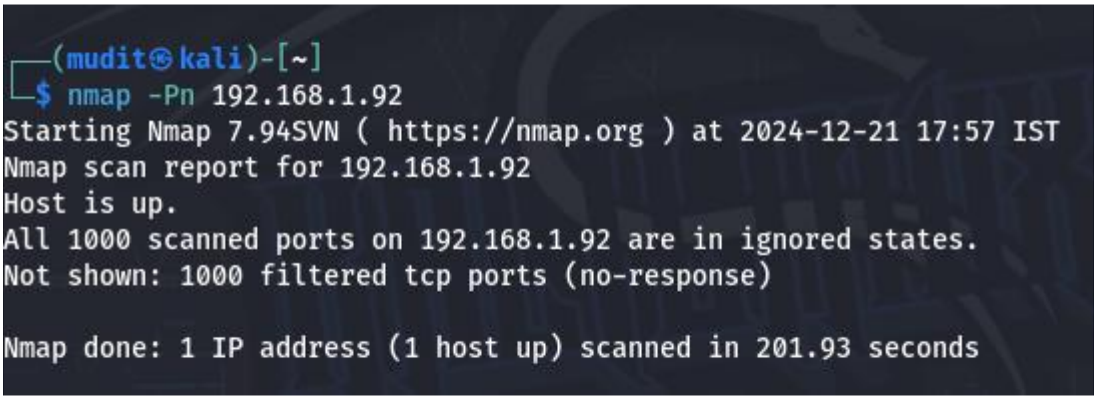
Date: / /

Lab Practical 2:

Perform NMAP tool for scanning system vulnerability.

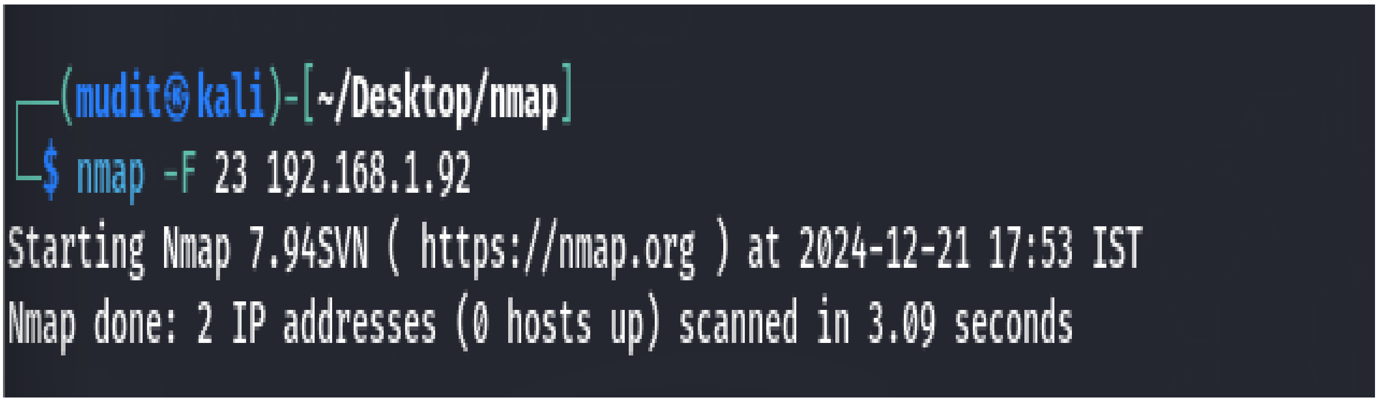
Commands:

- -Pn: The command is used for Port Scanning and no discovery of Hosts.



