DISICO

Uso SSH con Certificados Free BSD

Manual

Uso de SSH con Certificados
FreeBSD 6.2

Para crear los certificados se debe entrar con la cuenta de usuario que se va a crear el certificado. Esto puede realizarse también en jaulas donde en una de ellas están exclusivamente todos los usuarios.

Observación:

En el caso de las jaulas, en el archivo **/etc/ssh/sshd_config** de la máquina se debe mantener el puerto de los usuarios que acceden desde el exterior y desde el **ssh_config** de la jaula cambiar el puerto para los usuarios, en este caso la máquina tiene el puerto **22** y la jaula el **2222**.

Generación de claves

ssh-keygen –t rsa

Generará las llaves públicas y privadas, pedirá contraseña y la confirmación de esta.

Luego se entra al directorio para ver que estén generadas las llaves públicas y privadas

En este caso el usuario es **mferrand**.

Estando dentro de la jaula se accede al directorio del usuario

cd /home/mferrand/.ssh

Desde este directorio se podrán listar las claves publicas y privadas, estas son:

id_rsa

id_rsa.pub

Luego se debe crear el archivo **authorized_keys** con el mismo contenido que id**_rsa.pub**, eso se realiza de la siguiente forma

cat id_rsa.pub >> authorized_keys

Luego se comprueba que ambos archivos tengan el mismo peso.

Una vez verificado lo anterior, y chequear que se tiene los tres archivos en la cuenta **id_rsa, id_rsa.pub, authorized_keys,** para este ejemplo los archivos deberán encontrarse en **/home/mferrand/.ssh** se copian los archivos al equipo desde donde se conectará por ssh, una vez copiado estos archivos solo faltaría un archivo con la extensión **.ppk**.

Software puttygen-x86

Para generar este archivo se utiliza un software llamado **puttygen-x86.**

Este software en su parte superior tiene un menú con 4 pestañas, **File**, **Key**, **Conversions** y **Help**, se debe dirigir a **Conversions**, se escoge la opción **Import Key**, y se carga el archivo **ids_rsa,** luego se presiona el botón **Save Private Key,** ya realizado esto, se revisa en el mismo directorio (PC que se conectara por ssh al servidor) y se encontrará el archivo **.ppk** que en este ejemplo fue denominada como **mferrand.ppk**

Configuración SSH

Para este caso en particular donde se realiza el ssh con certificado, fue realizado en una jaula, por lo que se modifica el ssh de la jaula, el archivo a modificar es **/etc/ssh/sshd_config**.

Las líneas que se deben descomentar son las siguientes:

RSAAuthentication yes

PubkeyAuthentication yes

AuthorizedKeysFile .ssh/authorized_key

La siguiente línea se debe modificar, esta línea aparece como

#UsePAM yes

Se debe descomentar y dejar de la siguiente forma:

UsePAM no

Luego se reinicia el **ssh, /etc/rc.d/sshd restart**, y se entra con el usuario que se creo el certificado, cabe señalar que para cada usuario se deben realizar todos estos pasos señalados.