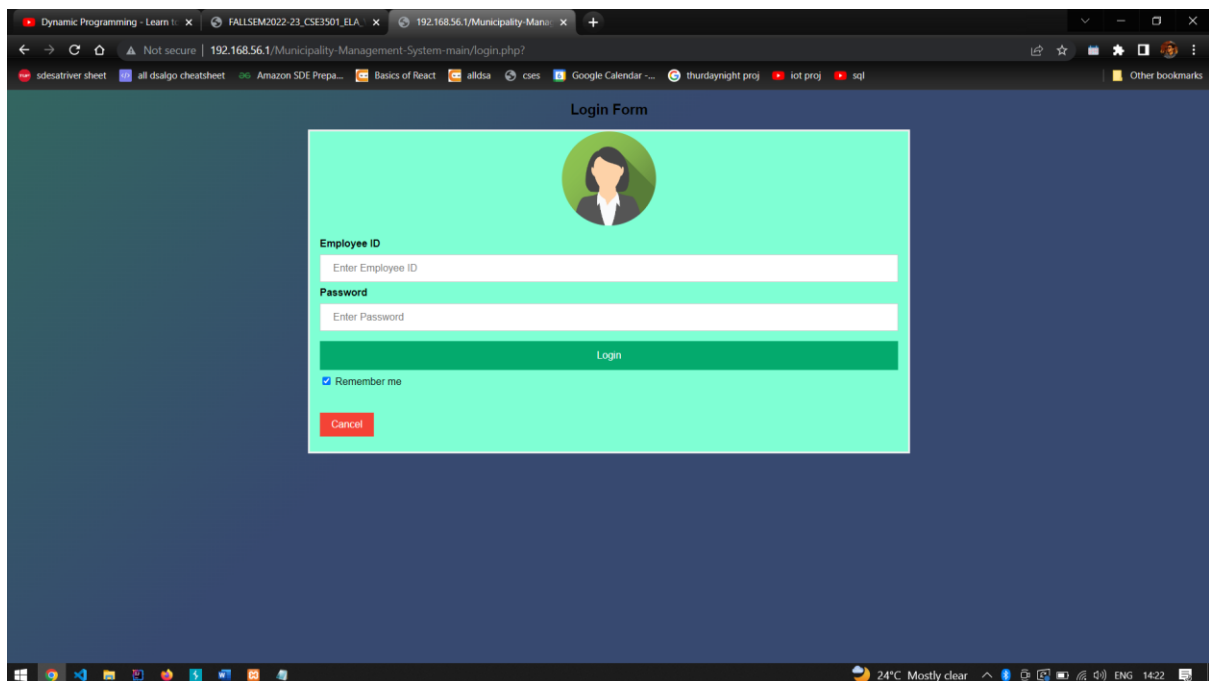


# ISA LAB ASSIGNMENT -5

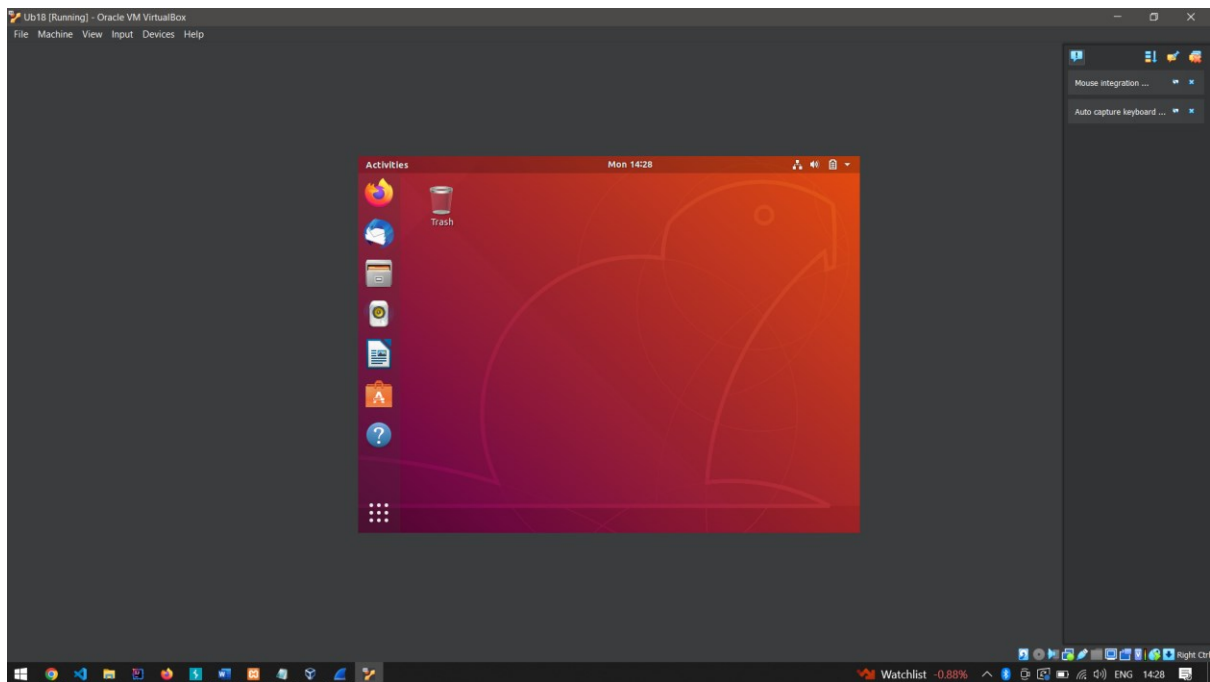
Name: Abhay Rathi

20BCE2905

HOSTING A RANDOM PROJECT ON IP: [192.168.56.1](http://192.168.56.1)



