

BOOTCAMP ESPECIALIDAD GNU/LINUX (2023)

---

## Lab 05 - Monitorización, análisis y almacenamiento de registros.

---

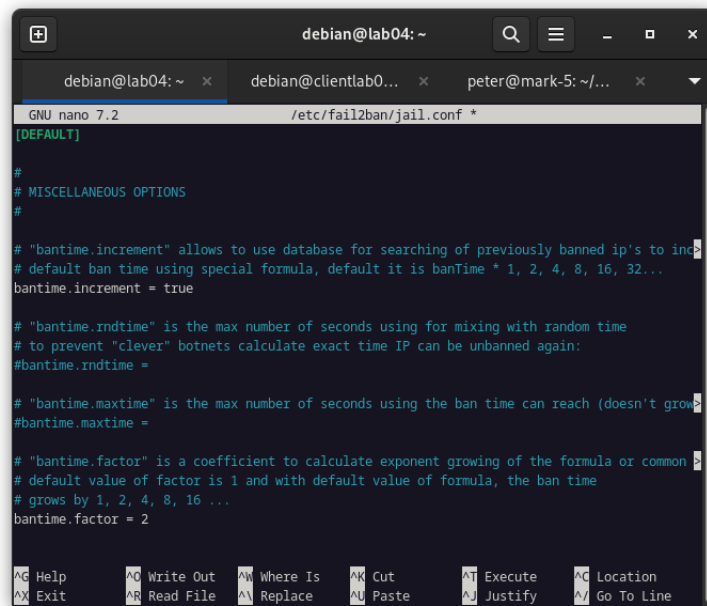
Pedro Antonio Mayorgas Parejo

7 de agosto de 2023

## Índice

1	Instalación y configuración de Fail2ban	3
2	Probando fail2ban	7





```
GNU nano 7.2 /etc/fail2ban/jail.conf *
[DEFAULT]

#
# MISCELLANEOUS OPTIONS
#

# "bantime.increment" allows to use database for searching of previously banned ip's to increment
# default ban time using special formula, default it is banTime * 1, 2, 4, 8, 16, 32...
bantime.increment = true

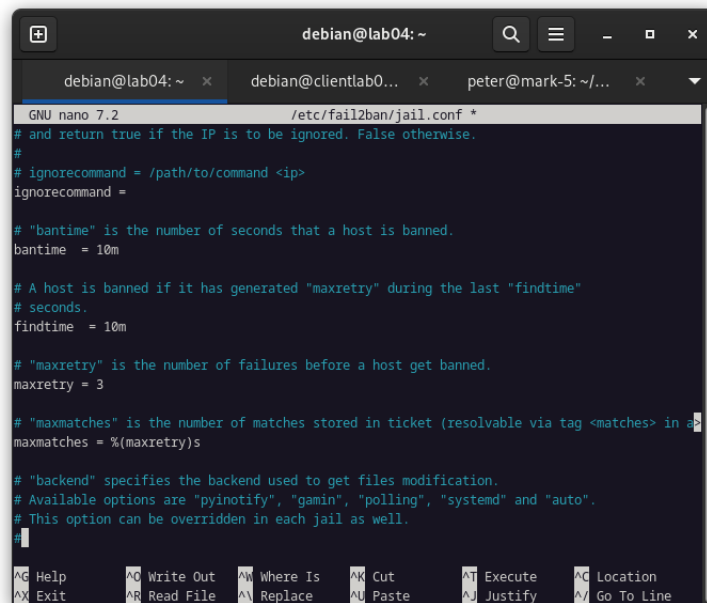
# "bantime.rndtime" is the max number of seconds using for mixing with random time
# to prevent "clever" botnets calculate exact time IP can be unbanned again:
#bantime.rndtime =

# "bantime.maxtime" is the max number of seconds using the ban time can reach (doesn't grow)
#bantime.maxtime =

# "bantime.factor" is a coefficient to calculate exponent growing of the formula or common
# default value of factor is 1 and with default value of formula, the ban time
# grows by 1, 2, 4, 8, 16 ...
bantime.factor = 2

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

Figura 2: Configuración del incremento de la expulsión.



