K.Gowtham
192011090

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)

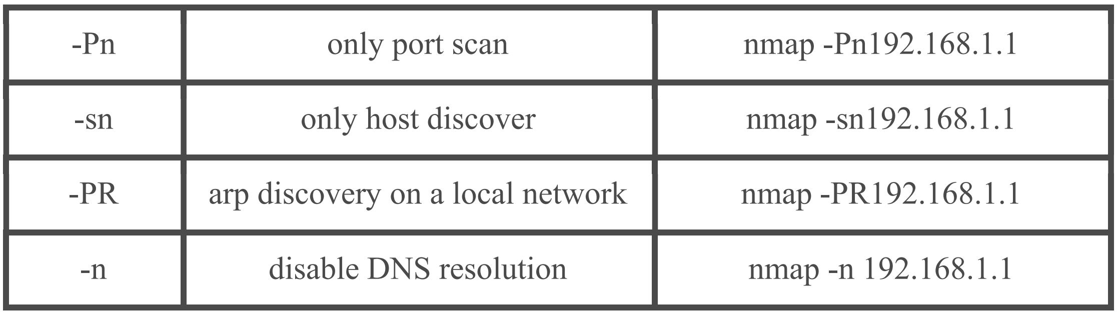
Step 2: Perform different types of scan
(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

