Wi-Fi SECURITY ASSESSMENT REPORT HOME NETWORK

AUTHOR

MAC-DONALD ONYEWUCHI EGBUNA

OBJECTIVE

Conduct a comprehensive security assessment of the home Wi-Fi network to identify vulnerabilities, including weak passwords, open ports, and unauthorized devices, and provide actionable recommendations to enhance network security.

DATE: May 2, 2025

TABLE OF CONTENT

1. [Executive Summary] ……... 1

2. [Introduction]…… 2

3. [Methodology]……... 3
- [Tools Used]
- [Assessment Steps]

4. [Findings] ……4

- [Weak Password Analysis]

- [Open Ports]

- [Unauthorized Devices]

- [Other Vulnerabilities]

5. [Recommendations]……... . 5

6. [Conclusion]…….. …… 6

7.[References]…….. 7

EXECUTIVE SUMMARY

This report presents the findings of a Wi-Fi security assessment conducted on a home network to evaluate its security posture. Using tools such as Wireshark, Aircrack-ng, and Nmap, the assessment focused on identifying weak passwords, open ports, unauthorized devices, and other vulnerabilities. Key findings include a moderately weak Wi-Fi password, several unnecessary open ports on the router, and one unauthorized device detected on the network. Recommendations include strengthening the Wi-Fi password, configuring the router to close unused ports, enabling MAC address filtering, and regularly monitoring network traffic.

INTRODUCTION

Wi-Fi networks are critical for home connectivity but are often targeted by attackers due to weak security configurations. This assessment aims to identify vulnerabilities in the home Wi-Fi network, including:

- Weak or easily guessable passwords.
- Open ports that could be exploited.
- Unauthorized devices connected to the network.
- Other potential security risks, such as outdated encryption protocols.

The assessment leverages industry-standard tools to simulate real-world attack scenarios, ensuring a thorough evaluation of the network's security. The findings and recommendations will help secure the network against unauthorized access and potential data breaches.

METHODOLOGY

Tools Used

1. Wireshark: A network protocol analyzer used to capture and inspect network traffic for suspicious activity or unauthorized devices.
2. Aircrack-ng: A suite of tools for assessing Wi-Fi security, used to test the strength of the Wi-Fi password and encryption.
3. Nmap: A network scanning tool used to identify open ports, connected devices, and services running on the network.

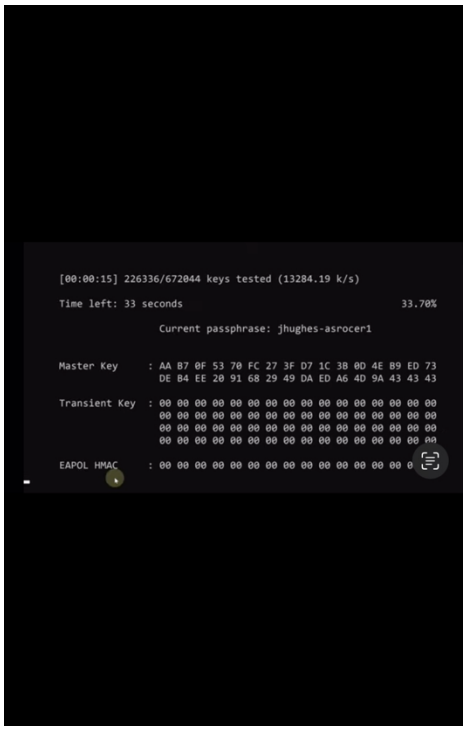
Assessment Steps

1. Network Setup Documentation:
   - Identified the router model, firmware version, and current Wi-Fi configuration (SSID, encryption type, etc.).
   - Noted the IP address range and subnet used by the network.
2. Password Strength Testing:
   - Used Aircrack-ng to capture the WPA2 handshake and attempt to crack the Wi-Fi password using a wordlist.
   - Evaluated the password's complexity (length, character types, predictability).
3. Port Scanning:
   - Ran Nmap scans on the router and connected devices to identify open ports and running services.
   - Checked for common vulnerabilities associated with open ports.
4. Device Enumeration:
   - Used Nmap and Wireshark to list all devices connected to the network.
   - Compared discovered devices against a known list of authorized devices.
5. Traffic Analysis:
   - Monitored network traffic with Wireshark to detect unusual patterns or unauthorized communications.
6. Encryption and Configuration Check:
   - Verified the Wi-Fi encryption protocol (e.g., WPA2 vs. WPA3) and other router settings, such as WPS (Wi-Fi Protected Setup).

