Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Maxima seguridad con dsniff. El sniffer total. (124234 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 19/10/2001 18:22 modificado el 19/10/2001 18:22

> **Dsniff** nos demuestra lo inseguras que son nuestras redes, sobretodo si nos empeñamos en enviar contraseñas en formato **texto plano**. Con este **sniffer**, nos daremos cuenta de los realmente importante que puede llegar a ser la utilizacion de la encriptacion en nuestras comunicaciones diarias ...

Tal y como dice el autor del programa *Dug Song*, él desarrollo esta potentísima aplicación para **auditar** sus propias redes y para demostrar la necesidad de usar **encriptación** de un modo habitual. *"Please do not abuse this software"*

Gracias a **dsniff**, tenemos un motivo mas para usar diariamente herramientas como **ssh** (la version 2, porque la 1 tiene algunos problemas de seguridad y es vulnerable) y **gpg** (Gnu pgp)

Para haceros una idea de las posibilidades del dsniff, conectaros a Internet como lo haceis habitualmente, en otra sesion como root teclear:

```
# dsniff -i ppp0
```

Ahora bajaros el correo, entrad en algun servidor/servicio que os pida contraseña y vereís como *por arte de magia* vais capturando los pares **usuario:contraseña.**

Entrad ahora usando **ssh** y vereís como en este caso nuestro sniffer **no** captura la contraseña. **;-)**

dsniff esta formado por una serie de programas que son:

- dsniff: simple password sniffer. (Yo realmente no lo consideria nada *simple*)
- arpspoof: redirect packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies.
- dnsspoof: forge replies to arbitrary DNS address / pointer queries on the LAN.
- filesnarf: saves selected files sniffed from NFS traffic in the current working directory.
- macof: flood the local network with random MAC addresses.
- mailsnarf: a fast and easy way to violate the Electronic Communications Privacy Act of 1986 (18 USC 2701-2711), be careful.
- msgsnarf: record selected messages from sniffed AOL Instant Messenger, ICQ 2000, IRC, and Yahoo! Messenger chat sessions.
- sshmitm: SSH monkey-in-the-middle.
- tcpkill: kills specified in-progress TCP connections.
- tcpnice: slow down specified TCP connections via "active" traffic shaping. (Se puede usar para evitar virus/gusanos tipo NIMDA). Os recomiendo que os paseis por : http://bulma.net/body.phtml?nIdNoticia=865[1]
- urlsnarf: output all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for offline post-processing
- webmitm: HTTP / HTTPS monkey-in-the-middle.
- webspy: sends URLs sniffed from a client to your local Netscape browser for display, a fun party trick

Pagina web del dsniff:
http://www.monkey.org/~dugsong/dsniff/[2]
Ademas de la version actual la 2.3[3], podemos encontrar una beta de la nueva version que esta en desarrollo con

nuevas características. http://www.monkey.org/~dugsong/dsniff/beta/dsniff-2.4b1.tar.gz[4]

Más informacion:
ftp://www6.software.ibm.com/software/developer/library/s-sniff.pdf[5]
ftp://www6.software.ibm.com/software/developer/library/s-sniff2.pdf[6]

Simplemente **I M P R E S I O N A N T E** .

En el proximo articulo os mostrare como detectar sniffer's en nuestra red local, estaros atentos.

--
Carlos (aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [7]

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=865
2. http://www.monkey.org/~dugsong/dsniff/
3. http://www.monkey.org/~dugsong/dsniff/dsniff-2.3.tar.gz
4. http://www.monkey.org/~dugsong/dsniff/beta/dsniff-2.4b1.tar.gz
5. ftp://www6.software.ibm.com/software/developer/library/s-sniff.pdf
6. ftp://www6.software.ibm.com/software/developer/library/s-sniff2.pdf
7. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com