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.

Open cmd and type: nmap

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>nmap
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
```

1. nmap –sA –T4 www.google.com OR nmap –sA – T4 scanme.nmap.org

```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:04 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 998 unfiltered ports
PORT     STATE    SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 19.01 seconds
```

2. nmap –p22,113,139 scname.nmap.org

```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -p21,17,99 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:05 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT   STATE  SERVICE
17/tcp closed qotd
21/tcp closed ftp
99/tcp closed metagram

Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
```

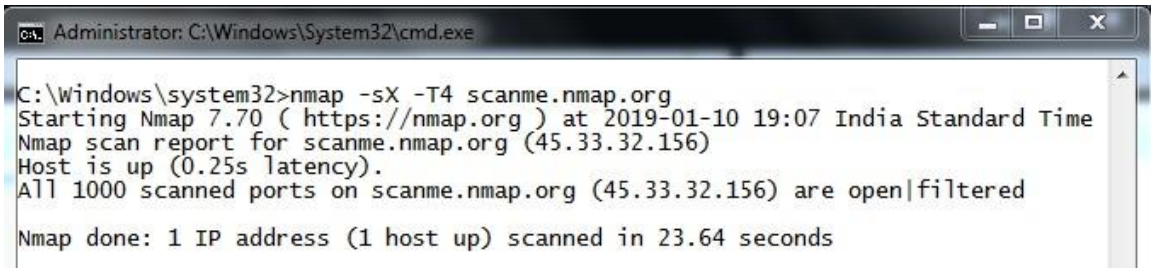
3. nmap –sF –T4 www.google.com

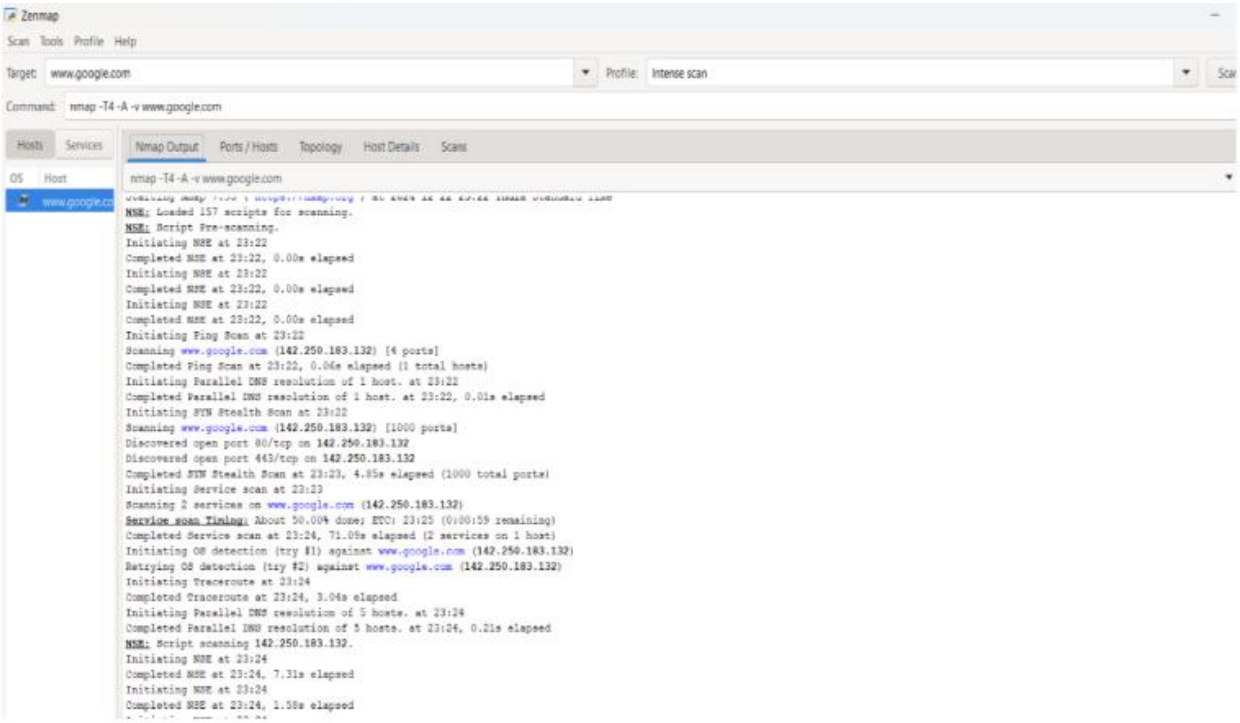
```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -sF -T4 www.google.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:06 India Standard Time
Nmap scan report for www.google.com (172.217.26.228)
Host is up (0.0074s latency).
