

Section – A

1) -sS: perform TCP-SYN scan

```
shankar@shankar-ThinkPad-L450:~$ sudo nmap -sS 192.168.1.5
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:41 IST
Nmap scan report for shankar-ThinkPad-L450 (192.168.1.5)
Host is up (0.0000070s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
3128/tcp  open  squid-http

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

2) -sV -p ssl-heartbleed: Probe open ports to determine service/version info,
check port for heartbleed vulnerability

```
shankar@shankar-ThinkPad-L450:~$ nmap -sV -p 443 --script=ssl-heartbleed $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:44 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).

PORT      STATE  SERVICE VERSION
443/tcp    filtered https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

3) -sV: Probe open ports to determine service/version info

```
shankar@shankar-ThinkPad-L450:~$ nmap -sV $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:46 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.19 seconds
```

4) -v: Increase verbosity level

```
shankar@shankar-ThinkPad-L450:~$ nmap -v $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:48 IST
Initiating Ping Scan at 18:48
Scanning 18.192.172.30 [2 ports]
Completed Ping Scan at 18:48, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:48
Completed Parallel DNS resolution of 1 host. at 18:48, 0.00s elapsed
Initiating Connect Scan at 18:48
Scanning ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30) [1000 ports]
Discovered open port 80/tcp on 18.192.172.30
Completed Connect Scan at 18:48, 11.35s elapsed (1000 total ports)
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.15s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.66 seconds
```

5) website: scans a particular website

```
shankar@shankar-ThinkPad-L450:~$ nmap www.vit.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:49 IST
Nmap scan report for www.vit.ac.in (136.233.9.13)
Host is up (0.071s latency).
rDNS record for 136.233.9.13: 136.233.9.13.static.jio.com
Not shown: 989 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open  https
445/tcp   filtered microsoft-ds
515/tcp   filtered printer
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1026/tcp  filtered LSA-or-nterm
9898/tcp  filtered monkeycom

Nmap done: 1 IP address (1 host up) scanned in 3.66 seconds
```

6) -sT: TCP connect scan

```
shankar@shankar-ThinkPad-L450:~$ nmap -sT $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:50 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.15s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
```

7) --script http-tittle: obtains the title of the root path of web sites

```
shankar@shankar-ThinkPad-L450:~$ nmap --script http-tittle $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:52 IST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 18:52 (0:00:00 remaining)
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.15s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
|_http-tittle: Home of Acunetix Art

Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
```

8) --script http-headers:

```
shankar@shankar-ThinkPad-L450:~$ nmap --script http-headers $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:52 IST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 18:52 (0:00:00 remaining)
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
| http-headers:
|   Server: nginx/1.19.0
|   Date: Sun, 27 Dec 2020 13:22:50 GMT
|   Content-Type: text/html; charset=UTF-8
|   Connection: close
|   X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
|
|_ (Request type: HEAD)

Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds
```

9) --script http-enum: effectively brute forces a web server path in order to discover web applications in use

```
shankar@shankar-ThinkPad-L450:~$ nmap --script http-enum $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:56 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /admin/: Possible admin folder
|   /login.php: Possible admin folder
|   /clientaccesspolicy.xml: Microsoft Silverlight crossdomain policy
|   /crossdomain.xml: Adobe Flash crossdomain policy
|   /CVS/: Potentially interesting folder w/ directory listing
|   /images/: Potentially interesting folder w/ directory listing
|   /pictures/: Potentially interesting folder w/ directory listing
|_  /secured/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 317.78 seconds
```

10) -p: check ports

```
shankar@shankar-ThinkPad-L450:~$ nmap -p 80,443 $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:54 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).

PORT      STATE      SERVICE
80/tcp    open       http
443/tcp    filtered   https

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
```

11) -pT: check ports for a time duration

```
shankar@shankar-ThinkPad-L450:~$ nmap -p T:8888,443 $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:55 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).

PORT      STATE      SERVICE
443/tcp    filtered   https
8888/tcp    filtered   sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 2.68 seconds
```

