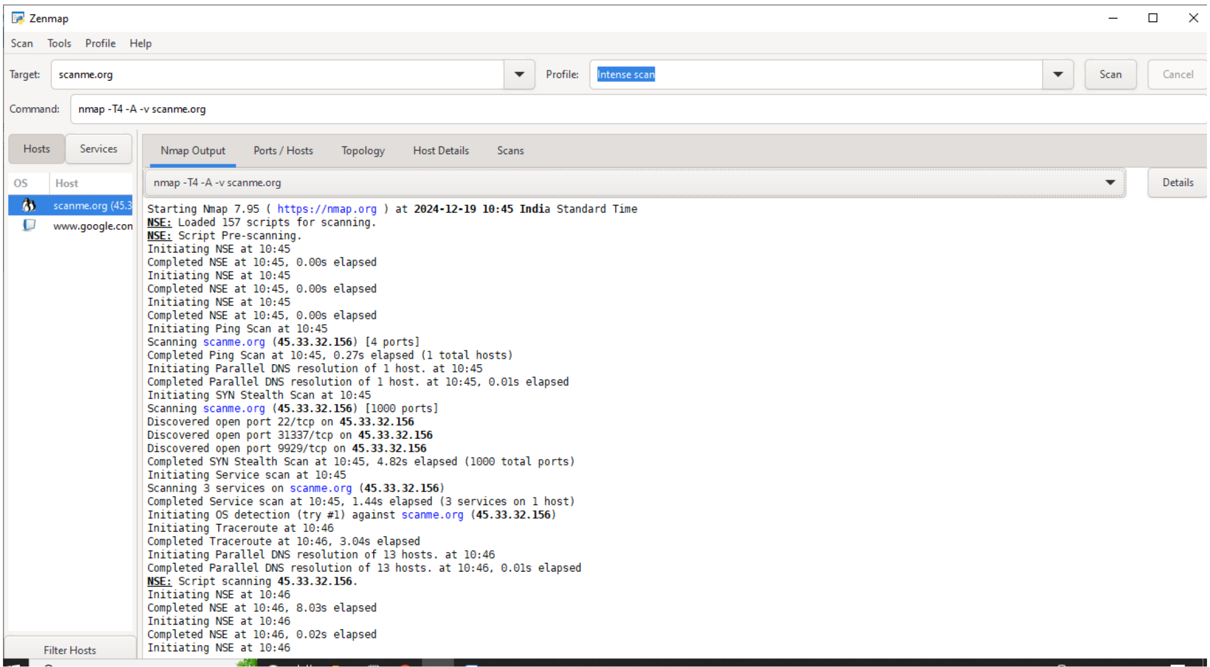
PRACTICAL NO 4

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.

Zenmap:-



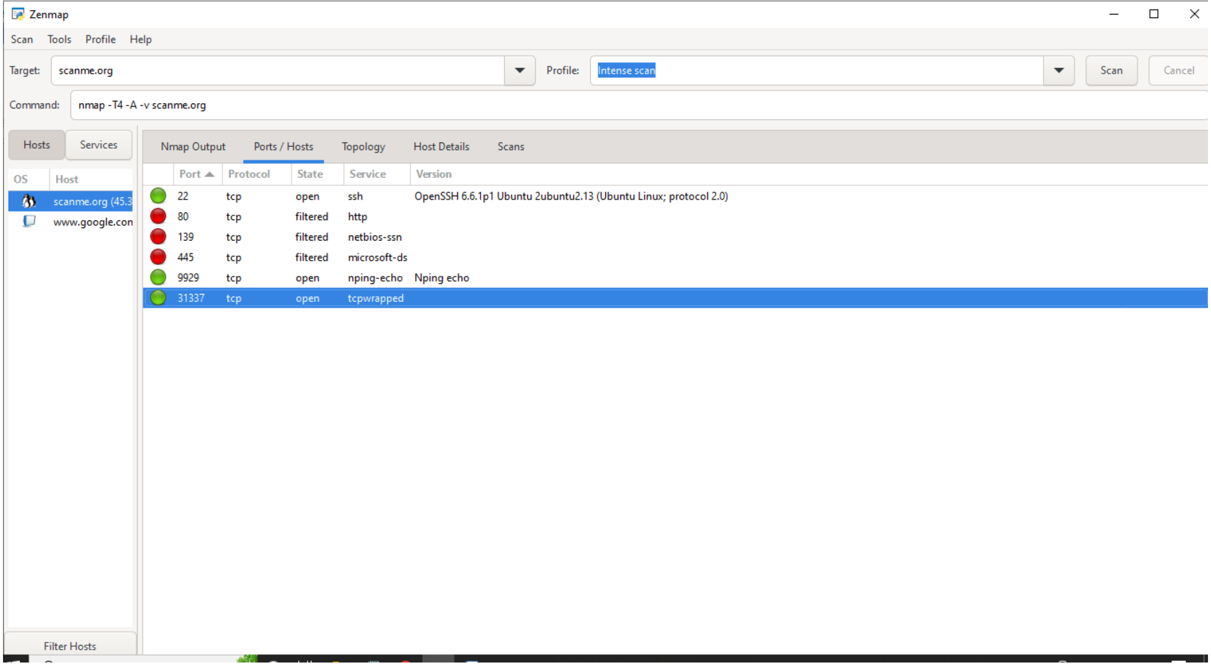
Target: scanme.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.org

