Nmap Scan

Aim :

To install and perform Nmap scan (note :- you may use ip address or website name)

Procedure :

Step 1: Open Nmap from Kali Linux (Goto Applications->select Information Gathering>select
Nmap)

Step 2: Perform different types of scan
(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

Scanning Techniques

Flag	Use	Example
-sS	**TCP syn port scan**	**nmap -sS 192.168.1.1**
-sT	**TCP connect port scan**	**nmap -sT 192.168.1.1**
-sU	**UDP port scan**	**nmap -sU 192.168.1.1**
-sA	**TCP ack port scan**	**nmap -sA 192.168.1.1**

Step 3:
To perform host discovery

-Pn	**only port scan**	**nmap -Pn192.168.1.1**
-sn	**only host discover**	**nmap -sn192.168.1.1**
-PR	**arp discovery on a local network**	**nmap -PR192.168.1.1**
-n	**disable DNS resolution**	**nmap -n 192.168.1.1**

Step 4: PORT SPECIFICATION

Flag	**Use**	**Use**
-p	**specify a port or port range**	**nmap -p 1-30 192.168.1.1**
-p-	**scan all ports**	**nmap -p- 192.168.1.1**
F	**fast port scan**	**nmap -F 192.168.1.1**

Step 5:

Service Version and OS Detection

Flag	Use	Example
-sV	**detect the version of services running**	**nmap -sV 192.168.1.1**
-A	**aggressive scan**	**nmap -A 192.168.1.1**
-O	**detect operating system of the target**	**nmap -O 192.168.1.1**

