#4

UNDERCODE

TALLER DE SEGURIDAD WIRELESS

TEMAS

INTRODUCCIÓN TEÓRICA
ASOCIACIÓN A LA RED
CRACKING POR DICCIONARIO
CRACKING CON FUERZA BRUTA
Y MÁS!

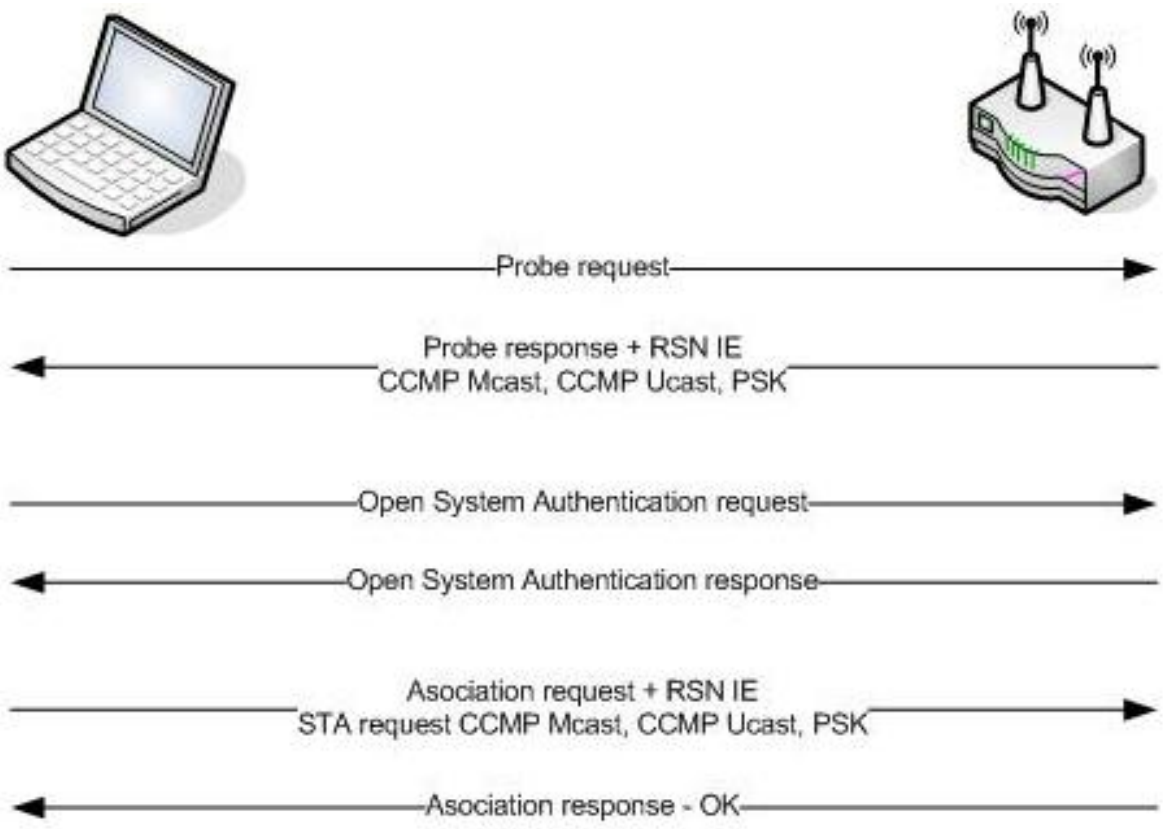
TUTOR

ANTRAX

Introducción

Para poder obtener la clave de una red con cifrado WPA/WPA2, debemos capturar el Handshake de algún cliente y luego desencriptarlo.

Para lo que no sepan lo que es el Handshake se genera en el momento en el que un dispositivo se conecta en una red. La clave pre-compartida puede tener un tamaño de 8 a 63 caracteres, por lo que parece imposible crackear la clave.



Como se muestra en la imagen, el dispositivo envía una solicitud de conexión al router, el router responde pidiendo la clave de acceso, el dispositivo envía la clave de acceso. El router responde a esa autenticación, si es correcta se produce la asociación a la red y el router responde con un OK, es decir, lo asocia a la red.

