TUTORIAL DE AIRCRACK-NG

Taller Realizado en FLISOL Los Ángeles

Abril 25 de 2009.-

Paolo Norambuena

paolo.norambuena@gmail.com

AIRCRACK-NG

Esta es una guía con fines ***educativos*** para el uso y manipulación de Aircrack-ng sobre las distintas distribuciones de Linux. Se explicará desde su instalación en sistemas como Mandriva, Ubuntu, Debian, OpenSuse y SlackWare para que posteriormente no existan dudas sobre ninguna distribución.

En primer lugar debemos tener instalado en nuestro sistema el Driver del Fabricante de nuestra tarjeta de red, ***aircrack-ng*** **no funciona con drivers emulados por** ***ndiswrapper.***

Instalando Aircrack-ng

En este apartado instalaremos aircrack-ng en las distintas distribuciones comenzando por Ubuntu.

Ubuntu.

$ sudo apt-get install aircrack-ng

Mandriva

urpmi aircrack-ng

OpenSUSE

Descargar:
ftp://ftp.pbone.net/mirror/packman.iu-bremen.de/suse/11.0/SRPMS/aircrack-ng-1.0rc3-0.pm.1.nosrc.rpm
Instalar haciendo Doble Click al paquete una vez descargado.

SlackWare

Descargar
http://repository.slacky.eu/slackware-12.2/security/aircrack-ng/1.0rc3/aircrack-ng-1.0rc3-i486-1dd.tgz

Una vez descargado por consola (terminal – konsole, etc), ejecutar

installpkg aircrack-ng-1.0rc3-i486-1dd.tgz

Paquetes complementarios.

Una vez instalado aircrack-ng puede ser necesario la instalación de un paquete adicional por lo cual descargaremos ***IW,*** que es un complemento para poner nuestra tarjeta inalámbrica en modo monitor.

según la distribución será necesario actualizar la librería **libnl**

$ sudo apt-get install libnl1* (ubuntu, debian)

 # urpmi -a libnl (mandriva)

Instalada y/o actualizada la librería procedemos a descargar iw.

wget http://wireless.kernel.org/download/iw/iw-0.9.13.tar.bz2
tar jxvf iw-0.9.13.tar.bz2
cd iw-0.9.13
make
#make install

Y de esta forma ya tenemos aircrack-ng y su componente para poner en modo monitor nuestra wireless.

Ahora solo nos queda empezar a crackear.

Crackeando redes.

Ahora empezamos nuestro trabajo, lo que se realizó anteriormente solo se hace una vez, que es para instalar y configurar de buena forma nuestra suite, lo que se realiza siempre es lo que a continuación se detalla.

Para quienes creen que cambiar su mac es necesario, pueden hacerlo asi

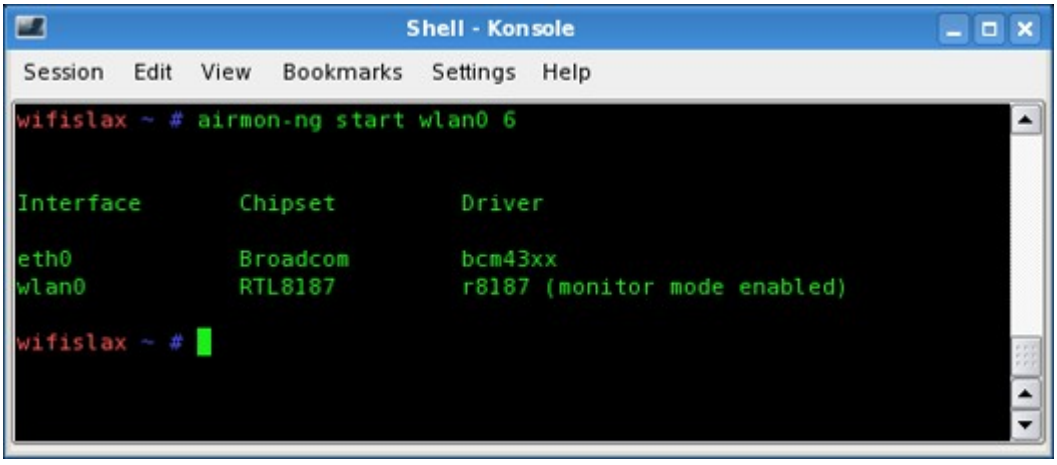
```
macchanger -m 00:11:22:33:44:55 wlan0
```

Aviso: Las direcciones mac SIEMPRE deben iniciar con 00

Airmon-ng.

