Group Midmen! Lab 4: Wi-Fi Hacking & Defense

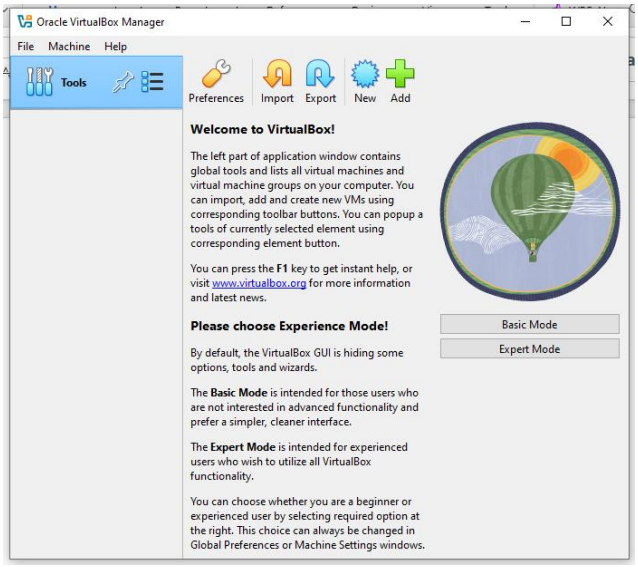
Objective: Crack WPA2 and recommend security improvements.

Tools:

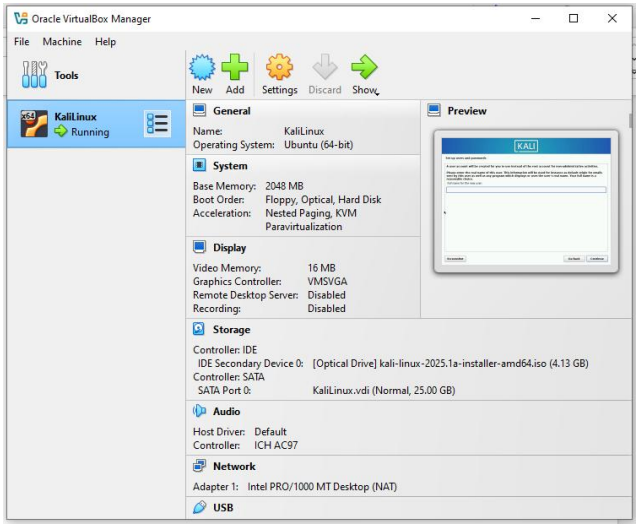
Kali Linux (Aircrack-ng, Wifite)

Step 0: Prepare Environment

- Install VirtualBox



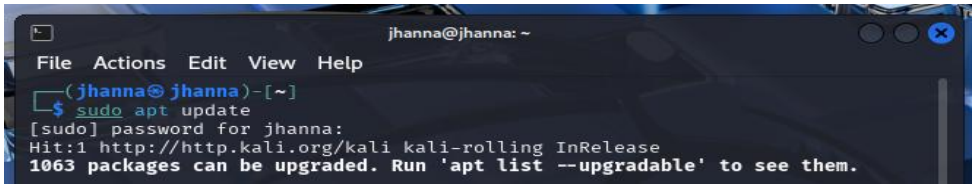
- Install Kali Linux and add it in Virtual Box

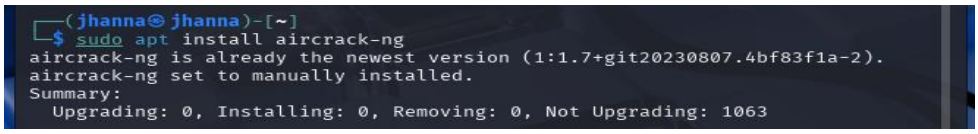


Step 1: Capture Handshake

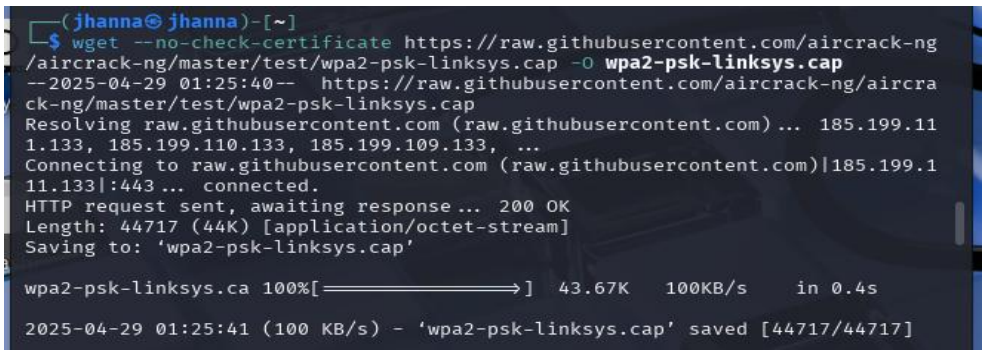
Supposedly, we would capture the handshake using airmon-ng and airodump-ng… Due to hardware limitations (lack of external Wi-Fi adapter), handshake capture was not performed. We proceed by analyzing a sample capture file found online.

