DEPI Incident Response Analyst Final Project Report

Done By:

Ahmed Ossama

Mohamed Moktar

Mohamed Shawqy

Alaa Abdelgawad

Islam Hegazy

Project Report: Cracking an Access Point Using Aircrack-ng, Airmon-ng and Network Capture On pcap via Wireshark

1. Introduction

This project demonstrates the use of penetration testing tools such as Airmon-ng and Wireshark to intercept and crack the security of a Wi-Fi access point. The objective is to capture the WPA handshake that occurs when a client reconnects to the access point after being forcibly disconnected. This captured handshake can then be used to attempt password cracking using wordlists. This process, though educational, is intended for understanding vulnerabilities in Wi-Fi security and enhancing security measures.

2. Prerequisites

Before starting this project, the following are required:

- A Wi-Fi network adapter that supports monitor mode.

- A laptop or computer running Kali Linux (either natively or through a virtual machine such as VirtualBox or VMware).
- A wordlist for password cracking, such as rockyou.txt.

Basic understanding of network concepts and WPA/WPA2 encryption.

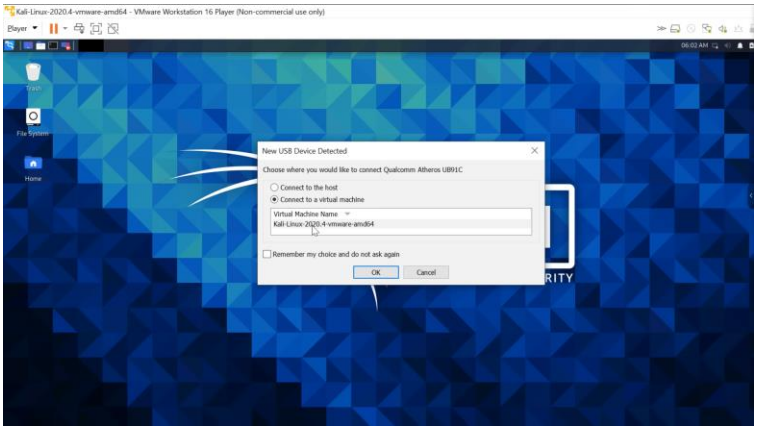
3. Setup and Environment

The project utilizes Kali Linux as the operating system to run the necessary commands for network interface control, packet monitoring, and analysis. A Wi-Fi network adapter capable of switching into monitor mode is essential to capture traffic from nearby wireless networks.

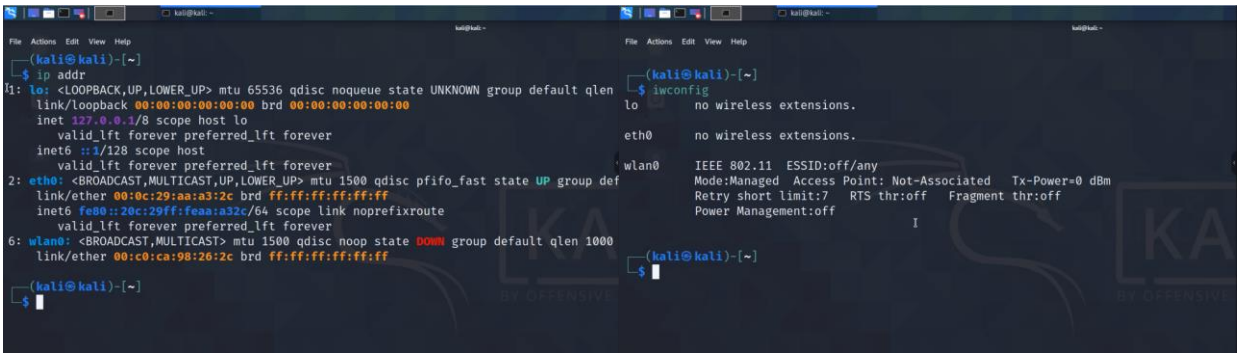
Steps to set up the environment:

Hardware Connection: Plug the Wi-Fi adapter into the laptop.

Virtual Machine Setup: Kali Linux should be running as a virtual machine. Ensure that the Wi-Fi adapter is properly recognized by the virtual machine.



Verifying Interfaces: Use the command ip addr **or** iwconfig to check the available network interfaces. The Wi-Fi adapter should appear here, usually as wlan0.



4. Switching to Monitor Mode

Wi-Fi adapters operate in "managed mode" by default, allowing them to connect to networks. However, for monitoring and capturing traffic, they need to be switched to "monitor mode."

