SSH Transparente

¿Cómo hacer que el ssh te valide sin pedirte las contraseñas (con la clave pública y la privada)?

- Asegurarse de que se tiene en ambas máquinas (maq1 y maq2) una versión de openssh actualizada y de que es la misma versión. (No tiene porque ser obligatorio en versiones recientes).
- Si queremos que el usuario pepe se conecte a la maq2 desde la maq1 con un 'ssh maq2' hacer lo siguiente:
  - Desde maq1 pepe hacer:

    ```
    ssh-keygen -t rsa
    ```

    . Se habrá generado la clave privada y la pública en maq1, más concretamente en el subdirectorio /home/pepe/.ssh/ . Dejar el nombre fichero que dice y no poner passphrase.

  - Añadir al fichero /home/pepe/.ssh/authorized_keys en maq2 la línea que contiene la clave pública de maq1 (fichero .pub), la que acabamos de generar. Crearlo si no existe. OJO , si la cortamos y pegamos, tener cuidado que este en una sola linea!!
  - Asegurarse que el directorio .ssh de la maquina destino tenga como permisos drwx——. Es decir, todos los permisos solo para ese usuario, sino esto no funciona!!!
  - Probar y hacer desde maq1 ssh maq2.
- Esta configuración es para generación de claves tipo rsa de nivel 2. Las hay rsa de nivel 1 y dsa. La configuración para ambas es diferente. Para enterarse bien hacer un man ssh y man ssh-keygen.
- Si no funciona, en /etc/ssh/sshd_config debería estar descomentado y activado: RSAAuthentication yes y PubkeyAuthentication yes.

Desactivar el login del root por ssh

Para desactivar conexiones remotas ssh a la cuenta root, como medida de prevención de ataques ssh.

```
# sudo vim /etc/sshd_config
```

```
PermitRootLogin no
```

Reiniciamos el servicio

```
# /etc/init.d/sshd restart
```

ssh en nautilus

Cuando estamos trabajando en otra máquina a través de una conexión ssh, ¿no es una lata tener que andar copiando ficheros con scp?

Una alternativa mucho más cómoda es iniciar sesión en dicha máquina con nuestro navegador de

archivos y arrastrar y soltar con el ratón. Para ello, en la barra de direcciones de nautilus escribiremos:

```
sftp://usuario@direccion_ip:puerto/directorio
```

Por ejemplo:

```
sftp://lc@192.168.2.1:5566/home/lc
```

Al darle a enter nos solicitará la contraseña y accederemos a la máquina. Si usamos el puerto por defecto para las conexiones ssh, y el usuario tiene permisos de lectura en la carpeta raíz, podemos obviar los datos puerto y directorio.

Configurar SSH

La configuración del servicio ssh se encuentra en /etc/ssh/sshd_config

Referencias

- http://blogofsysadmins.com/crear-un-proxy-socks-usando-un-tunel-ssh
- http://blogofsysadmins.com/secure-shell-hacks-linux
- http://submarley.espacioblog.com/post/2008/11/04/shh-dios-la-administracion-remota
- http://linuxamartillazos.blogspot.com/search/label/ssh
- http://www.vicente-navarro.com/blog/2009/05/24/creando-tuneles-tcpip-port-forwarding-con-ssh-los-8-escenarios-posibles-usando-openssh/