```
GNU nano 7.2 /etc/fail2ban/jail.conf *
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime = 10m

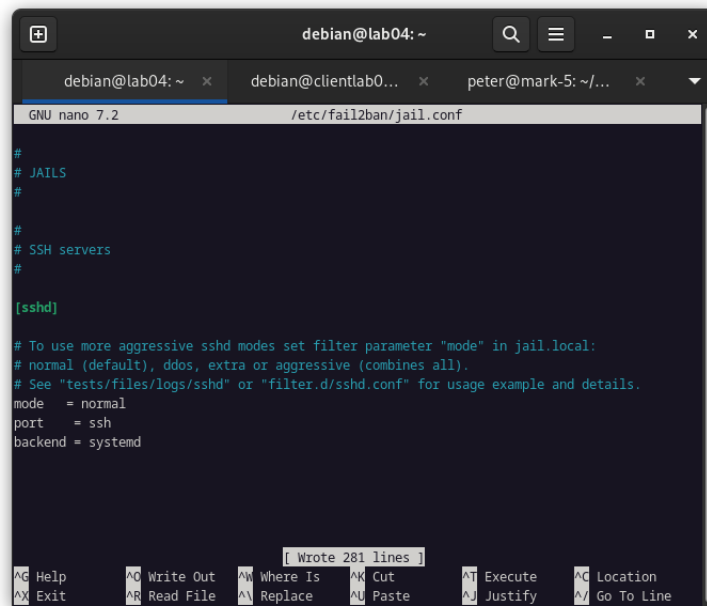
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 3

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in a
maxmatches = %(maxretry)s

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
```

Figura 3: Configuración de los intentos.



```
GNU nano 7.2 /etc/fail2ban/jail.conf

#
# JAILS
#
#
# SSH servers
#

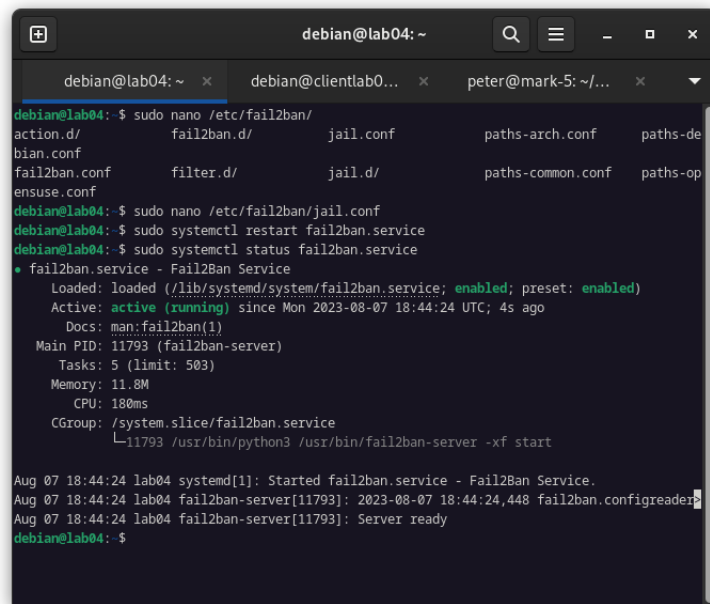
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
mode = normal
port = ssh
backend = systemd
```

Figura 4: Configuración de servicio sshd y backend.

Por último reiniciamos el servicio para aplicar los cambios y comprobar que funcionan correctamente con los siguientes comandos:

- 1 `sudo systemctl restart fail2ban.service`
- 2 `sudo systemctl status fail2ban.service`

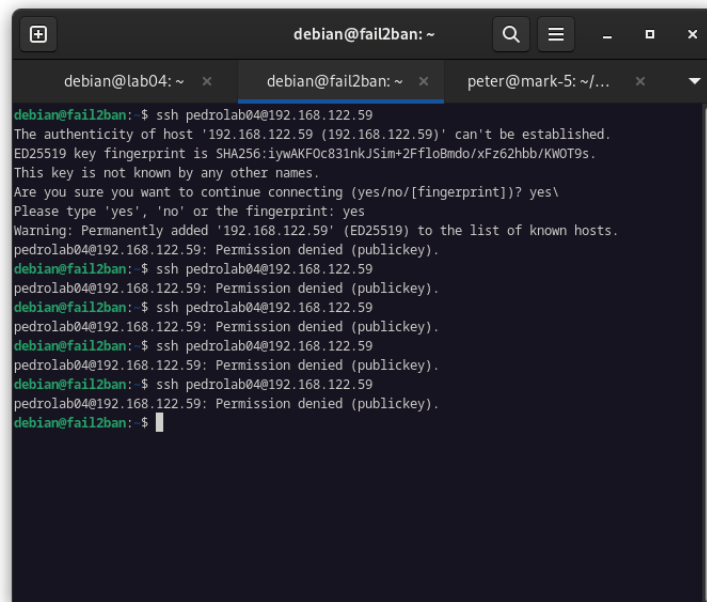