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

Flag	**Use**	**Example**
-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

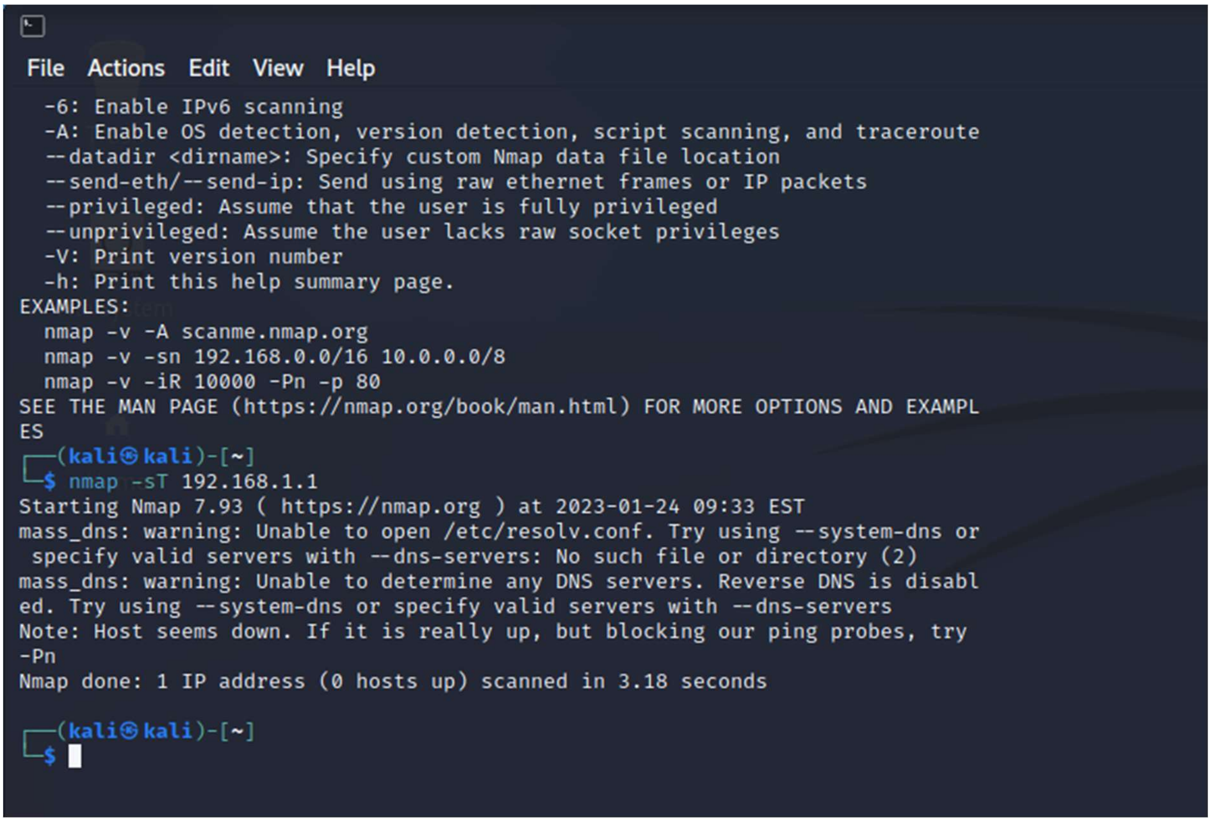
Step 6:-

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

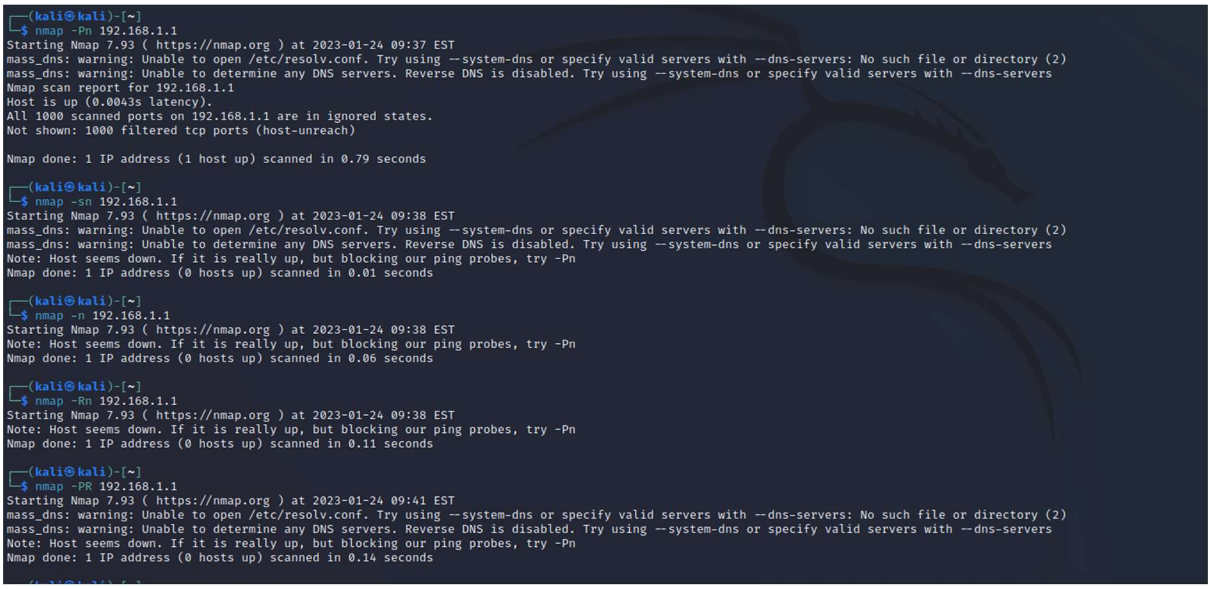
Output:

1.Scanning techniques



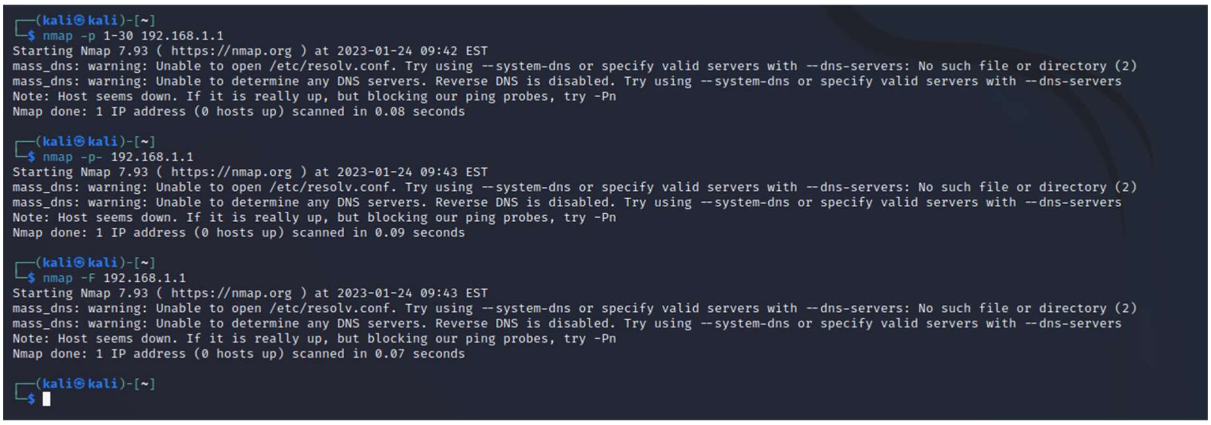
```
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: 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 EXAMPL
ES
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:33 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
 specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
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 3.18 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

2.Host Discovery



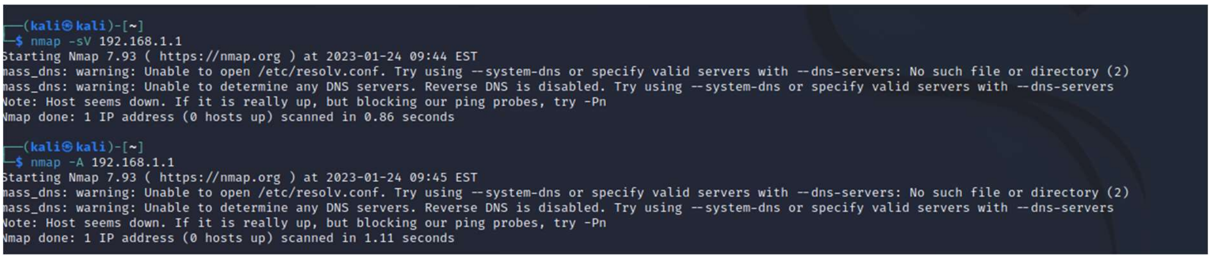
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:37 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.0043s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (host-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:38 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.01 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -n 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:38 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 0.06 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Rn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:38 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 0.11 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -PR 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:41 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.14 seconds

┌──(kali㉿kali)-[~]
```

