Autenticación en SSH

Autenticación mediante contraseña

La autenticación mediante contraseña es el método más básico. Los usuarios deben proporcionar su nombre de usuario y contraseña para acceder al servidor. Para habilitar este método, asegúrate de que la opción PasswordAuthentication esté habilitada en el archivo de configuración /etc/ssh/sshd_config. Puedes usar un editor de texto como nano o vi para modificar el archivo:

```
$ sudo nano /etc/ssh/sshd_config
```

Busca la línea PasswordAuthentication y asegúrate de que esté configurada como sigue:

```
PasswordAuthentication yes
```

Después, reinicia el servicio SSH para aplicar los cambios:

```
$ sudo service ssh restart
```

Autenticación mediante clave pública

La autenticación mediante clave pública es más segura que la autenticación por contraseña. Cada usuario genera un par de claves (pública y privada) y la clave pública se almacena en el servidor. Para habilitar este método, asegúrate de que la opción PubkeyAuthentication esté habilitada en /etc/ssh/sshd_config. También, cada usuario debe copiar su clave pública en el archivo ~/.ssh/authorized_keys de su cuenta en el servidor.

Como hacerlo: **1. Generar un par de claves SSH en tu máquina cliente** Si aún no tienes un par de claves SSH, puedes generar uno en tu máquina cliente (no en el servidor) utilizando el siguiente comando:

```
$ ssh-keygen
```

Asegúrate de seguir las instrucciones y, cuando se te pregunte dónde guardar la clave, utiliza la ubicación predeterminada (~/.ssh/id_rsa) y establece una contraseña segura si lo deseas. Este comando creará dos archivos id_rsa con la clave privada y id_pub con la clave pública

2. Copiar la clave pública al servidor Ahora, copia tu clave pública (normalmente se encuentra en ~/.ssh/id_rsa.pub) al servidor Ubuntu. Puedes hacerlo usando el comando ssh-copy-id. Asegúrate de reemplazar usuario con tu nombre de usuario en el servidor y servidor con la dirección IP o el nombre de host del servidor:

```
$ ssh-copy-id usuario@servidor
```

Se te pedirá la contraseña del usuario en el servidor para completar la copia de la clave pública. El comando ssh-copy-id es una utilidad que se utiliza para copiar la clave pública de un usuario al archivo ~/.ssh/authorized_keys en el servidor

3. Configurar OpenSSH para la autenticación mediante clave pública Asegúrate de que la autenticación mediante clave pública esté habilitada en la configuración de OpenSSH. Para hacerlo, edita el archivo de configuración del servidor SSH:

```
$ sudo nano /etc/ssh/sshd_config
```

Asegúrate de que las siguientes líneas estén configuradas de esta manera:

```
PubkeyAuthentication yes
PasswordAuthentication no
```

La primera línea habilita la autenticación mediante clave pública y la segunda deshabilita la autenticación mediante contraseña para mejorar la seguridad.

Autenticación mediante certificado

https://smallstep.com/blog/ssh-vs-x509-certificates/

https://sergiobelkin.com/posts/como-usar-certificados-ssh-para-autenticar/

PASOS:

1. **Generación de Certificados:** En lugar de simplemente intercambiar claves públicas, se generan certificados SSH. Estos certificados son firmados por una autoridad de certificación (CA) y contienen información sobre la clave pública del usuario, restricciones de uso y una firma digital.
2. **Autoridad de Certificación (CA):** La CA es una entidad de confianza que emite y firma certificados. Los servidores SSH y los clientes deben confiar en la misma CA.
3. **Firma Digital:** El certificado SSH incluye una firma digital generada por la CA. Esto asegura que el certificado no ha sido alterado y proviene de una fuente confiable.
4. **Intercambio del Certificado:** En lugar de enviar solo la clave pública al servidor, el usuario envía su certificado SSH firmado. El servidor puede verificar la autenticidad del certificado mediante la firma digital y permitir o denegar el acceso en consecuencia.

Empezamos.....

Si aún no tienes un par de claves SSH, puedes generar uno en tu máquina cliente (no en el servidor) utilizando el siguiente comando:

```
$ ssh-keygen
```

Asegúrate de seguir las instrucciones y, cuando se te pregunte dónde guardar la clave, utiliza la ubicación predeterminada (~/.ssh/id_rsa) y establece una contraseña segura si lo deseas. Este comando creará dos archivos id_rsa con la clave privada y id_pub con la clave pública

En un servidor crear un par de claves para firmar claves de usuario.

```
cd /etc/ssh
sudo ssh-keygen -f user_ca
```

Agregar en el archivo /etc/ssh/sshd_config:

```
TrustedUserCaKeys /etc/ssh/user_ca.pub
```

Reiniciar el servicio

```
$ systemctl restart ssh
```

Para lograr que los certificados que vamos a generar se puedan usar en otros servidores, habría que copiar en ellos la clave pública (user_ca.pub), agregar la misma línea y reiniciar el servicio ssh.

Copiar la clave pública del cliente ssh al servidor.

```
cliente --> scp ~/.ssh/id_rsa.pub admini@192.168.1.136:/home/id_rsa.pub
cliente -->ssh admini@192.168.1.136
servidor -->cp id_rsa.pub /etc/ssh
```

Podriamos ahorrarnos faena dejandolo en el home (mejorar)

Generar un certificado a partir de la clave pública.

```
$ sudo ssh-keygen -s /etc/ssh/user_ca -I user_cliente1 -n cliente1 -V +52w id_rsa.pub
```

```
Enter passphrase:
Signed user key id_rsa-cert.pub: id "user_cliente1" serial 0 for cliente1 valid from 2023-11-02T18:07:0
```

Copiar el certificado al host del usuario.

```
$ scp admini@192.168.1.136:/home/admini/id_rsa-cert.pub ~/.
```

Autenticarse con el certificado del usuario.

```
$ ssh-i ~/id_rsa-cert.pub admini@192.168.1.136
```

Autenticación mediante autenticación multifactor (MFA)

La autenticación multifactor combina varios métodos de autenticación para mejorar la seguridad. Puedes habilitar MFA en OpenSSH mediante herramientas de terceros como Google Authenticator.Autenticación mediante clave pública