



PRATICAL FILE

Dr. Gopal Singh Rawat
Course- Physical IT & Sec

Dhairya Jain
500105432 | R2142220251
B.Tech_CSE_CSF_B-1_Sem-III

Aim- Learn Network Scanning Tool - NMAP

- Kowing our own ip address:

```
(root@kali)-[/home/dhairya]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::d091:2a2d:a341:7b40 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:72:6a:99 txqueuelen 1000 (Ethernet)
    RX packets 281392 bytes 333060005 (317.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 180230 bytes 13944923 (13.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 172 bytes 17192 (16.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 172 bytes 17192 (16.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Scanning scanme.nmap.org to preform activity

- Scanning one ip / single ip:

```
(root@kali)-[/home/dhairya]
# nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-16 22:49 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00086s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 610 filtered tcp ports (no-response), 387 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 438.97 seconds
```

- Scanning entire subnet :

```
(root@kali)-[/home/dhairya]
└─$ nmap 192.168.0.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-28 14:05 IST
Stats: 0:11:18 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.42% done; ETC: 14:21 (0:03:51 remaining)
Nmap scan report for 192.168.0.0
Host is up (0.091s latency).
All 1000 scanned ports on 192.168.0.0 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.1
Host is up (0.0065s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 192.168.0.2
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.0.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.3
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.0.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.4
Host is up (0.040s latency).
All 1000 scanned ports on 192.168.0.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.5
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.0.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.6
Host is up (0.027s latency).
All 1000 scanned ports on 192.168.0.6 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.7
Host is up (0.024s latency).
All 1000 scanned ports on 192.168.0.7 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.57
Host is up (0.057s latency).
All 1000 scanned ports on 192.168.0.57 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.58
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.0.58 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.59
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.0.59 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.60
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.0.60 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.61
Host is up (0.017s latency).
All 1000 scanned ports on 192.168.0.61 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.62
Host is up (0.028s latency).
All 1000 scanned ports on 192.168.0.62 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.63
Host is up (0.027s latency).
All 1000 scanned ports on 192.168.0.63 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Warning: 192.168.0.123 giving up on port because retransmission cap hit (10).
Stats: 128:21:49 elapsed; 64 hosts completed (128 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.40% done; ETC: 18:13 (67:45:54 remaining)
Warning: 192.168.0.106 giving up on port because retransmission cap hit (10).
```

- ```
(root@kali)-[/home/dhairya]
nmap 45.33.32.156 192.168.0.1 10.0.2.15
Starting Nmap 7.93 (https://nmap.org) at 2023-12-03 22:31 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0023s latency).
Not shown: 501 closed tcp ports (reset), 496 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
9929/tcp open nping-echo
31337/tcp open Elite

Nmap scan report for 192.168.0.1
Host is up (0.0039s latency).
Not shown: 921 filtered tcp ports (no-response), 78 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http

Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 3 IP addresses (3 hosts up) scanned in 83.79 seconds
```

- [illegible]

- ```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -p80,21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-03 22:30 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.037s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
80/tcp    open       http

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

- Tcp syn scan(aka Stealth Scan) (-sS):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -sS -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-03 23:42 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (2).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

- TCP connect scan(-sT):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -sT -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-03 23:47 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0011s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
```

- UPD scan(-sU):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -sU -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-03 23:49 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (2).
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 27.90% done; ETC: 23:50 (0:01:12 remaining)
Stats: 0:03:59 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 59.13% done; ETC: 23:56 (0:02:46 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.57s latency).
Not shown: 681 filtered udp ports (port-unreach), 318 open|filtered udp ports (no-response)
PORT      STATE SERVICE
123/udp   open  ntp

Nmap done: 1 IP address (1 host up) scanned in 694.77 seconds
```

- FIN Scan(-sF):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -sF -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 00:09 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00047s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```


- Ping Scan(-sP):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -sP -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 00:10 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00032s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

- Version Detection(-sV):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 00:17 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.023s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
31337/tcp open  tcpwrapped
Service Info: 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 33.20 seconds
```

- Idle Scan (anonymous scan)(-sI):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -sI 45.33.32.175
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On the other hand, timing info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 00:43 IST
Idle scan using zombie 45.33.32.175 (45.33.32.175:443); Class: Incremental
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.014s latency).
Not shown: 999 closed|filtered tcp ports (no-ipid-change)
PORT      STATE SERVICE
3052/tcp  open  powerchute
Nmap done: 1 IP address (1 host up) scanned in 65.61 seconds
```

- Operating system scan(-O)

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -O -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 01:00 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.026s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Cisco Catalyst 1900 switch (93%), Nokia 3600i mobile phone (93%), Cisco ATA 188 VoIP adapter (91%), Apple Time Capsule NAS device (90%), Oracle Virtualbox (87%), QEMU user mode network gateway (87%), GNU Hurd 0.3 (87%), Huawei Echolife HG520-series ADSL modem (87%), TP-LINK TD-W8951ND wireless ADSL modem (87%), ZyXEL Prestige 660R ADSL router (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.85 seconds

(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -O
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 01:01 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.015s latency).
Not shown: 968 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (89%), QEMU (87%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (89%), QEMU user mode network gateway (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.28 seconds
```

- Slowest scan to fastest scan(-T(0 to 5)):

```
(root@kali)~[/home/dhairya]
# nmap 45.33.32.156 -T3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 17:52 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (10).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00098s latency).
Not shown: 626 closed tcp ports (reset), 370 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 4681.05 seconds