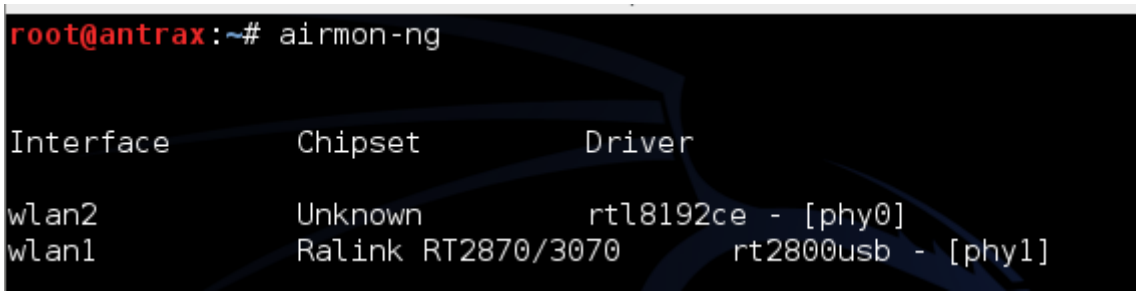
Esta negociación que se produce, es el Handshake (Apretón de manos) y lo que haremos en este taller, será capturarlo y descifrarlo, ya que la contraseña viene cifrada dentro de él.

No hay ninguna diferencia entre el crackeo de redes WPA o WPA2. El método de autenticación es básicamente el mismo. Por lo que las técnicas a usar son idénticas.

Colocando nuestra interface en modo monitor

Lo que haremos ahora será ver el nombre de nuestra interface, para ello tipeamos lo siguiente:

airmon-ng



En mi caso figuran dos interfaces:

Wlan2: La placa de red que tiene mi notebook

Wlan1: Mi USB Wifi externo

Debido a que la placa de mi notebook no sirve para usarla con aircrack, usaré mi USB Wifi externo, es decir, la **Wlan1**

Ahora la pondremos en modo monitor con el siguiente comando:

airmon-ng start wlan1

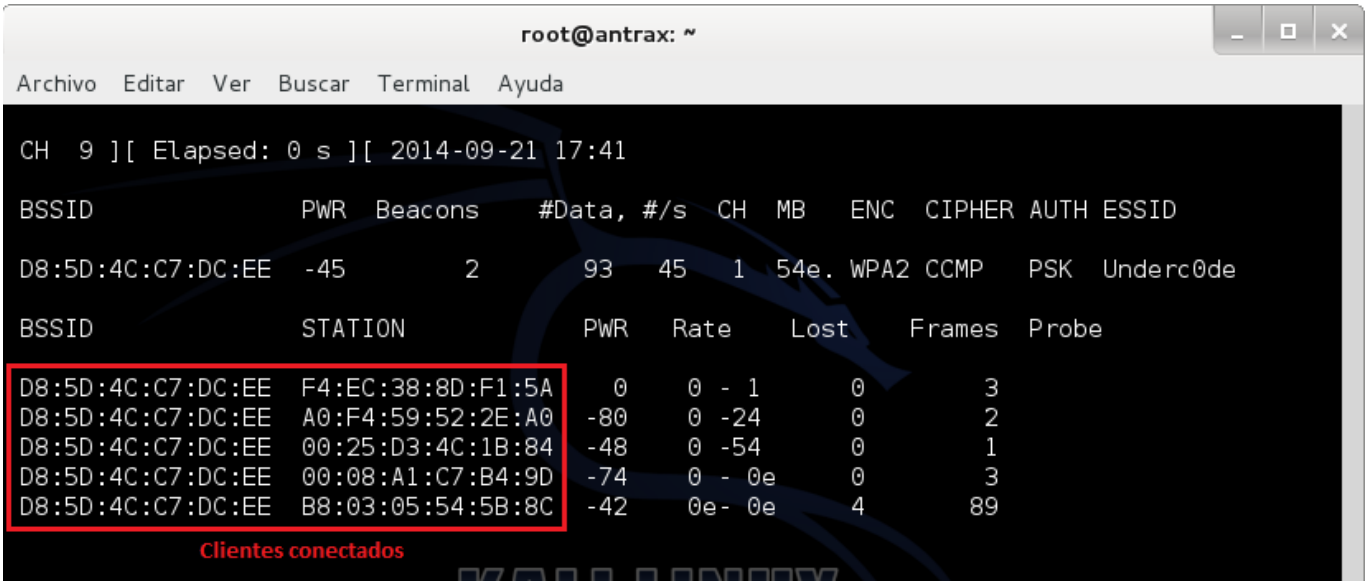
Como muestra la imagen, la coloca en modo monitor

(Monitor mode enablen on **mon0**)

Scanneo de las redes cercanas

Para ver las redes que tenemos cerca, lanzaremos el siguiente comando:

airodump-ng mon0



Como bien dijimos al principio de este taller, el Handshake se genera a la hora de que un cliente se conecta a la red. Es por ello, que nuestro objetivo ahora será tirar a un cliente conectado, y cuando intente conectarse nuevamente, capturaremos ese Handshake.

