

BOOTCAMP ESPECIALIDAD GNU/LINUX (2023)

Lab 04 - Procesos, servicios, demonios y su monitorización

Pedro Antonio Mayorgas Parejo

7 de agosto de 2023

Índice

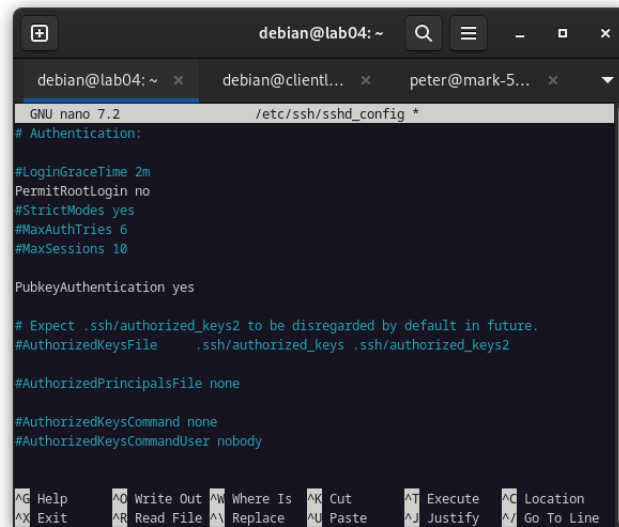
1	Usuario remoto y configuración de SSHD	3
2	Proceso de generación de par de claves en el cliente y copia en el servidor	7
3	Logs de ssh	10

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.

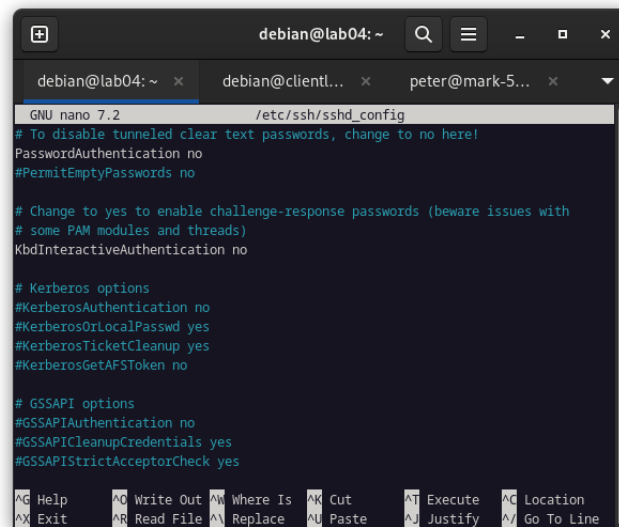
- 1 **# Creamos el usuario**
- 2 `sudo adduser pedrolab04`
- 3 **# Editamos el fichero de sshd**
- 4 `sudo nano /etc/ssh/sshd_config`

Las configuraciones editadas son las siguientes:



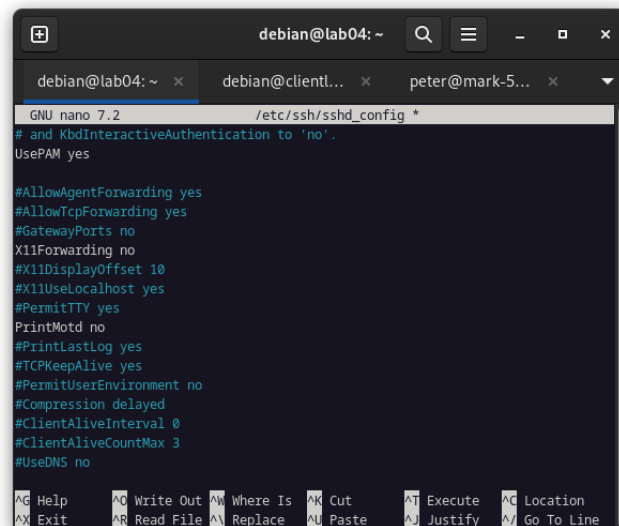
```
debian@lab04: ~  
debian@lab04: ~ x  debian@clientl... x  peter@mark-5... x  
GNU nano 7.2 /etc/ssh/sshd_config *  
# Authentication:  
  
#LoginGraceTime 2m  
PermitRootLogin no  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
  
PubkeyAuthentication yes  
  
# Expect .ssh/authorized_keys2 to be disregarded by default in future.  
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2  
  
#AuthorizedPrincipalsFile none  
  
#AuthorizedKeysCommand none  
#AuthorizedKeysCommandUser nobody  
  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^N Replace ^U Paste ^_ Justify ^_ Go To Line
```