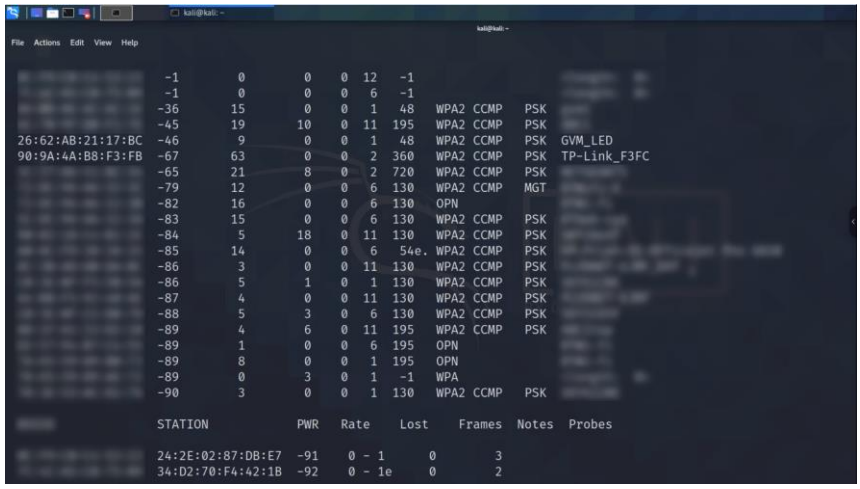
Kill Conflicting Processes: Run sudo airmon-ng check kill to stop processes that might interfere with capturing packets.

Enable Monitor Mode: Execute sudo airmon-ng start wlan0 to put the adapter into monitor mode. Verify this using the command sudo airmon-ng. If successful, the adapter will now be listed as wlan0mon.

5. Scanning for Access Points

With the Wi-Fi adapter in monitor mode, we can now scan for nearby Wi-Fi access points:

Use the command sudo airodump-ng wlan0mon to scan and list available wireless networks. The output will display the MAC addresses (BSSID), channels, encryption types, and other details of each access point.

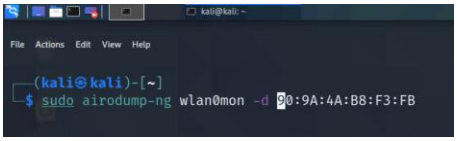


Choose an access point of interest and note its MAC address and channel.

6. Targeting a Specific Access Point

To filter and focus on one access point:

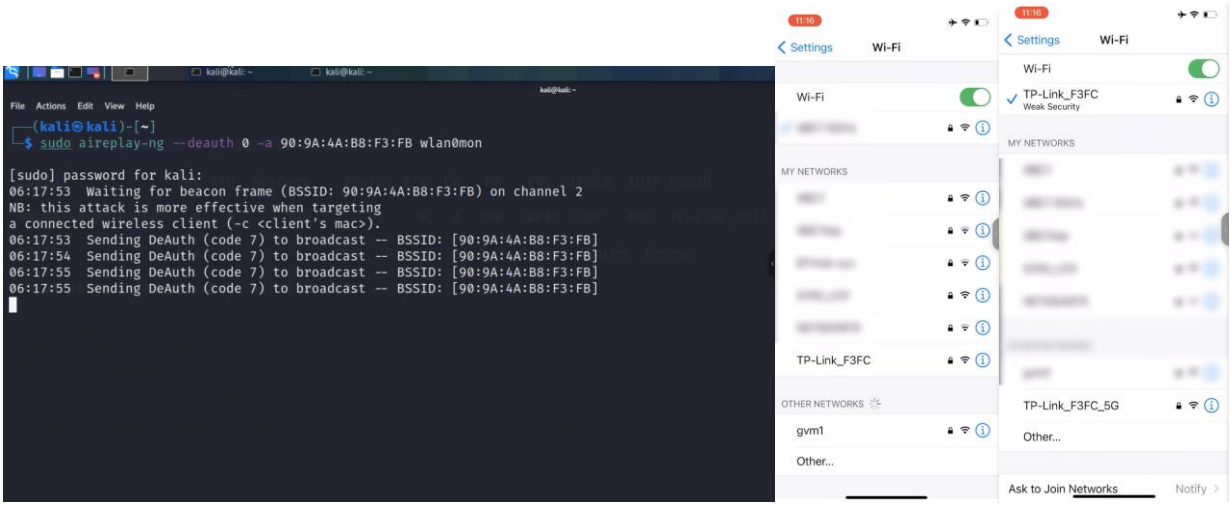
Run the command sudo airodump-ng -d <MAC Address> wlan0mon to display only traffic from the target access point.