Airmon-ng es parte de la suite de aircrack-ng la cual permite crear la interfaz ***mon0*** en modo monitor. Su utilización es la siguiente

 # airmon-ng start wlan0 (o el nombre de la interfaz que puede ser wlan0, eth1, etc)



En caso de que nos muestre un error podemos utilizar iw que instalamos anteriormente.

 # iw dev wlan0 interface add mon0 type monitor

Ya tenemos el primer paso completo.

Airodump-ng

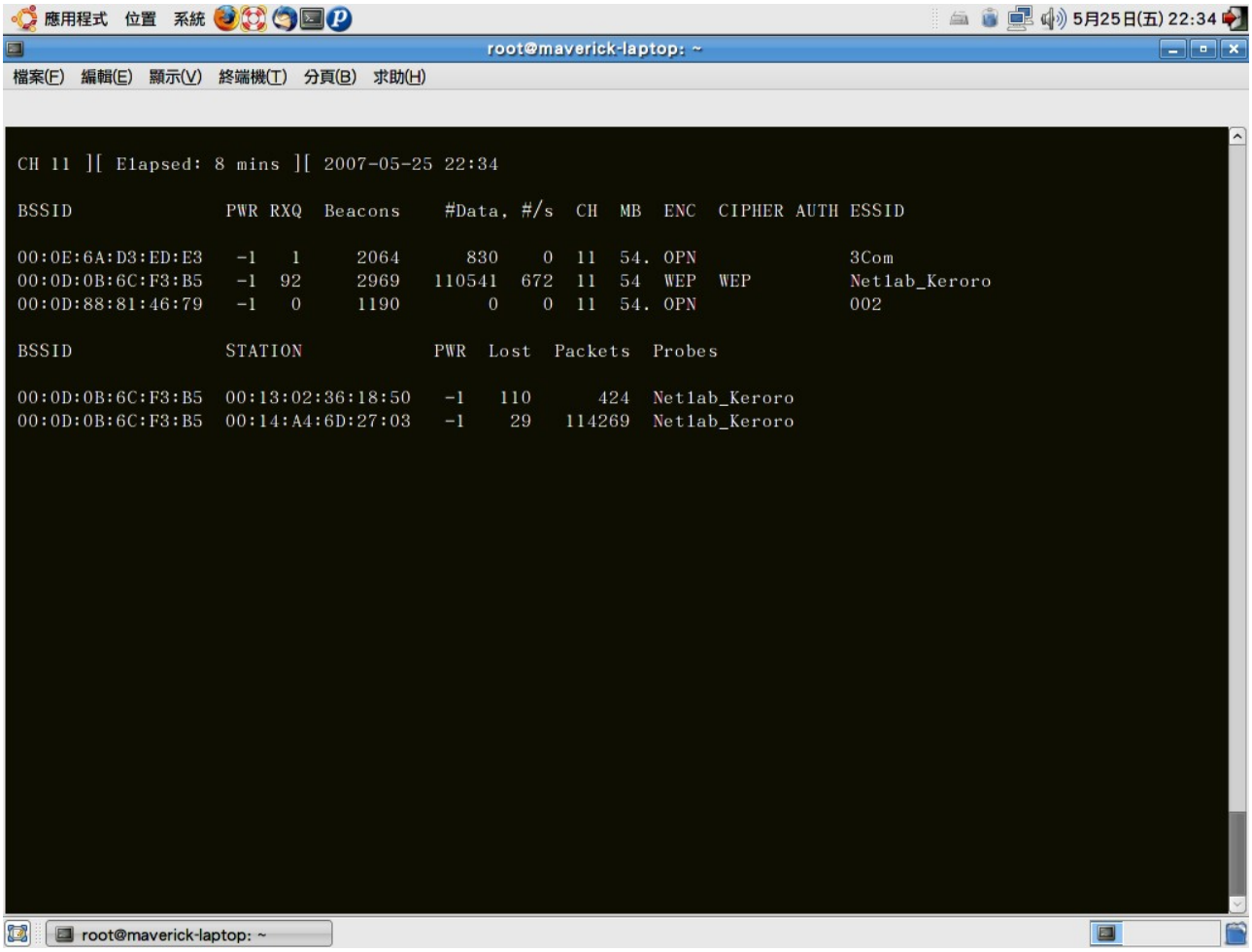
airodump-ng mon0

De esta forma veremos todas las redes disponibles con sus respectivos canales, una vez que ya decidimos que redes son las que vamos a atacar creamos un filtro, paramos la ejecución de airodump-ng presionando ***Ctrl + C,*** y posteriormente ejecutamos:

