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

Usando la herramienta netcat en Linux. La navaja suiza del protocolo TCP/IP. (41284 lectures)

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

Creado el 09/07/2001 23:09 modificado el 09/07/2001 23:09

> La utilidad netcat es un sencilla pero potente utilidad que se puede utilizar para practicamente cualquier cosa que se nos ocurra que tenga que ver con el protocolo TCP/IP, es como la denomina el autor de la misma, la navaja suiza del tcp/ip *(I think of netcat as my tcp/ip swiss army knife)*.
>
> *Os voy a mostrar algunos de los multiples usos que se le pueden dar a* ***netcat****...*

Antes que nada una pequeña aclaracion, muchas veces el fichero binario del netcat es simplemente *nc* y otras veces *netcat*.

Posibles usos del netcat :

a) Bajar/Borrar/Ver/Escribir correo electronico.
b) Identificacion de sistemas y servidores.
c) Realizacion de un sencillo chat, para 2 personas.

Aunque sus posibles utilidades y usos son practicamente ilimitados, (creo recordar que Javi Polo tenia incluso por ahi un programa para enviar mensajes sms, usando una pagina web de envio de sms gratuitas), solo es cuestion de imaginacion y un poco (o mucho) de practica.

a) Bajar/Borrar/Ver/Escribir correo electronico.

La mayoria de esta informacion sacada a partir de la e-zine CatHack disponible en http://www.sindominio.net/cathack/[1], que por cierto esta muy interesante y os recomiendo que le pegeis una hojeada a la e-zine. Concretamente en el numero numero 6.

La idea es poder usar el netcat para enviar correos usando directamente una conexion con el servidor smtp de nuestro (o no necesariamente nuestro) proveedor de la conexion a Internet.

```
netcat proveedor.internet.es 25

helo holahola
mail from:<elreydelbambo@maquina.com>
rcpt to:<destinatario@maquina.com>
250 Recipient <destinatario@maquina.com> Ok
data
354 Ok Send data ending with <CRLF>.<CRLF>
Subject: prova
X-Mailer: by-hand cutremail X'-D

Aqui ya no son cabeceras porque hemos dejado una linea en blanco.
. (Con el punto indicamos el final del mensaje, esta linea final solo contendra el punto.)
```

Aunque a mi lo que mas me gusto y lo que mas me interesaba es poder borrar esos correos que me bloqueaba de vez en cuando mi cuenta de correo, sobretodo porque muchas veces era spam enormes.

```
netcat proveedor.internet.es 110
```

```
+OK Bienvenido al servidor POP3 de TERRA
user carcoco
+OK password required for user carcoco
pass elpassword
list
1 2451
2 123433
3 323
dele 2
quit
+OK goodbye
```

Me interesaba borrar el segundo correo, cosa que consigo con el comando **dele 2**.

```
  USER usuari      Utilitzats en l'autentificació
  PASS password    Utilitzats en l'autentificació
  QUIT              Per sortir
  LIST [msg]       Per llistar els missatges que tens
  RETR msg         Per llegir missartges
  DELE msg         Per borrar missatges
  NOOP             El server et respon amb un OK
  LAST             Per llegir l'ultim missatge rebut
```

b) Identificacion de sistemas y servidores.
Podemos usar el netcat para averiguar que programa y que version estan usando para dar el servicio de paginas web.

```
$ netcat bulma.net 80

netcat bulma.net 80
get . /

...
Server: Apache/1.3.17 (Unix) PHP/4.0.6
Connection: close
Content-Type: text/html; charset=iso-8859-1

Your browser sent a request that this server could not understand.
Invalid URI in request get . /
```

Donde podemos ver que en el servidor web de Bulma, se utiliza la version 1.3.17 del Apache con el modulo 4.0.6 del PHP.

c) Realizacion de un sencillo chat, para 2 personas.
Usando el netcat podemos establecer una conexion directa entre dos puertos de dos ordenadores a traves de internet, de forma que se puede usar para emular un rudimentario chat entre dos personas.

Cuando conoci a Guillem a traves de la red, el fue el que me descubrio el netcat y lo usamos para establecer una conexion directa entre mi ordenador i el suyo a traves de Internet. I la verdad es que fue muy sencillo e instructivo hablar con Guillem, bueno al final abrimos dos conexiones simultaneas en dos puertos diferentes de forma que yo hablaba por una y el por la otra.

