**Lab 3 Part 01 - Passive Sniffing in 802.11 Networks**

* **Name**: Brandon Cortez
* **Student ID**: 820561762
* **Date**: 4/18/2025

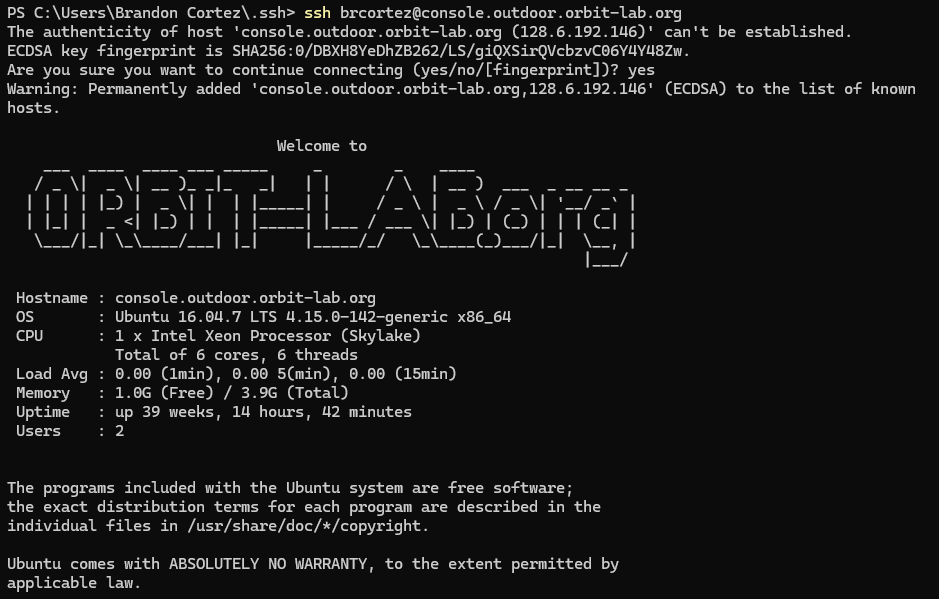
**1. Objective**

Read the entire lab document and briefly state the overall objective of the lab in your own words.

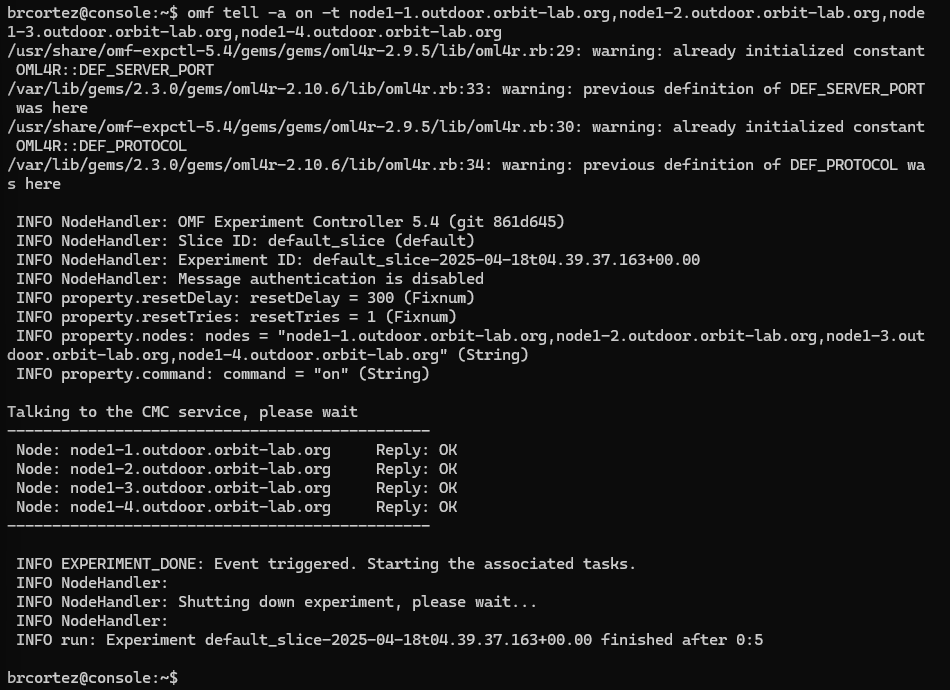
The objective of this lab is to evaluate the confidentiality of different Wi-Fi security protocols, Open, WEP, and WPA, by passively sniffing network traffic and analyzing whether an unauthorized observer can view or decrypt the transmitted data.

