Conectar a traves de cortafuegos: ssh invertido

Por Paco Aldarias Raya

Impreso: 24 de enero de 2006

Email: pacolinux arroba inicia punto es
Web: `http://pagina.de/pacodebian`
Con Linux Debian. En Valencia (España)

El documento tiene version .html, y .pdf, cambiando en el navegador la parte final podrás acceder a ambos.

Realizado con: LaTeX

Índice

1. Introducción

También llamado *Forwarding de puertos con ssh*.

Para que se pueda hacer un script tienes que hacer de forma que ssh se conecte con llave publica sin contraseña.

2. Escenario

Maquina en la empresa: maquinadetrabajo (protegido con un firewall o simplemente un router)

Maquina de casa: mimaquina (via adsl por ejemplo)

En las dos maquinas tiene que existir el mismo usuario (por ejemplo vicente)

"Se supone que "mimaquina"tenga IP fija, pero se puede hacer igual con dyndns o no-ip y tendrá por ejemplo: vicente.no-ip.org o simplemente 80.24.35.76 si tiene IP fijo

3. En maquinadetrabajo

Login como usuario vicente

```
# ssh-keygen -t dsa (a menos que tu ya no tengas llaves rsa)
```

NOTA: Dejar la frase vacia.

y obtendrás las llaves id_dsa (privada) e id_dsa.pub (publica) en

```
~/.ssh
```

necesitas copiar la llave en "mimaquina"

```
# ssh-copy-id -i ~/.ssh/id_dsa.pub mimaquina
```

Ahora puedes entrar en "mimaquina"sin contraseña vía ssh. Compruebalo:

```
# ssh vicente@mimaquina
```

PORT FORWARDING

Siempre en la maquina "maquinadetrabajo"

```
ssh -N -l vicente -R 23456:localhost:22 mimaquina &
```

ya está!

4. En mimaquina

Ahora corre a casa en tu maquina "mimaquina"

Abre un terminal como usuario vicente y escribe eso:

```
ssh -l vicente -p 23456 127.0.0.1
```

Ya estas dentro de tu maquina dentro la empresa sin que el firewall pueda molestarte.

5. A tener en cuenta

Cuidado 1

esta conexión puede caerse así que no estária mal escribir un pequeño scrip en la maquina de la empresa para que compruebe daca 10 minutos si la conexión sigue levantada.

He notado que no cae casi nunca si haces un ping o un echo cada 5 o 10 segundos para simular trafico de red.

Cuidado 2

Esta es la forma perfecta para hacer espionaje industrial sin que nadie se deen cuenta de inmediato.

Si alguien conigue entrar en tu maquina, tendrá aceso también a la red de la empresa.

6. Hacer que ssh siempre este conectado

Nos bajaremos autossh:
`http://www.harding.motd.ca/autossh/`

Debermos poner en el cron:

```
50/5 * * * * /etc/init.d/autossh.sh
```

```
cat /etc/init.d/autossh.sh
#!/bin/bash
PID=‘ps aux |  grep -v "grep" | grep ’autossh -M 20000’ | awk ’{ print $2 }’‘
as=/usr/local/bin/autossh

if [ -z $PID  ]; then
   su - paco "/usr/local/bin/autossh -M 20000 -f -N -R 23456:localhost:22 paco@alda
fi
```

Hacer el enlace simbolico ln -s /etc/init.d/autossh.sh /etc/rc5.d/S90autossh.sh

7. Bibliografia

1. Tunel ssh de inicio remoto (aka ssh -R) con autossh y sin contraseña
   `http://www.galpon.org/modules/weblog/details.php?blog_id=40`