In Lab 6 (and Homework 6) we looked at the 4-way Handshake and how to extract useful information from the Messages. We then generated the PMK and subsequently the PTK with the given passphrase.

The question then is how would you find the PMK if the passphrase is unknown?

Your task for Homework 7 will involve finding the passphrase for a WPA-PSK network. There are 3 pcap files, each containing the handshake between a client and an AP. Assume that the password for the network can be found in the wordlist rockyou.txt in each case. Use these pcaps to answer the questions below.

1. Was a deauthentication attack used to capture the handshake in any of the files? If so which file? **[0.25 pts]**
2. Which pcap contains a capture of the *neverssl.com* website being visited? **[0.5 pts]**
3. Which pcap file has a capture of an AP (involved in the handshake) using a hidden network name? **[0.25 pts]**
4. What was the AP operation channel for each network (in each pcap file)? **[0.75 pts]**
5. For **each** pcap file:
   - What is the BSSID and SSID of the captured network? **[0.75 pts]**
   - What is the passphrase for the network (different in each file)? **[1 pt]**
     - For HW7_pcap2 you discovered that the passphrase was 10 characters in length.
     - For HW7_pcap3 you discovered that the network had a passphrase of length 13 characters and starts with the letter ‘j’.
     - The provided python script (in lab files) can be used to make your word list shorter. For reference, the times taken to find the passphrase on my Ubuntu 20 machine using aircrack-ng for HW7_pcap1 was 00:03:40, for HW7_pcap2 was 00:03:20 and 00:00:01 for HW7_pcap3. For my DragonOS VM the times were 00:16:54, 00:17:19 and 00:00:05 respectively.
   - What is the Pairwise Master Key for the network? **[0.75 pts]**
   - What is the KCK, KEK and TK for the connection? **[0.75 pts]**

For question 5, please state the command and/or tools that were used to find the passphrase, PMK etc. Screenshots are welcome. Please also include the time taken to find the passphrase on your computer.

Bonus Questions

1. Is there a way to manually shorten the wordlist used to find the passphrase for HW7_pcap1 or shorten the rockyou.txt file in general for PMK passphrase cracking? If so how? **[0.25 pt]**
2. Can the PMKID attack be used on the AP used in the pcap files? Why or why not? **[0.25 pt]**
3. hw7.16800 and hw7.22000 contains the PMKID information for a wireless AP.
   a) What is the SSID for the AP? **[0.5 pt]**
   b) Using list.txt find the passphrase for the network. *(takes 3 to 5 seconds to find on my computer)* **[1 pt]**

Due Date: Check Moodle for date
Late Submission Deadline: Check Moodle for date (usually 1 week after due date)
Submission Files: The modified python ***password-extractor script*** (if used) and a ***file with the answers*** to questions 1 to 5 (if a script was used to calculate PMK/PTK provide that as well)
Location: Moodle Homework7 link

Example question 5 answer
For Lab6.pcap
1) **SSID**: LTAT.04.009Lab6
3) **Passphrase:** D@nger0us
4) **PMK:** E7 09 71 9A 39 07 D1 D5 D4 4B 63 DB 92 69 6F BB
B0 A0 F7 69 9A E8 5F DD 63 30 A4 3D 0B 7A 64 01
5) **KCK**: b91f6bd542bddf8d8c70aa1a67b5b0dc
KEK: 7830ba9261f8505a6e9e8ea1e5020d64
TK: 226297ca180da1795611bceadaf2a8f6
Command: aircrack-ng and **Tools:** Wireshark or Python script
Time: [00:00:00] 27/27 keys tested