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

Monitoriza los accesos por telnet con TTYSNOOP (7019 lectures)

Per **Miguel Ángel Calderón**, ***MAC*** ()

Creado el 21/02/2000 00:00 modificado el 21/02/2000 00:00

Con TTYSNOOP puedes duplicar las terminales de los accesos por telnet y rlogin. Puedes encontrar ttysnoop en:
Freshmeat.[1]

El código de TTYSNOOP viene preparado para soportar encriptación normal, shadow password y MD5 que curiosamente es novedad en las últimas distribuciones como la RH 6.x.

Para el uso de shadow password y MD5 hay que recompilar el código "-DSHADOW_PWD" y con la opción "-lcrypt". Todo esto se debe cambiar en el fichero Makefile que viene con el código fuente.

Por lo demás la configuración que recomiendo para el ttysnoop es la siguiente:
En el fichero /etc/snooptab dejar solo comentada la linea siguiente:

```
*    socket    login    /bin/login
```

En el fichero /etc/inetd.conf podemos modificar la linea del servicio telnet para que de paso a ttysnoops (programa servidor) en lugar del login tradicional, para ello hay que añadir un "-L /sbin/ttysnoops" después de la sentencia in.telned.

Esto nos permite recibir múltiples accesos y monitorizar el que deseemos. Para poder monitorizar una terminal duplicada con ttysnoops (acabado en s, es el servidor) utilizaremos el comando "ttysnoop terminal".
El código fuente está disponible en:
metalab.unc.edu. [2]

Lista de enlaces de este artículo:

1. http://www.freshmeat.net/appindex/1999/09/05/936520647.html
2. ftp://metalab.unc.edu/pub/Linux/utils/terminal/ttysnoop-0.12c.tar.gz

---

E-mail del autor: macal _ARROBA_ ono.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=225