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



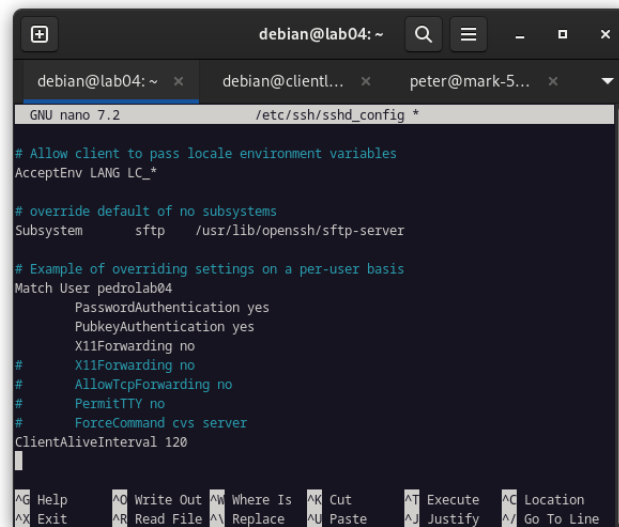
```
debian@lab04: ~  
GNU nano 7.2 /etc/ssh/sshd_config  
# To disable tunneled clear text passwords, change to no here!  
PasswordAuthentication no  
#PermitEmptyPasswords no  
  
# Change to yes to enable challenge-response passwords (beware issues with  
# some PAM modules and threads)  
KbdInteractiveAuthentication no  
  
# Kerberos options  
#KerberosAuthentication no  
#KerberosOrLocalPasswd yes  
#KerberosTicketCleanup yes  
#KerberosGetAFSToken no  
  
# GSSAPI options  
#GSSAPIAuthentication no  
#GSSAPICleanupCredentials yes  
#GSSAPIStrictAcceptorCheck yes  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

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



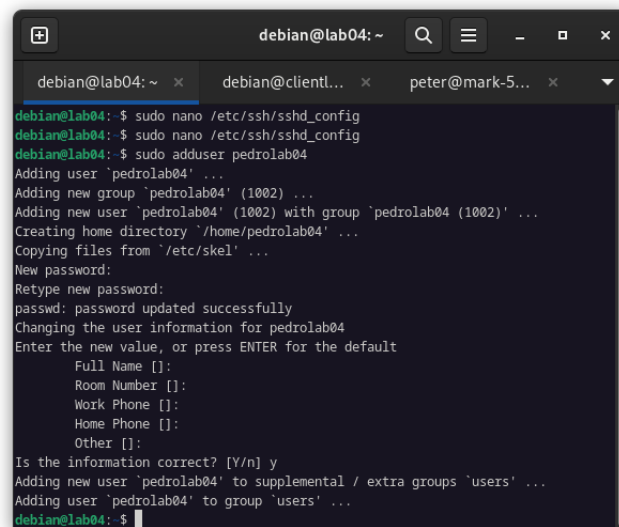
```
debian@lab04: ~  
GNU nano 7.2 /etc/ssh/sshd_config *  
# and KbdInteractiveAuthentication to 'no'.  
UsePAM yes  
  
