


Home Wi-Fi Security Assessment Report

 Date: 30 June 2025


 Prepared by: Mohammed Aleem Hasan

 Location: Udaipur, Rajasthan

Introduction

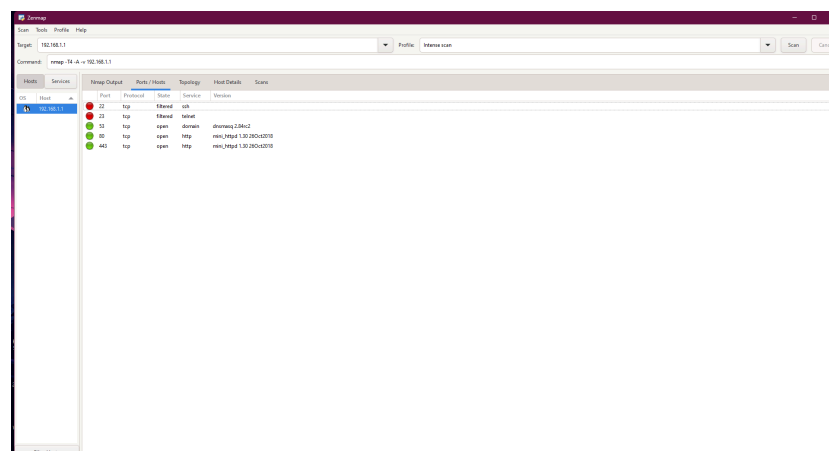
This report presents a basic security assessment of my personal home Wi-Fi network. The objective is to identify common vulnerabilities and apply simple yet effective fixes. All steps are performed manually using beginner-friendly tools,

Tools Used

 Zenmap (Nmap GUI) – for scanning open ports

 Router Admin Panel – for reviewing device info and settings

 Screenshots –



Network Details

Parameter Value

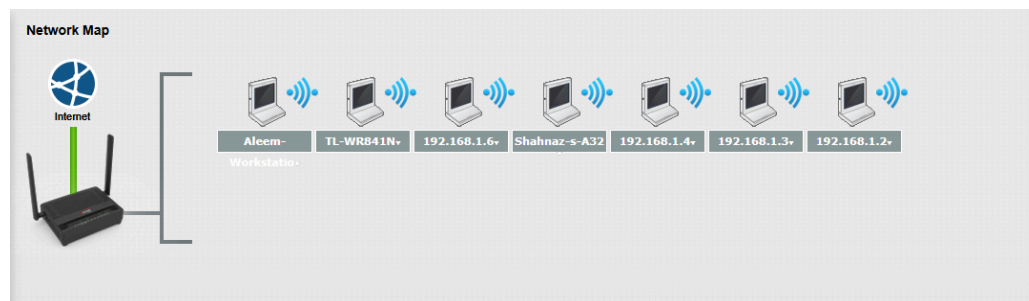
Router IP Address - 192.168.1.1 (or as per ISP)

SSID Name - Airtel_aleem (example)

Encryption Type - WPA/WPA2-Tkip-AES

WPS Status -  Disabled

Total Connected Devices - 6 (via admin panel)



Port Scan Results (via Zenmap)

Using Zenmap, a port scan was performed on the router IP to identify exposed network services.

Port Number	Service	Status	Risk Level
80	HTTP	Open	Potential risk
443	HTTPS	Open	Safe
22	FTP	Open	High Risk
23	SSH	Open	High Risk
53	TELNET	Open	Medium Risk

Router Security Audit

The following critical settings were reviewed from the router admin panel:

Security Check	Status	Risk Level	Recommendation
Default Password	Changed	✓ Safe	No action needed
WPS (Wi-Fi Setup)	✗ Disabled	✓ Safe	Already disabled
Firmware Version	Up to Date	✓ Safe	Check regularly for updates
Remote Access	✗ Disabled	✓ Safe	No action needed
Guest Network	Not Configured	● Neutral	Optional; enable with strong pass

Wireless 2.4GHz

General More AP MAC Authentication **WPS** Advanced Station Information

Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS.

General

WPS: ☐ Enable ☒ Disable (settings are invalid when disabled)

Note:
This feature is available only when WPA2-PSK, WPA-PSK/WPA2-PSK or No Security mode is configured.

Apply Undo

Wireless 2.4GHz

General **More AP** MAC Authentication WPS Advanced Station Information

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless Network Setup

Wireless Radio Button ☒ Enable Wi-Fi Radio
Wireless ☒ Enable Wireless LAN

Wireless Network Settings

Wireless Network Name (SSID):
☐ Hide SSID
BSSID: 14:33:75:75:6B:C6
Channel Selection:
Operating Channel: 1

Security Level
WPS functionality only supports WPA2-PSK security type.
Security Mode:

No Security Basic More Secure (Recommended)

Enter 8-63 characters.
Pre-Shared Key: [Show...](#)

Apply Cancel

🔑 **Wi-Fi Password Strength Audit**

Current Password: ***** (hidden)

Strength Analysis:

- ✓ 12+ characters
- ✓ Uppercase + lowercase + numbers
- ✓ No dictionary words
- > ✓ Strong Password in use

Recommendations

- ✓ WPS disabled (completed)
- ✓ Use strong and unique Wi-Fi passwords
- ✓ Change default router login credentials
- ✓ Keep router firmware up-to-date
- ✓ Monitor connected devices monthly
- ✓ Disable remote access if not needed

Conclusion

This beginner-level security audit of my home Wi-Fi network helped me understand basic vulnerabilities and apply real-world fixes. I identified exposed ports, disabled risky features like WPS, and confirmed the use of strong encryption and password practices. This process boosted my practical understanding of network security.

