MODULE 16 Hacking Wireless Networks
LAB REPORT

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab 01: Perform Wireless Traffic Analysis

Task 1: Wi-Fi Packet Analysis using Wireshark

Wireshark is a powerful network protocol analyzer that allows for the inspection and analysis of network traffic. In this task, we aimed to utilize Wireshark to conduct a packet analysis of Wi-Fi traffic. While capturing live Wi-Fi traffic requires a wireless adapter, we utilized a sample capture file (WEPcrack-01.cap) to demonstrate Wireshark's capabilities in analyzing Wi-Fi packets.

Steps:

1. **Accessing Wireshark:**
    - Opened the Windows 11 virtual machine.
    - Logged in using the provided credentials.
    - Navigated to the Desktop and launched Wireshark by searching for it in the search bar.
2. **Opening Capture File:**
    - In Wireshark, clicked on the "File" menu and selected "Open."
    - Navigated to the directory containing the sample capture file (WEPcrack-01.cap).
    - Selected the file and opened it in Wireshark for analysis.
3. **Analyzing Captured Packets:**
    - Examined the Wireshark window to view the details of the captured packets.
    - Identified wireless packets indicated by the 802.11 protocol.
    - Utilized Wireshark's filtering capabilities to narrow down packet searches and identify packets containing sensitive information.

4. **Conclusion and Documenting Information:**
    - Concluded the demonstration of Wi-Fi packet analysis using Wireshark.
    - Closed all open windows and documented the acquired information, including packet capture details, protocols used, and any identified patterns or anomalies.

Key Learnings: Through this task, several key learnings were obtained:

- Understanding of Wireshark as a network protocol analyzer capable of analyzing Wi-Fi traffic.
- Familiarity with capturing and examining wireless packets using Wireshark.
- Awareness of the importance of packet filtering for identifying specific types of packets, such as those containing sensitive information.
- Insight into the potential applications of Wireshark in network security, including detecting and mitigating potential threats such as session hijacking.

Lab 02: Perform Wireless Attacks

Task 1: Crack a WEP network using Aircrack-ng

Aircrack-ng is a powerful network software suite designed for 802.11 wireless networks. It includes various tools for network detection, packet sniffing, and encryption cracking. In this task, we utilized Aircrack-ng to crack the WEP encryption of a network, demonstrating its capability as a security testing tool.

Steps:

1. **Accessing Parrot Security Machine:**
    - Accessed the Parrot Security virtual machine provided for the task.
    - Logged in as the attacker user using the default credentials.

2. **Preparing Capture Files and Wordlist:**
    - Navigated to the Desktop and located the required folders: Sample Captures and Wordlist.
    - Copied both folders to the Desktop for easy access.
3. **Opening Terminal Window:**
    - Clicked on the MATE Terminal icon on the Desktop to open a Terminal window.
4. **Running Aircrack-ng as Root:**
    - In the Terminal window, switched to the root user by typing "sudo su" and entering the password "toor".
    - Executed the Aircrack-ng command with the appropriate syntax to crack the WEP key of the provided capture file (WEPcrack-01.cap).
5. **Cracking WEP Key:**
    - Aircrack-ng initiated the process to crack the WEP key of the network, displaying the progress in the Terminal window.
    - Upon successful cracking, the WEP key of the network (CEHLabs) was revealed, demonstrating the vulnerability of WEP encryption.
6. **Implications and Potential Attacks:**
    - Acknowledged the real-life implications of the cracked WEP key, allowing attackers to gain unauthorized access to the network.
    - Recognized potential follow-up attacks, such as scanning for open devices, vulnerability analysis, and exploitation of discovered vulnerabilities.
7. **Conclusion and Documentation:**
    - Concluded the demonstration of WEP network cracking using Aircrack-ng.
    - Closed all open windows and documented the acquired information, including the cracked WEP key and potential attack scenarios.

Key Learnings: Through this task, several key learnings were obtained:

- Understanding of Aircrack-ng as a comprehensive suite for wireless network security testing.
- Hands-on experience in utilizing Aircrack-ng to crack WEP encryption, highlighting the vulnerabilities associated with outdated security protocols.
- Awareness of the implications of network encryption cracking, including unauthorized access and subsequent malicious activities.
- Insight into the importance of robust encryption protocols and security measures to mitigate network vulnerabilities and attacks.

Task 2: Crack a WPA2 Network using Aircrack-ng

WPA2, considered a significant improvement over WEP and WPA, employs strong security measures for wireless networks. However, it is not immune to vulnerabilities, and tools like Aircrack-ng can be utilized to crack WPA2 encryption. This task demonstrates the process of cracking a WPA2 network using Aircrack-ng and highlights the importance of strong passphrase selection.

Steps:

1. **Preparation:**
    - Configured the access point router (CEHLabs) to operate in WPA2-PSK (Pre-Shared Key) encryption mode with the password "password1".
2. **Accessing Terminal:**
    - Clicked on the MATE Terminal icon on the Desktop to open a Terminal window.
3. **Switching to Root User:**
    - Entered "sudo su" in the Terminal window to switch to the root user, providing the password "toor" when prompted.
4. **Executing Aircrack-ng Command:**
    - Typed the Aircrack-ng command with appropriate parameters in the Terminal window to initiate the WPA2 network cracking process.

- Included the BSSID of the target router, the path to the wordlist file, and the path to the sample capture file (WPA2crack-01.cap).
- The "-a2" parameter specifies the WPA technique.
- Upon execution, Aircrack-ng captured the WPA handshake packet and commenced the cracking process.

5. **Cracking Process and Result:**
    - Aircrack-ng displayed the progress of the cracking process in the Terminal window.
    - Upon successfully cracking the WPA2 passphrase, the result was shown with the message "KEY FOUND!" followed by the plaintext password.
    - Note: The complexity of the password may influence the duration of the cracking process.
6. **Alternative Tools:**
    - Mentioned alternative tools such as Elcomsoft Wireless Security Auditor, Portable Penetrator, WepCrackGui, Pyrit, and WepAttack for cracking WEP/WPA/WPA2 encryption.
7. **Conclusion and Documentation:**
    - Concluded the demonstration of WPA2 network cracking using Aircrack-ng.
    - Closed all open windows and documented the acquired information, including the cracked WPA2 passphrase and the alternative tools mentioned for encryption cracking.

Key Learnings: Through this task, several key learnings were obtained:

- Understanding of the vulnerabilities associated with WPA2 encryption despite its stronger security compared to WEP and WPA.
- Hands-on experience in utilizing Aircrack-ng to crack WPA2 encryption, emphasizing the importance of strong passphrase selection.
- Awareness of the time-consuming nature of password cracking and the influence of passphrase complexity on cracking duration.

- Knowledge of alternative tools available for encryption cracking, providing flexibility in security testing methodologies.