

Assessment Date: 2025-05-26

Tool Used: Nmap & Wireshark v4.x

Network SSID: 10.0.2.15

Assessor: Rohit Kumar

Task 1 = Scan Your Local Network for Open Ports.

Objective = Learn to discover open ports on devices in your local network to understand network exposure.

1. Finding Ip (ifconfig)

```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(sifir@sifir)-[~]
$ 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 fd17:625c:f037:2:a00:27ff:fe9b:c3c prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe9b:c3c prefixlen 64 scopeid 0<link>
    inet6 fd17:625c:f037:2:5b2e:8160:cfda:9de3 prefixlen 64 scopeid 0<global>
    ether 08:00:27:9b:0c:3c txqueuelen 1000 (Ethernet)
    RX packets 9 bytes 3699 (3.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 4955 (4.8 KiB)
    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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

2. scanning network for open ports (nmap -sS 10.2.15/24)

```
(sifir@sifir)-[~]
$ nmap -sS 10.0.2.15/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 19:03 IST
Nmap scan report for 10.0.2.2
Host is up (0.0021s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
1042/tcp   open  afrog
1043/tcp   open  boinc
7778/tcp   open  interwise
MAC Address: 52:55:0A:00:02:02 (Unknown)

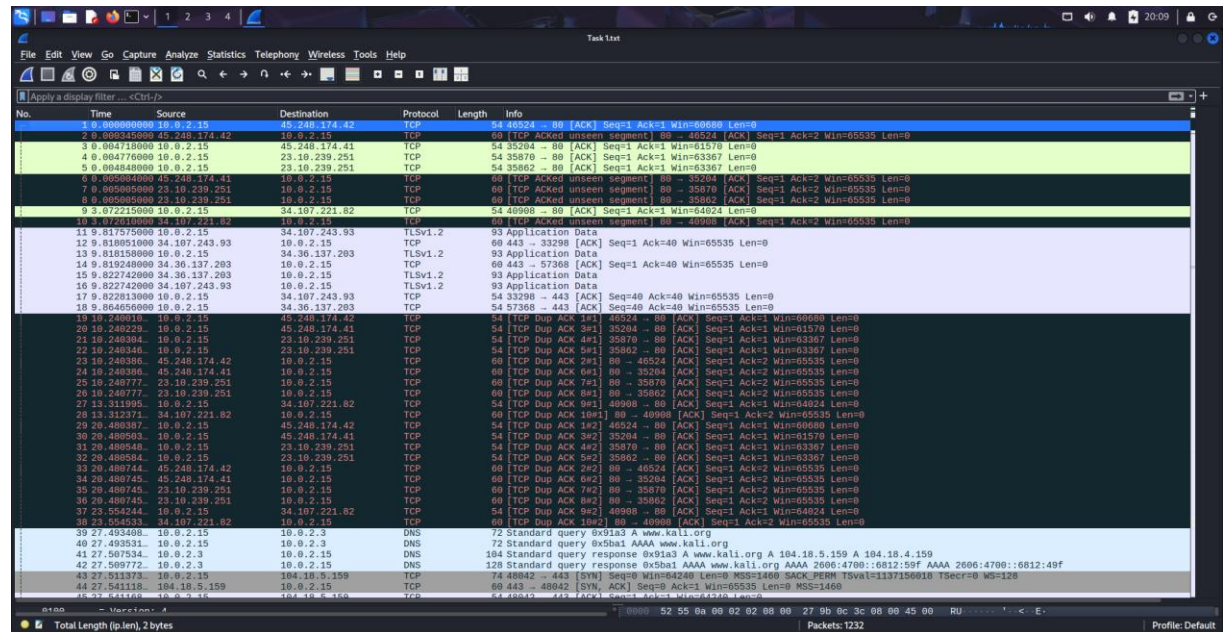
Nmap scan report for 10.0.2.3
Host is up (0.0022s latency).
Not shown: 999 filtered tcp ports (net-unreach)
PORT      STATE SERVICE
53/tcp     open  domain
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