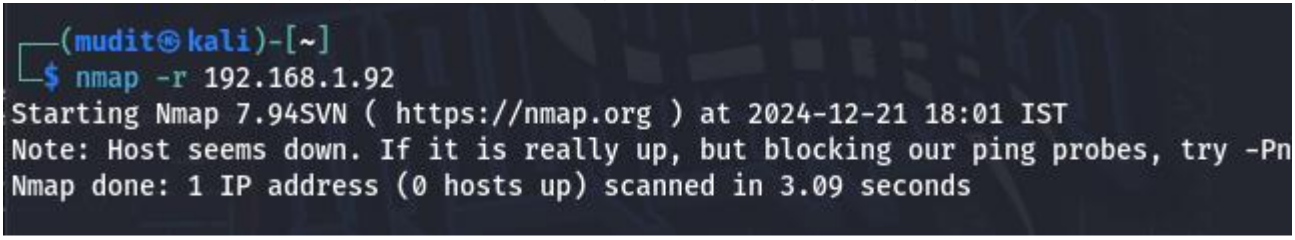
```
┌──(mudit㉿kali)-[~]
└─$ nmap -Pn 192.168.1.92
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 17:57 IST
Nmap scan report for 192.168.1.92
Host is up.
All 1000 scanned ports on 192.168.1.92 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.93 seconds
```

- -F: Fast scanning of ports for speeding up the process.



```
┌──(mudit㉿kali)-[~/Desktop/nmap]
└─$ nmap -F 23 192.168.1.92
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 17:53 IST
Nmap done: 2 IP addresses (0 hosts up) scanned in 3.09 seconds
```

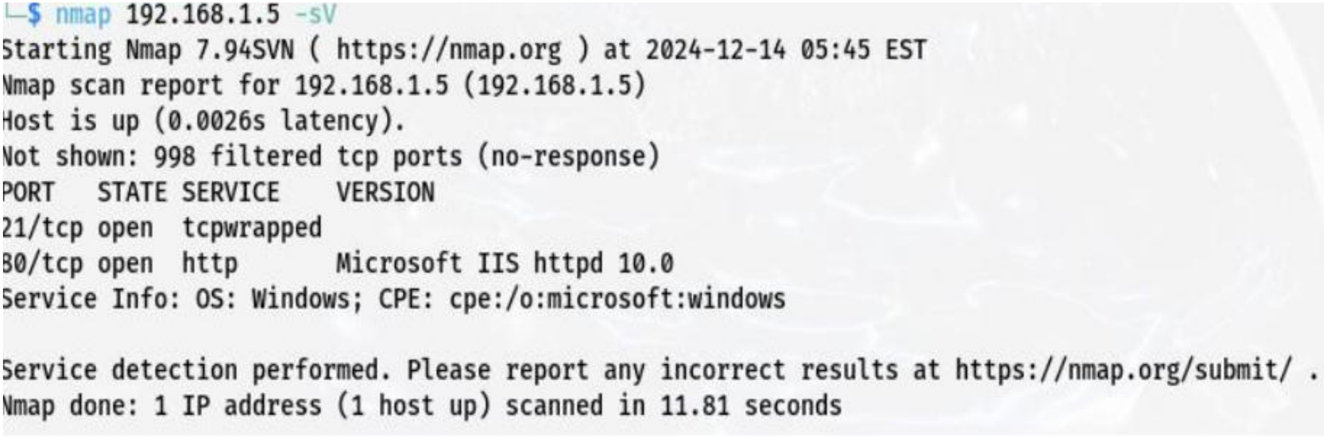
- -r: The command option is used for sequential scanning of the port.



```
┌──(mudit㉿kali)-[~]
└─$ nmap -r 192.168.1.92
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 18:01 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
```

