://vulners.com/github/exploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
| 2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/github/exploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
| CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/g
Right Ctrl
Type here to search
30°C Partly sunny
ENG
21:23
04-02-2025

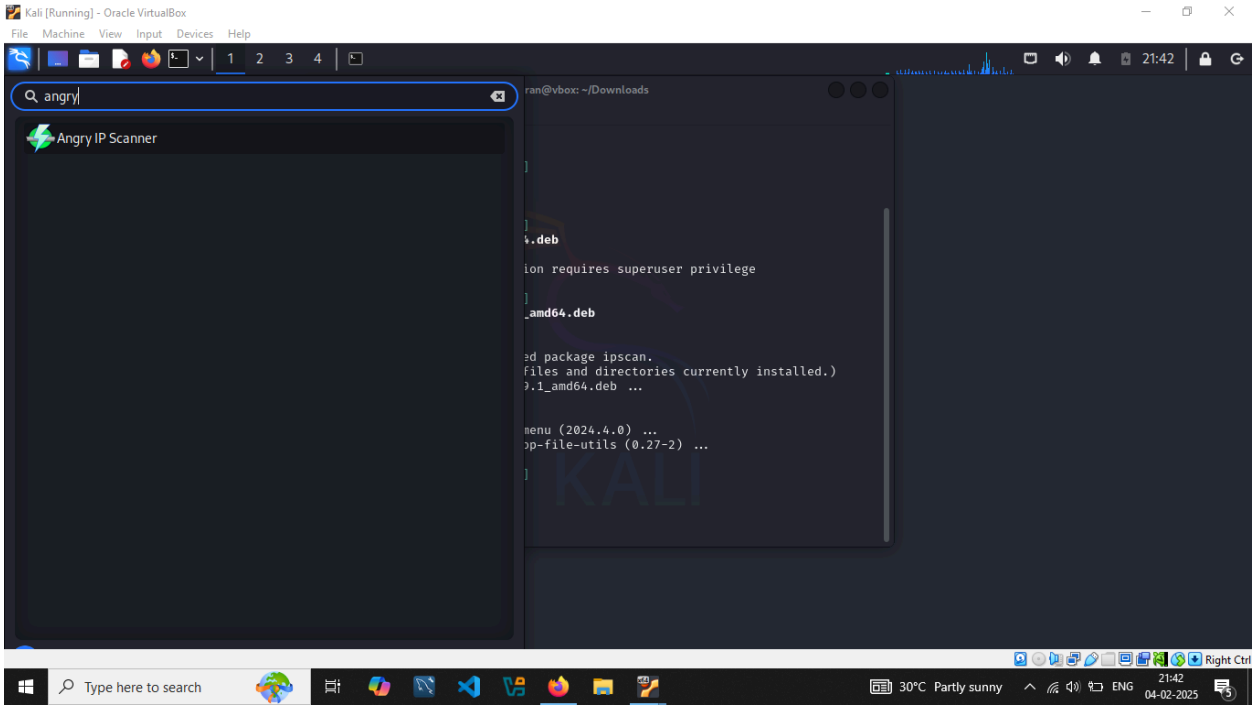
8.Performed network scanning with other tool (Angry Ip scanner):

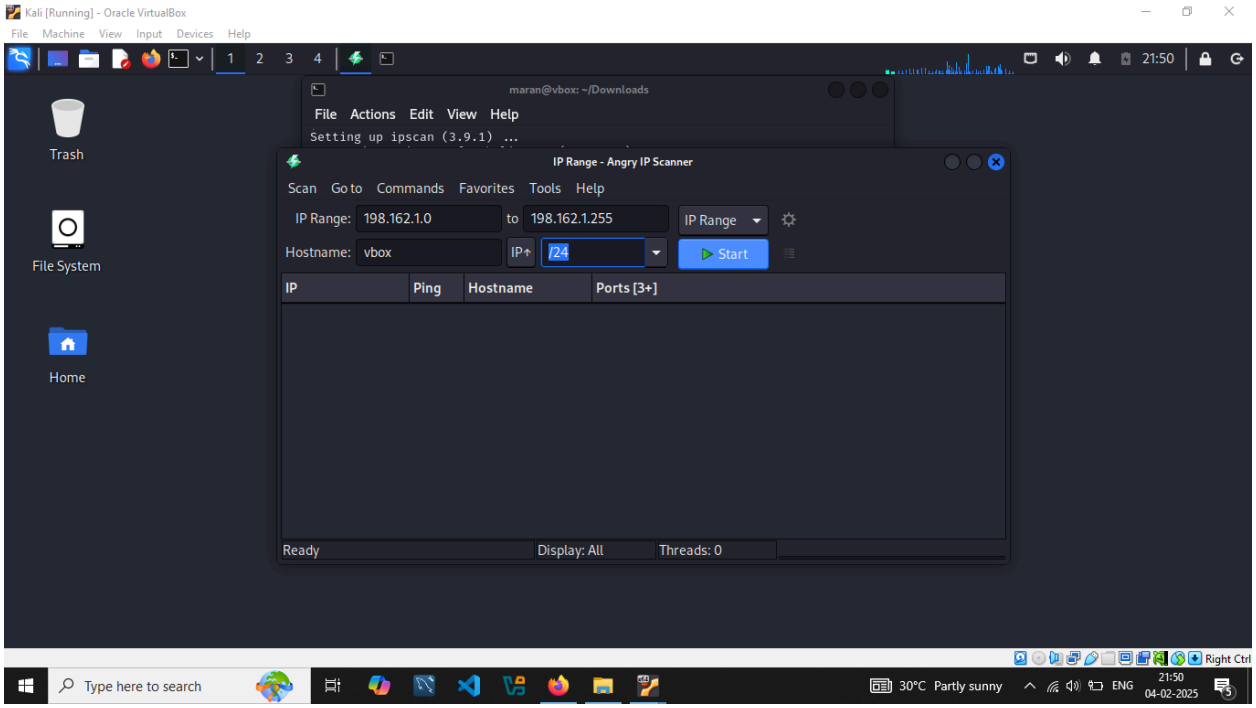
- Opened firefox in the kali linux entering Angry IP Scanner - Download for Windows, Mac or Linux to download angry ip scanner.
- Downloading `x86 64-bit DEB Package` for my kali linux operating system as specified in the website.
- Navigating to `Downloads` directory `cd` command in the kali linux.
- Using `ls` command to list the items in the Downloads directory there is a package named `ipscan_3.9.1_amd64.deb` which is the package of Angry IP Scanner.
- To install the Angry IP Scanner package using the `dpkg` command, which is a depackage tool.
- Enter the command `sudo dpkg -i ipscan_3.9.1_amd64.deb` to install the Angry IP Scanner tool.
- After installing the tool, searching it in the search bar using the keyword `angry`.
- Opening the Angry IP Scanner tool to scan the network, entering the target ip range `198.162.1.1` to `198.162.1.255` entering subnet mask as `/24` starting the scan by clicing the start button.
- Angry IP Scanner is scanning the network and giving the `scan statistics` after completing the scan.
- Scan statistics shows time taken for the scan, number of hosts scanned, alive hosts and hosts with open ports.
- In my scan statistics `time taken for the scan is 16.21 sec`, `number of hosts scanned is 254`, `alive hosts 6` and `hosts with open ports is 1`.
- The red dotted ip addresses are not active, green dotted ip addresses are active hosts, blue dotted ip addresses are their own system.

