Nwachukwu Edumanichukwu

Bellevue University

CYBR 430, Penetration Testing and Incident Response

Professor Kyle Kennedy

March 28, 2023

# 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.

**Response-**

***Note:*** I used my personal router when conducting this test.

To capture a WPA or WPA2 handshake, you need a wireless USB WiFi Adapter. I use Atheros Ar9271, but you can use WIFI Pineapple or Coconut wireless test equipment. On Kali Linux, I choose to use wifite because it’s faster and less complex than the airmon-ng.

On the Kali Linux VM terminal, simply type sudo wifite, press enter and type in your password. This will automatically put your wireless adapter in monitor mode, and you should be able to see lists of ESSID, Channels, encryption type, power, WPS and Number list.

Ctrl+C to stop the scan and proceed to selecting the corresponding num of the target wireless network. Wifite will automatically attempt to capture a PMKID or WPA handshake. It names and saves the data automatically as well.

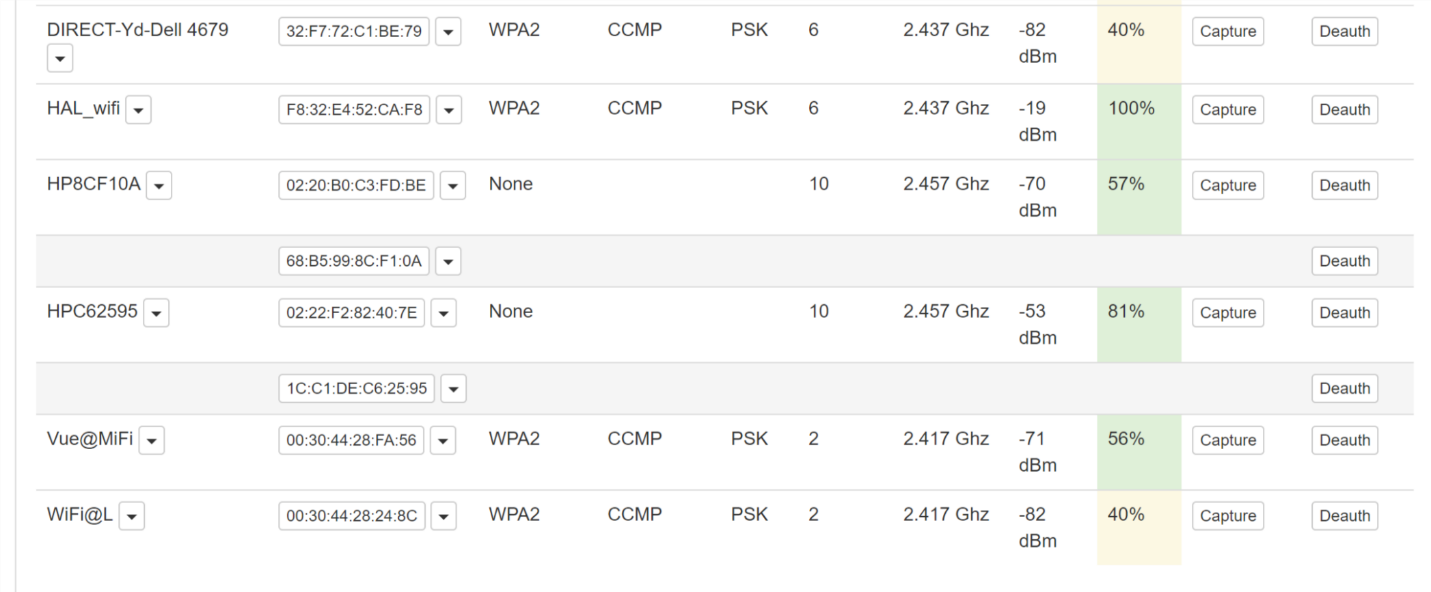


**Part 2: Cracking a captured WPA handshake (25 pts)**

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.

The Happy Accident Labs PSK is huskersare#1

A screenshot of a computer

Description automatically generated with medium confidenceA picture containing graphical user interface

Description automatically generatedA screenshot of a computer

Description automatically generated with medium confidence