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

Confianza SSH entre Sistemas Unix: evitar el tecleo continuo de claves.

Per **LauraCeldranS**, ***LauraCS*** (http://laura.celdran.name)

Creado el 21/05/2005 11:54 modificado el 23/05/2005 00:01

> Introducir en cada conexión remota a un sistema el *password*, que normalmente suele tener privilegios de root-administrador, es más bien poco seguro; además de incómodo.
>
> Es evidente que dejar un sistema sin clave de acceso es más inseguro aún, pero la pregunta es *¿con los esfuerzos en criptología que se están llevando a cavo estos últimos años, es seguro enviar la clave de root aunque esta vaya cifrada?*, *¿se puede asegurar que un protocolo que hoy es seguro mañana lo seguirá siendo?*
>
> Pues bien, os expongo como crear enlaces de confianza SSH, mediante clave privada y pública, entre sistemas Unix para teclear la clave una única vez.[1]
>
> Una idea... Puesto que a raiz de este artículo he mantenido muchas **conversaciones** vía mail con distintas personas bastante conocedoras de esta materia se me ha ocurrido escribir todo el conocimiento reportado en unos **post** en ***http://laura.celdran.name***[1]
>
> Espero que esto os sea útil

Para esas personas a las que le inquieta la seguridad, una buena forma de securizar, aún más, el acceso a servidores Unix de forma remota...

El proceso es muy sencillo: ya es bien conocido que ssh v1 ha sido atacada (pero aún así todavía se considera seguro), así que para esas personas que buscan jugar más a ponérselo difíciles a los atacantes, a continuación se describe en 6 breves pasos como hacer que se establezcan enlaces de confianza entre nuestros servidores Unix, con las ventajas que esto reporta.

Pasos:

1. Entrar en el "equipo X" y teclear ssh-keygen -t rsa.

```
su - usuarioX
ssh-keygen -t rsa
```

2. Se recomienda dejar todos los campos en blancos, símplemente pulsa enter. Esto nos habrá creado un subdirectorio **".ssh"** en el "home del usuarioX" (/home/usarioX/.ssh/), que contendrá nuestras claves públicas y privadas.

```
Generating public/private rsa key pair
Enter file in wich to save the key (/home/usuarioX/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Entre same passphrase again:
Your identidication has been saved in /usuarioX/.ssh/id_rsa
Your public key has been saved in /usuarioX/.ssh/id_rsa.pub
The key fingerprint is:
89:5a:de:4a:9c:8e:..... usuarioX@equipoX
```

3. Darle a este directorio los **permisos** apropiados, para que nuestro equipo no desconfie del host remoto.

```
equipoX:/.ssh# ls -l
-rw------- 1 usuarioX usuarioX .... id_rsa
-rw-r--r-- 1 usuarioX usuarioX .... id_rsa.pub
-rw-r--r-- 1 usuarioX usuarioX .... know_hosts

equipoX:/.ssh#
```

4. Repetir estos pasos en el "equipo Y".
5. Copiar el contenido del fichero **"id_rsa.pub"** del "equipoX" (/home/usuarioX/.ssh/id_rsa.pub), al fichero **"authorized_keys"** (/home/usuarioY/.ssh/authorized_keys) del "equipoY" y viceversa.

   Nota: Como apunta nuestro amigo "Anónimo": Para copiar las llaves publicas a maquinas remotas basta con poner

   ssh-copy-id -i key.pub usuario@HOST_DESTINO

   De esa forma va añade directamente al fichero authorized_keys del usuario

6. Intente conectar desde el equipoX como usuarioX, al equipoY como usuarioY. La primera vez, el sistema, pide que se introduzca la contraseña y ya no la volverá a pedir mientras no se hagan cambios en la versión de SSH.

Esto permite crear niveles de segurida muy altos, puesto que por la red únicamente viaja la clave pública del equipo y que además viaja cifrada (SSH).

Espero que os haya sido útil esta pequeña recopilación de conceptos.

Lista de enlaces de este artículo:

1. http://laura.celdran.name

E-mail del autor: laura _ARROBA_ laura.celdran.name
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=2190