

Practical No.4

Aim: Port Scanning with NMap

- Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
- Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
- Analyze the scan results to gather information about the target system's network services.

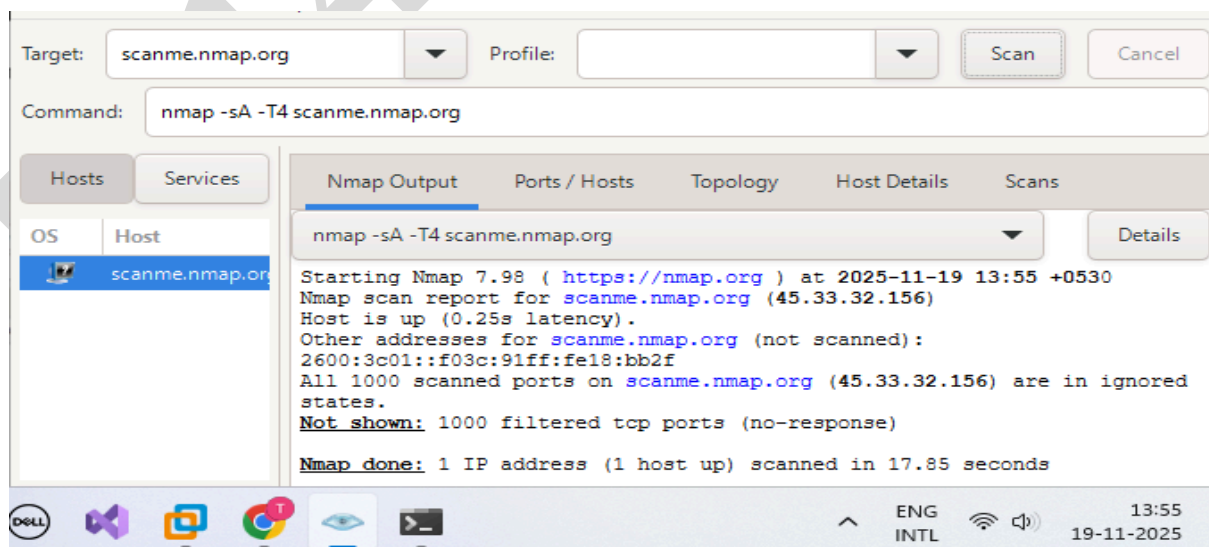
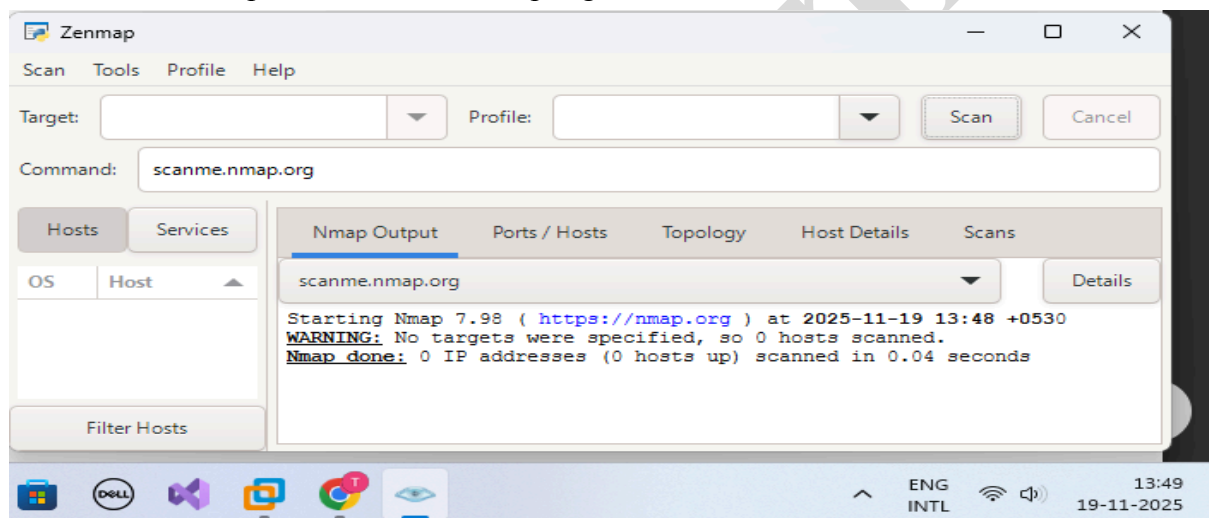
A. Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.

Step 1 : Install nmap from : <https://nmap.org/download> and open it.