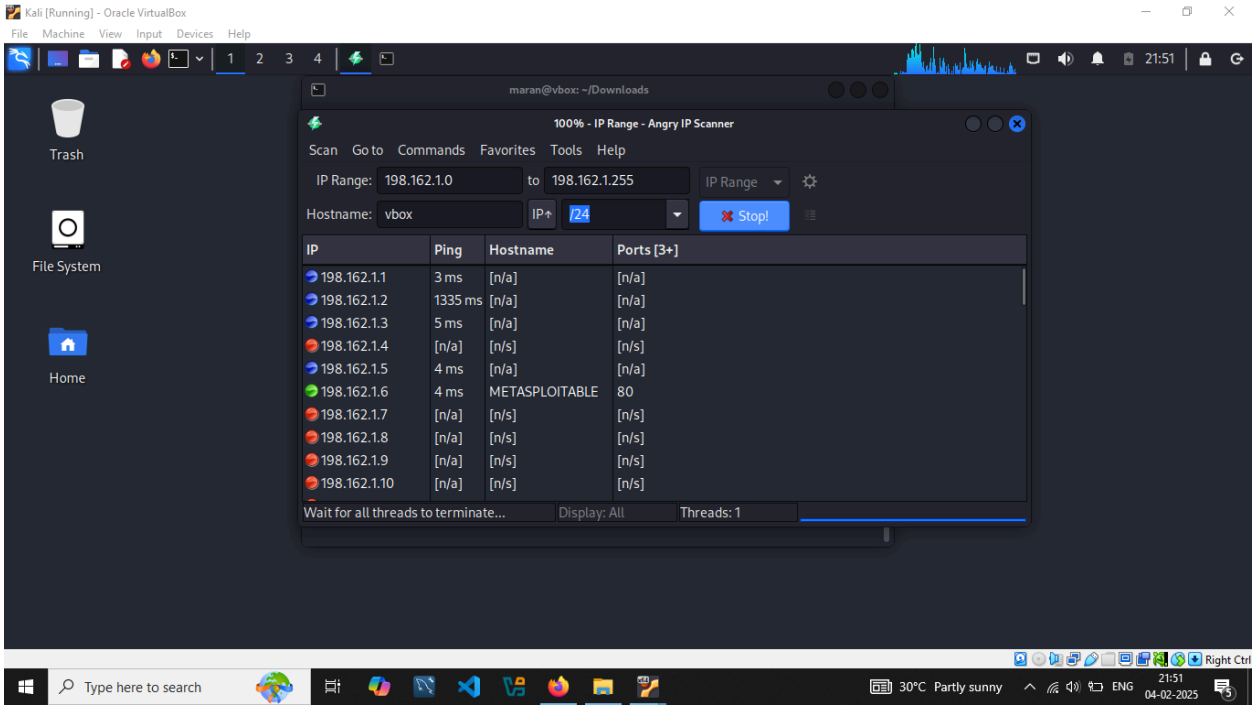
Screenshots:

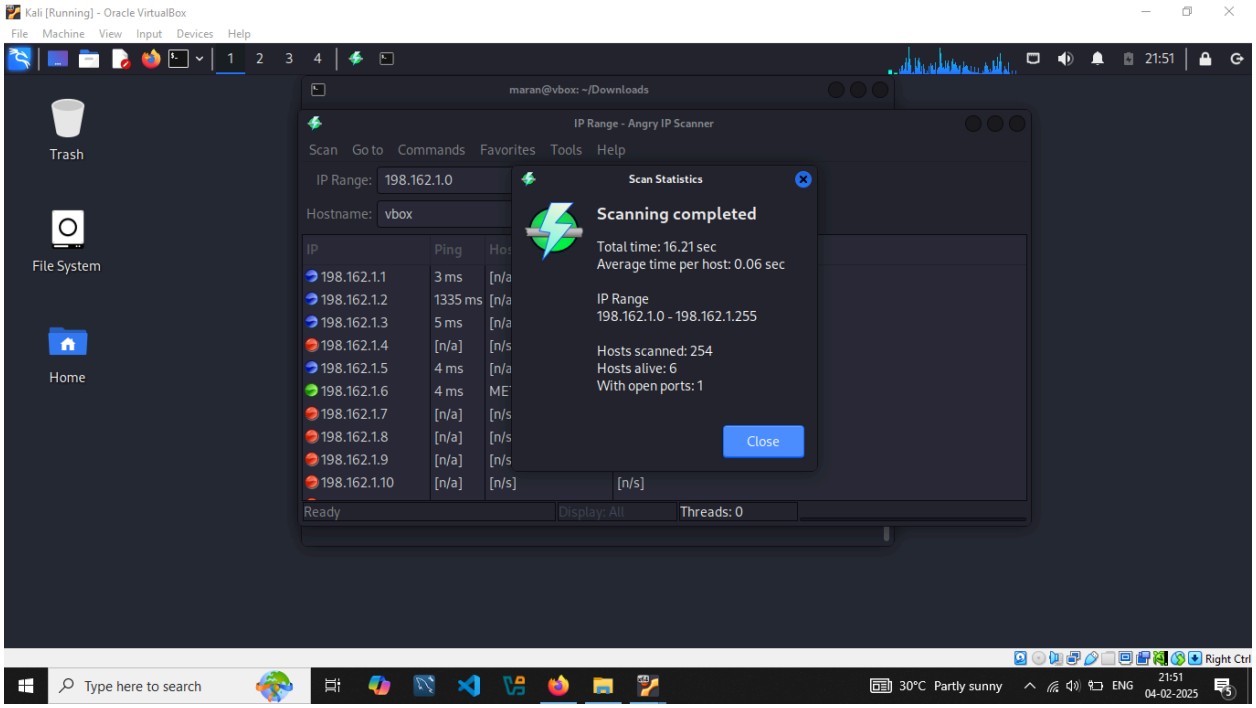


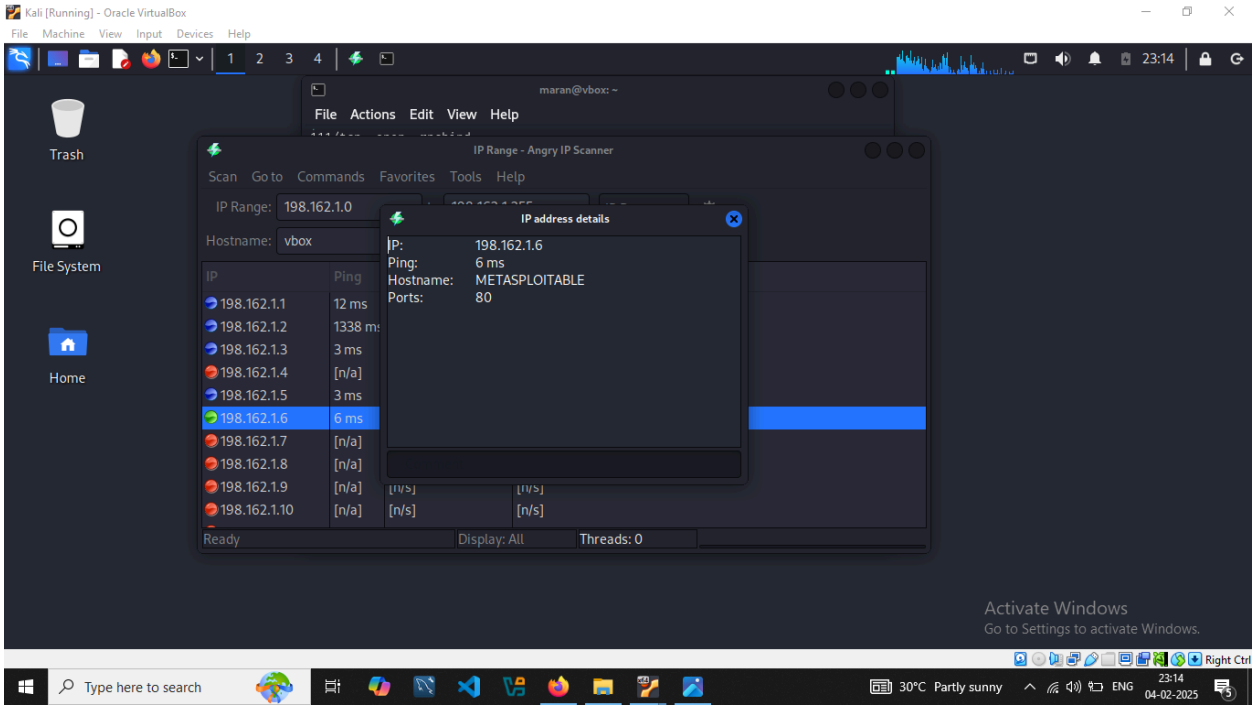

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:41
Trash
File System
Home
maran@vbox: ~/Downloads
File Actions Edit View Help
maran@vbox: ~
maran@vbox: ~/Downloads
└─$ cd Downloads
┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb
┌──(maran㉿vbox)-[~/Downloads]
└─$ dpkg -i ipscan_3.9.1_amd64.deb
dpkg: error: requested operation requires superuser privilege
┌──(maran㉿vbox)-[~/Downloads]
└─$ sudo dpkg -i ipscan_3.9.1_amd64.deb
[sudo] password for maran:
Selecting previously unselected package ipscan.
(Reading database ... 400207 files and directories currently installed.)
Preparing to unpack ipscan_3.9.1_amd64.deb ...
Unpacking ipscan (3.9.1) ...
Setting up ipscan (3.9.1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for desktop-file-utils (0.27-2) ...
┌──(maran㉿vbox)-[~/Downloads]
└─$
Right Ctrl
Type here to search
30°C Partly sunny
ENG
21:41
04-02-2025