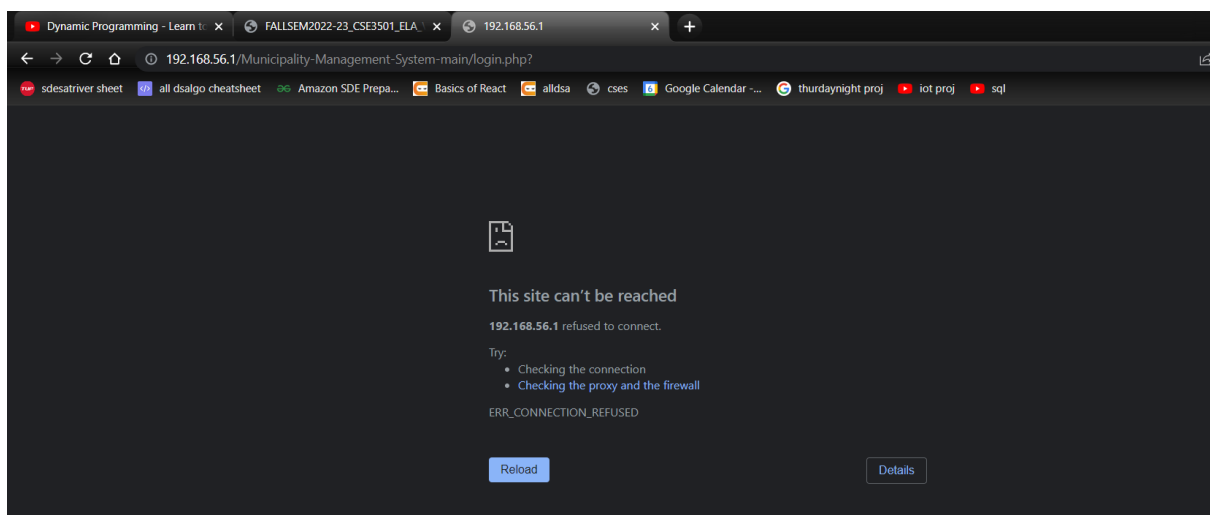
Now running ubuntu on vmbox



Now in command terminal of ubuntu

```
root@Ub18:/home/vboxuser# ^C
root@Ub18:/home/vboxuser# hping3 -S 192.168.56.1 -d 120 -p 80 --flood --rand-source
HPING 192.168.56.1 (enp0s3 192.168.56.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Project:



Confirming through wireshark

| * Adapter for loopback traffic capture                                     |            |              |              |          |        |  |  |
|--|------------|--------------|--------------|----------|--------|--|--|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help |            |              |              |          |        |  |  |
| [ip.addr == 192.168.56.1]  |            |              |              |          |        |  |  |
| No.  | Time       | Source       | Destination  | Protocol | Length | Info   |  |
| 99010  | 708.777374 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61900 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99011  | 708.777395 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61900 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99012  | 708.782050 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61901 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99013  | 708.782139 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99014  | 708.785074 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61902 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99015  | 708.785099 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61902 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99016  | 708.792632 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61903 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99017  | 708.792662 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61903 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99018  | 708.793885 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61904 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99019  | 708.793908 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99020  | 708.801189 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61905 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99021  | 708.801235 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61905 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99022  | 708.810914 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61906 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99023  | 708.810939 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61906 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99024  | 708.810977 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61907 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99025  | 708.810996 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61907 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99026  | 708.813841 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61908 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99027  | 708.813885 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61908 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99028  | 708.817717 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61909 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99029  | 708.817740 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61909 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |
| 99030  | 708.920145 | 192.168.56.1 | 192.168.56.1 | TCP      | 56     | [TCP Retransmission] [TCP Port numbers reused] 61910 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 S |  |
| 99031  | 708.920177 | 192.168.56.1 | 192.168.56.1 | TCP      | 44     | 80 → 61910 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0  |  |

After attack:

# Wi-Fi Qualcomm QCA61x4A 802.11ac Wireless Ada...

Throughput

100 Kbps



60 seconds

0

Send  
0 Kbps

Receive  
0 Kbps

Adapter name: Wi-Fi  
SSID: I am God  
Connection type: 802.11n  
IPv4 address: 192.168.183.120  
IPv6 address: -  
Signal strength:

ARP spoofing

```
root@Ub18:/home/vboxuser# ip r
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
root@Ub18:/home/vboxuser#
```

Default gateway ip is 10.0.2.2

Let's say we need to know victim ip of 10.0.2

So

"ifconfig" to know the interface and mac id we are using

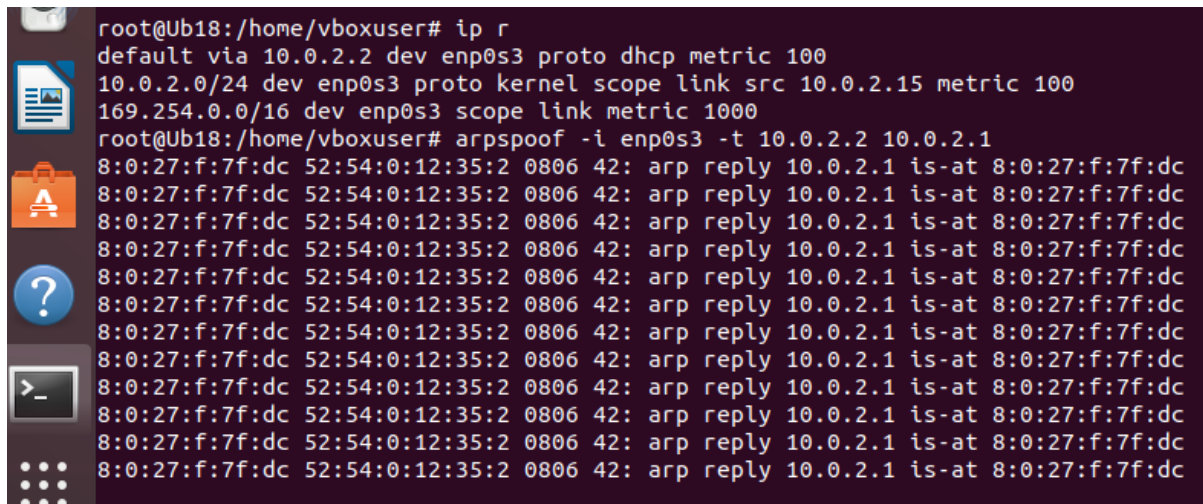
```
root@Ub18:/home/vboxuser# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::ef10:44ae:6e7b:3794 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0f:7f:dc txqueuelen 1000 (Ethernet)
    RX packets 353373 bytes 154290868 (154.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 330196 bytes 27222921 (27.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 309 bytes 26629 (26.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 309 bytes 26629 (26.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

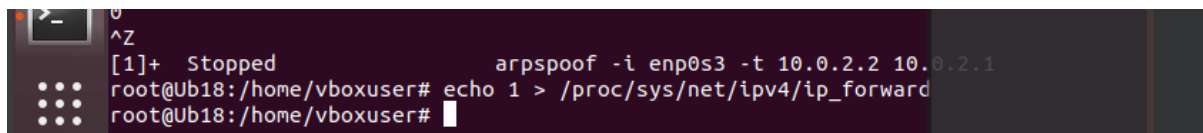
root@Ub18:/home/vboxuser#
```

Mac id: is 08:00::27:0f:7f:dc

Interface: lo



```
root@Ub18:/home/vboxuser# ip r
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
root@Ub18:/home/vboxuser# arpspoof -i enp0s3 -t 10.0.2.2 10.0.2.1
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
8:0:27:f:7f:dc 52:54:0:12:35:2 0806 42: arp reply 10.0.2.1 is-at 8:0:27:f:7f:dc
```



```
0
^Z
[1]+  Stopped                  arpspoof -i enp0s3 -t 10.0.2.2 10.0.2.1
root@Ub18:/home/vboxuser# echo 1 > /proc/sys/net/ipv4/ip_forward
root@Ub18:/home/vboxuser#
```

Before spoofing

```
Interface: 172.16.102.53 --- 0x11
  Internet Address      Physical Address      Type
  172.16.96.1           00-15-17-c8-09-b0    dynamic
  172.16.103.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.2             01-00-5e-00-00-02    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

After spoofing

```
Microsoft Windows [Version 10.0.19045.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Dell>arp -a

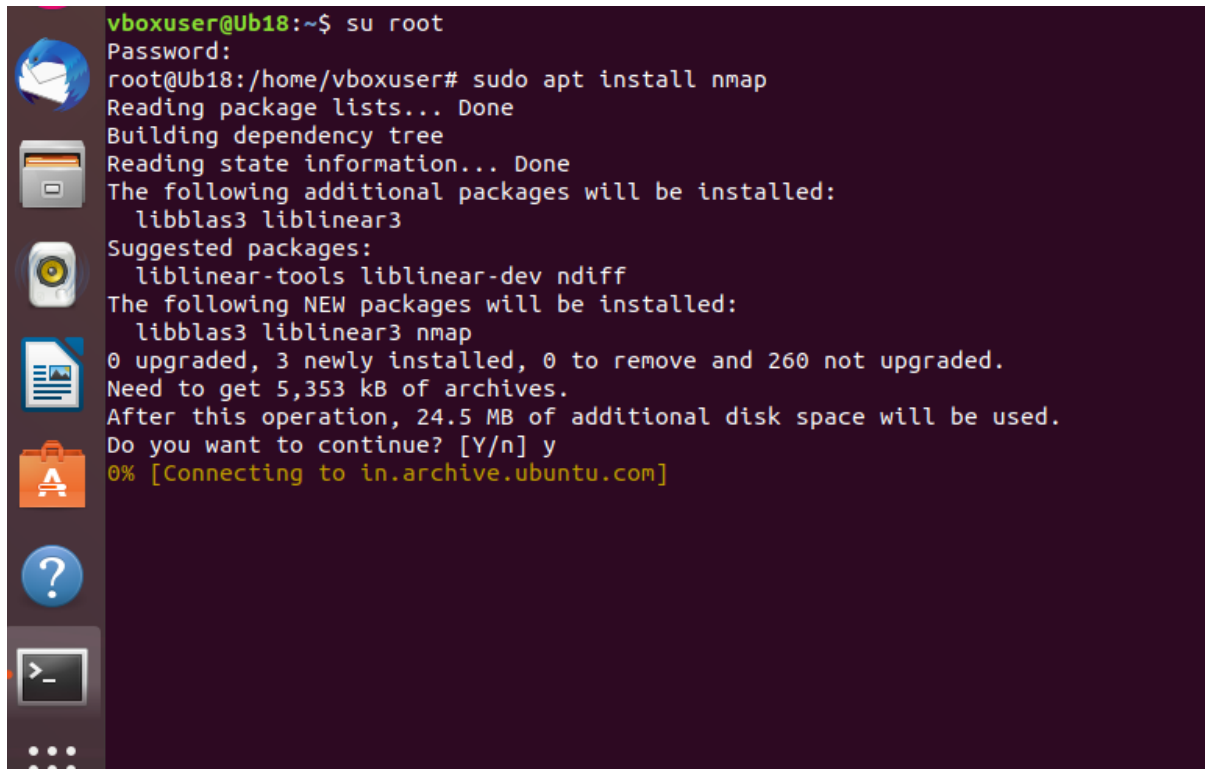
Interface: 172.16.102.53 --- 0x11
  Internet Address      Physical Address      Type
  172.16.96.1           00-15-17-c8-09-b0    dynamic
  172.16.103.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.2             01-00-5e-00-00-02    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x14
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.2             01-00-5e-00-00-02    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Dell>
```

