Software and Cybersecurity Lab

CS445 Lab7

Name: Dipean Dasgupta **ID: 202151188**

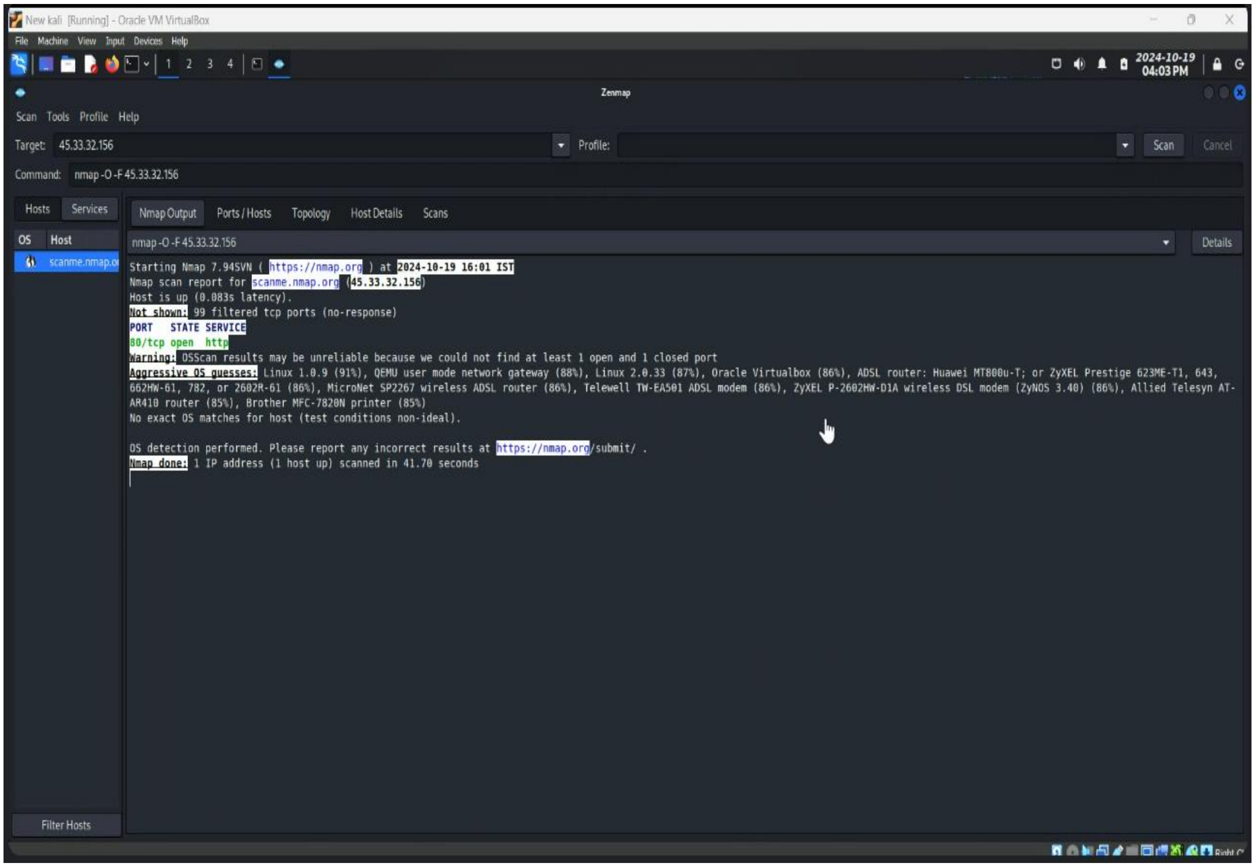
Task: Exploring Information gathering tools such as nmap and zenmap in Kali linux and setup of metasploitable linux os.

Exploring Nmap and Zenmap

First of all, from the application center, first of all click on **Zenmap**. Here the Ip address that we are targeting is: 45.33.32.156.

1st command: **nmap -O 45.33.32.156**

Results displayed:


New kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2024-10-19
04:03 PM
Zenmap
Scan Tools Profile Help
Scan
Cancel
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Details
OS Host
scanme.nmap.o
Filter Hosts

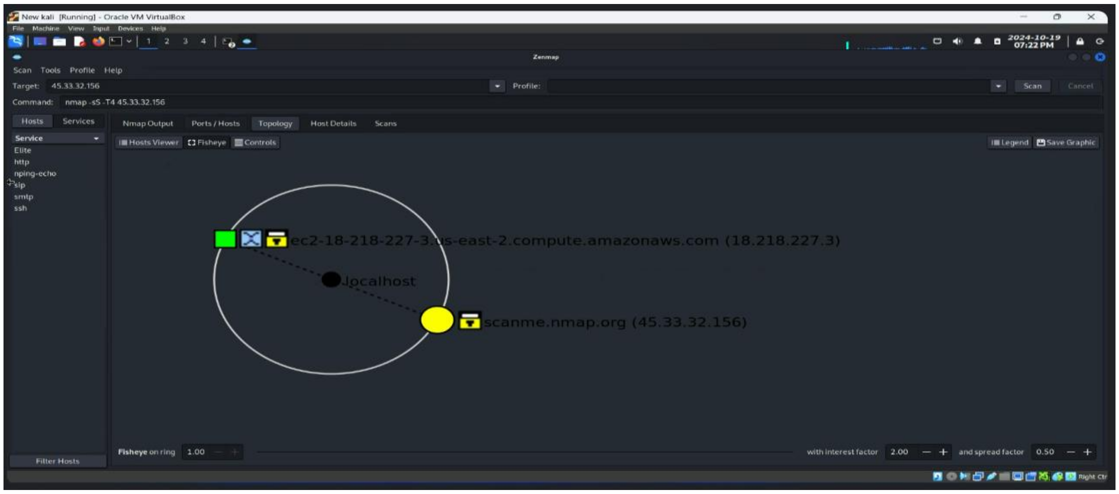
Target: 45.33.32.156

Profile:

Command: nmap -O -F 45.33.32.156

```
nmap -O -F 45.33.32.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 16:01 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.083s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 1.0.9 (91%), QEMU user mode network gateway (88%), Linux 2.0.33 (87%), Oracle Virtualbox (86%), ADSL router: Huawei MT800u-T; or ZyXEL Prestige 623ME-T1, 643, 662HW-61, 782, or 2602R-61 (86%), MicroNet SP2267 wireless ADSL router (86%), Telewell TW-EA501 ADSL modem (86%), ZyXEL P-2602HW-D1A wireless DSL modem (ZyNOS 3.40) (86%), Allied Telesyn AT-AR410 router (85%), Brother MFC-7820N printer (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.70 seconds
```

Here zenmap found 1 port 30/tcp http which is open. OS detection is also performed in zenmap.

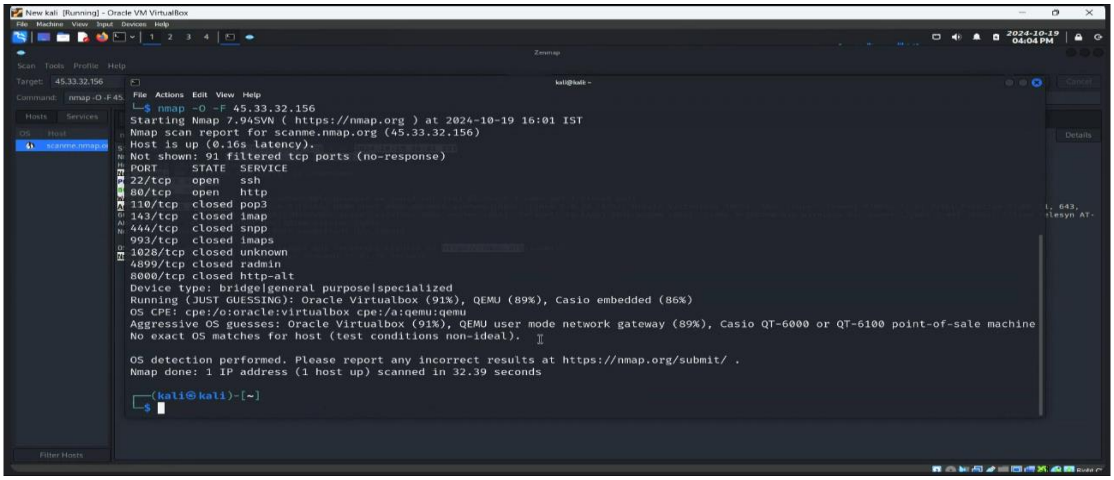

New kali [Running] - Oracle VM VirtualBox
Scan Tools Profile Help
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Graphic
Service
Elite
http
nping-echo
sip
smtp
ssh
ec2-18-218-227-3.us-east-2.compute.amazonaws.com (18.218.227.3)
localhost
scanme.nmap.org (45.33.32.156)
Filter Hosts
2024-10-19
07:22 PM

Target: 45.33.32.156

Command: nmap -sS -T4 45.33.32.156

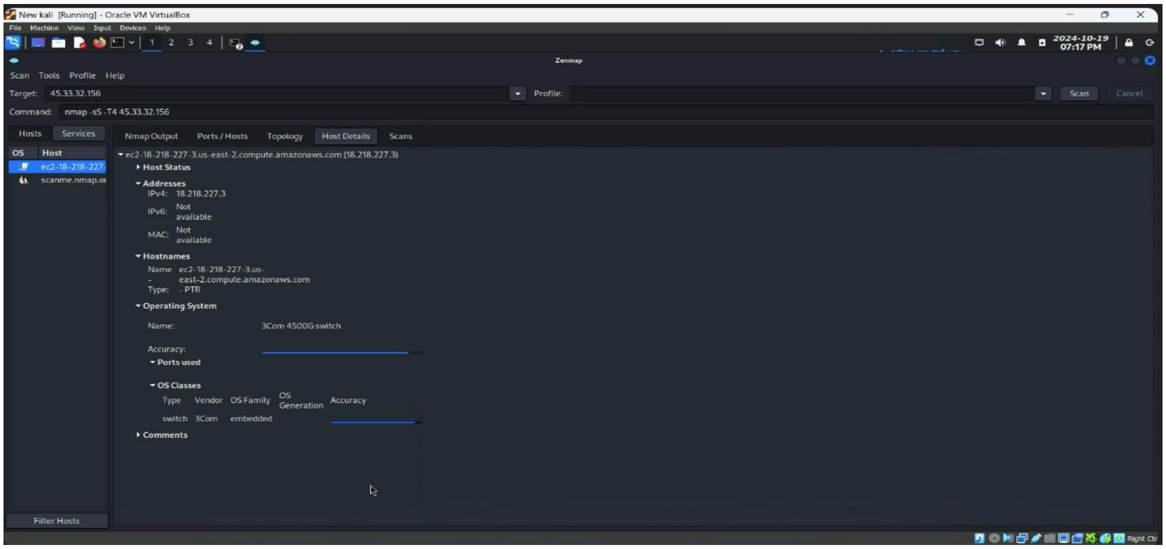
Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

The topology of the scan is shared above.


