**ETHICAL HACKING – II**

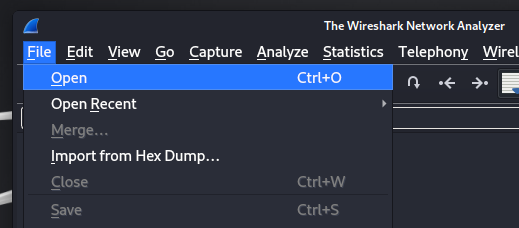
**LAB ASSIGNMENT 1**

Exercise 1: Analyzing Wireless Traffic Using Wireshark.

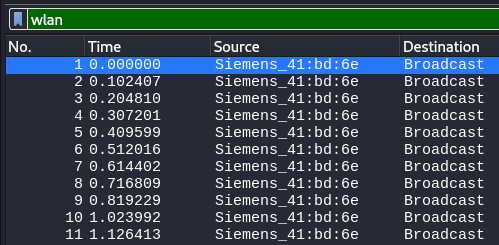
Objective: Learn how to open and analyze pre-captured wireless network traffic.

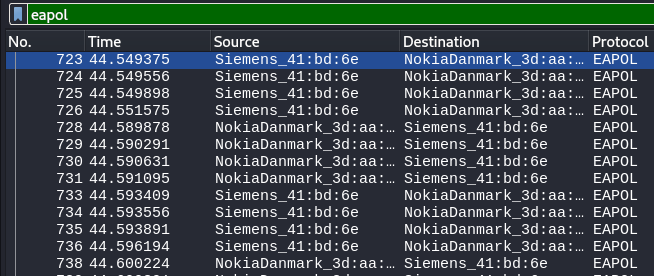
Steps:

1. \*\*Open Wireshark\*\*:  
      - Launch Wireshark on your computer.  
      - Load a pre-captured file (e.g., WPA handshake):  
        - Go to `File` > `Open` > Select the `.pcap` file.



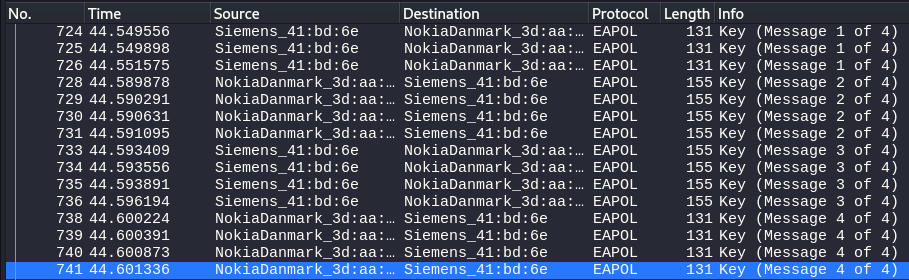
1. \*\*Filter Wireless Traffic\*\*:  
      - Use filters to isolate wireless packets:  
        - For WPA handshake: `eapol`.





1. \*\*Analyze Packets\*\*:  
      - Identify the following components in the capture:  
        - \*\*SSID\*\*: **“martinet3”**  
        - \*\*BSSID\*\*: **Siemens\_41:bd:6e (00:01:e3:41:bd:6e)**  
        - \*\*Handshake Packets\*\*: Look for EAPOL packets.

**Note: A complete WPA/WPA2 handshake consists of 4 EAPOL messages**



1. \*\*Document Observations\*\*:

-Time: 44.549375 to 44.601336 (WPA Handshake)

-Source address: Siemens\_41:bd:6e (00:01:e3:41:bd:6e)

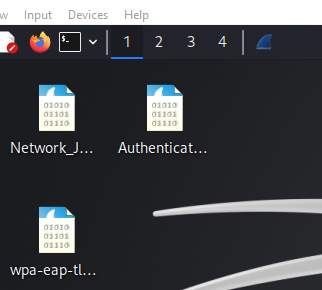
-Destination address: NokiaDanmark\_3d:aa:57 (00:16:bc:3d:aa:57)

Exercise 2: Cracking WPA/WPA2 Encryption Using a Pre-Captured Handshake

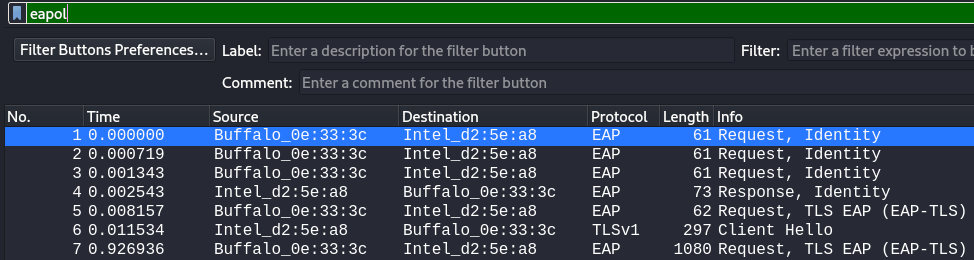
Objective: Simulate cracking a WPA/WPA2-encrypted network using a captured handshake and dictionary attack.

