Home Network Security Audit Report

Date: September 12, 2024

Assessor: Mohammad Zakaria

# 1. Introduction

This home network security audit aims to assess the overall security posture of my home network, identify vulnerabilities, and provide recommendations to enhance the security of connected devices, the Wi-Fi network, and the router. The assessment covers the main and guest Wi-Fi networks, router settings, and all connected devices.

# 2. Network Overview

## Router Information:

- Manufacturer: TP-Link

- Model Number: Archer C6 v3.30

- Firmware Version: **1.0.16** Build 20230828 rel.44667(5553)

- Security Features: WPA3 encryption, firewall enabled, SPI firewall, DoS Protection, IP & MAC Binding ( ARP binding), guest network, OpenVpn Support.

## Wi-Fi Network:

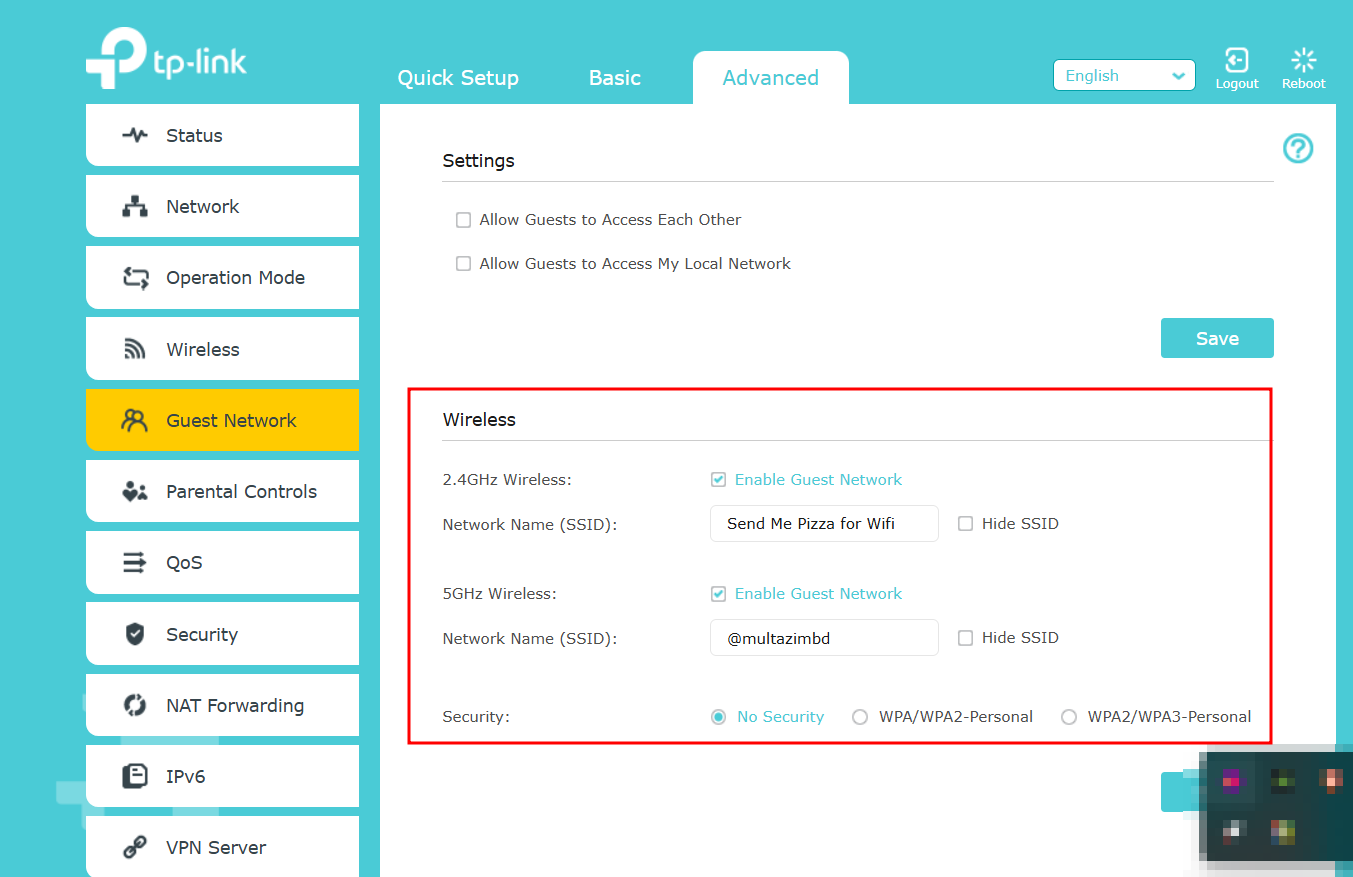
- Main Network SSID: TeslaElectroNetSIDC

