SUITE BACK TRACK 5

– Autentificar redes WEP usando comandos en terminales

Hoy les traigo uno de esos programas que es la delicia de muchos de vosotros. Os recuerdo que este post esta orientado **ÚNICA Y EXCLUSIVAMENTE** a la educación y al aprendizaje del ejecutable. El uso fraudulento que cada cual le quiera dar a esta aplicación es **ÚNICA Y EXCLUSIVAMENTE** responsabilidad suya. Una vez dicho esto, empezamos la tutoria.

Hace falta tener el liveCD de Back track 5 (en adelante BT5) en imagen ISO para que una vez que lo insertemos en nuestro lector de DVD o USB, el ordenador arranque desde él. Si no podeis, entonces teneis que entrar en la BIOS de vuestro sisitema y modificar las órdenes de arranque. Estas cosas son obvias, con lo que no me voy a molestar en explicaros como se hacen. También necesitais una tarjeta que inyecte paquetes, en este caso se ha utilizado una RTL818BvB.

Antes de empezar vamos a aclarar algunos puntos importantes.

Este tuttorial está pensado para que no tengais problemas a la hora de entenderlo, por eso se intentará guiar paso a paso a través de él. Cada número que aparece al lado de cada comando, al final del tutorial es una terminal que teneis que abrir. Si el número se repietiese, es porque el siguiente comando con el mismo número se debe de ejecutar en la misma terminal.

Una vez que teneis todo eso y el ordenador arrancado desde el DVD o el USB, os aparecerá el escritorio de BT5 (Foto 1).

FOTO 1

En la parte superior izquierda de la pantalla aparece un icono con forma de televisión. Pinchad ahí y os aparecerá el terminal desde donde teneis que empezar a colocar comandos. (Foto 2)

FOTO 2

El siguiente paso, es comprobar si teneis la interface en modo monitor para poder capturar paquetes. Para eso, escribís **ifcongif** y os aparecerá los interface que teneis. En mi caso tengo estós. (Foto 3)

FOTO 3

Una vez hecho esto, comprobamos si alguna de ellas está en modo monitor. Para ello escribís **iwconfig** para verlo. En mi caso si que está en modo monitor. (Foto 4)