#AllowAgentForwarding yes  
#AllowTcpForwarding yes  
#GatewayPorts no  
X11Forwarding no  
#X11DisplayOffset 10  
#X11UseLocalhost yes  
#PermitTTY yes  
PrintMotd no  
#PrintLastLog yes  
#TCPKeepAlive yes  
#PermitUserEnvironment no  
#Compression delayed  
#ClientAliveInterval 0  
#ClientAliveCountMax 3  
#UseDNS no  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

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



```
debian@lab04: ~  
GNU nano 7.2 /etc/ssh/sshd_config *  
  
# Allow client to pass locale environment variables  
AcceptEnv LANG LC_*  
  
# override default of no subsystems  
Subsystem sftp /usr/lib/openssh/sftp-server  
  
# Example of overriding settings on a per-user basis  
Match User pedrolab04  
    PasswordAuthentication yes  
    PubkeyAuthentication yes  
    X11Forwarding no  
#    X11Forwarding no  
#    AllowTcpForwarding no  
#    PermitTTY no  
#    ForceCommand cvs server  
ClientAliveInterval 120  
  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^V Replace ^U Paste ^J Justify ^_ Go To Line
```

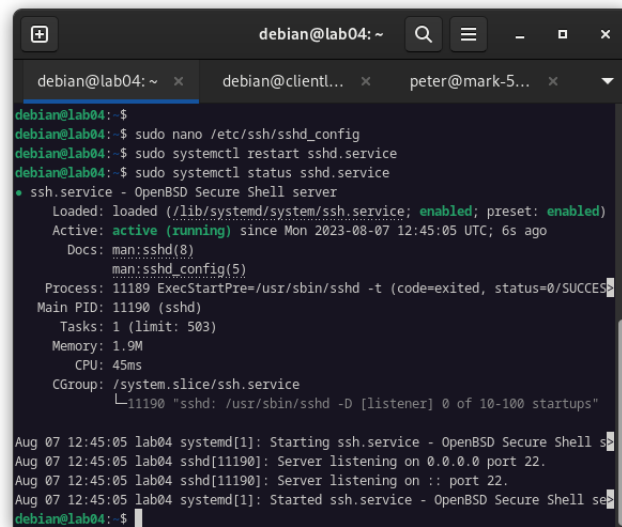
Figura 4: Aquí hacemos un match del usuario que se ha creado para la conectividad SSH, se permite el uso de contraseña para permitir la copia de la clave con ssh-copy-id.



```
debian@lab04: ~  
debian@lab04: $ sudo nano /etc/ssh/sshd_config  
debian@lab04: $ sudo nano /etc/ssh/sshd_config  
debian@lab04: $ sudo adduser pedrolab04  
Adding user 'pedrolab04' ...  
Adding new group 'pedrolab04' (1002) ...  
Adding new user 'pedrolab04' (1002) with group 'pedrolab04 (1002)' ...  
Creating home directory '/home/pedrolab04' ...  
Copying files from '/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for pedrolab04  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y  
Adding new user 'pedrolab04' to supplemental / extra groups 'users' ...  
Adding user 'pedrolab04' to group 'users' ...  
debian@lab04: $
```

Figura 5: Creación del usuario.

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

A terminal window titled 'debian@lab04: ~' with three tabs: 'debian@lab04: ~', 'debian@clientl...', and 'peter@mark-5...'. The terminal shows the following commands and output:

```
debian@lab04: $  
debian@lab04: $ sudo nano /etc/ssh/sshd_config  
debian@lab04: $ sudo systemctl restart sshd.service  
debian@lab04: $ sudo systemctl status sshd.service  
* ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)  
   Active: active (running) since Mon 2023-08-07 12:45:05 UTC; 6s ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Process: 11189 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  
    Main PID: 11190 (sshd)  
      Tasks: 1 (limit: 503)  
    Memory: 1.9M  
       CPU: 45ms  
   CGroup: /system.slice/ssh.service  
           └─11190 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Aug 07 12:45:05 lab04 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server:  
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:  
debian@lab04: $
```