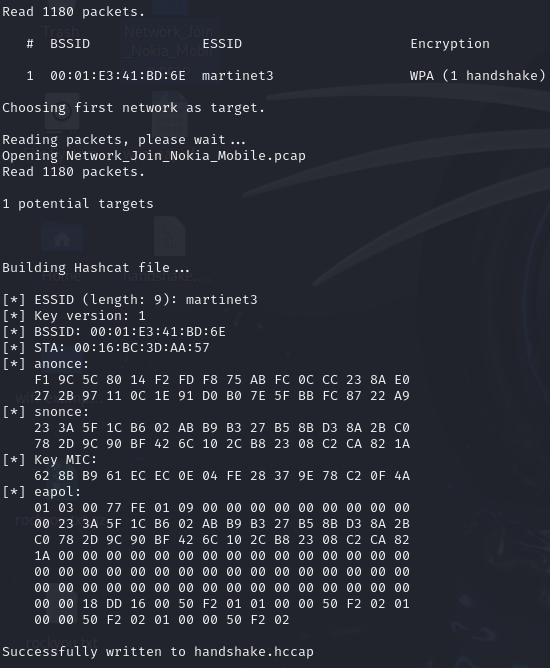
Steps:

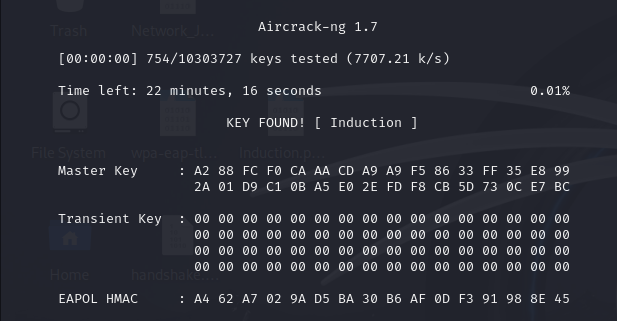
1. \*\*\*Download a WPA Handshake File\*\*:  
      - Obtain a `.cap` file with a valid handshake (e.g., from GitHub).



1. \*\*Verify the Handshake\*\*:  
      - Open the file in Wireshark.  
      - Use the filter `eapol` to ensure handshake packets are present.



1. \*\*Convert the Capture File\*\*:  
      - Use `aircrack-ng` to convert the `.cap` file to `.hccapx` format for Hashcat (optional):  
        ```bash  
        aircrack-ng handshake.cap -J handshake  
        ```
2. \*\*Run Aircrack-ng\*\*:  
      - Attempt to crack the handshake using a dictionary file:  
        ```bash  
        aircrack-ng -w /usr/share/wordlists/rockyou.txt handshake.cap  
        ```



Exercise 3: Simulating an Evil Twin Attack (Theoretical)

Objective:

The goal of this exercise is to understand the concept of a rogue access point (Evil Twin) and its implications for network security. By the end of this exercise, you should be aware of how attackers exploit Wi-Fi networks and the defensive measures that can mitigate such attacks.

Steps:

1. Setup Overview:
   * Rogue Access Point: An Evil Twin attack involves creating a fake Wi-Fi access point that mimics a legitimate one. Attackers use tools like Fluxion or Airgeddon to set up these fake APs.
     + Fluxion: A popular tool for conducting Evil Twin attacks. It automates the process of creating a fake AP and capturing user credentials via a captive portal.
     + Airgeddon: Another tool that combines various Wi-Fi attack techniques, including Evil Twin attacks.
   * Note: Since this exercise is theoretical, you won’t be setting up a real rogue AP. Instead, focus on understanding how these tools work and the steps involved in an attack.
2. Captive Portal:
   * How It Works: Once a victim connects to the rogue AP, they are redirected to a fake login page (captive portal) that mimics a legitimate one (e.g., a coffee shop’s Wi-Fi login page).
   * Social Engineering: The victim is tricked into entering sensitive information, such as login credentials or payment details, which are then captured by the attacker.
   * Example: A user connects to a fake Wi-Fi network named "Free Airport Wi-Fi" and is prompted to enter their email and password to access the internet. The attacker captures this information.
3. Defensive Measures:
   * HTTPS: Always ensure that websites use HTTPS (look for the padlock icon in the browser). HTTPS encrypts data between the user and the website, making it harder for attackers to intercept sensitive information.
   * VPNs: Using a Virtual Private Network (VPN) encrypts all internet traffic, protecting it from being intercepted by rogue APs.
   * Verify Network Names: Be cautious when connecting to public Wi-Fi. Verify the network name with the establishment’s staff if possible.
   * Avoid Sensitive Transactions: Avoid logging into sensitive accounts (e.g., banking) or entering personal information when connected to public Wi-Fi.