A.mukesh
192011505l
Ethical Hacking for mobile applications - ITA1437

Ex.No. 5- **: Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.**

Ack -sA (tcp ack scan)

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

```
C:\Users\Mukesh>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 13:16 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.069s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.36 seconds
```

SYN(Stealth) scan (-sS)

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

```
Select Command Prompt
Nmap done: 0 IP addresses (0 hosts up) scanned in 6.92 seconds

C:\Users\Mukesh>nmap -p 22,113,139 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 13:14 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.025s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 9.99 seconds
```

FIN Scan (-sF)
Command: **nmap -sF -T4 para**

```
C:\Users\Mukesh>nmap -sF -T4 para
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 13:13 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 6.92 seconds
```

NULL Scan (-sF)

Command: nmap –sN –p 22 scanme.nmap.org

```
C:\Users\Mukesh>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 13:31 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.012s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 8.64 seconds
```

XMAS Scan(-sX)

Command: **nmap -sX -T4 scanme.nmap.org**

```
C:\Users\Mukesh>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-14 13:15 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.076s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 18.53 seconds
```