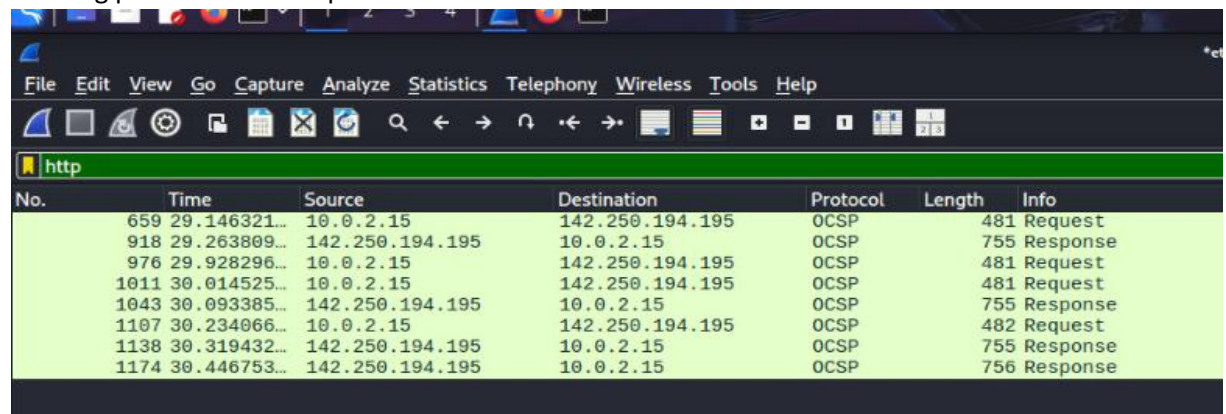
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.75 seconds