- Make sure aircrack-ng is installed (since it's pre-installed in Kali Linux most of the time, but just in case).





- From this repository, *https://github.com/aircrack-ng/aircrack-ng/blob/master/test/wpa2-psk-linksys.cap*, we downloaded a handshake capture file - *wpa2-psk-linksys.cap*

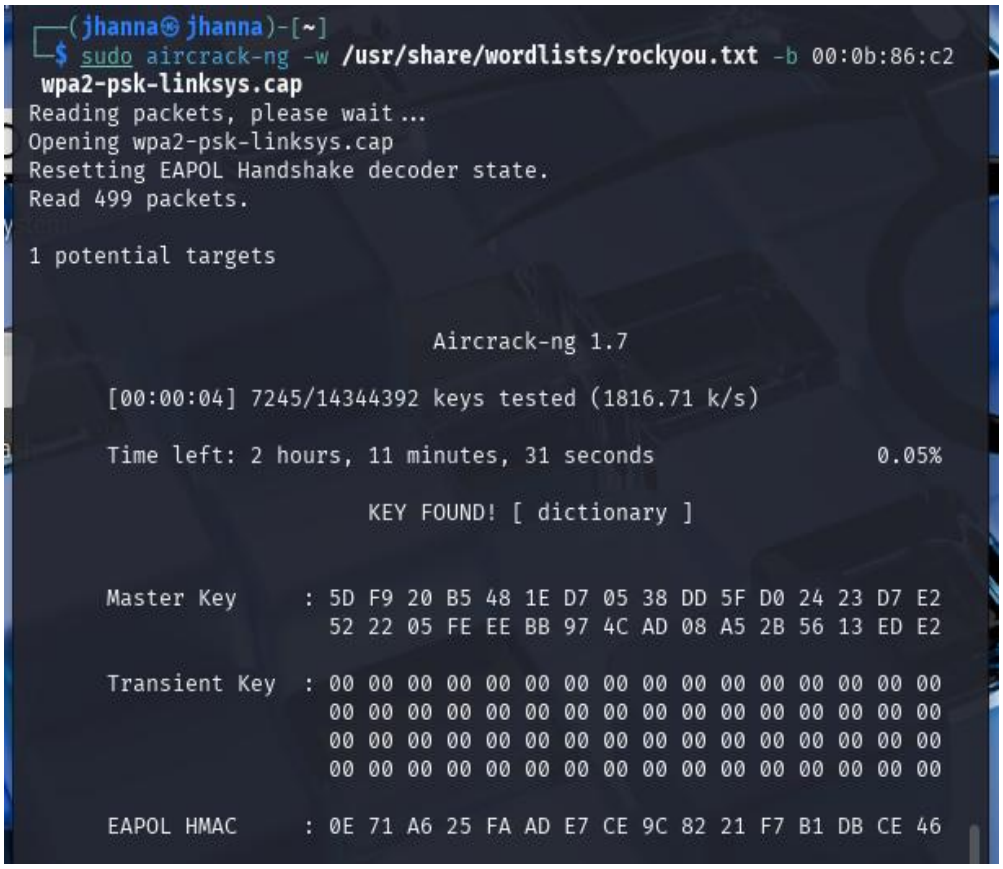


- Verify the handshake in the file with aircrack-ng and we found it.

Step 2: Crack password

- In Kali Linux rockyou.txt (contains a list of common passwords) is already built in; however, it is compressed as rockyou.txt.gz so we need to extract it first.

- Now, after cracking it using aircrack-ng rockyou.txt and specifying its BSSID, we found the password, *dictionary*.



Step 3: Defend

- It is recommended to use WPA3 or RADIUS Authentication for better security.
  - **WPA3** is the latest Wi-Fi security protocol, offering significant improvements over WPA2. It provides stronger encryption and better protection against brute-force attacks.

- **How to implement:**

  1. Ensure your wireless router supports WPA3.
  2. Update the router's firmware to the latest version.
  3. In the router's settings, select WPA3 as the security protocol.
  4. Clients must also support WPA3 to connect using this protocol.

- **RADIUS (802.1X)** provides centralized authentication, authorization, and accounting. It is more secure than pre-shared key methods (like WPA2/3-PSK) as it requires each user to have unique credentials.

