Date: 15/12 / 2024

Lab Practical 2__Nmap:

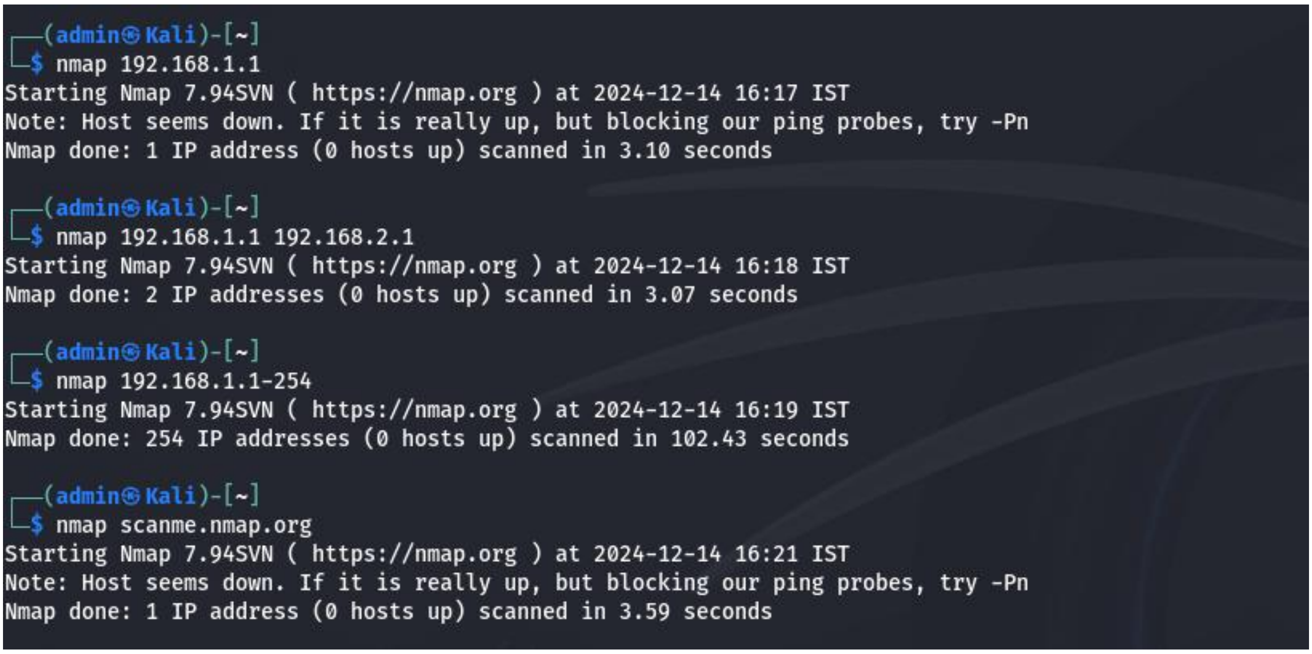
Nmap (Network Mapper):

Nmap is a powerful open-source network scanning tool widely used for network discovery, security auditing, and penetration testing. It allows you to identify live hosts, services, operating systems, and potential vulnerabilities in a network.

nmap 192.168.1.1: Scan for open TCP ports on a target.

nmap 192.168.1.1 192.168.1.2 : Scan List of Ips.

nmap 192.168.1.1-254 : To scan a specific range of IP.



```
┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:17 IST
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 3.10 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1 192.168.2.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:18 IST
Nmap done: 2 IP addresses (0 hosts up) scanned in 3.07 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1-254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:19 IST
Nmap done: 254 IP addresses (0 hosts up) scanned in 102.43 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:21 IST
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 3.59 seconds
```

Host /192.168.1.1 Discovery :

-sL (nmap 192.168.1.1-3 -sL):

