

## EXPERIMENT 5

### ACK scan:

Command Prompt

```
C:\Users\dell>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-26 11:43 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.36s latency).
Other addresses for scanme.nmap.org (not scanned): 64:ff9b::2d21:209c
Not shown: 997 unfiltered tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
554/tcp   filtered rtsp
1723/tcp  filtered pptp

Nmap done: 1 IP address (1 host up) scanned in 31.24 seconds

C:\Users\dell>
```



## SYN scan:

```
Command Prompt

C:\Users\dell>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-26 11:46 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.41s latency).
Other addresses for scanme.nmap.org (not scanned): 64:ff9b::2d21:209c

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 3.75 seconds

C:\Users\dell>
```



# FIN scan

```
Command Prompt
C:\Users\dell>nmap -sF -T4 para
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-27 09:05 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 6.89 seconds

C:\Users\dell>
```

# NULL scan

```
Command Prompt
C:\Users\dell>nmap -sN -p22 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-26 11:51 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.42s latency).
Other addresses for scanme.nmap.org (not scanned): 64:ff9b::2d21:209c

PORT      STATE      SERVICE
22/tcp    open|filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 7.64 seconds
C:\Users\dell>
```

## XMAS scan:

```
Command Prompt
C:\Users\dell> nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-26 11:53 India Standard Time
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 15.50% done; ETC: 11:57 (0:03:38 remaining)
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 24.15% done; ETC: 11:57 (0:03:15 remaining)
Stats: 0:01:54 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 42.85% done; ETC: 11:58 (0:02:32 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 55.75% done; ETC: 11:57 (0:01:55 remaining)
Stats: 0:04:14 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 97.90% done; ETC: 11:57 (0:00:05 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.45s latency).
Other addresses for scanme.nmap.org (not scanned): 64:ff9b::2d21:209c
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 261.63 seconds
C:\Users\dell>
```