Name: **Mareena Fernandes**
Roll No.: **8669**
Class: **TE IT**
Batch: **B**

EXPERIMENT NO: 7

1)

```
mareenalinux@mareenalinux:~Desktop$ sudo apt-get install nmap
[sudo] password for roblinux:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libblas3 liblinear4 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 lua-lpeg nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,553 kB of archives.
After this operation, 26.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0-1build1 [142
kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64 2.3.0+dfsg-
3build1 [41.7 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap-common all 7.80+dfsg1-
2build1 [3,676 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 nmap amd64 7.80+dfsg1-
2build1 [1,662 kB]
Fetched 5,553 kB in 2s (2,462 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 186157 files and directories currently installed.)
Preparing to unpack .../libblas3_3.9.0-1build1_amd64.deb ...
Unpacking libblas3:amd64 (3.9.0-1build1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../liblinear4_2.3.0+dfsg-3build1_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.80+dfsg1-2build1_all.deb ...
Unpacking nmap-common (7.80+dfsg1-2build1) ...
```

```
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.80+dfsg1-2build1_amd64.deb ...
Unpacking nmap (7.80+dfsg1-2build1) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up libblas3:amd64 (3.9.0-1build1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up nmap-common (7.80+dfsg1-2build1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-3build1) ...
Setting up nmap (7.80+dfsg1-2build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
```

2)

```
mareenalinux@mareenalinux:~Desktop$ nmap 192.168.1.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:02 IST
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 3.07 seconds
```

3)

```
mareenalinux@mareenalinux:~Desktop$ nmap google.co.in
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:04 IST
Nmap scan report for google.co.in (172.217.174.227)
Host is up (0.022s latency).
Other addresses for google.co.in (not scanned): 2404:6800:4009:80d::2003
rDNS record for 172.217.174.227: bom12s03-in-f3.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds
```

4)

```
mareenalinux@mareenalinux:~Desktop$ host google.co.in
google.co.in has address 172.217.174.227
google.co.in has IPv6 address 2404:6800:4009:80d::2003
google.co.in mail is handled by 50 alt4.aspmx.l.google.com.
google.co.in mail is handled by 20 alt1.aspmx.l.google.com.
google.co.in mail is handled by 40 alt3.aspmx.l.google.com.
google.co.in mail is handled by 30 alt2.aspmx.l.google.com.
google.co.in mail is handled by 10 aspmx.l.google.com.
```

5)

```
mareenalinux@mareenalinux:~Desktop$ nmap 172.217.174.227
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:07 IST
Nmap scan report for bom12s03-in-f3.1e100.net (172.217.174.227)
Host is up (0.023s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds
```

6)

```
mareenalinux@mareenalinux:~Desktop$ nmap facebook.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:09 IST
Nmap scan report for facebook.com (157.240.16.35)
Host is up (0.025s latency).
Other addresses for facebook.com (not scanned): 2a03:2880:f12f:83:face:b00c:0:25de
rDNS record for 157.240.16.35: edge-star-mini-shv-01-bom1.facebook.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
```

7)

```
mareenalinux@mareenalinux:~Desktop$ nmap 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:10 IST
Nmap scan report for 192.168.0.1
Host is up (0.020s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.02 seconds
```

8)

```
mareenalinux@mareenalinux:~Desktop$  nmap 192.168.0.101 192.168.0.102 192.168.0.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:11 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.11 seconds
```

9)

```
mareenalinux@mareenalinux:~Desktop$ nmap 192.168.0.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:12 IST
Nmap scan report for 192.168.0.1
Host is up (0.026s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Nmap done: 256 IP addresses (1 host up) scanned in 8.19 seconds
```

10)

```
mareenalinux@mareenalinux:~Desktop$  nmap 192.168.0.101,102,103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:13 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.07 seconds
```

11)

```
mareenalinux@mareenalinux:~Desktop$ nmap -A 192.168.0.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:14 IST
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 3.44 seconds
```

12)

```
mareenalinux@mareenalinux:~Desktop$ nmap -A 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:14 IST
```