nmap -T4 -A -v scanme.org

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-19 10:45 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Initiating NSE at 10:45
Completed NSE at 10:45, 0.00s elapsed
Initiating Ping Scan at 10:45
Scanning scanme.org (45.33.32.156) [4 ports]
Completed Ping Scan at 10:45, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:45
Completed Parallel DNS resolution of 1 host. at 10:45, 0.01s elapsed
Initiating SYN Stealth Scan at 10:45
Scanning scanme.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed SYN Stealth Scan at 10:45, 4.82s elapsed (1000 total ports)
Initiating Service scan at 10:45
Scanning 3 services on scanme.org (45.33.32.156)
Completed Service scan at 10:45, 1.44s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against scanme.org (45.33.32.156)
Initiating Traceroute at 10:46
Completed Traceroute at 10:46, 3.04s elapsed
Initiating Parallel DNS resolution of 13 hosts. at 10:46
Completed Parallel DNS resolution of 13 hosts. at 10:46, 0.01s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 10:46
Completed NSE at 10:46, 8.03s elapsed
Initiating NSE at 10:46
Completed NSE at 10:46, 0.02s elapsed
Initiating NSE at 10:46
```

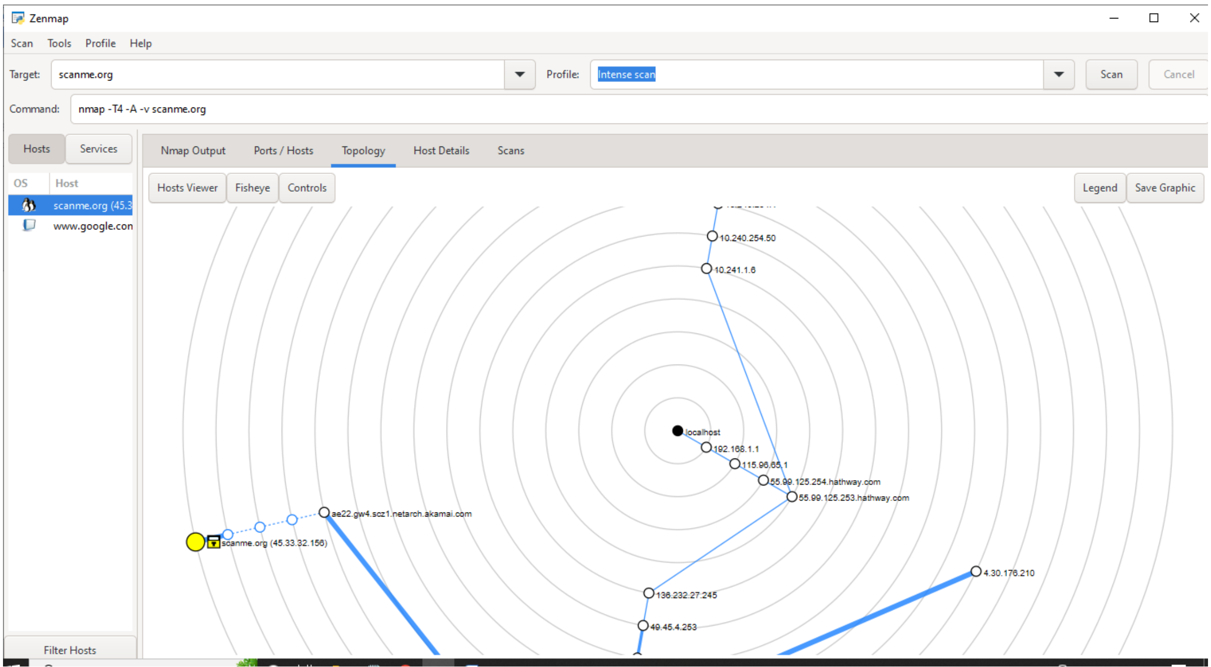


Target: scanme.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.org

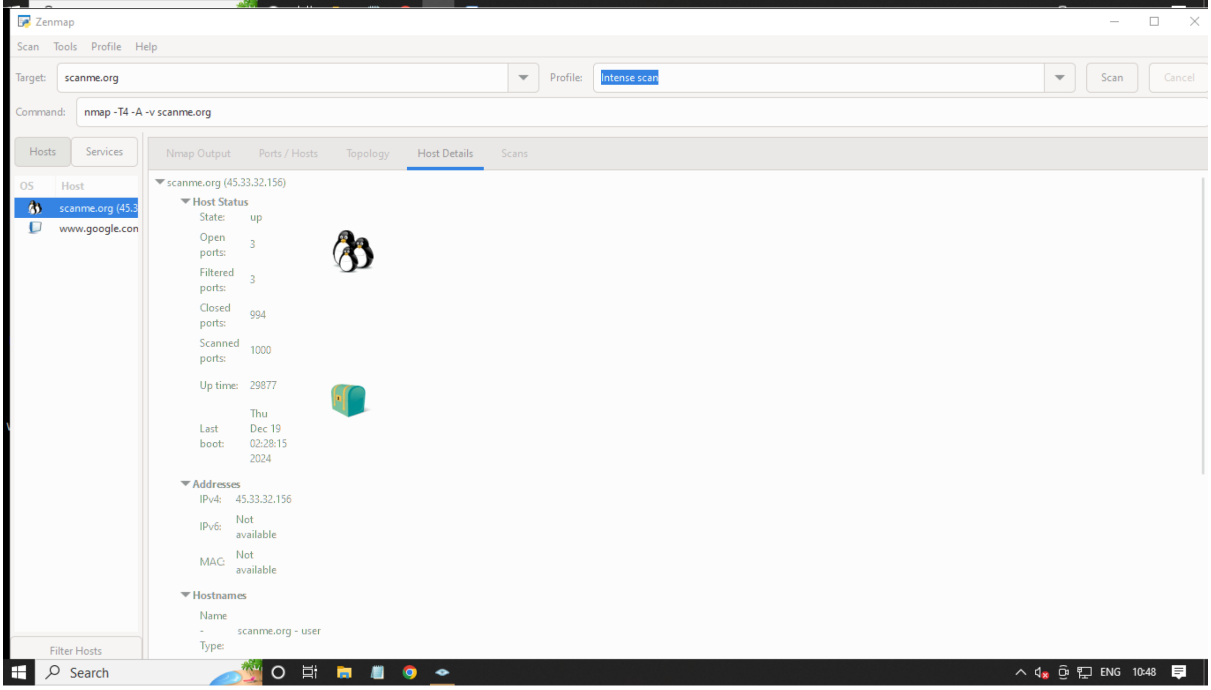
	Port ▲	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
●	80	tcp	filtered	http	
●	139	tcp	filtered	netbios-ssn	
●	445	tcp	filtered	microsoft-ds	
●	9929	tcp	open	nping-echo	Nping echo
●	31337	tcp	open	tcpwrapped	



