**1. Introducción a SSH**

SSH cifra la conexión entre el cliente y el servidor, proporcionando una comunicación segura sobre una red no segura, como Internet. Para utilizar SSH en Linux, debes asegurarte de tener el software SSH instalado en tu sistema. En la mayoría de las distribuciones de Linux, SSH viene preinstalado.

**2. Conectarse a un Servidor SSH**

Para conectarte a un servidor SSH, utiliza el siguiente comando en la terminal:

bash

ssh usuario@direccion\_ip\_o\_nombre\_de\_host

Ejemplo:

bash

ssh usuario@192.168.0.1

**3. Autenticación con Contraseña**

Cuando te conectas por primera vez a un servidor, SSH te pedirá la contraseña del usuario remoto. Ingresarás la contraseña asociada con el usuario que intentas utilizar.

**4. Autenticación con Clave SSH**

La autenticación mediante clave SSH es más segura que el uso de contraseñas. Para generar un par de claves SSH en tu máquina local, utiliza el siguiente comando:

bash

ssh-keygen -t rsa -b 2048

Este comando generará un par de claves pública y privada. La clave pública (id\_rsa.pub) se encuentra en ~/.ssh/ y es lo que debes copiar al servidor remoto. Puedes hacerlo manualmente o usando el comando ssh-copy-id:

bash

ssh-copy-id usuario@direccion\_ip\_o\_nombre\_de\_host

**5. Configuración Avanzada de SSH**

El archivo de configuración de SSH se encuentra en /etc/ssh/sshd\_config. Puedes personalizar diversas configuraciones, como el puerto de escucha, la autenticación y las claves permitidas.

**6. Copiar Archivos de Forma Segura con SCP**

SSH también permite copiar archivos de forma segura entre sistemas. Utiliza scp (Secure Copy Protocol) para copiar archivos de un sistema a otro:

bash

scp archivo usuario@direccion\_ip\_o\_nombre\_de\_host:/ruta/destino

**7. Cierre de Sesión SSH**

Para cerrar una sesión SSH, simplemente escribe exit o presiona Ctrl + D en la terminal.