7. Capturing the WPA Handshake

Start Packet Capture: To capture packets from the target access point, execute sudo airodump-ng -w <file_name> -c <channel> --bssid <MAC Address> wlan0mon. The -w flag specifies the output file where the captured data will be saved, and the -c flag specifies the channel of the access point.

Deauthentication Attack: Open a new terminal and run sudo aireplay-ng --deauth 0 -a <MAC Address> wlan0mon to deauthenticate clients from the target network. This forces the clients to reconnect, during which their authentication details (the WPA handshake) will be transmitted and captured.

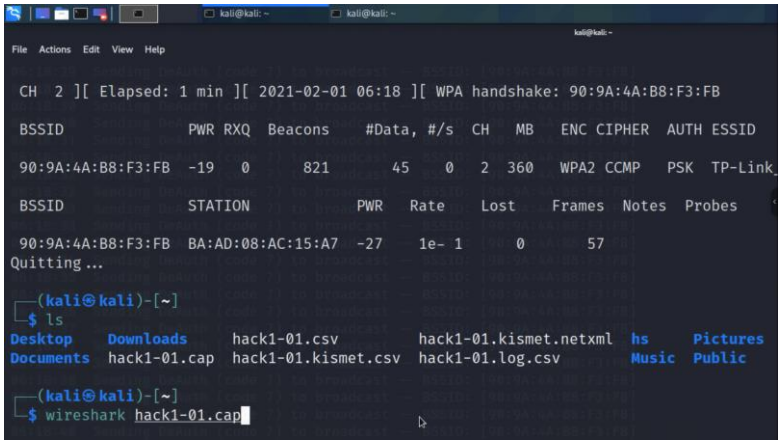


Monitoring Handshake Capture: After deauthentication, check the captured file for the WPA handshake. The captured file should appear in the directory as <file_name>-01.cap.

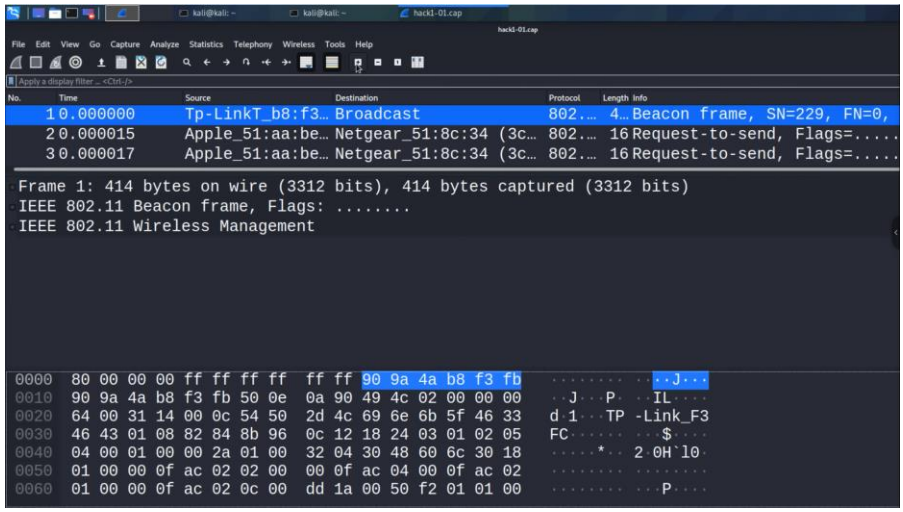
8. Analyzing the Capture with Wireshark

Wireshark is used to visually inspect the captured handshake and ensure that all necessary information is available:

Run wireshark <file_name>-01.cap to open the capture file.