Target: scanme.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.org



Target: scanme.org

Profile: Intense scan

Command: nmap -T4 -A -v scanme.org

scanme.org (45.33.32.156)

Host Status

State: up

Open ports: 3

Filtered ports: 3

Closed ports: 994

Scanned ports: 1000

Up time: 29877

Last boot: Thu Dec 19 02:28:15 2024

Addresses

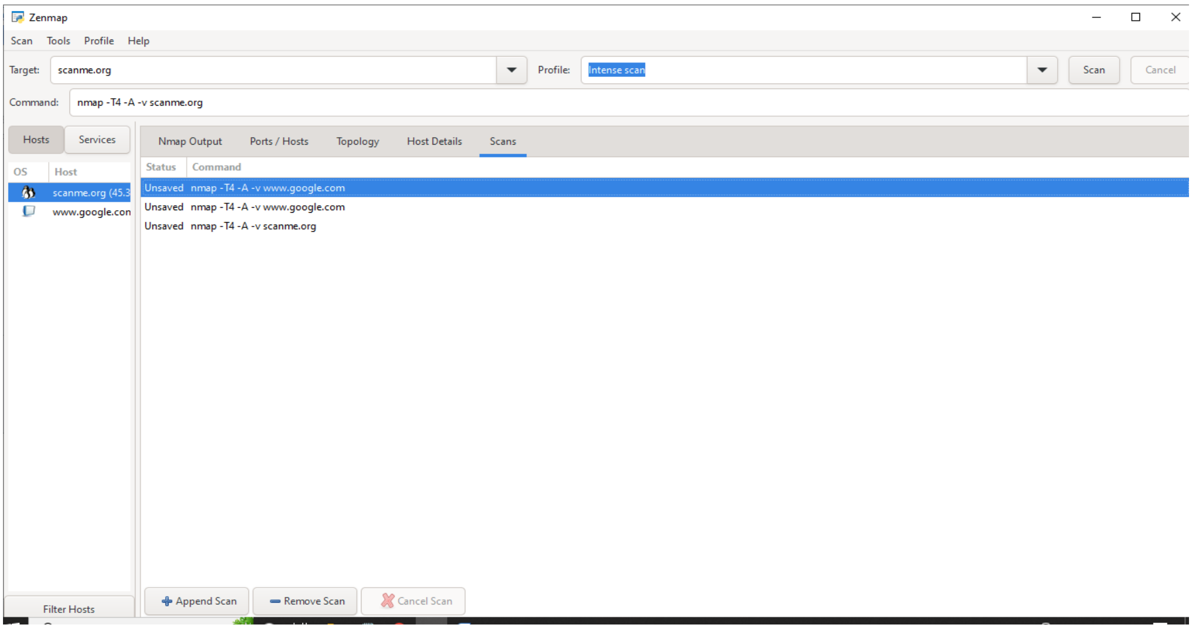
IPv4: 45.33.32.156

IPv6: Not available

MAC: Not available

Hostnames

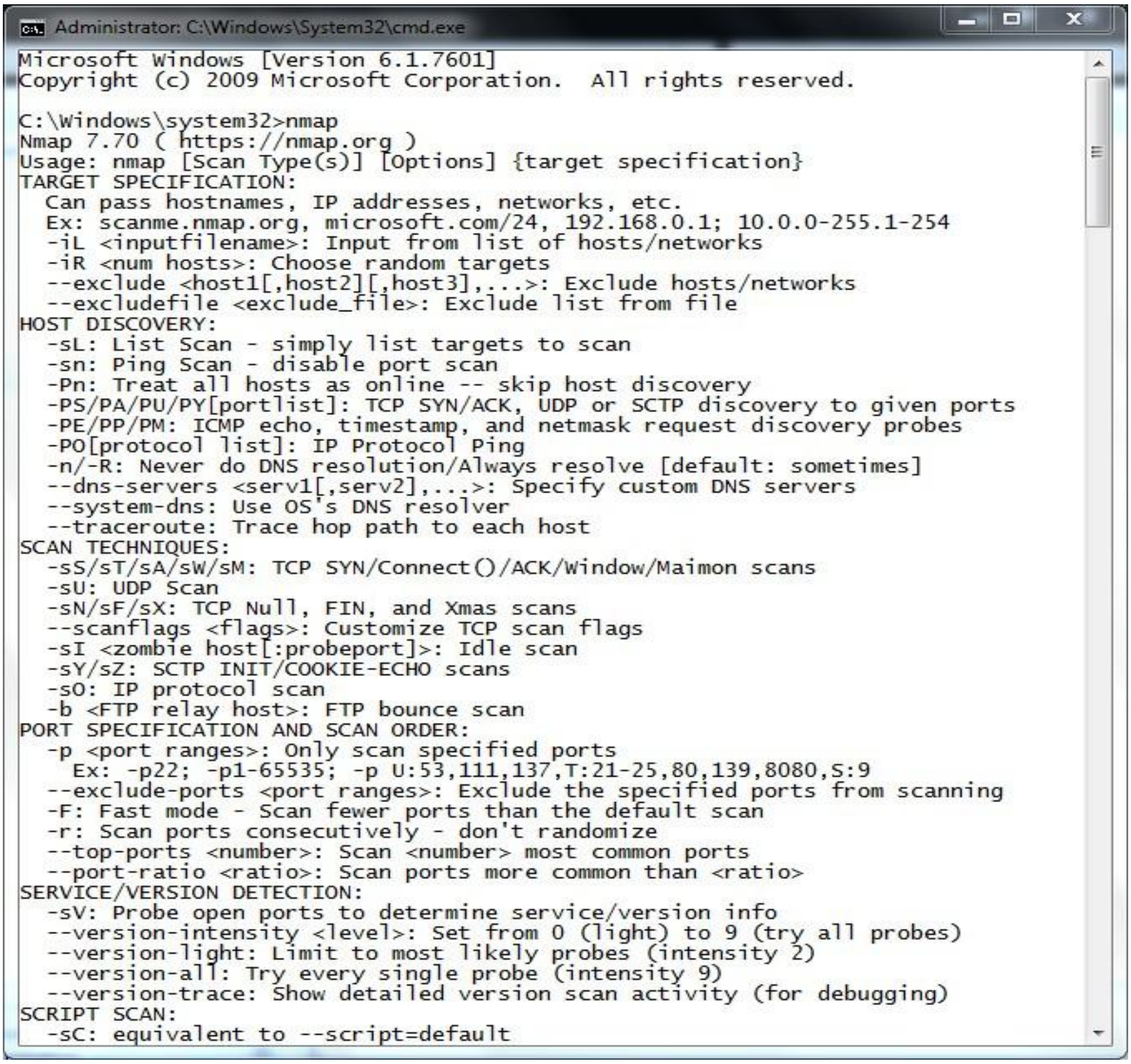
Name - Type: scanme.org - user



Target: scanme.org
Profile: Intense scan
Command: nmap -T4 -A -v scanme.org

Status	Command
Unsaved	nmap -T4 -A -v www.google.com
Unsaved	nmap -T4 -A -v www.google.com
Unsaved	nmap -T4 -A -v scanme.org

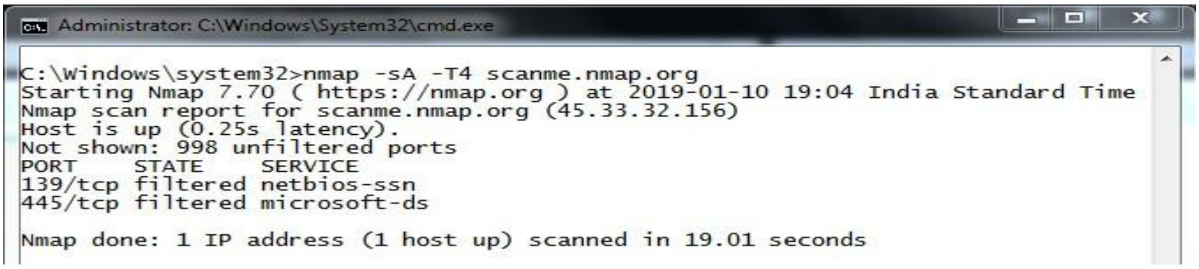
CMD:-