(root@kali)~[/home/dhairya]
# nmap 45.33.32.156 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 19:11 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.062s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 13.94 seconds
(root@kali)~[/home/dhairya]
```

- Aggressive Scan (Enable OS detection, version detection, script scanning, and traceroute --datadir : Specify custom Nmap data file location --send-eth/--send-ip: Send using raw ethernet frames or IP packets --privileged: Assume that the user is fully privileged --unprivileged: Assume the user lacks raw socket privileges)(-A):

```
(root@kali)~[/home/dhairya]
# nmap 45.33.32.156 -A -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 19:18 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (2).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.045s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 ac00a01a82ffcc5599dc672b34976b75 (DSA)
|   2048 203d2d44622ab05a9db5b30514c2a6b2 (RSA)
|   256 9602bb5e57541c4e452f564c4a24b257 (ECDSA)
|_  256 33fa910fe0e17b1f6d05a2b0f1544156 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-favicon: Nmap Project
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   1.34 ms  10.0.2.2
2   1.46 ms  scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.76 seconds
```

- the verbosity of the output(-vvv):

```
(root@kali)-[/home/dhairya]
# nmap 45.33.32.156 -vvv -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-04 19:20 IST
Initiating Ping Scan at 19:20
Scanning 45.33.32.156 [4 ports]
Completed Ping Scan at 19:20, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:20
Completed Parallel DNS resolution of 1 host. at 19:20, 0.01s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 19:20
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 21 dropped probes since last increase.
Completed SYN Stealth Scan at 19:21, 20.09s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 255 (0.038s latency).
Scanned at 2023-12-04 19:20:50 IST for 20s
Not shown: 921 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
366/tcp   closed odmr     reset ttl 255
464/tcp   closed kpasswd5  reset ttl 255
497/tcp   closed retrospect reset ttl 255
700/tcp   closed epp       reset ttl 255
911/tcp   closed xact-backup reset ttl 255
1026/tcp  closed lsa-or-nterm reset ttl 255
1076/tcp  closed sns_credit reset ttl 255
1087/tcp  closed cplscrambler-in reset ttl 255
1096/tcp  closed cnrprotocol reset ttl 255
1102/tcp  closed adobeserver-1 reset ttl 255
1111/tcp  closed lmsocialserver reset ttl 255
1114/tcp  closed mini-sql   reset ttl 255
1132/tcp  closed kvm-via-ip  reset ttl 255
1152/tcp  closed winopplanmess reset ttl 255
1164/tcp  closed qsm-proxy   reset ttl 255
1233/tcp  closed univ-appserver reset ttl 255
1272/tcp  closed cspmlckmgr  reset ttl 255
1296/tcp  closed dproxy      reset ttl 255
1311/tcp  closed rxmon       reset ttl 255
1322/tcp  closed novation    reset ttl 255
1334/tcp  closed writesrv    reset ttl 255
1583/tcp  closed simbaexpress reset ttl 255
1839/tcp  closed netopia-vol  reset ttl 255
1875/tcp  closed westell-stats reset ttl 255
2007/tcp  closed dectalk     reset ttl 255
4045/tcp  closed lockd       reset ttl 255
4445/tcp  closed upnotifyp   reset ttl 255
5001/tcp  closed complex-link reset ttl 255
5051/tcp  closed ida-agent    reset ttl 255
5431/tcp  closed park-agent   reset ttl 255
5432/tcp  closed postgresql   reset ttl 255
5440/tcp  closed unknown     reset ttl 255
5633/tcp  closed beorl       reset ttl 255
5678/tcp  closed rrac        reset ttl 255
5850/tcp  closed unknown     reset ttl 255
5862/tcp  closed unknown     reset ttl 255
5903/tcp  closed vnc-3       reset ttl 255
5963/tcp  closed indy        reset ttl 255
6007/tcp  closed X11:7       reset ttl 255
6009/tcp  closed X11:9       reset ttl 255
6389/tcp  closed clariion-evr01 reset ttl 255
6510/tcp  closed mcer-port    reset ttl 255
8010/tcp  closed xmpp        reset ttl 255
8093/tcp  closed unknown     reset ttl 255
8383/tcp  closed m2mservices  reset ttl 255
8701/tcp  closed unknown     reset ttl 255
9011/tcp  closed d-star      reset ttl 255
9040/tcp  closed tor-trans    reset ttl 255
9415/tcp  closed unknown     reset ttl 255
9929/tcp  open  nping-echo syn-ack ttl 64
10010/tcp closed rxapi       reset ttl 255
10778/tcp closed unknown     reset ttl 255
11110/tcp closed sgi-soap     reset ttl 255
13722/tcp closed netbackup    reset ttl 255
15002/tcp closed onep-tls     reset ttl 255
15742/tcp closed unknown     reset ttl 255
16018/tcp closed unknown     reset ttl 255
19283/tcp closed keysrvr     reset ttl 255
26214/tcp closed unknown     reset ttl 255
31337/tcp open  Elite     syn-ack ttl 64
32769/tcp closed fillenet-rpc reset ttl 255
32781/tcp closed unknown     reset ttl 255
49161/tcp closed unknown     reset ttl 255
50800/tcp closed unknown     reset ttl 255
55555/tcp closed unknown     reset ttl 255
56738/tcp closed unknown     reset ttl 255
57294/tcp closed unknown     reset ttl 255
65000/tcp closed unknown     reset ttl 255

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 20.44 seconds
Raw packets sent: 2943 (129.416KB) | Rcvd: 1380 (55.208KB)
```