Date: 15/12 / 2024

No Scan. List targets only

-sn(nmap 192.168.1.1/24 -sn) :
Disable port scanning

-Pn (nmap 192.168.1.1-5 -Pn) :
Disable host discovery. Port scan only

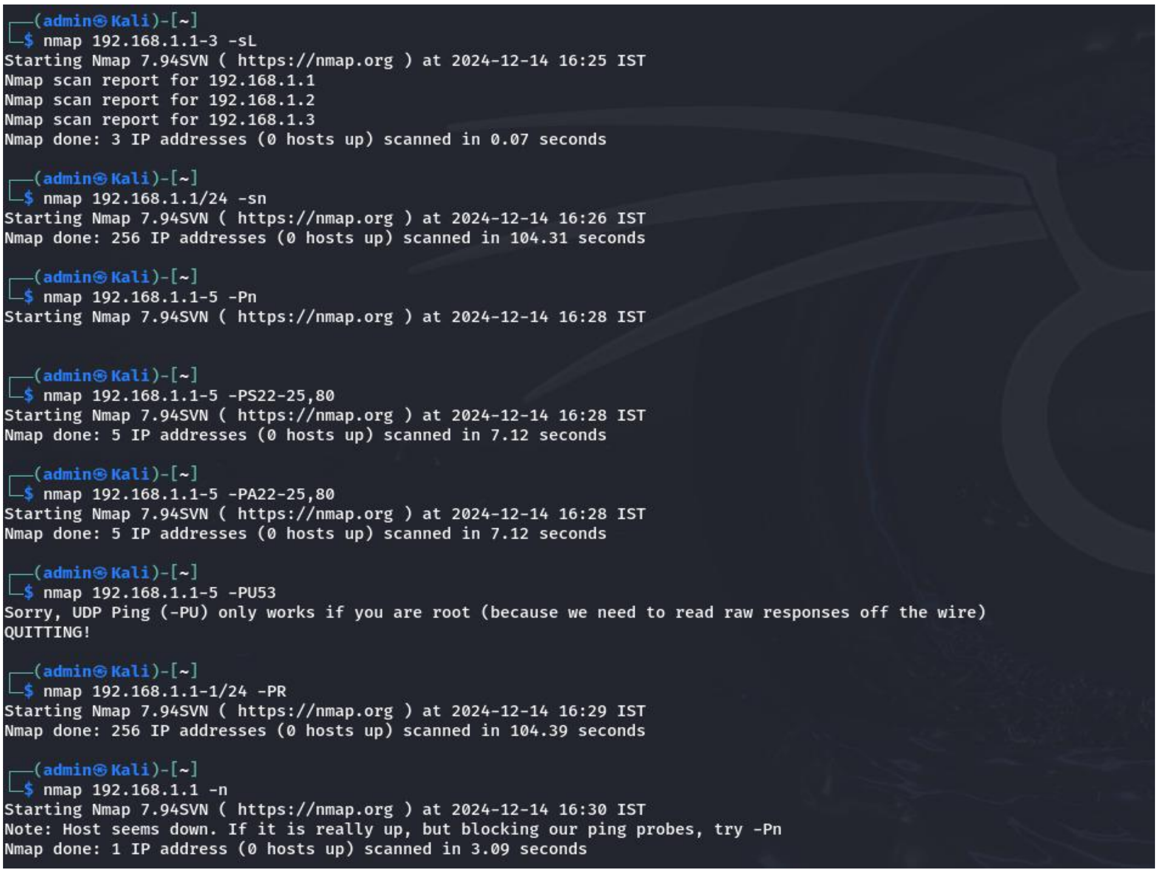
-PS (nmap 192.168.1.1-5 -PS22-25,80) :
TCP SYN discovery on port x. Port 80 by default

-PA (nmap 192.168.1.1-5 -PA22-25,80):
TCP ACK discovery on port x. Port 80 by default

-PU (nmap 192.168.1.1-5 -PU53):
UDP discovery on port x. Port 40125 by default

-PR (nmap 192.168.1.1-1/24 -PR):
ARP discovery on local network

-n (nmap 192.168.1.1 -n):
Never do DNS resolution



```
┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1-3 -sL
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:25 IST
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.3
Nmap done: 3 IP addresses (0 hosts up) scanned in 0.07 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1/24 -sn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:26 IST
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.31 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1-5 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:28 IST


┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1-5 -PS22-25,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:28 IST
Nmap done: 5 IP addresses (0 hosts up) scanned in 7.12 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1-5 -PA22-25,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:28 IST
Nmap done: 5 IP addresses (0 hosts up) scanned in 7.12 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1-5 -PU53
Sorry, UDP Ping (-PU) only works if you are root (because we need to read raw responses off the wire)
QUITTING!

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1-1/24 -PR
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:29 IST
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.39 seconds

┌──(admin㉿Kali)-[~]
└─$ nmap 192.168.1.1 -n
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:30 IST
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 3.09 seconds
```

