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

# Buscando e Identificando servidores SSH. (11307 lectures)

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

Creado el 04/12/2001 09:13 modificado el 04/12/2001 09:13

> Imagina que son las 10 de la noche y has acabado, *por fin*, la actualización del **todos** tus servidores **ssh** de tu red local, debido a los últimos problemas[1] de **seguridad** relativos al **SSH** ...

Recurres al potente **nmap**, para averiguar si todo ha funcionado correctamente, pero aún así, necesitas una herramienta que **detecte** e **identifique** estos servidores **SSH**.
La solución es **scanssh** de **Niels Provos**, que nos permite identicar exactamente el nombre y la versión de los servicios **SSH**, de una forma sencilla y rápida:

```
$ scanssh 127.0.0.1
127.0.0.1 SSH-1.99-OpenSSH_2.9.9p2
```

El resultado es similar al obtenido si hubiera ejecutado algo como:

```
$ netcat 127.0.0.1 22
SSH-1.99-OpenSSH_2.9.9p2
help
Protocol mismatch.
```

Pero con la diferencia de que tenemos más opciones con **scanssh**, y que cada vez que ejecuto **scanssh** en el log del sistema queda registrado algo como:

```
Dec  1 21:26:59 linuxalcoy sshd[1868]:
Disconnecting: Your ssh version is too
old and is no longer supported.
Please install a newer version.
```

Pero en cambio al ejecutar el **netcat**, en el log se registra la **IP** desde donde se realiza la conexión:

```
Dec  4 23:06:34 carlets sshd[1246]:
Bad protocol version identification
'help' from 127.0.0.1
```

```
$ scanssh -h
scanssh: [-VIERh] [-n port] [-e excludefile]
[-b alias] [-p ifaddr] ...
-V         print version number of scanssh,
-I         do not send identification string,
-E         exit if exclude file is missing,
-R         do not honor exclude file for random addresses
-n <port>  the port number to scan.  Either 22 or 80.
-e <file>  exclude the IP addresses and networks in ,
-b <alias> specifies the IP alias to connect from,
-p <ifaddr>specifies the local interface address,
-h         this message.
```

Aquí teneís el resultado al interrogar con **scanssh** la dirección, de un conocido, activo y interesante grupo linuxero ;-)

```
$ scanssh
./scanssh 233.23.11.233
233.23.11.233 SSH-1.99-OpenSSH_2.3.0p1
```

http://www.monkey.org/~provos/scanssh/
http://www.monkey.org/~provos/scanssh-1.6b.tar.gz[2]

--
Carlos Cortes(aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [3]

---

**Lista de enlaces de este artículo:**

1. http://www.linuxsecurity.com/advisories/suse_advisory-1728.html
2. http://www.monkey.org/~provos/scanssh/
3. http://bulma.net/todos.phtml?id_autor=132

---

E-mail del autor: carcoco _ARROBA_ gmail.com