Nmap tool

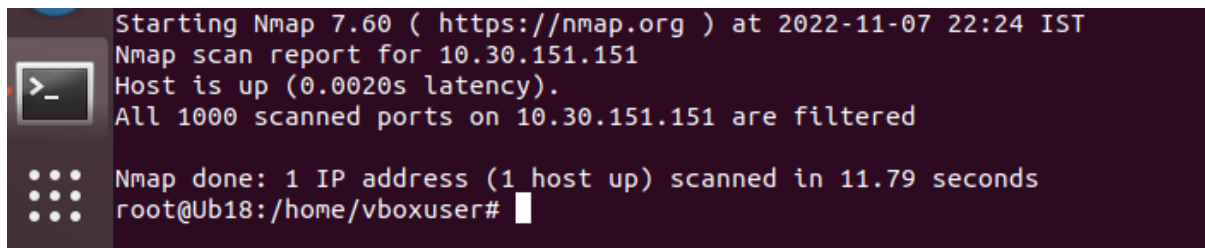
Sudo apt install nmap

A terminal window with a dark purple background and a sidebar on the left containing various application icons. The terminal text shows a user switching to root and installing nmap using apt. The output lists additional packages to be installed, suggested packages, and the disk space requirements. The installation is confirmed with 'y' and shows progress at 0% connecting to the archive.

```
vboxuser@Ub18:~$ su root
Password:
root@Ub18:/home/vboxuser# sudo apt install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear3
Suggested packages:
  liblinear-tools liblinear-dev ndiff
The following NEW packages will be installed:
  libblas3 liblinear3 nmap
0 upgraded, 3 newly installed, 0 to remove and 260 not upgraded.
Need to get 5,353 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
0% [Connecting to in.archive.ubuntu.com]
```

Scanning a single ip:

10.30.151.150

A terminal window showing the output of an Nmap scan. The text indicates that Nmap 7.60 was started at 2022-11-07 22:24 IST. The scan report for 10.30.151.151 shows the host is up with a latency of 0.0020s. All 1000 scanned ports are filtered. The scan took 11.79 seconds to complete.


```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:24 IST
Nmap scan report for 10.30.151.151
Host is up (0.0020s latency).
All 1000 scanned ports on 10.30.151.151 are filtered

Nmap done: 1 IP address (1 host up) scanned in 11.79 seconds
root@Ub18:/home/vboxuser#
```



Scan a host:

[www.facebook.com](http://www.facebook.com)

A terminal window with a dark purple background and light blue text. The window shows the output of Nmap scans. The first scan is for the IP address 10.30.151.151, which is up and has all 1000 scanned ports filtered. The second scan is for the domain www.facebook.com, which is up and has ports 80/tcp (http) and 443/tcp (https) open. The terminal also shows the installation of Nmap and the setup of triggers for man-db and libc-bin.

```
to mode
Setting up liblinear3:amd64 (2.1.0+dfsg-2) ...
Setting up nmap (7.60-1ubuntu5) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.4) ...
root@Ub18:/home/vboxuser# nmap 10.30.151.151

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:24 IST
Nmap scan report for 10.30.151.151
Host is up (0.0020s latency).
All 1000 scanned ports on 10.30.151.151 are filtered

Nmap done: 1 IP address (1 host up) scanned in 11.79 seconds
root@Ub18:/home/vboxuser# nmap www.facebook.com

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:26 IST
Nmap scan report for www.facebook.com (157.240.23.35)
Host is up (0.0052s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f137:83:face:b00c:0:25de
rDNS record for 157.240.23.35: edge-star-mini-shv-01-maa2.facebook.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 15.63 seconds
root@Ub18:/home/vboxuser#
```

Scanning a range of ip

Nmap 10.30.158.11-20

```
an
SYN Stealth Scan Timing: About 100.00% done; ETC: 22:29 (0:00:00 remaining)
Nmap scan report for 10.30.158.11
Host is up (0.075s latency).
All 1000 scanned ports on 10.30.158.11 are filtered

Nmap scan report for 10.30.158.12
Host is up (0.0065s latency).
All 1000 scanned ports on 10.30.158.12 are filtered

Nmap scan report for 10.30.158.13
Host is up (0.013s latency).
All 1000 scanned ports on 10.30.158.13 are filtered

Nmap scan report for 10.30.158.14
Host is up (0.0075s latency).
All 1000 scanned ports on 10.30.158.14 are filtered

Nmap scan report for 10.30.158.15
Host is up (0.0071s latency).
All 1000 scanned ports on 10.30.158.15 are filtered

Nmap scan report for 10.30.158.16
Host is up (0.0065s latency).
All 1000 scanned ports on 10.30.158.16 are filtered

Nmap scan report for 10.30.158.17
Host is up (0.024s latency).
```

```
Nmap scan report for 10.30.158.14
Host is up (0.0075s latency).
All 1000 scanned ports on 10.30.158.14 are filtered

Nmap scan report for 10.30.158.15
Host is up (0.0071s latency).
All 1000 scanned ports on 10.30.158.15 are filtered

Nmap scan report for 10.30.158.16
Host is up (0.0065s latency).
All 1000 scanned ports on 10.30.158.16 are filtered

Nmap scan report for 10.30.158.17
Host is up (0.024s latency).
All 1000 scanned ports on 10.30.158.17 are filtered

Nmap scan report for 10.30.158.18
Host is up (0.0069s latency).
All 1000 scanned ports on 10.30.158.18 are filtered

Nmap scan report for 10.30.158.19
Host is up (0.0067s latency).
All 1000 scanned ports on 10.30.158.19 are filtered

Nmap scan report for 10.30.158.20
Host is up (0.0049s latency).
All 1000 scanned ports on 10.30.158.20 are filtered
```

