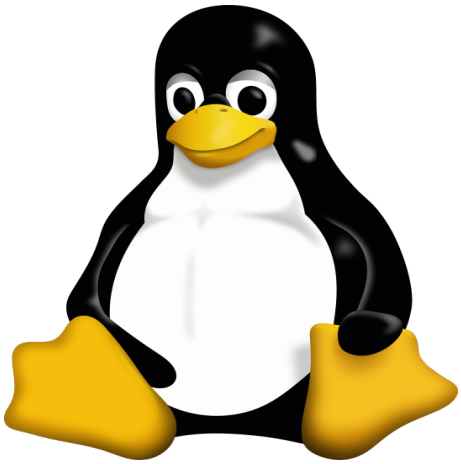

Bootcamp Especialidad GNU/Linux (2023)

Lab 04 - Procesos, servicios, demonios y su monitorización

Pedro Antonio Mayorgas Parejo

7 de agosto de 2023

Índice

1. Usuario remoto y configuración de SSHD

Creamos un usuario remoto que permita el acceso con SSH, para ello tenemos que tener un usuario que podamos autenticar en el servidor.

```
# Creamos el usuario
sudo adduser pedrolab04
# Editamos el fichero de sshd
sudo nano /etc/ssh/sshd_config
```

Las configuraciones editadas son las siguientes:

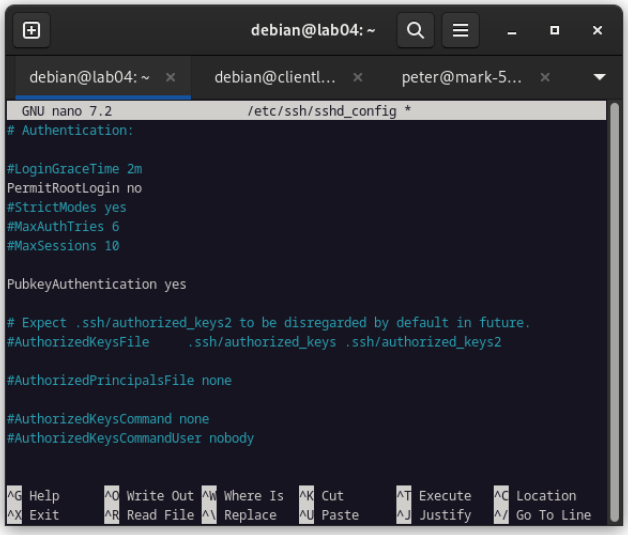

Figura 1: Aquí indicamos las opciones de seguridad de no autenticar el usuario root y permitir por norma general la autenticación por clave pública.

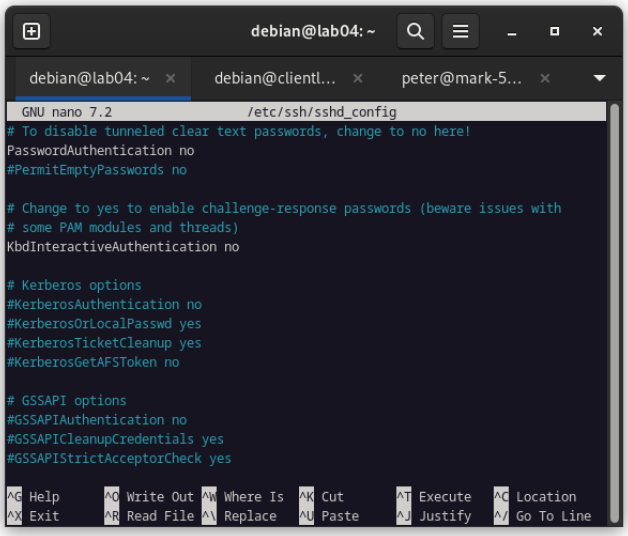

Figura 2: Aquí desactivamos la autenticación por contraseña por norma general, forzando el uso de par de claves.

