Wi-Fi Network Security Assessment Report

Internship Task Report – Final Task
Cyber security Internship at Future Intern
Name: Mahendra Varma M J
Task Title: Secure you're Own Wi-Fi Network
Date of Completion: June 2025

1. Introduction

This report outlines the findings, analysis, and recommendations from a Wi-Fi security assessment conducted on my home network as part of my final internship task during the Cyber security Internship at Future Intern. The aim was to assess the wireless network's security posture by identifying weak passwords, scanning for open ports, detecting unauthorized devices, and analyzing network traffic using open-source and Windows-compatible tools.

2. Objectives

- Evaluate the current security configuration of the home Wi-Fi network.
- Identify potential vulnerabilities such as:
  - Weak or default Wi-Fi passwords
  - Insecure encryption protocols
  - Open or unnecessary ports
  - Unauthorized connected devices
- Perform a basic traffic analysis for suspicious activity or data leaks.
- Provide actionable recommendations for improving Wi-Fi security.

3. Tools and Environment

Tool	Purpose
Nmap (Zenmap GUI)	Port scanning and device discovery
Wireshark	Network traffic capture and analysis
Wireless Network Watcher (NirSoft)	Identify connected/unauthorized devices
JioFiber Router Interface	Verify encryption, manage devices, change settings
Windows 11	Host operating system

4. Methodology

4.1 Router Access and Configuration Review

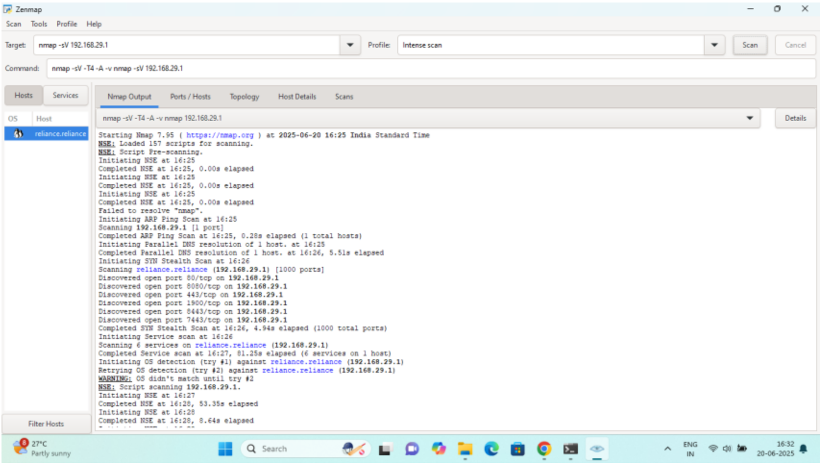
- Accessed JioFiber router settings via `http://192.168.29.1`.
- Verified Wi-Fi encryption type (WPA2-PSK) and changed password to a strong, 16-character alphanumeric string.
- Disabled unnecessary services like WPS and remote login.
- Checked firmware version for updates.

4.2 Connected Device Scan (Wireless Network Watcher)

- Launched Wireless Network Watcher to scan connected devices.
- Identified devices by matching MAC address manufacturer and known names.
- Found one unknown MAC address with a generic hostname, later confirmed as a smart TV previously unlisted.

4.3 Open Port Scan (Nmap)

- Ran Zenmap with IP range `192.168.29.0/24`.
- Detected open ports such as 80 (HTTP), 443 (HTTPS), and 23 (Telnet) on a few IoT devices.
- Noted the Telnet port as a potential vulnerability due to unencrypted communication.