rDNS record for 172.217.26.228: bom05s09-in-f4.1e100.net
All 1000 scanned ports on www.google.com (172.217.26.228) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds
```

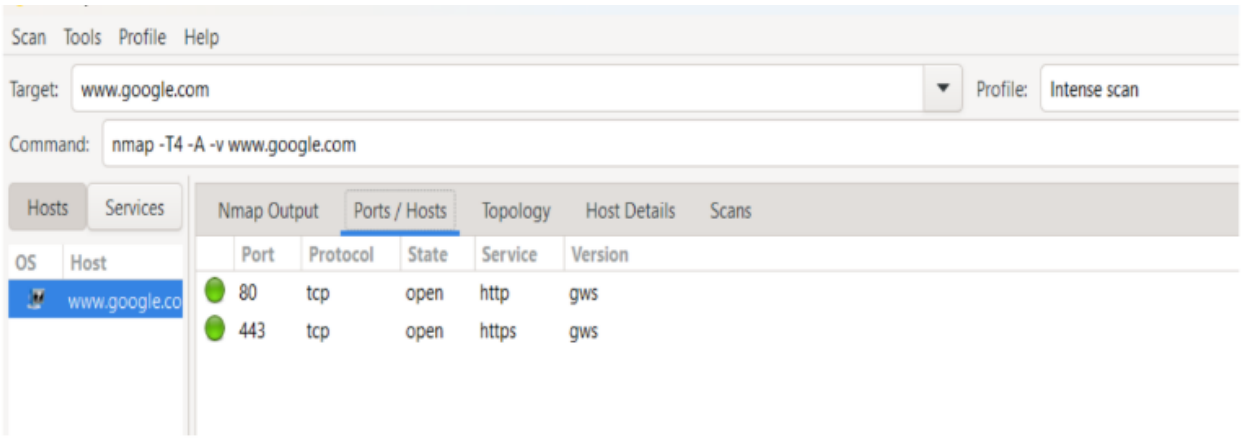
4. nmap –sN –p21 scanme.nmap.org

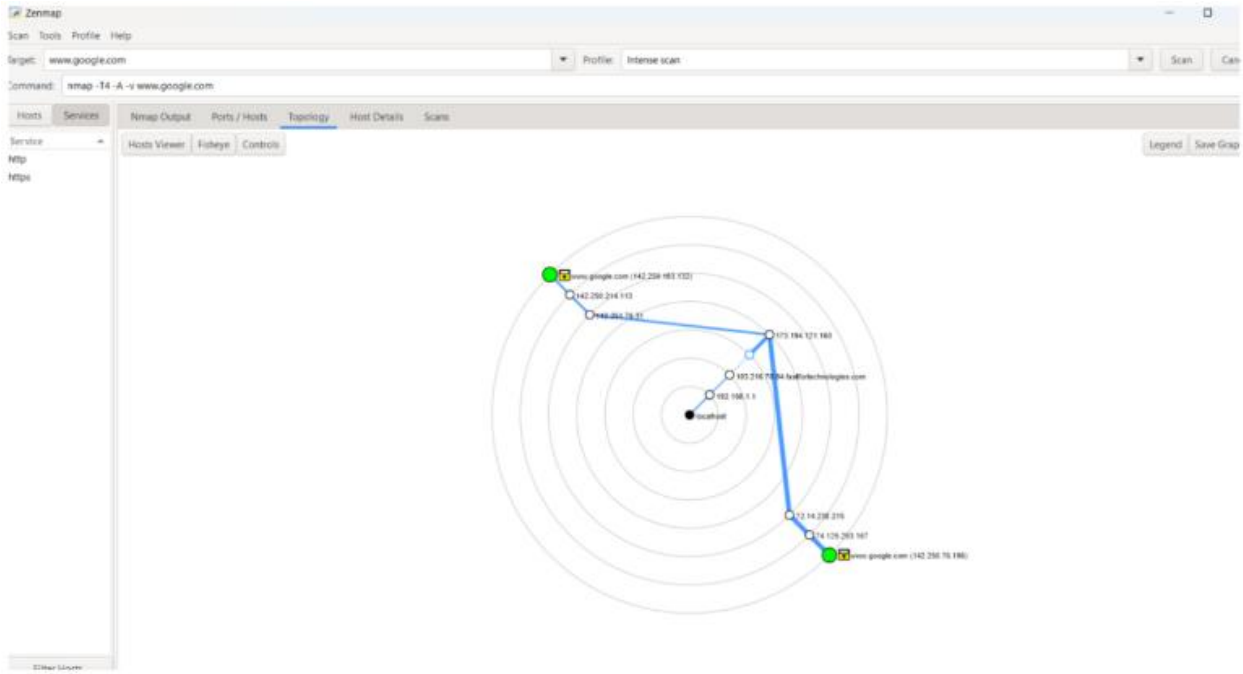
```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -sN -p21 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT   STATE         SERVICE