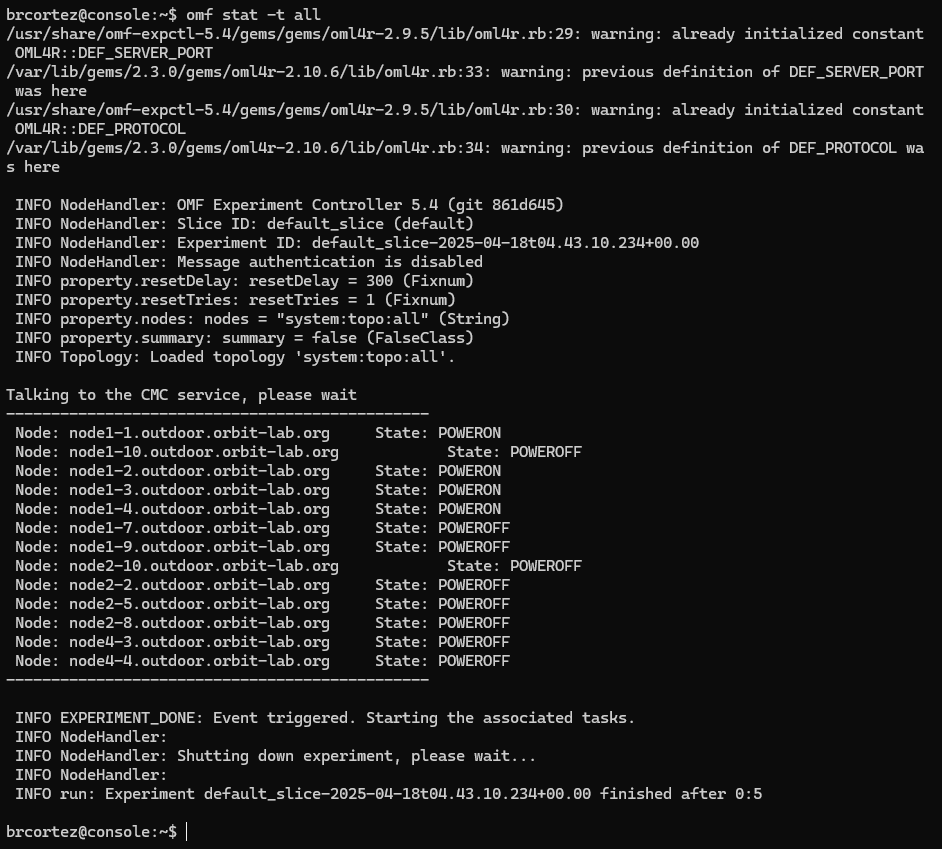
**2. Testbed Setup**

* Reserve the ORBIT "outdoor testbed (or another sandbox if unavailable) and SSH into the testbed console.
  + Show successful SSH access to the console.

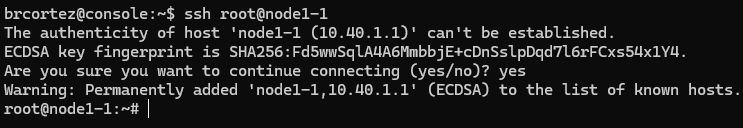


* Configure the 4 nodes (e.g., node1-1, node1-2, node1-3, node1-4 ) on the testbed for the experiment. (Note: You may use any radio nodes within range that have the Atheros AR 9xxx wireless adapter)
  + Show confirmation of nodes successfully being reset and powered on.

