**CYBR430, Penetration Testing and Incident Response  
Week 3 Lab – Cracking WPA/WPA2**

The lab for this week has two parts. In part one you will summarize the steps necessary to capture a WPA handshake so that you can conduct offline analysis and attempt to determine the pre-shared key (PSK). In part two you will use a provided packet capture file which contains a WPA handshake to determine the PSK.

**Part 1: Capturing a WPA handshake (25 pts)**

Summarize below the steps necessary to capture a WPA or WPA2 handshake. Begin with how to identify a target access point and continue through conducting a packet capture on the handshake. Provide screen shots for as much of the process that your penetration test lab will support. Use the readings for this week as reference as well as any other material you may find appropriate.

Note: There is no penalty for not having the appropriate equipment to support part one of this week’s lab. Screenshots, while potentially making your explanation easier, are not required.

I was able to do most of this lab by using my physical Ubuntu workstation. I looked up some information on how to do this in a VM and it looked like it would be way easier and more likely to work using my computer.

1. First, I had to install aircrack-ng

Text

Description automatically generated

1. I looked to see what interfaces were available, I had to make sure I had a wireless connection available to use

Text

Description automatically generated

1. In this step, I used to enp4s0 connection, disconnected it, and started it in promiscuous mode. In order to do this I had to kill certain processes that might be disruptive. To do this I ran the command airmon-ng check kill

Text

Description automatically generated

1. After several attempts to get this to work, I eventually ended up with the wlan0mon interface that I needed to continue to use in later steps. For whatever reason, it would continually not work even though I tried using several interfaces. One of them eventually ended up working and I was able to continue

Text

Description automatically generated

1. In this step I run the command airodump-ng wlan0mon. This shows a bunch of available networks around me that I can use. For the purposes of this assignment I used my own network. The most important value here is the BSSID

Text

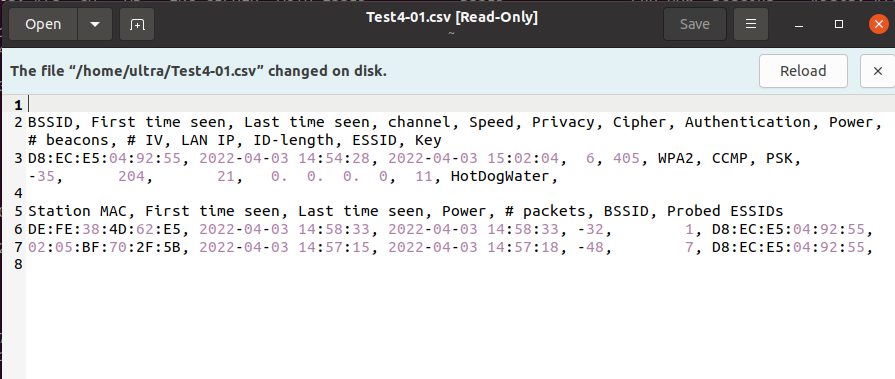
Description automatically generated with low confidence

1. Next, I run the command airodump-ng -d <BSSID> -c11 -w Test (I ended up trying this multiple times so the -w was Test4 when I got everything to work). This scans the identified network looking for devices to connect. I could run deauthenticate commands in order to make devices that are already connected disconnect and reconnect to the network, but since I had my own devices connected I was able to do this manually

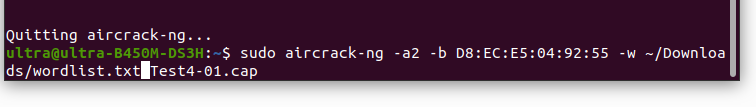
A screenshot of a computer

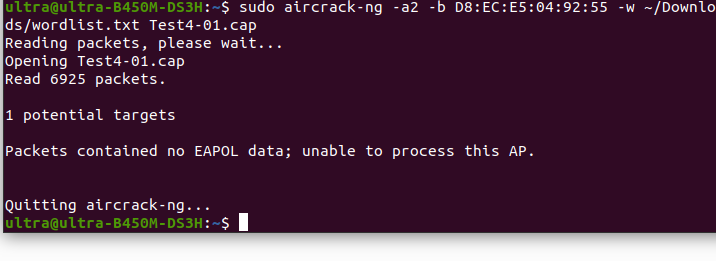
Description automatically generated with medium confidence

1. This is the file created in the previous step. It shows that 2 devices connected to the wireless network while I was scanning it



1. I use the information in the file created by the previous command to attempt to find the password. This is done using a wordlist file that can be of the users choice. I attempted to do this several times but I could not get the program to actually look for passwords and test them





Resources used in this part:

<https://shehackske.medium.com/capturing-and-cracking-wpa-handshake-using-aircrack-ng-d9496f30c7c3>