12) --iflist: Print host interfaces and routes

```
shankar@shankar-ThinkPad-L450:~$ nmap --iflist
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:55 IST
*****INTERFACES*****
DEV      (SHORT)  IP/MASK      TYPE      UP      MTU      MAC
lo        (lo)       127.0.0.1/8   loopback  up      65536    00:00:00:00:00:00
lo        (lo)       ::1/128       loopback  up      65536    00:00:00:00:00:00
enp0s25   (enp0s25)  (none)/0     ethernet  down    1500     68:F7:28:A8:02:C3
wlp4s0    (wlp4s0)   192.168.1.5/24 ethernet  up      1500     60:57:18:D7:D5:E8
wlp4s0    (wlp4s0)   fd1c:6758:7368:9a00:633b:85a2:165d:644e/64 ethernet  up      1500     60:57:18:D7:D5:E8
wlp4s0    (wlp4s0)   fe80::626c:1a2b:1090:fb9c/64 ethernet  up      1500     60:57:18:D7:D5:E8
wlp4s0    (wlp4s0)   fd1c:6758:7368:9a00:66d5:7c1d:dabd:5b3b/64 ethernet  up      1500     60:57:18:D7:D5:E8
anbox0    (anbox0)   192.168.250.1/24 ethernet  up      1500     6A:2D:6C:28:FD:88
anbox0    (anbox0)   fe80::682d:6cff:fe28:fd88/64 ethernet  up      1500     6A:2D:6C:28:FD:88

*****ROUTES*****
DST/MASK      DEV      METRIC  GATEWAY
192.168.250.0/24  anbox0  0
192.168.1.0/24   wlp4s0  600
169.254.0.0/16   wlp4s0  1000
0.0.0.0/0        wlp4s0  600     192.168.1.1
::1/128          lo       0
fd1c:6758:7368:9a00:633b:85a2:165d:644e/128 wlp4s0  0
fd1c:6758:7368:9a00:66d5:7c1d:dabd:5b3b/128 wlp4s0  0
fe80::626c:1a2b:1090:fb9c/128 wlp4s0  0
fe80::682d:6cff:fe28:fd88/128 anbox0  0
::1/128          lo       256
fe80::/64        anbox0  256
fd1c:6758:7368:9a00::/64 wlp4s0  600
fe80::/64        wlp4s0  600
ff00::/8         anbox0  256
ff00::/8         wlp4s0  256
```

13) -f: flag checks

```
shankar@shankar-ThinkPad-L450:~$ sudo nmap -f $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:57 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.06 seconds
```

14) -A: enables version detection among other things

```
shankar@shankar-ThinkPad-L450:~$ sudo nmap -A $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:57 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx/1.19.0
|_http-server-header: nginx/1.19.0
|_http-title: Home of Acunetix Art
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Crestron XPanel control system (90%), Linux 3.13 or 4.2 (88%), XBMCbuntu Frodo v12.2 (Linux 3.X) (88%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 28 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1 15.75 ms _gateway (192.168.1.1)
2 22.89 ms abts-kk-dynamic-001.4.179.122.airtelbroadband.in (122.179.4.1)
3 22.73 ms 125.18.238.241
4 137.66 ms 116.119.55.246
5 135.43 ms 99.83.67.148
6 131.57 ms 150.222.96.1
7 145.35 ms 52.93.21.113
8 121.64 ms 99.83.67.148
9 158.92 ms 54.239.43.251
10 ... 27
28 139.87 ms ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submt/ .
Nmap done: 1 IP address (1 host up) scanned in 41.57 seconds
```

15) -p [range]: checks a range of port nums

```
shankar@shankar-ThinkPad-L450:~$ nmap -p 1-65535 localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:57 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000092s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp    open  ipp
1716/tcp   open  xmsg
3128/tcp   open  squid-http
6463/tcp   open  unknown
8388/tcp   open  unknown
9050/tcp   open  tor-socks
40399/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

16) --top-ports: most accessed ports