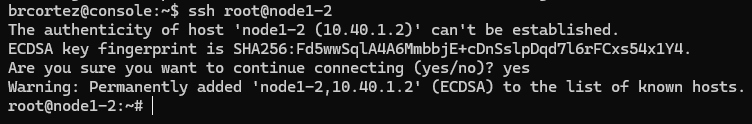




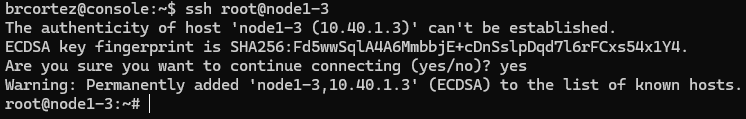
* Verify the status of the nodes by navigating to the status page or using any appropriate commands.
  + Show successful SSH access to the 4 nodes
    - Node1-1



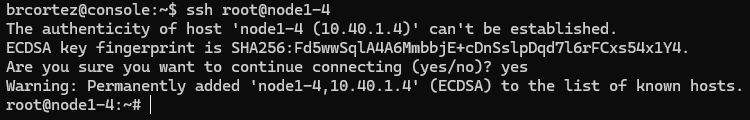
* + - Node1-2



* + - Node1-3

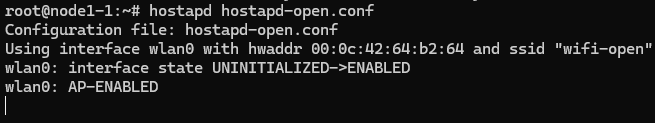


* + - Node1-4

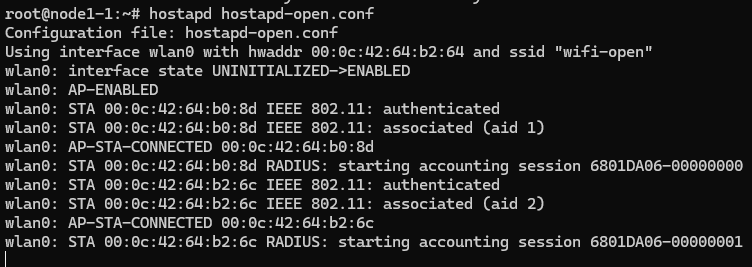


**3. Open Wi-Fi Network Configuration**

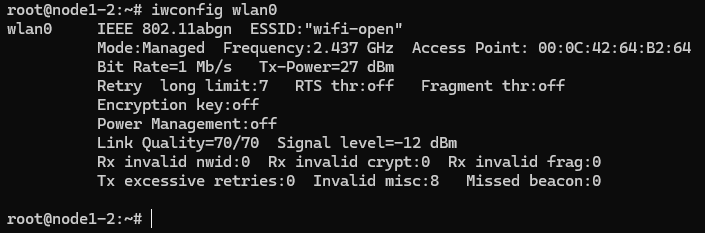
* Start the wireless AP on the designated node.
  + Show terminal output after starting the wireless AP.



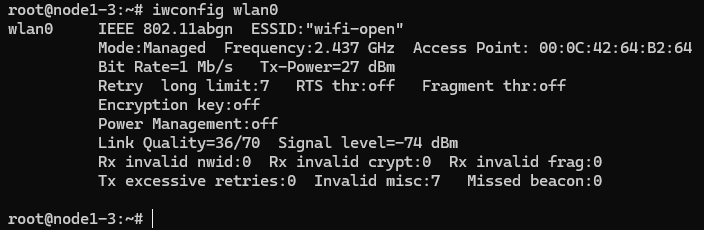
* Connect Alice and Bob to the open Wi-Fi network.
  + Show the output of iwconfig after Alice and Bob successfully connect to the AP as well as the successful connection on the AP terminal
    - AP