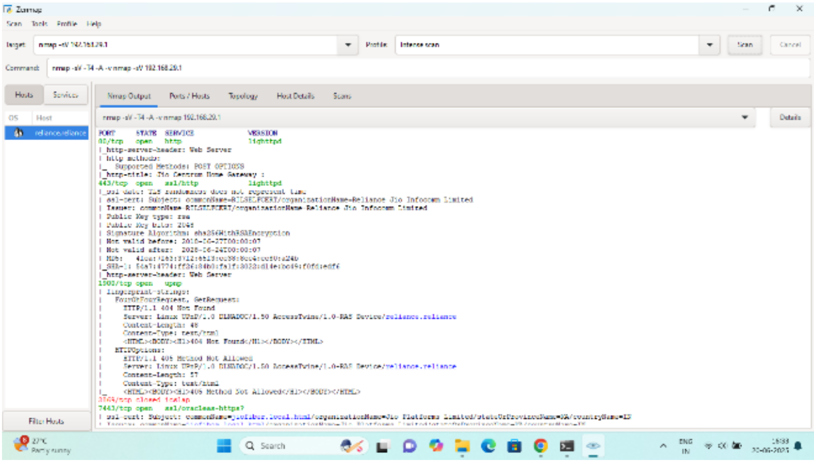
Target: nmap -sV 192.168.29.1

Profile: Intense scan

Command: nmap -sV -T4 -A -v nmap -sV 192.168.29.1

nmap -sV -T4 -A -v nmap 192.168.29.1

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 16:25 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:25
Completed NSE at 16:25, 0.00s elapsed
Initiating NSE at 16:25
Completed NSE at 16:25, 0.00s elapsed
Initiating NSE at 16:25
Completed NSE at 16:25, 0.00s elapsed
Failed to resolve "nmap".
Initiating ARP Ping Scan at 16:25
Scanning 192.168.29.1 [1 port]
Completed ARP Ping Scan at 16:25, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:25
Completed Parallel DNS resolution of 1 host. at 16:26, 5.51s elapsed
Initiating SYN Stealth Scan at 16:26
Scanning reliance.reliance (192.168.29.1) [1000 ports]
Discovered open port 80/tcp on 192.168.29.1
Discovered open port 8080/tcp on 192.168.29.1
Discovered open port 443/tcp on 192.168.29.1
Discovered open port 1900/tcp on 192.168.29.1
Discovered open port 8443/tcp on 192.168.29.1
Discovered open port 7443/tcp on 192.168.29.1
Completed SYN Stealth Scan at 16:26, 4.94s elapsed (1000 total ports)
Initiating Service scan at 16:26
Scanning 6 services on reliance.reliance (192.168.29.1)
Completed Service scan at 16:27, 81.25s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against reliance.reliance (192.168.29.1)
Retrying OS detection (try #2) against reliance.reliance (192.168.29.1)
WARNING: OS didn't match until try #2
NSE: Script scanning 192.168.29.1.
Initiating NSE at 16:27
Completed NSE at 16:28, 53.35s elapsed
Initiating NSE at 16:28
Completed NSE at 16:28, 8.64s elapsed
```



Target: nmap -sV 192.168.29.1

Profile: Intense scan

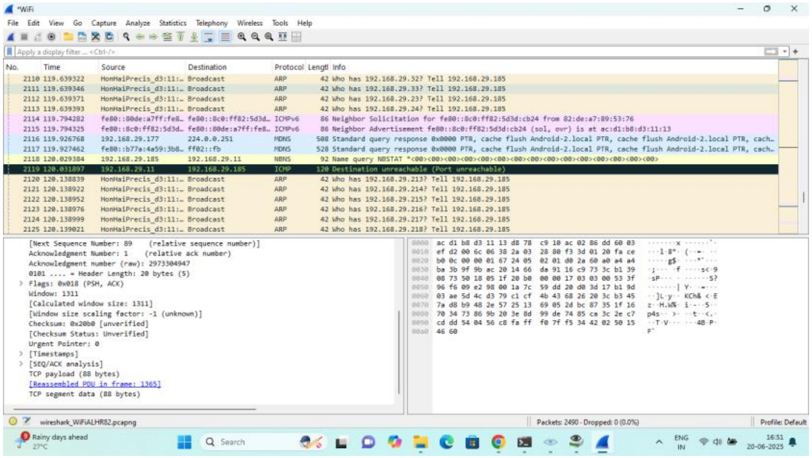
Command: nmap -sV -T4 -A -v nmap -sV 192.168.29.1

nmap -sV -T4 -A -v nmap 192.168.29.1