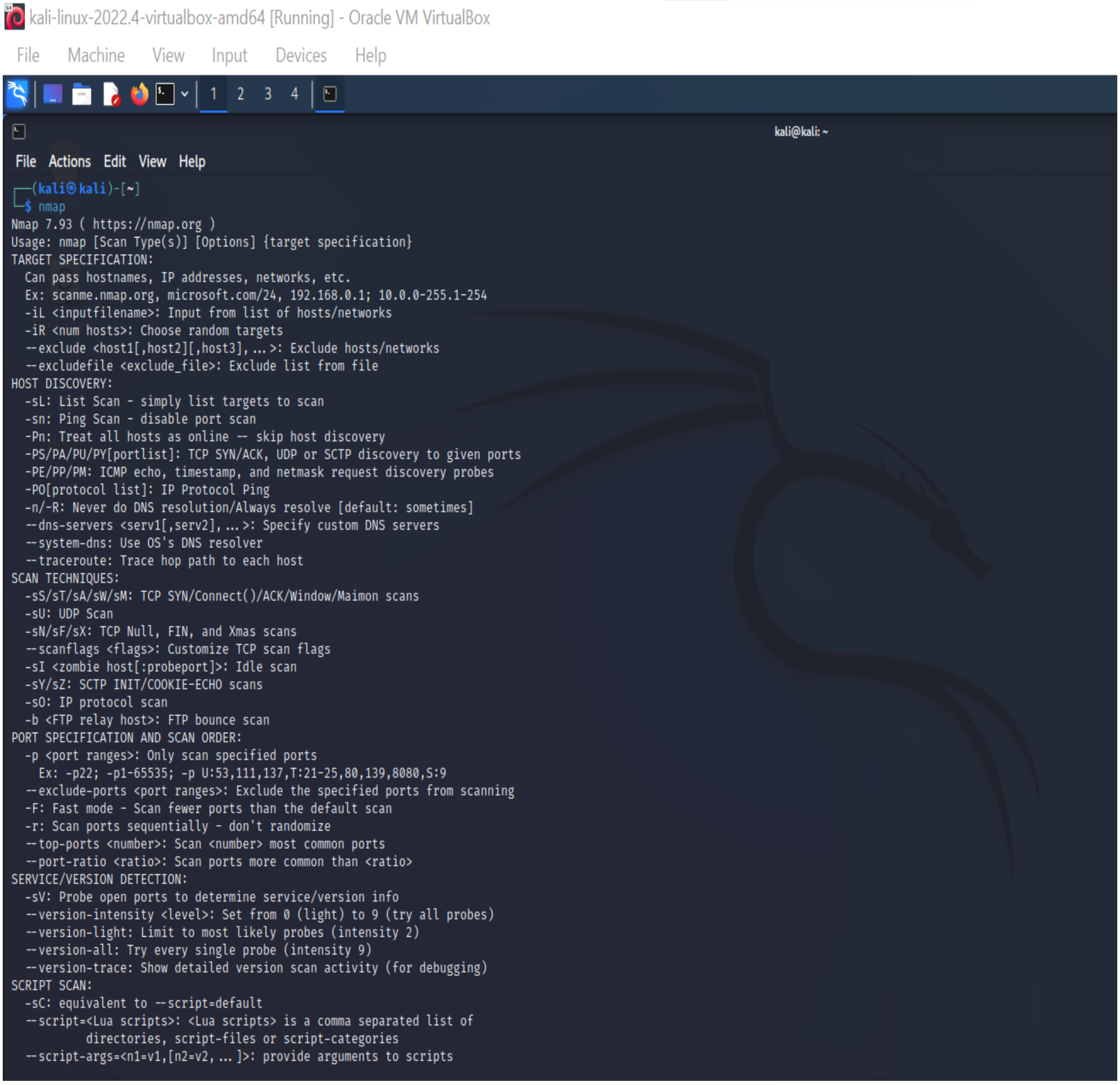
Step 6:-

Timing and Performance

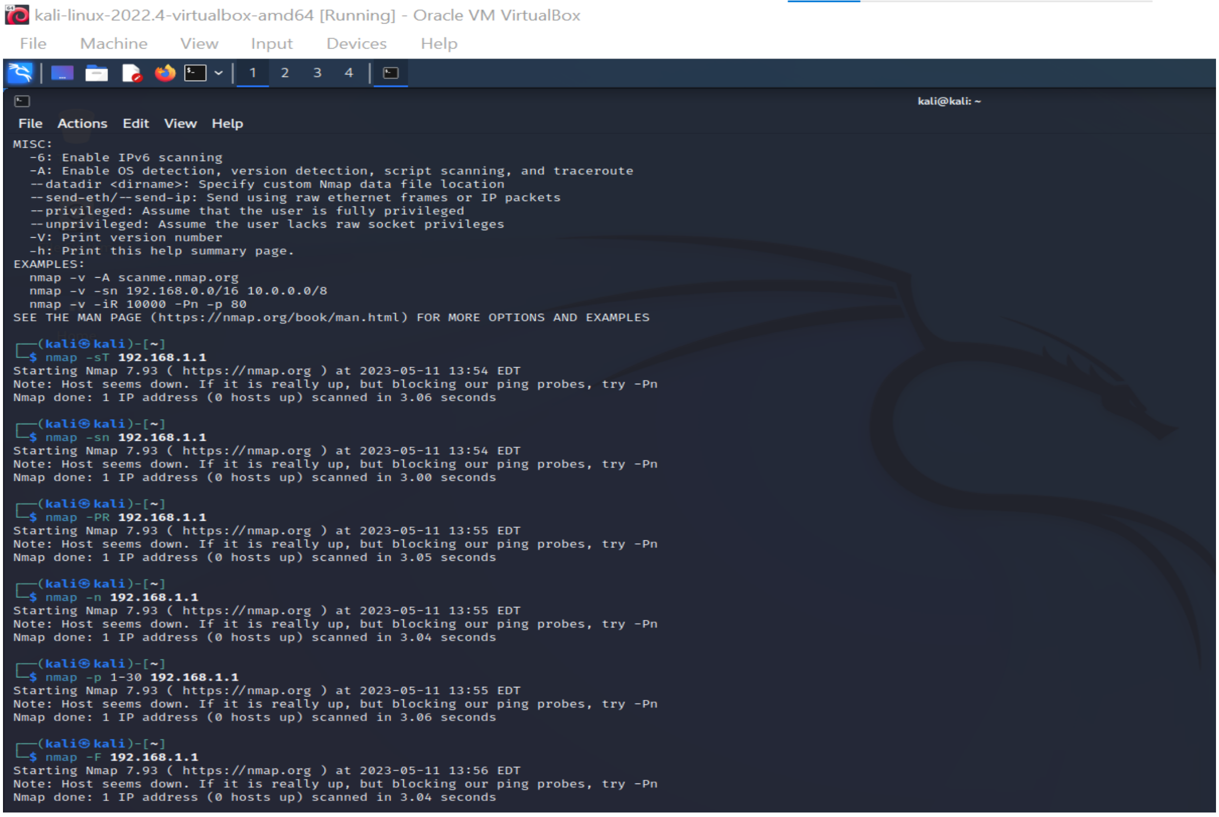
Flag	Use	Example
-T0	**paranoid IDS evasion**	**nmap -T0 192.168.1.1**
-T1	**sneaky IDS evasion**	**nmap -T1 192.168.1.1**
-T2	**polite IDS evasion**	**nmap -T2 192.168.1.1**

-T3	normal IDS evasion	nmap -T3 192.168.1.1
-T4	aggressive speed scan	nmap -T4 192.168.1.1
-T5	insane speed scan	nmap -T5 192.168.1.1

