SSH sin Contraseña

Podemos habilitar SSH con:

- Autenticación basada en contraseña
- Autenticación basada en clave pública

La autenticación basada en clave pública también se le conoce como SSH sin contraseña.

A veces nos puede parecer que las contraseñas son difíciles de recordar e incómodas, en especial si estamos en un entorno donde necesitamos poner una contraseña con frecuencia.

Algunas **ventajas de usar SSH sin contraseña** son:

- Ofrece un inicio de sesión fácil y no interactivo. Los usuarios no tienen que escribir la contraseña para cada nueva sesión.
- Es una alternativa más segura que utilizando contraseñas, ya que funciona con criptografía de clave pública-privada.
- Es más segura.
- Brinda una mejor gestión de autenticación y autorización.
- Es una buena solución tanto para infraestructuras pequeñas como grandes.
- Es fácil de construir y mantener.

PASOS PARA LA CONFIGURACIÓN SIN CONTRASEÑA

① Generar una clave pública.

Para generar una clave pública y privada se usa el comando:

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

La **opción -t** significa tipo, mientras que **RSA** es el protocolo utilizado para la generación de claves. RSA es el tipo predeterminado, así que también puedes usar la versión más simple del comando:

ssh-keygen

La clave predeterminada es de 2048 bits. Sin embargo, si deseas una seguridad más fuerte, puedes cambiar el valor a 4096 bits utilizando **la opción -b**. En ese caso, el comando será:

ssh-keygen -t rsa -b 4096

Se trata de un proceso interactivo de generación de claves y por ello se hacen algunas preguntas, como:

- Escribe el nombre del archivo en el que guardarás la clave (~/.ssh/id_rsa)
- Escribe la passphrase (vacía si quieres dejarlo sin passphrase)

Se puede presionar Intro para ambas preguntas y el sistema tomará los valores predeterminados.

La **passphrase** es una cadena de caracteres, usada para cifrar la clave privada; sin embargo, no es obligatoria y puede dejarse en blanco.

La clave privada se guardará en la ubicación predeterminada: **.ssh/id_rsa.**

La clave pública se guardará en el archivo **.ssh/id_rsa.pub**.

Se pueden verificar los archivos utilizando cualquier editor.

② **Copiar la clave que se ha generado en el paso 1.**

La copia de la clave pública en una máquina de destino se puede hacer de tres maneras:

- Usando el comando ssh-copy-id
- Usando SSH
- Manualmente

La primera opción es la más utilizada y la más rápida, por tanto, nosotros utilizaremos esa opción, la cual se explica a continuación.

La sintaxis básica para usar este comando (ssh-copy-id) es la que se detalla a continuación:

ssh-copy-id remote_username@remote_IP_Address

Al escribirlo recibirás un mensaje con la contraseña de la máquina remota. Una vez que la autenticación sea exitosa, la clave pública SSH generada se agregará al archivo authorized_keys del equipo remoto. Después de escribir la clave, la conexión se cerrará automáticamente.

③ **Probar el funcionamiento.**

Para probar que todo ha ido bien, se puede intentar acceder al servidor remoto a través del servidor de origen. La sintaxis del comando sería:

ssh remote_username@remote_IP_Address

Y si todo funcionó correctamente, se podrá iniciar sesión automáticamente sin tener que escribir la contraseña.