Averiguar clave WEP con Linux Back Track (Diciembre 2009)

I. López Espejo

En este tutorial se muestra cómo averiguar una clave WEP de una red inalámbrica que use este tipo de cifrado. Lo único que necesitamos es un ordenador con tarjeta de red con alguna interfaz wireless y alguna distribución reciente de Linux Back Track, especial para auditorías de seguridad.

I. Procedimiento

Una vez hayamos grabado la imagen descargada de Linux Back Track en un CD, preparamos el ordenador para que arranque desde CD reiniciándolo con el disco dentro del lector (si es necesario, entraremos en la BIOS del sistema presionando la tecla *Supr* nada más encender el PC o, si es un Mac, directamente dejaremos pulsada la tecla *C* con el disco dentro para que arranque desde él). Una vez iniciado Linux Back Track (si nos pide login y password teclearemos *root* y *toor* respectivamente) seguiremos los siguientes pasos.

1. Abrimos una ventana de consola y escribimos el siguiente comando a fin de averiguar el nombre de la interfaz wireless de nuestro adaptador: `iwconfig`. Dicho nombre de interfaz se corresponderá con aquel de la izquierda tal que presente información sobre la interfaz y no la frase `no wireless extensions`. Información relevante para nuestro propósito será la correspondiente con `Mode` y con `Access Point`. Supongamos que nuestra interfaz se llama, de ahora en adelante, `eth1`. Cualquier operación que realicemos sobre la misma se traducirá en la agregación del nombre al final de cada comando, por lo que resulta imprescindible.
2. Ocultaremos nuestra MAC con el siguiente comando: `macchanger –m 11:22:33:44:55:66 eth1`. Podemos sustituir la MAC del ejemplo, `11:22:33:44:55:66`, por cualquier otra si queremos. Y, como vemos, al final de la sentencia habremos de indicar sobre qué interfaz del adaptador estamos operando para la realización del cambio de MAC.
3. Activamos la tarjeta en modo monitor con el siguiente comando: `airmon-ng start eth1`.
4. Comprobamos que se han realizado correctamente los cambios: `iwconfig`. En la nueva configuración debe figurar `Mode: Monitor` y `Access Point: 11:22:33:44:55:66`. Las tarjetas de Broadcom suelen dar problemas, figurando `Access Point: Invalid`. No obstante, por mi experiencia personal, si eso es así, podemos continuar con el siguiente paso sin preocuparnos por ello.
5. Con el siguiente comando comprobamos si existen redes inalámbricas en el entorno cuyas claves WEP podamos desencriptar: `airodump-ng eth1`. A continuación se irá desplegando un listado con las redes alcanzables disponibles. Debemos fijarnos en las redes cuya encriptación y cifrado figure como WEP y, a ser posible, que no se requiera de autenticación o esta figure como abierta (OPN). Estas son las redes potenciales de las que podremos averiguar, lógicamente, su clave WEP. Seleccionaremos nuestras redes de interés anotando los siguientes datos: `ESSID` (Nombre de la red), `BSSID` (Dirección MAC del punto de acceso a la red) y `Channel` (Canal de transmisión de la red). Una vez seleccionadas nuestras redes potenciales, presionaremos *Ctrl+C* para finalizar la búsqueda.
6. Con nuestra tarjeta ya configurada en modo monitor, captaremos paquetes de una red determinada (de la red de la que queremos averiguar la clave WEP) mediante el siguiente comando: `airodump-ng –d BSSID --channel Canal --write Pass eth1`, donde `BSSID` lo habremos de sustituir por la dirección MAC del punto de acceso a la red de la que queremos obtener su clave WEP, `Canal` se corresponderá con el número anotado previamente de canal de transmisión de la red en cuestión y donde `Pass` es el nombre del fichero donde queremos que se almacenen los datos procedentes de la captura de paquetes de dicha red. Sería suficiente con indicar el canal pero, hay casos en los que por el mismo canal captamos más de una red, por lo que si queremos particularizar el ataque sobre una en concreto indicamos también su `BSSID`. No obstante sería correcto capturar datos de paquetes de las distintas redes confluyentes en un mismo canal pero no lo recomiendo. Mi experiencia fue que de la red de mi interés apenas se recibían datos y sí de otra. En principio, no habría problema, pues espero a tener suficientes paquetes de la red de interés. No obstante, al ser un SO live, la memoria está muy limitada y puede que paquetes de otras redes que no son de nuestro interés la saturen enseguida tirando todo el trabajo a la basura, por lo que es recomendable, por una mayor eficiencia, usar el anterior comando así.
7. Abrimos una nueva ventana de consola. Con el programa `aireplay` procederemos con la reinyección. Esto fomenta el incremento de recepción de datos procedentes de la red atacada al, por ejemplo, intercambiar paquetes ARP o los propios generados por un proceso de autenticación. No es imprescindible, pero puede agilizar el proceso. Recomiendo consultar

la ayuda del programa y ver todas las opciones, esto es, con el comando `man aireplay-ng`. Aquí van un par de propuestas: `aireplay-ng -1 Interv –e ESSID –a BSSID –h Nuestra MAC eth1`, donde `Interv` es un número entero mayor o igual a cero que especifica en segundos el intervalo esperado para la repetición del proceso, `ESSID` es el nombre de la red atacada, `BSSID` la MAC del punto de acceso a la red, siendo `Nuestra MAC` la dirección explícita en nuestro `macchanger` (`11:22:33:44:55:66` en este caso). O también, por ejemplo: `aireplay-ng -3 –e ESSID –a BSSID –h Nuestra MAC –x P/s eth1`, donde la opción `-3` indica en este caso que se trata de la realización de peticiones ARP, siendo `ESSID` el nombre de la red atacada, `BSSID` la MAC del punto de acceso a la red, siendo `Nuestra MAC` la direción explícita en nuestro `macchanger` y donde `P/s` indica los paquetes ARP generados por segundo.

8. Una vez observemos en la primera ventana de consola de todo el proceso que poseemos de la red atacada, al menos, en torno a 50000 paquetes de datos (vectores de inicialización o IV's), lanzaremos en la segunda ventana de consola el siguiente comando: `aircrack-ng Pass-01.cap`. Este último programa se encarga de intentar desencriptar de los vectores de inicialización la clave WEP. Si todo va con éxito, aparecerá `Key Found!` y la clave. Si no, volverá a reintentar la desencriptación mediante la relectura del fichero una vez se haya incrementado el número de vectores de inicialización observados. Notar que `Pass` se corresponde con el nombre del fichero que indicamos en el paso 6.