13)

```
mareenalinux@mareenalinux:~Desktop$ nmap -A 172.217.174.227
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:15 IST
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 12:17 (0:01:00 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.25% done; ETC: 12:16 (0:00:00 remaining)
Nmap scan report for bom12s03-in-f3.1e100.net (172.217.174.227)
Host is up (0.023s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      gws
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Mon, 09 Nov 2020 06:45:57 GMT
|     Expires: -1
|     Cache-Control: private, max-age=0
|     Content-Type: text/html; charset=ISO-8859-1
|     P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
|     Server: gws
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     Set-Cookie: 1P_JAR=2020-11-09-06; expires=Wed, 09-Dec-2020 06:45:57 GMT; path=/;
domain=.google.com; Secure
|     Set-Cookie: NID=204=0-J-
9Rqu75P23DPye6pSUaDhww3E24f0IPpaAYsJFh5xDZWPPt9Y660p_Q8fn5BZo9oJFMIQNbX0Gpm5gv
kiCtOqFN2Z-BUNQGtt4VddtomtmuIdoaOK-S0LxgXV9gp0kL7hJJh4Pgz2w4d2GX30M_F-
QOhRT2gTPdmlTUC9TlA; expires=Tue, 11-May-2021 06:45:57 GMT; path=/; domain=.google.com;
HttpOnly
|     Accept-Ranges: none
|     Vary: Accept-Encoding
|     <!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-
IN"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta
content="/images/branding/googleg
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
```

```
|     Allow: GET, HEAD
|     Date: Mon, 09 Nov 2020 06:45:57 GMT
|     Content-Type: text/html; charset=UTF-8
|     Server: gws
|     Content-Length: 1592
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     <!DOCTYPE html>
|     <html lang=en>
|     <meta charset=utf-8>
|     <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
|     <title>Error 405 (Method Not Allowed)!!1</title>
|     <style>
|_    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-
serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-
width:390px;min-height:180px;padding:30px 0 15px}* >
body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-
right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a
img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-
width:none;padding-right:0}}#l
|_http-server-header: gws
|_http-title: Error 404 (Not Found)!!1
443/tcp open  ssl/https gws
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Mon, 09 Nov 2020 06:46:03 GMT
|     Expires: -1
|     Cache-Control: private, max-age=0
|     Content-Type: text/html; charset=ISO-8859-1
|     P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
|     Server: gws
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     Set-Cookie: 1P_JAR=2020-11-09-06; expires=Wed, 09-Dec-2020 06:46:03 GMT; path=/;
domain=.google.com; Secure
|     Set-Cookie: NID=204=z3jlGTSidNQiB5WTvVJJxqniBKXKk7oNHFGroqQSMgqt05tBHTy-_nk0TCf-
UJq93NiEDHd7z29ONTp4t_o6suzLPpWPzhaWhNSz_hCHvwKBl_GKTnO590eZGoXE8_OYfIqc6sgnGIJ
Omnenj8xrGcYHtp18dx8-iRFm9ZAyNFU; expires=Tue, 11-May-2021 06:46:03 GMT; path=/;
domain=.google.com; HttpOnly
|     Alt-Svc: h3-Q050=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443";
ma=2592000,h3-T050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443";
ma=2592000,quic=":443"; ma=2592000; v="46,43"
|     Accept-Ranges: none
|     Vary: Accept-Enc
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: GET, HEAD
|     Date: Mon, 09 Nov 2020 06:46:03 GMT
```

```
|     Content-Type: text/html; charset=UTF-8
|     Server: gws
|     Content-Length: 1592
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     Alt-Svc: h3-Q050=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443";
ma=2592000,h3-T050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443";
ma=2592000,quic=":443"; ma=2592000; v="46,43"
|     <!DOCTYPE html>
|     <html lang=en>
|     <meta charset=utf-8>
|     <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
|     <title>Error 405 (Method Not Allowed)!!1</title>
|     <style>
|_    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-
serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-
width:390px;min-height:180px;padding:30px 0 15px}* >
body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding
|_http-server-header: gws
|_http-title: Error 404 (Not Found)!!1
| ssl-cert: Subject: commonName=invalid2.invalid
| Not valid before: 2015-01-01T00:00:00
|_Not valid after:  2030-01-01T00:00:00
|_ssl-date: 2020-11-09T06:46:59+00:00; -1s from scanner time.
| tls-alpn:
|   grpc-exp
|   h2
|_  http/1.1
| tls-nextprotoneg:
|   grpc-exp
|   h2
|_  http/1.1
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.80%I=7%D=11/9%Time=5FA8E5A6%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,1A7C,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Mon,\x2009\x20Nov\x2020
SF:20\x2006:45:57\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20private,\x
SF:20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\nP3P
