CFSS Project: Wi-Fi Security

Submitted by :- Ahatesham Bandenavaz Mopagar

CFSS Cybersecurity Analyst Intern

1. Introduction: Understanding Wi-Fi Security

- **Objective**: To analyze common Wi-Fi security standards, encryption techniques, and known vulnerabilities.
- **Goals**:
    - Explore the history of Wi-Fi encryption standards (WEP, WPA, WPA2, WPA3).
    - Identify common attacks and threats to Wi-Fi networks.
    - Implement secure practices to defend against these threats.

---

2. Research and Background

Wi-Fi Standards:

Wired Equivalent Privacy (WEP):

- One of the earliest encryption standards (introduced in 1997).
- Uses 64-bit or 128-bit encryption keys.
- Weak security due to vulnerabilities in its key generation method, making it easily crackable with modern tools.
- No longer considered secure and is deprecated.

Wi-Fi Protected Access (WPA):

- Introduced in 2003 as an improvement over WEP.
- Uses Temporal Key Integrity Protocol (TKIP) for encryption, which dynamically changes keys.
- More secure than WEP, but TKIP still has vulnerabilities and is less secure compared to modern standards.

Wi-Fi Protected Access II (WPA2):

- Released in 2004, it became the industry standard for many years.
- Uses Advanced Encryption Standard (AES), which is much more secure than TKIP.
- WPA2-PSK (Pre-Shared Key) is for home networks, while WPA2-Enterprise adds additional authentication methods for enterprise environments.

- Still widely used, though certain attacks (e.g., KRACK attack) have exposed some weaknesses.

Wi-Fi Protected Access III (WPA3):

- Introduced in 2018 to address weaknesses in WPA2.
- Improves security with Simultaneous Authentication of Equals (SAE), which provides stronger protection against brute-force attacks.
- Offers better protection for weak passwords and forward secrecy (even if a key is compromised, previous sessions remain secure).
- WPA3-Personal uses SAE for home networks, while WPA3-Enterprise offers even more robust encryption for organizations

- **Security Features**:
  - **Encryption**: Explain how WPA2 uses AES encryption and why this is better than WEP's RC4.
  - **Authentication**: WPA2 with Pre-Shared Key (PSK) versus Enterprise mode using RADIUS.
  - **Security Flaws**: Discuss known vulnerabilities like KRACK (Key Reinstallation Attack) on WPA2 and mitigations in WPA3.

---

3. Key Components of the Project

Component 1: Wi-Fi Security Vulnerabilities

- **Wi-Fi Attacks**:
  - **WEP Cracking**: Demonstrate how WEP can be cracked using tools like aircrack-ng. Show how the weak initialization vector (IV) can be exploited.
  - **WPA/WPA2 PSK Cracking**: Demonstrate brute-forcing WPA2 PSK using tools like **hashcat**. Capture a WPA2 handshake using **airmon-ng** and **airodump-ng**, and perform dictionary attacks.
  - **KRACK Attack on WPA2**: Understand and simulate a simplified version of the KRACK attack, which exploits vulnerabilities in the WPA2 handshake.
- **Rogue Access Points (Evil Twin Attack)**:
  - Simulate a rogue access point using tools like airbase-ng to show how attackers can steal credentials by mimicking legitimate Wi-Fi networks.
- **Deauthentication Attacks**:

- Use aireplay-ng to carry out deauthentication attacks, forcing legitimate users to disconnect from a network.

Component 2: Defending Against Wi-Fi Attacks

- **Securing Wi-Fi Networks**:
  - **Encryption**: Ensure the network uses WPA3 if available, or WPA2 with AES encryption. Discuss why TKIP is weaker.
  - **Strong Passwords**: Use long, complex passphrases to defend against brute-force attacks.
  - **Hidden SSID and MAC Filtering**: Show why hidden SSIDs and MAC filtering are weak defenses and easily bypassed.
- **Tools for Defense**:
  - **Wireshark**: Demonstrate how to monitor wireless traffic and detect malicious activities such as deauthentication attacks.
  - **Hostapd-WPE**: Show how to test your own network against Enterprise-level attacks using Hostapd-WPE, which allows for testing attacks on WPA2 Enterprise networks.
- **Rogue AP Detection**:
  - Use tools like Wifiphisher to simulate and defend against rogue access points.

Component 3: Mitigation Techniques

- **Network Segmentation**: Explain the concept of separating guest Wi-Fi from critical infrastructure to limit the impact of a compromised network.
- **VPN over Wi-Fi**: Recommend using a VPN to encrypt traffic even if the Wi-Fi connection is compromised.
- **Regular Firmware Updates**: Ensure routers and access points are always updated to patch known vulnerabilities.
- **802.1X Authentication**: Explore advanced security mechanisms like 802.1X, which uses RADIUS authentication servers for Enterprise Wi-Fi networks.

