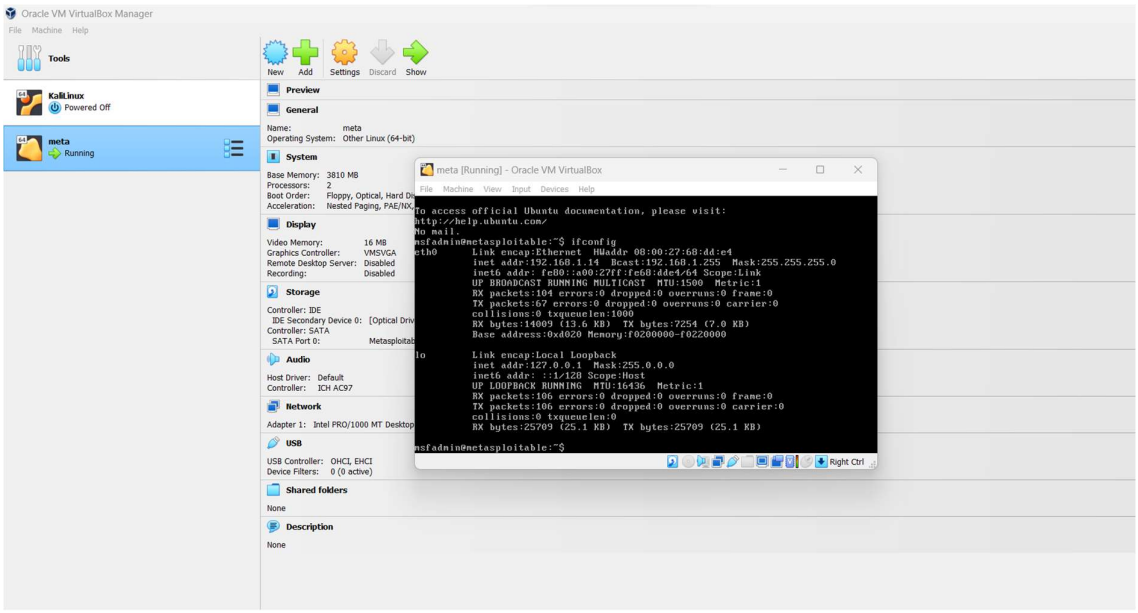
NAME :- M Om Nivas REG no :- 21BCE9706

Email :- omnivas.21bce9706@vitapstudent.ac.in

Task – 9

Installation of Metasploit in Virtual box and Exploring Nmap tool

Installing Metasploit in Virtual box :-



Exploring and Executing some Nmap commands in kali Linux.

nmap -A 192.168.1.14 – execute this command in kali Linux CLI

Nmap Cheat Sheet

comparitech

Different usage options
Port discovery and specification
Host discovery and specification
Vulnerability scanning
Application and service version detection
Software version detection against the ports
Firewall / IDS Spoofing

Port Specification Options

Syntax	Example	Description
-P	nmap -p 23 172.16.1.1	Port scanning port specific port
-P	nmap -p 23-100 172.16.1.1	Port scanning port specific port range
-p	nmap -pU:110,T:23-25,443 172.16.1.1	U-UDP,T-TCP different port types scan
-p-	nmap -p- 172.16.1.1	Port scan for all ports
-p	nmap -smtp,https 172.16.1.1	Port scan from specified protocols
-F	nmap -F 172.16.1.1	Fast port scan for speed up
-P "*"	namp -p "*" ftp 172.16.1.1	Port scan using name
-r	nmap -r 172.16.1.1	Sequential port scan

Scanning Types

Switch/Syntax	Example	Description
-sS	nmap 172.16.1.1 -sS	TCP SYN port scan
-sT	nmap 172.16.1.1 -sT	TCP connect port scan
-sA	nmap 172.16.1.1 -sA	TCP ACK port scan
-sU	nmap 172.16.1.1 -sU	UDP port scan
-Sf	nmap -Sf 172.16.1.1	TCP FIN scan
-sX	nmap -SX 172.16.1.1	XMAS scan
-Sp	nmap -Sp 172.16.1.1	Ping scan
-sU	nmap -Su 172.16.1.1	UDP scan
-sA	nmap -Sa 172.16.1.1	TCP ACK scan
-SL	nmap -Sl 172.16.1.1	list scan

