Name: Kulvir Singh
Register Number: 19BCE2074

Information Security and Audit Analysis
Lab DA 3

NMAPS

1. Scan a single host or an IP address (IPv4) using nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 01:49 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0092s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 17.78 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

2. Scan multiple IP address or subnet (IPv4)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap 192.168.1.*
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 01:54 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0065s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap scan report for 192.168.1.255
Host is up (0.0062s latency).
Not shown: 999 closed ports
PORT     STATE    SERVICE
514/tcp  filtered shell

Nmap done: 256 IP addresses (2 hosts up) scanned in 25.57 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

3. Read list of hosts/networks from a file (IPv4)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ cat>/tmp/test.txt
192.168.1.0/24
192.168.1.1/24
10.1.2.3
localhost
^C
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -iL /tmp/test.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:05 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.255
Host is up (0.0089s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.255
Host is up (0.0072s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap scan report for localhost (127.0.0.1)
Host is up (0.00040s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp

Nmap done: 514 IP addresses (5 hosts up) scanned in 49.24 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

4. Excluding hosts/networks (IPv4) from nmap scan examples

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap 192.168.1.0/24 --exclude 192.168.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:09 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0071s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 255 IP addresses (1 host up) scanned in 65.78 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

5. Turn on OS and version detection scanning script (IPv4) with nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -v -A 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:11 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating Ping Scan at 02:11
Scanning 192.168.1.1 [2 ports]
Completed Ping Scan at 02:11, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:11
Completed Parallel DNS resolution of 1 host. at 02:12, 13.00s elapsed
Initiating Connect Scan at 02:12
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed Connect Scan at 02:12, 23.11s elapsed (1000 total ports)
Initiating Service scan at 02:12
Scanning 5 services on 192.168.1.1
Completed Service scan at 02:12, 7.07s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.1.
Initiating NSE at 02:12
Completed NSE at 02:12, 20.15s elapsed
Initiating NSE at 02:12
Completed NSE at 02:13, 15.62s elapsed
Initiating NSE at 02:13
Completed NSE at 02:13, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE        VERSION
21/tcp  open  ftp            GNU Inetutils FTPd 1.9.4
| ftp-syst:
|   SYST: Version: Linux 3.18.24
|   STAT:
|  localhost.localdomain FTP server status:
|      ftpd (GNU inetutils) 1.9.4
|      Connected to  (::ffff:192.168.1.37)
|      Waiting for user name
|      TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: Stream
|      No data connection
| End of status
```

6. Find out if a host/network is protected by a firewall using namp command

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --privileged -sA -v 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:18 PDT
Initiating Ping Scan at 02:18
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 02:18, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:18
Completed Parallel DNS resolution of 1 host. at 02:18, 13.00s elapsed
Initiating ACK Scan at 02:18
Scanning 192.168.1.1 [1000 ports]
Completed ACK Scan at 02:18, 0.07s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.000048s latency).
All 1000 scanned ports on 192.168.1.1 are unfiltered

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
           Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

7. Scan a host when protected by the firewall

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PN 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:20 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0060s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 45.28 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

8. Scan an IPv6 host/address examples

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -v A -6 2607:f0d0:1002:51::4
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:22 PDT
Failed to resolve "A".
Initiating Ping Scan at 02:22
Scanning 2607:f0d0:1002:51::4 [2 ports]
Completed Ping Scan at 02:22, 0.00s elapsed (1 total hosts)
Nmap scan report for 2607:f0d0:1002:51::4 [host down]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.13 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

9. Scan a network and find out which servers and devices are up and running

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:23 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0050s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 39.89 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

10. perform a fast scan using the namp

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -F 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:25 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0064s latency).
Not shown: 95 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 29.70 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

11. Display the reason a port is in a particular state

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -reason 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:26 PDT
Nmap scan report for 192.168.1.1
Host is up, received syn-ack (0.0061s latency).
Not shown: 995 filtered ports
Reason: 995 no-responses
PORT     STATE SERVICE REASON
21/tcp   open  ftp     syn-ack
22/tcp   open  ssh     syn-ack
53/tcp   open  domain  syn-ack
80/tcp   open  http    syn-ack
443/tcp  open  https   syn-ack

Nmap done: 1 IP address (1 host up) scanned in 31.21 seconds
```

12. Only show open (or possibly open) ports using nmap command in Linux

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -open 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:28 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
Not shown: 995 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 29.77 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