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

3. Capturing packets using wireshark



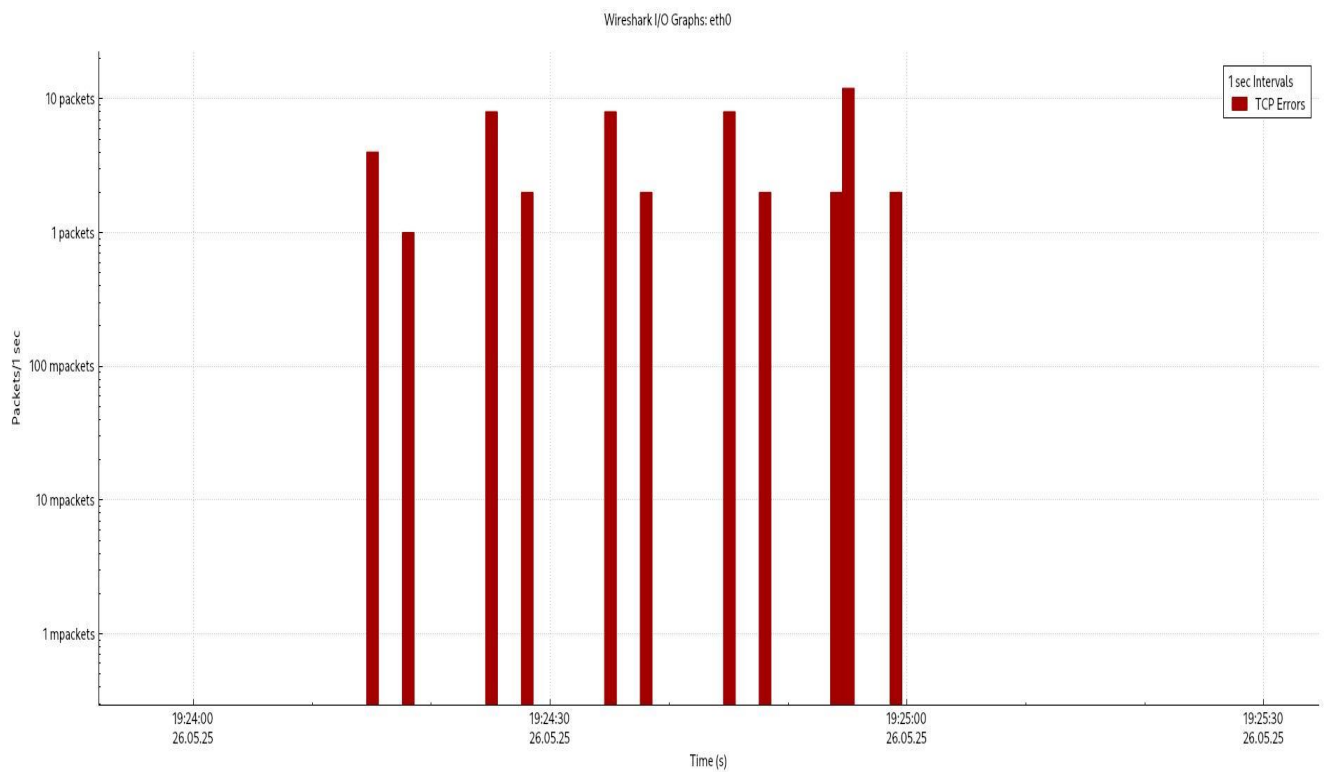
4. Filtering packets to see Http



5. Checking Conversation happening Between different devices

Wireshark - Conversations - Task List															
Conversation Settings															
Ethernet - 2		IPv4 - 17		IPv6		TCP - 18		UDP - 8							
Name resolution	Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A + B	Bytes A + B	Packets B + A	Bytes B + A	Rel Start	Duration	Bits/s A + B	Bits/s B + A
Absolute start time	10.0.2.15	35862	23.10.239.251	80	10	570 bytes	3	5	270 bytes	5	300 bytes	0.004848	40.9573	52 bits/s	58 bits/s
Limit to display filter	10.0.2.15	35870	23.10.239.251	80	10	570 bytes	2	5	270 bytes	5	300 bytes	0.004776	40.9574	52 bits/s	58 bits/s
	10.0.2.15	57368	34.36.137.203	443	4	300 bytes	6	2	147 bytes	2	153 bytes	9.818158	0.0465	25 kbps	26 kbps
	10.0.2.15	44614	34.49.51.44	443	4	300 bytes	13	2	147 bytes	2	153 bytes	38.215142	0.0498	23 kbps	24 kbps
	10.0.2.15	40908	34.107.221.82	80	10	570 bytes	4	5	270 bytes	5	300 bytes	3.072215	40.9602	52 bits/s	58 bits/s
	10.0.2.15	33298	34.107.243.93	443	4	300 bytes	5	2	147 bytes	2	153 bytes	9.817575	0.0052	224 kbps	233 kbps
	10.0.2.15	51332	34.149.100.209	443	4	300 bytes	17	2	147 bytes	2	153 bytes	38.215598	0.0493	23 kbps	24 kbps
	10.0.2.15	56000	34.160.144.191	443	4	300 bytes	16	2	154 bytes	2	160 bytes	38.215146	0.0494	24 kbps	25 kbps
	10.0.2.15	41504	35.244.181.201	443	4	300 bytes	15	2	154 bytes	2	160 bytes	38.215336	0.0495	24 kbps	25 kbps
	10.0.2.15	35204	45.248.174.41	80	10	570 bytes	1	5	270 bytes	5	300 bytes	0.004718	40.9574	52 bits/s	58 bits/s
	10.0.2.15	46524	45.248.174.42	80	10	570 bytes	0	5	270 bytes	5	300 bytes	0.000000	40.9643	52 bits/s	58 bits/s
	10.0.2.15	48042	104.18.5.159	443	886	2 MB	7	335	25 kb	551	2 MB	27.511373	2.5098	80 kbps	6,876 kbps
	10.0.2.15	47802	142.250.194.10	443	30	9 kb	8	15	2 kb	15	7 kb	29.042785	0.3539	50 kbps	148 kbps
	10.0.2.15	48548	142.250.194.138	443	24	9 kb	11	12	2 kb	12	7 kb	29.990326	0.1903	78 kbps	309 kbps
	10.0.2.15	34638	142.250.194.195	80	9	2 kb	9	5	717 bytes	4	935 bytes	28.115937	10.1485	565 bits/s	737 bits/s
	10.0.2.15	34640	142.250.194.195	80	9	2 kb	10	5	717 bytes	4	935 bytes	28.973441	10.3969	551 bits/s	719 bits/s
	10.0.2.15	43606	142.250.194.195	80	13	3 kb	12	7	1 kb	6	2 kb	30.005864	10.4428	959 bits/s	1,341 bits/s
	10.0.2.15	51744	151.101.129.91	443	4	300 bytes	14	2	154 bytes	2	160 bytes	38.215279	0.0056	221 kbps	229 kbps

6. I/O Graph for TCP Errors



Recommendations

- Close unused ports on devices (e.g., via firewall/router settings)
- Disable insecure services like Telnet
- Keep firmware and operating systems updated
- Use network segmentation to limit exposure