Day 21

WiFi Hacking - Day 1 Report

Introduction to WiFi Hacking

WiFi hacking refers to the unauthorized access or exploitation of wireless networks. Given the widespread adoption of wireless technology in homes, businesses, and public spaces, WiFi hacking has become a significant security concern. Understanding the various methods and techniques used by hackers is essential for developing effective countermeasures.

Basics of WiFi Technology

1. **Wireless Standards**: WiFi operates based on several standards defined by the IEEE (Institute of Electrical and Electronics Engineers), most commonly the 802.11 family. The main standards include:
    - **802.11b**: Operates at 2.4 GHz, provides up to 11 Mbps.
    - **802.11g**: Also at 2.4 GHz, but up to 54 Mbps.
    - **802.11n**: Operates at 2.4 GHz and 5 GHz, up to 600 Mbps.
    - **802.11ac**: Operates at 5 GHz, up to 3.46 Gbps.
2. **Encryption Protocols**: WiFi security is primarily based on encryption protocols that protect data transmitted over the network.
    - **WEP (Wired Equivalent Privacy)**: An older protocol, now considered insecure due to several vulnerabilities.
    - **WPA (WiFi Protected Access)**: An improvement over WEP, but WPA1 has known weaknesses.
    - **WPA2**: The current standard, using AES encryption, is much more secure than WEP and WPA.
    - **WPA3**: The latest standard, providing enhanced security features.

Common WiFi Hacking Techniques

1. **Passive Attacks**:
    - **Eavesdropping**: Capturing and analyzing data packets transmitted over the network without altering them. Tools like Wireshark can be used for this purpose.
    - **Network Scanning**: Identifying available wireless networks and their characteristics using tools like Kismet.
2. **Active Attacks**:
    - **Deauthentication Attack**: Forcing devices to disconnect from a network by sending deauth packets, allowing an attacker to capture the handshake when the device reconnects.

   - **Man-in-the-Middle (MITM) Attack**: Intercepting and potentially altering communication between two devices on a network. Tools like Ettercap can facilitate MITM attacks.

3. **Brute Force Attacks**:
   - **Password Cracking**: Using tools like Aircrack-ng or Hashcat to guess the network password through brute force or dictionary attacks.

Tools Used in WiFi Hacking

1. **Aircrack-ng Suite**: A comprehensive set of tools for auditing wireless networks.
   - **Airmon-ng**: Enables monitor mode on wireless interfaces.
   - **Airodump-ng**: Captures raw 802.11 frames.
   - **Aircrack-ng**: Cracks WEP and WPA-PSK keys.
2. **Wireshark**: A network protocol analyzer that can capture and display packets of data being transmitted over a network.
3. **Kismet**: A wireless network detector, sniffer, and intrusion detection system.
4. **Reaver**: A tool for exploiting the WPS (WiFi Protected Setup) vulnerability to recover WPA/WPA2 passphrases.
5. **Hashcat**: An advanced password recovery tool that can be used to crack WPA/WPA2 handshakes.

Real-World Examples

1. **Public WiFi Attacks**: Hackers often target public WiFi networks because they are usually less secure. For example, a hacker can set up a rogue access point to intercept data from users connecting to what they think is a legitimate network.
2. **Home Network Attacks**: Attackers might target home networks, especially those using outdated encryption like WEP or weak passwords, to gain unauthorized access.
3. **Corporate Network Breaches**: Businesses with insufficient WiFi security measures can fall victim to attacks that compromise sensitive data or disrupt operations.