13. Show all packets sent and received

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --packet-trace 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:30 PDT
CONN (0.0298s) TCP localhost > 192.168.1.1:80 => Operation now in progress
CONN (0.0299s) TCP localhost > 192.168.1.1:443 => Operation now in progress
CONN (0.0348s) TCP localhost > 192.168.1.1:80 => Connected
NSOCK INFO [0.0350s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0350s] nsock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.0350s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
NSOCK INFO [0.0350s] nsock_write(): Write request for 42 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.0350s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.0350s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [4.0350s] nsock_write(): Write request for 42 bytes to IOD #1 EID 35 [127.0.0.53:53]
NSOCK INFO [4.0350s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 35 [127.0.0.53:53]
NSOCK INFO [8.0360s] nsock_write(): Write request for 42 bytes to IOD #1 EID 43 [127.0.0.53:53]
NSOCK INFO [8.0370s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [127.0.0.53:53]
NSOCK INFO [13.0380s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [13.0380s] nevent_delete(): nevent_delete on event #18 (type READ)
CONN (13.0388s) TCP localhost > 192.168.1.1:80 => Operation now in progress
CONN (13.0389s) TCP localhost > 192.168.1.1:8888 => Operation now in progress
CONN (13.0390s) TCP localhost > 192.168.1.1:23 => Operation now in progress
CONN (13.0392s) TCP localhost > 192.168.1.1:53 => Operation now in progress
CONN (13.0394s) TCP localhost > 192.168.1.1:995 => Operation now in progress
CONN (13.0394s) TCP localhost > 192.168.1.1:113 => Operation now in progress
CONN (13.0395s) TCP localhost > 192.168.1.1:554 => Operation now in progress
CONN (13.0396s) TCP localhost > 192.168.1.1:199 => Operation now in progress
CONN (13.0396s) TCP localhost > 192.168.1.1:110 => Operation now in progress
CONN (13.0397s) TCP localhost > 192.168.1.1:443 => Operation now in progress
CONN (13.0428s) TCP localhost > 192.168.1.1:80 => Connected
CONN (13.0430s) TCP localhost > 192.168.1.1:5900 => Operation now in progress
CONN (13.0431s) TCP localhost > 192.168.1.1:1723 => Operation now in progress
CONN (13.0441s) TCP localhost > 192.168.1.1:53 => Connected
CONN (13.0443s) TCP localhost > 192.168.1.1:1720 => Operation now in progress
CONN (13.0444s) TCP localhost > 192.168.1.1:587 => Operation now in progress
CONN (14.0603s) TCP localhost > 192.168.1.1:443 => Connected
CONN (14.1397s) TCP localhost > 192.168.1.1:23 => Operation now in progress
CONN (14.1397s) TCP localhost > 192.168.1.1:8888 => Operation now in progress
CONN (14.1398s) TCP localhost > 192.168.1.1:3306 => Operation now in progress
CONN (14.1399s) TCP localhost > 192.168.1.1:445 => Operation now in progress
CONN (14.1401s) TCP localhost > 192.168.1.1:25 => Operation now in progress
CONN (14.1965s) TCP localhost > 192.168.1.1:199 => Operation now in progress
CONN (14.1966s) TCP localhost > 192.168.1.1:554 => Operation now in progress
CONN (14.1967s) TCP localhost > 192.168.1.1:113 => Operation now in progress
CONN (14.1968s) TCP localhost > 192.168.1.1:995 => Operation now in progress
CONN (14.1970s) TCP localhost > 192.168.1.1:110 => Operation now in progress
CONN (14.1999s) TCP localhost > 192.168.1.1:5900 => Operation now in progress
CONN (14.2000s) TCP localhost > 192.168.1.1:1723 => Operation now in progress
```

14. Show host interfaces and routes

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:31 PDT
************************INTERFACES************************
DEV   (SHORT) IP/MASK                      TYPE     UP MTU   MAC
lo    (lo)    127.0.0.1/8                  loopback up 65536
lo    (lo)    ::1/128                      loopback up 65536
ens33 (ens33) 192.168.159.128/24           ethernet up 1500  00:0C:29:45:75:69
ens33 (ens33) fe80::1734:e78d:b2c0:bd9f/64 ethernet up 1500  00:0C:29:45:75:69

**************************ROUTES**************************
DST/MASK                      DEV   METRIC GATEWAY
192.168.159.0/24              ens33 100
169.254.0.0/16                ens33 1000
0.0.0.0/0                     ens33 100    192.168.159.2
::1/128                       lo    0
fe80::1734:e78d:b2c0:bd9f/128 ens33 0
::1/128                       lo    256
fe80::/64                     ens33 100
ff00::/8                      ens33 256

kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

15. scan specific ports using nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -p 80 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:32 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0056s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

16. fastest way to scan all your devices/computers for open ports

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -T5 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:33 PDT
Warning: 192.168.1.255 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap scan report for 192.168.1.255
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.255 are closed (905) or filtered (95)

Nmap done: 256 IP addresses (2 hosts up) scanned in 50.64 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

17. detect remote operating system with the help of nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -O -v 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:43 PDT
Initiating Ping Scan at 02:43
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 02:43, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:43
Completed Parallel DNS resolution of 1 host. at 02:44, 13.00s elapsed
Initiating SYN Stealth Scan at 02:44
Scanning 192.168.1.1 [1000 ports]
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Completed SYN Stealth Scan at 02:44, 21.69s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.1
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.23 seconds
           Raw packets sent: 4068 (181.070KB) | Rcvd: 1549 (62.362KB)
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

18. detect remote services (server / daemon) version numbers

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -sV 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:45 PDT
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        GNU Inetutils FTPd 1.9.4
22/tcp   open  ssh        Dropbear sshd 0.48 (protocol 2.0)
53/tcp   open  domain     dnsmasq 2.80
80/tcp   open  tcpwrapped
443/tcp  open  ssl/http   Boa HTTPd 0.93.15
Service Info: Host: localhost.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.90 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

19. Scan a host using TCP ACK (PA) and TCP Syn (PS) ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PS 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:46 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 24.01 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PA 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:47 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0048s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 17.57 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

20. Scan a host using IP protocol ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -PO 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:47 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 25.64 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

21. Scan a host using UDP ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -PU 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:50 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.11 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

22. Find out the most commonly used TCP ports using TCP SYN Scan

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sT 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:53 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

23. Scan a host for UDP services (UDP scan)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sU 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:54 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.1.1 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 17.20 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

24. Scan for IP protocol

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sO 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:56 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0015s latency).
Not shown: 252 filtered protocols
PROTOCOL STATE         SERVICE
1        open          icmp
6        open          tcp
17       open|filtered udp
47       open|filtered gre

Nmap done: 1 IP address (1 host up) scanned in 14.35 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

25. Scan a firewall for security weakness

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sN 192.168.1.254
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:58 PDT
Nmap scan report for 192.168.1.254
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.1.254 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 17.22 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

26. Scan a firewall for packets fragments

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -f 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0034s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.71 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

27. Cloak a scan with decoys

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:04 PDT
Nmap scan report for 192.168.1.5
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.1.5 are filtered

Nmap done: 1 IP address (1 host up) scanned in 138.65 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

28. Scan a firewall for MAC address spoofing

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -v -sT -PN --spoof-mac 0 192.168.1.1
Warning: The -PN option is deprecated. Please use -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:13 PDT
Spoofing MAC address 80:1C:08:53:B6:5E (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Initiating Parallel DNS resolution of 1 host. at 03:13
Completed Parallel DNS resolution of 1 host. at 03:13, 13.00s elapsed
Initiating Connect Scan at 03:13
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed Connect Scan at 03:13, 14.41s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.0058s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.46 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

29. Save output to a text file

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap 192.168.1.1 > output.txt
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

Open

output.txt
~/Desktop/ISAA/nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:15 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 18.07 seconds
```