-c = Filtro de canal 6, 11, 1, etc.
-w = Escribir resultados en un documento.

airodump-ng -c 11 -w nombre mon0

De esta forma hemos creado un filtro que solo trabajará en el canal indicado (11).

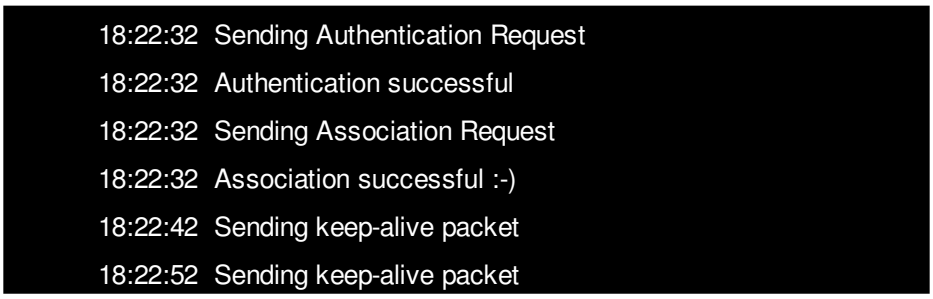


Aireplay-Ng

Una vez que airodump-ng ya está trabajando, abrimos una nueva consola donde empezaremos a trabajar con aireplay-ng.

Lo primero que debemos hacer con aireplay-ng es asociarnos a la red a la cual atacaremos.

#aireplay-ng -1 6000 -q 10 -o 1 -e (ESSID victima) -a (Mac Victima) -h (nuestra mac) mon0