Date: 15/12 / 2024

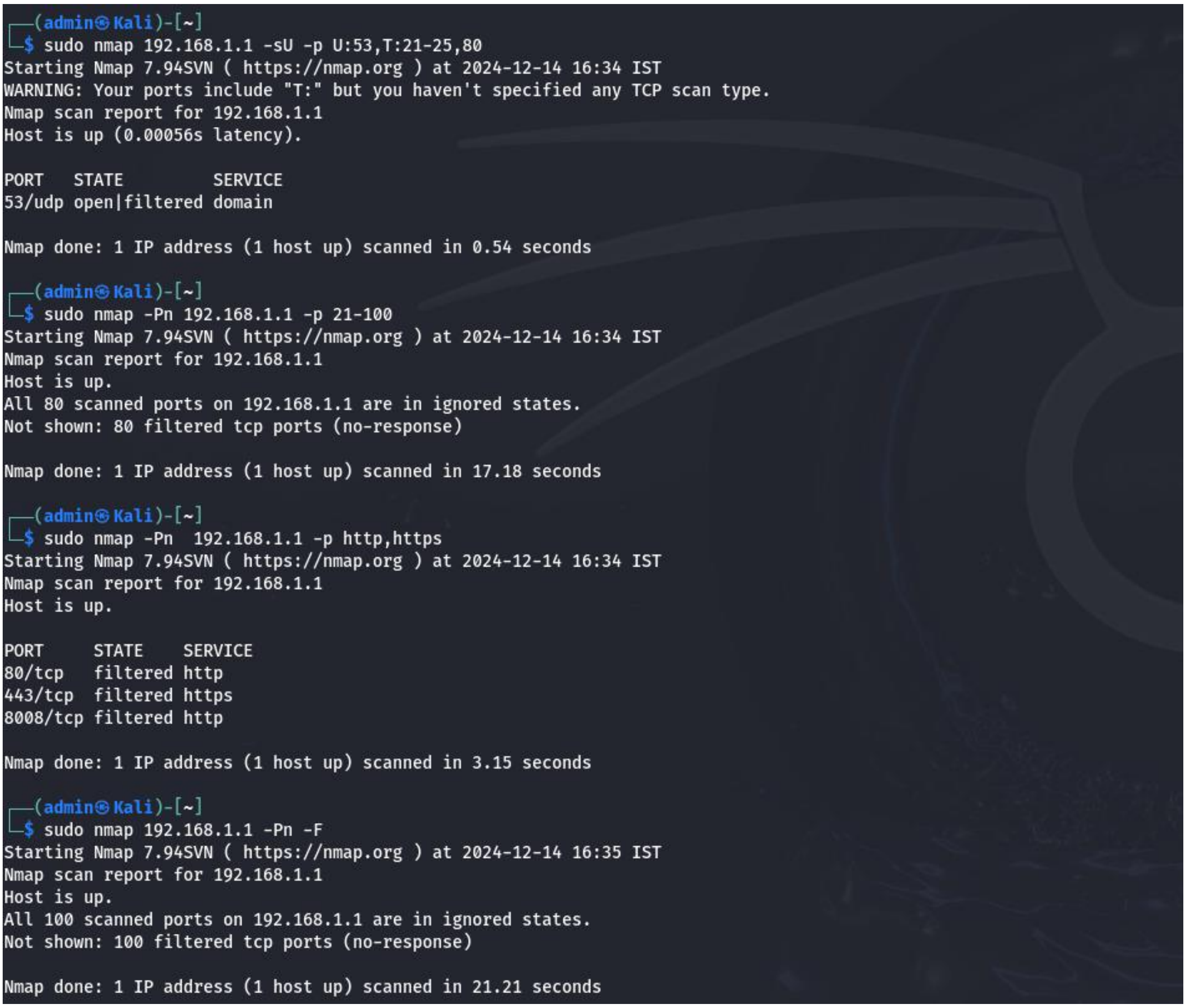
Port Specification :

-p (nmap 192.168.1.1 -p U:53,T:21-25,80):
Port scan multiple TCP and UDP ports

-p (nmap 192.168.1.1 -p 21-100) :
Port range.

-p (nmap 192.168.1.1 -p http,https) :
Port scan from service name

-F (nmap 192.168.1.1 –F) :
Fast port scan (100 ports)