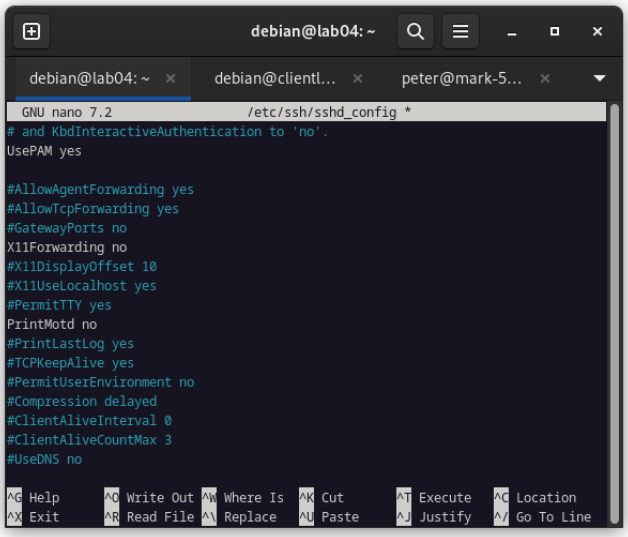

Figura 3: Aquí desactivamos el uso de X11 ya que el servidor no tiene entorno gráfico.

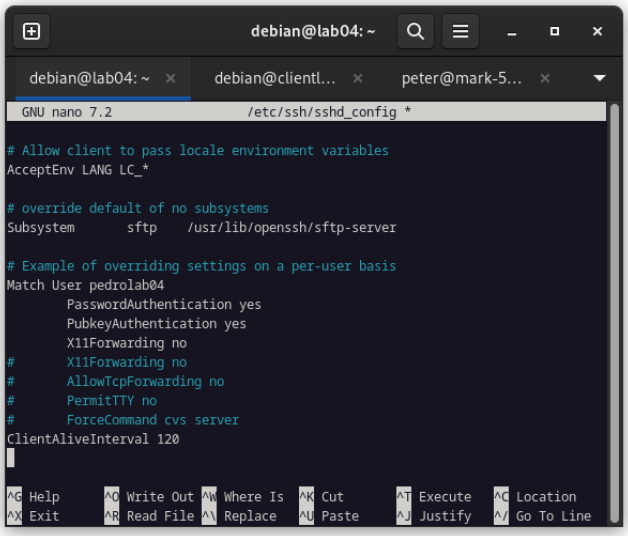

Figura 4: Aquí hacemos un mach del usuario que se ha creado para la conectividad SSH, se permite el uso de contraseña para permitir la copia de la clave con ssh-copy-id.

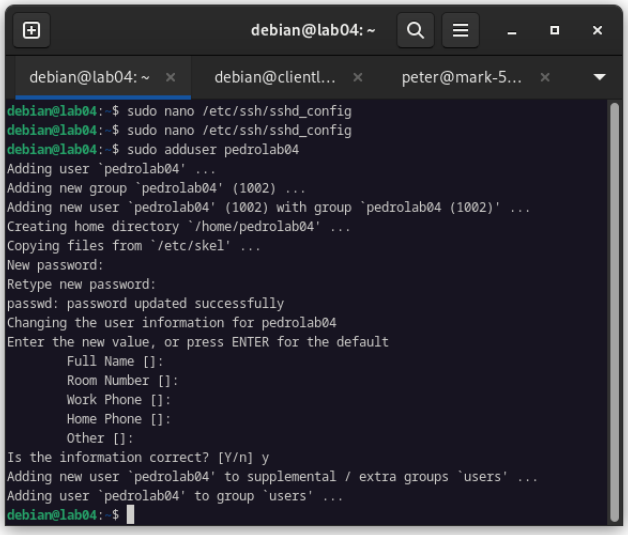

Figura 5: Creación del usuario.

Ahora reiniciamos el servicio de sshd, para aplicar los cambios y verificamos que no exista ningún error de configuración.