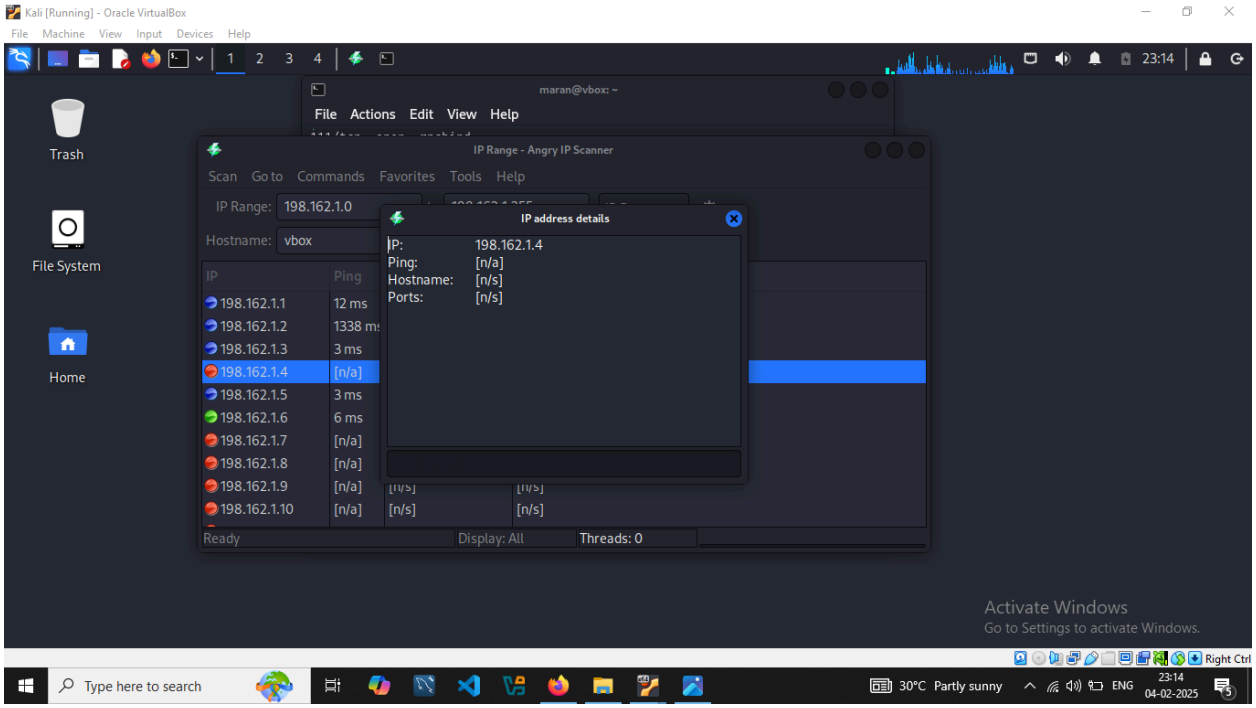

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:42
angry
Angry IP Scanner
Right Ctrl
Type here to search
30°C Partly sunny
ENG
21:42
04-02-2025

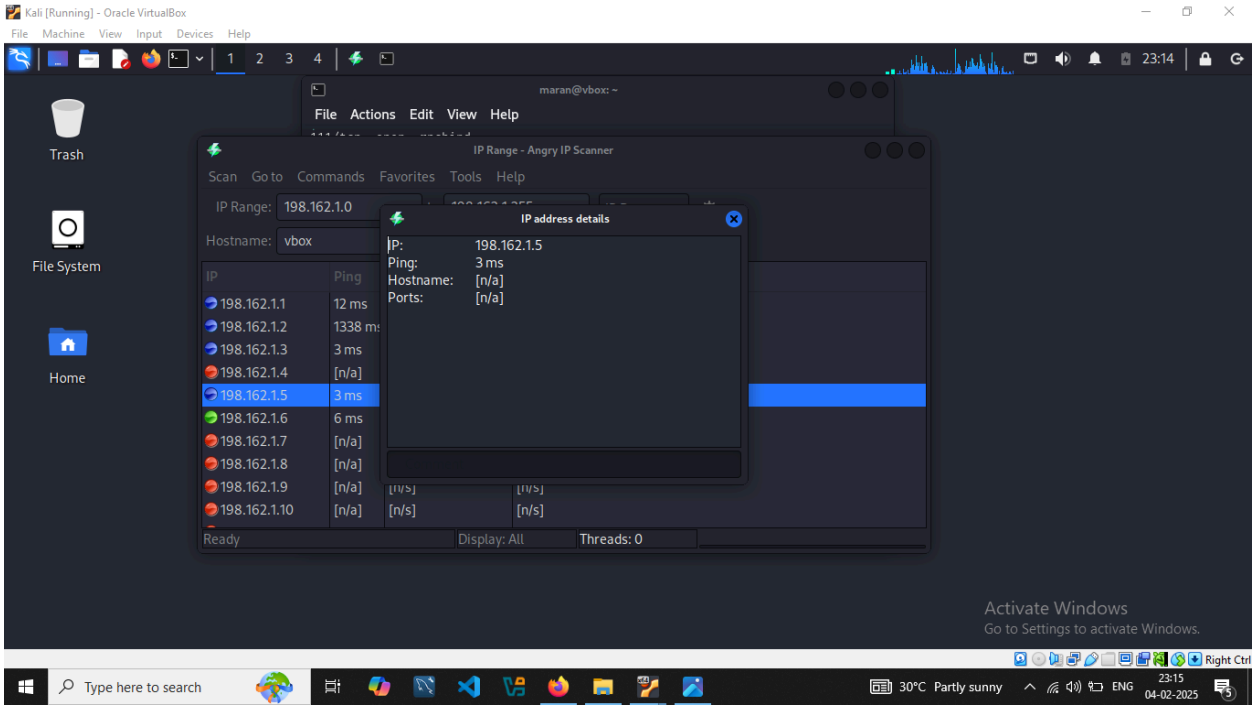

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:50
Trash
File System
Home
maran@vbox: ~/Downloads
File Actions Edit View Help
Setting up ipscan (3.9.1) ...
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 198.162.1.0 to 198.162.1.255
IP Range
Hostname: vbox
IP↑
/24
Start
IP Ping Hostname Ports [3+]
Ready
Display: All
Threads: 0
Right Ctrl
Type here to search
30°C Partly sunny
ENG
21:50
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:51
Trash
File System
Home
maran@vbox: ~/Downloads
100% - IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 198.162.1.0 to 198.162.1.255
IP Range
Hostname: vbox
IP↑
/24
Stop!
IP Ping Hostname Ports [3+]
198.162.1.1 3 ms [n/a] [n/a]
198.162.1.2 1335 ms [n/a] [n/a]
198.162.1.3 5 ms [n/a] [n/a]
198.162.1.4 [n/a] [n/s] [n/s]
198.162.1.5 4 ms [n/a] [n/a]
198.162.1.6 4 ms METASPLOITABLE 80
198.162.1.7 [n/a] [n/s] [n/s]
198.162.1.8 [n/a] [n/s] [n/s]
198.162.1.9 [n/a] [n/s] [n/s]
198.162.1.10 [n/a] [n/s] [n/s]
Wait for all threads to terminate...
Display: All
Threads: 1
Right Ctrl
Type here to search
30°C Partly sunny
ENG
21:51
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:51
maran@vbox: ~/Downloads
Trash
File System
Home
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 198.162.1.0
Hostname: vbox
Scan Statistics
Scanning completed
Total time: 16.21 sec
Average time per host: 0.06 sec
IP Range
198.162.1.0 - 198.162.1.255
Hosts scanned: 254
Hosts alive: 6
With open ports: 1
Close
IP Ping
198.162.1.1 3 ms
198.162.1.2 1335 ms
198.162.1.3 5 ms
198.162.1.4 [n/a]
198.162.1.5 4 ms
198.162.1.6 4 ms
198.162.1.7 [n/a]
198.162.1.8 [n/a]
198.162.1.9 [n/a]
198.162.1.10 [n/a]
[n/s]
Ready
Display: All
Threads: 0
Right Ctrl
Type here to search
30°C Partly sunny
ENG
21:51
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
23:14
maran@vbox: ~
File Actions Edit View Help
Trash
File System
Home
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 198.162.1.0
Hostname: vbox
IP address details
IP: 198.162.1.6
Ping: 6 ms
Hostname: METASPLOITABLE
Ports: 80
IP Ping
198.162.1.1 12 ms
198.162.1.2 1338 ms
198.162.1.3 3 ms
198.162.1.4 [n/a]
198.162.1.5 3 ms
198.162.1.6 6 ms
198.162.1.7 [n/a]
198.162.1.8 [n/a]
198.162.1.9 [n/a]
198.162.1.10 [n/a]
[n/s]
Ready
Display: All
Threads: 0
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
Type here to search
30°C Partly sunny
ENG
23:14
04-02-2025