New kali [Running] - Oracle VM VirtualBox
File Actions Edit View Help
Zenmap
2024-10-19
04:04 PM

```
└─$ nmap -O -F 45.33.32.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 16:01 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Not shown: 91 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
110/tcp   closed pop3
143/tcp   closed imap
444/tcp   closed snpp
993/tcp   closed imaps
1028/tcp closed unknown
4899/tcp closed radmin
8000/tcp closed http-alt
Device type: bridge|general purpose|specialized
Running (JUST GUESSING): Oracle Virtualbox (91%), QEMU (89%), Casio embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (91%), QEMU user mode network gateway (89%), Casio QT-6000 or QT-6100 point-of-sale machine
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.39 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Same scan is done in **nmap** and the following was received. 2 open ports and 7 closed ports.


New kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap
Scan Tools Profile Help
Scan Cancel
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
ec2-18-218-227-
scanme.nmap.or
Filter Hosts
2024-10-19
07:17 PM

Target: 45.33.32.156

Command: nmap -sS -T4 45.33.32.156

ec2-18-218-227-3.us-east-2.compute.amazonaws.com (18.218.227.3)

- Host Status
- Addresses
  - IPv4: 18.218.227.3
  - IPv6: Not available
  - MAC: Not available
- Hostnames
  - Name - ec2-18-218-227-3.us-east-2.compute.amazonaws.com
  - Type: - PTR
- Operating System
  - Name: 3Com 4500G switch
  - Accuracy:
  - Ports used
  - OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
switch	3Com	embedded		

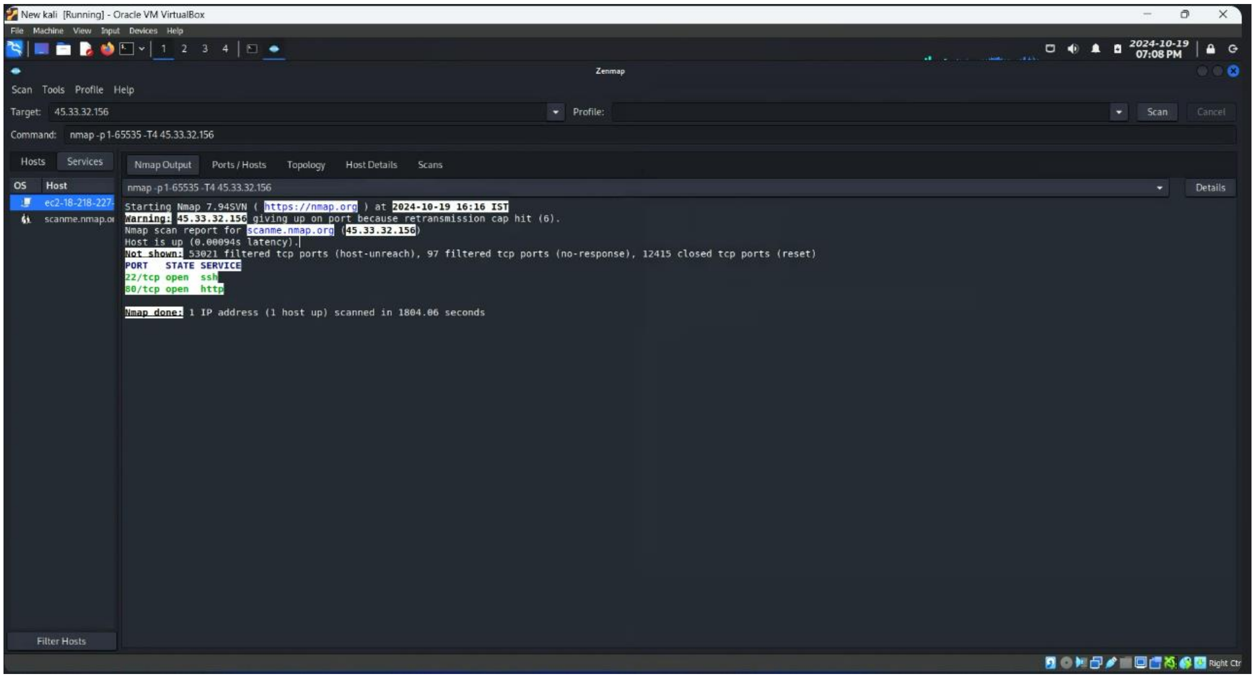
- Comments

As per the OS report, scan was carried out in **3Com 4500G switch** OS.

Scanning All TCP Ports:

Target IP: 45.33.32.156

Command: **nmap -p 1-65535 -T4 45.33.32.156**



Target: 45.33.32.156

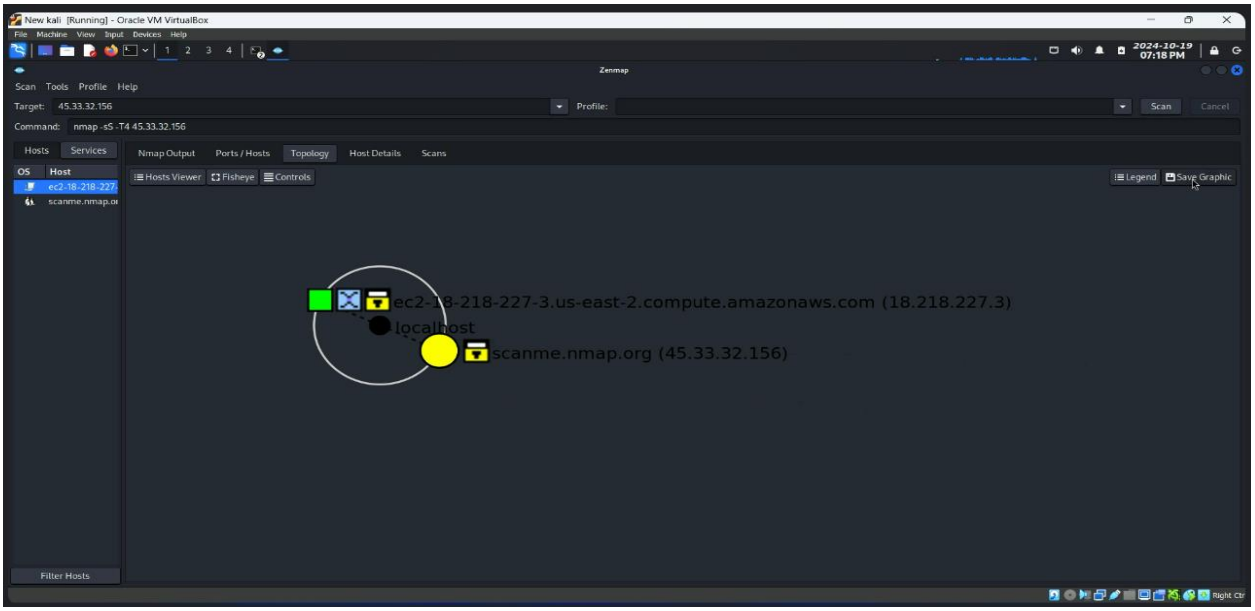
Command: nmap -p 1-65535 -T4 45.33.32.156

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 16:16 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00094s latency).
Not shown: 53021 filtered tcp ports (host-unreach), 97 filtered tcp ports (no-response), 12415 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1804.06 seconds
```

