The exercises are designed for students to finish in an individual capacity. The exercises are not designed to be completed in tutorial sessions but rather to give you some tasks and a starting point to continue and complete on your own.

---

1 WPA/WPA2 Handshake

1.1 Understanding the 4-Way Handshake

Review the four messages in the WPA/WPA2 4-way handshake. What does each message include, and what is its purpose?
(W10 Lecture slide 22)

1.2 Find the Hash

Let's examine a real packet capture of a WPA2 handshake between a WiFi Client and an Access Point to observe the **Key MIC (Message Integrity Code)**.

Download the packet capture using this link and open it in Wireshark. Enter "EAPOL" as a display filter in Wireshark to locate the WPA2 4-way handshake and identify the **Key MIC** field in the EAPOL Key frame. Which packet contains the MIC and what is its 16-byte value?

2 Offline Dictionary / Brute-force against the PSK

In this lab we will perform an offline dictionary attack against WPA/WPA2 PSK. We will be using aircrack-ng suite to perform the tasks.

2.1 Aircrack-ng

The Aircrack-ng suite comprises the following tools, each designed for a specific purpose:

- aircrack-ng
- airdecap-ng
- airmon-ng
- aireplay-ng
- airodump-ng
- airtun-ng
- packetforge-ng
- airbase-ng
- airdecloak-ng
- airolib-ng
- airserv-ng
- buddy-ng
- ivstools
- easside-ng
- tkiptun-ng

- wesside-ng

Note: Aircrack-ng is a legitimate Wi-Fi auditing toolkit, but using it against networks without permission is illegal. It should only be used for authorized security testing, research, or learning on your own lab networks.
Reference: Aircrack-ng Wiki.

2.2 Capturing the Handshake

2.2.1

In the previous tasks we inspected a captured WPA/WPA2 handshake. How do you capture a handshake from a live Wi-Fi network? Describe how you would perform the capture using the Aircrack-ng suite, and list which tools from the suite you would use.

2.2.2

How can you capture a WPA/WPA2 handshake when all users are already authenticated? Explain how you would do it with the Aircrack-ng tools and name which utilities in the suite you'd rely on.

Note: To run the Aircrack-ng tools you need a wireless adapter that supports monitor mode and packet injection. Most built-in laptop adapters do not support these features, so we will not perform those tasks in this lab.

Reference: Aircrack-ng Wiki - Cracking WPA.

2.3 Cracking WPA(2) Personal Password

Let's use the Aircrack-ng tool to crack the hash from a captured WPA/WPA2 handshake. We'll run a dictionary attack using a large wordlist to try to recover the passphrase.

2.3.1 Prepare the packet capture

Download the .cap file to the GNS3 VM by running the below command on the GNS3 VM.

```
gdown 1wlr6sIgd3eY0ya4lMbVTXZs4noBqF3wx
```

2.3.2 Prepare the dictionary

Download the `rockyou.txt` password file and extract it.

Note: rockyou.txt is a very widely used password wordlist — a plain-text list of real passwords (one per line) derived from the 2009 RockYou data breach. Security testers and researchers use it as a basic benchmark wordlist for dictionary attacks, password strength testing, and training tools. (two commands)

```
wget https://weakpass.com/download/90/rockyou.txt.gz
gzip -dk rockyou.txt.gz
```

2.3.3 Find the WiFi networks in the packet capture.

Use the following command to scan the .cap file and list all networks (BSSID) inside it. BSSID refers to Basic Service Set Identifier. This is the unique identifier of each AP.

```
aircrack-ng wifiauth.cap
```

2.3.4 Crack the Hash

Run the below command to crack the hash (replace BSSID, PASSWORDFILE and PCAPFILE with the correct values).

```
sudo aircrack-ng -b 'BSSID' -w 'PASSWORDFILE' 'PCAPFILE'
```

- **BSSID**: BSSID from task **2.3.3**
- **PASSWORDFILE**: Dictionary file (rockyou.txt)
- **PCAPFILE**: Packet Capture file which include the handshake.

Note: Note the password-cracking speed observed with Aircrack-ng during the exercise.

3 Questions for group discussion

1. What are the minimum and maximum PSK (passphrase) lengths for WPA/WPA2?
2. WPA2 passphrases are ASCII. If the minimum length is used, how many possible passwords exist?
3. Given the password-cracking speed you measured earlier, how long would a brute-force attack take on your machine (on average) to crack a WPA2 passphrase?
4. Using a NVIDIA GeForce RTX 5090 GPU, how long would the same brute-force attack take?

   Refer to the below links for password cracking speeds to different GPUs:

   - https://gist.github.com/GermanAizek/f968d0bb213b2b7c8d9b35bbc4d031e4
   - https://gist.github.com/Chick3nman/09bac0775e6393468c2925c1e1363d5c
5. Based on what you've learned so far, discuss the best practices for creating secure passwords in WPA/WPA2-Personal networks.
6. Discuss how WPA3 protects against offline dictionary and brute-force attacks.
7. Download and install NetSpot Wi-Fi Analyzer: (https://www.netspotapp.com/download.html). Run it from while you are in the class and find which WiFi networks are using **WPA2** and **WPA3**. Which ones are using **Personal** and which ones are using **Enterprise**?
8. Start a hotspot on your mobile device and use **NetSpot** to check which security type it uses.

4 Tasks to try at home:

Important – Ethical and Legal Notice: Onlyperform the following tasks on networks you personally own or on those for which you have explicit, written permission to test. All testing and analysis should be conducted in a controlled, authorised environment. Attempting to access or interfere with networks without consent is illegal and unethical.

1. Using NetSpot, check whether your home network is using WPA2 or WPA3.
2. If it's WPA2 and you own the network, you may proceed with locally authorized testing. If it's WPA3, the offline PSK attack described earlier is not applicable in the same way.
3. On your host machine, disconnect (or "forget") the target Wi-Fi network so the client will need to re-authenticate.
4. Open Wireshark and start monitoring traffic on your wireless interface (monitor mode if available).
5. Reconnect to the Wi-Fi network from your host. This will trigger a fresh 4-way handshake that Wireshark can capture.

6. Stop Wireshark capture once the reconnect completes. Filter for eapol and inspect the packets to confirm you captured the handshake (look for an EAPOL Key frame with a 16-byte Key MIC).

7. Save the capture to a .pcap file on your host (for example, wifiauth.pcap).

8. Transfer the .pcap to the GNS3 VM via SSH. Example (from your host):

```
cat wifiauth.pcap | ssh -p 22 gns3@172.16.133.131 \
'cat > /home/gns3/wifiauth.pcap'
```

9. Run the dictionary attack on the captured handshake as you've done in step **2.3.4** to find out if your home WiFi password is in the rockyou password list.