```
debian@lab04: ~  
debian@lab04:~$ sudo nano /etc/fail2ban/  
action.d/      fail2ban.d/      jail.conf      paths-arch.conf  paths-de  
bian.conf  
fail2ban.conf  filter.d/        jail.d/        paths-common.conf paths-op  
ensuse.conf  
debian@lab04:~$ sudo nano /etc/fail2ban/jail.conf  
debian@lab04:~$ sudo systemctl restart fail2ban.service  
debian@lab04:~$ sudo systemctl status fail2ban.service  
● fail2ban.service - Fail2Ban Service  
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)  
   Active: active (running) since Mon 2023-08-07 18:44:24 UTC; 4s ago  
     Docs: man:fail2ban(1)  
    Main PID: 11793 (fail2ban-server)  
      Tasks: 5 (limit: 503)  
    Memory: 11.8M  
       CPU: 180ms  
    CGroup: /system.slice/fail2ban.service  
            └─11793 /usr/bin/python3 /usr/bin/fail2ban-server -xf start  
  
Aug 07 18:44:24 lab04 systemd[1]: Started fail2ban.service - Fail2Ban Service.  
Aug 07 18:44:24 lab04 fail2ban-server[11793]: 2023-08-07 18:44:24,448 fail2ban.configreader:  
Aug 07 18:44:24 lab04 fail2ban-server[11793]: Server ready  
debian@lab04:~$
```

Figura 5: Aplicando los cambios a fail2ban.

## 2. Probando fail2ban

Ahora con un cliente que no tenga clave pública probamos que efectivamente se aplique el fail2ban y mostramos el log. Primero tenemos que habilitar el acceso por contraseña, ya que si lo hacemos por clave pública solo, fail2ban no salta, es decir porque está protegido el sshd. En este caso habilitamos la opción de contraseña para el usuario pedrolab04, para hacer intentos por contraseña.