3.Port specification



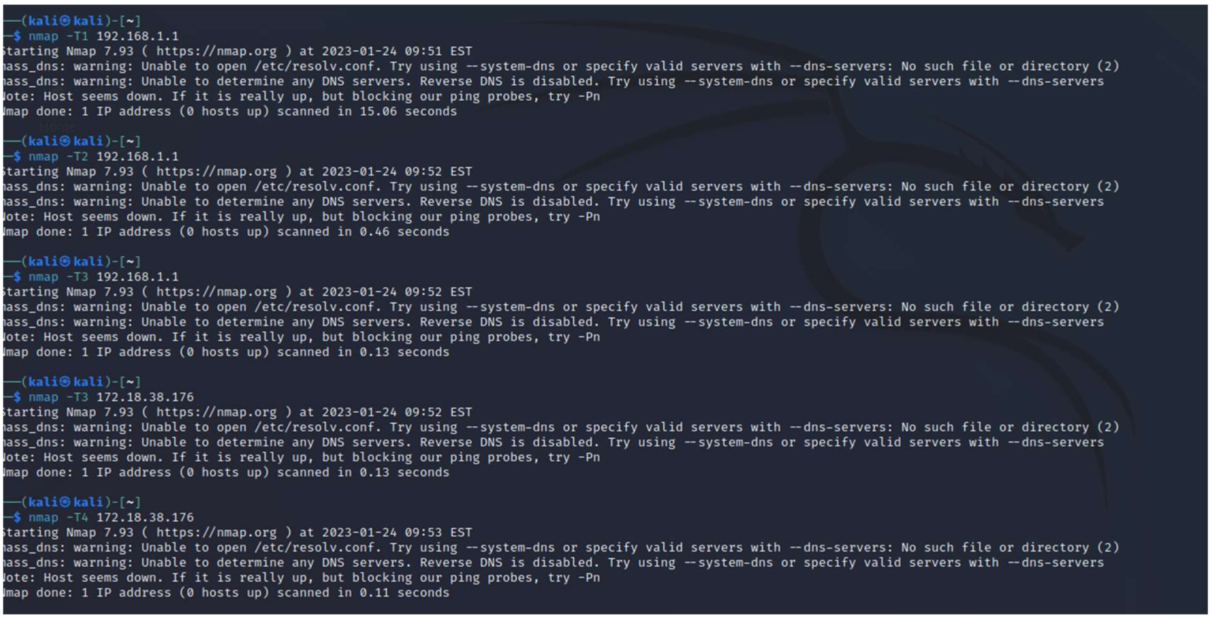
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-30 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:42 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.08 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:43 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.09 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:43 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.07 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

4.Service version and Os detection



```
──(kali㉿kali)-[~]
─$ nmap -sV 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:44 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.86 seconds

──(kali㉿kali)-[~]
─$ nmap -A 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:45 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 1.11 seconds
```

5.Tming and Performance



```
──(kali㉿kali)-[~]
─$ nmap -T1 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:51 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 15.06 seconds

──(kali㉿kali)-[~]
─$ nmap -T2 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:52 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.46 seconds

──(kali㉿kali)-[~]
─$ nmap -T3 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:52 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.13 seconds

──(kali㉿kali)-[~]
─$ nmap -T3 172.18.38.176
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:52 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.13 seconds

──(kali㉿kali)-[~]
─$ nmap -T4 172.18.38.176
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 09:53 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 0.11 seconds
```

Result:

Hence the nmap scan performed successfully.