Scan a subnet 10.30.159.11/22

```
Nmap scan report for 10.30.158.18
Host is up (0.0069s latency).
All 1000 scanned ports on 10.30.158.18 are filtered

Nmap scan report for 10.30.158.19
Host is up (0.0067s latency).
All 1000 scanned ports on 10.30.158.19 are filtered

Nmap scan report for 10.30.158.20
Host is up (0.0049s latency).
All 1000 scanned ports on 10.30.158.20 are filtered

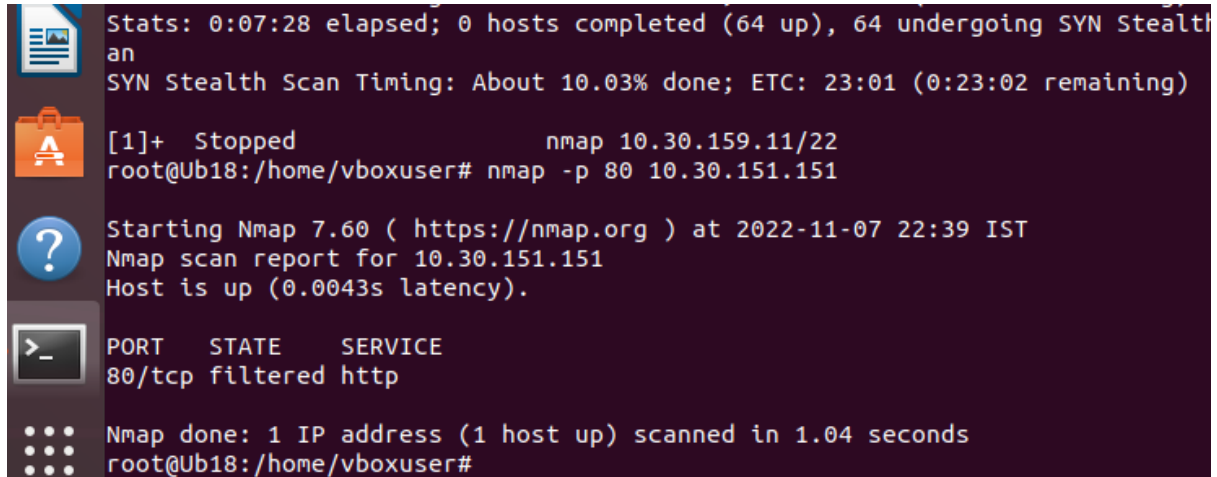
Nmap done: 10 IP addresses (10 hosts up) scanned in 159.27 seconds
root@Ub18:/home/vboxuser#
root@Ub18:/home/vboxuser# nmap 10.30.159.11/22
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:31 IST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1024 undergoing Ping Scan
Ping Scan Timing: About 0.24% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1024 undergoing Ping Scan
Ping Scan Timing: About 0.49% done
Stats: 0:00:30 elapsed; 0 hosts completed (0 up), 1024 undergoing Ping Scan
Ping Scan Timing: About 3.66% done; ETC: 22:45 (0:13:36 remaining)
Stats: 0:00:34 elapsed; 0 hosts completed (0 up), 1024 undergoing Ping Scan
Ping Scan Timing: About 4.15% done; ETC: 22:45 (0:13:28 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (0 up), 1024 undergoing Ping Scan
Ping Scan Timing: About 4.39% done; ETC: 22:45 (0:13:25 remaining)
```

```
Stats: 0:07:18 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 9.25% done; ETC: 23:02 (0:23:23 remaining)
Stats: 0:07:20 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 9.49% done; ETC: 23:01 (0:23:12 remaining)
Stats: 0:07:20 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 9.55% done; ETC: 23:01 (0:23:02 remaining)
Stats: 0:07:27 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 9.98% done; ETC: 23:01 (0:23:00 remaining)
Stats: 0:07:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 9.99% done; ETC: 23:01 (0:22:58 remaining)
Stats: 0:07:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 10.00% done; ETC: 23:01 (0:22:57 remaining)
Stats: 0:07:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 10.01% done; ETC: 23:01 (0:22:55 remaining)
Stats: 0:07:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 10.02% done; ETC: 23:01 (0:23:03 remaining)
Stats: 0:07:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 10.03% done; ETC: 23:01 (0:23:02 remaining)
```

Nmap selecting a single port

Nmap -p 80 10.30.151.151



```
Stats: 0:07:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.03% done; ETC: 23:01 (0:23:02 remaining)

[1]+  Stopped                  nmap 10.30.159.11/22
root@Ub18:/home/vboxuser# nmap -p 80 10.30.151.151

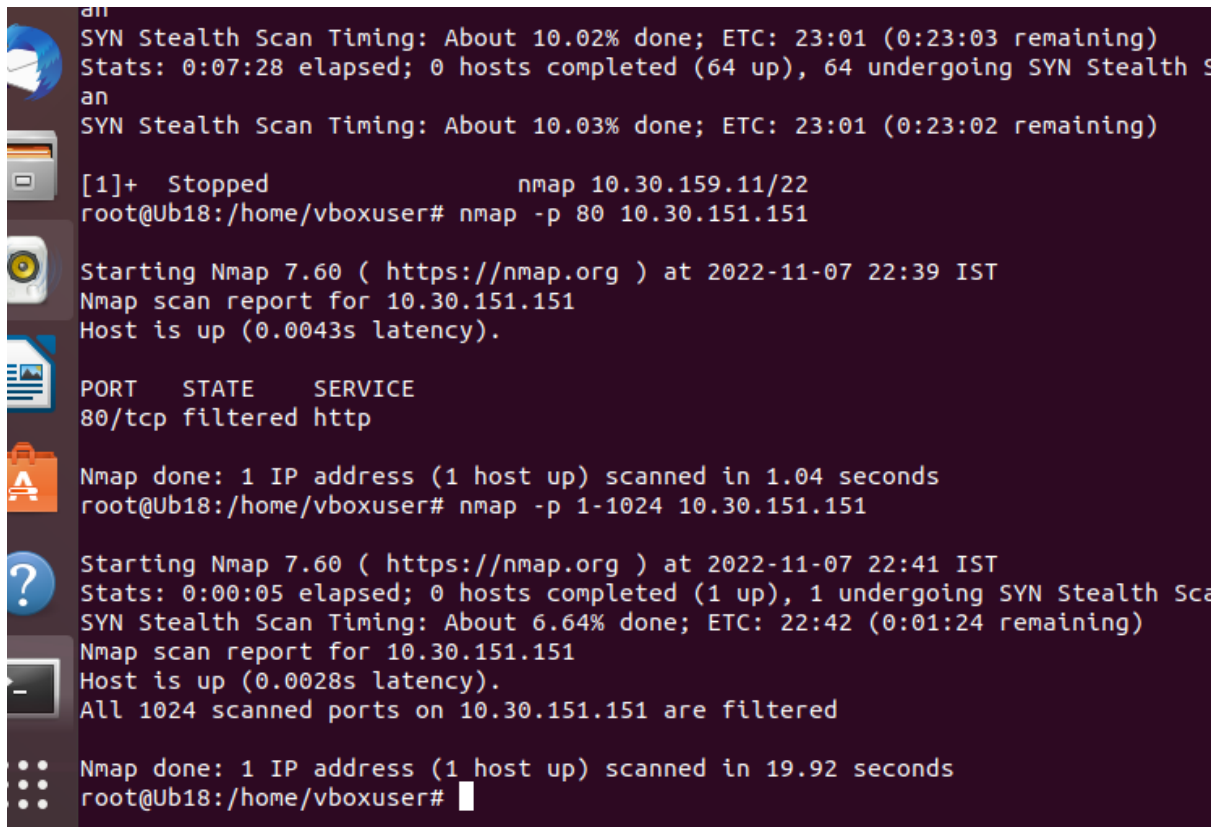
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:39 IST
Nmap scan report for 10.30.151.151
Host is up (0.0043s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
root@Ub18:/home/vboxuser#
```

Scan a range of ports

Nmap -p 1-25 10.30.151.151



```
SYN Stealth Scan Timing: About 10.02% done; ETC: 23:01 (0:23:03 remaining)
Stats: 0:07:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.03% done; ETC: 23:01 (0:23:02 remaining)

[1]+  Stopped                  nmap 10.30.159.11/22
root@Ub18:/home/vboxuser# nmap -p 80 10.30.151.151

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:39 IST
Nmap scan report for 10.30.151.151
Host is up (0.0043s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

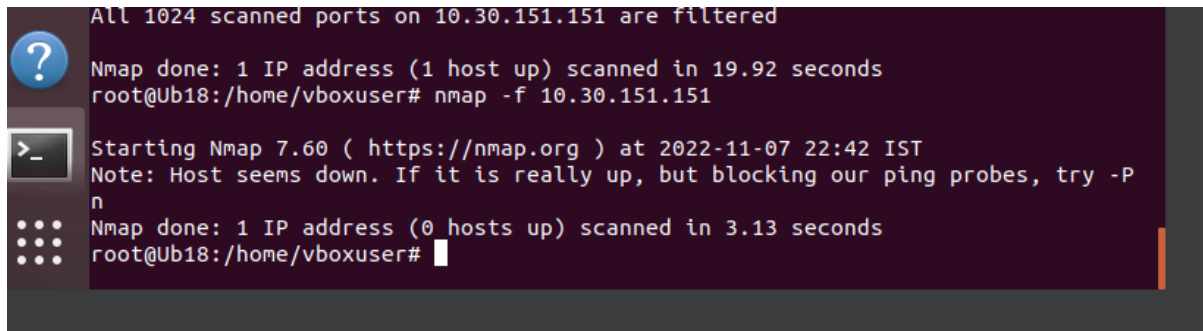
Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
root@Ub18:/home/vboxuser# nmap -p 1-1024 10.30.151.151

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:41 IST
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.64% done; ETC: 22:42 (0:01:24 remaining)
Nmap scan report for 10.30.151.151
Host is up (0.0028s latency).
All 1024 scanned ports on 10.30.151.151 are filtered

Nmap done: 1 IP address (1 host up) scanned in 19.92 seconds
root@Ub18:/home/vboxuser#
```