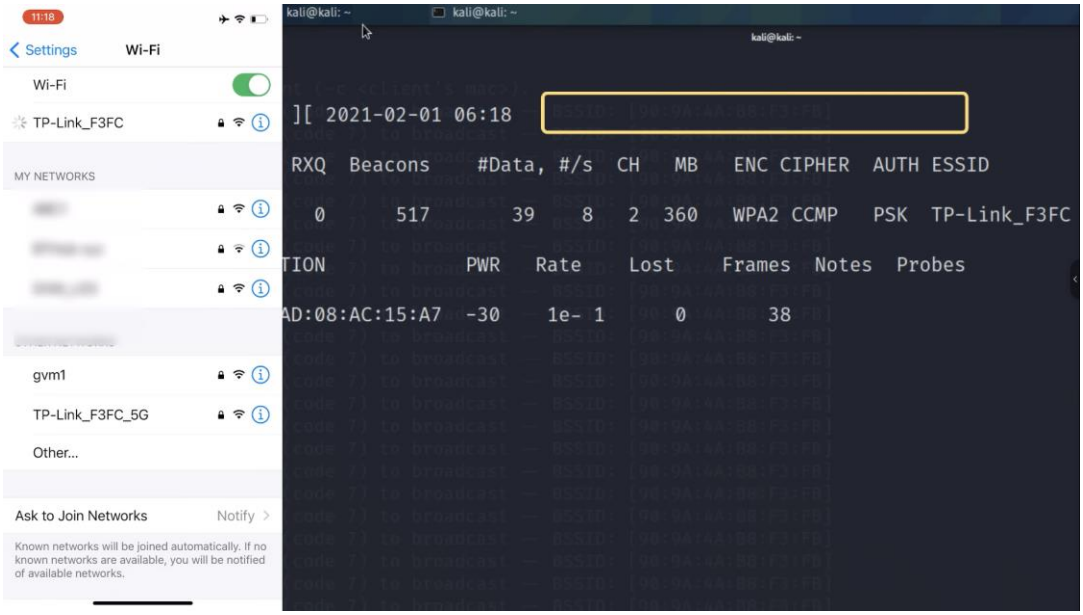


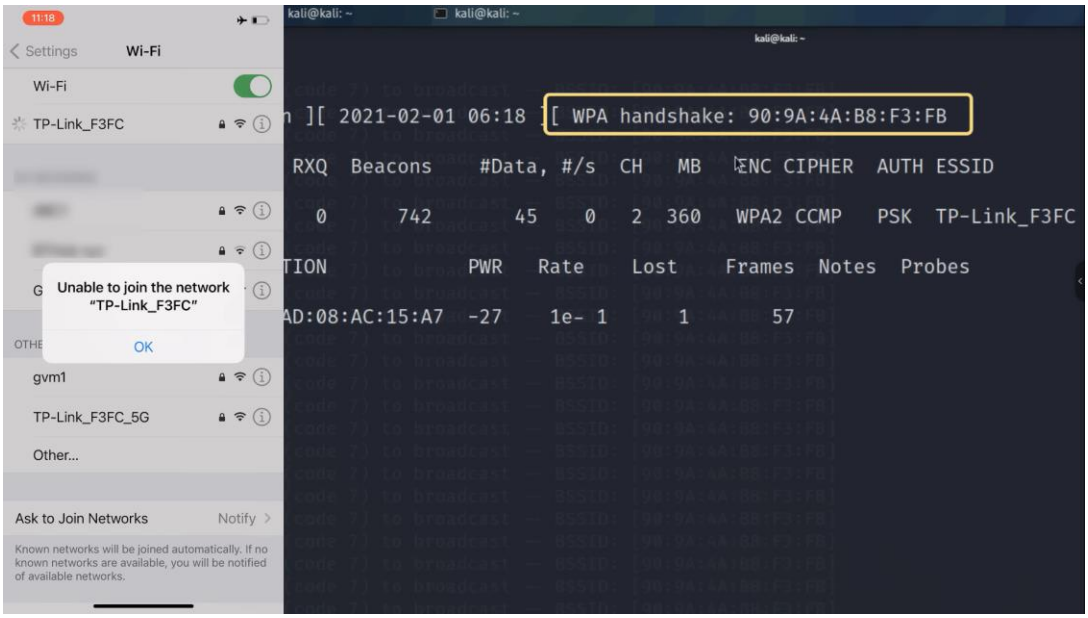
Within Wireshark, look for the 4-way WPA handshake packets. These packets include the information needed to attempt cracking the password.