- Encryption Type: WPA2-PSKA screenshot of a computer

Description automatically generated

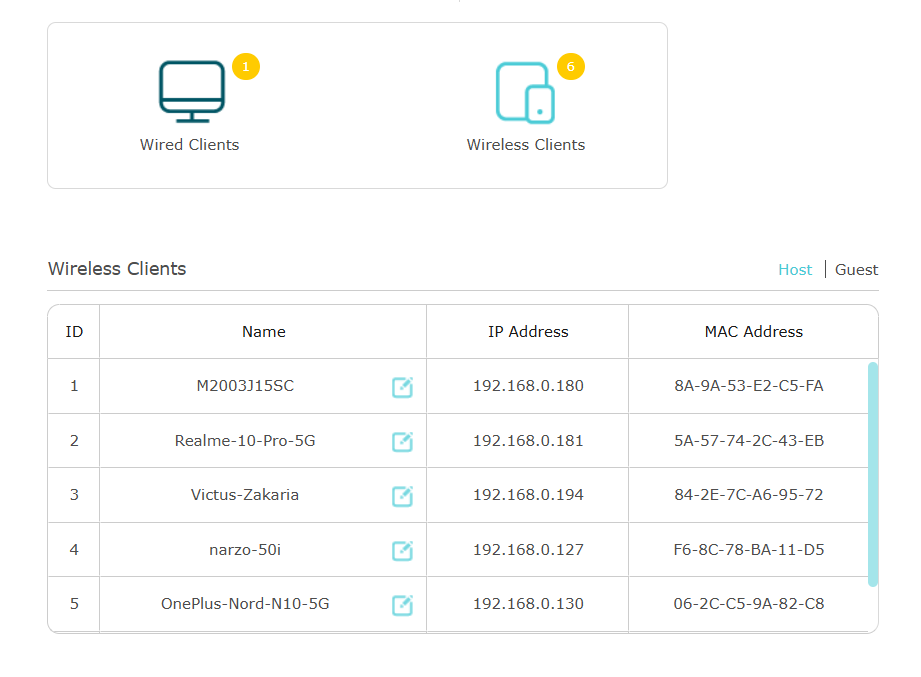
- Guest Network SSID: Send Me Pizza for Wifi (2.4GHz Wireless) and @multazimbd ( for 5GHz Wireless)

- Encryption Type: No Security

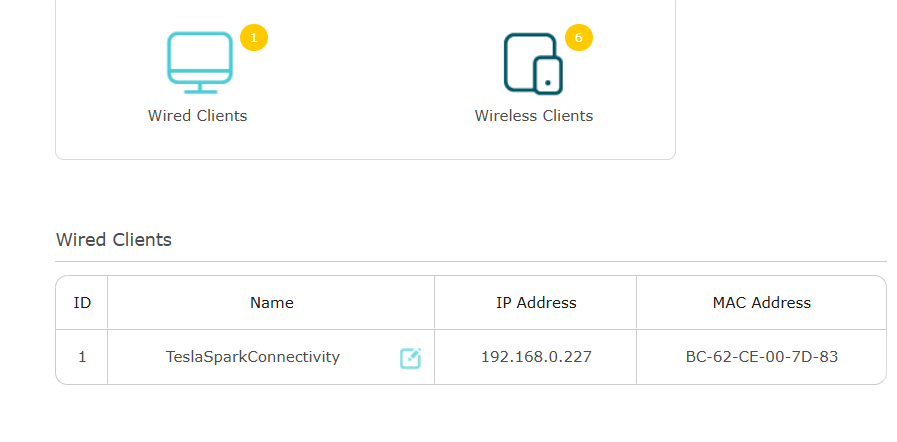


## Connected Devices: (Wireless)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Type | Device Name | IP Address | MAC Address | Security Status |
| Laptop | M2003J15SC | 192.168.0.180 | 8A-9A-53-E2-C5-FA |  |
| Mobile | Realme-10-Pro-5G | 192.168.0.181 | 5A-57-74-2C-43-EB |  |
| Laptop | Victus-Zakaria | 192.168.0.194 | 84-2E-7C-A6-95-72 |  |
| Mobile | Narzo-50i | 192.168.0.127 | F6-8C-78-BA-11-D5 |  |
| Mobile | OnePlus-Nord-N10-5G | 192.168.0.130 | 06-2C-C5-9A-82-C8 |  |
| Mobile | Redmi7-Redmi | 192.168.0.135 | B4-C4-FC-EF-49-4D |  |
| Laptop | Lenevo Sajid | 192.168.0.172 | B0-60-88-38-EF-50 |  |

  
Connected Device: (Wired)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Type | Device Name | IP Address | MAC Address | Security Status |
| Laptop | TeslaSparkConnectivity | 192.168.0.227 | BC-62-CE-00-7D-83 |  |



# 3. Security Objectives

The security objectives of this audit are:  
- To protect the network from unauthorized access.  
- To ensure that all devices are using strong encryption.  
- To separate guest and IoT devices on a secure network.  
- To maintain updated firmware and software across all devices.  
- To enable logging and monitoring on the router for potential threats.

# 4. Threats and Vulnerabilities Identified

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SL | Threat/Vulnerability | Description | Risk Level | Action Required |
|  | No Guest Network Password | The guest networks use no password | HIGH | Set a strong password |

# 5. Security Recommendations

|  |  |  |  |
| --- | --- | --- | --- |
| SL | Recommendation | Action Required | Priority |
| 1 | Enable WPA-3 | For stronger protection **Enable** WPA-3 option for the standard authentication method based on Pre-shared Key (PSK), aka passphrase | Medium |
| 2 | Secure Guest Network | Set password to Guest network | HIGH |
| 3 | Enable 2FA | Enable 2FA for any device/account that support it. | Low |

# 6. Testing and Evaluation

- Port Scan Results:

- Wi-Fi Password Strength Test: Wi-Fi password meets strong password requirements (16 characters, random).  
- Router Logs: No suspicious activities or unauthorized login attempts observed.

# 7. Conclusion

The home network security audit revealed several critical vulnerabilities including No password setting in Guest network. Addressing these vulnerabilities through firmware updates, stronger passwords method like WPA-3 and Securing guest network will significantly improve the network’s security. Implementing these changes will ensure the protection of personal data and reduce the risk of unauthorized access.

# 8. Appendix

1. Screenshots,

2. Network scan results,

3. logs

4. Additional data collected during the audit:

## Tools Used:

- Router Admin Page (Accessed via 192.168.0.1)  
- Nmap (for port scanning)  
- Wireshark (for network traffic monitoring)  
- Online Password Strength Test (for evaluating Wi-Fi password)