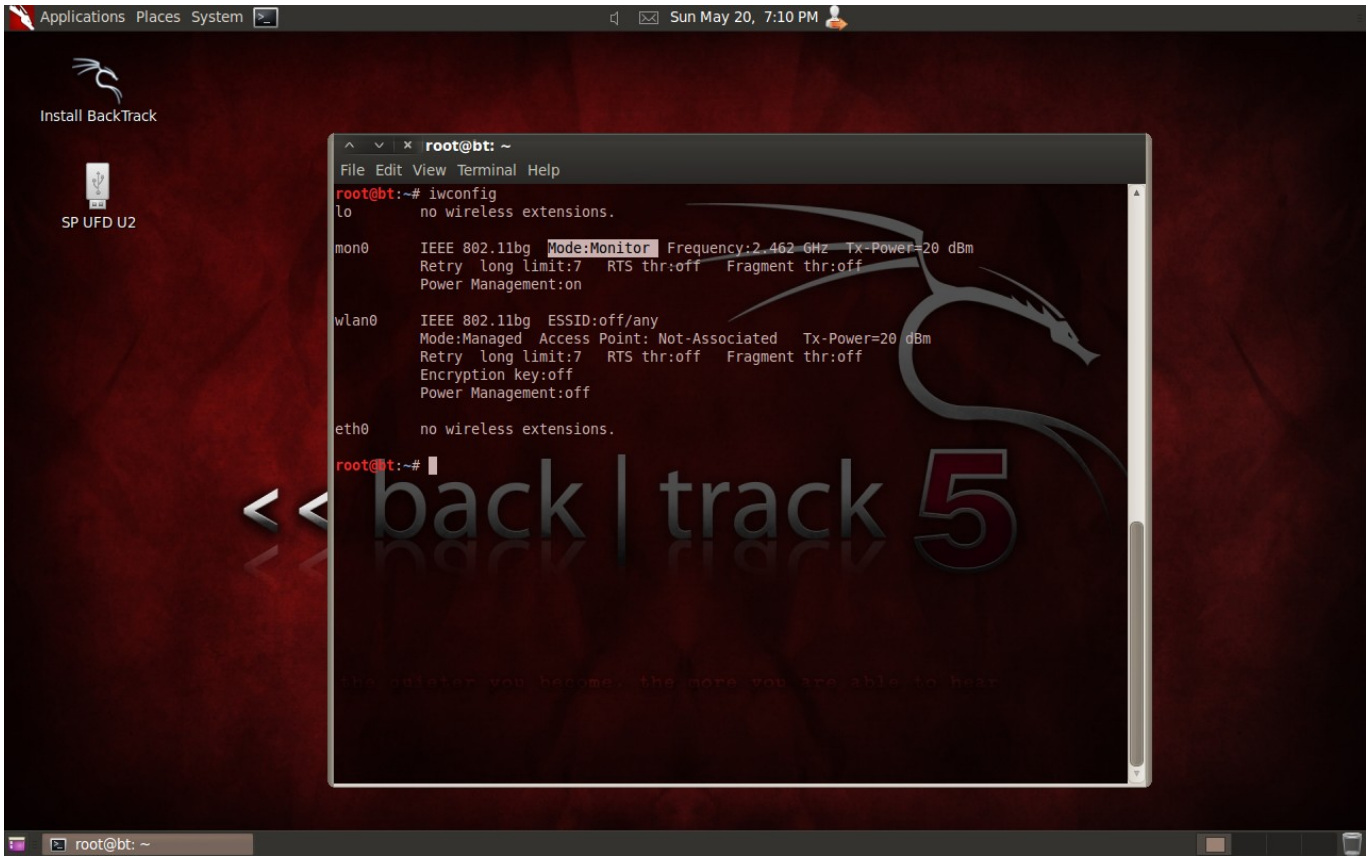

FOTO 4

Bien, si no la ves no te preocupes, ya que la puedes poner tú, siempre y cuando tu tarjeta de red soporte esta función. De todas maneras hay varias formas de cambiar tu interface a modo monitor. Yo uso el siguiente comando: **airmon-ng start mon0**, también lo puedes hacer de la siguiente manera:

airmon-ng stop <tu interface>, esto lo que hace es que al aplicar al comando el parámetro **stop**, conseguimos desactivar la interface para que puedas después colocarla en mono monitor. En mi caso sería **airmon-ng stop eth0**.

airmon-ng start <tu interface>, esto lo que hace es que al aplicar al comando el parámetro start, conseguimos poner la tarjeta en modo monitor. En mi caso sería **airmon-ng start mon0**, ya que estoy usando el driver RTL818BvB. En vuestro caso será otra.

Una vez hecho este paso previo, ya podemos sniffar los paquetes de la red wireless a la que tenemos pensado acceder y así empezar a autentificar esar red.

Una vez tenemos todo, empezamos la tarea. Como nota os puedo indicar que para borrar la pantalla en este sistema operativo, basta con teclear **clear** y toda la pantalla desaparecerá. Es el equivalente a **cls** que se usa en Windows cuando accedemos al simbolo del sistema. Pues bien, al ataque. Para saber cuantas redes tenemos a nuesttro alrededor, en la terminal pulsamos el siguiente comando: **airodump-ng mon0** (para facilitar la explicación, pongo mi interface, pero en vuestro caso teneis que colocar la vuestra, que lo tengais presente). Para parar la búsqueda pulsais Ctrl+C y para de buscar. Cuando lo tengais claro, debes de apuntar tres datos importantes de esa red: el BSSID, el canal (CH) y el ESSID. Os aparecerá una pantalla así. (Foto 5).

