Practical - 1

Aim: TCP Scanning using nmap

nmap -V : Used to know version of nmap

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\VB>nmap -V

Nmap version 7.50 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.3.3 openssl-1.0.2l nmap-libpcre-7.6 Npcap-0.91 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select

C:\Users\VB>
```

nmap IP_addr : To scan the IP

```
C:\Users\VB>nmap 100.100.112.231

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 10:14 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.010s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
3389/tcp open  ms-wbt-server
MAC Address: B0:83:FE:A5:83:92 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds

C:\Users\VB>_
```

To scan range of IP address

```
C:\Users\VB>nmap 100.100.112.220-235

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 10:18 India Standard Time
Stats: 0:00:22 elapsed; 7 hosts completed (8 up), 15 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:27 elapsed; 7 hosts completed (8 up), 8 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.13% done; ETC: 10:19 (0:00:02 remaining)
Stats: 0:00:27 elapsed; 7 hosts completed (8 up), 8 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 50.84% done; ETC: 10:19 (0:00:02 remaining)
Stats: 0:00:28 elapsed; 7 hosts completed (8 up), 8 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.70% done; ETC: 10:19 (0:00:02 remaining)
Stats: 0:00:28 elapsed; 7 hosts completed (8 up), 8 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.01% done; ETC: 10:19 (0:00:02 remaining)
Stats: 0:00:28 elapsed; 7 hosts completed (8 up), 8 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.32% done; ETC: 10:19 (0:00:02 remaining)
Stats: 0:00:28 elapsed; 7 hosts completed (8 up), 8 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.51% done; ETC: 10:19 (0:00:02 remaining)
```

To scan the subnet of IP

```
Nmap scan report for 100.100.112.222
Host is up (0.0034s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
3389/tcp open  ms-wbt-server
MAC Address: B0:83:FE:A5:8A:0F (Dell)

Nmap scan report for 100.100.112.223
Host is up (0.00s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1029/tcp open  ms-lsa
MAC Address: B0:83:FE:A5:89:4D (Dell)
```

To scan OS of IP

```
C:\Users\VB>nmap -O 100.100.112.231

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 10:27 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.000061s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
3389/tcp open  ms-wbt-server
MAC Address: B0:83:FE:A5:83:92 (Dell)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft
:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.90 seconds
```

Practical - 2

Aim: Port Scanning using nmap

To scan port IP

Nmap –p port_num ip

```
C:\Users\VB>nmap -p 135 100.100.112.231

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 10:33 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.014s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: B0:83:FE:A5:83:92 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

To scan range of port IP

Nmap –p port_range ip

```
C:\Users\VB>nmap -p 100-200 100.100.112.231

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 10:35 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.00010s latency).
Not shown: 99 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
MAC Address: B0:83:FE:A5:83:92 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

To scan all the ports of IP

Nmap –p- ip

```
C:\Users\VB>nmap -p- 100.100.112.231

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 10:37 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.000077s latency).
Not shown: 65523 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
```

To scan most common ports of IP

Nmap -f ip

```
C:\Users\VB>nmap -f 100.100.112.231
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD.  This may or may not work.

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 10:41 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.00068s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
3389/tcp open  ms-wbt-server
MAC Address: B0:83:FE:A5:83:92 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds
```

To scan ports in form of IPv6 IP

nmap -6

```
C:\Users\VB>nmap -6 fe80::85fd:cad5:fa36:61dd

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 11:13 India Standard Time
Nmap scan report for fe80::85fd:cad5:fa36:61dd
Host is up (0.00017s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
3389/tcp open  ms-wbt-server
MAC Address: B0:83:FE:A5:83:92 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 17.08 seconds
```

Show ports with version

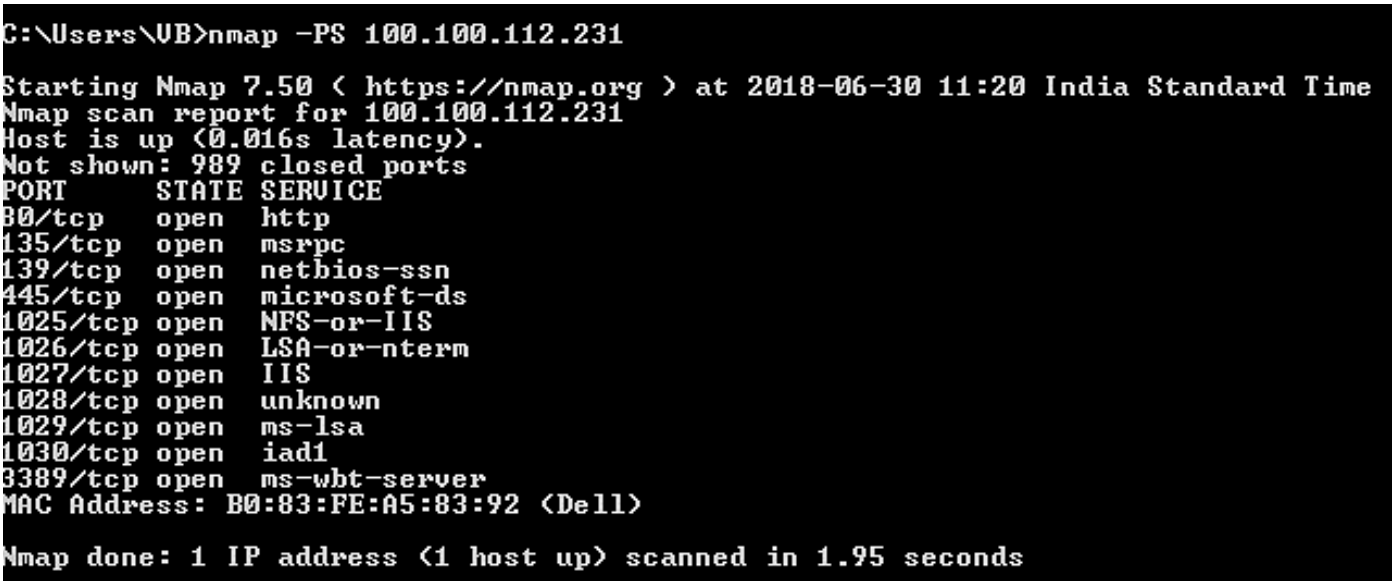
nmap –sV

```
C:\Users\VB>nmap -sV 100.100.112.231

Starting Nmap 7.50 ( https://nmap.org ) at 2018-06-30 11:16 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.011s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.9 (PHP/5.5.12)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1025/tcp open  msrpc         Microsoft Windows RPC
1026/tcp open  msrpc         Microsoft Windows RPC
1027/tcp open  msrpc         Microsoft Windows RPC
1028/tcp open  msrpc         Microsoft Windows RPC
1029/tcp open  msrpc         Microsoft Windows RPC
1030/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Service
MAC Address: B0:83:FE:A5:83:92 (Dell)
Service Info: Hosts: localhost, ITME2T13; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Show ports without version

nmap –PS


C:\Users\VB>nmap -PS 100.100.112.231
Starting Nmap 7.50 (https://nmap.org) at 2018-06-30 11:20 India Standard Time
Nmap scan report for 100.100.112.231
Host is up (0.016s latency).
Not shown: 989 closed ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1027/tcp open IIS
1028/tcp open unknown
1029/tcp open ms-lsa
1030/tcp open iad1
3389/tcp open ms-wbt-server
MAC Address: B0:83:FE:A5:83:92 (Dell)
Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds