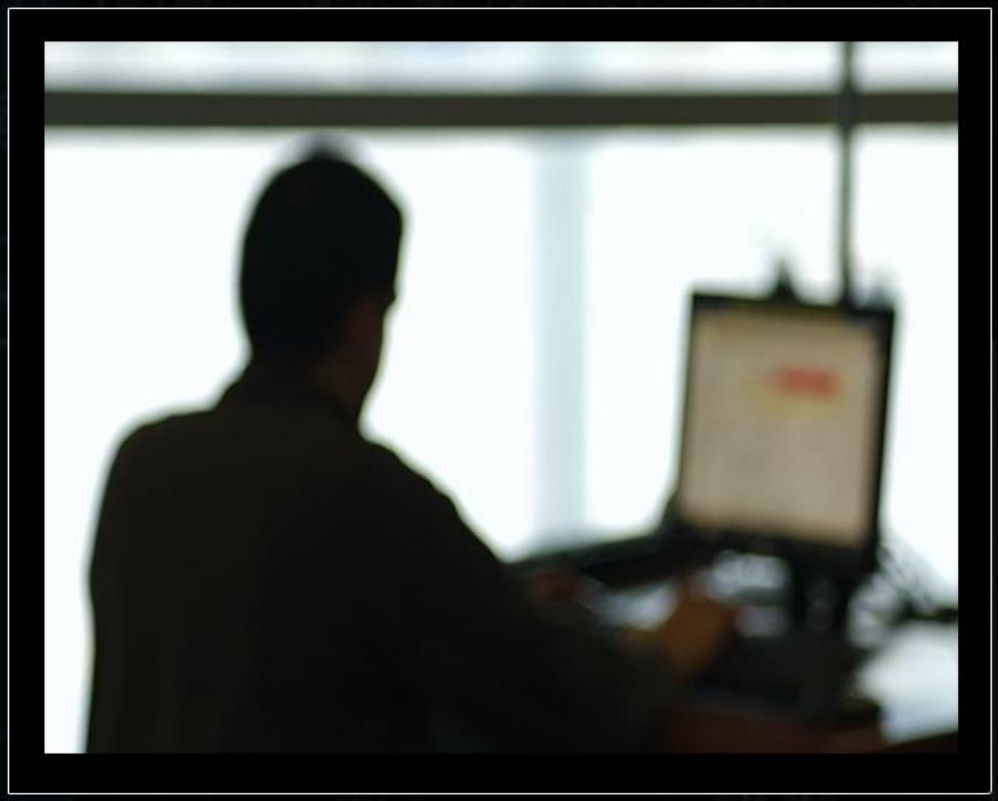
#3

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.

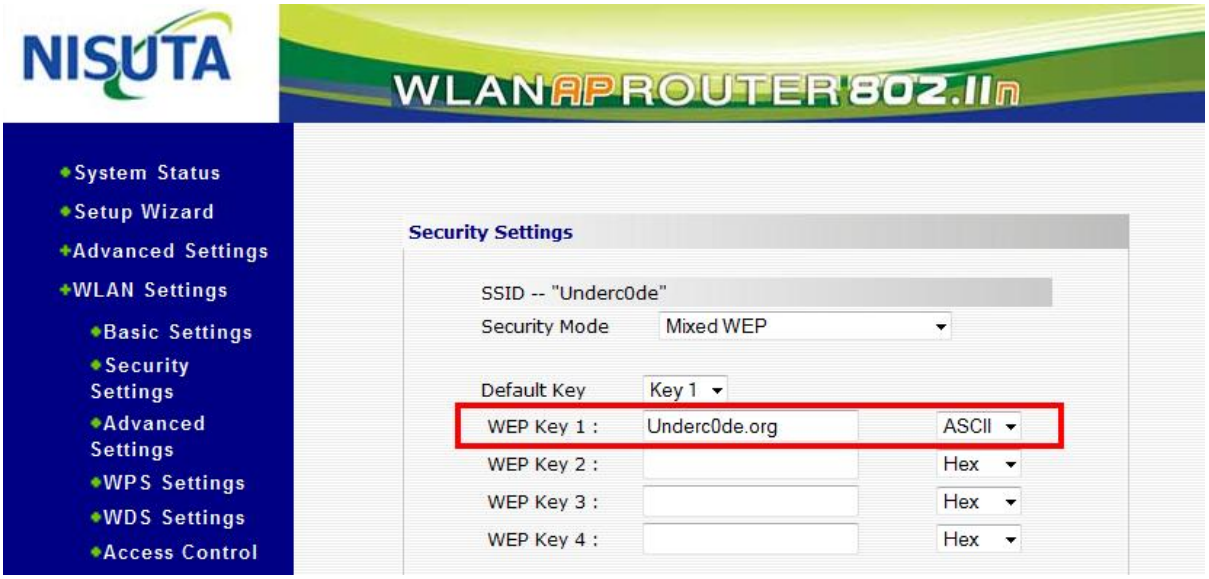
ARP es un protocolo de resolución de direcciones: Es un protocolo TCP/IP usado para convertir una dirección IP en una dirección física, como por ejemplo una dirección Ethernet. Un cliente que desea obtener una dirección envía a todo el que le escuche (broadcasts) una petición ARP (ARP request) dentro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