```
debian@fail2ban: ~  
debian@lab04: ~ x  debian@fail2ban: ~ x  peter@mark-5: ~/... x  
debian@fail2ban: $ ssh pedrolab04@192.168.122.59  
The authenticity of host '192.168.122.59 (192.168.122.59)' can't be established.  
ED25519 key fingerprint is SHA256:iywAKF0c831nkJSim+2Ff1o8mdo/xFz62hbb/KWOT9s.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes\  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '192.168.122.59' (ED25519) to the list of known hosts.  
pedrolab04@192.168.122.59: Permission denied (publickey).  
debian@fail2ban: $ ssh pedrolab04@192.168.122.59  
pedrolab04@192.168.122.59: Permission denied (publickey).  
debian@fail2ban: $ ssh pedrolab04@192.168.122.59  
pedrolab04@192.168.122.59: Permission denied (publickey).  
debian@fail2ban: $ ssh pedrolab04@192.168.122.59  
pedrolab04@192.168.122.59: Permission denied (publickey).  
debian@fail2ban: $ ssh pedrolab04@192.168.122.59  
pedrolab04@192.168.122.59: Permission denied (publickey).  
debian@fail2ban: $
```

Figura 6: Si aplicamos solo clave pública no funcionará fail2ban, no le hace falta.

El ban por IP se puede comprobar cuando intentamos realizar una conexión que en vez de preguntarnos por la contraseña nos indica que se ha rechazado la conexión. Es decir el siguiente mensaje:

**ssh: connect to host 192.168.122.59 port 22: Connection refused**

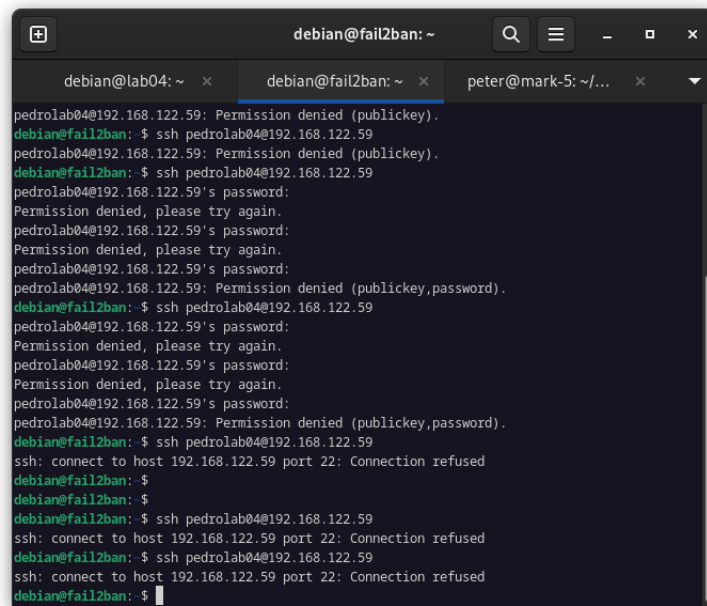
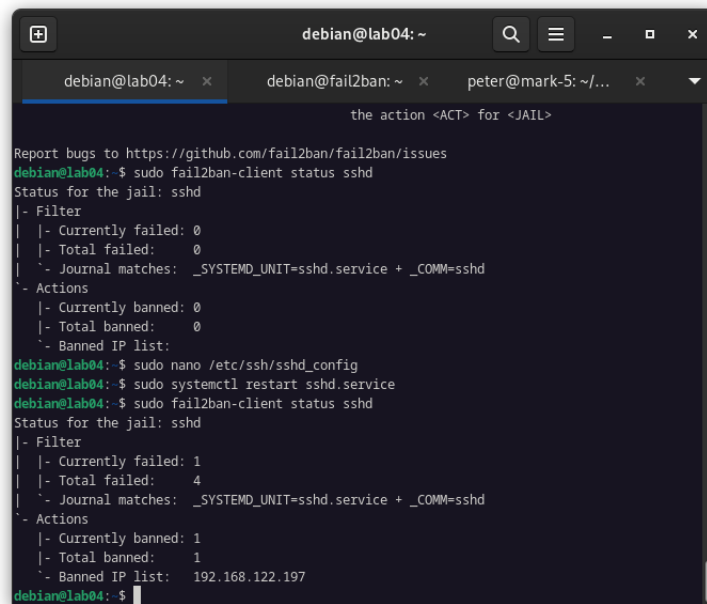
A terminal window titled 'debian@fail2ban: ~' with three tabs: 'debian@lab04: ~', 'debian@fail2ban: ~', and 'peter@mark-5: ~/...'. The terminal shows a series of SSH login attempts from 'pedrolab04@192.168.122.59'. The first two attempts fail with 'Permission denied (publickey)'. The third attempt fails with 'Permission denied, please try again.' after a password prompt. The fourth attempt also fails with 'Permission denied, please try again.' after a password prompt. The fifth attempt fails with 'Permission denied (publickey,password)' after a password prompt. The sixth attempt fails with 'Permission denied, please try again.' after a password prompt. The seventh attempt fails with 'Permission denied, please try again.' after a password prompt. The eighth attempt fails with 'Permission denied (publickey,password)' after a password prompt. The ninth attempt fails with 'ssh: connect to host 192.168.122.59 port 22: Connection refused'. The tenth attempt fails with 'ssh: connect to host 192.168.122.59 port 22: Connection refused'. The eleventh attempt fails with 'ssh: connect to host 192.168.122.59 port 22: Connection refused'. The twelfth attempt fails with 'ssh: connect to host 192.168.122.59 port 22: Connection refused'. The terminal ends with 'debian@fail2ban: \$'.

Figura 7: Una vez aplicado la autenticación por contraseña al tercer intento se banea por IP.

Una vez que el ban se aplica se puede ver el estado del ban en un comando de fail2ban.