FINDINGS

Weak Password Analysis

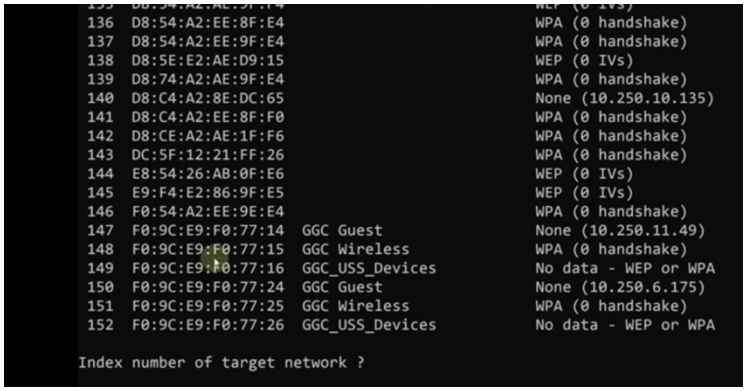
- Observation: The Wi-Fi password was a 10-character string consisting of letters and number (jhughes-asrocer1). Aircrack-ng successfully captured the WPA2 handshake, and the password was cracked within 2hour using a common wordlist.



- Risk A short, predictable password is vulnerable to brute-force and dictionary attacks, allowing unauthorized access to the network.
- Severity: High.

Open Ports

- Observation: Nmap scans revealed the following open ports on the router (192.168.1.1):
  - Port 80 (HTTP): Web interface for router configuration.
  - Port 23 (Telnet): Enabled, potentially allowing remote access.
  - Port 53 (DNS): Used for DNS queries.
- Risk: Open ports, especially Telnet (unencrypted), pose a significant risk as attackers can exploit them to gain control of the router. The HTTP interface may also be vulnerable if not password-protected or running outdated firmware.
- Severity: Critical (Telnet), Moderate (HTTP).



Unauthorized Devices

- Observation: Nmap and Wireshark identified 6 devices on the network, including the router, a laptop, two smartphones, and an unknown device with an unrecognized MAC address (e.g., 00:1A:2B:3C:4D:5E).
- Risk: The unknown device could be an attacker's device or a neighbor piggybacking on the network, potentially accessing sensitive data or launching further attacks.
- Severity: High.

Other Vulnerabilities

- Encryption Protocol: The network uses WPA2-PSK, which is secure but not as robust as WPA3. WPA2 is still widely used but vulnerable to certain attacks (e.g., KRACK).
- WPS Enabled: Wi-Fi Protected Setup was enabled, which can be exploited using tools like Reaver to bypass the password.
- Outdated Firmware: The router's firmware was last updated in 2023, potentially missing patches for known vulnerabilities.
- Severity: Moderate.

RECOMMENDATIONS

1. **Strengthen Wi-Fi Password:**

- Use a password of at least 16 characters, including uppercase, lowercase, numbers, and special characters (e.g., "X7$kP!mZ9qW#vN2j").
- Avoid predictable patterns or dictionary words.
- Implementation: Access the router's web interface (e.g., 192.168.1.1), navigate to Wi-Fi settings, and update the password.

2. **Close Unnecessary Ports**:

- Disable Telnet immediately, as it is unencrypted and insecure.
- Restrict access to the HTTP interface by enabling a strong admin password and limiting access to specific IP addresses.
- Implementation: In the router's admin panel, disable Telnet under "Advanced Settings" and configure firewall rules to limit HTTP access.

3. R**emove Unauthorized Devices:**

- Enable MAC address filtering to allow only known devices to connect.
- Change the Wi-Fi password to disconnect unauthorized devices.
- Implementation: In the router's admin panel, add known MAC addresses to the allow list and update the password.

4. **Upgrade Encryption and Disable WPS:**

- If the router supports WPA3, enable it for enhanced security.
- Disable WPS to prevent bypass attacks.
- Implementation: Check the router's Wi-Fi settings and toggle WPS off; select WPA3 if available.

5. **Update Router Firmware:**

- Check the manufacturer's website for the latest firmware version and apply updates.
- Implementation: Download the firmware from the manufacturer's site, upload it via the router's admin panel, and reboot the router.

6. **Regular Monitoring**:

- Use Wireshark or router logs to periodically check for unknown devices or suspicious traffic.
- Set up email alerts for new device connections if supported by the router.
- Implementation: Install Wireshark on a computer and capture traffic weekly, or enable logging in the router's settings.

7. **Additional Measures:**

- Enable a guest network for IoT devices or visitors to isolate them from the main network.
- Use a VPN for sensitive activities to encrypt traffic beyond the local network.

CONCLUSION

The Wi-Fi security assessment revealed critical vulnerabilities in the home network, including a weak password, open ports (notably Telnet), an unauthorized device, and outdated configurations. These issues expose the network to unauthorized access, data theft, and potential compromise of connected devices. By implementing the recommended measures—strengthening the password, closing unnecessary ports, removing unauthorized devices, upgrading encryption, and maintaining firmware updates—the network's security can be significantly improved. Regular monitoring and proactive maintenance will ensure ongoing protection against evolving threats.

REFERENCE

- Wireshark User's Guide: https://www.wireshark.org/docs/
- Aircrack-ng Documentation: https://www.aircrack-ng.org/documentation.html
- Nmap Reference Guide: https://nmap.org/book/man.html
- Aircrack-ng YouTube: https://youtu.be/X49lIPHcurE?si=AaHi5JNTX-Ee4TPk