In zenmap, scan report shows:

53821 filtered tcp (host unreached), 97 filtered tcp ports (no-response), 12415 tcp ports (reset)

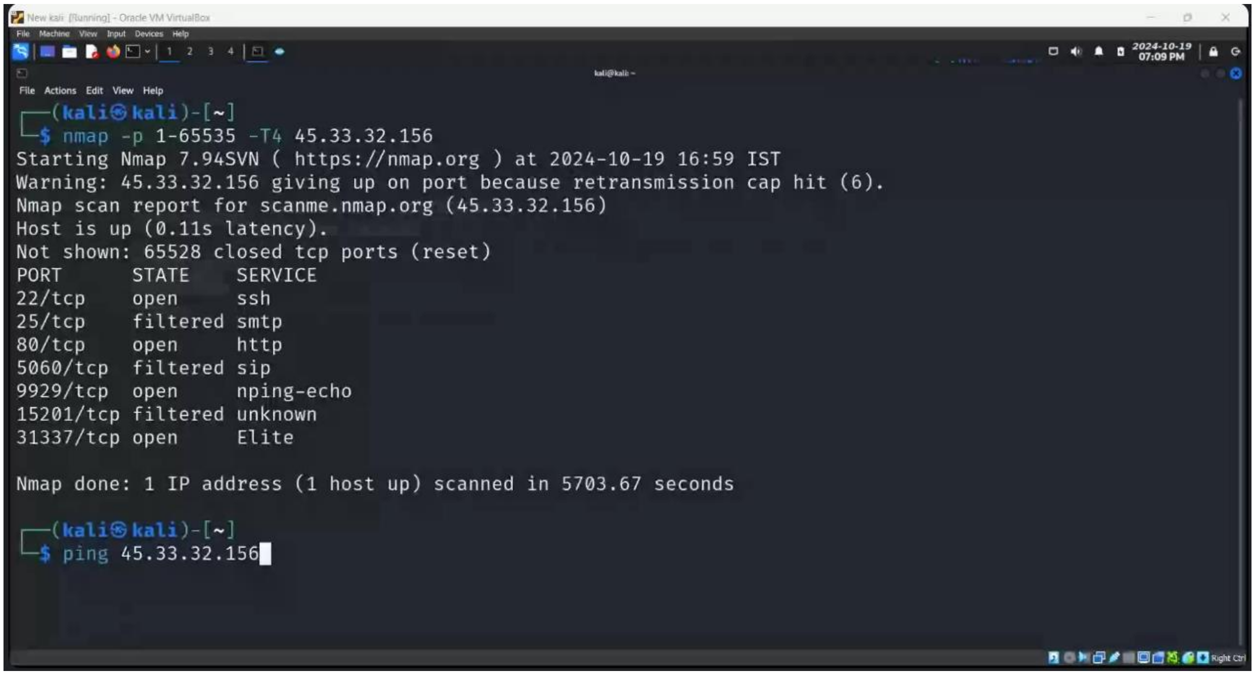
2 open ports ssh and http.


New kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
2024-10-19 07:18 PM
Zenmap
Scan Tools Profile Help
Profile:
Scan
Cancel
Hosts Services
OS Host
ec2-18-218-227-
scanme.nmap.or
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
ec2-18-218-227-3.us-east-2.compute.amazonaws.com (18.218.227.3)
localhost
scanme.nmap.org (45.33.32.156)
Filter Hosts

Target: 45.33.32.156

Command: nmap -sS -T4 45.33.32.156

Topological map.



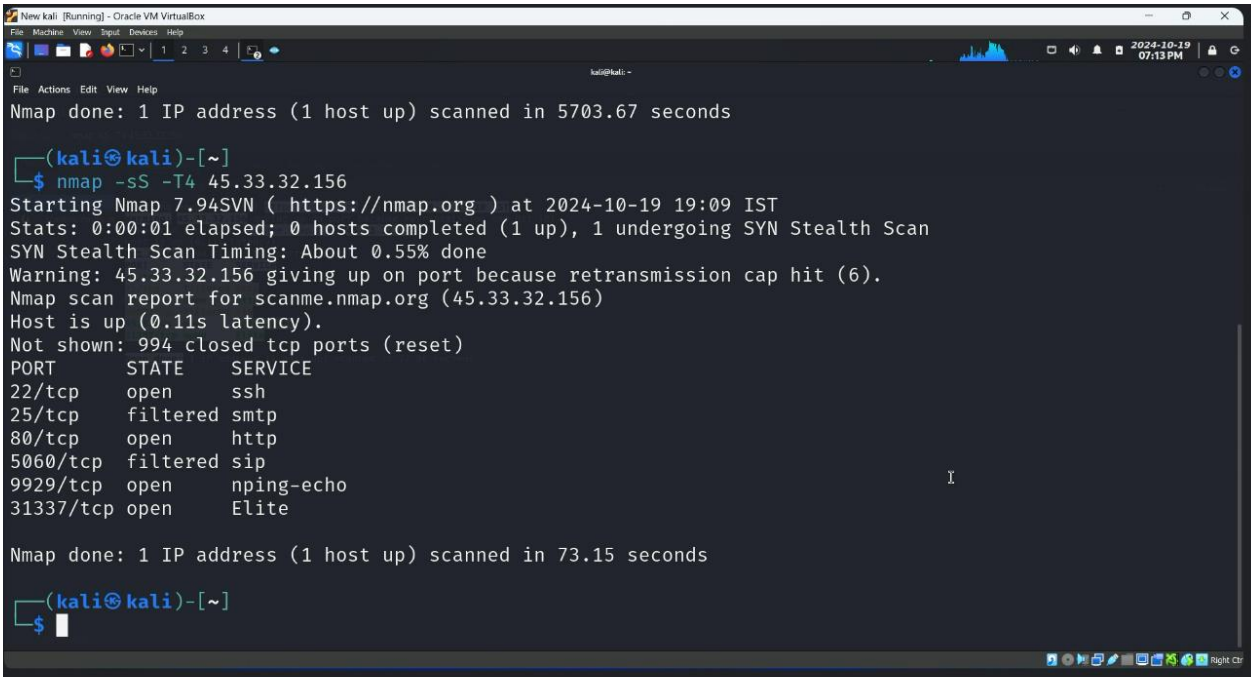
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-65535 -T4 45.33.32.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 16:59 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
5060/tcp  filtered sip
9929/tcp  open     nping-echo
15201/tcp filtered unknown
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 5703.67 seconds

┌──(kali㉿kali)-[~]
└─$ ping 45.33.32.156
```

In similar scan by nmap,

4 open ports found providing services: ssh, http, elite, nping echo

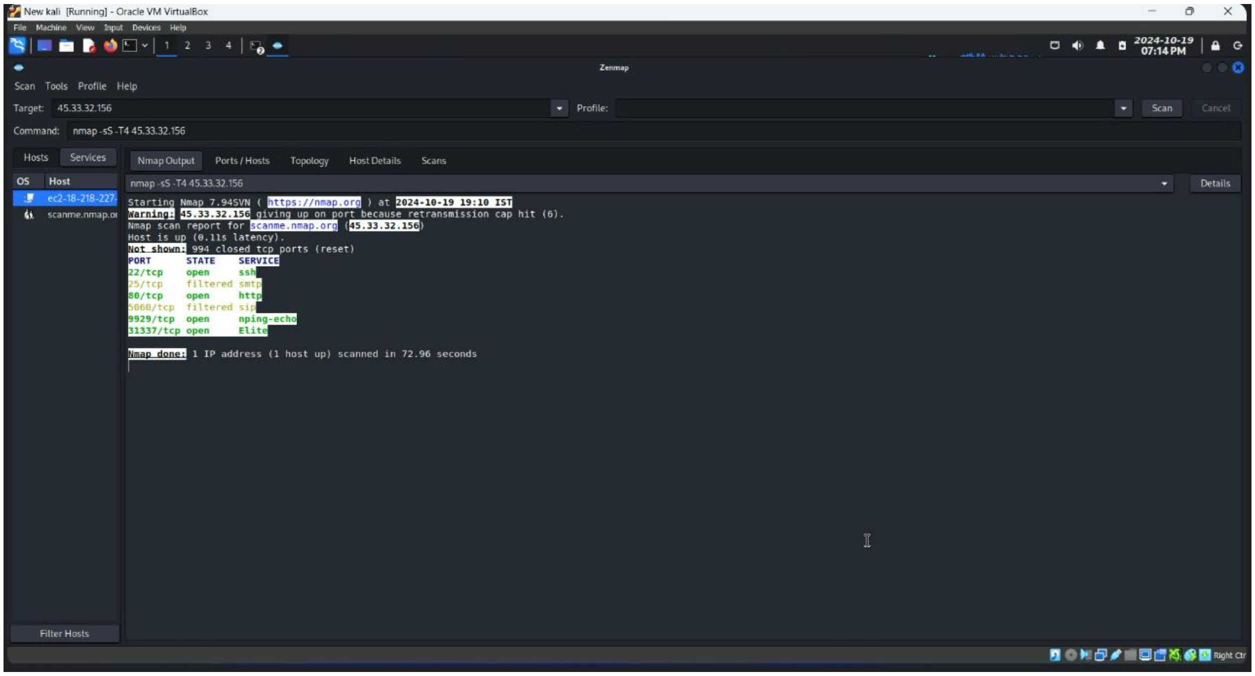
65528 ports were closed.

Stealth scan



