

PRACTICAL NO – 04

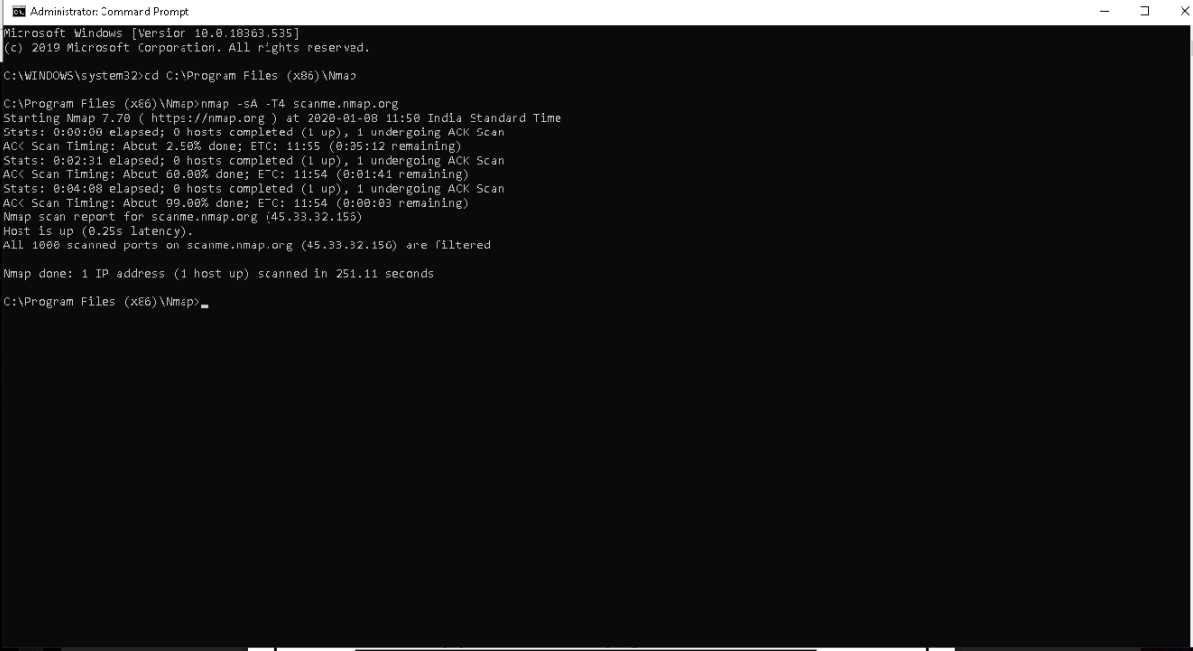
AIM : Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.

NOTE : Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

(A) TYPE THE COMMANDS IN COMMAND PROMPT :

(i) ACK -sA (TCP ACK scan)

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files (x86)\Nmap>

C:\Program Files (x86)\Nmap>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-09 11:50 India Standard Time
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 2.50% done; ETC: 11:55 (0:35:12 remaining)
Stats: 0:02:31 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 60.00% done; ETC: 11:54 (0:01:41 remaining)
Stats: 0:04:08 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 99.00% done; ETC: 11:54 (0:00:03 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.155)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.155) are filtered

Nmap done: 1 IP address (1 host up) scanned in 251.11 seconds

C:\Program Files (x86)\Nmap>
```

(ii) SYN (Stealth) Scan (-sS)

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

```
Administrator: Command Prompt

C:\Program Files (x86)\Nmap\nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-08 11:55 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.153)
Host is up (0.25s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
113/tcp    closed ident
139/tcp    closed netbios-ssr

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
C:\Program Files (x86)\Nmap>
```

(iii) FIN Scan (-sF)

Command : **nmap -sF -T4 192.168.0.5**

```
Administrator: Command Prompt

C:\Program Files (x86)\Nmap\nmap -sF -T4 192.168.0.5
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-08 11:56 India Standard Time
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing FIN Scan
FIN Scan Timing: About 0.50% done
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing FIN Scan
FIN Scan Timing: About 1.50% done; ETC: 12:00 (0:04:23 remaining)
Stats: 0:02:40 elapsed; 0 hosts completed (1 up), 1 undergoing FIN Scan
FIN Scan Timing: About 83.50% done; ETC: 11:59 (0:00:33 remaining)
Nmap scan report for 192.168.0.5
Host is up (0.20s latency).
All 1000 scanned ports on 192.168.0.5 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 201.16 seconds
C:\Program Files (x86)\Nmap>
```

(iv) NULL Scan (-sN)

Command : **nmap -sN -p 22 scanme.nmap.org**

```
Administrator: Command Prompt

Nmap done: 1 IP address (1 host up) scanned in 281.16 seconds

C:\Program Files (x86)\Nmap\nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-08 12:00 India Standard Time
Failed to resolve "0sN".
Failed to resolve "0p".
Failed to resolve "22".
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.00% done; ETC: 12:00 (0:00:01 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.155)
Host is up (0.25s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
1330/tcp  filtered h323hostcallsc
1720/tcp  filtered h323q9:1
9920/tcp  open  nping-echo
31337/tcp open  elite

