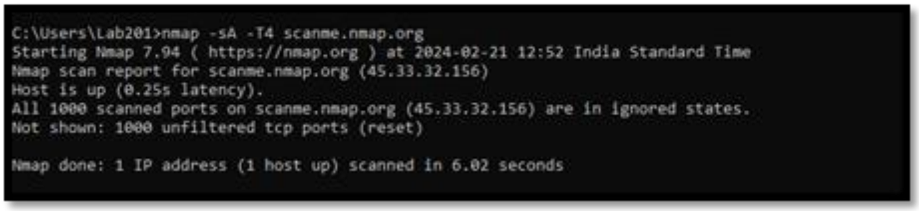
Practical 4

Use Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.

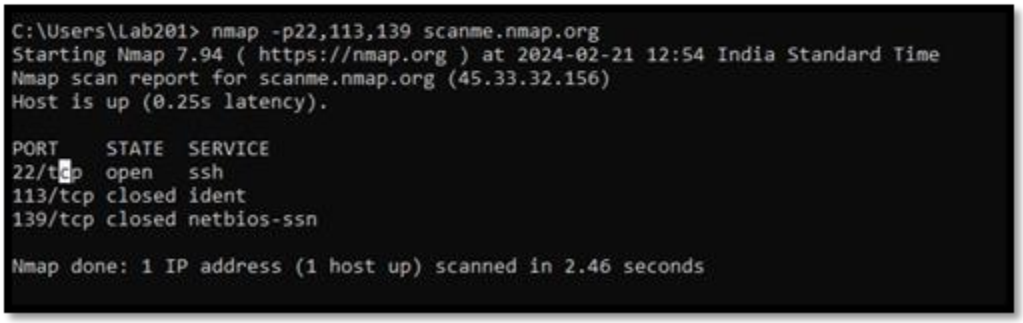
1. ACK -sA (TCP ACK scan)



```
C:\Users\Lab201>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 12:52 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 6.02 seconds
```

Command: nmap -sA -T4 scanme.nmap.org

2. SYN (Stealth) Scan (-sS)

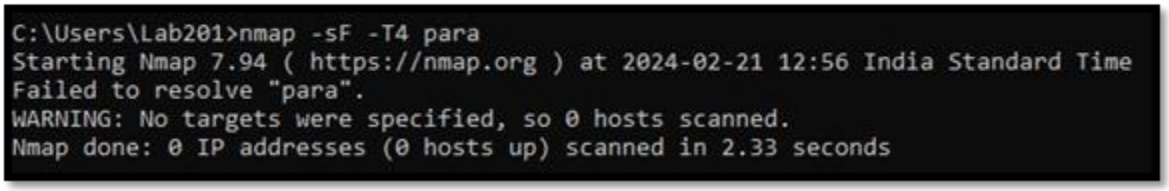


```
C:\Users\Lab201> nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 12:54 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
113/tcp closed ident
139/tcp closed netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
```

Command: nmap -p22,113,139 scanme.nmap.org

3. FIN Scan (-sF)

Command: nmap -sF -T4 para



```
C:\Users\Lab201>nmap -sF -T4 para
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-21 12:56 India Standard Time
Failed to resolve "para".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.33 seconds
```

Conclusion:- Above practical was successfully executed.