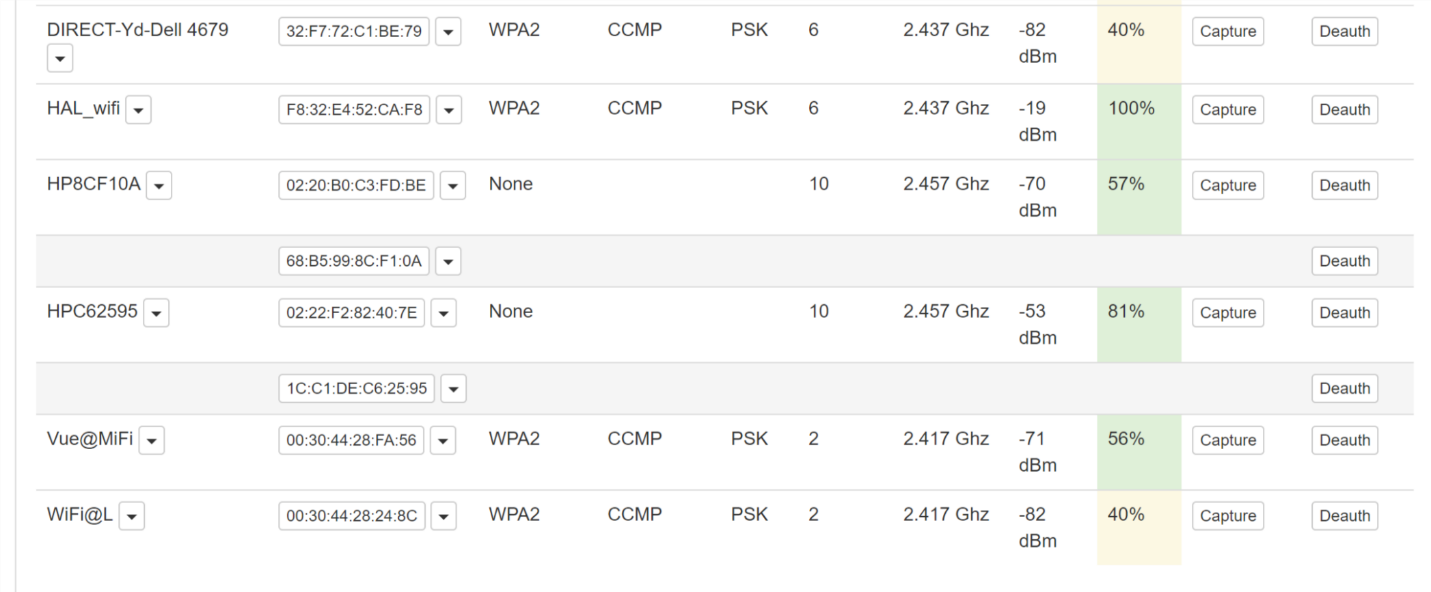
<https://www.youtube.com/watch?v=TreIFFNGMGU>

**Part 2: Cracking a captured WPA handshake (25 pts)**

Attached in Blackboard to this lab is the file ***HAL.cap***. This file contains a captured WPA handshake of one of the HAL corporate clients. Utilizing aircrack-ng in your Kali distribution and the wordlist ***rockyou.txt*** determine the pre-shared key for the Happy Accident Labs wifi access point. **Include screen shots of your activity as well as the clear text PSK.**

**Information you will need to complete this lab:**

A wifi pineapple was used to scan access points and capture the WPA handshake. The below screen capture shows the identifying information for the Happy Accident Labs access point.



Locate the line with the Happy Accident Labs access point – **HAL\_wifi** would be a good guess. Looking across the line you will need to record some key data for later use, the first column is the bssid address which identifies the targeted access point. The second column identifies the type of encryption utilized, in this case it’s **WPA2**. The fourth column indicates the access point is using a pre-shared key. Finally, the fifth column shows the channel number for the communication. In this case its channel 6.

Before running aircrack you will also need to make sure a proper word list is available. You will be conducting a dictionary attack against the encrypted PSK. This means that each word in the word list, which consists of often used passwords, will be encrypted and compared against the encrypted PSK. If the encrypted words match you have found the PSK. The wordlist you will be using is included in the Kali distribution and called rockyou.txt. It is located in the **/usr/share/wordlists** directory. Due to its size it is zipped (rockyou.txt.gz) so you will need to use the command **gunzip rockyou.txt.gz.**

You are now ready to crack the handshake to determine the PSK. You will use aircrack-ng, the format of which is:

**Aircrack-ng –b** <bssid> **-w** <path to wordlist> <path to packet capture file>

Be patient, depending on your computer it may take several hours to determine the correct PSK.

Provide screenshots and the Happy Accident Labs PSK when you turn in the lab.

1. Went to the Bellevue site in my Kali VM and downloaded the HAL.cap Wireshark file

Rectangle

Description automatically generated with low confidence

1. Open the Wireshark file

Graphical user interface, text, application

Description automatically generated

1. Unzip the rockyou.txt file for later use

Text

Description automatically generated

1. Use the provided image to obtain necessary information

Graphical user interface, table

Description automatically generated

1. Run the command

BSSID: F8:32:E4:52:CA:F8

Path to wordlist: ~/Downloads/rockyou.txt (moved to here)

Path to capture file: ~/Downloads/HAL.cap

**Aircrack-ng –b** <bssid> **-w** <path to wordlist> <path to packet capture file>

Command: aircrack-ng -b F8:32:E4:52:CA:F8 -w ~/Downloads/rockyou.txt ~/Downloads/HAL.cap

A screenshot of a computer

Description automatically generated

1. Wait for the program to crack the password

A screenshot of a computer

Description automatically generated with medium confidence

1. After an hour or so, I found the password!

A screenshot of a computer

Description automatically generated with medium confidence

The password is: huskersare#1