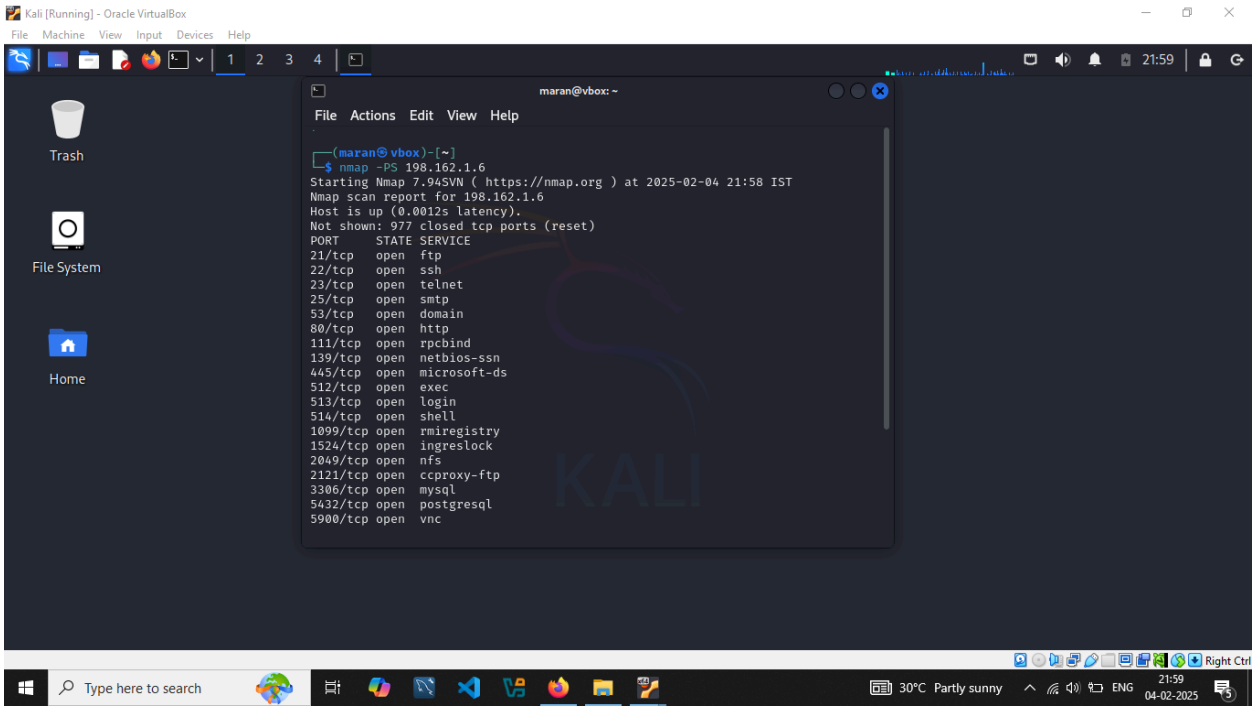

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 198.162.1.0
Hostname: vbox
IP address details
IP: 198.162.1.4
Ping: [n/a]
Hostname: [n/s]
Ports: [n/s]
198.162.1.1 12 ms
198.162.1.2 1338 ms
198.162.1.3 3 ms
198.162.1.4 [n/a]
198.162.1.5 3 ms
198.162.1.6 6 ms
198.162.1.7 [n/a]
198.162.1.8 [n/a]
198.162.1.9 [n/a]
198.162.1.10 [n/a]
Ready
Display: All
Threads: 0
Trash
File System
Home
Activate Windows
Go to Settings to activate Windows.
Type here to search
30°C Partly sunny
ENG
23:14
04-02-2025