```
Nmap done: 1 IP address (1 host up) scanned in 5703.67 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS -T4 45.33.32.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 19:09 IST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.55% done
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
5060/tcp  filtered sip
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 73.15 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Stealth scan conducted by nmap, finds the same 4 ports as active.



Target: 45.33.32.156

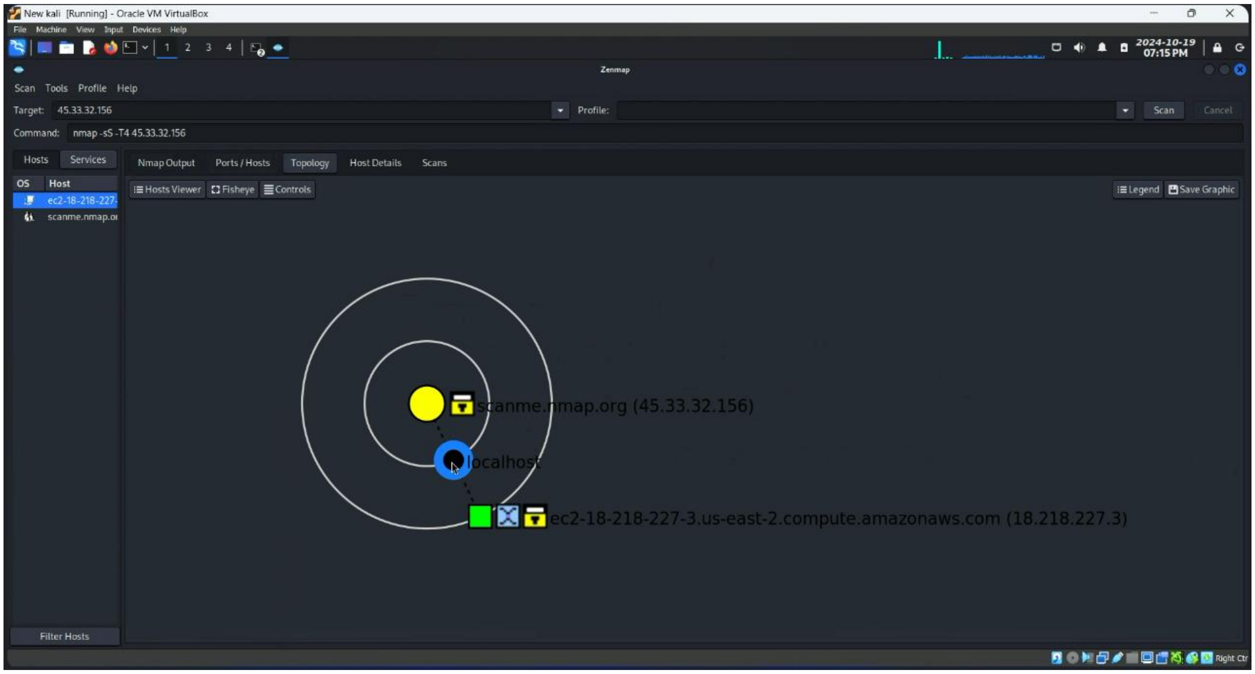
Command: nmap -sS -T4 45.33.32.156

```
nmap -sS -T4 45.33.32.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 19:10 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
5060/tcp  filtered sip
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 72.96 seconds
```

Stealth scan in **zenmap** also finds the same 4 ports as open.

Target IP: 45.33.32.156

Command: **nmap -sS -T4 45.33.32.156**



New kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap
Scan Tools Profile Help
Profile:
Scan
Cancel
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
OS Host
ec2-18-218-227-
scanme.nmap.or
scanme.nmap.org (45.33.32.156)
localhost
ec2-18-218-227-3.us-east-2.compute.amazonaws.com (18.218.227.3)
Filter Hosts
2024-10-19
07:15 PM