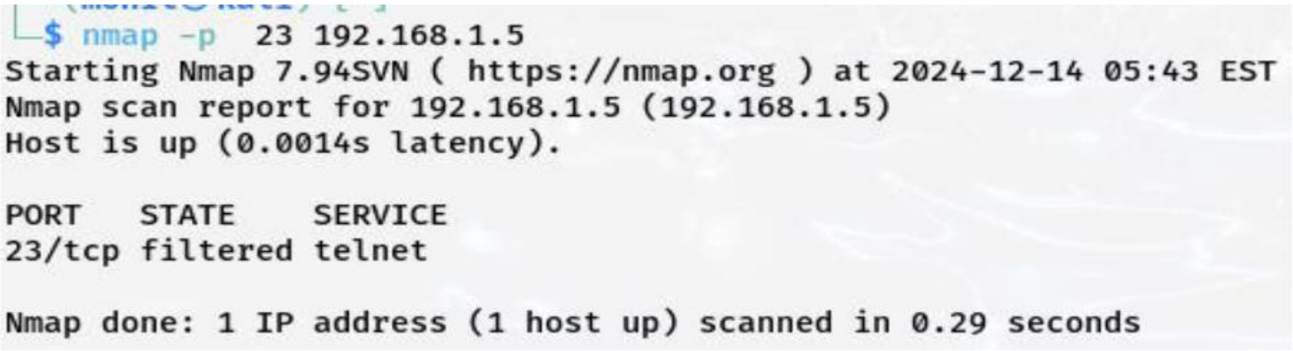
Date: / /

- -Sv: The command is used to identify and check for the version of service on that port.



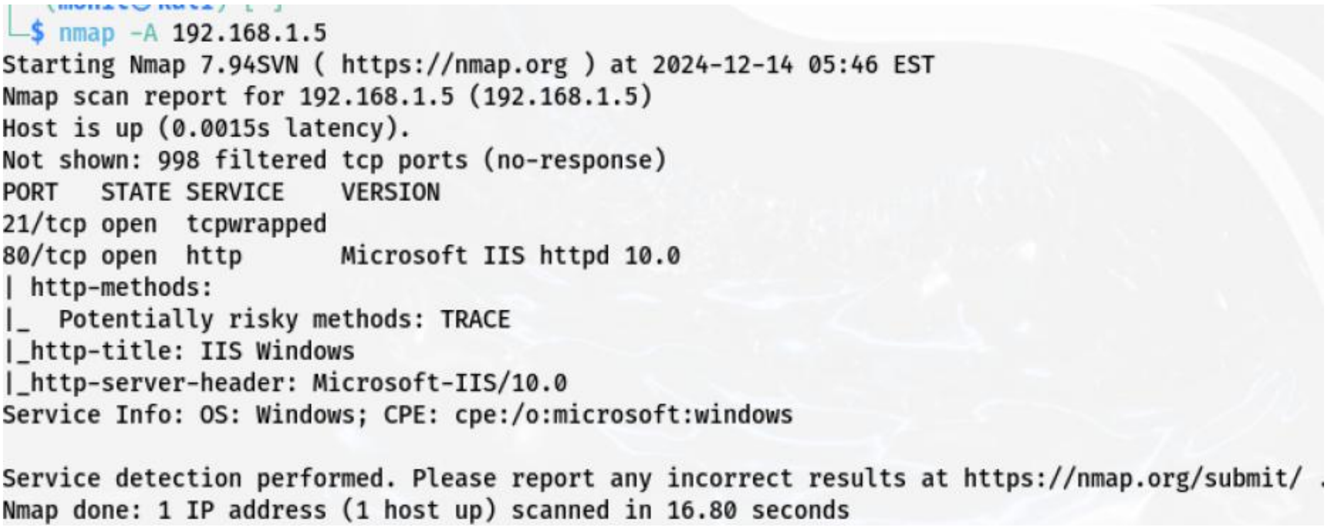
```
└─$ nmap 192.168.1.5 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 05:45 EST
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.0026s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
80/tcp open  http       Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.81 seconds
```

