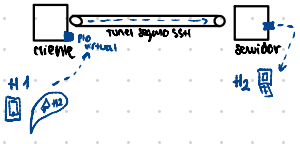
T5: Secure Shell (SSH)

Secure Shell (SSH)

- Permite acceso remoto de forma 🔒
- Funcidad básica: conexiones 🔒 modo terminal (+ Autenticación usuario)
- Funcidades avanzadas: Autenticación Fuerte ⇄ 🔒 de ficheros / Ficheros cifrados
  SSH 1 y SSH 2
  ↳ +Nivel & +Fiabilidad

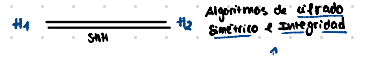


OpenSSH

- OpenSource para SSH (Unix)
  Cliente (SSH) | Servidor (SSHd)
- Características:
  - reenvío por X11 (sesiones X Windows)
  - reenvío por puertos
  - Interoperabilidad (soporte versión 1 y 2)
  - Soporte SFTP
  - Compresión datos
- Componentes
  - SSH: Cliente
  - SSHd: Servidor
  - SFTP: Cliente FTP 🔒
  - SCP: Copia de archivos segura con SSH
  - SFTP-server: servidor FTP (invoc. autom. con SSHd)
  - ssh-keygen: Generador clave pública / privada
  - ssh-copy-id: Copiar claves públicas al servidor

Establecimiento canal 🔒

1) SSH negocia capacidades extremos



2) ⇄🔒 de clave compartida base para

3) Establecer canal 🔒 ⇒ clave pública / privada del servidor (RSA, DSA, ECDSA, ...)

Clave Pública → Cliente acepta 1ª conexión
Almacena ? ~/.ssh/known_hosts
conexiones posteriores ✔ comprobará

Terminal clave ? ssh-keygen -R "hostname"

Clave Priv → Cliente Exige
↳ Si - (cifrada) + clave pública
Servidor

canal seguro Activado

Autenticación del Cliente

2 modos de Autenticación

⇄ contraseñas: user + password

Clave Pública & Priv.:

Cliente ↳ Parja claves ← Pública / Priv
Clave pública ? ~/.ssh/id_rsa.pub
Almacena ? Servidor: ~/.ssh/authorized_keys
puede comprar con ssh-copy-id clave_pública servidor

Clave privada → Almacena ? Cliente ~/ssh/id_rsa
protegida con frase de paso
↳ usa reto-respuesta para autenticar al Cliente
opción -i para indicar ubi de la clave

Autenticación por host en desuso

Configuración servidor SSH

Archivo /etc/ssh/sshd_config directivas:

- **Port**. Puerto de escucha [22]
- **Protocol**. Versiones de SSH soportadas [2]
- **PermitRootLogin**. Permite el acceso de root [no]
- **AllowGroups**. Especifica qué grupos tienen acceso por SSH [todos los grupos]
- **PasswordAuthentication**. [yes]
- **PubkeyAuthentication**. [yes]
- **HostbasedAuthentication**. [no]
- **PermitEmptyPasswords**. Se permite el acceso a cuentas que no posean clave. [no]
- **StrictModes**. Especifica si sshd debe comprobar los permisos de los ficheros (600) y del directorio ~/.ssh (700) antes de aceptar una conexión [yes]

Autentificación lenta:
UseDNS no
GSSAPIAuthentication no

⚠ ssh_config ⇒ cliente
sshd_config ⇒ Servidor

Intercambio archivos

SCP ⟵ directorio ⟶ user@IP_maquina:⟵directorio⟶
? Windows (Principal) ? Ubuntu (VM)

SFTP user@IP_maquina:⟵directorio⟶
↳ get ⟵archivo⟶
↳ Put ⟵archivo⟶

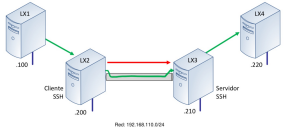
Túneles Dinámicos

usar SSH como equipo intermedio

Opción -D de SSH

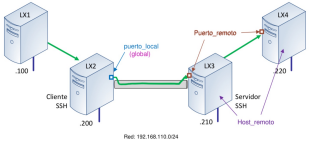
ANONIMIZAR

Túneles SSH



- Redirige tráfico (Transmisión SSH) puerto local
  Para su entrega a un equipo y puerto visibles desde máquina remota o viceversa
- Protege ⇄ SSH / \ -L -R local remoto — TCP@ IP_maquina
- Sintaxis Linux:

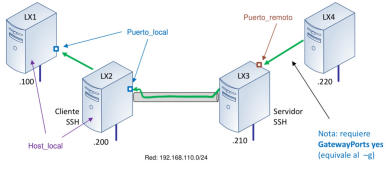
```
ssh [-g] -L puerto_local:host_remoto:puerto_remoto
usuario@servidor
ssh -R puerto_remoto:host_local:puerto_local
usuario@servidor
```




```
ssh [-g] -L puerto_local:host_remoto:puerto_remoto
usuario@servidor
```

-g: cualquiera q sea capaz de llegar a este puerto podrá usar el túnel [Filtros IP con IPtables, ...]

Inversa:

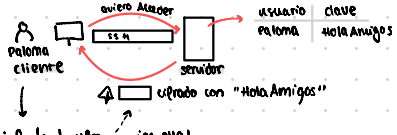



```
ssh -R puerto_remoto:host_local:puerto_local
usuario@servidor
```

T5: Secure Shell (SSH)

Apuntes Extra de Clase

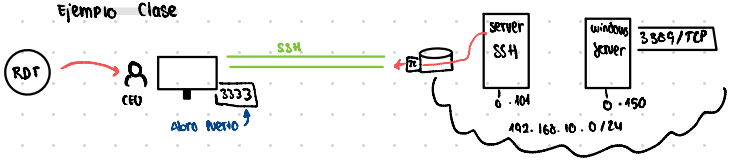
- → intercambio archivos scp, sftp
- → túneles
- → Autenticación "Fuerte" → Clave Pública & Privada



si A lo descifra → ¡es ella!

sshpass utilidad q te permite inyectar la contraseña cuando te la piden (Para AUTOMATIZAR)

Ejemplo Clase



? CEU quiero abrir conexión a Windows Sewer

¿Cómo? Mediante Túnel SSH con un puerto Local (ej: 3333 q está vacío)

? Putty

- Abrir sesión SSH con ip_maquina_ssh
- connection >> SSH >> definir un Túnel mientras abro la conexión

SourcePort: 3333
Destination: ip_maquina_windows : Puerto
192.168.10.150 : 3389
ADD

- vuelvo a la sesión y conecto

CEU (windows 11) → ? Conexión a Escritorio Remoto
localhost:3333
¡¡conectado al Windows Sewer!!

Necesito { Acceso a SSH; Servicio conexión remoto activado; user + Password en Windows Sewer }

Parte Práctica a Ordenador

La clave Privada se suele proteger con una clave de Paso

#SSh root@ip_mimaquina [Cliente]

- Genero pareja de clave Pública y Privada
  - #ssh-keygen → te saldrá la opción de frase de Paso
- #ls /root/.ssh → OO los archivos
- Vamos a copiar la clave Pública ? Servidor
  - # ssh copy-id -i /root/.ssh/id_rsa.pub teo@ip_maquina_ssh
    - /root/.ssh/id_rsa.pub: ubicar clave Pública

#SSh root@ip_maquina_ssh [Servidor]

- OO archivos copiados
  - #ls /.ssh
    - OO authorized_keys

Investigar USO sshpass

```
sudo apt-get install sshpass
```

```
sshpass -p 'tu_contraseña' ssh usuario@hostname
```