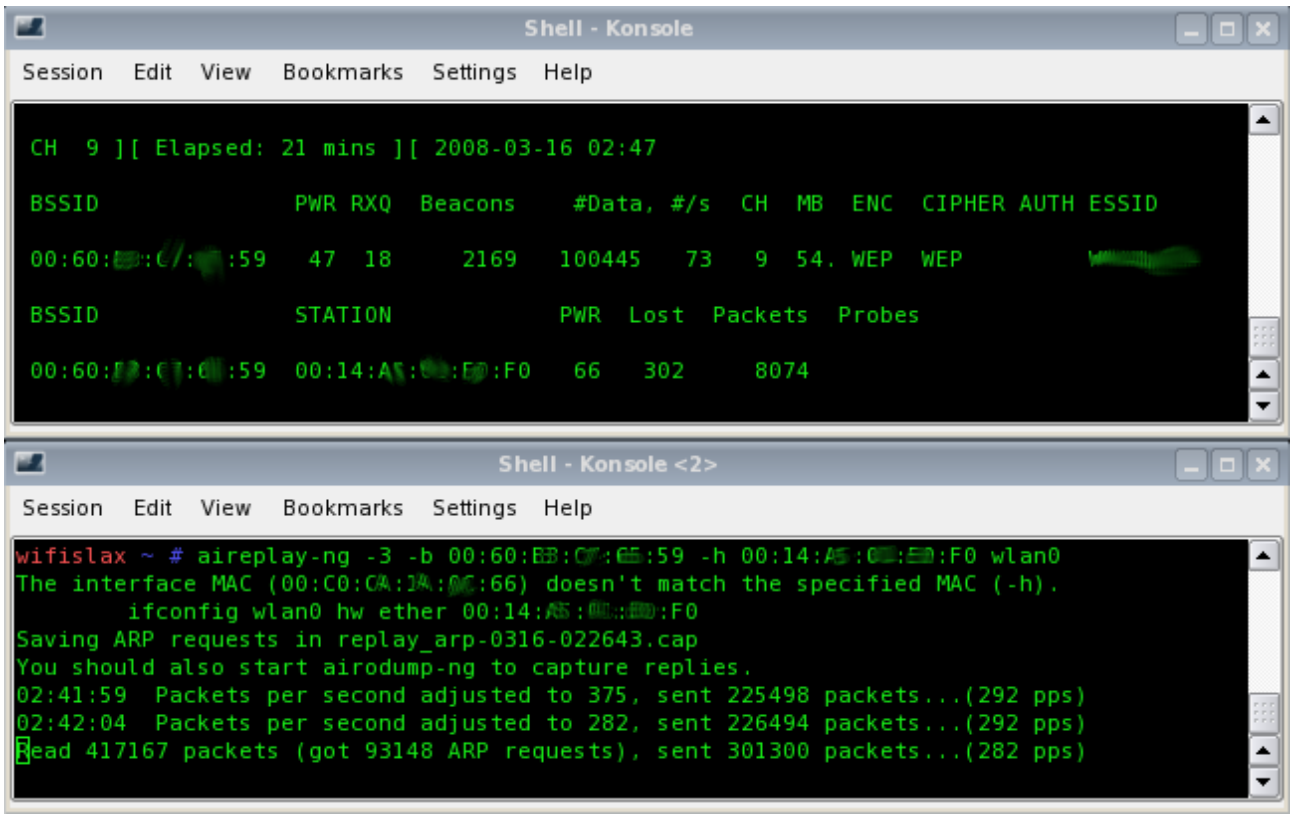


Creo que muchos se pueden preguntar, ¿de donde obtengo el ESSID y la Mac de la víctima?. Bueno, si recordamos en la consola anterior ejecutamos airodump-ng, de esa pantalla encontramos las columnas BSSID y ESSID que corresponden a la mac y la ESSID o nombre del router respectivamente.

De esta forma estaremos asociados a la red la cual cada 10 segundos aireplay-ng mandará un paquete llamado "KEEP-ALIVE", lo que avisará al router que seguimos asociados y asi no nos botará a cada rato.

Ya asociados procedemos a enviar y capturar paquetes, para eso en una nueva consola ejecutaremos nuevamente aireplay-ng pero en modo agresivo.

#aireplay-ng -3 -b (Mac Víctima) -h (nuestra mac) mon0



De la imagen anterior lo que nos interesa es que aumenten los ARP, ya que son esos los paquetes capturados y los que además nos entregarán la clave buscada.

Una vez que tenemos desde 150.000 paquetes capturados empezamos a trabajar con aircrack-ng.

Nunca está demás recordar que mientras mas paquetes capturados, es mucho mejor, ya que más pronto obtendremos la clave.

