Wireless Network Security Audit

Shashank, Sai Prasad

February 12, 2025

Introduction

Wireless networks are very common in today's connected world; however, their convenience often comes at the cost of security vulnerabilities. This project addresses the critical need to evaluate and enhance the security of Wi-Fi networks by simulating real-world attacks using Kali Linux—a robust penetration testing platform. Understanding and testing the security of wireless networks is essential for preventing unauthorized access, protecting sensitive data, and maintaining overall network integrity.

Objectives

- **Assess Wireless Vulnerabilities:** To analyze the security of Wi-Fi networks by capturing and scrutinizing network data.
- **Simulate Attacks:** To demonstrate how weak Wi-Fi security can be exploited using tools available in Kali Linux.
- **Educate on Best Practices:** To highlight the importance of strong encryption methods and secure password policies.

Scope of the Project

Inclusions:

- Setting up a wireless network testing environment using Kali Linux.
- Capturing WPA/WPA2 handshakes using a built in wireless adapter in monitor mode.
- Conducting simulated attacks to force device re-authentication.
- Analyzing captured data with tools such as Wireshark and Aircrack-ng.
- Documenting findings and providing security recommendations.

Limitations:

- Real-world exploitation on unauthorized networks is strictly prohibited.
- The focus is on WPA/WPA2 networks, excluding other security protocols.

Methodology

Setting Up the System:

- Deploy Kali Linux on a suitable platform.
- Configure a Built-in wireless adapter that supports monitor mode.

Scanning for Networks:

- Utilize `airodump-ng` to detect and list nearby Wi-Fi networks.
- Collect relevant network data such as SSID, channel, and encryption type.

Capturing Handshakes:

- Monitor and capture the WPA/WPA2 handshake during device authentication.
- Use `aireplay-ng` to deauthenticate devices, forcing a reconnection and ensuring handshake capture.

Data Analysis:

- Verify the integrity of captured handshakes using Wireshark.

Expected Outcome

- **Detailed Vulnerability Report:** A comprehensive analysis of the tested Wi-Fi networks, highlighting potential security weaknesses.
- **Demonstrated Exploitation Techniques:** A practical demonstration of how attackers can exploit weak Wi-Fi security.
- **Security Recommendations:** Actionable steps for network administrators to enhance security, including improved encryption practices and robust password policies.

Tools & Technologies Used

Operating System: Kali Linux

Built-in Wireless Adapter: Device capable of monitor mode operation

Tools:

- `airodump-ng`: For scanning and capturing Wi-Fi network data.
- `aireplay-ng`: For deauthentication attacks to capture handshakes.
- `aircrack-ng`: For testing the strength of captured WPA/WPA2 handshakes.
- `Wireshark`: For in-depth analysis of captured network packets.

Additional Resources:

- Wordlists for password cracking.

Timeline

Phase 1 – System Setup (Weeks 1-2)

- Install Kali Linux and update system packages.
- Set up a built-in wireless adapter for monitor mode.

Phase 2 – Network Scanning (Week 3)

- Use airodump-ng to scan for nearby Wi-Fi networks.
- Gather SSID, encryption type, and channel information.

Phase 3 – Capturing Handshakes (Weeks 4-5)

- Monitor network traffic and capture WPA/WPA2 handshakes.
- Use aireplay-ng to deauthenticate devices and force reconnections.

Phase 4 – Password Testing (Week 6)

- Analyze captured handshakes using Wireshark.
- Attempt password cracking using Aircrack-ng with a wordlist.

Conclusion

This project offers a hands-on approach to understanding and assessing wireless network security. By simulating controlled attacks on Wi-Fi networks using Kali Linux, it highlights the vulnerabilities inherent in weak encryption and poor password management. The insights gained will not only educate on the risks but also pave the way for implementing stronger security measures. Ultimately, this project reinforces the importance of proactive cybersecurity practices in safeguarding our increasingly wireless-dependent world.

References I

[1] Scribd, "Network Security Audit Project Report." https://www.scribd.com/document/789966331/Network-Security-Audit-Project-Report

[2] QualySec, "Network Security Audit." https://qualysec.com/network-security-audit/

[3] ITM Conferences, "Network Security Audit Research Paper." https://www.itm-conferences.org/articles/itmconf/pdf/2016/02/itmconf_ita2016_03001.pdf

NETWORK
SECURITY
PROTOCOLS