Nmap done: 1 IP address (1 host up) scanned in 26.40 seconds

C:\Program Files (x86)\Nmap>
```

(v) XMAS Scan (-sX)

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

```
Administrator: Command Prompt

C:\Program Files (x86)\Nmap\nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-08 12:01 India Standard Time
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 0.50% done
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 5.50% done; ETC: 12:05 (0:04:18 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 46.55% done; ETC: 12:05 (3:02:31 remaining)
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 59.50% done; ETC: 12:05 (3:01:46 remaining)
Stats: 0:03:44 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 88.50% done; ETC: 12:05 (3:00:29 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.155)
Host is up (0.27s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.155) are open|filtered

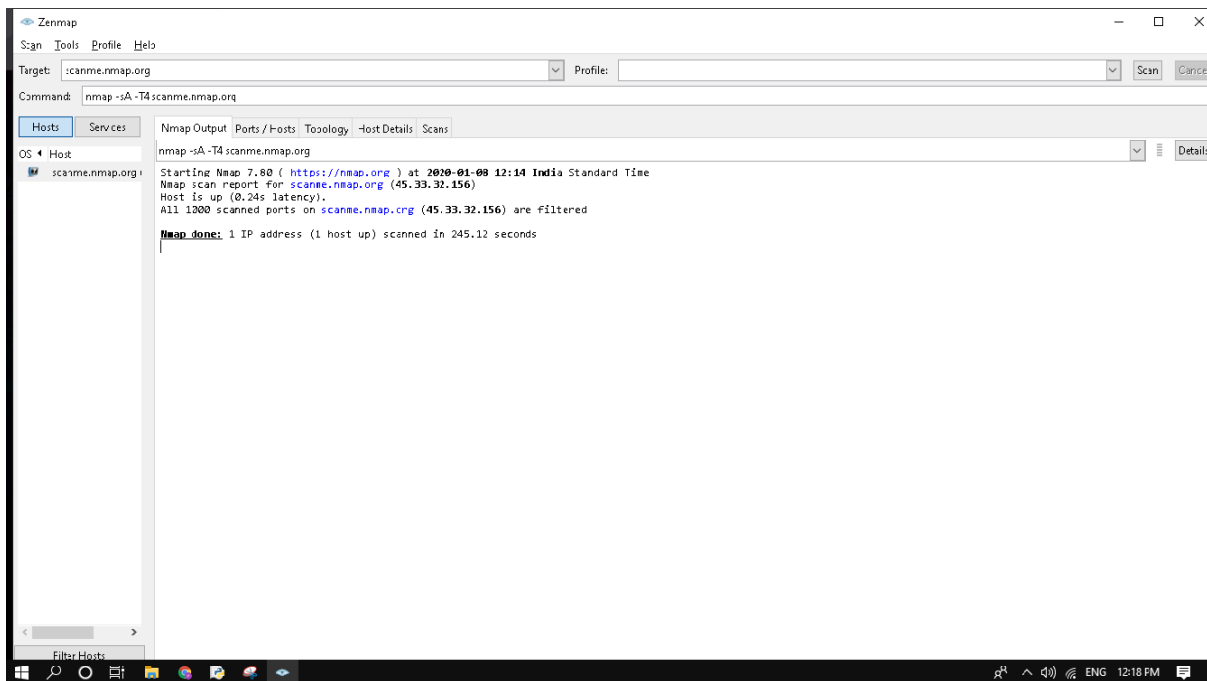
Nmap done: 1 IP address (1 host up) scanned in 253.91 seconds

