

Network Security

Roll: MC233104

Name: Saif Md. Zulker Nein Chowdhury

Mobile: 01672947867

Email: julker@gmail.com

Exercise 1: Nmap Practice

In the following exercise, I have used these commands.

1. Version Check: `nmap -v -A scanme.nmap.org`

```
(kali@kali)-[~]
$ nmap -v -A scanme.nmap.org

Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:49 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:49
Completed NSE at 09:49, 0.00s elapsed
Initiating NSE at 09:49
Completed NSE at 09:49, 0.00s elapsed
Initiating NSE at 09:49
Completed NSE at 09:49, 0.00s elapsed
Initiating Ping Scan at 09:49
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 09:49, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:49
Completed Parallel DNS resolution of 1 host. at 09:49, 0.04s elapsed
Initiating Connect Scan at 09:49
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 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 09:49, 43.52s elapsed (1000 total ports)
Initiating Service scan at 09:49
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 09:50, 6.58s elapsed (4 services on 1 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 09:50
Completed NSE at 09:50, 16.25s elapsed
Initiating NSE at 09:50
Completed NSE at 09:50, 1.15s elapsed
Initiating NSE at 09:50
Completed NSE at 09:50, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
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-title: Go ahead and ScanMe!
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
```

2. Scanning Website: **nmap facebook.com**

```
(kali@kali)-[~]
$ nmap facebook.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:54 EST
Nmap scan report for facebook.com (157.240.235.35)
Host is up (0.060s latency).
Other addresses for facebook.com (not scanned): 2a03:2880:f10c:381:face:b00c:0:25de
rDNS record for 157.240.235.35: edge-star-mini-shv-04-sin6.facebook.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 21.07 seconds
```

3. Host Discovery – **Traceout: sudo nmap -traceout 51.23.48.15**

```
(kali@kali)-[~]
$ sudo nmap -traceroute 51.23.48.15
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:57 EST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Parallel DNS resolution of 2 hosts. Timing: About 50.00% done; ETC: 09:57 (0:00:03 remaining)
Nmap scan report for 51.23.48.15
Host is up (0.010s latency).
All 1000 scanned ports on 51.23.48.15 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   14.23 ms  10.0.2.2
2   14.24 ms  51.23.48.15

Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds

(kali@kali)-[~]
$
```