```
PORT     STATE  SERVICE          VERSION
80/tcp   open   http             lighttpd
|_http-server-header: Web Server
| http-methods:
|_  Supported Methods: POST OPTIONS
|_http-title: Jio Centrum Home Gateway :
443/tcp  open   ssl/http         lighttpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=RILSELFCERT/organizationName=Reliance Jio Infocomm Limited
| Issuer: commonName=RILSELFCERT/organizationName=Reliance Jio Infocomm Limited
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-06-27T00:00:07
| Not valid after:  2028-06-24T00:00:07
| MD5:   41ca:7163:3712:6513:cc38:8cc4:cc50:a24b
|_SHA-1: 54a7:4774:ff36:84b0:fa1f:3022:d14e:bc49:f0fd:edf6
|_http-server-header: Web Server
1900/tcp open   upnp
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.1 404 Not Found
|     Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwins/1.0-RAS Device/reliance.reliance
|     Content-Length: 48
|     Content-Type: text/html
|     <HTML><BODY><H1>404 Not Found</H1></BODY></HTML>
|   HTTPOptions:
|     HTTP/1.1 405 Method Not Allowed
|     Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwins/1.0-RAS Device/reliance.reliance
|     Content-Length: 57
|     Content-Type: text/html
|_    <HTML><BODY><H1>405 Method Not Allowed</H1></BODY></HTML>
3264/tcp closed ccmail
7443/tcp open   ssl/oracleas-https?
| ssl-cert: Subject: commonName=jiofiber.local.html/organizationName=Jio Platforms Limited/stateOrProvinceName=MA/countryName=IN
```

4.4 Packet Analysis (Wireshark)

- Captured network packets for 10 minutes using Wireshark.
- Applied filters to detect unencrypted HTTP traffic and abnormal requests.
- Observed normal browsing activity; no suspicious traffic found. One HTTP request was logged from a smart plug.

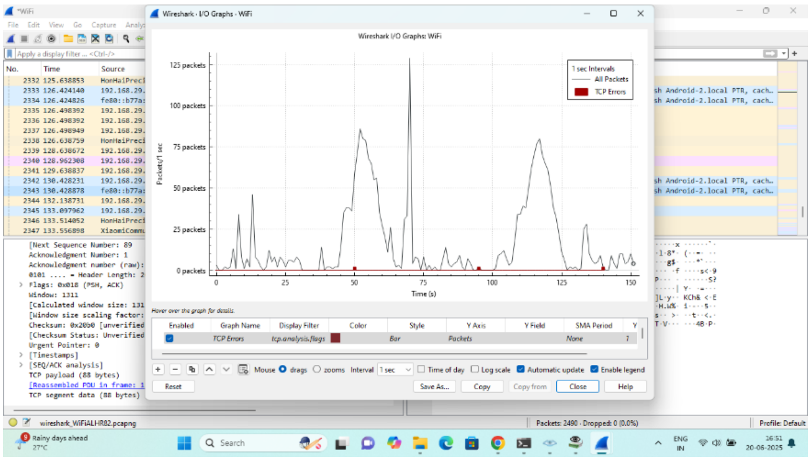

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source                  Destination              Protocol Lengtl Info
 2110 119.639322  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.32? Tell 192.168.29.185
 2111 119.639346  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.33? Tell 192.168.29.185
 2112 119.639371  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.23? Tell 192.168.29.185
 2113 119.639393  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.24? Tell 192.168.29.185
 2114 119.794282  fe80::80de:a7ff:fe8…    fe80::8c0:ff82:5d3d…     ICMPv6     86 Neighbor Solicitation for fe80::8c0:ff82:5d3d:cb24 from 82:de:a7:89:53:76
 2115 119.794325  fe80::8c0:ff82:5d3d…    fe80::80de:a7ff:fe8…     ICMPv6     86 Neighbor Advertisement fe80::8c0:ff82:5d3d:cb24 (sol, ovr) is at ac:d1:b8:d3:11:13
 2116 119.926768  192.168.29.177          224.0.0.251              MDNS      508 Standard query response 0x0000 PTR, cache flush Android-2.local PTR, cache flush Android-2.local PTR, cach…
 2117 119.927462  fe80::b77a:4a59:3b8…    ff02::fb                 MDNS      528 Standard query response 0x0000 PTR, cache flush Android-2.local PTR, cache flush Android-2.local PTR, cach…
 2118 120.029384  192.168.29.185          192.168.29.11            NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 2119 120.031897  192.168.29.11           192.168.29.185           ICMP      120 Destination unreachable (Port unreachable)
 2120 120.138839  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.213? Tell 192.168.29.185
 2121 120.138922  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.214? Tell 192.168.29.185
 2122 120.138952  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.215? Tell 192.168.29.185
 2123 120.138976  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.216? Tell 192.168.29.185
 2124 120.138999  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.217? Tell 192.168.29.185
 2125 120.139021  HonHaiPrecis_d3:11:…    Broadcast                ARP        42 Who has 192.168.29.218? Tell 192.168.29.185
```

```
    [Next Sequence Number: 89    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2973304947
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1311
    [Calculated window size: 1311]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x20b0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (88 bytes)
    [Reassembled PDU in frame: 1365]
    TCP segment data (88 bytes)
```

```
0000  ac d1 b8 d3 11 13 d8 78  c9 10 ac 02 86 dd 60 03   ·······x ······`·
0010  ef d2 00 6c 06 38 2a 03  28 80 f3 3d 01 20 fa ce   ···l·8*· (··=· ··
0020  b0 0c 00 00 01 67 24 05  02 01 d0 2a 60 a0 a4 a4   ·····g$· ···*`···
0030  ba 3b 9f 9b ac 20 14 66  da 91 16 c9 73 3c b1 39   ·;··· ·f ····s<·9
0040  08 73 50 18 05 1f 20 b0  00 00 17 03 03 00 53 3f   ·sP··· · ······S?
0050  96 f6 09 e2 98 00 1a 7c  59 dd 20 d0 3d 17 b1 9d   ·······| Y· ·=···
0060  03 ae 5d 4c d3 79 c1 cf  4b 43 68 26 20 3c b3 45   ··]L·y·· KCh& <·E
0070  7a d8 b9 48 2e 57 25 13  69 05 2d bc 87 35 1f 16   z··H.W%· i·-··5··
0080  70 34 73 86 9b 20 3e 8d  99 de 74 85 ca 3c 2e c7   p4s·· >· ··t··<.·
0090  cd dd 54 04 56 c8 fa ff  f0 7f f5 34 42 02 50 15   ··T·V··· ···4B·P·
00a0  46 60                                              F`
```