  - **How to implement:**

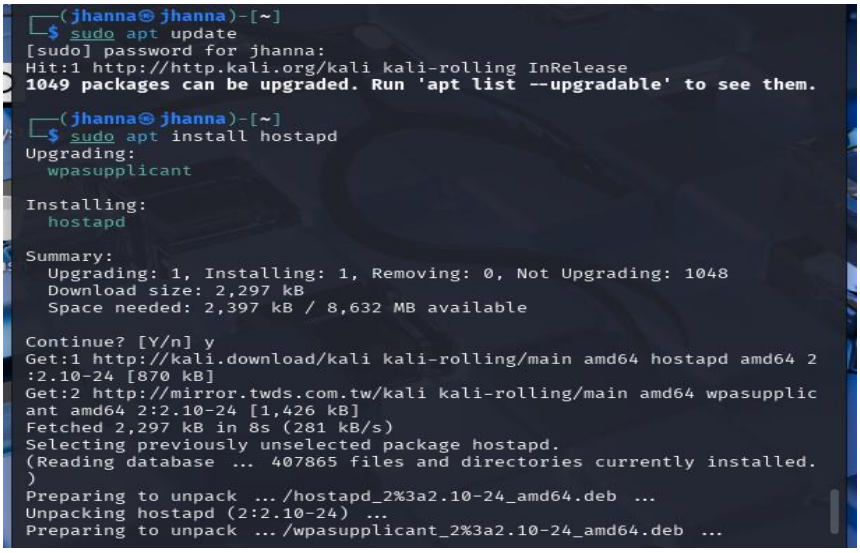
    1. Set up a RADIUS server (e.g., FreeRADIUS) on a server within your network.
    2. Configure the wireless router to use the RADIUS server for authentication.
    3. Create user accounts on the RADIUS server.
    4. Clients authenticate using their individual credentials.

- Set Up a Honeypot AP (hostapd)

  - A **honeypot** is a decoy access point designed to attract attackers. It allows you to monitor and gather information about unauthorized access attempts.

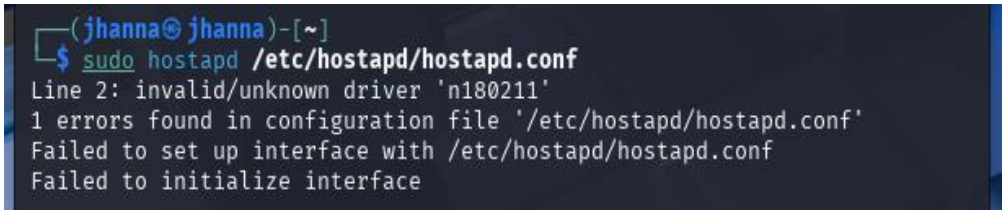
    - **How to implement:**

      1. Install hostapd



2. Configure hostapd (we use nano). Interface was supposed to be a wireless one but without a wireless adapter there's no wireless interface. Instead we use *eth0*, a standard ethernet interface.

3. Start hostapd and as expected, it won't work because of the wireless interface. But if there's a wireless adapter, these are the same commands to implement.



Secure Wi-Fi Configuration Guide

Follow these steps to ensure your Wi-Fi network is protected from unauthorized access and cyber threats:

1. Change Default Admin Credentials

- Log in to your router's admin panel (usually via a web browser, using the router's IP address).
- Change the default administrator username and password to strong, unique values. Default credentials are widely known and easily exploited.

2. Change the Default SSID (Network Name)

- Set a unique SSID (avoid using personal information or router brand/model).

- This makes it harder for attackers to identify your router and exploit known vulnerabilities.

3. Use Strong Wi-Fi Passwords

- Create a complex Wi-Fi password with a mix of uppercase, lowercase, numbers, and symbols.
- Avoid simple or common passwords like “password123” or “admin”.

4. Enable Strong Encryption (WPA3 or WPA2)

- Select WPA3 as your security protocol if available; otherwise, use WPA2.
- Avoid older protocols like WEP or WPA, which are insecure.

5. Disable WPS (Wi-Fi Protected Setup)

- WPS can be easily exploited by attackers. Turn it off in your router’s security settings.

6. Update Router Firmware Regularly

- Check for and install firmware updates from your router manufacturer to patch vulnerabilities and improve security.

7. Disable Remote Management

- Turn off remote management features unless absolutely necessary. This prevents external access to your router’s settings.

8. Hide SSID Broadcast (Optional)

- Disable SSID broadcast to make your network less visible. Note: This is not a strong security measure on its own, but can deter casual snooping.

9. Enable the Router Firewall

- Activate your router’s built-in firewall to help block malicious traffic.

10. Limit Connected Devices

- Restrict the number of devices that can connect to your network, or use MAC address filtering for an added layer of control.