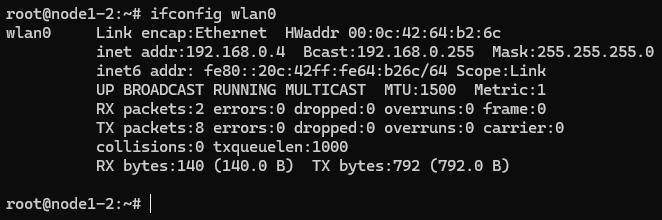
* + - Bob



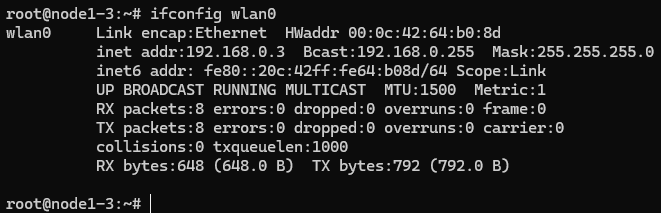
* + - Alice



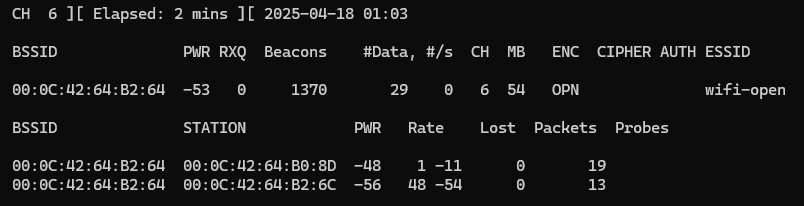
* Assign IP addresses to Alice and Bob.
  + Provide evidence that the IP addresses are successfully assigned.
    - Bob



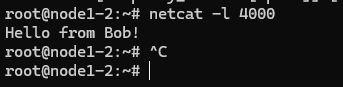
* + - Alice



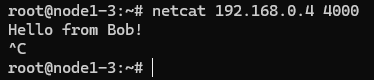
* Put Mallory in monitor mode and begin capturing traffic.
  + Show Mallory’s capture using airodump-ng.



* Pass user data between Alice and Bob using netcat.
  + Show that the message typed on Alice or Bob appears in the terminal of the other.
    - Bob

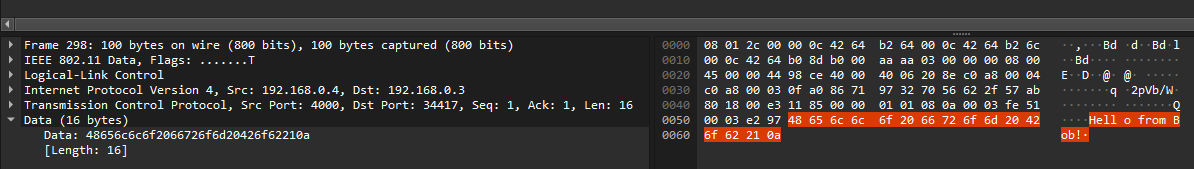


* + - Alice



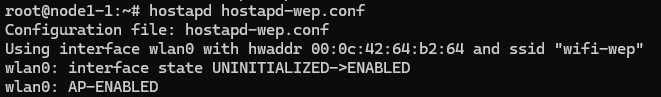
* Can Mallory, the attacker, see the data in plaintext? What do you observe from the captured traffic? Use Wireshark to inspect the captured file and provide screenshots and analysis to back your claims. Provide screenshots from your capture to back up your answer.

In the open network Mallory can indeed see the messages sent between Alice and Bob in plaintext.