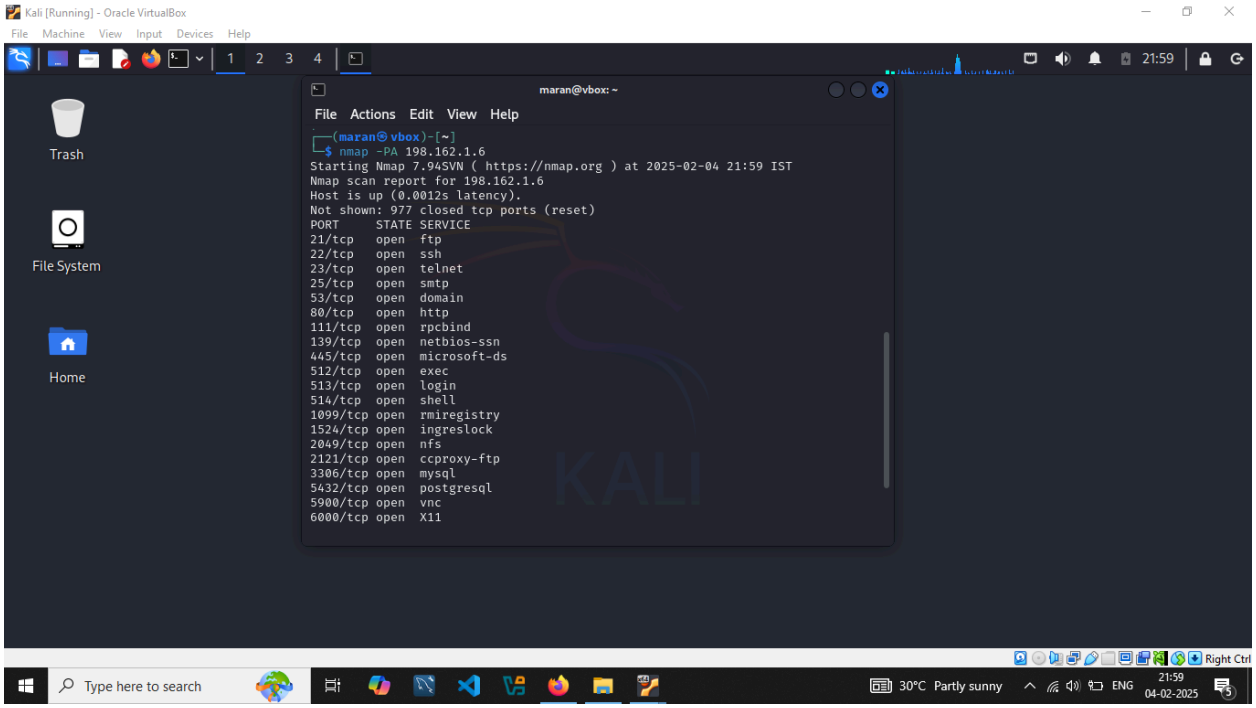

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 198.162.1.0
Hostname: vbox
IP address details
IP: 198.162.1.5
Ping: 3 ms
Hostname: [n/a]
Ports: [n/a]
198.162.1.1 12 ms
198.162.1.2 1338 ms
198.162.1.3 3 ms
198.162.1.4 [n/a]
198.162.1.5 3 ms
198.162.1.6 6 ms
198.162.1.7 [n/a]
198.162.1.8 [n/a]
198.162.1.9 [n/a]
198.162.1.10 [n/a]
Ready
Display: All
Threads: 0
Trash
File System
Home
Activate Windows
Go to Settings to activate Windows.
Type here to search
30°C Partly sunny
ENG
23:15
04-02-2025

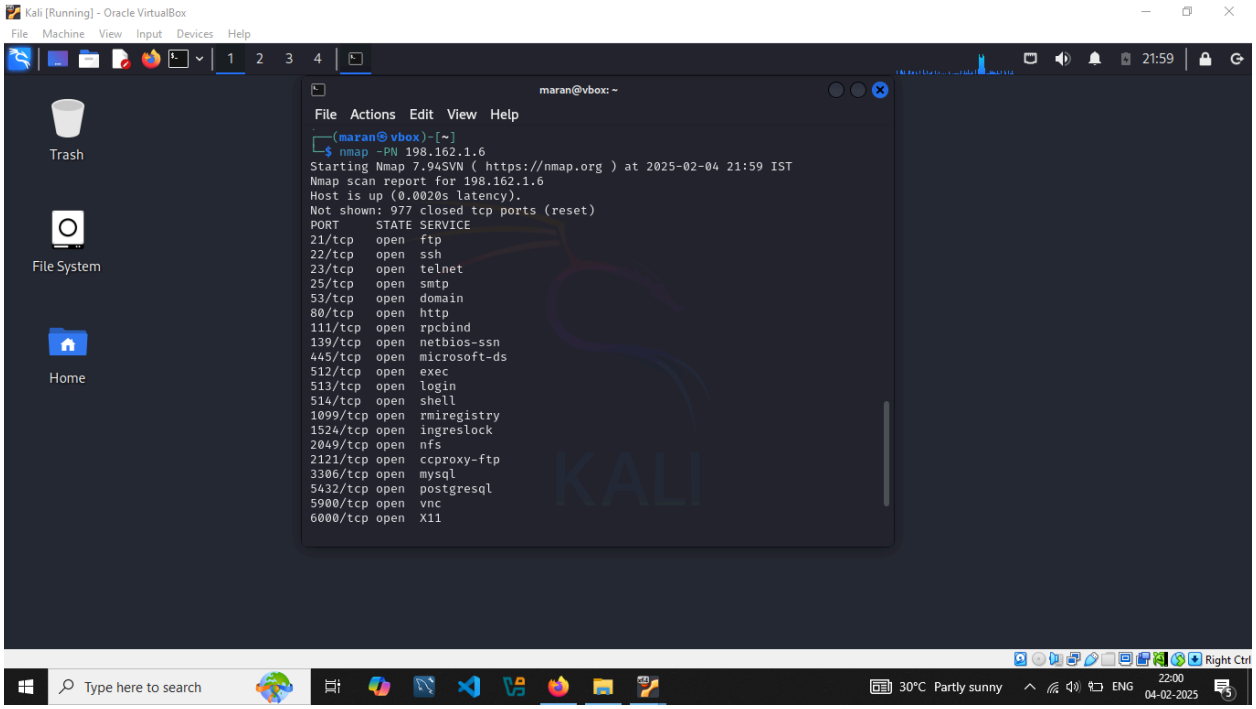
9.Perform 5 more active scans using nmap and record what you had analyzed from it:

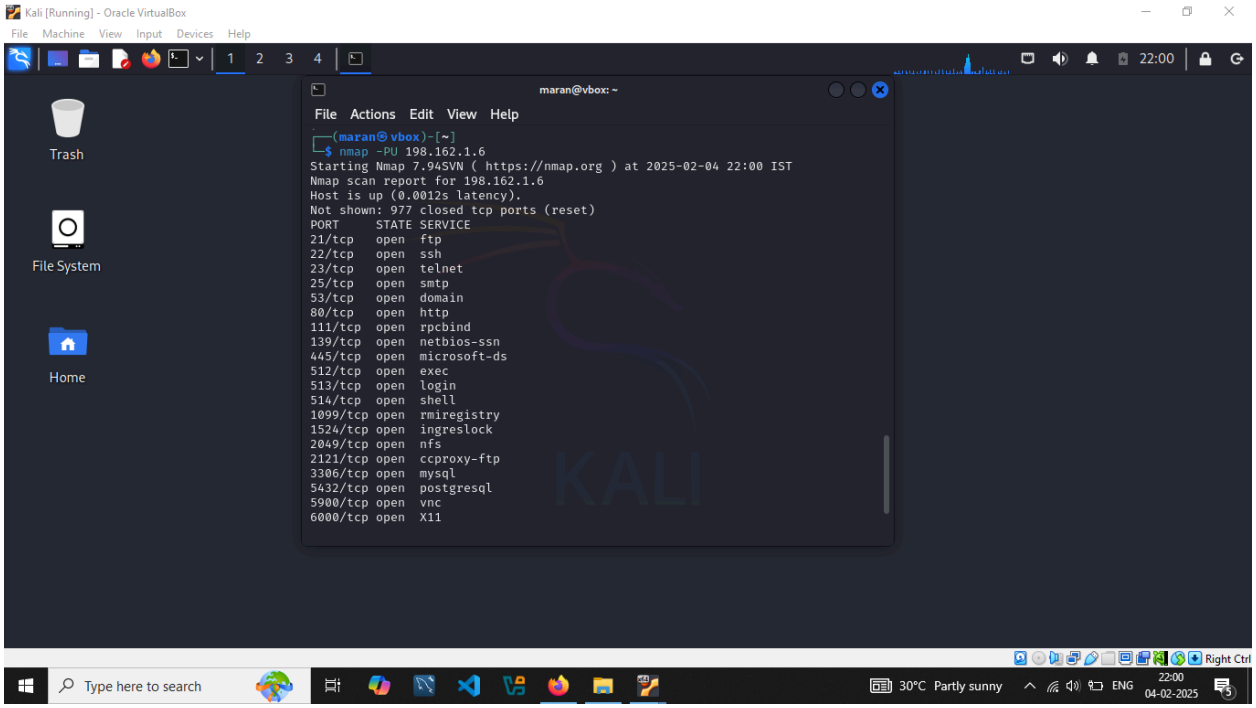
- Performing TCP SYN Ping scan with the Metasploitable host 198.162.1.6 using command `nmap -PS 198.162.1.6`.
- Performing TCP ACK Ping scan with the Metasploitable host 198.162.1.6 using command `nmap -PA 198.162.1.6`.
- Performing Dont Ping scan with the Metasploitable host 198.162.1.6 using command `nmap -PN 198.162.1.6`.
- Performing UDP scan with the Metasploitable host 198.162.1.6 using command `nmap -PU 198.162.1.6`.
- Performing Ping scan only with the Metasploitable host 198.162.1.6 using command `nmap -sP 198.162.1.6`.
- Performing nmap traceroute with the Metasploitable host 198.162.1.6 using command `nmap -traceroute 198.162.1.6`.
- I have done different types of scans with the Metasploitable host 198.162.1.6, every scan has their uniqueness in the scanning activity but with this limited environment these scans all perform in a similar way this is my analysis of these scan records.