Scan 100 most common ports

Nmap -f 10.30.151.151

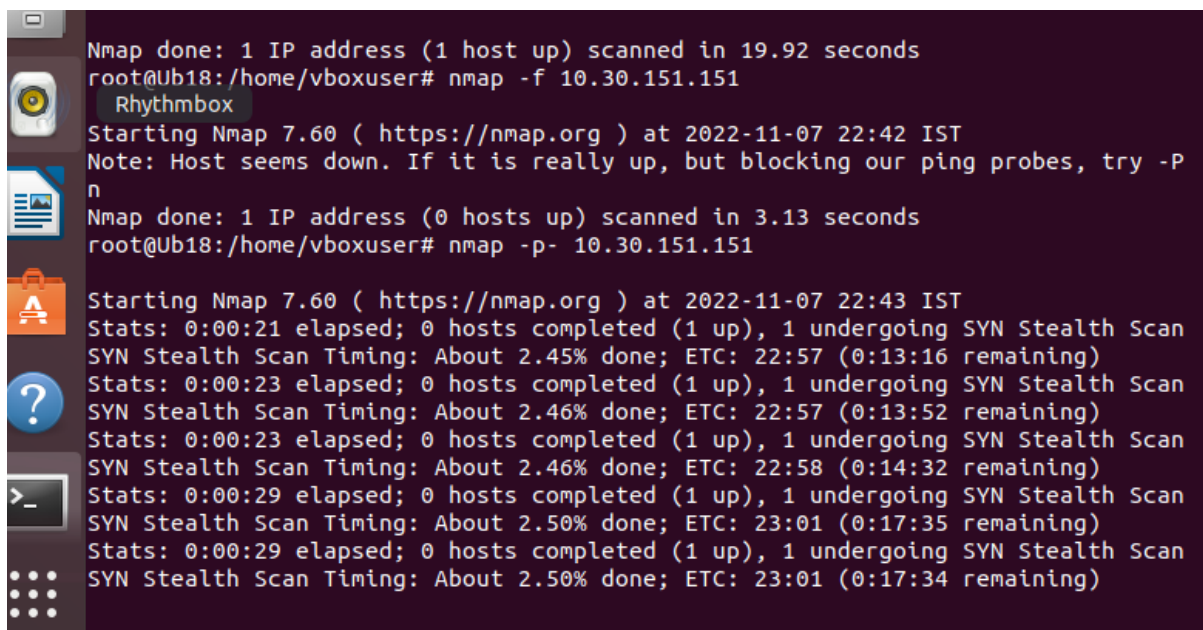


```
All 1024 scanned ports on 10.30.151.151 are filtered
Nmap done: 1 IP address (1 host up) scanned in 19.92 seconds
root@Ub18:/home/vboxuser# nmap -f 10.30.151.151

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:42 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
root@Ub18:/home/vboxuser#
```

Scan all 65535 ports

Nmap -p 10.30.151.151

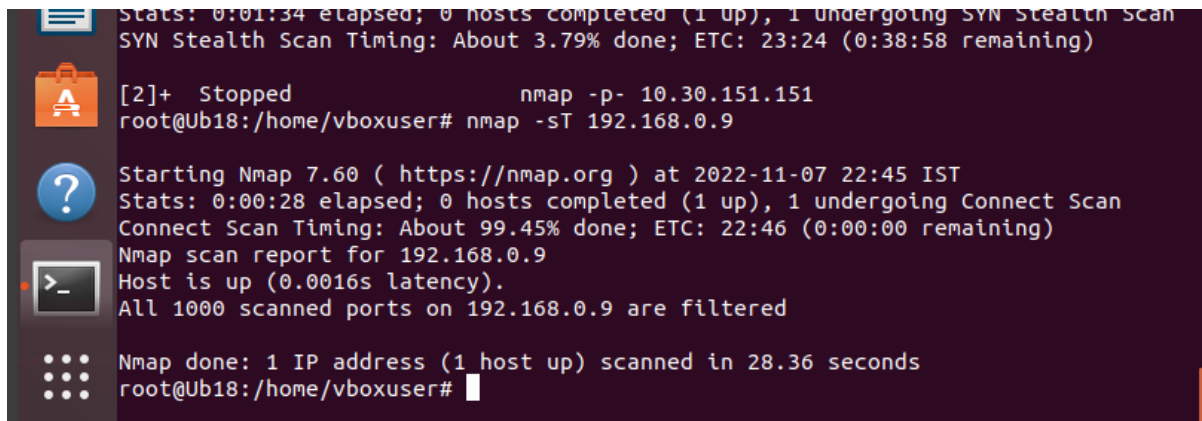


```
Nmap done: 1 IP address (1 host up) scanned in 19.92 seconds
root@Ub18:/home/vboxuser# nmap -f 10.30.151.151
Rhythmbox
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:42 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
root@Ub18:/home/vboxuser# nmap -p- 10.30.151.151

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:43 IST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.45% done; ETC: 22:57 (0:13:16 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.46% done; ETC: 22:57 (0:13:52 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.46% done; ETC: 22:58 (0:14:32 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.50% done; ETC: 23:01 (0:17:35 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.50% done; ETC: 23:01 (0:17:34 remaining)
```

Scan using tcp connect

Nmap -sT 192.168.0.9

A terminal window with a dark purple background and light blue text. It shows the execution of an Nmap SYN Stealth Scan on 192.168.0.9. The output indicates that the host is up and that all 1000 scanned ports are filtered. The scan took 28.36 seconds.

```
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.79% done; ETC: 23:24 (0:38:58 remaining)

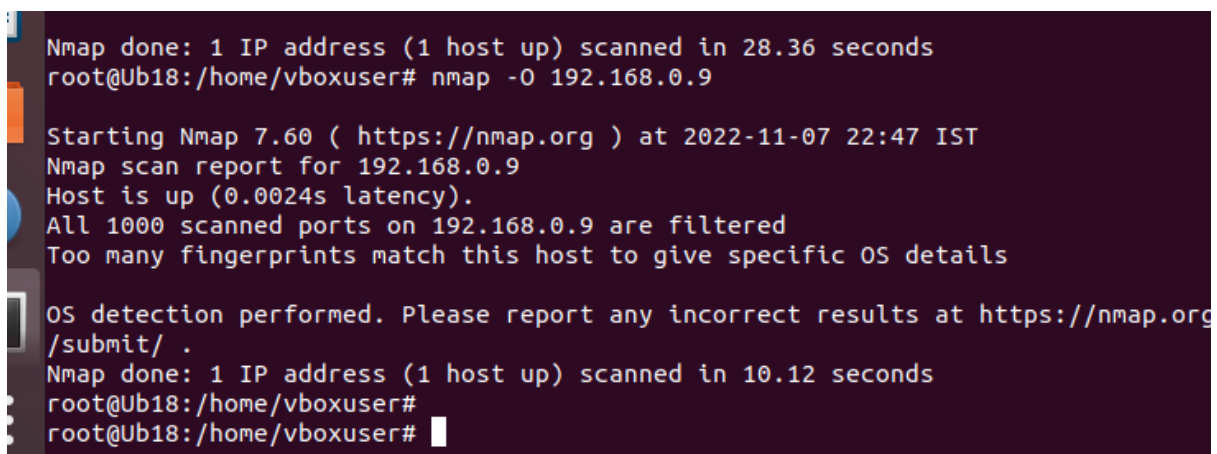
[2]+  Stopped                  nmap -p- 10.30.151.151
root@Ub18:/home/vboxuser# nmap -sT 192.168.0.9

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:45 IST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.45% done; ETC: 22:46 (0:00:00 remaining)
Nmap scan report for 192.168.0.9
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.0.9 are filtered

Nmap done: 1 IP address (1 host up) scanned in 28.36 seconds
root@Ub18:/home/vboxuser#
```

Detect OS and Services

Nmap -O 192.168.0.9

A terminal window with a dark purple background and light blue text. It shows the execution of an Nmap OS detection scan on 192.168.0.9. The output indicates that the host is up and that all 1000 scanned ports are filtered. It also shows that OS detection was performed but no specific OS details were provided due to too many fingerprints matching. The scan took 10.12 seconds.