30. Speed up nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -v -sS -A -T4 192.168.2.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:21 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating NSE at 03:21
Completed NSE at 03:21, 0.00s elapsed
Initiating Ping Scan at 03:21
Scanning 192.168.2.5 [4 ports]
Completed Ping Scan at 03:21, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:21
Completed Parallel DNS resolution of 1 host. at 03:21, 0.17s elapsed
Initiating SYN Stealth Scan at 03:21
Scanning 192.168.2.5 [1000 ports]
Increasing send delay for 192.168.2.5 from 0 to 5 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 192.168.2.5 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed SYN Stealth Scan at 03:22, 51.42s elapsed (1000 total ports)
Initiating Service scan at 03:22
Initiating OS detection (try #1) against 192.168.2.5
Initiating Traceroute at 03:22
Completed Traceroute at 03:22, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 03:22
Completed Parallel DNS resolution of 2 hosts. at 03:22, 5.26s elapsed
NSE: Script scanning 192.168.2.5.
Initiating NSE at 03:22
Completed NSE at 03:22, 0.04s elapsed
Initiating NSE at 03:22
Completed NSE at 03:22, 0.00s elapsed
Initiating NSE at 03:22
Completed NSE at 03:22, 0.00s elapsed
Nmap scan report for 192.168.2.5
Host is up (0.0038s latency).
All 1000 scanned ports on 192.168.2.5 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual
 NAT device
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.25 ms _gateway (192.168.159.2)
2   0.29 ms 192.168.2.5
```