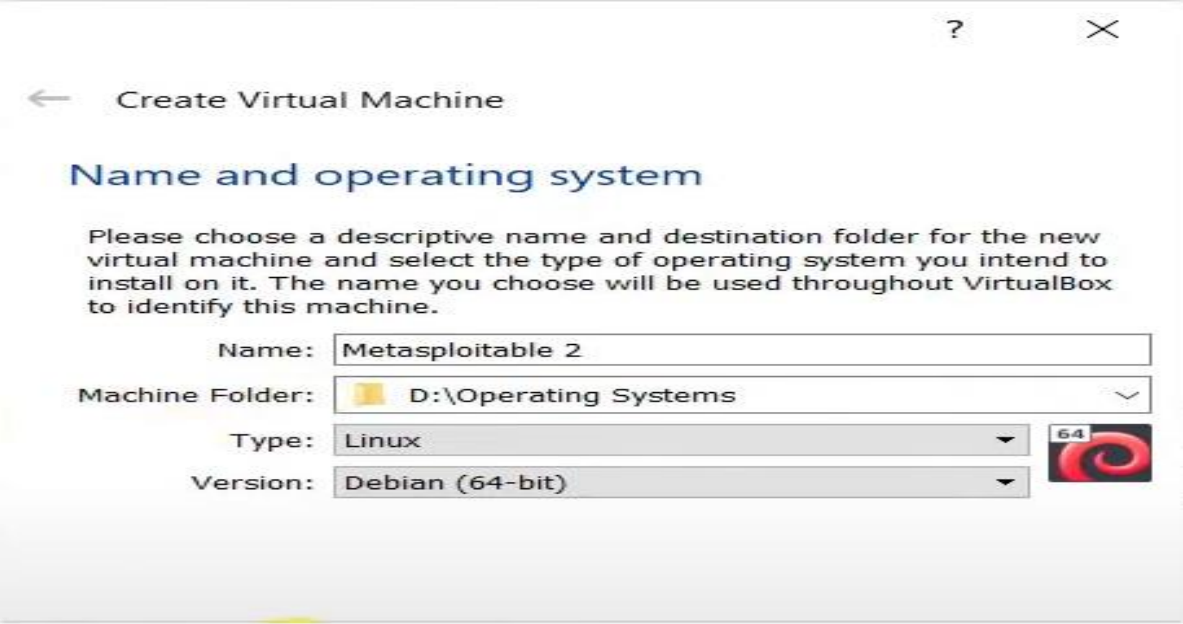
Target: 45.33.32.156

Command: nmap -sS -T4 45.33.32.156

Topology map shared.

Metasploitable

Installing Metasploitable:



Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

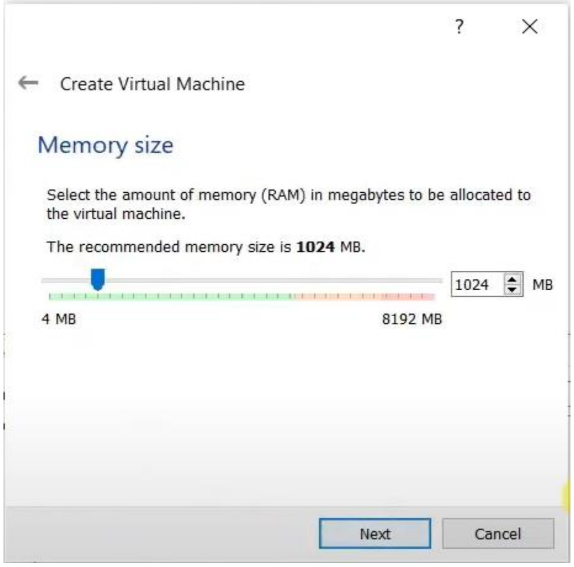
Name: Metasploitable 2

Machine Folder: D:\Operating Systems

Type: Linux

Version: Debian (64-bit)

Allocating Memory and space:



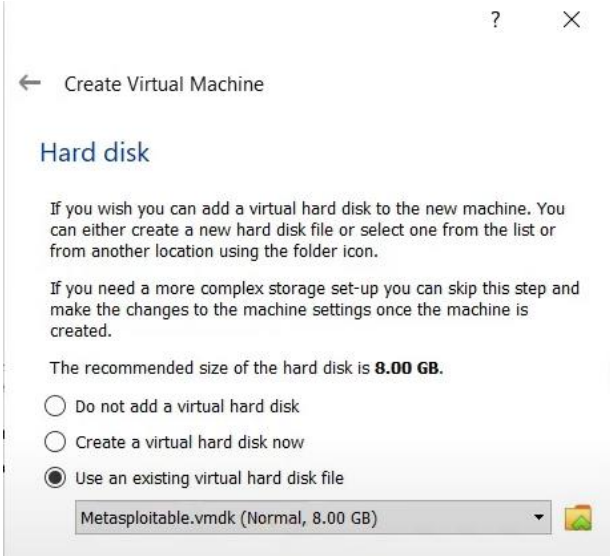
Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