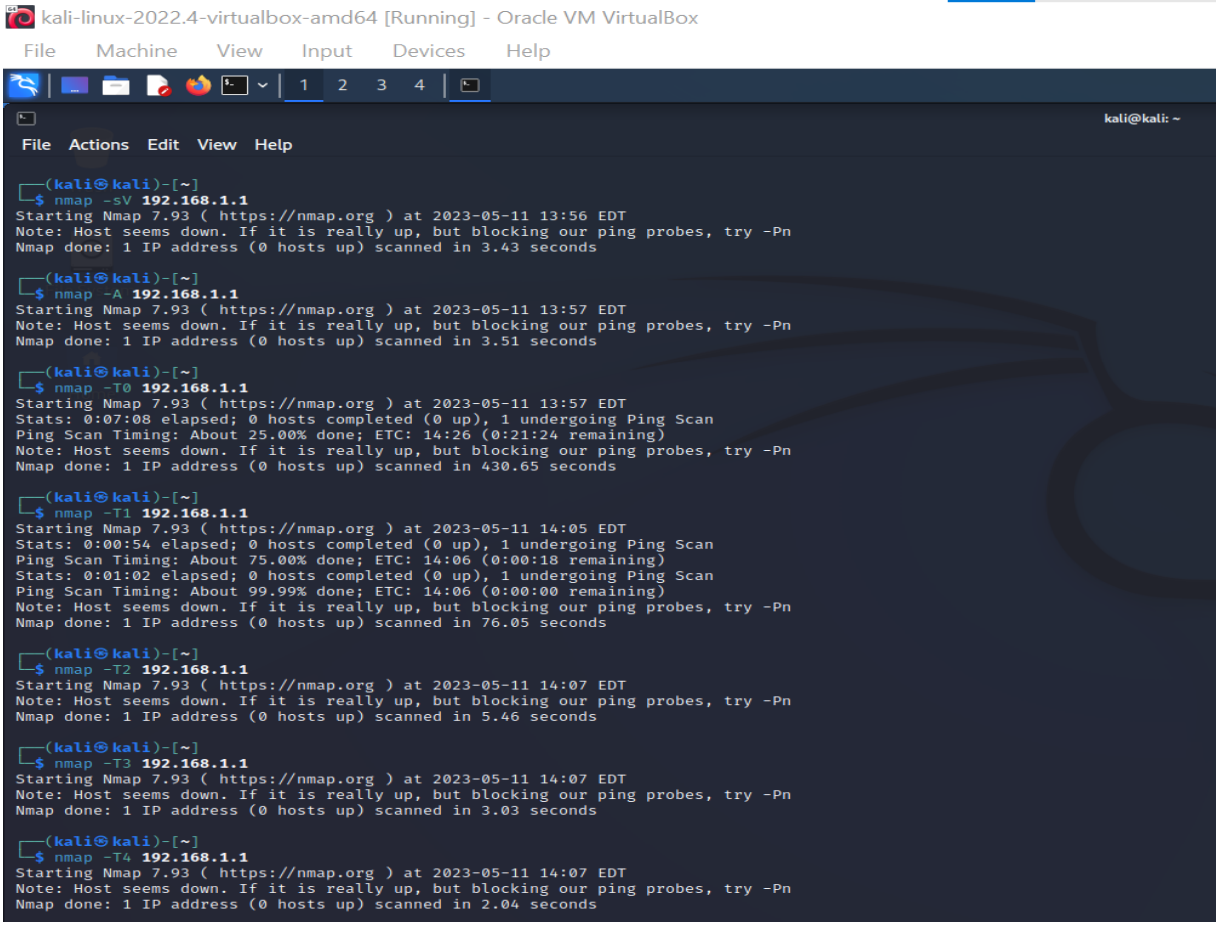
Output :


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

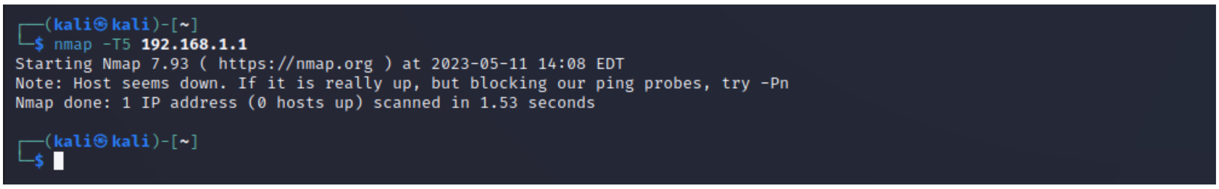
```
┌──(kali㉿kali)-[~]
└─$ nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:54 EDT
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 3.06 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:54 EDT
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 3.00 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -PR 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:55 EDT
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 3.05 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -n 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:55 EDT
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 3.04 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 1-30 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:55 EDT
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 3.06 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:56 EDT
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 3.04 seconds
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:56 EDT
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 3.43 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:57 EDT
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 3.51 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T0 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 13:57 EDT
Stats: 0:07:08 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 25.00% done; ETC: 14:26 (0:21:24 remaining)
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 430.65 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T1 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:05 EDT
Stats: 0:00:54 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 75.00% done; ETC: 14:06 (0:00:18 remaining)
Stats: 0:01:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 99.99% done; ETC: 14:06 (0:00:00 remaining)
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 76.05 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T2 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:07 EDT
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 5.46 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T3 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:07 EDT
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 3.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T4 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:07 EDT
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 2.04 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -T5 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 14:08 EDT
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 1.53 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Result :

Hence the nmap scan performed successfully