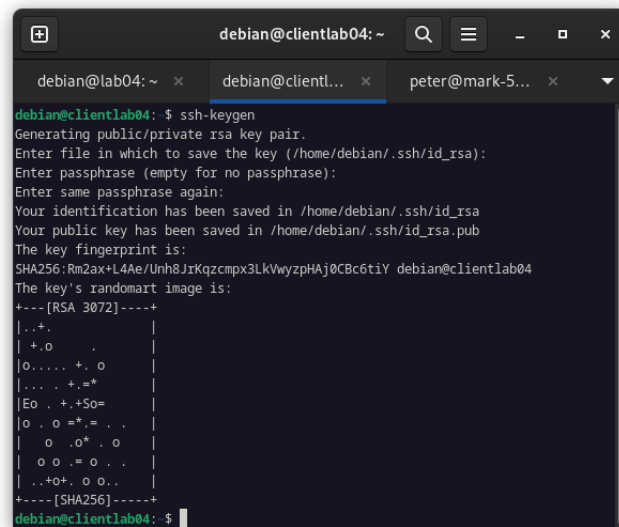
Figura 6: Reinicio del servicio de SSHd.

- 1 sudo systemctl restart sshd.service
- 2 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:

```
1 ssh-keygen
```



```
debian@clientlab04: ~  
debian@lab04: ~ x  debian@clientl... x  peter@mark-5... x  
debian@clientlab04: ~$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/debian/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/debian/.ssh/id_rsa  
Your public key has been saved in /home/debian/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:Rm2ax+L4Ae/Unh8JrKqzcmpx3LkVwyzpHAj0CBc6tiY debian@clientlab04  
The key's randomart image is:  
+---[RSA 3072]-----+  
|. .+. |  
|+.o. |  
|o....+.o |  
|...+.=* |  
|Eo.+.+So= |  
|o.o.=*,= |  
|o.o*.o |  
|o.o.=o. |  
|..+o+.o.o. |  
+---[SHA256]-----+  
debian@clientlab04: ~$
```

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:

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

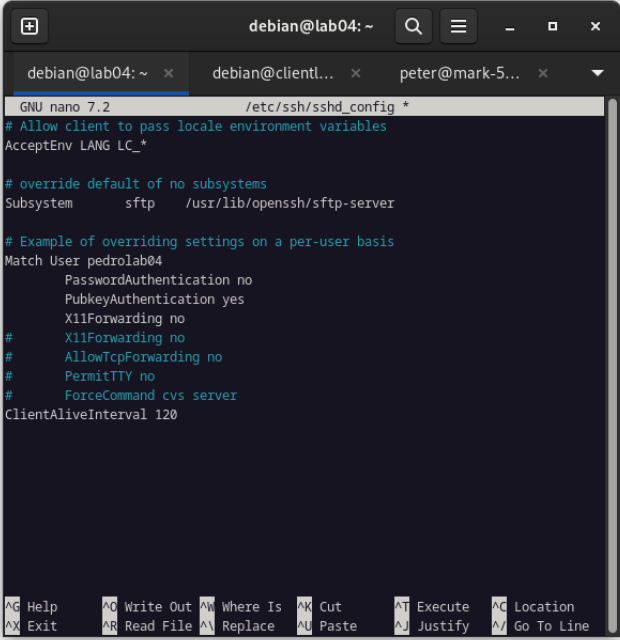
```
pedrolab04@lab04: ~  
debian@lab04:~ x pedrolab04@l... x peter@mark-5... x  
debian@clientlab04:~$ ssh-copy-id pedrolab04@192.168.122.59  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/debian/.ssh  
/id_rsa.pub"  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter  
out any that are already installed  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt  
ed now it is to install the new keys  
pedrolab04@192.168.122.59's password:  
Number of key(s) added: 1  
Now try logging into the machine, with: "ssh 'pedrolab04@192.168.122.59'"  
and check to make sure that only the key(s) you wanted were added.  
debian@clientlab04:~$ ssh pedrolab04@192.168.122.59  
> ^C  
debian@clientlab04:~$ ssh pedrolab04@192.168.122.59  
Linux lab04 6.1.0-9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1 (2023-05-08) x8  
6_64  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
pedrolab04@lab04:~$ cat .ssh/authorized_keys  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCchoHT7BI+tLGR9RTk820HYZVdQkLokNbFefz7tZ0LC
```