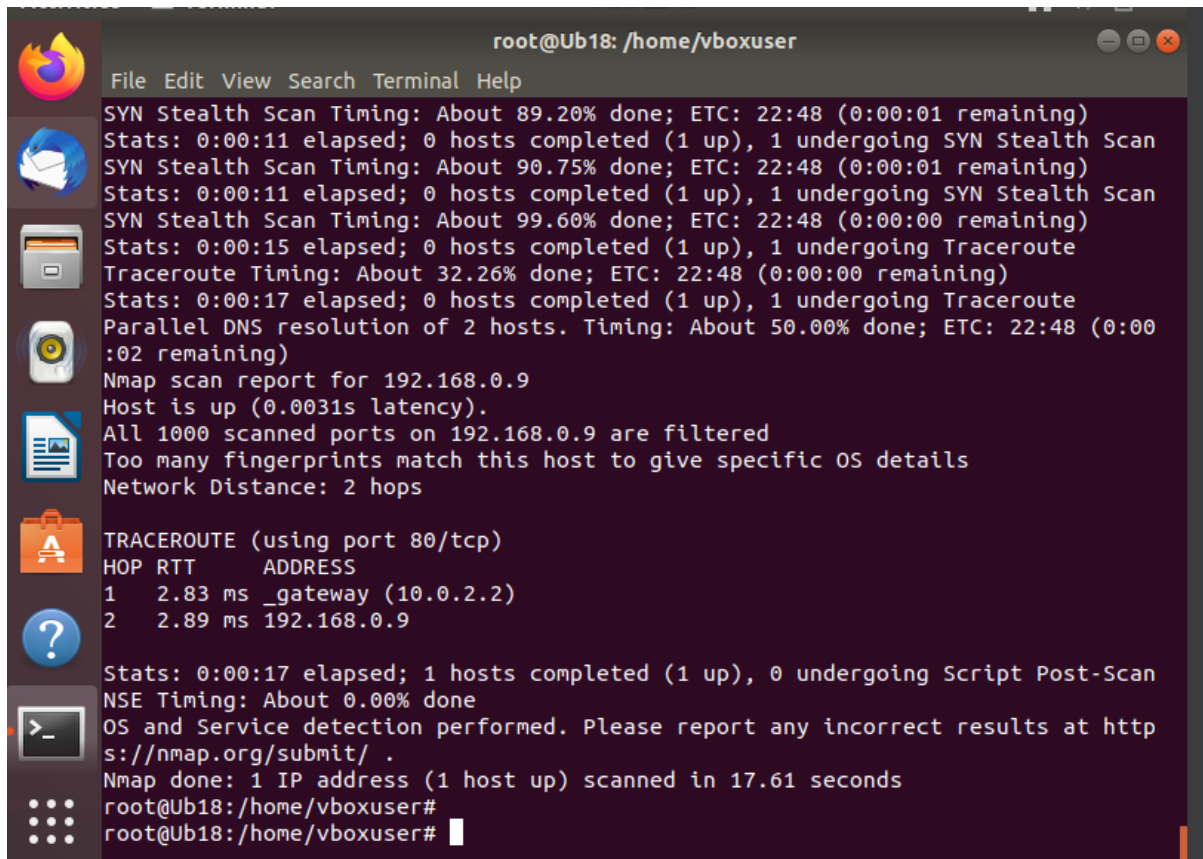
```
Nmap done: 1 IP address (1 host up) scanned in 28.36 seconds
root@Ub18:/home/vboxuser# nmap -O 192.168.0.9

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:47 IST
Nmap scan report for 192.168.0.9
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.0.9 are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds
root@Ub18:/home/vboxuser#
root@Ub18:/home/vboxuser#
```

Nmap -A 192.168.0.9





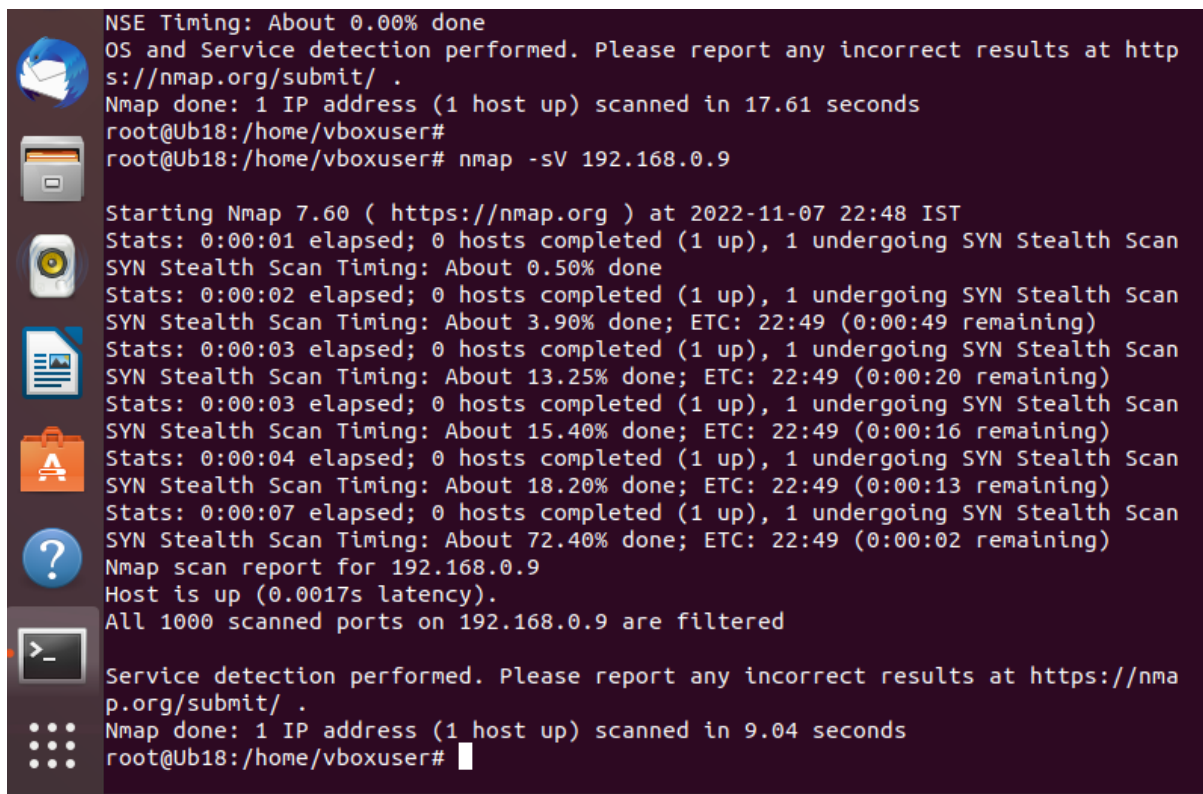
```
root@Ub18: /home/vboxuser
File Edit View Search Terminal Help
SYN Stealth Scan Timing: About 89.20% done; ETC: 22:48 (0:00:01 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.75% done; ETC: 22:48 (0:00:01 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.60% done; ETC: 22:48 (0:00:00 remaining)
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Traceroute Timing: About 32.26% done; ETC: 22:48 (0:00:00 remaining)
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Parallel DNS resolution of 2 hosts. Timing: About 50.00% done; ETC: 22:48 (0:00:02 remaining)
Nmap scan report for 192.168.0.9
Host is up (0.0031s latency).
All 1000 scanned ports on 192.168.0.9 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.83 ms _gateway (10.0.2.2)
2 2.89 ms 192.168.0.9

Stats: 0:00:17 elapsed; 1 hosts completed (1 up), 0 undergoing Script Post-Scan
NSE Timing: About 0.00% done
OS and Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
root@Ub18:/home/vboxuser#
root@Ub18:/home/vboxuser#
```