Extraido 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**



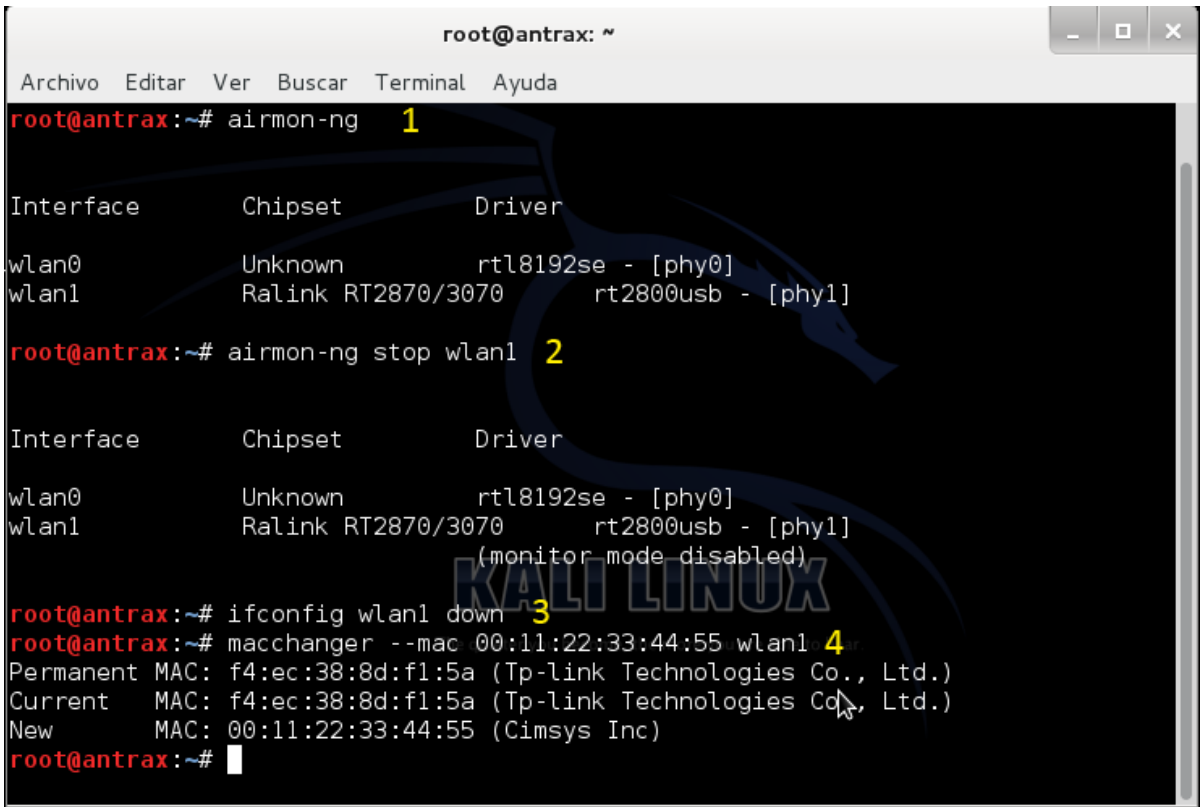
Aclaración general, todos los parámetros colocados de color azul, pueden variar dependiendo del escenario en el que se encuentren. Estos valores son (Interface de red, MAC, Canal, etc)