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

```
debian@clientlab04: ~  
debian@lab04:~ x debian@clientl... x peter@mark-5... x  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
pedrolab04@lab04:~$ cat .ssh/authorized_keys  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCchoHT7BI+tLGR9RTk820HYZVdQkLokNbFefz7tZ0LC  
h79NB3ZqFQY68uLckeG2uyBCzN215NRggQRgSYy34UQicG4SInIDfwY28VV+lq30b2gyvRHFJ5VNVJ/O  
iRVRNG0kJgNsHayzMMwFvyV0mJf2Bxos2q2PtjsQmw/Zegz/XXDHihdNvrN2ZYzgcHjUBdmakdoG/zPe  
bHmYkdsA0wVo/1BTalTzv+skvRqsYhXdnTwa8gk/BniRm9ojHdA2E1kpDU357anZKzhaDjL0yA2mNU  
kqJazQhi9pU6oAB3gsnJhnpD9WjuS3APxQ8WQMNhVY57yf3BrIxvEh9zDVh9ZvumQkoajV1iqxtBEys  
nZSLC0151y83pfNMA10vKBH2T05zSMIbBKZN2tMFULxcDwm/x6KId8x0BY3/WdfvfdLLxMjY1kSKjSk  
F31K8amljhcR+AGm4AwYbgcfBHeGMXjMFwfdZq+I5QQcyabbYINvgf0679e1swM0o50zyYs= debian@  
clientlab04  
pedrolab04@lab04:~$ exit  
logout  
Connection to 192.168.122.59 closed.  
debian@clientlab04:~$ cat .ssh/id_rsa.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCchoHT7BI+tLGR9RTk820HYZVdQkLokNbFefz7tZ0LC  
h79NB3ZqFQY68uLckeG2uyBCzN215NRggQRgSYy34UQicG4SInIDfwY28VV+lq30b2gyvRHFJ5VNVJ/O  
iRVRNG0kJgNsHayzMMwFvyV0mJf2Bxos2q2PtjsQmw/Zegz/XXDHihdNvrN2ZYzgcHjUBdmakdoG/zPe  
bHmYkdsA0wVo/1BTalTzv+skvRqsYhXdnTwa8gk/BniRm9ojHdA2E1kpDU357anZKzhaDjL0yA2mNU  
kqJazQhi9pU6oAB3gsnJhnpD9WjuS3APxQ8WQMNhVY57yf3BrIxvEh9zDVh9ZvumQkoajV1iqxtBEys  
nZSLC0151y83pfNMA10vKBH2T05zSMIbBKZN2tMFULxcDwm/x6KId8x0BY3/WdfvfdLLxMjY1kSKjSk  
F31K8amljhcR+AGm4AwYbgcfBHeGMXjMFwfdZq+I5QQcyabbYINvgf0679e1swM0o50zyYs= debian@  
clientlab04  
debian@clientlab04:~$
```

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

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



```
GNU nano 7.2 /etc/ssh/sshd_config *
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
Match User pedrolab04
    PasswordAuthentication no
    PubkeyAuthentication yes
    X11Forwarding no
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
ClientAliveInterval 120

^G Help      ^O Write Out ^M Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File ^N Replace  ^U Paste    ^J Justify  ^_ Go To Line
```

Figura 10: Desactivación del uso de contraseñas.

Finalmente reiniciamos el servicio.

- 1 `sudo systemctl restart sshd.service`
- 2 `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 corresponde 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:

```
1 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 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
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.
Aug 07 12:54:51 lab04 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
```

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

Fuentes ¹ ²

¹https://manpages.debian.org/testing/openssh-server/sshd_config.5.en.html#LogLevel

²https://manpages.debian.org/testing/openssh-client/ssh_config.5.en.html