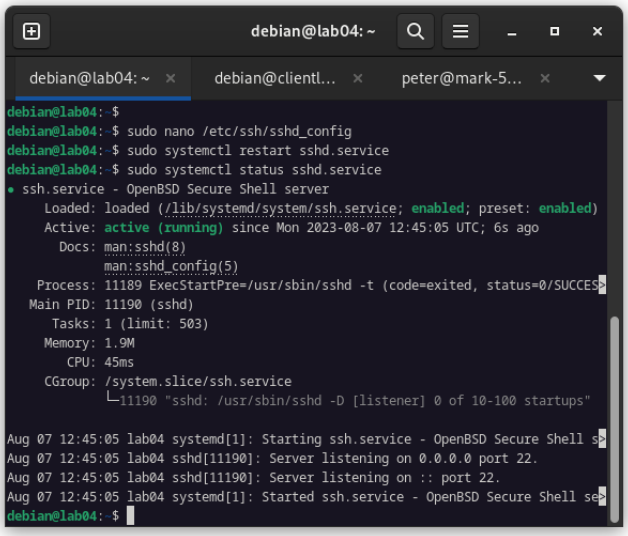

Figura 6: Reinicio del servicio de SSHd.

```
sudo systemctl restart sshd.service
sudo systemctl status sshd.service
```

2. Proceso de generación de par de claves en el cliente y copia en el servidor

Ahora en el cliente debemos crear un par de claves de RSA, para poder usarlas para autenticación sin contraseña en el lado del servidor. El comando utilizado es:

```
ssh-keygen
```

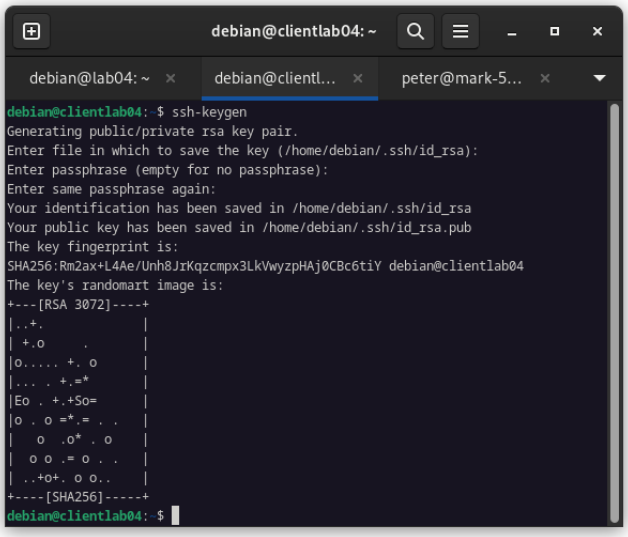

Figura 7: Generación de la clave.

Una vez generada debemos copiarla en el servidor de destino hacia el usuario con el que queramos autenticarnos, en este caso pedrolab04, dicho usuario cuando se autentique copiará la clave pública id_rsa.pub que se almacenará en su HOME, en concreto en un directorio oculto localizado en **.ssh/authorized_keys**.

Comando para la copia de la clave:

```
ssh-copy-id pedrolab04@192.168.122.59
```

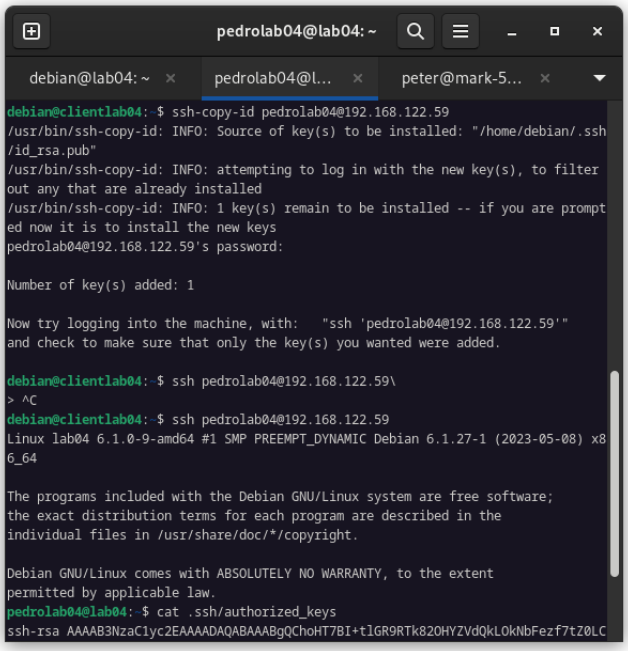

Figura 8: Copia de la clave y autenticación sin contraseña.