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:



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

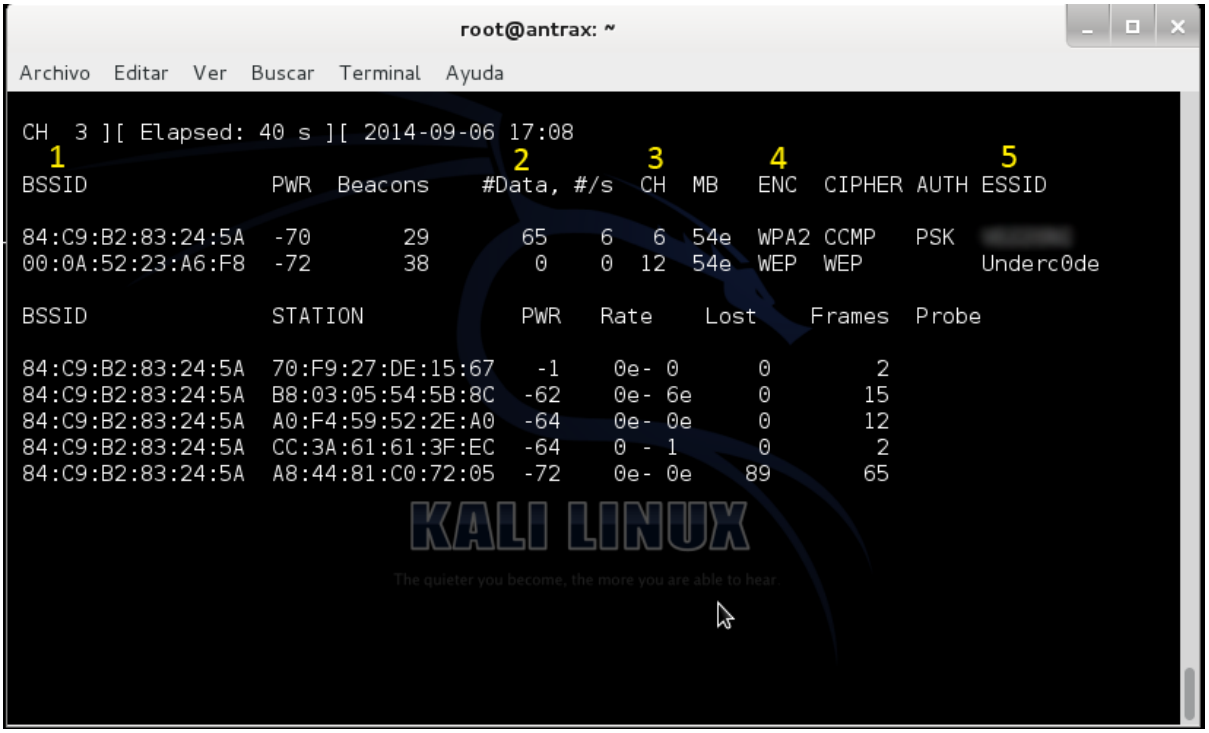
4) Cambiamos nuestra MAC por una más fácil de recordar

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



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.

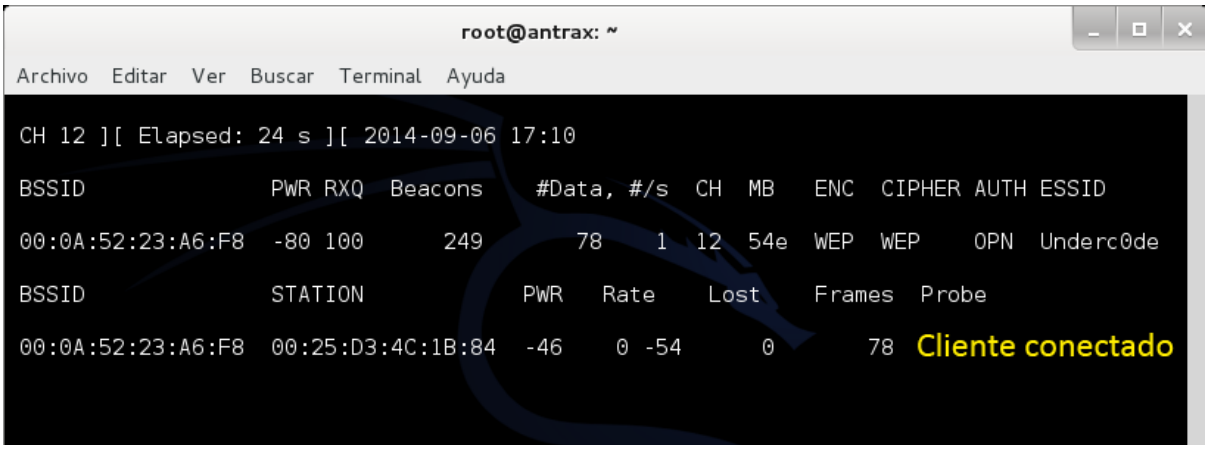
Presionamos la combinación de teclas: **CTRL + C** y esto detendrá el scanneo, permitiéndonos ingresar otro comando.