```
shankar@shankar-ThinkPad-L450:~$ nmap --top-ports 20 $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 18:59 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
53/tcp    filtered  domain
80/tcp    open      http
110/tcp   filtered  pop3
111/tcp   filtered  rpcbind
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
143/tcp   filtered  imap
443/tcp   filtered  https
445/tcp   filtered  microsoft-ds
993/tcp   filtered  imaps
995/tcp   filtered  pop3s
1723/tcp  filtered  pptp
3306/tcp  filtered  mysql
3389/tcp  filtered  ms-wbt-server
5900/tcp  filtered  vnc
8080/tcp  filtered  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds
```

17) -T4 -A: speed check and enables version detection

```
shankar@shankar-ThinkPad-L450:~$ nmap -T4 -A cloudflare.com
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 19:00 IST
Nmap scan report for cloudflare.com (104.16.133.229)
Host is up (0.016s latency).
Other addresses for cloudflare.com (not scanned): 104.16.132.229 2606:4700::6810:84e5 2606:4700::6810:85e5
Not shown: 996 filtered ports
PORT      STATE      SERVICE      VERSION
80/tcp    open      http         Cloudflare http proxy
|_ http-server-header: cloudflare
|_ http-title: Did not follow redirect to https://www.cloudflare.com/
443/tcp   open      ssl/http     Cloudflare http proxy
|_ http-server-header: cloudflare
|_ http-title: Did not follow redirect to https://www.cloudflare.com/
|_ ssl-cert: Subject: commonName=cloudflare.com/organizationName=Cloudflare, Inc./stateOrProvinceName=CA/countryName=US
|_ Subject Alternative Name: DNS:*.cloudflare.com, DNS:cloudflare.com, DNS:*.dns.cloudflare.com, DNS:*.amp.cloudflare.com, DNS:*.staging.cloudflare.com
|_ Not valid before: 2020-07-04T00:00:00
|_ Not valid after: 2021-07-04T12:00:00
|_ ssl-date: 2020-12-27T13:30:37+00:00; 0s from scanner time.
|_ tls-alpn:
|_   h2
|_   http/1.1
|_ tls-nextprotoneg:
|_   h2
|_   http/1.1
8080/tcp  open      http         Cloudflare http proxy
|_ http-server-header: cloudflare
|_ http-title: Did not follow redirect to https://www.cloudflare.com/
8443/tcp  open      ssl/http     Cloudflare http proxy
|_ http-server-header: cloudflare
|_ http-title: Did not follow redirect to https://www.cloudflare.com/
|_ ssl-cert: Subject: commonName=cloudflare.com/organizationName=Cloudflare, Inc./stateOrProvinceName=CA/countryName=US
|_ Subject Alternative Name: DNS:*.cloudflare.com, DNS:cloudflare.com, DNS:*.dns.cloudflare.com, DNS:*.amp.cloudflare.com, DNS:*.staging.cloudflare.com
|_ Not valid before: 2020-07-04T00:00:00
|_ Not valid after: 2021-07-04T12:00:00
|_ ssl-date: 2020-12-27T13:30:37+00:00; 0s from scanner time.
|_ tls-alpn:
|_   h2
|_   http/1.1
|_ tls-nextprotoneg:
|_   h2
|_   http/1.1
```


18) -Pn --script vuln: Treat all hosts as online

```
shankar@shankar-ThinkPad-L450:~$ nmap -Pn --script vuln $ipaddr
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 19:00 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).
Not shown: 999 filtered ports
```

19) -sV --script: check for version and for vulnerability

```
shankar@shankar-ThinkPad-L450:~$ nmap -sV --script http-malware-host $ipaddr
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 19:04 IST
Nmap scan report for ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.172.30)
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.19.0
|_http-malware-host: Host appears to be clean
|_http-server-header: nginx/1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.86 seconds
```

1) Use of > as a stream modifier between the command and the destination file.

Usage: command > output.txt

2) To scan ipv6 use the parameter (-6).

Usage: nmap -6 --rest of command

Section-B