Lo que debemos recordar de esta consola, son los siguientes datos:

BSSID (MAC del router)

STATION (MAC del Cliente conectado)

CH (Canal)

Frenamos el scanneo con la siguiente combinación de teclas **CTRL + C**

Seguido a esto, colocamos el siguiente comando:

airodump-ng mon0 --channel 1 --bssid D8:5D:4C:C7:DC:EE -w /underc0de

Explicaré brevemente los parámetros de este comando:

mon0 (Nuestra interface en modo monitor)

--channel (Canal)

--bssid (MAC del router al que atacaremos)

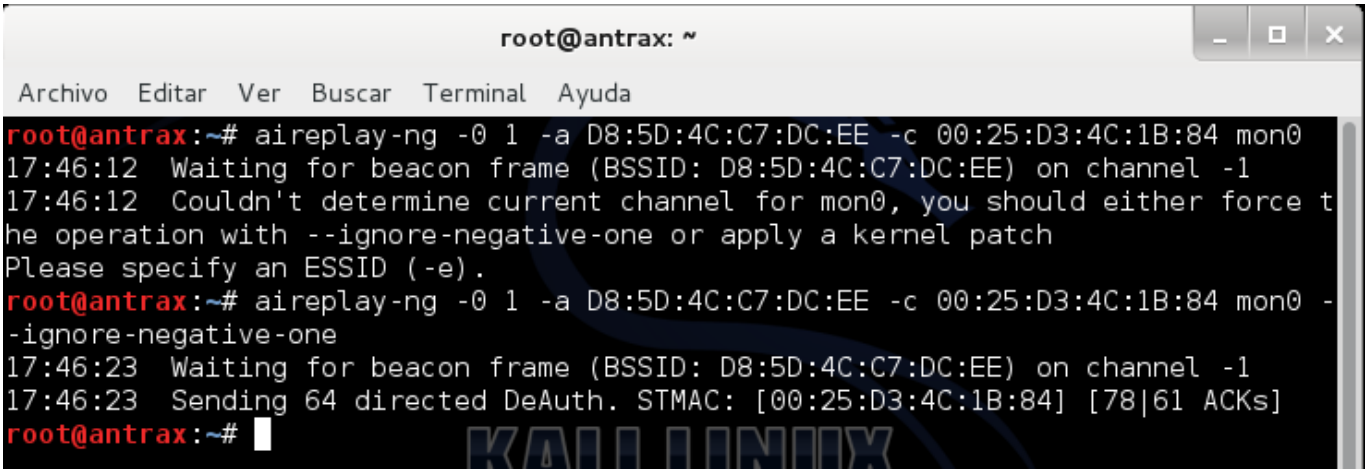
-w (Nombre del archivo en donde se guardará el handshake)

Volveremos a ver la misma pantalla que la anterior, pero esta vez solo observaremos el movimiento que está generando el router al que atraparemos.

Capturando el Handshake

En una nueva consola, procederemos a conectar uno de los clientes conectados para capturarle el Handshake, para ello, tipearemos el siguiente comando:

aireplay-ng -0 1 -a D8:5D:4C:C7:DC:EE -c 00:25:D3:4C:1B:84 mon0



En caso de que al tipear el comando, aparezca un error como el de la imagen, al mismo comando le añadimos **--ignore-negative-one**

aireplay-ng -0 1 -a D8:5D:4C:C7:DC:EE -c 00:25:D3:4C:1B:84 mon0 --ignore-negative-one

Esto sucede porque tenemos que aplicarle un parche a nuestro kernel, pero la forma más rápida es añadiendo la extensión al comando como hicimos.

Al ejecutar el comando, veremos como desconecta al cliente conectado, y en la otra consola podremos ver lo siguiente en la parte superior:

Como podemos observar, aparece el **[WPA handshake D8:5D:4C:C7:DC:EE]**

Eso quiere decir que ya capturamos el Handshake de la red. Ahora podemos cerrar todas las consolas activas e iniciar el proceso de cracking.

Crackeando el Handshake por Fuerza bruta

Para crackear el handshake por fuerza bruta, utilizaremos John The Ripper, el cual es un excelente para este tipo de tareas.