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.

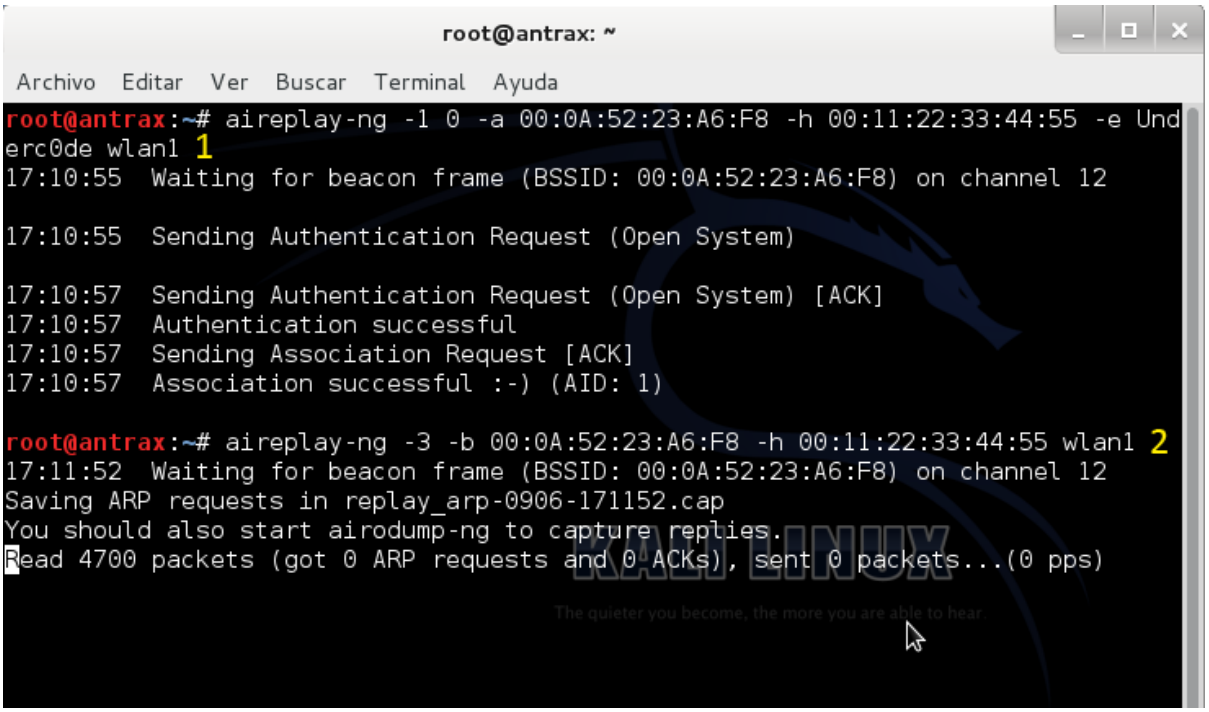


Esta pantalla es muy similar a la anterior, solo que ahora estamos capturando los #Data o IVs que son los que utilizaremos más adelante para romper la clave.
Como se puede ver también, tiene un cliente conectado. Esto es muy favorable, ya que el cliente produce tráfico en la red y facilitará la captura 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.



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.