En un ordenador se crear el "pseudo servidor" de esta forma:

```
netcat -l -p 12345
```

I en el otro ordenador (o el mismo si quereis hacer pruebas, se ejecutara el "pseudo-cliente" con:

```
netcat servidor.internet.com 12345
```

Li baix demanar a Guillem que en tirara una maneta (ja que ell habia sigut que m'habia explicat aixo del netcat) i aci esta part de la seua resposta, molt interesant, per cert :

```
...

Si, per exemple pots transferir fitxers entre màquines fàcilment... amb una
única comanda a cada màquina:

[stark@PII_400 stark]$ nc -l -p 4000 <fitxer
[stark@MII_300 stark]$ nc PII_400 4000 > fitxer

(Hauràs de tallar la connexió quan hagi acabat)

I si saps com va FTP, pots fer qualsevol cosa sense tenir cap client FTP. Però
això ja és més dificil d'explicar perquè necessites _dues_ terminals (per dues
connexions simultànies com a minim). Mira aquest exemple, et posaré el volcat
de les dues terminals, però si fas l'experiment tu mateix veuràs millor
com van passant les coses. Transferiré un llistat de fitxers usant FTP actiu, i
després transferiré un fitxer usant FTP passiu. No ha d'esser necessàriament
així, però ho faré perquè vegis els dos modes:

NOTA: Posaré [...] a les parts llargues i prescindibles, per no liar més
la cosa.

----------------------------------- Terminal 1 (connexió de control):

[stark@MII_300 stark]$ nc ftp.lip6.fr 21
220-
220-        -- BIENVENUE SUR LE NOUVEAU SERVEUR FTP LIP6/JUSSIEU --
[...més missatges...]
220 ftp.lip6.fr FTP server ready.
user anonymous
331 Guest login ok, send your complete e-mail address as password.
pass hola@que.tal
230-
230-    Ce service est assure par le Laboratoire d'Informatique de
230-l'universite Paris 6 (LIP6) et le Centre de Calcul Recherche (CCR) du
230-campus Jussieu.
[...més missatges...]
230 Guest login ok, access restrictions apply.
port 62,42,197,18,4,1
200 PORT command successful.
list /pub/OpenBSD/
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
pasv
227 Entering Passive Mode (195,83,118,1,44,227)
retr /pub/OpenBSD/README
150 Opening ASCII mode data connection for /pub/OpenBSD/README (1879 bytes).
226 Transfer complete.
quit
221-You have transferred 1918 bytes in 1 files.
221-Total traffic for this session was 4767 bytes in 2 transfers.
221-Thank you for using the FTP service on ftp.lip6.fr.
221 Goodbye.
[stark@MII_300 stark]$

----------------------------------- Terminal 2 (connexions de dades):

[stark@MII_300 stark]$ nc -l -p 1025
total 7228
lrwxrwxrwx    1 victor   root            6 Feb  9 12:10 .message -> README
drwxr-xr-x   15 victor   root         4096 Apr 23 02:10 2.8
drwxr-xr-x   15 victor   victor       4096 Jun 21 16:31 2.9
-r--r--r--    1 victor   victor       1879 Jun  1 13:11 README
-r--r--r--    1 victor   root         3590 Jun 13  2000 fl
-r--r--r--    1 victor   victor       5116 Jun 29 13:54 ftplist
-r--r--r--    1 victor   root         3282 Jun 15  2000 ftplist~
-r--r--r--    1 victor   victor    6202751 Jun 29 16:23 ls-lR
-r--r--r--    1 victor   victor    1135530 Jun 29 16:23 ls-lR.gz
drwxr-xr-x   10 victor   root         4096 Jun 27 02:14 patches
drwxr-xr-x   20 victor   root         4096 Jun 28 02:06 src
drwxr-xr-x    2 victor   root         4096 Apr 24  1999 tools
[stark@MII_300 stark]$ nc ftp.lip6.fr 11491
```

```
Welcome to ftp.OpenBSD.org
Located at the University of Alberta in Edmonton, Alberta, Canada.
For other mirror sites visit http://www.openbsd.org/ftp.html

[...la resta del fitxer...]
[stark@MII_300 stark]$

...

Bé, i això no és res... les possibilitats son infinites :-) Fins i tot amb FTP
pots fer mil coses més: pujar fitxers al servidor, usar el mode proxy, etc. El
mode proxy-FTP és interessant: estableixes dues connexions de control amb dos
servidors ftp diferents, i els envies comandes perquè estableixin connexions de
dades entre ells i s'intercanviin fitxers directament, sense passar per la teva
màquina. Quan aconsegueixes això, saps que has entès el protocol FTP X'-D

Amb altres protocols més complicats poden fer moltes més coses, sempre amb
l'ajuda de NetCat o d'un senzill programa que faci més o manco el mateix...

....
```

--
Carlos Cortes

Lista de enlaces de este artículo:

1. http://www.sindominio.net/cathack/

E-mail del autor: carcoco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=714