Wi-Fi Security

Index

Introduction

Wi-Fi security and penetration testing focus on assessing and fortifying the security of wireless networks. This document outlines key concepts, including Wi-Fi security fundamentals, essential tools for air cracking, methods for attacking various Wi-Fi security protocols, rogue access points, and captive portals. Additionally, a step-by-step lab guide is provided for practical learning.

Wi-Fi Security

Wi-Fi security aims to protect wireless networks from unauthorized access and data breaches. The primary security protocols used in Wi-Fi networks are WEP, WPA, and WPA2.

- **WEP (Wired Equivalent Privacy)**: An outdated and vulnerable protocol using RC4 encryption.
- **WPA (Wi-Fi Protected Access)**: An improvement over WEP, using TKIP (Temporal Key Integrity Protocol).
- **WPA2 (Wi-Fi Protected Access II)**: The most widely used protocol, employing AES (Advanced Encryption Standard) for stronger security.

Air Cracking Essentials

Air cracking involves intercepting and analyzing wireless traffic to identify and exploit vulnerabilities. Essential tools include:

- **Aircrack-ng**: A suite of tools for assessing Wi-Fi network security.
    - **Airodump-ng**: Captures raw 802.11 frames.
    - **Aireplay-ng**: Injects frames to generate traffic.
    - **Aircrack-ng**: Performs the actual cracking of WEP and WPA-PSK keys.

Attacking Wi-Fi Security Protocols

WEP

1. **Capture Packets**:
    - Use airodump-ng to capture packets from the target network.

airodump-ng --bssid [BSSID] --channel [channel] -w [filename] [interface]

2. **Generate Traffic**:
    - Use aireplay-ng to generate traffic and capture IVs (Initialization Vectors).

aireplay-ng --arpreplay -b [BSSID] -h [MAC] [interface]

3. **Crack WEP Key**:
    - Use aircrack-ng to crack the captured IVs.

aircrack-ng -b [BSSID] [filename].cap

WPA/WPA2

1. **Capture Handshake**:
    - Use airodump-ng to capture the 4-way handshake.

airodump-ng --bssid [BSSID] --channel [channel] -w [filename] [interface]

2. **Deauthenticate Clients**:
    - Use aireplay-ng to deauthenticate clients and capture the handshake.

aireplay-ng --deauth 10 -a [BSSID] -c [client MAC] [interface]

3. **Crack WPA Key**:
    - Use aircrack-ng with a wordlist to crack the WPA/WPA2 passphrase.

aircrack-ng -w [wordlist] -b [BSSID] [filename].cap

Rogue Access Points

Rogue access points (APs) are unauthorized APs installed on a network, often used to intercept and manipulate network traffic.

- **Scenario**: An attacker sets up a rogue AP with the same SSID as a legitimate network to trick users into connecting.
- **Detection**: Use tools like airmon-ng and airodump-ng to identify suspicious APs.
- **Mitigation**: Regularly scan for and remove unauthorized APs.

Attacking Captive Portals

Captive portals are web pages that users must interact with before accessing a network, commonly found in public Wi-Fi hotspots.

- **Scenario**: Bypassing a captive portal to gain unauthorized access.
- **Techniques**:
    - **MAC Spoofing**: Change your device's MAC address to one that has already authenticated.

ifconfig [interface] hw ether [MAC address]

- **DNS Manipulation**: Use tools like dnsmasq to redirect DNS queries.
- **Exploit Vulnerabilities**: Look for weaknesses in the captive portal implementation.

Lab Guide

Prerequisites

- Basic understanding of wireless networking and security concepts.
- Installed tools: Aircrack-ng suite, a compatible wireless network adapter.

Step 1: Setting Up the Lab Environment

1. **Install Aircrack-ng Suite**:
    - **Linux**:

sudo apt-get install aircrack-ng

2. **Prepare a Test Network**:
    - Set up a Wi-Fi network with WEP/WPA/WPA2 security using a spare router.

Step 2: Information Gathering

1. **Enable Monitor Mode**:
    - Use airmon-ng to enable monitor mode on your wireless adapter.

airmon-ng start [interface]

2. **Capture Network Traffic**:
    - Use airodump-ng to capture packets.

airodump-ng [interface]

Step 3: Attacking WEP

1. **Capture Packets**:
    - Target the WEP network and capture packets.

airodump-ng --bssid [BSSID] --channel [channel] -w wep_capture [interface]

2. **Generate Traffic**:
    - Use aireplay-ng to generate ARP requests.

aireplay-ng --arpreplay -b [BSSID] -h [MAC] [interface]

3. **Crack WEP Key**:
    - Crack the captured IVs using aircrack-ng.

aircrack-ng -b [BSSID] wep_capture.cap

Step 4: Attacking WPA/WPA2

1. **Capture Handshake**:
    - Use airodump-ng to capture the WPA handshake.

airodump-ng --bssid [BSSID] --channel [channel] -w wpa_capture [interface]

2. **Deauthenticate Clients**:
    - Use aireplay-ng to deauthenticate a client.

aireplay-ng --deauth 10 -a [BSSID] -c [client MAC] [interface]

3. **Crack WPA Key**:
    - Crack the WPA handshake using aircrack-ng with a wordlist.

aircrack-ng -w [wordlist] -b [BSSID] wpa_capture.cap

Step 5: Setting Up a Rogue Access Point

1. **Configure Rogue AP**:
    - Use tools like hostapd to configure a rogue AP.

hostapd rogue_ap.conf

2. **Monitor for Connections**:
    - Use airodump-ng to monitor clients connecting to the rogue AP.

Step 6: Attacking Captive Portals

1. **MAC Spoofing**:
    - Change your MAC address to bypass the portal.

ifconfig [interface] hw ether [MAC address]

2. **DNS Manipulation**:
    - Set up a DNS server to redirect captive portal requests.
3. **Exploiting Vulnerabilities**:
    - Look for and exploit weaknesses in the portal's implementation.

Conclusion

Wi-Fi security and penetration testing are critical for identifying and mitigating vulnerabilities in wireless networks. By following the outlined steps and using the described tools, you can effectively assess and enhance the security of Wi-Fi networks. Regular testing and vigilance are essential to protect against evolving wireless threats.