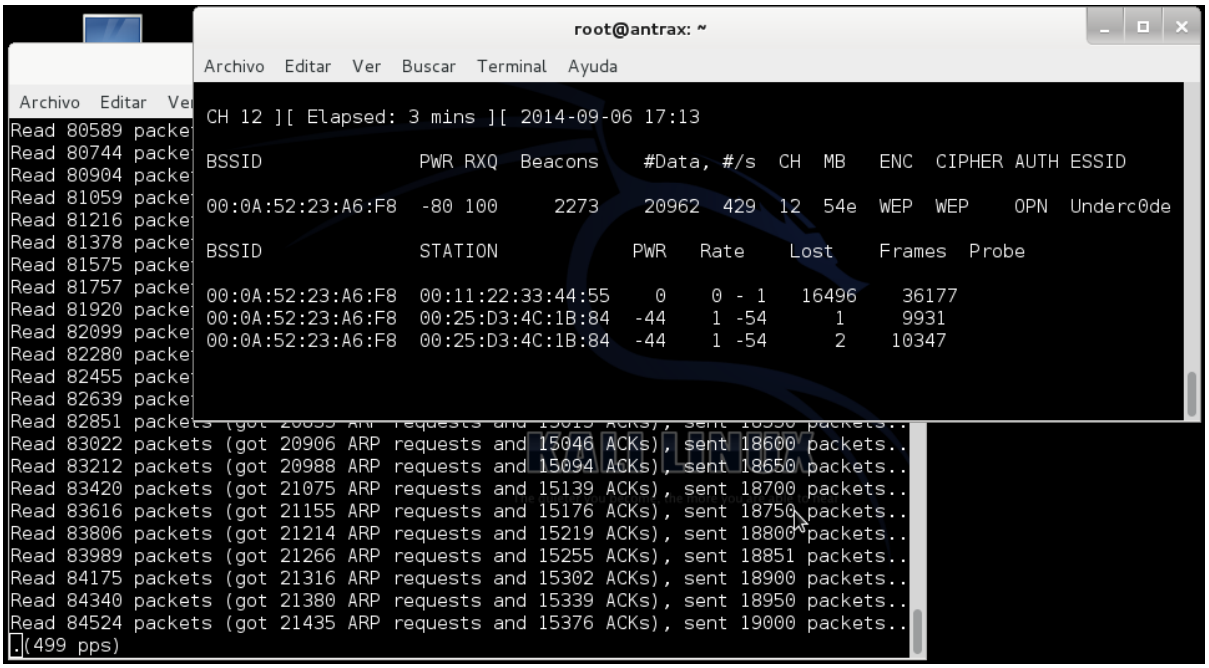
2) Inyectamos tráfico a la red con el siguiente comando

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



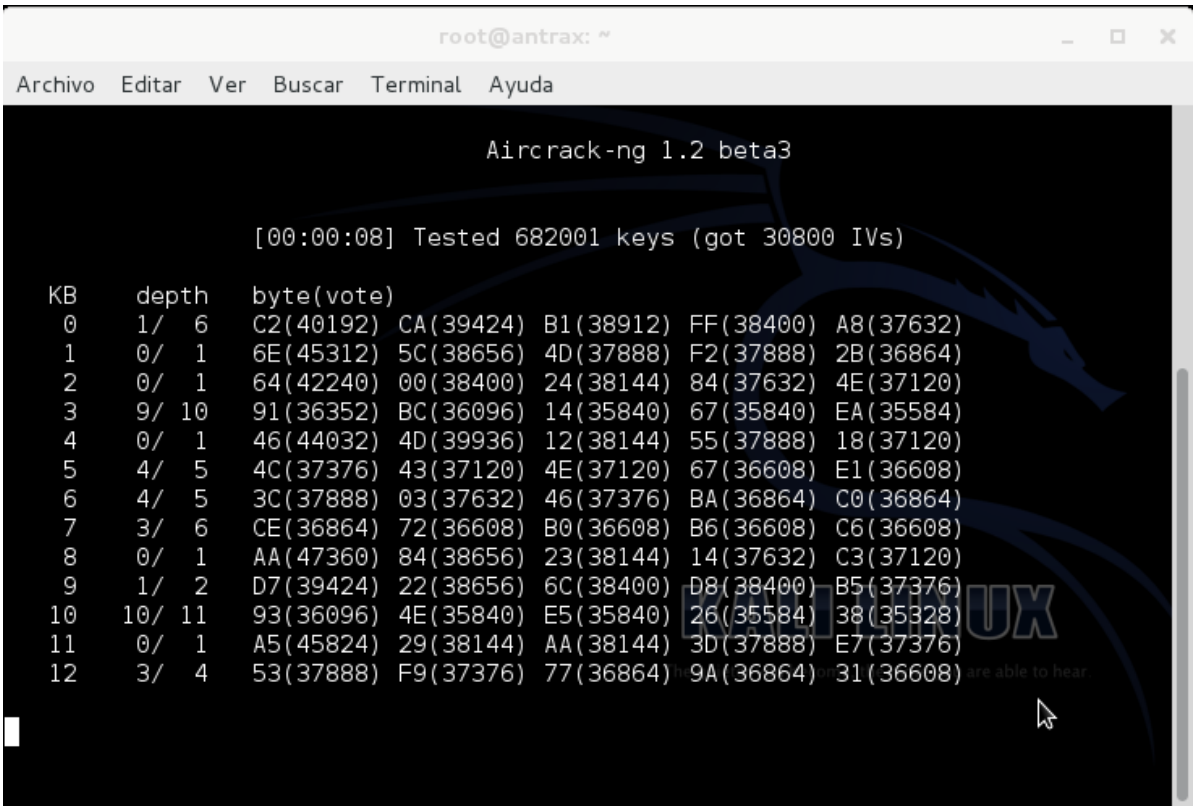
En la imagen se puede apreciar como en la consola de atrás, inyectamos y realizamos el ARP, mientras que en la consola de adelante vemos como incrementan los #Data que necesitamos para romper la pass.