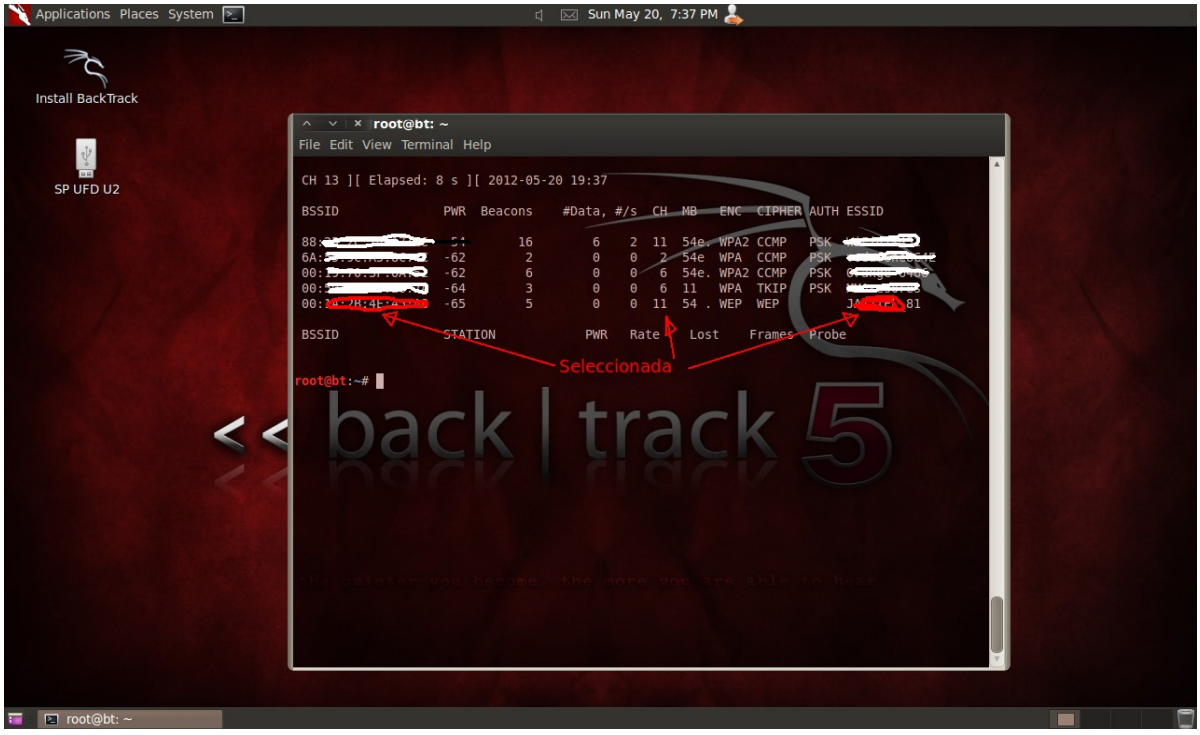

FOTO 5

Una vez tengasis los datos anteriores, escribimos lo siguiente:

airodump-ng mon0 - w <nombrefichero> - channel <canal>

en donde **- w** es el parámetro para crear el archivo en donde se guardarán los datos capturados. Podeis darle el nombre que querais; **- channel**, es el número de canal en donde se encuentra la red que estais autentificando. Muchas veces puede ocurrir que os de error a la hora de colocar estos parámetros, pero normalmente suele ser porque falta o sobra algún guión.

Una vez hecho esto, abrimos otro terminal y ejecutamos el siguiente comando:

aireplay-ng -1 0 mon0 -e <essid de la red a atacar> -a <BSSID de la red a atacar> -h <tu MAC es decir tu BSSID>

en donde **-1** es el tipo de ataque que utiliza aireplay; **0** es el numero que indica cada cuanto hace una falsa autentificación, puedes utilizar caulquier cantidad, éste en concreto son infinitos ataques; **-e** es el nombre de la red a atacar; **-a** la BSSID de la red a atacar normalmente viene expresada en números y letras mayusculas agrupadas de dos en dos con un total de 12; **-h** tu BSSID o tu MAC.

En otro terminal, escribimos el siguiente comando:

aireplay-ng -3 mon0 -b <BSSID de la red a atacar> -h <tu MAC es decir tu BSSID> -x 300

en donde **-3** es el tipo de ataque que utiliza aireplay; **-b** es el BSSID de la red a atacar para desautentificarla; **-h** vuestra MAC o BSSID y **-x** que es un parámetro que utiliza aireplay para ejecutar el ataque y **300** que es un ratio.

Una vez tengamos todo esto, dejamos trabajar a los comandos. La rapidez de la desautentificación dependerá de lo larga que sea la key found, de los caracteres que tenga y de la mezcla de los mismos. Puede tardar entre 10' o días. Pero para estar seguros de que el ataque ha sido un éxito, en la columna AUTH debe de aparecer OPN. (Foto 6)