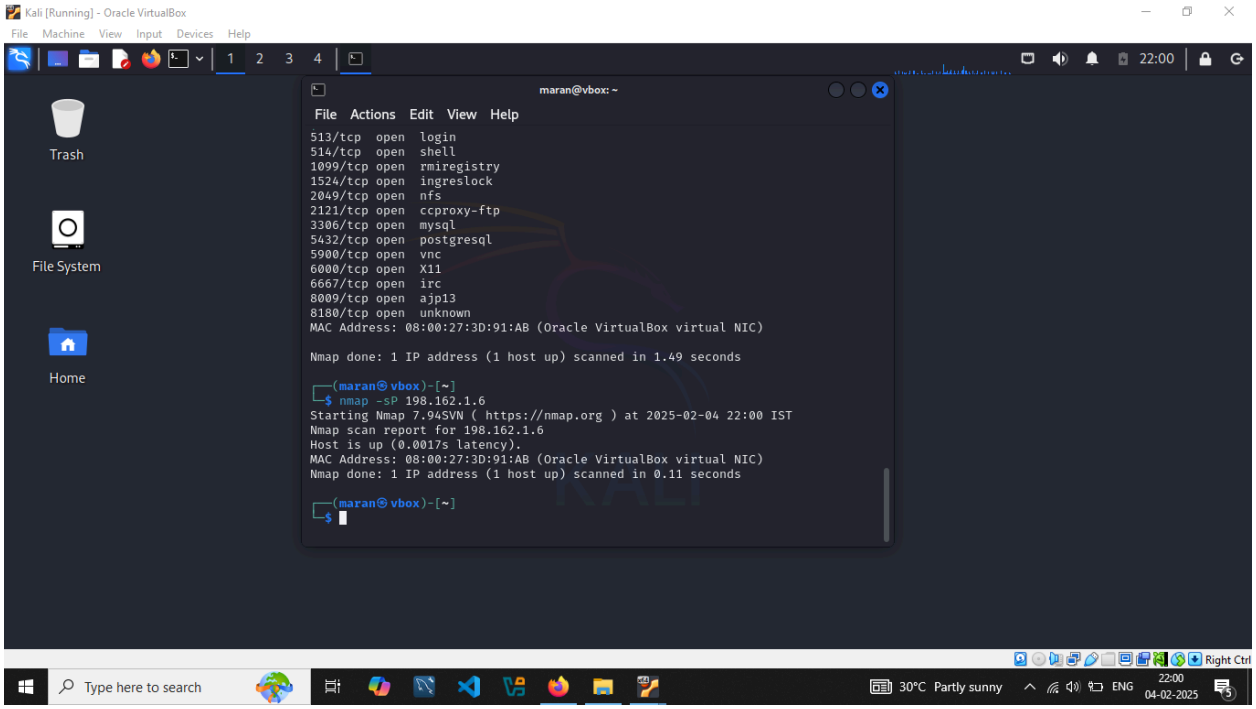
Screenshots:

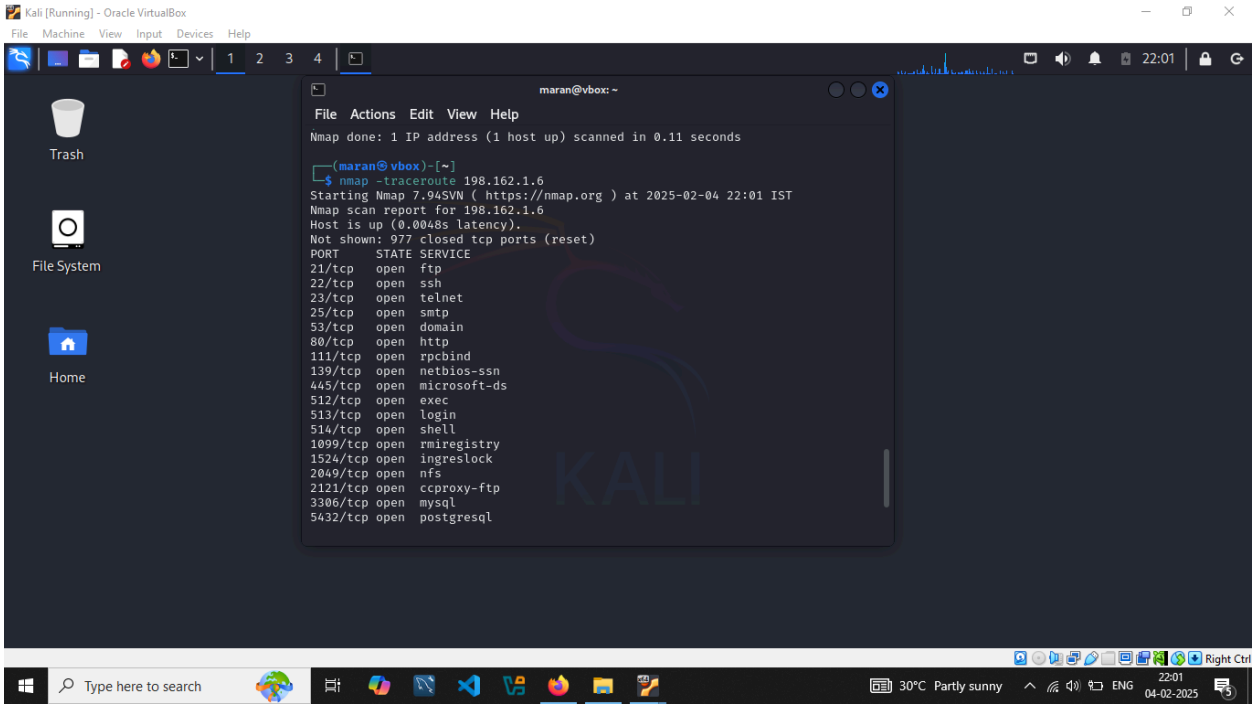


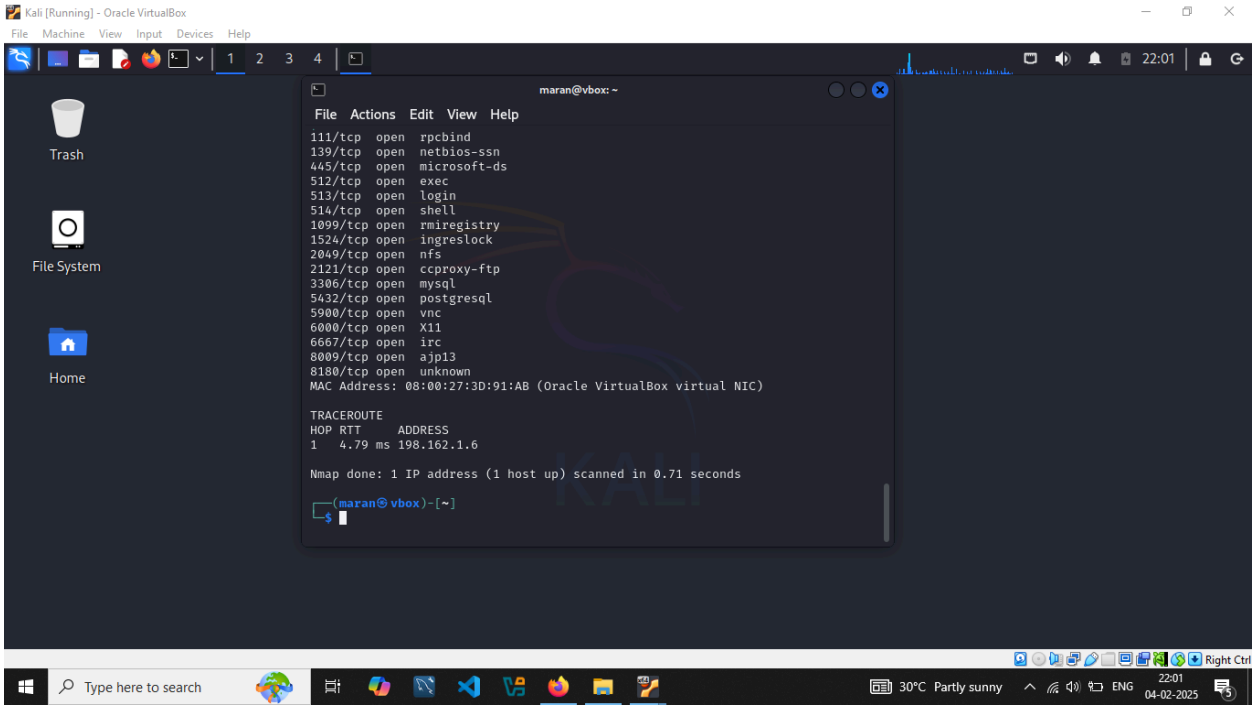

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:59
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ nmap -PA 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 21:59 IST
Nmap scan report for 198.162.1.6
Host is up (0.0012s 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
Right Ctrl
Type here to search
30°C Partly sunny
ENG
21:59
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:59
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ nmap -PN 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 21:59 IST
Nmap scan report for 198.162.1.6
Host is up (0.0020s 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
Right Ctrl
Type here to search
30°C Partly sunny
ENG
22:00
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
(maran㉿vbox)-[~]
$ nmap -PU 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 22:00 IST
Nmap scan report for 198.162.1.6
Host is up (0.0012s 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
Trash
File System
Home
Type here to search
30°C Partly sunny
ENG
22:00
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
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: 08:00:27:3D:91:AB (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
(maran㉿vbox)-[~]
$ nmap -sP 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 22:00 IST
Nmap scan report for 198.162.1.6
Host is up (0.0017s latency).
MAC Address: 08:00:27:3D:91:AB (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(maran㉿vbox)-[~]
$
Trash
File System
Home
Type here to search
30°C Partly sunny
ENG
22:00
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(maran㉿vbox)-[~]
$ nmap -traceroute 198.162.1.6
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-04 22:01 IST
Nmap scan report for 198.162.1.6
Host is up (0.0048s 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
Trash
File System
Home
Type here to search
30°C Partly sunny
ENG
22:01
04-02-2025


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~
File Actions Edit View Help
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: 08:00:27:3D:91:AB (Oracle VirtualBox virtual NIC)
TRACEROUTE
HOP RTT ADDRESS
1 4.79 ms 198.162.1.6
Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
(maran㉿vbox)-[~]
$
Trash
File System
Home
Type here to search
30°C Partly sunny
ENG
22:01
04-02-2025

Results of comparisons:

- Nmap:
    I. Nmap is an advanced, well known network scanner tool used for almost every network scanning activity and vulnerability assessment with pre-installed scripts.
    II. It's open source and free.
    III. Usable with the command line, need knowledge about terminal before getting started.

- Angry IP Scanner:
    I. It has a GUI interface.
    II. Showing scan statistics after completing the scan, Suitable for beginners to start and gain knowledge.
    III. It's open source and free.
    IV. It has lots of limitations compared to nmap.