Reventando la contraseña

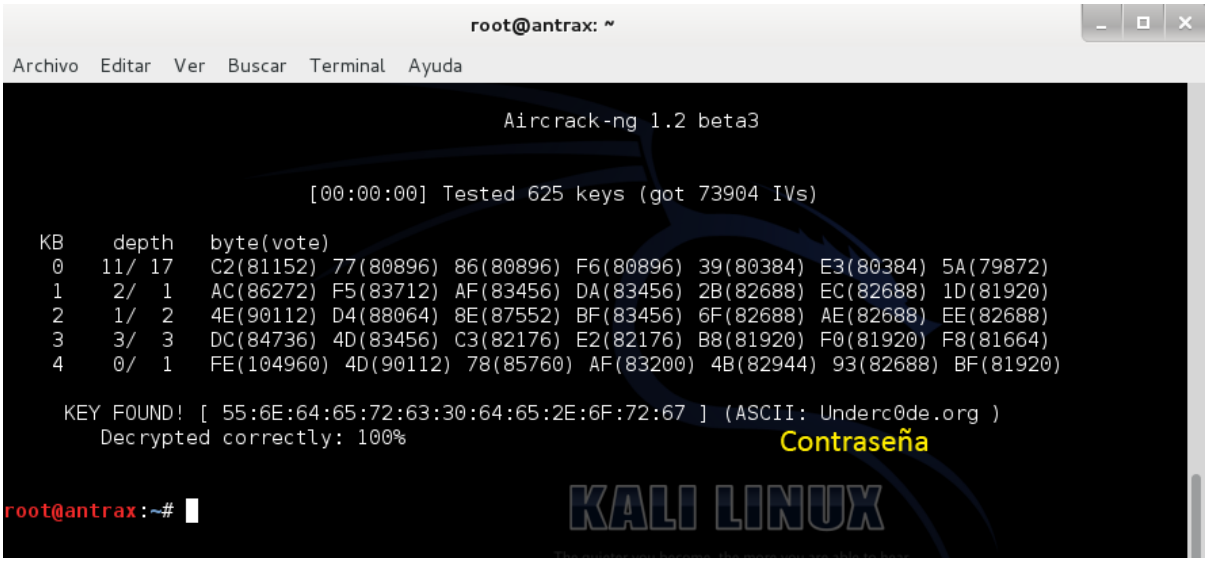
Si llegamos a este paso, es porque todo nos ha salido a la perfección y solo nos queda tomar todos los #Data o IVs capturados y descifrar la contraseña. Para ello ejecutamos el siguiente comando

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.



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



Como podrán ver, hemos obtenido la contraseña!