Standard service detection

Nmap -sV 192.168.0.9



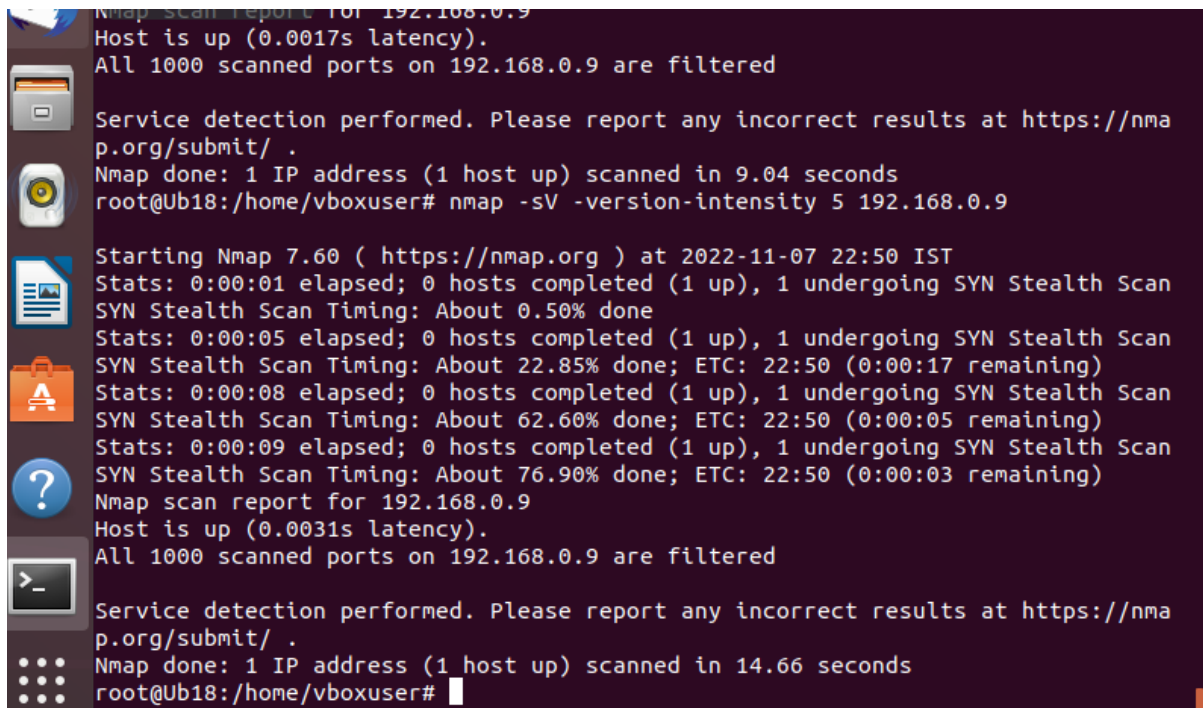
```
NSE Timing: About 0.00% done
OS and Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
root@Ub18:/home/vboxuser#
root@Ub18:/home/vboxuser# nmap -sV 192.168.0.9

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:48 IST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.90% done; ETC: 22:49 (0:00:49 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.25% done; ETC: 22:49 (0:00:20 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 15.40% done; ETC: 22:49 (0:00:16 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.20% done; ETC: 22:49 (0:00:13 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 72.40% done; ETC: 22:49 (0:00:02 remaining)
Nmap scan report for 192.168.0.9
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.0.9 are filtered

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.04 seconds
root@Ub18:/home/vboxuser#
```

More aggressive service detection

Nmap -sV -version-intensity 5 192.168.0.9



```
Nmap scan report for 192.168.0.9
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.0.9 are filtered

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.04 seconds
root@Ub18:/home/vboxuser# nmap -sV -version-intensity 5 192.168.0.9

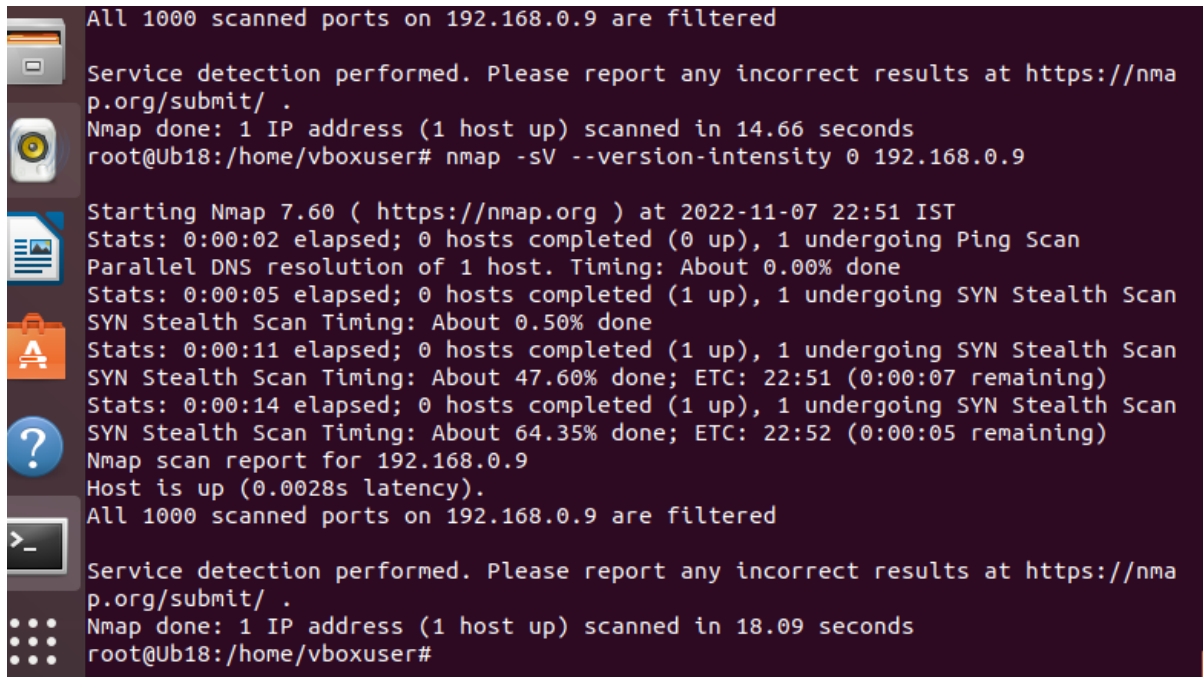
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:50 IST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.85% done; ETC: 22:50 (0:00:17 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.60% done; ETC: 22:50 (0:00:05 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.90% done; ETC: 22:50 (0:00:03 remaining)
Nmap scan report for 192.168.0.9
Host is up (0.0031s latency).
All 1000 scanned ports on 192.168.0.9 are filtered

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
root@Ub18:/home/vboxuser#
```



Lighter banner grabbing detection

Nmap -sV --version-intensity 0 192.168.0.9



```
All 1000 scanned ports on 192.168.0.9 are filtered

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
root@Ub18:/home/vboxuser# nmap -sV --version-intensity 0 192.168.0.9

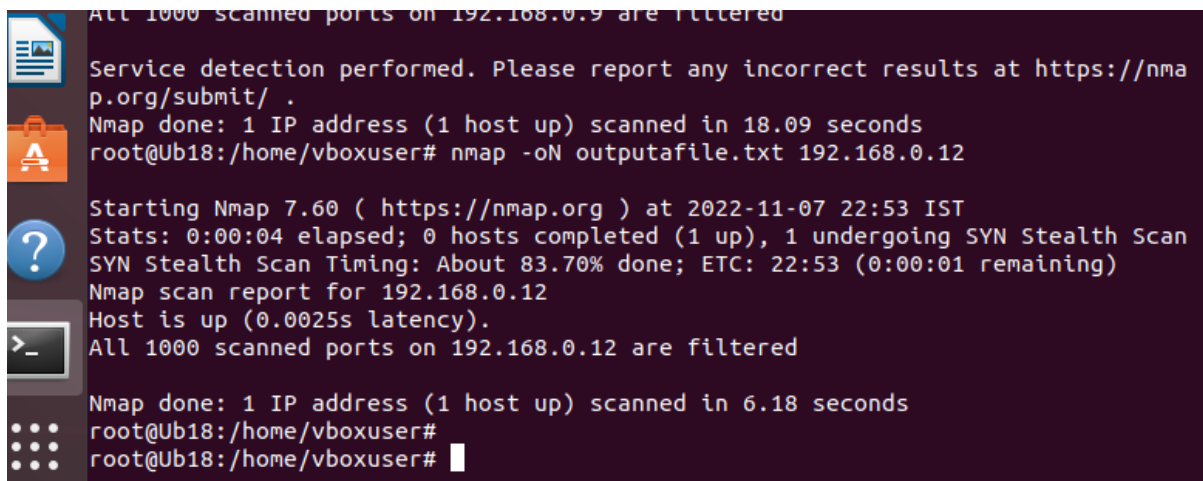
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:51 IST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.60% done; ETC: 22:51 (0:00:07 remaining)
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.35% done; ETC: 22:52 (0:00:05 remaining)
Nmap scan report for 192.168.0.9
Host is up (0.0028s latency).
All 1000 scanned ports on 192.168.0.9 are filtered

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
root@Ub18:/home/vboxuser#
```