- -p: The command is used for scanning a specific port.



```
└─$ nmap -p  23 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 05:43 EST
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.0014s latency).

PORT    STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

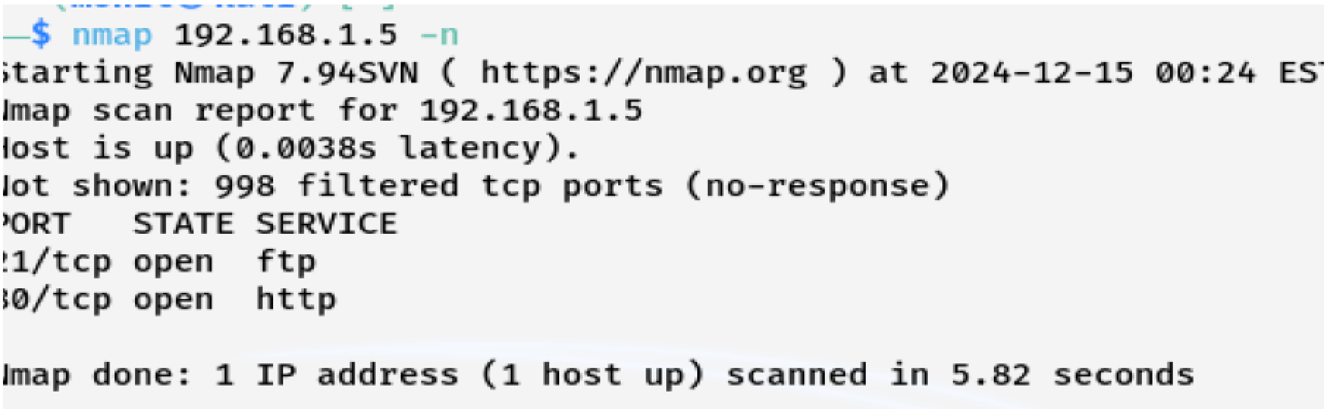
- -A: It enables OS detection, version detection, script tracing, traceroute.



```
└─$ nmap -A 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 05:46 EST
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
80/tcp open  http       Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

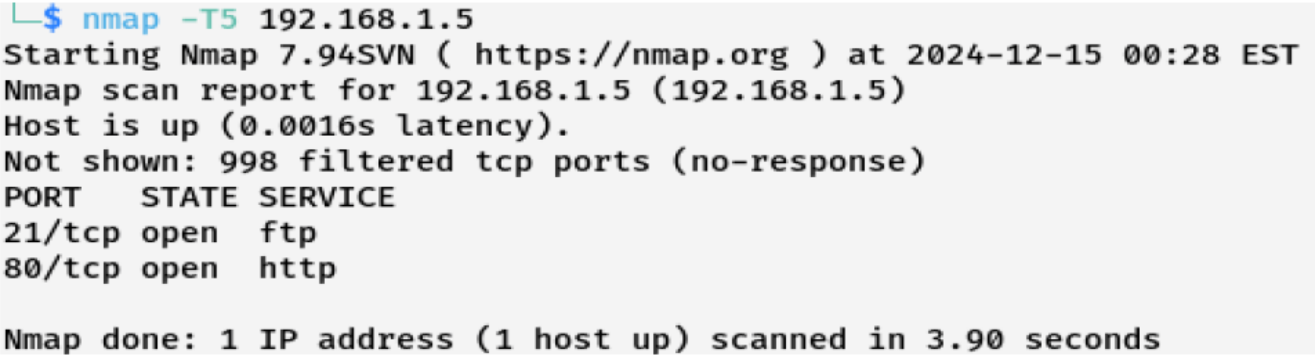
Date: / /

- -n: No DNA resolution over the port.