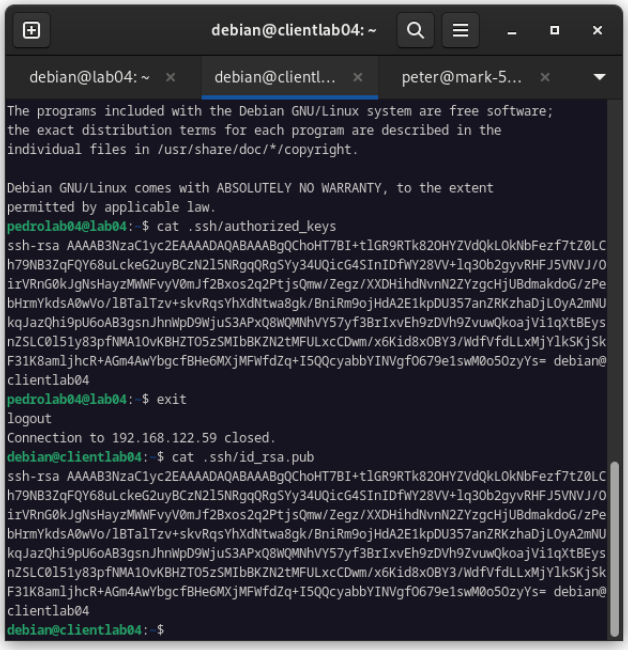

Figura 9: Comparación del fichero authorized_keys con la clave públicas.

Una vez termiando, debemos realizar el siguiente cambio para desactivar la autenticación por contraseña y permitir solo el uso de clave pública.

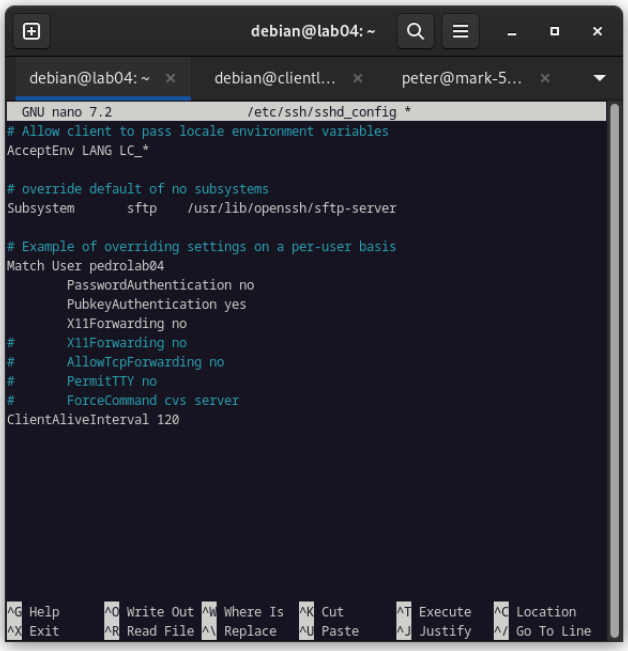

Figura 10: Desactivación del uso de contraseñas.

Finalmente reiniciamos el servicio.

```
sudo systemctl restart sshd.service
sudo systemctl status sshd.service
```

3. Logs de ssh

Antes en el intento de copiar la clave, he realizado un intento erróneo para poder generar entradas en el log de intentos fallados y de intentos legítimos. En primer lugar después de iniciar el servicio, se puede ver un intento fallido de pedrolab04 con contraseña incorrecta, luego se puede ver un intento legítimo que se corrresponde con el de la copia de la clave que es un comando generalmente y finalmente la autenticación sin contraseña legítima después de realizar la copia de seguridad.
El comando utilizado para ver dicho log es **journalctl**, en concreto con los siguientes parámetros:

```
sudo journalctl -u ssh
```

```
Aug 07 12:45:05 lab04 sshd[11190]: Server listening on :: port 22.
Aug 07 12:45:05 lab04 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Aug 07 12:52:12 lab04 sshd[11209]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 56956 [preauth]
Aug 07 12:52:12 lab04 sshd[11211]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35192 [preauth]
Aug 07 12:52:16 lab04 sshd[11213]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.122.50  user=pedrolab04
Aug 07 12:52:18 lab04 sshd[11213]: Failed password for pedrolab04 from 192.168.122.50 port 35196 ssh2
Aug 07 12:52:20 lab04 sshd[11213]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35196 [preauth]
Aug 07 12:52:21 lab04 sshd[11215]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35210 [preauth]
Aug 07 12:52:21 lab04 sshd[11217]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35214 [preauth]
Aug 07 12:52:23 lab04 sshd[11219]: Accepted password for pedrolab04 from 192.168.122.50 port 35218 ssh2
Aug 07 12:52:23 lab04 sshd[11219]: pam_unix(sshd:session): session opened for user pedrolab04(uid=1002) by (uid=0)
Aug 07 12:52:23 lab04 sshd[11219]: pam_env(sshd:session): deprecated reading of user environment enabled
```

