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.

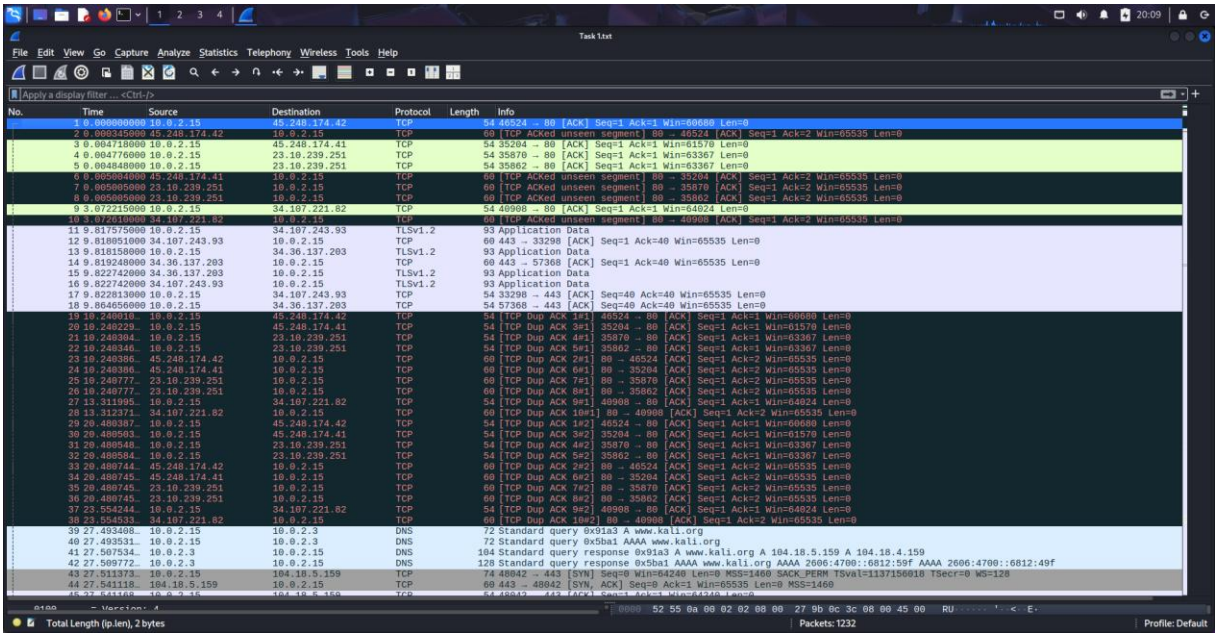
1. Finding Ip (ifconfig)

```
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 0x0<global>
        inet6 fe80::a00:27ff:fe9b:c3c  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:5b2e:8160:cfda:9de3  prefixlen 64  scopeid 0x0<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 0x10<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)-[~]
└─$
```

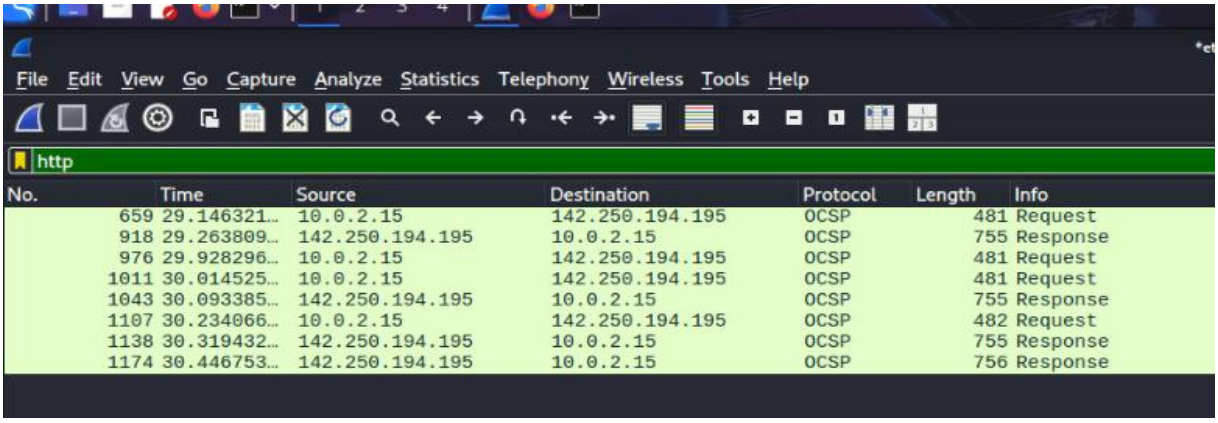
2. scanning network for open ports (nmap -sS 10.2.15/24)

```
┌──(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)-[~]
└─$
```

