[Remoto] SSH: Primer contacto

Conexiones a través de ssh

- SSH es un programa que permite acceder a otro ordenador a través de la red, ejecutar comandos en la máquina remota y mover ficheros entre dos máquinas. Provee autenticación y comunicaciones seguras sobre canales inseguros. Es un reemplazo de `rlogin`, `rsh` y `rcp`.
- Cuando nos conectamos con un cliente SSH a un equipo remoto, los comandos, programas y scripts que lancemos desde el cliente SSH se ejecutarán en la máquina remota. Por lo tanto, utilizarán los recursos de la máquina remota (CPU, memoria, disco, etc). Esta arquitectura es muy útil, por ejemplo, para tener un servidor de aplicaciones más potente y varios clientes que ejecutan aplicaciones en dicho servidor.
- Por defecto, y por seguridad, `ssh` no permite conectarse como `root` a la máquina remota. Podemos conectarnos como un usuario normal del equipo y luego en la consola pasar a `root` con `su`... O podemos modificar la configuración para permitir el acceso del `root` a través de `ssh`, algo que no se recomienda pues rebajaría el nivel de seguridad del equipo.

Instalación y activación

- Instalaremos ssh en los equipos que se van a conectar.

```
# aptitude install ssh
```

  y a su vez activaremos el servicio con

```
# service ssh start
```

Utilización

```
usuario@host:~$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
```

Permitir conectarse por ssh como root (peligroso)

Para editar el archivo `/etc/ssh/sshd_config` en Debian 13 y realizar configuraciones como permitir conexión `ssh` como `root` (u otros ajustes), seguiremos estos pasos:

1. Abrir una terminal y asegurarnos de tener privilegios de superusuario.
2. Hacer una copia de seguridad del archivo original por precaución:

```
# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
```

3. Editar el archivo con un editor de texto en consola, el más común es `nano`:

```
# nano /etc/ssh/sshd_config
```

4. Dentro del editor nano:
    1. Usar las teclas de cursor para desplazarnos por el archivo.
    2. Localizar la línea a modificar. Por ejemplo:
        1. Para permitir acceso root cambiar o añadir: `PermitRootLogin yes`
        2. Para permitir autenticación por contraseña: `PasswordAuthentication yes`
        3. O cualquier otro parámetro de configuración (puerto SSH, usuarios permitidos, etc.)
    3. Si la línea está comentada con un `#`, eliminar ese símbolo para activar la línea.
    4. Realizar las modificaciones necesarias.
5. Guardar los cambios y salir del editor:
    1. Presionar `Ctrl + X` para salir.
    2. Cuando pregunte si guardar, presionar Y.
    3. Presionar `Enter` para confirmar el nombre del archivo.
6. Reiniciar el **servicio ssh** para que los cambios tengan efecto:

```
# systemctl restart ssh
```

7. Ya podemos probar la conexión ssh con la nueva configuración.

Apoyo

1. Ejecutar aplicaciones gráficas via SSH
2. Servidor de terminales con SSH
3. Cómo configurar ssh de forma que no nos pida una contraseña
4. ¿Cómo ejecutar aplicaciones gráficas a través de SSH?