wireshark_WiFiALHR82.pcapng | Packets: 2490 · Dropped: 0 (0.0%) | Profile: Default



```
No.   Time        Source
 2332 125.638853  HonHaiPreci
 2333 126.424140  192.168.29.
 2334 126.424826  fe80::b77a:
 2335 126.498392  192.168.29.
 2336 126.498392  192.168.29.
 2337 126.498949  192.168.29.
 2338 126.638759  HonHaiPreci
 2339 128.638672  192.168.29.
 2340 128.962308  192.168.29.
 2341 129.638837  192.168.29.
 2342 130.428231  192.168.29.
 2343 130.428878  fe80::b77a:
 2344 132.138731  192.168.29.
 2345 133.097962  192.168.29.
 2346 133.514052  HonHaiPreci
 2347 133.556898  XiaomiCommu
```

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None	1

+ − ○ drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

wireshark_WiFiALHR82.pcapng | Packets: 2490 · Dropped: 0 (0.0%) | Profile: Default

5. Observations and Findings

Area	Observation	Risk Level
Wi-Fi Encryption	WPA2-PSK enabled	Low
Wi-Fi Password	Previously weak; now updated	Medium → Low
Open Ports	Telnet (port 23) open on smart plug	High
Unauthorized Devices	One unrecognized device (verified later)	Medium
Network Traffic	Mostly HTTPS; one device using HTTP	Low

6. Recommendations

- **Upgrade to WPA3** if supported by router and devices.
- **Disable Telnet** on smart plug and restrict open ports via firewall.
- **Regularly scan** for unknown devices using Wireless Network Watcher.
- **Enforce strong passwords** for both Wi-Fi and router login.
- **Schedule periodic traffic captures** using Wireshark to detect any unusual behaviour.

7. Skills Gained

- Practical understanding of home network security.
- Use of open-source tools for network and port scanning.
- Packet inspection and filter usage in Wireshark.
- Identifying and managing connected devices using MAC addresses.
- Exposure to router security configuration and settings.

8. Conclusion

This Wi-Fi security assessment served as a practical application of core cyber security concepts in a real-world home network setup. The use of GUI-based open-source tools provided an accessible yet effective method to identify and resolve common wireless network vulnerabilities. The final deliverable of this project is a secure and hardened Wi-Fi network environment, validated by a structured scan and analysis methodology.

Attachments (in GitHub Repo):

- `WiFi_Security_Assessment_Report_Mahendra.pdf`
- `nmap_scan_results.txt`
- `wireless_devices_scan.txt`
- `screenshots/` folder showing router settings and findings