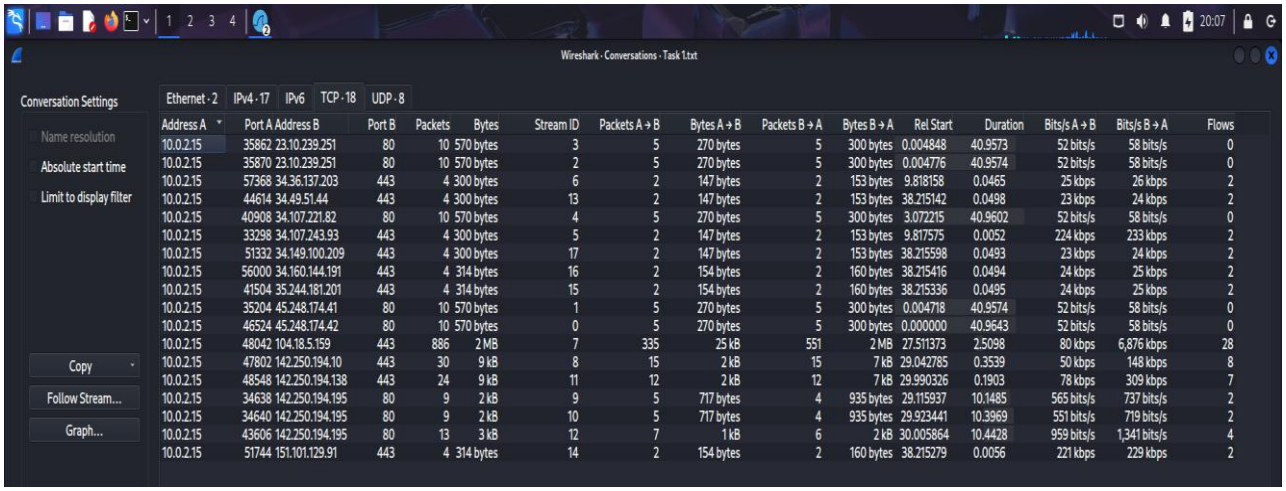
3. Capturing packets using wireshark



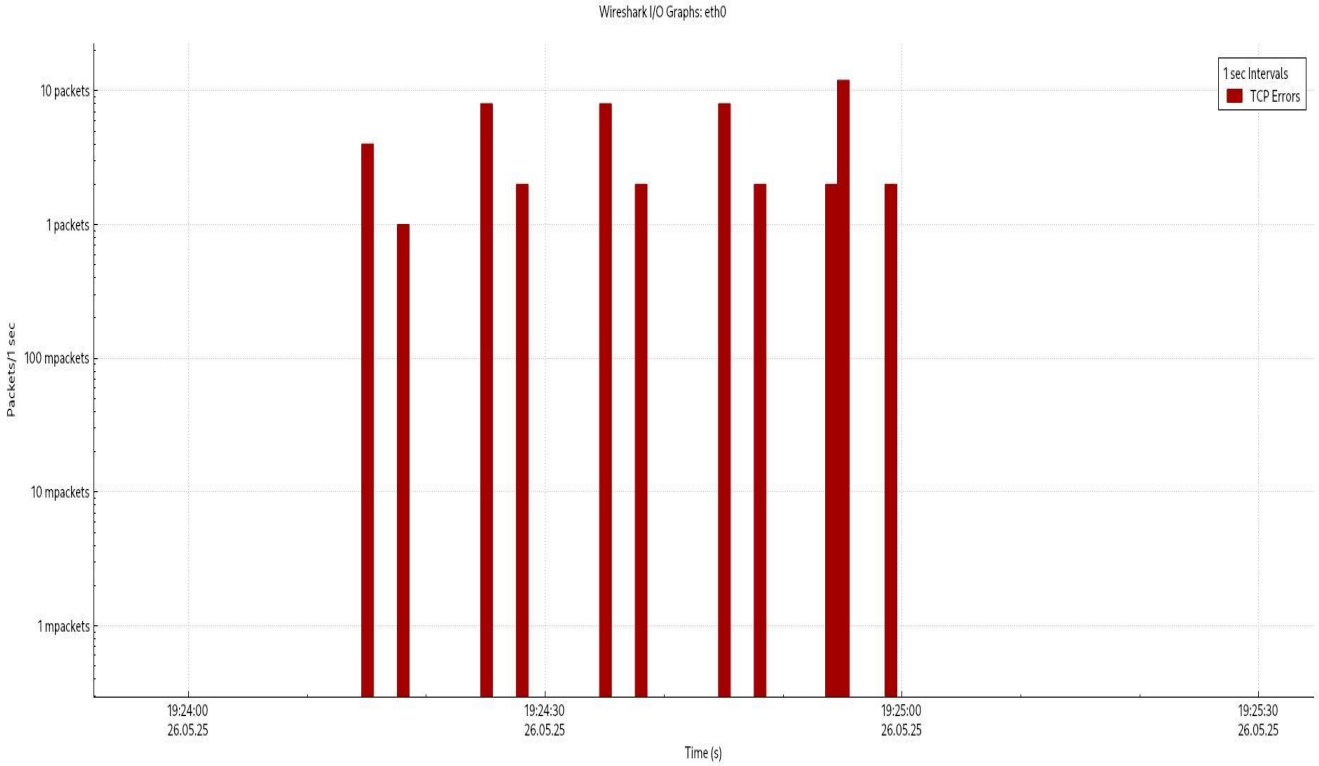
4. Filtering packets to see Http



5. Checking Conversation happening Between different devices



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