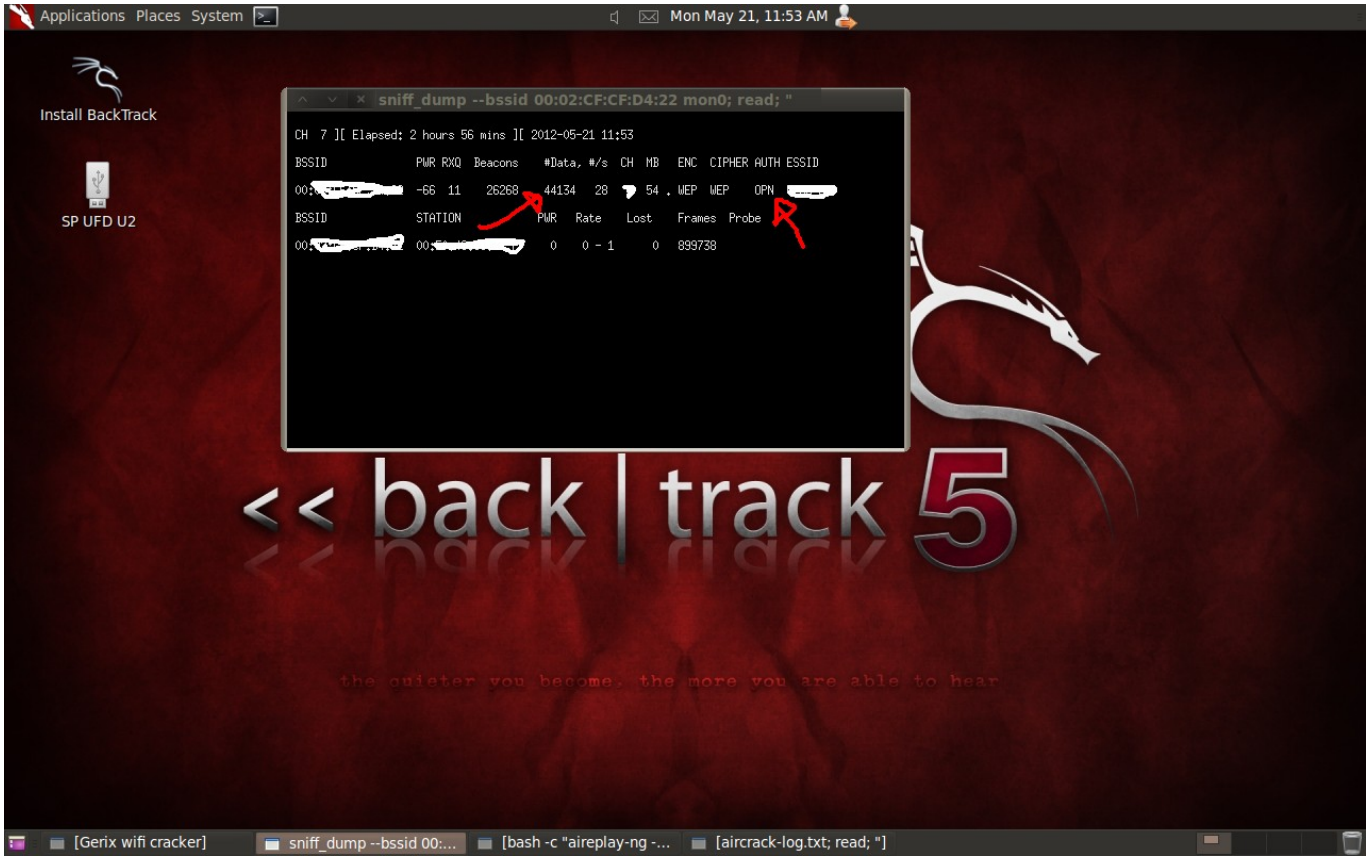

FOTO 6

Abrimos otro terminal y es en este en donde sacaramos la key found de la red. Para ello escribimos:

aircrack-ng <nombrefichero>

acordaros que el <nombrefichero> se lo dimos la 2ª vez que usamos airodump-ng y después del parámetro **-w**.

Para ver el nombre del fichero, debeis de escribir en un terminal el siguiente comando:

ls -la

y os aparecera un fichero con la extensión **.cap**, es decir en mi caso sería **nombrefichero.cap**, y cuando tengais hecho todos estos pasos, se tendrá que ver una pantalla como esta (Foto 7), en donde se puede ver en la columna inferior izquierda como trabaja el aireplay y en la columna de la derecha como ha desencriptado la key found, tanto en hexadecimal como en ASCII. Daros cuenta que en la columna superior izquierda los datos de #Datas van por los 64000, pero con 5000 debe de haber suficientes. Esto demuestra que la clave de esta red es larga y compleja.