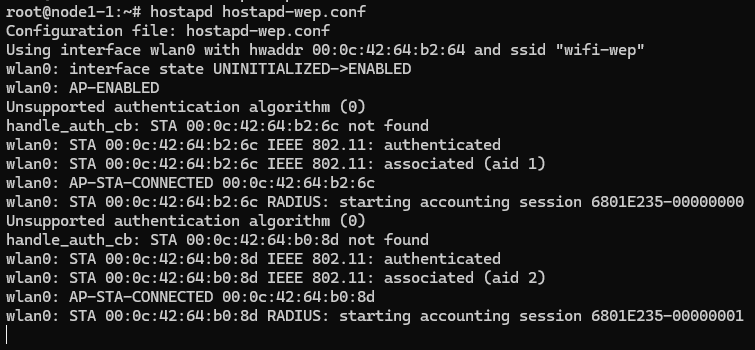


**4. WEP Network Configuration**

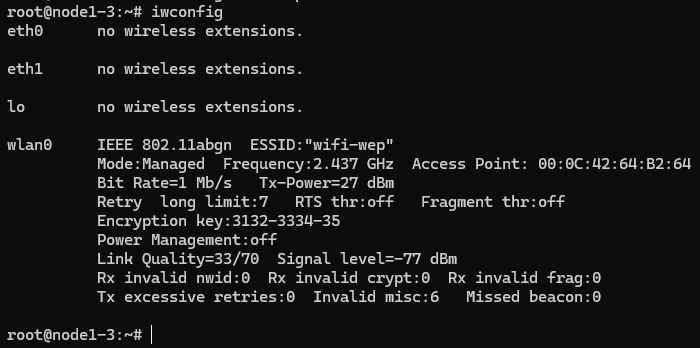
* Start the wireless AP for the WEP network.
  + Show terminal output after starting the WEP AP.



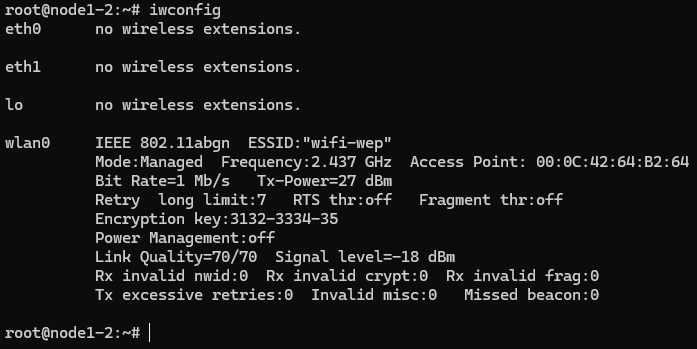
* Connect Alice and Bob to the WEP network.
  + Show Alice and Bob’s connection using iwconfig as well as the successful connection on the AP terminal.
    - AP