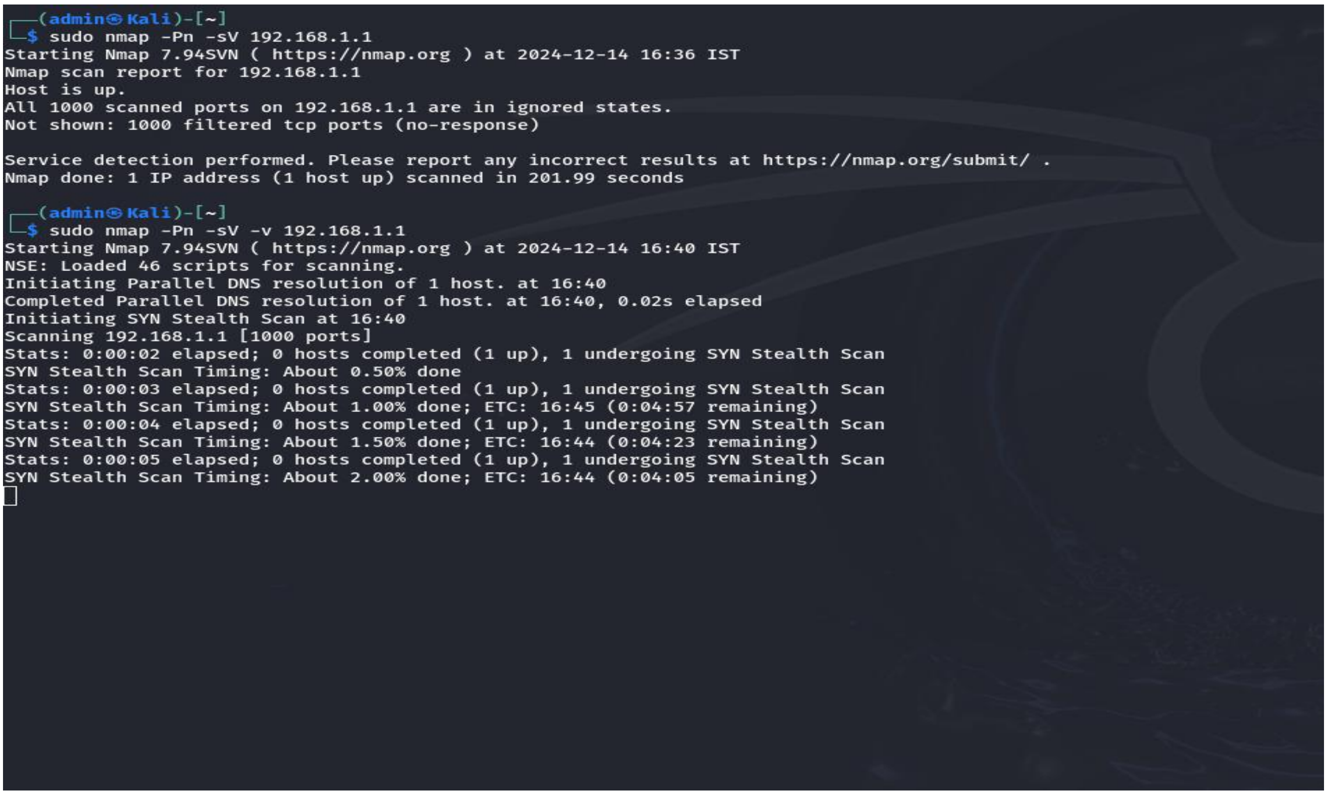
```
┌──(admin㉿Kali)-[~]
└─$ sudo nmap 192.168.1.1 -sU -p U:53,T:21-25,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:34 IST
WARNING: Your ports include "T:" but you haven't specified any TCP scan type.
Nmap scan report for 192.168.1.1
Host is up (0.00056s latency).

PORT   STATE         SERVICE
53/udp open|filtered domain

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds

┌──(admin㉿Kali)-[~]
└─$ sudo nmap -Pn 192.168.1.1 -p 21-100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:34 IST
Nmap scan report for 192.168.1.1
Host is up.
All 80 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 80 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 17.18 seconds

┌──(admin㉿Kali)-[~]
└─$ sudo nmap -Pn  192.168.1.1 -p http,https
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:34 IST
Nmap scan report for 192.168.1.1
Host is up.

PORT     STATE    SERVICE
80/tcp   filtered http
443/tcp  filtered https
8008/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds

┌──(admin㉿Kali)-[~]
└─$ sudo nmap 192.168.1.1 -Pn -F
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:35 IST
Nmap scan report for 192.168.1.1
Host is up.
All 100 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.21 seconds
```

Date: 15/12 / 2024

Service and Version Detection :

-sV (nmap 192.168.1.1 –sV) :
Attempts to determine the version of the service running on port.

-sV (nmap 192.168.1.1 –sV –v):
Shows the process of the command



```
┌──(admin㉿Kali)-[~]
└─$ sudo nmap -Pn -sV 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:36 IST
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.99 seconds

┌──(admin㉿Kali)-[~]
└─$ sudo nmap -Pn -sV -v 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 16:40 IST
NSE: Loaded 46 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 16:40
Completed Parallel DNS resolution of 1 host. at 16:40, 0.02s elapsed
Initiating SYN Stealth Scan at 16:40
Scanning 192.168.1.1 [1000 ports]
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.00% done; ETC: 16:45 (0:04:57 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.50% done; ETC: 16:44 (0:04:23 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.00% done; ETC: 16:44 (0:04:05 remaining)
```