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

Deteccion de virus con tcpdump (14323 lectures)

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

Creado el 10/09/2001 12:47 modificado el 10/09/2001 12:47

> Usando el polivalente y potente **tcpdump**, se puede detectar que maquina/s de nuestra red local esta infectada/s por alguno de los virus de ultima hornada, en este caso concreto el virus se propagaba buscando y usando las carpetas compartidas de las maquinas windows :-(...

Lo primero que tuve que hacer fue, ir a una maquina windows (llamada *maq_caracol*) y quitar la comparticion de carpetas, excepto la disquetera, que sera la que utilizaremos de *cepo* para el virus.

Luego nos vamos a una maquina **unix** y ejecutamos el tcpdump de la siguiente forma:

```
tcpdump -e -s 4000 dst host maq_caracol \
and src host not server1 \
and src host not server2
```

Lo que basicamente significa, que capture todo el trafico que vaya dirigido a la maquina *maq_caracol* y que no provenga de ninguno de estos servidores: server1 y server2.

Ahora solo falta esperar a que el virus intente acceder a la carpeta compartida (la disquetera) y volia!!! ya sabremos en que maquina de nuestra red esta el virus.

Realmente no utilice tcpdump, sino una version hackeada del mismo **smbtcpdump-3.4**, enfocada en el protocolo smb, pero para este caso no implica diferencia alguna.

--
Carlos Cortes (aka carcoco)

E-mail del autor: carcoco _ARROBA_ gmail.com