Host /172.16.1.1 Discovery

Switch/Syntax	Example	Description
-sL	nmap 172.16.1.1-5 -sL	List 172.16.1.1 without scanning
-sn	nmap 172.16.1.1/8 -sn	Disable port scanning
-Pn	nmap 172.16.1.1-8 -Pn	Port scans only and no host discovery
-PS	nmap 172.16.1.185 -PS22-25,80	TCP SYN discovery on specified port
-PA	nmap 172.16.1.185 -PA22-25,80	TCP ACK discovery on specified port
-PU	nmap 172.16.1.1-8 -PU53	UDP discovery on specified port
-PR	nmap 172.16.1.1-1/8 -PR	ARP discovery within local network
-n	nmap 172.16.1.1 -n	no DNS resolution

Scanning Command Syntax

nmap [scan types] [options] {172.16.1.1 specification}

Use of Nmap Scripts NSE

nmap --script= test script 172.16.1.0/24	execute thoe listed script against target IP address
nmap --script-update-db	adding new scripts
nmap -sV -sC	use of safe default scripts for scan
nmap --script-help="Test Script"	get help for script

Version Detection

Switch/Syntax	Example	Description
-sV	nmap 172.16.1.1 -sV	Try to find the version of the service running on port
-sV --version-intensity	nmap 172.16.1.1 -sV --version-intensity 6	Intensity level range 0 to 9.
-sV --version-all	nmap 172.16.1.1 -sV --version-all	Set intensity level to 9
-sV --version-light	nmap 172.16.1.1 -sV --version-light	Enable light mode
-A	nmap 172.16.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute
-O	nmap 172.16.1.1 -O	Remote OS detection

Nmap output Formats

Default/normal output	nmap -oN scan.txt 172.16.1.1
XML	nmap -oX scanr.xml 172.16.1.1
Grepable format	snmap -oG grep.txt 172.16.1.1
All formats	nmap -oA 172.16.1.1

172.16.1.1 Specification

nmap 172.16.1.1	single IP scan
nmap 172.16.1.1 172.16.100.1	scan specific IPs
nmap 172.16.1.1-254	scan a range of IPs
nmap xyz.org	scan a domain
nmap 10.1.1.0/8	scan using CIDR notation
nmap -iL scan.txt	scan 172.16.1.1s from a file
nmap --exclude 172.16.1.1	specified IP s exclude from scan

Firewall Proofing

nmap -f [172.16.1.1]	scan fragment packets
nmap -mtu [MTU] [172.16.1.1]	specify MTU
nmap -sI [zombie] [172.16.1.1]	scan idle zoombie
nmap -source-port [port] [172.16.1.1]	manual source port - specify
nmap -data-length [size] [172.16.1.1]	randomly append data
nmap -randomize-hosts [172.16.1.1]	172.16.1.1 scan order randomization
nmap -badsum [172.16.1.1]	bad checksum

Miscellaneous Commands

nmap -6	scan IPV6 targets
nmap -proxies proxy 1 URL, proxy 2 URL	Run in targets with proxies
nmap -open	Show open ports only