4. Port Specification: **nmap 51.23.48.15 -p443**

```
(kali@kali)-[~]
$ nmap 51.23.48.15 -p3000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:59 EST
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 3.06 seconds

(kali@kali)-[~]
$ nmap 51.23.48.15 -p80
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:59 EST
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 3.04 seconds

(kali@kali)-[~]
$ nmap 51.23.48.15 -p80 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:59 EST
Nmap scan report for 51.23.48.15
Host is up.

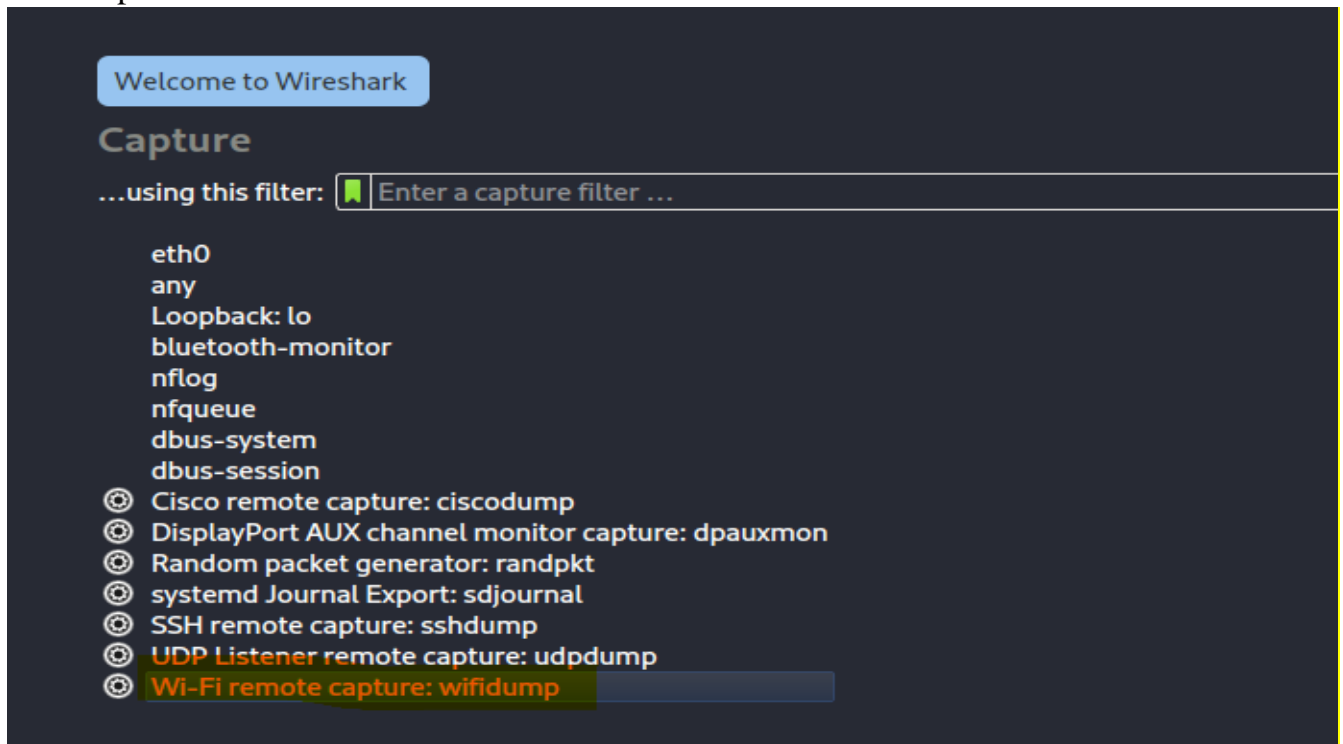
PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds

(kali@kali)-[~]
$
```

Exercise 2: Wireshark Practice

Wifi Capture:



Apply a display filter ... <Ctrl-/>

Interface

Channel

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	34.117.237.239	TLSv1.2	93	Application Data
2	0.000860454	34.117.237.239	10.0.2.15	TCP	60	443 → 49778 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3	0.059081648	34.117.237.239	10.0.2.15	TLSv1.2	93	Application Data
4	0.106598515	10.0.2.15	34.117.237.239	TCP	54	49778 → 443 [ACK] Seq=40 Ack=40 Win=64028 Len=0
5	2.001818358	10.0.2.15	34.149.100.209	TLSv1.2	100	Application Data
6	2.002585218	34.149.100.209	10.0.2.15	TCP	60	443 → 36542 [ACK] Seq=1 Ack=47 Win=65535 Len=0
7	2.061279185	34.149.100.209	10.0.2.15	TLSv1.2	100	Application Data
8	2.101926108	10.0.2.15	34.149.100.209	TCP	54	36542 → 443 [ACK] Seq=47 Ack=47 Win=63540 Len=0

▶ Frame 5: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface eth0, id 0

▶ Ethernet II, Src: PcsCompu_53:0c:ba (08:00:27:53:0c:ba), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.149.100.209

▶ Transmission Control Protocol, Src Port: 36542, Dst Port: 443, Seq: 1, Ack: 1, Len: 46

▶ Transport Layer Security

0000 52 54 00 12 35 02 08 00 27 53 0c ba 08 00 45 00 RT 5 'S...E

0010 00 56 90 f3 40 00 40 06 16 3a 0a 00 02 0f 22 95 V @ @ :....".

0020 64 d1 8e be 01 bb b8 08 93 ee 0f e6 fa d8 50 18 dP

0030 f8 34 93 bd 00 00 17 03 03 00 29 00 00 00 00 00 4)

0040 00 00 07 5a 26 7d 65 75 be ad 40 e4 6c c0 3a 49 Z&}eu @ l :I

0050 fc 6d 7f 59 8d eb e0 15 1b 14 1c c2 c2 34 16 bb m Y.....4..

0060 50 54 05 f6 PT..