SF::\x20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p3ph
SF:elp\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection:\x
SF:200\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x201P_JAR=2020-11-
SF:09-06;\x20expires=Wed,\x2009-Dec-2020\x2006:45:57\x20GMT;\x20path=/;\x2
SF:0domain=\.google\.com;\x20Secure\r\nSet-Cookie:\x20NID=204=0-J-9Rqu75P2
SF:3DPye6pSUaDhww3E24f0IPpaAYsJFh5xDZWPPt9Y660p_Q8fn5BZo9oJFMIQNbX0Gpm5gvk
SF:iCtOqFN2Z-BUNQGtt4VddtomtmuIdoaOK-S0LxgXV9gp0kL7hJJh4Pgz2w4d2GX30M_F-QO
SF:hRT2gTPdmlTUC9TlA;\x20expires=Tue,\x2011-May-2021\x2006:45:57\x20GMT;\x
SF:20path=/;\x20domain=\.google\.com;\x20HttpOnly\r\nAccept-Ranges:\x20non
SF:e\r\nVary:\x20Accept-Encoding\r\n\r\n<!doctype\x20html><html\x20itemsco
```

```
SF:pe=\"\"\x20itemtype=\"http://schema\.org/WebPage\"\x20lang=\"en-IN\"><h
SF:ead><meta\x20content=\"text/html;\x20charset=UTF-8\"\x20http-equiv=\"Co
SF:ntent-Type\"><meta\x20content=\"/images/branding/googleg")%r(HTTPOption
SF:s,70F,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\nAllow:\x20GET,\x
SF:20HEAD\r\nDate:\x20Mon,\x2009\x20Nov\x202020\x2006:45:57\x20GMT\r\nCont
SF:ent-Type:\x20text/html;\x20charset=UTF-8\r\nServer:\x20gws\r\nContent-L
SF:ength:\x201592\r\nX-XSS-Protection:\x200\r\nX-Frame-Options:\x20SAMEORI
SF:GIN\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=en>\n\x20\x20<meta\x20char
SF:set=utf-8>\n\x20\x20<meta\x20name=viewport\x20content=\"initial-scale=1
SF:,\x20minimum-scale=1,\x20width=device-width\">\n\x20\x20<title>Error\x2
SF:0405\x20\(Method\x20Not\x20Allowed\)!!1</title>\n\x20\x20<style>\n\x20\
SF:x20\x20\x20\*{margin:0;padding:0}html,code{font:15px/22px\x20arial,sans
SF:-serif}html{background:#fff;color:#222;padding:15px}body{margin:7%\x20a
SF:uto\x200;max-width:390px;min-height:180px;padding:30px\x200\x2015px}\*\
SF:x20>\x20body{background:url\(//www\.google\.com/images/errors/robot\.pn
SF:g\)\x20100%\x205px\x20no-repeat;padding-right:205px}p{margin:11px\x200\
SF:x2022px;overflow:hidden}ins{color:#777;text-decoration:none}a\x20img{bo
SF:rder:0}@media\x20screen\x20and\x20\(max-width:772px\){body{background:n
SF:one;margin-top:0;max-width:none;padding-right:0}}#l");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=11/9%Time=5FA8E5AD%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,1D04,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Mon,\x2009\x20No
SF:v\x202020\x2006:46:03\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20pri
SF:vate,\x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1
SF:\r\nP3P:\x20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.
SF:co/p3phelp\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protec
SF:tion:\x200\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x201P_JAR=2
SF:020-11-09-06;\x20expires=Wed,\x2009-Dec-2020\x2006:46:03\x20GMT;\x20pat
SF:h=/;\x20domain=\.google\.com;\x20Secure\r\nSet-Cookie:\x20NID=204=z3jlG
SF:TSidNQiB5WTvVJJxqniBKXKk7oNHFGroqQSMgqt05tBHTy-_nk0TCf-UJq93NiEDHd7z29O
SF:NTp4t_o6suzLPpWPzhaWhNSz_hCHvwKBl_GKTnO590eZGoXE8_OYfIqc6sgnGIJOmnenj8x
SF:rGcYHtp18dx8-iRFm9ZAyNFU;\x20expires=Tue,\x2011-May-2021\x2006:46:03\x2
SF:0GMT;\x20path=/;\x20domain=\.google\.com;\x20HttpOnly\r\nAlt-Svc:\x20h3
SF:-Q050=\":443\";\x20ma=2592000,h3-29=\":443\";\x20ma=2592000,h3-T051=\":
SF:443\";\x20ma=2592000,h3-T050=\":443\";\x20ma=2592000,h3-Q046=\":443\";\
SF:x20ma=2592000,h3-Q043=\":443\";\x20ma=2592000,quic=\":443\";\x20ma=2592
SF:000;\x20v=\"46,43\"\r\nAccept-Ranges:\x20none\r\nVary:\x20Accept-Enc")%
SF:r(HTTPOptions,7DC,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\nAllo
SF:w:\x20GET,\x20HEAD\r\nDate:\x20Mon,\x2009\x20Nov\x202020\x2006:46:03\x2
SF:0GMT\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nServer:\x20gws\
SF:r\nContent-Length:\x201592\r\nX-XSS-Protection:\x200\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nAlt-Svc:\x20h3-Q050=\":443\";\x20ma=2592000,h3-29=\"
SF::443\";\x20ma=2592000,h3-T051=\":443\";\x20ma=2592000,h3-T050=\":443\";
SF:\x20ma=2592000,h3-Q046=\":443\";\x20ma=2592000,h3-Q043=\":443\";\x20ma=
SF:2592000,quic=\":443\";\x20ma=2592000;\x20v=\"46,43\"\r\n\r\n<!DOCTYPE\x
SF:20html>\n<html\x20lang=en>\n\x20\x20<meta\x20charset=utf-8>\n\x20\x20<m
SF:eta\x20name=viewport\x20content=\"initial-scale=1,\x20minimum-scale=1,\
SF:x20width=device-width\">\n\x20\x20<title>Error\x20405\x20\(Method\x20No
SF:t\x20Allowed\)!!1</title>\n\x20\x20<style>\n\x20\x20\x20\x20\*{margin:0
```

```
SF:;padding:0}html,code{font:15px/22px\x20arial,sans-serif}html{background
SF::#fff;color:#222;padding:15px}body{margin:7%\x20auto\x200;max-width:390
SF:px;min-height:180px;padding:30px\x200\x2015px}\*\x20>\x20body{backgroun
SF:d:url\(//www\.google\.com/images/errors/robot\.png\)\x20100%\x205px\x20
SF:no-repeat;padding");

Host script results:
|_clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.25 seconds
```

