Day 22

WiFi Hacking - Day 2 Report

Advanced WiFi Hacking Techniques

While Day 1 covered the basics of WiFi hacking, today's focus will be on more advanced techniques that hackers use to breach wireless networks.

Evil Twin Attack

1. **Concept**: An Evil Twin attack involves setting up a rogue access point that mimics a legitimate network. Unsuspecting users connect to the rogue AP, thinking it's a trusted network.
2. **Execution**:
    - **Step 1**: The attacker creates a fake access point with the same SSID (Service Set Identifier) as the target network.
    - **Step 2**: The attacker can use deauthentication attacks to disconnect users from the legitimate network, pushing them to connect to the rogue AP.
    - **Step 3**: Once users are connected to the rogue AP, the attacker can capture all traffic, including sensitive information like login credentials.
3. **Tools**:
    - **Airbase-ng**: Part of the Aircrack-ng suite, used to create rogue access points.
    - **WiFi Pineapple**: A hardware device designed for penetration testing, particularly effective for executing Evil Twin attacks.

WPS Pin Attacks

1. **Overview**: WiFi Protected Setup (WPS) is designed to simplify the process of connecting devices to a wireless network. However, it has vulnerabilities that can be exploited to recover the network’s WPA/WPA2 passphrase.
2. **Execution**:
    - **Step 1**: The attacker uses a tool like Reaver to repeatedly attempt to guess the WPS PIN.
    - **Step 2**: Once the correct PIN is found, the network’s WPA/WPA2 passphrase can be recovered.
3. **Mitigation**: Disabling WPS on the router can prevent this type of attack.

Packet Injection

1. **Concept**: Packet injection involves sending forged packets into the network. This technique can be used for various attacks, including injecting malicious data, disrupting communication, or forcing re-authentication.
2. **Execution**:
    - **Step 1**: The attacker captures packets on the network using a tool like Airodump-ng.

- **Step 2**: Using Aireplay-ng, the attacker injects crafted packets into the network.

3. **Applications**:
    - **ARP Spoofing**: Injecting ARP packets to associate the attacker's MAC address with the IP address of a legitimate device, enabling MITM attacks.
    - **Deauthentication**: Forcing devices to reconnect to the network, capturing the handshake for WPA/WPA2 cracking.

Bluetooth and IoT Exploitation

1. **Bluetooth Attacks**:
    - **Bluesnarfing**: Unauthorized access to information from a Bluetooth-enabled device.
    - **Bluejacking**: Sending unsolicited messages to Bluetooth-enabled devices.
2. **IoT Vulnerabilities**: Many Internet of Things (IoT) devices connect to WiFi networks and are often poorly secured, making them attractive targets for attackers. Common issues include weak default passwords, lack of updates, and insecure communication protocols.

Countermeasures for Advanced Attacks

1. **Network Segmentation**: Isolate sensitive devices and networks to limit the potential impact of a breach. For example, separate guest WiFi networks from internal networks.
2. **Regular Firmware Updates**: Ensure all wireless routers, access points, and connected devices have the latest firmware updates to patch known vulnerabilities.
3. **Enhanced Authentication**: Use multifactor authentication (MFA) and strong, unique passwords for all network devices and services.
4. **Monitoring and Intrusion Detection**: Implement systems to monitor network traffic for unusual activity and potential intrusions. Tools like Snort or Suricata can help detect and respond to attacks.

Real-World Examples of Advanced Attacks

1. **KRACK Attack (2017)**: The Key Reinstallation Attack exploited vulnerabilities in the WPA2 protocol, allowing attackers to decrypt and potentially manipulate data transmitted over WiFi networks. This attack highlighted the need for robust protocol design and timely updates to mitigate vulnerabilities.
2. **Mirai Botnet (2016)**: The Mirai botnet exploited weak security in IoT devices, including those connected to WiFi networks, to launch massive distributed denial-of-service (DDoS) attacks. This incident underscored the importance of securing all network-connected devices, not just traditional computers and smartphones.
3. **Dragonblood Vulnerabilities (2019)**: These vulnerabilities affected WPA3, the latest WiFi security protocol, allowing attackers to perform downgrading and side-channel attacks. This example demonstrates that even the newest security technologies can have flaws that need to be addressed.