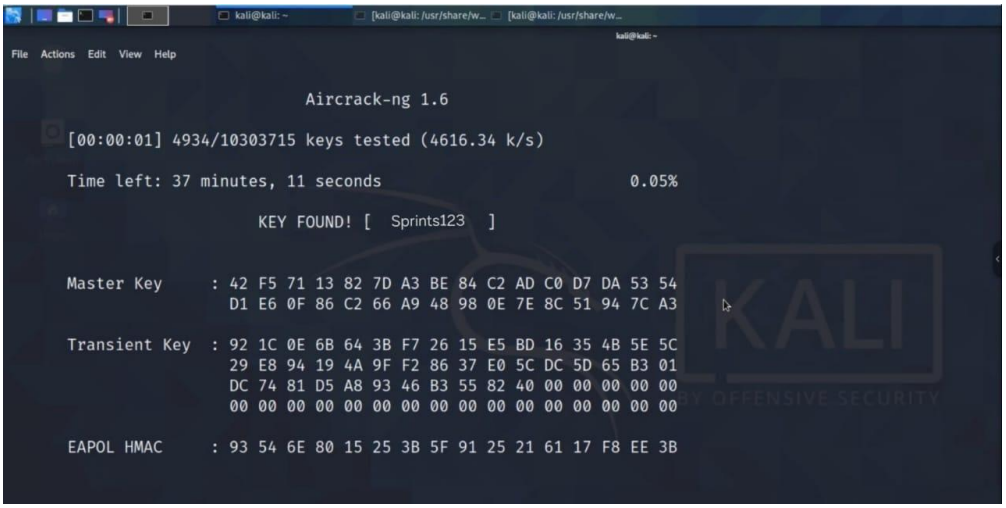
9. Cracking the Password

The captured handshake contains encrypted authentication data. To decrypt it:





Use aircrack-ng <file_name>-01.cap -w /usr/share/wordlists/rockyou.txt, where rockyou.txt is a wordlist containing millions of potential passwords. Aircrack-ng will try each word from the list until it finds the correct password.

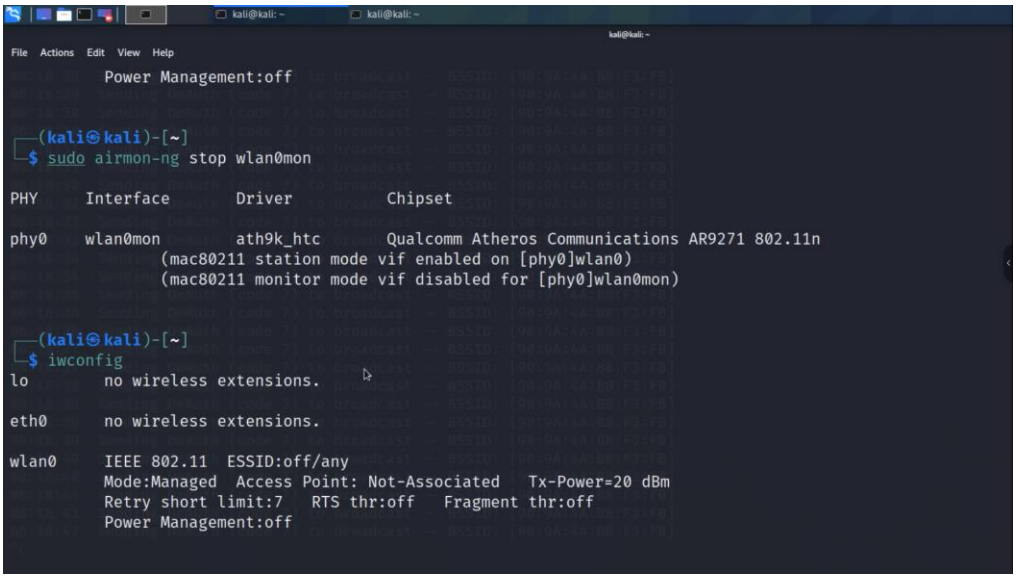


10. Restoring Normal Network Operations

Once the handshake has been captured and the cracking attempt begins, restore normal functionality to the network:

Stop the monitor mode on the adapter by running sudo airmon-ng stop wlan0mon.

This will allow clients to reconnect to the network.



11. Conclusion

This project demonstrates the vulnerability of WPA/WPA2 secured networks to deauthentication and brute-force attacks, emphasizing the importance of strong passwords and additional security layers. While this technique is widely used in penetration testing and ethical hacking, it also highlights the need for responsible use of such methods to prevent unauthorized access.

12. Recommendations

To mitigate risks associated with Wi-Fi cracking:

Use complex passwords and avoid using common words or patterns.

Implement WPA3, which provides stronger security mechanisms.

Employ additional security measures such as MAC address filtering and disabling WPS.

This report provides a structured breakdown of how a Wi-Fi network can be breached using standard tools and methods available on Kali Linux. The steps detailed are aimed at helping to understand potential weaknesses in wireless security and reinforcing the need for robust protection strategies.