1024 MB



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

○ Do not add a virtual hard disk

○ Create a virtual hard disk now

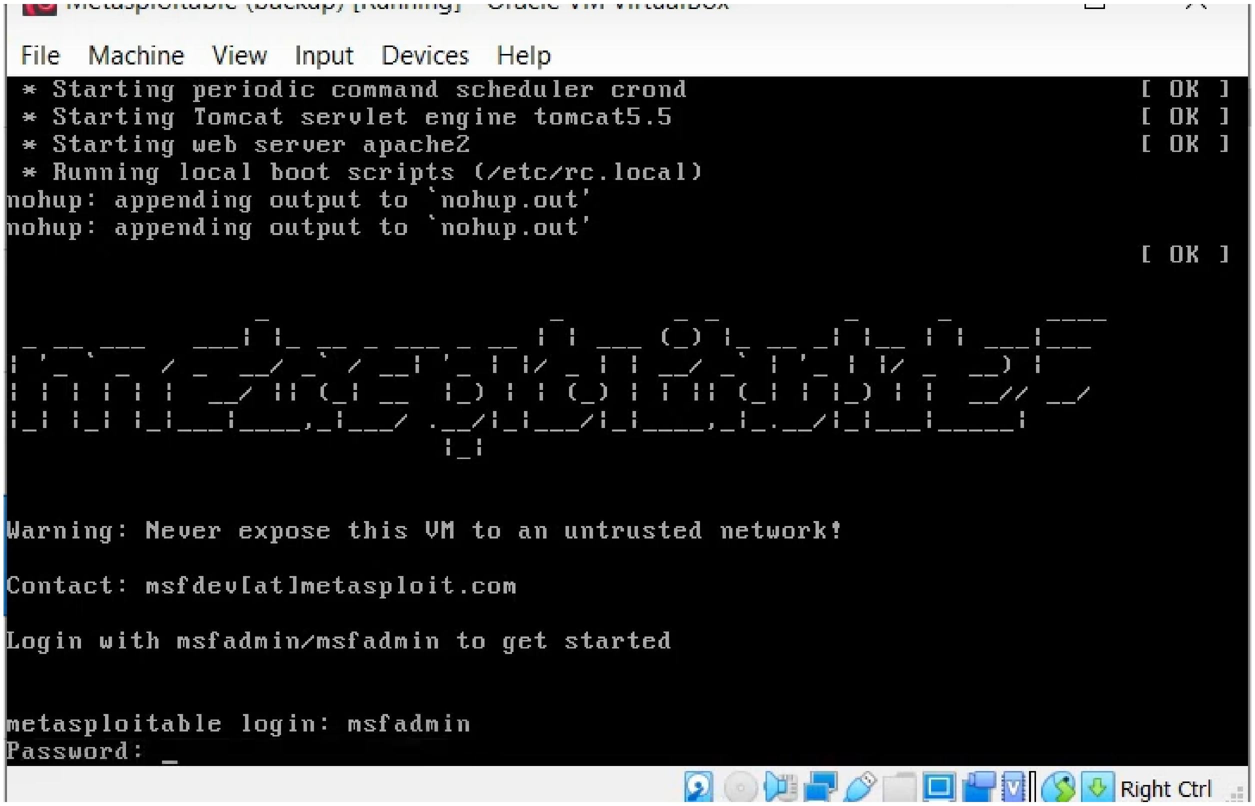
● Use an existing virtual hard disk file

Metasploitable.vmdk (Normal, 8.00 GB)

RAM: 1GB

Disk Space: 8GB

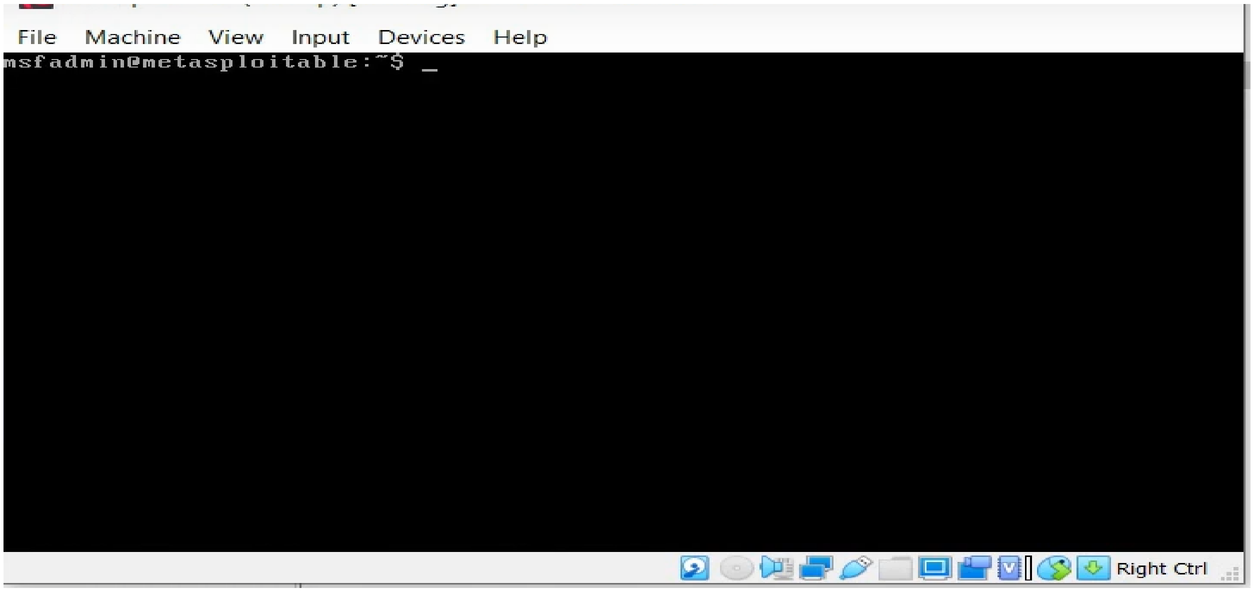
Login to metasploitable:



```
 * Starting periodic command scheduler crond                              [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                               [ OK ]
 * Starting web server apache2                                            [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                          [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password: _
```

Username: msfadmin

Password: msfadmin



```
msfadmin@metasploitable:~$ _
```

Successfully logged in to metasploitable.