14)

```
mareenalinux@mareenalinux:~Desktop$ nmap -Onmap -O server2.tecmint.com
Unknown argument to -O.
QUITTING!
```

15)

```
mareenalinux@mareenalinux:~Desktop$ nmap -O server2.tecmint.com
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
```

16)

```
mareenalinux@mareenalinux:~Desktop$ nmap -O 172.217.174.227
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
```

17)

```
mareenalinux@mareenalinux:~Desktop$ sudo nmap -O server2.tecmint.com
[sudo] password for roblinux:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:23 IST
Failed to resolve "server2.tecmint.com".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.26 seconds
```

18)

```
mareenalinux@mareenalinux:~Desktop$ sudo nmap -O scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:24 IST
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.92% done; ETC: 12:24 (0:00:36 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 30.02% done; ETC: 12:25 (0:00:42 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 31.68% done; ETC: 12:25 (0:00:45 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 31.09% done; ETC: 12:25 (0:00:51 remaining)
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 32.41% done; ETC: 12:25 (0:00:50 remaining)
```

19)

```
mareenalinux@mareenalinux:~Desktop$ nmap -sP 192.168.0.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:27 IST
Nmap scan report for 192.168.0.1
Host is up (0.019s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 3.40 seconds
```

20)

```
mareenalinux@mareenalinux:~Desktop$ nmap -F 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:28 IST
Nmap scan report for 192.168.0.1
Host is up (0.017s latency).
Not shown: 96 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
```

21)

```
mareenalinux@mareenalinux:~Desktop$  nmap -V
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1d nmap-libssh2-1.8.2 libz-1.2.11 libpcre-8.39 libpcap-1.9.1
nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

22)

