CYSE 301: Cybersecurity Technique and Operations

Assignment 5 – Part-2: Wi-Fi Password Cracking

By: Trey Smith

Task C: 20 points

Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

1. Decrypt the lab5wep-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

```
┌──(root㉿kali)-[~/Desktop/VMshare/Lab Resources/WPA traffic]
└─# airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen            37
Total number of packets read        404693
Total number of WEP data packets    142415
Total number of WPA data packets     27852
Number of plaintext data packets       170
Number of decrypted WEP  packets    142415
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
Warning: WDS packets detected, but no BSSID specified

┌──(root㉿kali)-[~/Desktop/VMshare/Lab Resources/WPA traffic]
└─#
```

2. Decrypt the lab5wpa2-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

```
┌──(root㉿kali)-[~/Desktop/VMshare/Lab Resources/WPA traffic]
└─# airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
Total number of stations seen            13
Total number of packets read         10074
Total number of WEP data packets        19
Total number of WPA data packets      2284
Number of plaintext data packets         7
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      2228
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
Warning: WDS packets detected, but no BSSID specified
```

Task D: 30 points

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the last digit of the hash for svatsa is **8**. Thus, I should pick up the file "WPA2-P3-01.cap."

*MD5 of **svatsa** is fe2943715a4e07c670b242559f5974f**8***

```
┌──(root㉿kali)-[~]
└─# echo -n svatsa | md5sum
fe2943715a4e07c670b242559f5974f8  -
```

```
┌──(root㉿kali)-[~/Desktop/VMshare/Lab Resources/WPA traffic]
└─# echo -n gsmit036 | md5sum
f16707c325f79a1cbd1618d8a9d96c0b  -
```

You can find an online MD5 hash generator or the following command to get the hash of a text string,

Last digit of your MD5	Filename
0~3	**WPA2-P1-01.cap**
4~5	WPA2-P2-01.cap
6~8	WPA2-P3-01.cap
9~B	WPA2-P4-01.cap
C~F	WPA2-P5-01.cap

- The above files are zipped in a folder named "Lab Resources (2023 Spring)." You can locate the zipped folder in your VMshare in any Kali Linux VM. Then, extract the zipped file and find the assigned WPA file under the sub-folder "WPA traffic."
- Please note that - it is recommended to copy the zip file to your local folder before extracting the whole file in the VMshare folder.

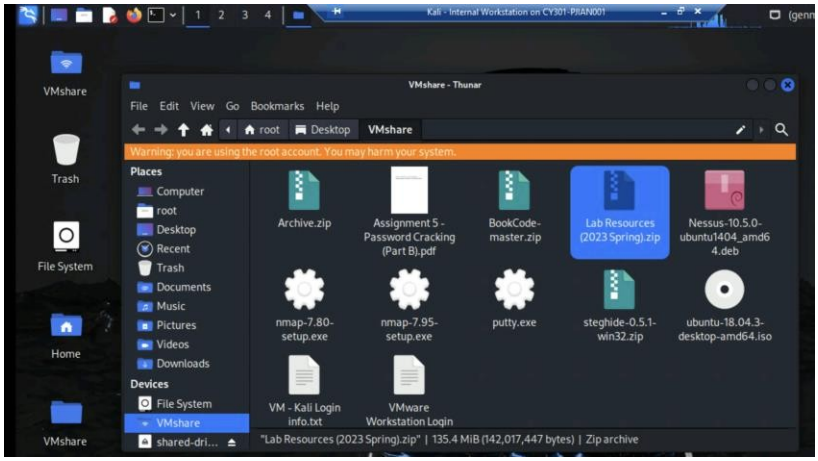

Figure 1 Location of Lab Resource (2023 Spring) in the VMshare folder.

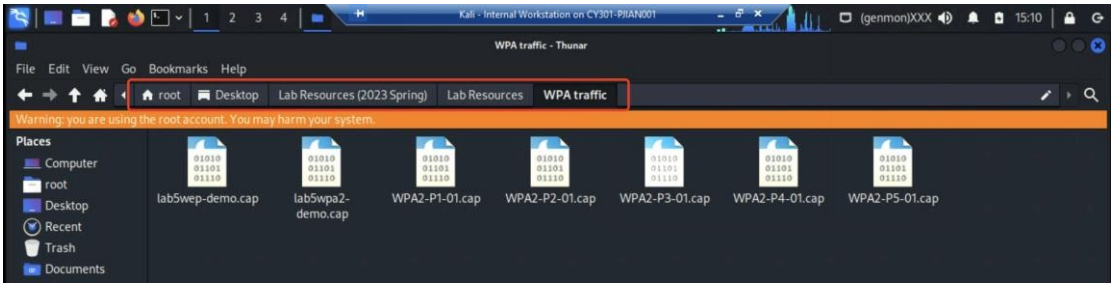

Figure 2 I copied the zip file to the Desktop and then extracted it to access the WPA traffic folder.

Then complete the following steps:

1. Implement a dictionary attack and decrypt the traffic using the correct file based on your last character of md5 hash for your midas name. - 20 points

```
┌──(root㉿kali)-[~/Desktop/VMshare/Lab Resources/WPA traffic]
└─# echo -n gsmit036 | md5sum
f16707c325f79a1cbd1618d8a9d96c0b  -
```

```
Reading packets, please wait...
Opening WPA2-P1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:2F  CyberPHY                  WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening WPA2-P1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:01] 739/10303727 keys tested (1006.20 k/s)

      Time left: 2 hours, 50 minutes, 39 seconds                0.01%

                           KEY FOUND! [ PASSWORD ]


      Master Key     : F1 5F 48 C3 DC 4B E3 2A BE 2E 2D 87 FB 98 28 89
                       30 BC 6F 72 60 96 04 86 46 54 84 B6 24 11 B8 56

      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     : 6B E1 32 DE B3 47 90 E0 E0 C8 ED AC 79 BE 11 29
```

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file (using wireshark). -10 points

```
┌──(root㉿kali)-[~/Desktop/VMshare/Lab Resources/WPA traffic]
└─# airdecap-ng WPA2-P1-01.cap -p PASSWORD -e CyberPHY
Total number of stations seen            12
Total number of packets read           2660
Total number of WEP data packets          0
Total number of WPA data packets        629
Number of plaintext data packets          0
Number of decrypted WEP  packets          0
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets        471
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0
```

Using Wireshark we can find a multitude of things for example

Using these lists of Ips I can use Wireshark to see if there are any communications between these devices and due to the traffic being decrypted, I can see what been sent.

Just doing some digging I have found A certificate being sent over, a server key exchange, and a client key exchange.

I have also found a handshake probably the original three way handshake that I cracked.