21/tcp open|filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds
```

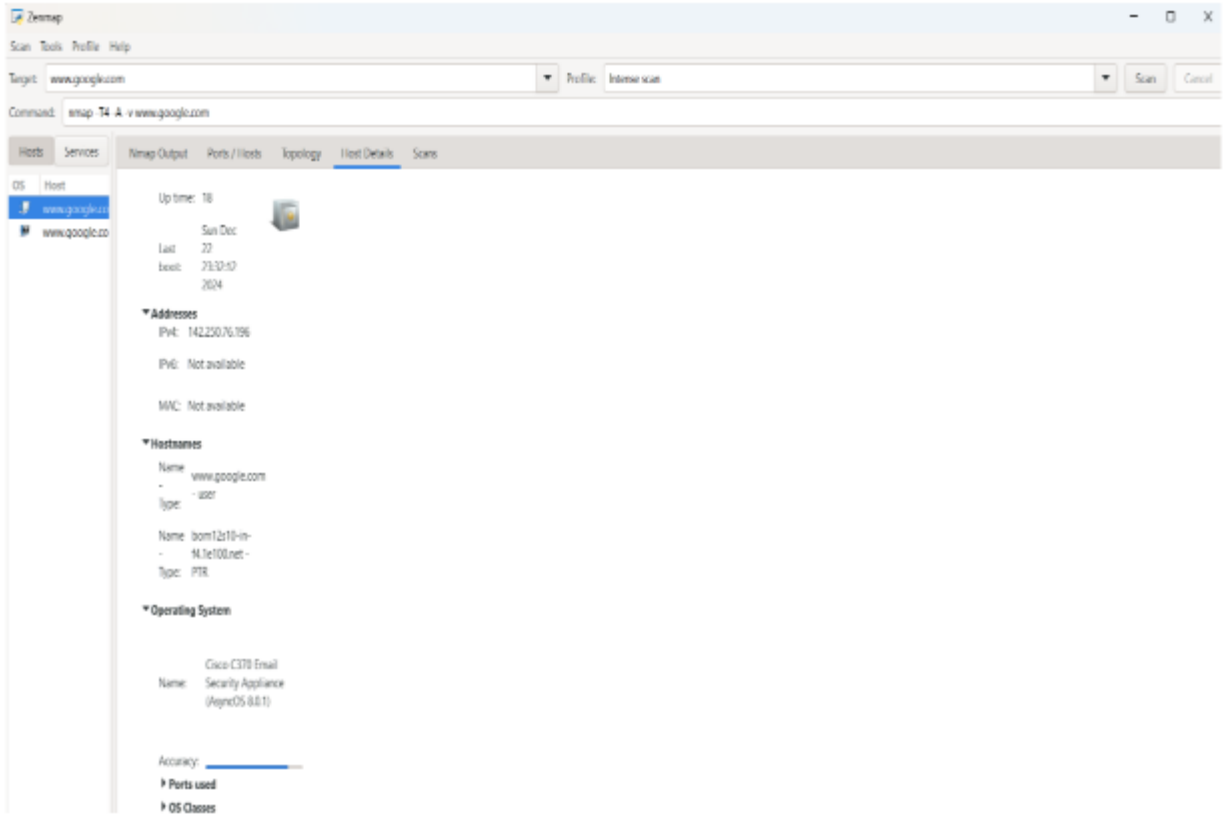
5. nmap –sX –T4 scanme.nmap.org

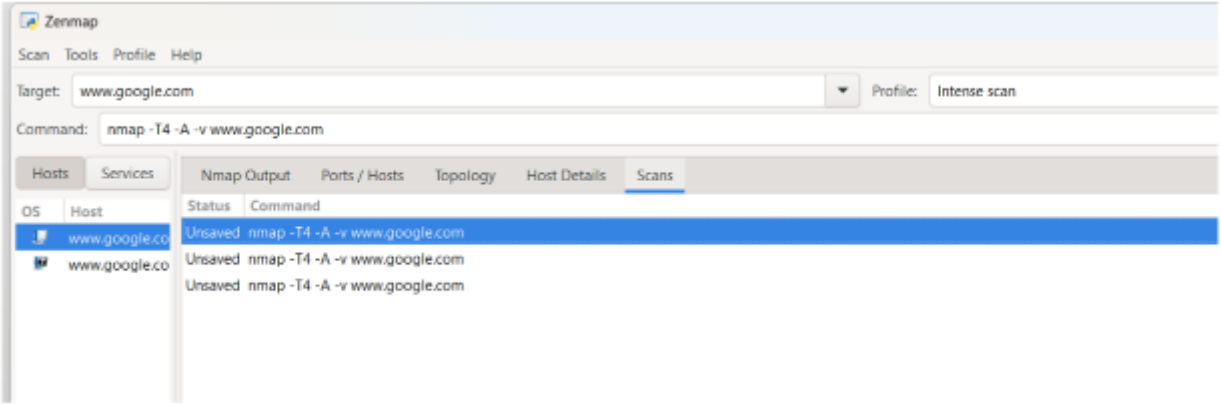







Zenmap
Scan Tools Profile Help
Target: www.google.com
Profile: Intense scan
Scan
Command: nmap -T4 -A -v www.google.com
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Grap
Service
http
https


Zenmap
Scan Tools Profile Help
Target: www.google.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v www.google.com
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
www.google.com
Up time: 18
Sun Dec 22 23:32:57 2024
Addresses
IPv4: 142.250.76.196
IPv6: Not available
MAC: Not available
Hostnames
Name: www.google.com
Type: user
Name: bom12s10-in-f4.1e100.net
Type: PTR
Operating System
Name: Cisco C370 Email Security Appliance (AsyncOS 8.0.1)
Accuracy:
Ports used
OS Classes



CONCLUSION: Using Nmap (Network mapping) the commands are successfully executed.