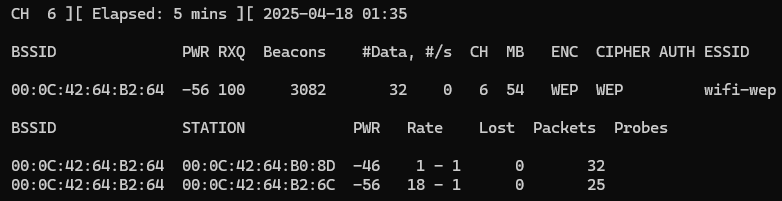
* + - Alice

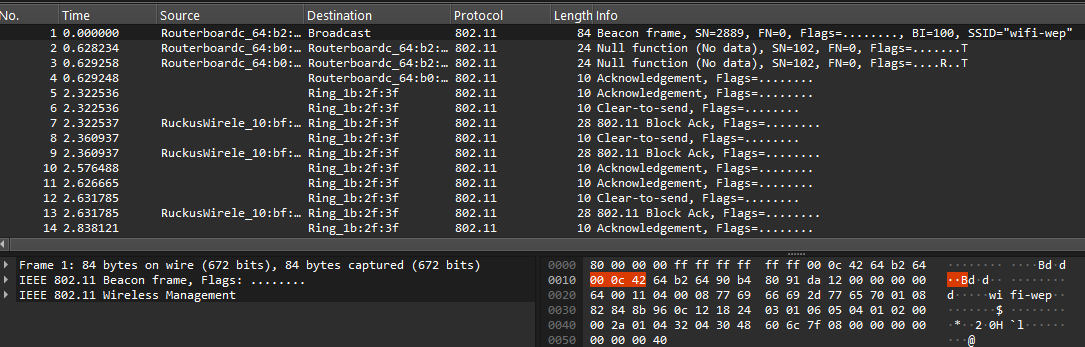


* + - Bob

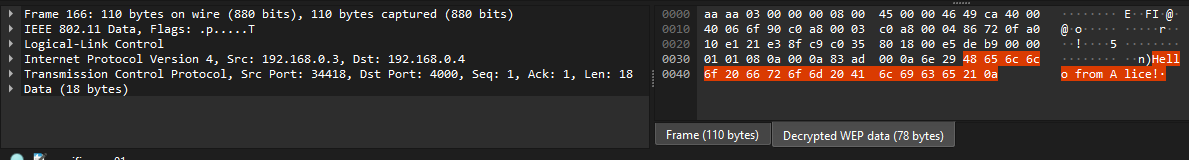


* Capture traffic on Mallory’s node.
  + Show the Wireshark capture of WEP traffic on Mallory’s node.





* Analyze the captured traffic and attempt to decrypt it using Wireshark.
  + Show the decrypted WEP packets.

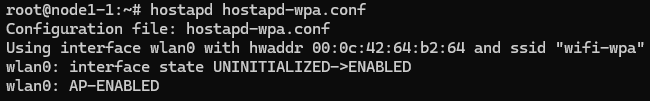


* Without knowing the WEP key, can Mallory see the data in plaintext? If Mallory later finds out the key, is she able to decrypt the traffic? Explain your findings.

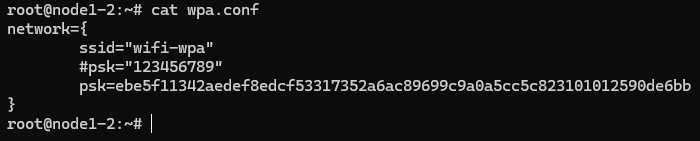
Without the WEP key, Mallory cannot see the data in plaintext, packets appear encrypted in Wireshark. Once the key is known and added, the traffic can be decrypted, revealing the plaintext message. This shows that WEP's encryption is weak and offers little protection once the key is compromised.

**5. WPA Network Configuration**

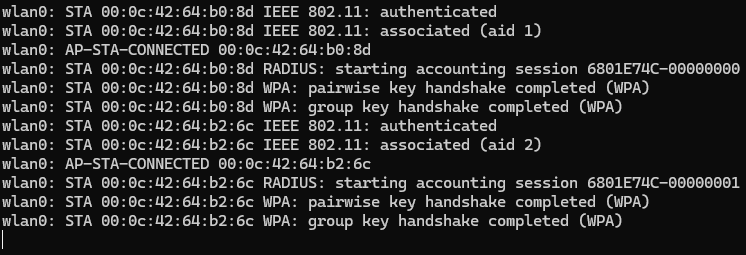
* Start the wireless AP for the WPA network.
  + Show terminal output after starting the WPA AP.



* + Provide the contents of the wpa.conf file



* Connect Alice and Bob to the WPA network using wpa\_supplicant.
  + Show Alice and Bob’s connection using wpa\_supplicant as well as the successful connection on the AP terminal.
    - AP



* + - Alice



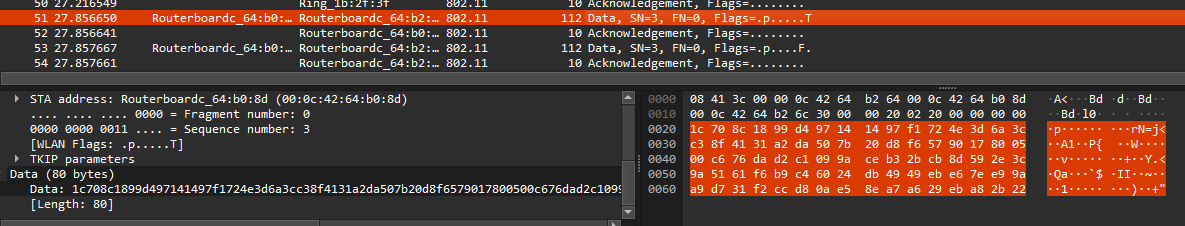
* + - Bob



* Analyze the captured traffic in Wireshark.
  + Look for the data packets containing the secret message - is the attacker able to see the data in plaintext?