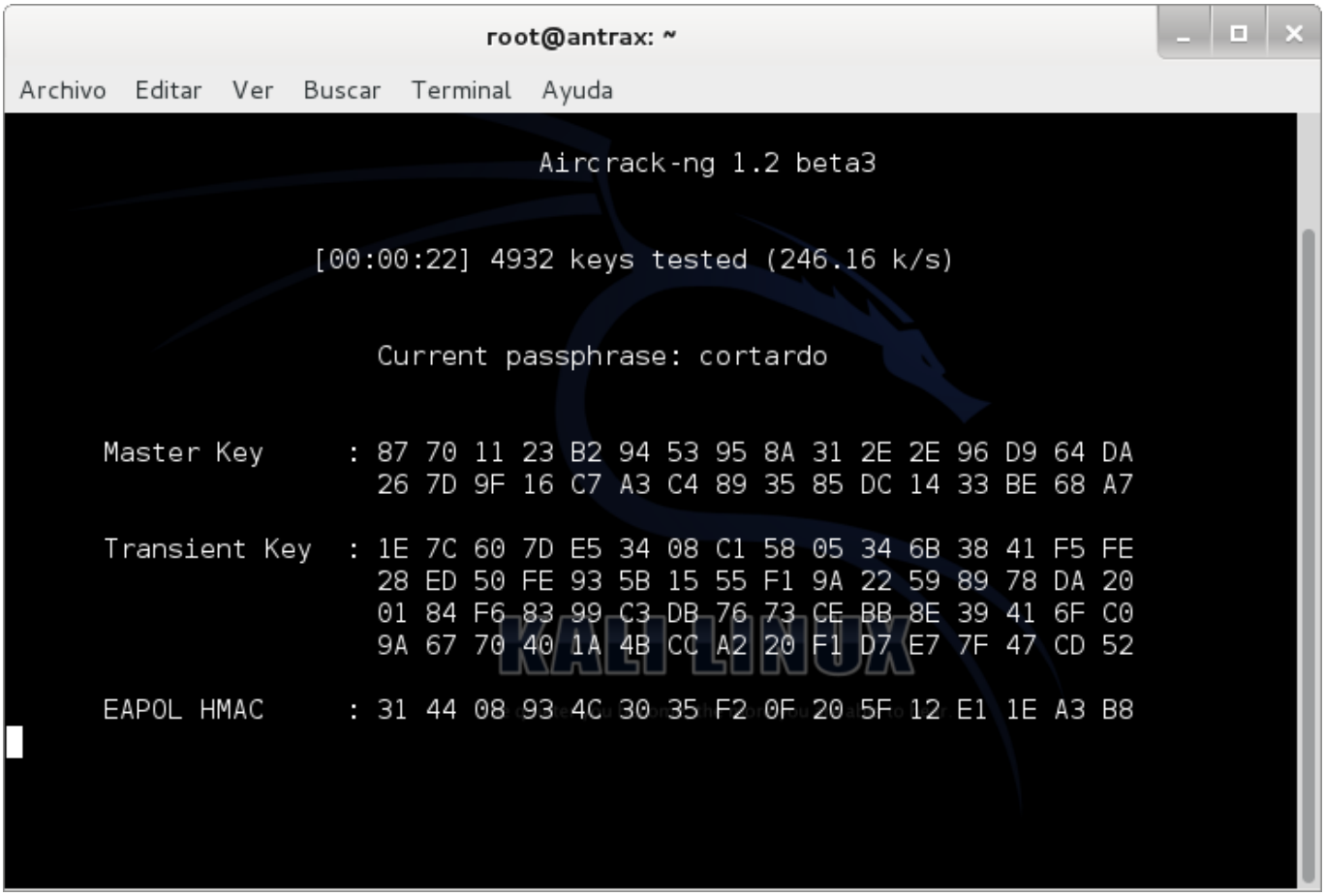
En una consola tipeamos lo siguiente

john –stdout:XX --incremental:YY | aircrack-ng -b D8:5D:4C:C7:DC:EE -w - /underc0de*.cap

En el comando se pueden reemplazar las **XX** por:

alpha (solo letras)
digits (solo números)
alnum (numeros y letras)
all (Todos los caracteres incluidos ",.-#%&)

Las **YY** son los números de caracteres que puede tener la contraseña, si colocamos 8, John the ripper combinará desde 1 hasta 8 caracteres.



Lo malo de esto, es que puede demorar desde minutos a años en sacar una clave. Y depende mucho del hardware que tengamos en nuestra pc.