```
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
```

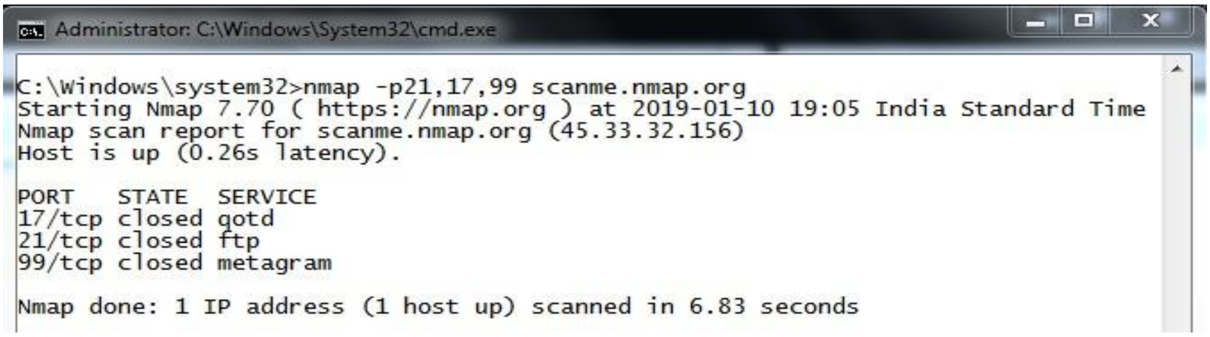
1. nmap –sA –T4 www.google.com OR nmap –sA – T4 scanme.nmap.org



