

Utilizando un Sniffer

El autor del manual “Kicking People” no se hace responsable del mal uso que se le pueda dar al contenido expuesto en el texto.

Esto significa que usen sus cabezas porque si lo hacen sin el consentimiento del propietario de lo que husmean pueden tener problemas. Esto es solo educativo, no es mucho pero es lo que hay.

En esta práctica se va a enseñar con los pasos detallados a utilizar el sniffer de uno de los programas más conocidos:

- Cain & Abel

Este programa es una completa maravilla, no solo sirve de Sniffer sino que también puede crackear muchísimas cosas. Recomiendo que le den una ojeada general y vean que es capaz de hacer este completísimo programa. Su página principal es www.oxid.it

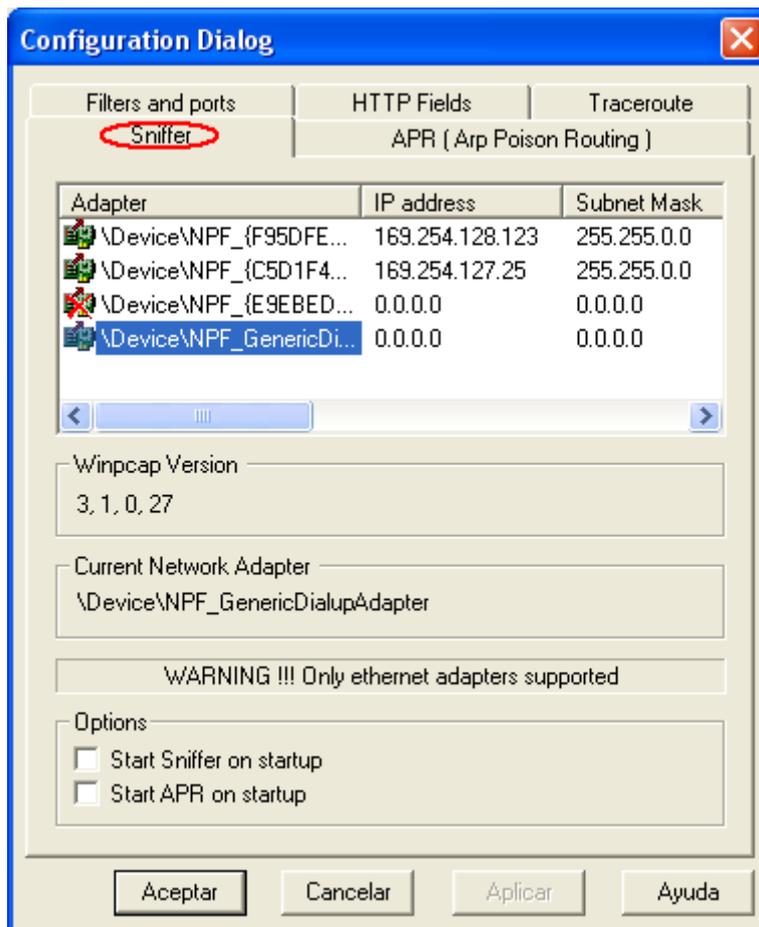
Primero vamos a tomar unos conceptos de que es lo que hace un sniffer y después voy a entrar a detallar el modo de uso.

Un sniffer, captura los paquetes que envía nuestra Red (ya sea una computadora en la LAN o nuestro PC), en esos paquetes viaja toda la información que envía el usuario, así como Usuarios y Contraseñas de muchos servicios de internet. Algunos de estos servicios que utilizan Usuarios y Contraseñas o datos confidenciales, están encriptados o codificados para que no se puedan leer. Muchos otros como el servicio de FTP (File Transfer Protocol) viajan en texto plano, de manera que cualquiera que intercepte esos paquetes puede llegar a interpretar los datos.

Vamos con la práctica:

Cain & Abel:

Para capturar los paquetes con Cain & Abel hay que configurar el programa con la placa de Red para que capture los paquetes que esta envíe. Para hacer esto hay que dirigirse a la Pestaña “Configure” y seleccionar la placa que utilizaremos.



Luego filtrar los Protocolos que queremos Sniffar en la ventana "Filters and Ports".

Una vez activado el Sniffer solo queda esperar a que inicien una sesión de FTP.
Vamos a iniciar una para hacer una muestra ☺.

Timestamp	FTP server	Client	Username	Password
05/12/2008-08:22:00	192.168.1.57.10	192.168.1.106	admin	admin

Y WALA!!! Capturamos el paquete.

Ahora vamos a describir las pestañas:

- **Timestamp:** Es la fecha y hora en que se inició la sesión.
- **FTP Server:** Es la IP del servidor FTP
- **Client:** Es la IP de la PC que inicia sesión (en este caso la mia ☺)
- **Username:** Nombre de Usuario
- **Password:** Como todos ya saben, la contraseña :P

Así también se pueden capturar los tipos de contraseña que aparecen en la lista (Telnet, ICQ, MySQL, etc.), siempre y cuando se elijan los puertos apropiados para dichos procesos.

Espero que les guste el manual, no soy experto en protocolos ni nada de eso, a duras penas pude confeccionar este manual, son pocos los conocimientos pero a mi me gusta compartirlos y mas cuando se trata de las personas/comunidades que me ayudaron a llegar a estos conocimientos.

Quiero hacer unos agradecimiento generales a dos foros muy populares <http://foro.elhacker.net> y el foro de HackxCrack (www.hackxcrack.com) y a todos los que los componen (usuarios, administradores, colaboradores, etc.), que gracias a las revistas de este último muchos han agrandado sus conocimientos.

Este manual puede ser copiado siempre y cuando se mantenga como ha sido escrito por su autor “Kicking People” y se lo nombre cuando a éste manual se haga referencia.

By Kicking People

kicking.people@gmail.com