No, the attacker is not able to see the data in plaintext. Without the WEP key, the captured packets appear encrypted in Wireshark, and the message content is unreadable.

* + Provide a screenshot showing whether Mallory can see any useful data without decryption.



* + Add the WPA passphrase to Wireshark's decryption settings and attempt to decrypt the captured traffic.

No Mallory is not able to read the message in plaintext after acquiring the WPA passphrase, the data still appears encrypted in Wireshark.

* + Show the WPA decryption attempt in Wireshark and comment on whether the traffic is decrypted successfully after capturing the handshake.

After capturing the four-way handshake I was able to find the decrypted secret message in the Decrypted TKIP data field.

A screenshot of a computer

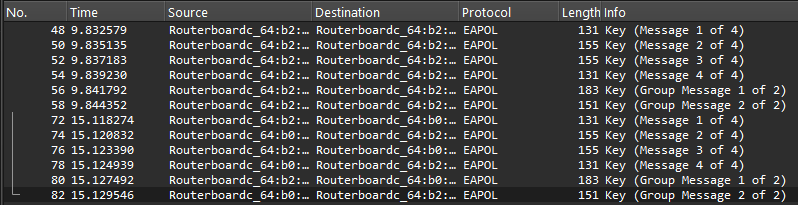
AI-generated content may be incorrect.

* Given the new scenario after capturing the WPA handshake, can Mallory decrypt the traffic? Look for the data packets containing the secret message, and specifically look for a "Decrypted TKIP data" tab on the bottom - is Mallory able to read the data if she has captured the 4-way handshakes?

Even after capturing the WPA 4-way handshake, Mallory cannot decrypt the traffic unless she also knows the correct WPA passphrase. In this scenario, if Mallory does not also have the passphrase, the captured packets do not show a "Decrypted TKIP data" section, confirming that the traffic remains encrypted. Therefore, the secret message cannot be read. This demonstrates that capturing the handshake alone is not sufficient for decryption without the shared key.

* Provide screenshots and analysis showing the 4-way handshake and whether the traffic is decrypted successfully after capturing the handshake.

After successfully capturing the four-way handshake we can read the secret message in plaintext since we also have the passphrase.



A screenshot of a computer

AI-generated content may be incorrect.

* Why does capturing the 4-way handshake help an attacker decrypt WPA traffic? What information does Mallory gain from the handshake?

Capturing the four-way handshake helps an attacker because it contains the information needed to calculate the temporary encryption key used for that session. If Mallory also knows the WPA passphrase, she can use the handshake to generate the same key the client and access point use to encrypt and decrypt data. This makes it possible to read the traffic.

**6. Summary and Conclusions**

Summarize the security implications for each network type (open, WEP, WPA). Discuss how each network performs in terms of confidentiality based on the experiment results. How secure is each network in terms of passive sniffing, and what lessons can be learned about the effectiveness of WEP and WPA encryption methods?

From the experiment, it’s clear that each network type offers a different level of confidentiality.

* The **open** network had no encryption at all, allowing Mallory to easily capture and read plaintext messages through sniffing. This shows that open networks offer zero protection for user data.
* The **WEP** network, while encrypted, was still vulnerable. Without the key, Mallory couldn’t read the messages initially. However, once the WEP key was known, the traffic was easily decrypted in Wireshark, proving that WEP encryption is weak and outdated. It provides only minimal protection and should not be relied on for secure communication.
* The **WPA** network was the most secure. Even after capturing the full 4-way handshake, Mallory couldn’t decrypt the traffic without the correct WPA passphrase. This shows that WPA provides strong protection against passive sniffing as long as the passphrase remains secret.

Overall, the lab demonstrates that open and WEP networks are insecure, and WPA is significantly more effective at protecting user data.