```
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

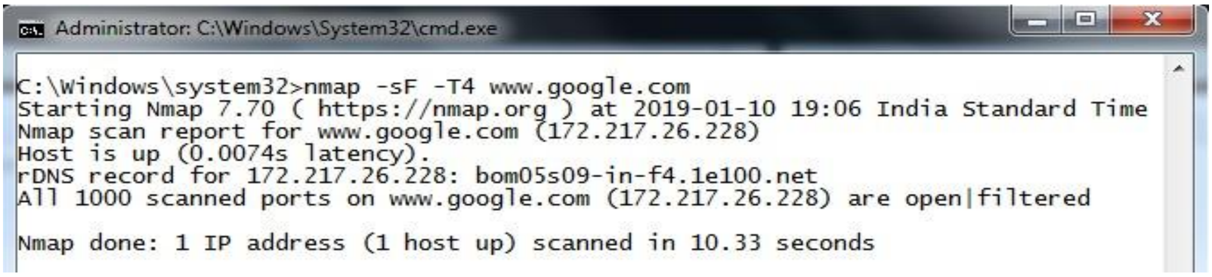


```
C:\Windows\system32>nmap -p21,17,99 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:05 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

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
```

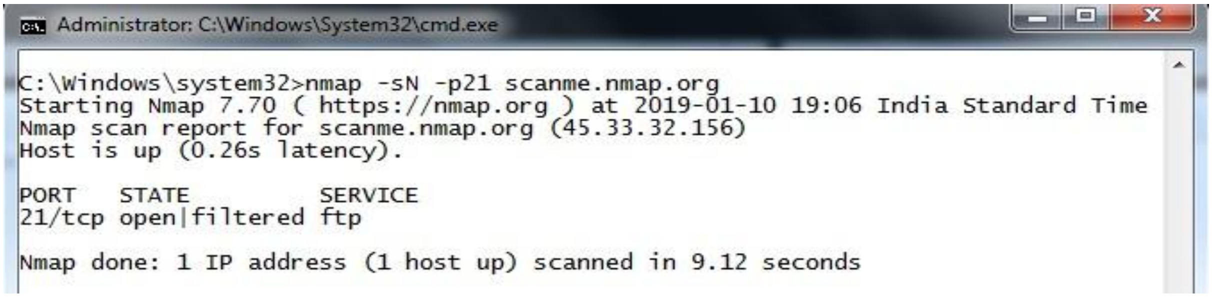
3. nmap –sF –T4 www.google.com



```
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

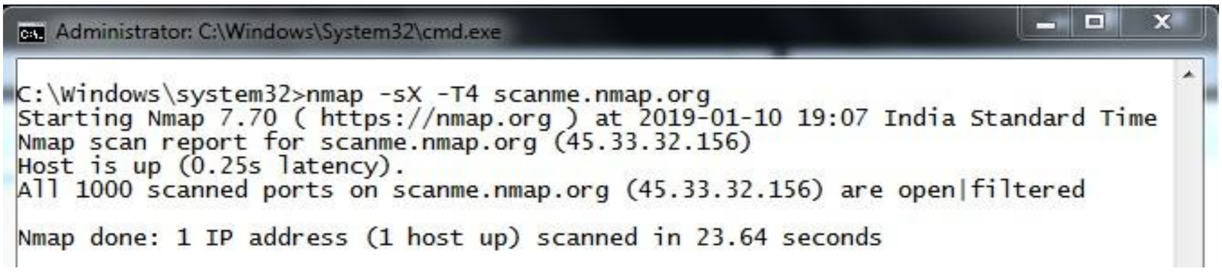


```
C:\Windows\system32>nmap -sN -p21 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

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



```
C:\Windows\system32>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:07 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 open|filtered

Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds
```