C:\Program Files (x86)\Nmap>
```

(B) TYPE THE COMMANDS IN Nmap :

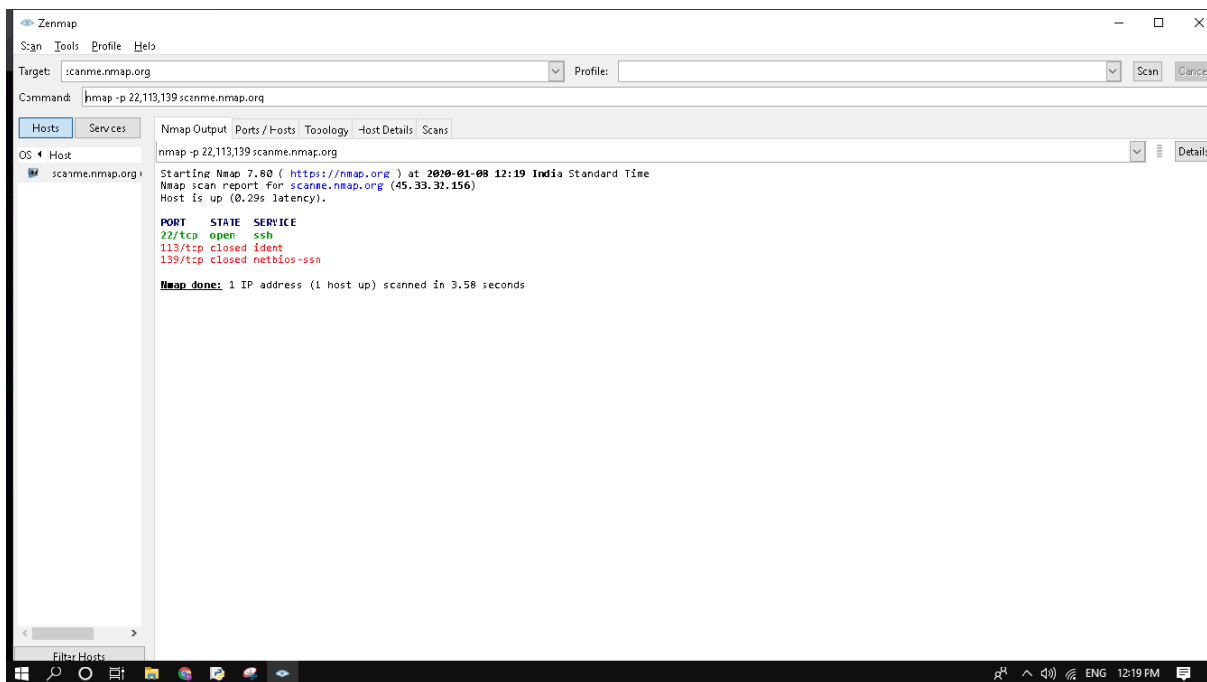
(i) ACK -sA (TCP ACK scan)

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



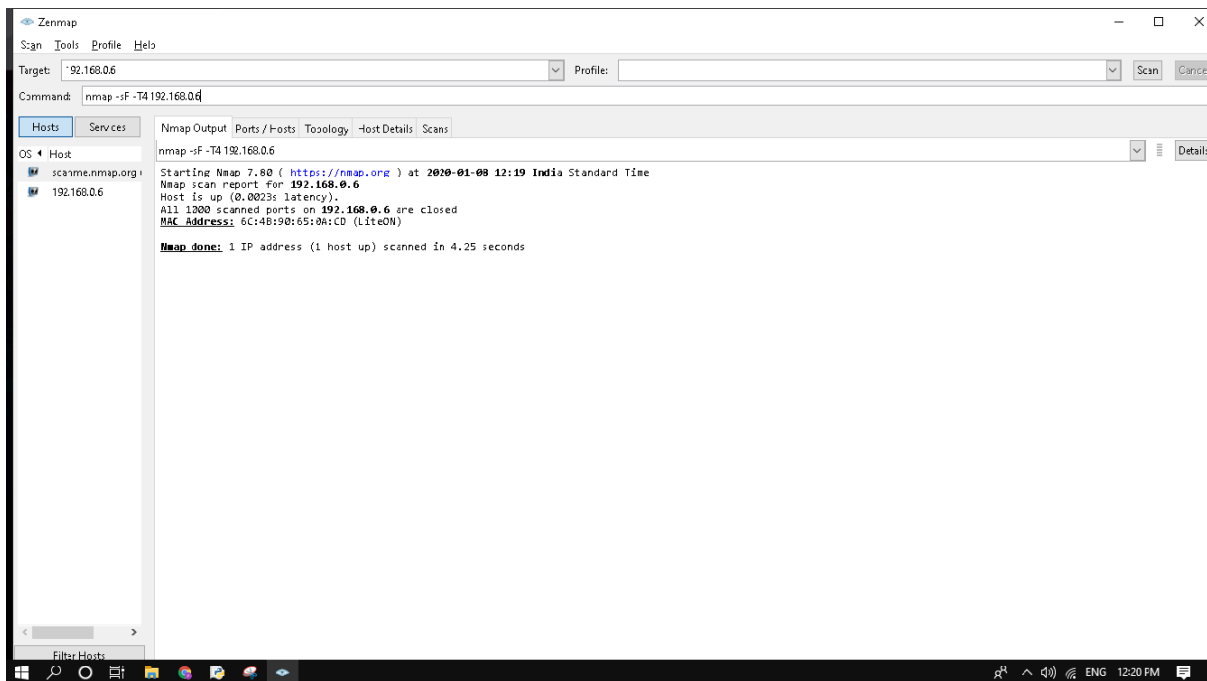
(ii) SYN (Stealth) Scan (-sS)

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



(iii) FIN Scan (-sF)

Command : `nmap -sF -T4 192.168.0.5`



(iv) NULL Scan (-sN)

Command : **nmap -sN -p 22 scanme.nmap.org**



(v) XMAS Scan (-sX)

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

