Conexión remota vía SSH

¿Qué es SSH?

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.

Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

Cualquier usuario de Linux, macOS o Windows puede usar SSH en su servidor remoto directamente desde la ventana del terminal. Puedes ejecutar comandos shell de la misma manera que lo harías si estuvieras operando físicamente el equipo remoto.

El comando **SSH** consta **de 3 partes** distintas:

ssh {user}@{host}

- **SSH** le indica a tu sistema que desea abrir una Conexión de Shell Segura y cifrada.
- **{user}** representa la cuenta a la que deseas acceder. Por ejemplo, puede que quieras acceder al usuario root, que es básicamente para el administrador del sistema con derechos completos para modificar cualquier cosa en el sistema.
- **{host}** hace referencia al equipo al que quieres acceder. Esto puede ser una dirección IP (por ejemplo, 244.235.23.19) o un nombre de dominio (por ejemplo, www.xyzdomain.com).

Al pulsar enter, se te pedirá que escribas la contraseña de la cuenta solicitada. Al escribirla, nada aparecerá en la pantalla, pero tu contraseña, de hecho, se está transmitiendo. Una vez que hayas terminado de escribir, pulsa enter una vez más. Si tu contraseña es correcta, verás una ventana de terminal remota.

Instalar servidor SSH en Linux Ubuntu

Para instalar el servicio SSH en la máquina Linux Ubuntu se ejecuta el siguiente comando

```
sudo apt-get install openssh-server
```

```
pru@pru-VirtualBox:~$ sudo apt-get install openssh-server
[sudo] contraseña para pru:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  libflashrom1 libftdi1-2 libllvm13
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh-askpass
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 10 no actualizados.
Se necesita descargar 750 kB de archivos.
Se utilizarán 6.046 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Para comprobar que funciona correctamente, ejecutamos el comando:

```
sudo service sshd status
```

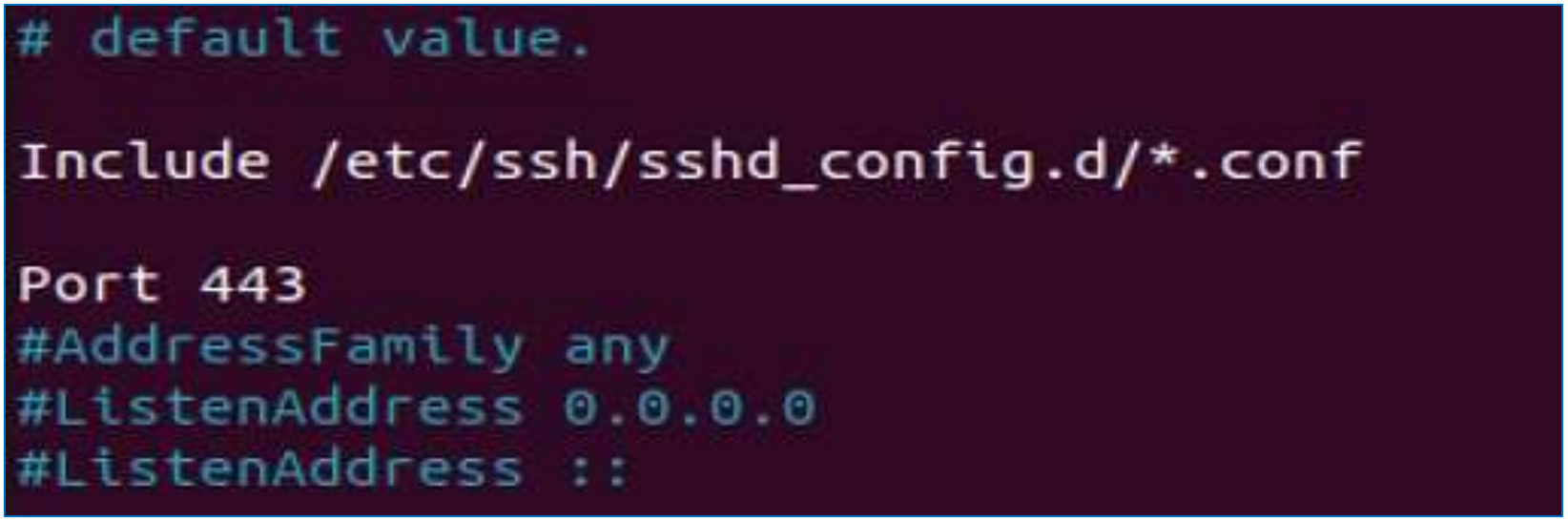
```
pru@pru-VirtualBox:~$ sudo  service sshd status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-04-29 04:46:54 WEST; 2min 24s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 6765 (sshd)
      Tasks: 1 (limit: 4597)
     Memory: 1.7M
        CPU: 15ms
     CGroup: /system.slice/ssh.service
             └─6765 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