Nmap output formats

Save default output to a file

Nmap -oN outputfile.txt 192.168.0.12



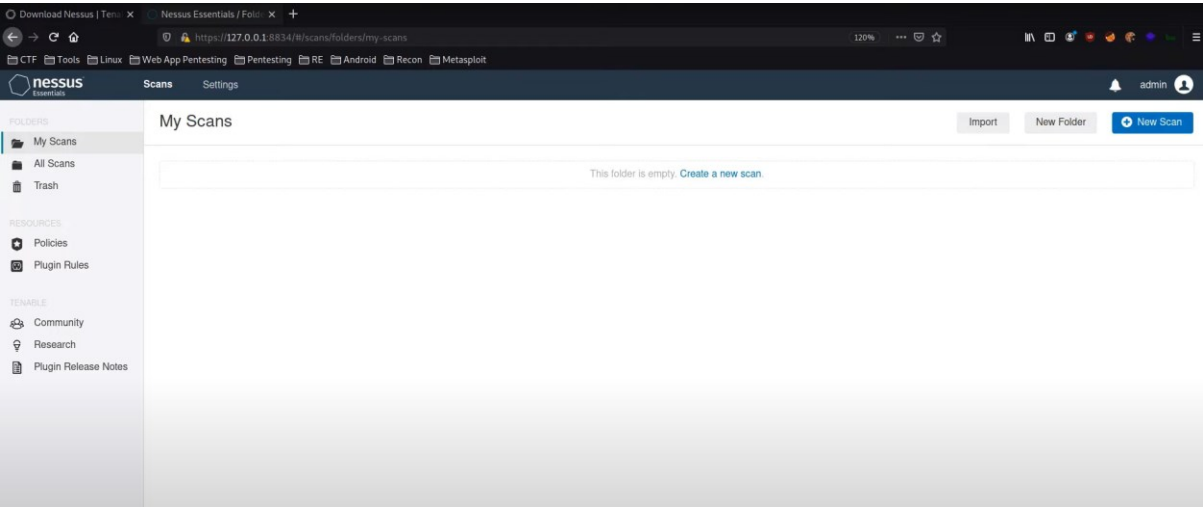
```
All 1000 scanned ports on 192.168.0.9 are filtered

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
root@Ub18:/home/vboxuser# nmap -oN outputfile.txt 192.168.0.12

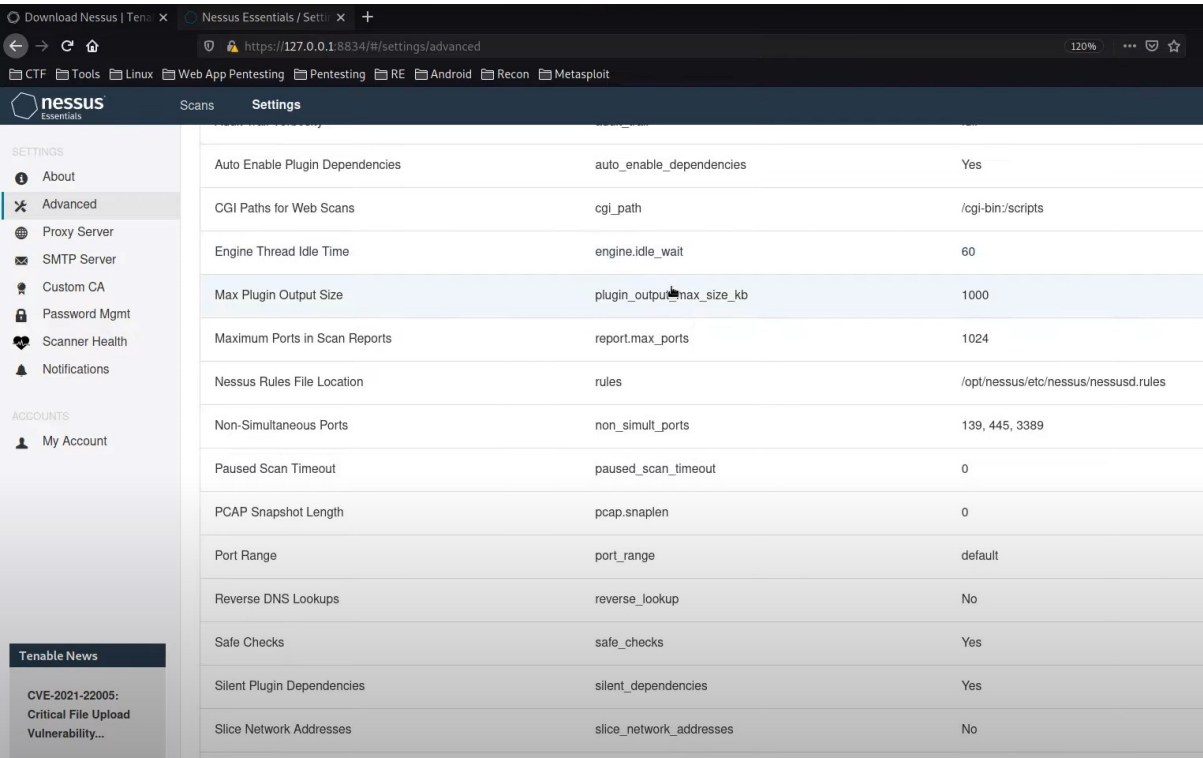
Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-07 22:53 IST
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.70% done; ETC: 22:53 (0:00:01 remaining)
Nmap scan report for 192.168.0.12
Host is up (0.0025s latency).
All 1000 scanned ports on 192.168.0.12 are filtered

Nmap done: 1 IP address (1 host up) scanned in 6.18 seconds
root@Ub18:/home/vboxuser#
root@Ub18:/home/vboxuser#
```

# NESSUS TOOL



## Configuration:



nessus

Essentials

ScansSettings

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

TENABLE

Community

Research

Plugin Release Notes

New Scan / Host Discovery

[Back to Scan Templates](#)

SettingsPlugins

BASIC

GeneralScheduleNotifications

DISCOVERY

REPORT

ADVANCED

NameHost Discovery - Local Network

Description

FolderMy Scans

Targets192.168.2.1/24

Upload Targets

[Add File](#)

CTFToolsLinuxWeb App PentestingPentestingREAndroidReconMetasploit

nessus

ScansSettings

admin

FOLDERS

My Scans

Windows Hosts

All Scans

Trash

RESOURCES

Policies

Plugin Rules

TENABLE

Community

Research

Plugin Release Notes

|                          |          |   |                   |    |  |  |
|--------------------------|----------|---|-------------------|----|--|--|
| <input type="checkbox"/> | MIXED    | Zohocorp Manageengine Desktop Central (Multiple Issues) | CGI abuses        | 12 |  |  |
| <input type="checkbox"/> | MIXED    | Apache HTTP Server (Multiple Issues)                    | Web Servers       | 11 |  |  |
| <input type="checkbox"/> | MIXED    | Microsoft Windows (Multiple Issues)                     | Windows           | 8  |  |  |
| <input type="checkbox"/> | MIXED    | Web Server (Multiple Issues)                            | Web Servers       | 4  |  |  |
| <input type="checkbox"/> | CRITICAL | Apache Httpd (Multiple Issues)                          | Web Servers       | 2  |  |  |
| <input type="checkbox"/> | MIXED    | SSL (Multiple Issues)                                   | General           | 23 |  |  |
| <input type="checkbox"/> | MIXED    | SNMP (Multiple Issues)                                  | SNMP              | 7  |  |  |
| <input type="checkbox"/> | MIXED    | IETF Md5 (Multiple Issues)                              | General           | 3  |  |  |
| <input type="checkbox"/> | MIXED    | HTTP (Multiple Issues)                                  | Web Servers       | 15 |  |  |
| <input type="checkbox"/> | MIXED    | TLS (Multiple Issues)                                   | Service detection | 6  |  |  |
| <input type="checkbox"/> | MIXED    | Microsoft Windows (Multiple Issues)                     | Misc.             | 4  |  |  |
| <input type="checkbox"/> | MIXED    | SSL Anonymous Cipher Suites Supported                   | Service detection | 2  |  |  |

Scanner: Local Scanner

Start: Today at 8:13 PM

End: Today at 8:30 PM

Elapsed: 17 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