Crackeando el Handshake por Diccionario

Para poder romper la clave por diccionario, colocaremos en la consola el siguiente comando:

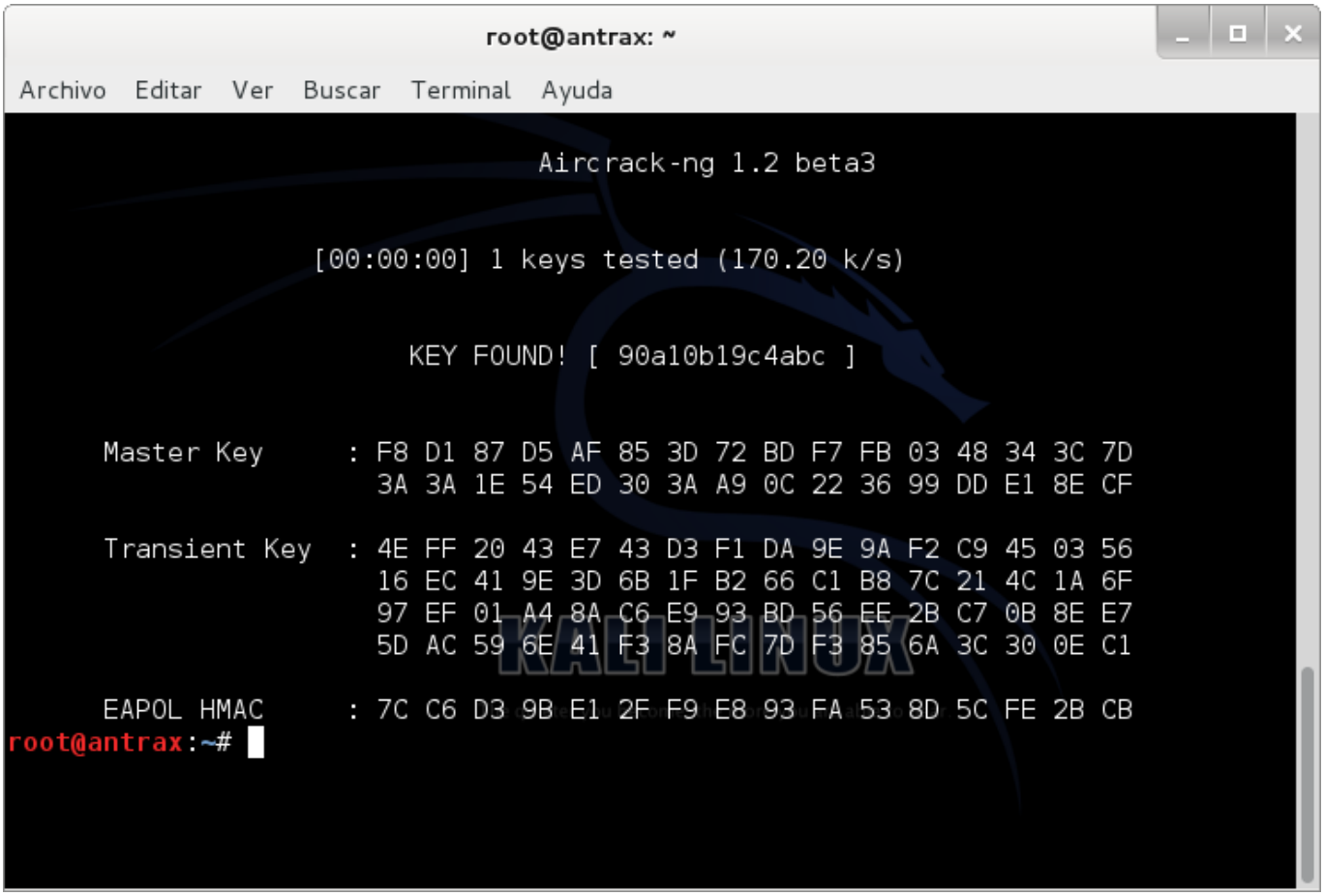
aircrack-ng -w diccionario.txt -b D8:5D:4C:C7:DC:EE /underc0de*.cap

Rapidamente explicaré los parámetros del comando

-w (Nombre del diccionario)

-b (MAC del router)

Y finalmente el **nombre** del Handshake



Como se puede ver en la imagen, en mi caso pudo sacar la contraseña, porque la contraseña se encontraba en mi diccionario, pero habrán casos en los que deberemos probar con varios diccionarios, y aún así quizás no tengamos suerte.