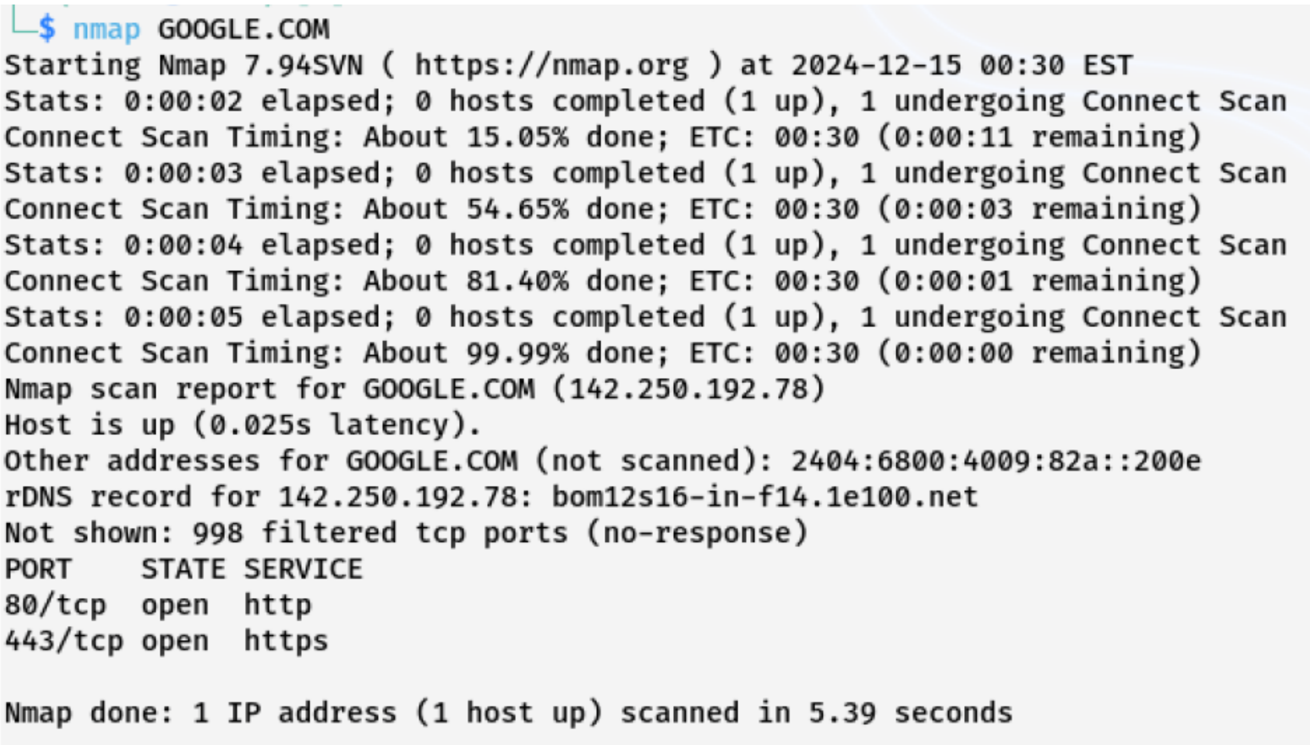


```
─$ nmap 192.168.1.5 -n
tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 00:24 ES
Imap scan report for 192.168.1.5
lost is up (0.0038s latency).
Iot shown: 998 filtered tcp ports (no-response)
ORT    STATE SERVICE
1/tcp open  ftp
0/tcp open  http

Imap done: 1 IP address (1 host up) scanned in 5.82 seconds
```

- -T5: Very aggressive scanning on the port.



```
└─$ nmap -T5 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 00:28 EST
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.0016s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```



```
└─$ nmap GOOGLE.COM
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 00:30 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 15.05% done; ETC: 00:30 (0:00:11 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 54.65% done; ETC: 00:30 (0:00:03 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 81.40% done; ETC: 00:30 (0:00:01 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 00:30 (0:00:00 remaining)
Nmap scan report for GOOGLE.COM (142.250.192.78)
Host is up (0.025s latency).
Other addresses for GOOGLE.COM (not scanned): 2404:6800:4009:82a::200e
rDNS record for 142.250.192.78: bom12s16-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.39 seconds
```