```
mareenalinux@mareenalinux:~Desktop$ nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:30 IST
************************INTERFACES************************
DEV    (SHORT)  IP/MASK                    TYPE     UP MTU    MAC
enp0s3 (enp0s3) 10.0.2.15/24               ethernet up 1500  08:00:27:13:B3:29
enp0s3 (enp0s3) fe80::22a2:11af:4ecb:5311/64 ethernet up 1500  08:00:27:13:B3:29
lo     (lo)     127.0.0.1/8                loopback up 65536
lo     (lo)     ::1/128                    loopback up 65536

**************************ROUTES**************************
DST/MASK                  DEV    METRIC GATEWAY
10.0.2.0/24               enp0s3 100
169.254.0.0/16            enp0s3 1000
0.0.0.0/0                 enp0s3 100    10.0.2.2
::1/128                   lo     0
fe80::22a2:11af:4ecb:5311/128 enp0s3 0
::1/128                   lo     256
fe80::/64                 enp0s3 100
ff00::/8                  enp0s3 256
```

23)

```
mareenalinux@mareenalinux:~Desktop$ nmap -p 80 server2.tecmint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:30 IST
Failed to resolve "server2.tecmint.com".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds
```

24)

```
mareenalinux@mareenalinux:~Desktop$ nmap -p 80 google.co.in
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:31 IST
Nmap scan report for google.co.in (172.217.166.67)
Host is up (0.019s latency).
Other addresses for google.co.in (not scanned): 2404:6800:4009:80d::2003
rDNS record for 172.217.166.67: bom05s15-in-f3.1e100.net

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

25)

```
mareenalinux@mareenalinux:~Desktop$  nmap -sU 53 google.co.in
You requested a scan type which requires root privileges.
QUITTING!
```

26)

```
mareenalinux@mareenalinux:~Desktop$ sudo nmap -p 80 google.co.in
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:32 IST
Nmap scan report for google.co.in (172.217.166.67)
Host is up (0.0023s latency).
Other addresses for google.co.in (not scanned): 2404:6800:4009:80d::2003
rDNS record for 172.217.166.67: bom05s15-in-f3.1e100.net

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

27)

```
mareenalinux@mareenalinux:~Desktop$ nmap -p 80,443 192.168.0.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:32 IST
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 3.11 seconds
```

28)

```
mareenalinux@mareenalinux:~Desktop$ nmap -p 80,443 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:32 IST
Nmap scan report for 192.168.0.1
Host is up (0.017s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

29)

```
mareenalinux@mareenalinux:~Desktop$ nmap -PS 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:33 IST
Nmap scan report for 192.168.0.1
Host is up (0.022s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
```

30)

```
mareenalinux@mareenalinux:~Desktop$ nmap -PA -p 22,80 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:34 IST
Nmap scan report for 192.168.0.1
Host is up (0.017s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

31)

```
mareenalinux@mareenalinux:~Desktop$  nmap -sS 192.168.0.1
You requested a scan type which requires root privileges.
QUITTING!
```

32)

```
mareenalinux@mareenalinux:~Desktop$ sudo nmap -sS 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:34 IST
Nmap scan report for 192.168.0.1
Host is up (0.012s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.86 seconds
```

33)

```
mareenalinux@mareenalinux:~Desktop$ nmap -sN 192.168.0.1
You requested a scan type which requires root privileges.
QUITTING!
```

34)

```
mareenalinux@mareenalinux:~Desktop$ sudo nmap -sN 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-09 12:35 IST
Nmap scan report for 192.168.0.1
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.0.1 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Post labs:

1. Explore features of any other port scanner tool.

Ans:

The original netcat's features include:

- Outbound or inbound connections, TCP or UDP, to or from any ports
- Full DNS forward/reverse checking, with appropriate warnings
- Ability to use any local source port
- Ability to use any locally configured network source address
- Built-in port-scanning capabilities, with randomization
- Built-in loose source-routing capability
- Can read command line arguments from standard input
- Slow-send mode, one line every N seconds
- Hex dump of transmitted and received data
- Optional ability to let another program service establish connections
- Optional telnet-options responder
- Rewrites like GNU's and OpenBSD's support additional features. For example, OpenBSD's netcat supports TLS, and GNU netcat natively supports a tunnelling mode supporting UDP and TCP (optionally allowing one to be tunnelled over the other) in a single command,[3] where other versions may require piping data from one netcat instance to another.