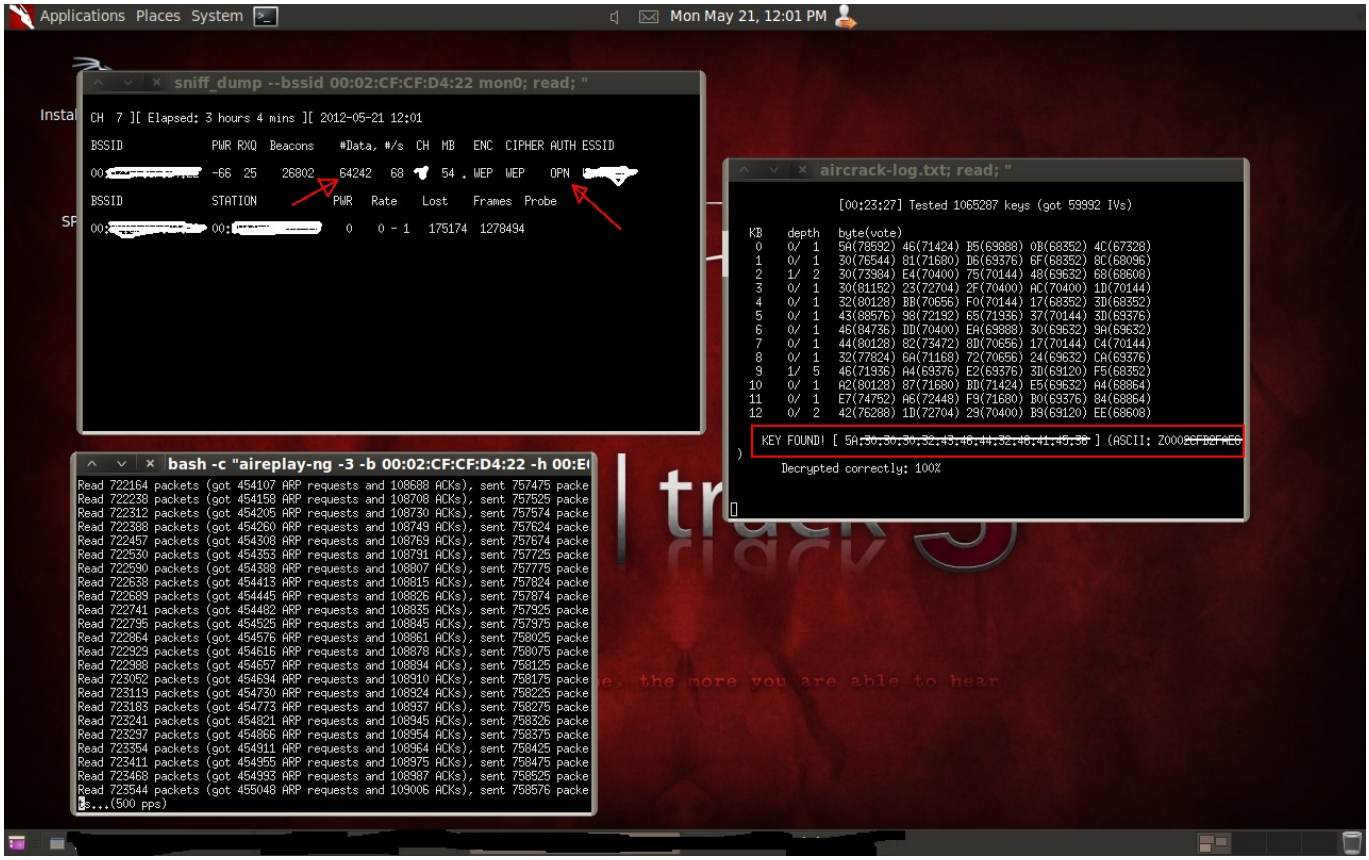

FOTO 7

Ahora os hago todo el desarrollo al completo.

1-> ifconfig
1-> iwconfig
1-> airmon-ng stop <tu interface>
1-> airmon-ng start <tu interface>
2-> airodump-ng mon0
2-> airodump-ng mon0 - w <nombrefichero> - channel <canal>
3-> aireplay-ng -1 0 mon0 -e <essid de la red a atacar> -a <BSSID de la red a atacar> -h <tu MAC es decir tu BSSID>
4-> aireplay-ng -3 mon0 -b <BSSID de la red a atacar> -h <tu MAC es decir tu BSSID> -x 300
5-> ls -la
6-> aircrack-ng <nombrefichero>

Os recuerdo que cada número delante de cada comando, indica el número de terminal en el que hay que ejecutar los comandos. ¿Fácil eh?. Tened en cuenta también que a mí me funciona así, pero hay infinidad de formas de ejecutar estos comandos. Hay que tener muy claro cual es cada cual y para que sirve cada uno, y cuando lo sepais pues podreis usarlos de la mejor manera que veais.
Bueno pues ahora a disfrutar y a navegar. Espero que este tutorial os hay sido de utilidad.