abr 29 04:46:54 pru-VirtualBox systemd[1]: Starting OpenBSD Secure Shell server...
abr 29 04:46:54 pru-VirtualBox sshd[6765]: Server listening on 0.0.0.0 port 22.
abr 29 04:46:54 pru-VirtualBox sshd[6765]: Server listening on :: port 22.
abr 29 04:46:54 pru-VirtualBox systemd[1]: Started OpenBSD Secure Shell server.
```

Configuración de puerto 443

El puerto por defecto es el 22. Para cambiarlo al puerto 443, vamos al archivo de configuración y hacemos el cambio:

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



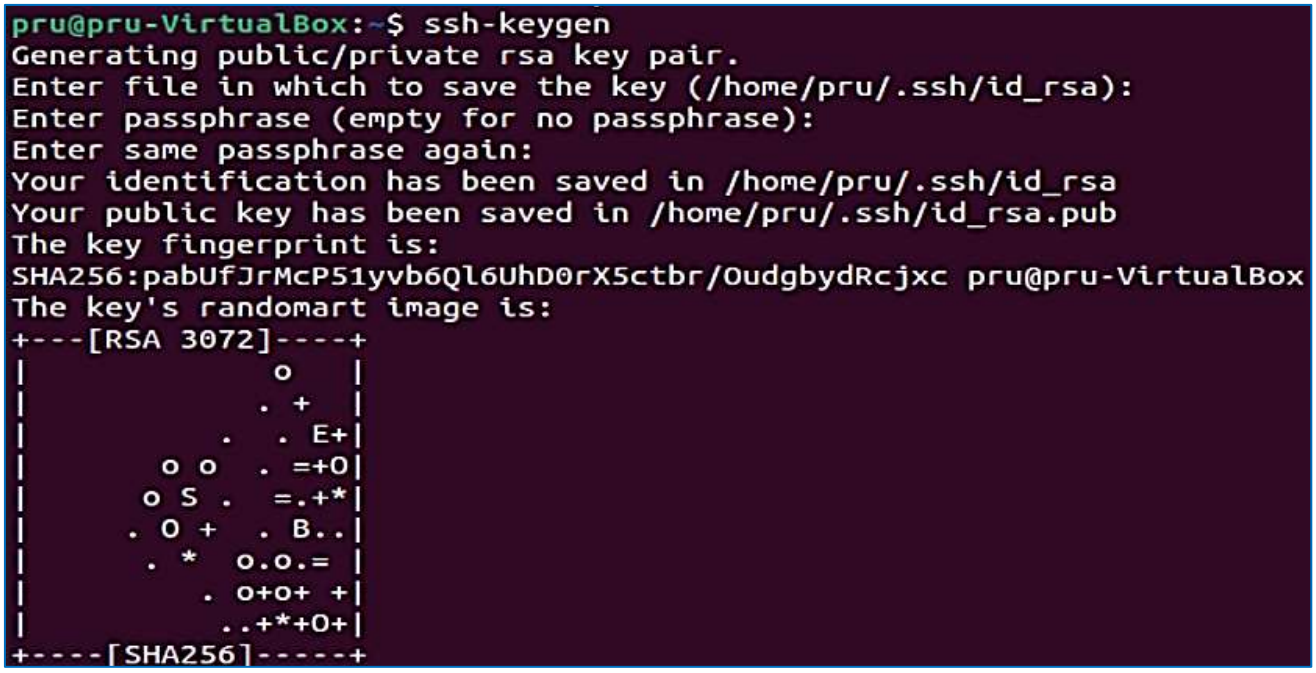
Y reiniciamos el servicio:

```
sudo service sshd restart
```

Ahora, vamos a crear una llave ssh, que nos va a generar una carpeta, en la cual se van a añadir las claves de los usuarios autorizados.

En primer lugar, escribimos el comando:

```
ssh-keygen
```



Esto genera el directorio /home/pru/.ssh (pru es el nombre de usuario en un equipo)

Generaremos el fichero authorized_keys:

```
touch /home/pru/.ssh/authorized_keys
```

```
pru@pru-VirtualBox:~$ touch  /home/pru/.ssh/authorized_keys
pru@pru-VirtualBox:~$ ls /home/pru/.ssh
authorized_keys  id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

Ahora, desde el cliente ssh nos conectamos, por el puerto 443:

```
C:\Users\Usuario>ssh pru@192.168.1.44 -p 443
The authenticity of host '[192.168.1.44]:443 ([192.168.1.44]:443)' can't be established.
ED25519 key fingerprint is SHA256:NGk89C7Pa1Z8yF0syUIdIxd++SLqH/BTh6xWmUnJ0j8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.44]:443' (ED25519) to the list of known hosts.
pru@192.168.1.44's password:
```

Se establece la conexión. Salimos con exit.

```
Last login: Wed May 31 09:25:46 2023 from 192.168.1.36
pru@pru-VirtualBox:~$ exit
cerrar sesión
Connection to 192.168.1.44 closed.
```