---

4. Tools for the Project

- **Wi-Fi Hacking Tools**:
  - **Aircrack-ng**: Suite of tools for Wi-Fi network auditing, including WEP/WPA cracking.
  - **hashcat**: A powerful password-cracking tool used for WPA/WPA2 pre-shared key cracking.
  - **Wireshark**: Network protocol analyzer for monitoring and analyzing Wi-Fi traffic.

- **Wifiphisher**: Tool for performing rogue AP attacks and phishing.
- **Hostapd-WPE**: For testing and breaking WPA Enterprise networks.
- **Kismet**: A network detector and packet sniffer that helps discover rogue devices.

Wi-Fi Hacking Open Source Tools in 2024

Aircrack-ng

Aircrack-ng is one of the most well-known Wi-Fi security audit tools. It focuses on monitoring, attacking, testing, and cracking wireless networks. It's commonly used for cracking WEP and WPA/WPA2-PSK keys.

Key Features:

• - Packet capturing

• - WEP and WPA/WPA2 cracking

• - Network monitoring

GitHub: https://github.com/aircrack-ng/aircrack-ng

Kismet

Kismet is a powerful network detector, sniffer, and intrusion detection system for Wi-Fi. It works with Wi-Fi, Bluetooth, and other wireless standards.

Key Features:

• - Captures and analyzes traffic

• - Identifies hidden networks

• - Supports Wi-Fi, Bluetooth, and SDR capture

GitHub: https://github.com/kismetwireless/kismet

Wifite

Wifite is a Python-based tool that automates the process of cracking WEP, WPA, and WPS. It is designed to streamline the attack process for wireless networks.

Key Features:

• - Automated WEP and WPA handshake capturing

• - WPA/WPA2 password cracking via dictionary attack

• - Automated targeting of multiple access points

GitHub: https://github.com/derv82/wifite2

Hashcat

Hashcat is a popular password-cracking tool that can crack hashed passwords using brute force or dictionary attacks. It's especially powerful when combined with captured Wi-Fi handshakes from tools like Aircrack-ng.

Key Features:

• - Supports a wide variety of hash algorithms

• - GPU-accelerated password cracking

GitHub: https://github.com/hashcat/hashcat

Bettercap

Bettercap is a complete, modular framework for performing a wide range of network attacks, including Wi-Fi monitoring, man-in-the-middle attacks, and password sniffing.

Key Features:

• - Real-time network analysis

• - ARP poisoning and DNS spoofing

• - Wi-Fi reconnaissance and monitoring

GitHub: https://github.com/bettercap/bettercap

Reaver

Reaver is a tool primarily used for brute-forcing WPS (Wi-Fi Protected Setup) PINs to recover WPA/WPA2 passphrases. It's particularly effective against routers that have WPS enabled.

Key Features:

• - WPS PIN brute-forcing

• - WPS vulnerability exploitation

GitHub: https://github.com/t6x/reaver-wps-fork-t6x Fern

Wi-Fi Cracker Fern

Wi-Fi Cracker is a GUI-based tool for cracking and recovering WEP/WPA/WPA2 keys. It also supports attacks such as man-in-the-middle, session hijacking, and ARP poisoning.

Key Features:

• - GUI-based interface

• - Supports WEP, WPA, WPA2, and WPS

• - Can conduct MITM and phishing attacks

GitHub: https://github.com/savio-code/fern-wifi-cracker

Fluxion

Fluxion is a unique social engineering tool that works by launching a man-in-the-middle attack to capture WPA/WPA2 passwords by tricking users into connecting to a fake access point.

Key Features:

• - Evil twin attack to capture handshakes

• - Automated setup of fake access points

• - Real-time password capture via social engineering

GitHub: https://github.com/FluxionNetwork/fluxion

Wireshark

Wireshark is a powerful packet analyzer used for network troubleshooting, analysis, and security audits. It is widely used for capturing and analyzing network traffic.

Key Features:

• - Detailed packet capture and analysis

• - Cross-platform support

• - Wide range of protocol dissectors

GitHub: https://github.com/wireshark/wireshark

Pyrit

Pyrit focuses on WPA/WPA2-PSK key recovery, using massive amounts of computational power for brute-force attacks. It can leverage multi-core processors and GPUs to accelerate password cracking.

Key Features:

- - Optimized for multi-core processors
- - GPU acceleration support
- - Powerful dictionary-based password attacks

GitHub: https://github.com/JPaulMora/Pyrit

5. Ethical Considerations

- Always obtain permission before testing on any Wi-Fi network. Ensure you understand the legal implications of performing Wi-Fi penetration testing in your region.
- Use a controlled lab environment to simulate attacks and defenses. Consider setting up a home Wi-Fi network with a test router for this project.