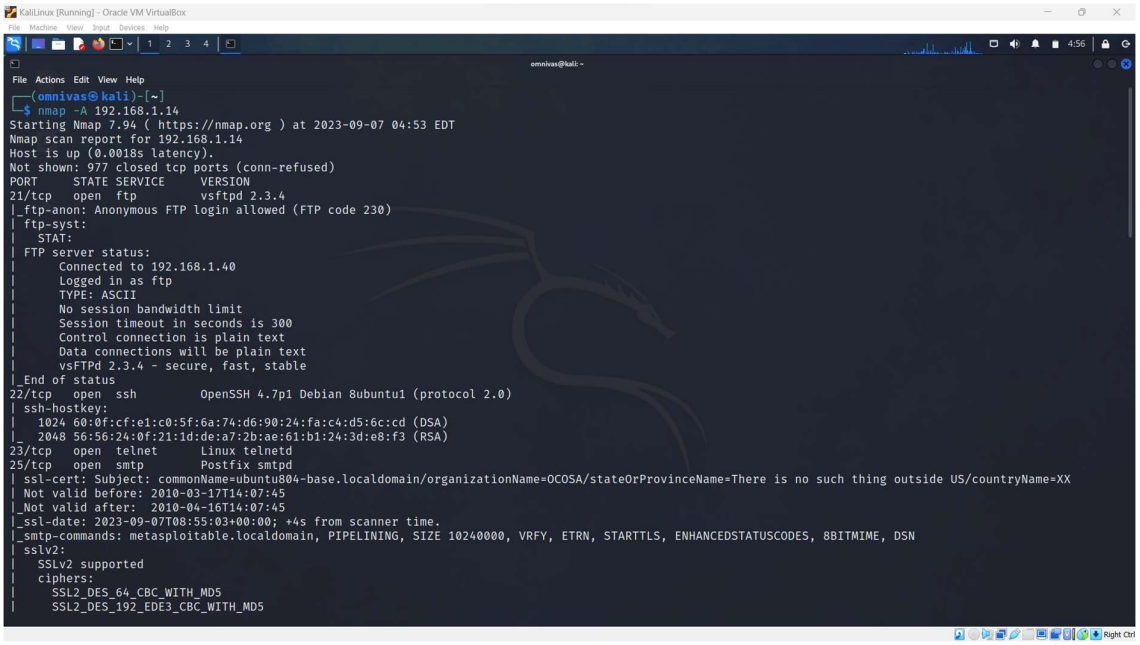
Nmap Timing Options

Syntax	Description
nmap -T0 172.16.1.1	Slowest scan
nmap -T1 172.16.1.1	Tricky scan to avoid IDS
nmap -T2 172.16.1.1	Timely scan
nmap -T3 172.16.1.1	Default scan timer
nmap -T4 172.16.1.1	Aggressive scan
nmap -T5 172.16.1.1	Very aggressive scan

Scan Options

Syntax	Description
nmap -sP 172.16.1.1	Ping scan only
nmap -PU 172.16.1.1	UDP ping scan
nmap -PE 172.16.1.1	ICMP echo ping
nmap -PO 172.16.1.1	IP protocol ping
nmap -PR 172.16.1.1	ARP ping
nmap -Pn 172.16.1.1	Scan without pinging
nmap -traceroute 172.16.1.1	Traceroute

Aggressive Scan in Nmap



Port-Scanning in Nmap

```
┌──(omnivas㉿kali)-[~]
└─$ nmap -p 443 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 10:59 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00033s latency).

PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds

┌──(omnivas㉿kali)-[~]
└─$ nmap -p 80 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 11:00 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00015s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

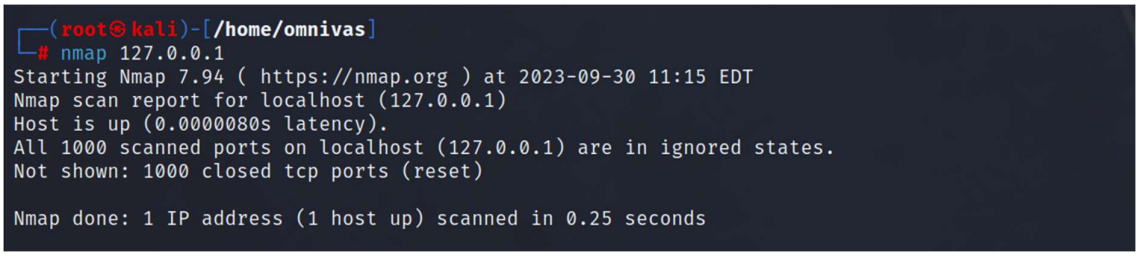
TCP Syn port scan

```
┌──(root㉿kali)-[/home/omnivas]
└─# nmap 127.0.0.1 -sS
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 11:01 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000080s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

TCP connect port Scan

```
┌──(root㉿kali)-[/home/omnivas]
└─# nmap 127.0.0.1 -sT
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 11:03 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00021s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Normal Nmap Scanning



And some more commands