Figura 11: Fallo de intento de contraseña y intento correcto con copia de clave visto en el log.

```
Aug 07 12:52:23 lab04 sshd[11219]: pam_unix(sshd:session): session closed for user pedrolab04
Aug 07 12:52:40 lab04 sshd[11241]: Accepted publickey for pedrolab04 from 192.168.122.50 port 42802 ssh2: RSA SHA256:Rm2ax+L4Ae/Unh8JrKqzcmpx3LkVwyzpHAj0CBc6tiY
Aug 07 12:52:40 lab04 sshd[11241]: pam_unix(sshd:session): session opened for user pedrolab04(uid=1002) by (uid=0)
Aug 07 12:52:40 lab04 sshd[11241]: pam_env(sshd:session): deprecated reading of user environment enabled
Aug 07 12:54:51 lab04 sshd[11190]: Received signal 15; terminating.
Aug 07 12:54:51 lab04 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
```

Figura 12: Uso del par de claves visto en el log.

```
Aug 07 12:45:05 lab04 sshd[11190]: Server listening on 0.0.0.0 port 22.
Aug 07 12:45:05 lab04 sshd[11190]: Server listening on :: port 22.
Aug 07 12:45:05 lab04 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Aug 07 12:52:12 lab04 sshd[11209]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 56956 [preauth]
Aug 07 12:52:12 lab04 sshd[11211]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35192 [preauth]
Aug 07 12:52:16 lab04 sshd[11213]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.122.50  user=pedrolab04
Aug 07 12:52:18 lab04 sshd[11213]: Failed password for pedrolab04 from 192.168.122.50 port 35196 ssh2
Aug 07 12:52:20 lab04 sshd[11213]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35196 [preauth]
Aug 07 12:52:21 lab04 sshd[11215]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35210 [preauth]
Aug 07 12:52:21 lab04 sshd[11217]: Connection closed by authenticating user pedrolab04 192.168.122.50 port 35214 [preauth]
Aug 07 12:52:23 lab04 sshd[11219]: Accepted password for pedrolab04 from 192.168.122.50 port 35218 ssh2
Aug 07 12:52:23 lab04 sshd[11219]: pam_unix(sshd:session): session opened for user pedrolab04(uid=1002) by (uid=0)
Aug 07 12:52:23 lab04 sshd[11219]: pam_env(sshd:session): deprecated reading of user environment enabled
Aug 07 12:52:23 lab04 sshd[11219]: pam_unix(sshd:session): session closed for user pedrolab04
Aug 07 12:52:40 lab04 sshd[11241]: Accepted publickey for pedrolab04 from 192.168.122.50 port 42802 ssh2: RSA SHA256:Rm2ax+L4Ae/Unh8JrKqzcmpx3LkVwyzpHAj0CBc6tiY
Aug 07 12:52:40 lab04 sshd[11241]: pam_unix(sshd:session): session opened for user pedrolab04(uid=1002) by (uid=0)
Aug 07 12:52:40 lab04 sshd[11241]: pam_env(sshd:session): deprecated reading of user environment enabled
Aug 07 12:54:51 lab04 sshd[11190]: Received signal 15; terminating.
```

Figura 13: Visión general de todo el proceso en el log.

Fuentes [1] [2]

[1] https://manpages.debian.org/testing/openssh-server/sshd_config.5.en.html#LogLevel
[2] https://manpages.debian.org/testing/openssh-client/ssh_config.5.en.html