Aircrack-Ng

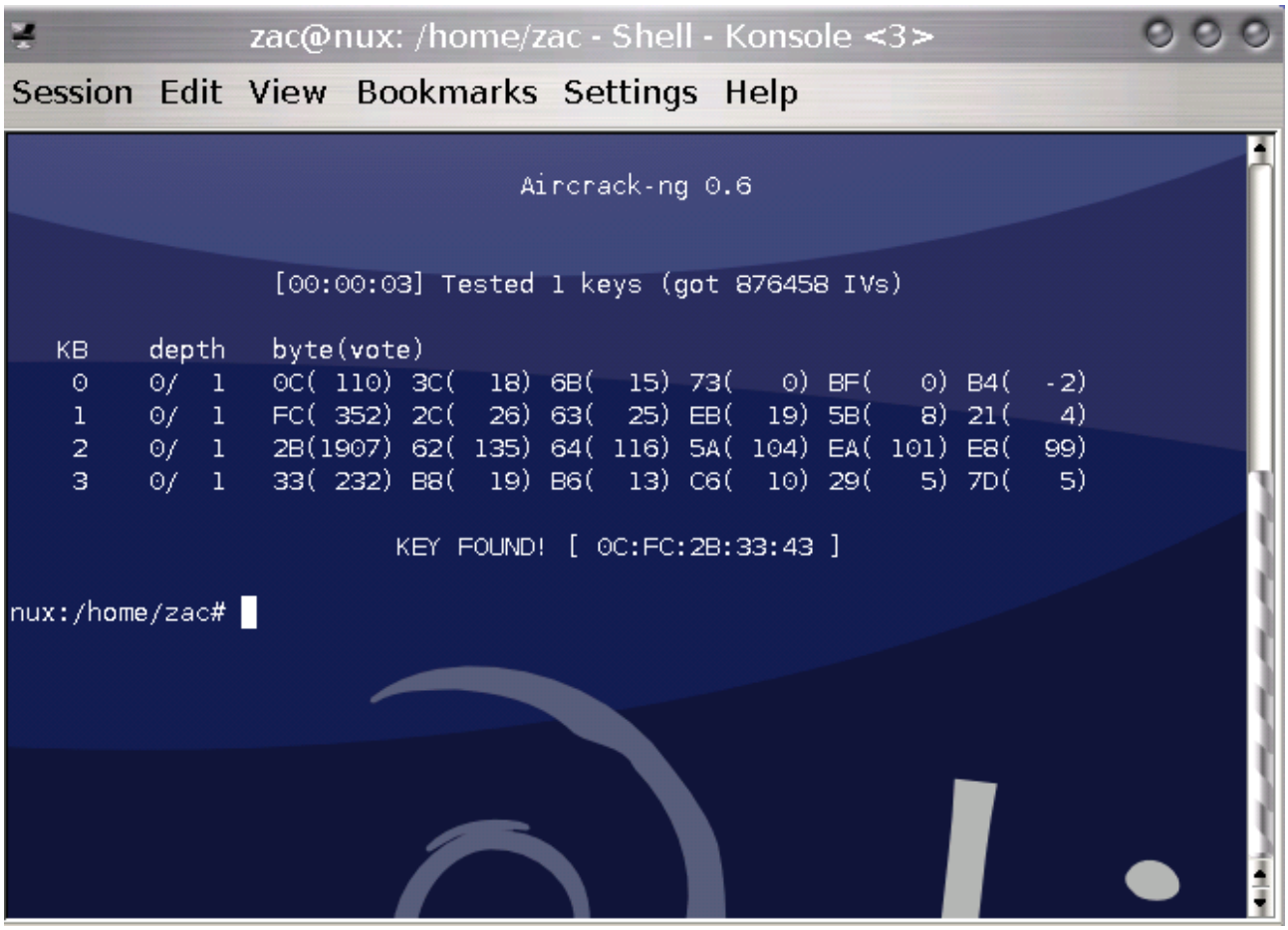
Ya estamos en el paso final, con los paquetes de datos capturados procedemos a ejecutar aircrack-ng, para lo cual tenemos dos formas, una lenta pero efectiva, y una rápida pero se necesita una mayor cantidad de paquetes para desencriptar la clave.

Forma lenta

#aircrack-ng *.cap

Forma Rápida (se necesita mayor cantidad de paquetes capturados)

#aircrack-ng -z *.cap



De esta forma ya hemos desencriptado la clave que buscabamos, ahora a disfrutar de internet.

Recordatorio.

- Al finalizar este tutorial, cabe recordar que la distancia afecta nuestro trabajo, si estamos muy lejos de la red a atacar la transferencia y captura de paquetes será muy lenta llegando incluso a ser nula. Por lo cual es recomendable estar a una distancia prudente para poder realizar la captura de forma rápida.

- Los drivers para las tarjetas inalambricas deben ser los propietarios, no se puede realizar por emulación de drivers, en este caso con ndiswrapper, por ejemplo.

- Las acciones deben ser ejecutadas como Super Usuario (root) en los sistemas que lo permitan, en caso de Ubuntu, se debe ejecutar con **sudo.**

- Las direcciones mac SIEMPRE deben iniciar con 00 en caso de que las cambien en forma manual.

Finalizando.

Espero que este tutorial sea de utilidad para cada persona que lo lea. Este tutorial está enfocado en una forma de ataque, en aircrack-ng existen muchos otros métodos, algunos más complicados que otros, pero la idea es aprender y adoptar la forma más cómoda para cada uno.

En caso de duda, contactar a paolo.norambuena@gmail.com