Step 2 : Type “scanme.nmap.org” to check nmap

ACK-SA (TCP ACK scan)

COMMAND: `nmap -sA -T4 scanme.nmap.org`



```
C:\Users\itlab>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-19 13:59 +05
30
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f
03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in
ignored states.
Not shown: 1000 filtered tcp ports (no response)
```

B. Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their

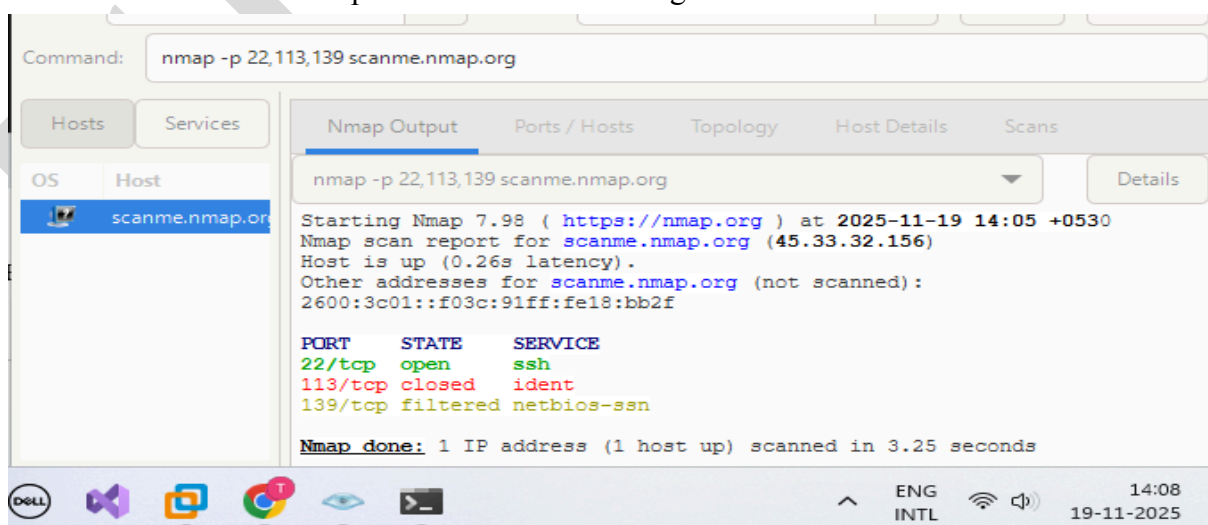
1) SYN (Stealth) Scan (-sS)

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



2) FIN (-sF)

COMMAND: nmap-sF-T4 scanme.name.org

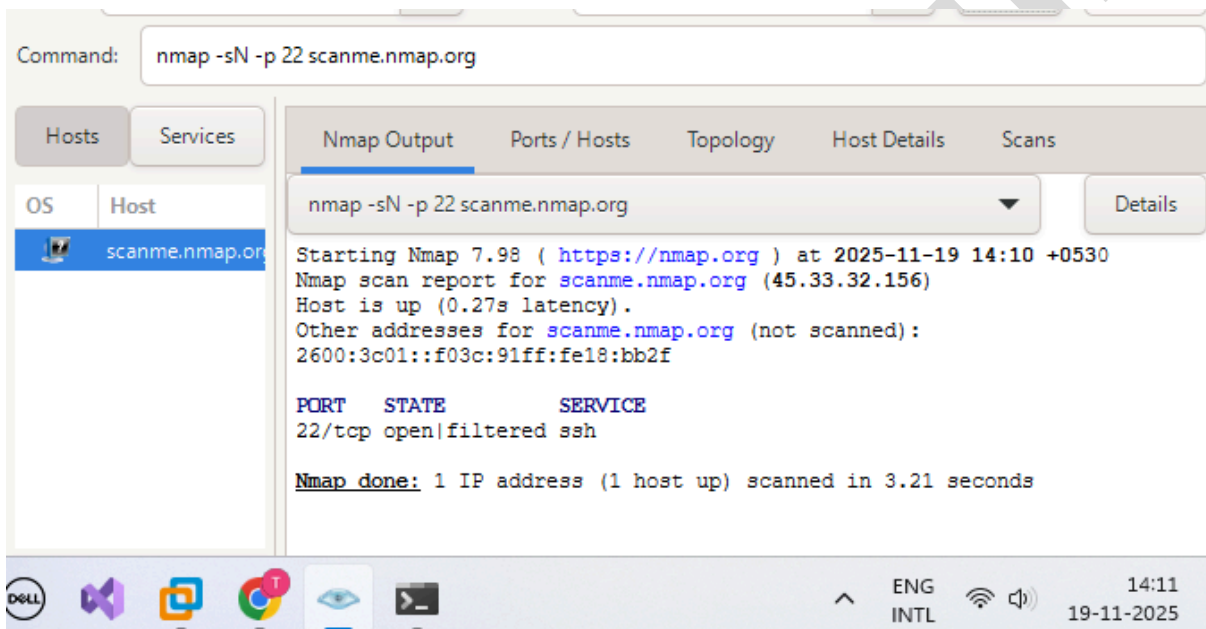


```
C:\Users\itlab>nmap -p 22,113,139 scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-19 14:07 +05
30
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f
03c:91ff:fe18:bb2f

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

3) NULL Scan (-sN)

COMMAND: nmap -sN -p 22 scanme.nmap.org



```
C:\Users\itlab>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-19 14:10 +05
30
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f
03c:91ff:fe18:bb2f

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 2.77 seconds
```

4) XMAS Scan (-sX)

COMMAND: nmap -sX -T4 scanme.nmap.org

