

## Exercise No 1: 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

#### Step4

#### PORT SPECIFICATION

<u>Flag</u>	<u>Use</u>	<u>Use</u>
<b>-p</b>	<b>specify a port or port range</b>	<b>nmap -p 1-30 192.168.1.1</b>
<b>-p-</b>	<b>scan all ports</b>	<b>nmap -p- 192.168.1.1</b>
<b>F</b>	<b>fast port scan</b>	<b>nmap -F 192.168.1.1</b>

#### 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@kali: ~
File Actions Edit View Help
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/url>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
--G: 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 scanner.nmap.org
nmap -v -sn 192.168.0.0/26 10.0.0.0/8
nmap -v -iR 100000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

kali@kali:~$ nmap -T4 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:38 EST
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 -p 1-20 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:38 EST
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 -F 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:39 EST
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:~$

```

RESULT: Hence the nmap scan performed successfully