```
1 sudo fail2ban -client status sshd
```





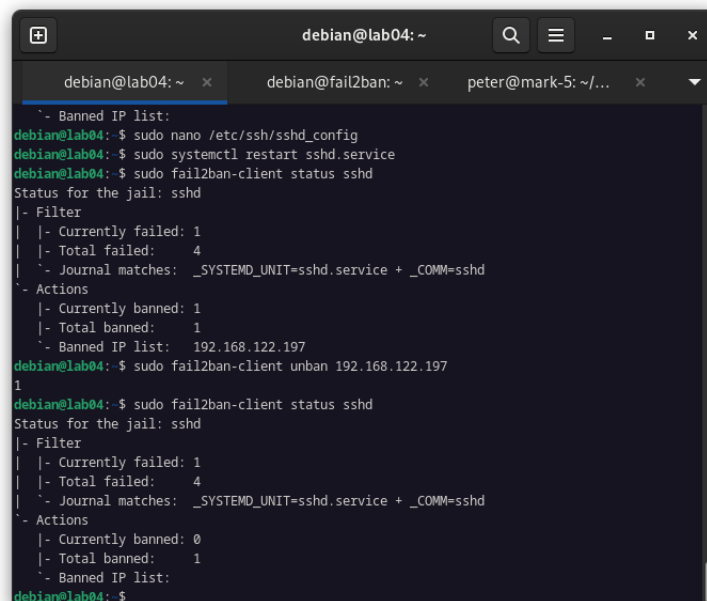
A terminal window titled 'debian@lab04: ~' with three tabs: 'debian@lab04: ~', 'debian@fail2ban: ~', and 'peter@mark-5: ~/...'. The terminal shows the following commands and output:

```
Report bugs to https://github.com/fail2ban/fail2ban/issues
debian@lab04:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
    |- Currently banned: 0
    |- Total banned: 0
    \- Banned IP list:
debian@lab04:~$ sudo nano /etc/ssh/sshd_config
debian@lab04:~$ sudo systemctl restart sshd.service
debian@lab04:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
    |- Currently banned: 1
    |- Total banned: 1
    \- Banned IP list: 192.168.122.197
debian@lab04:~$
```

Figura 8: Podemos ver el ban en el comando y la IP.

Para hacer unban al cliente sin esperar, tenemos que introducir el siguiente comando:

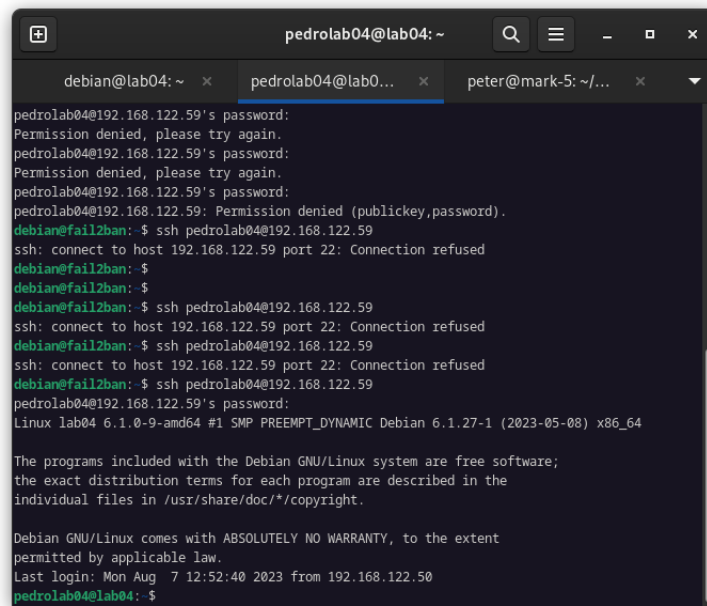
```
1 sudo fail2ban-client unban 192.168.122.197
```



A terminal window titled 'debian@lab04: ~' with the same three tabs as Figure 8. The terminal shows the following commands and output:

```
\- Banned IP list:
debian@lab04:~$ sudo nano /etc/ssh/sshd_config
debian@lab04:~$ sudo systemctl restart sshd.service
debian@lab04:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
    |- Currently banned: 1
    |- Total banned: 1
    \- Banned IP list: 192.168.122.197
debian@lab04:~$ sudo fail2ban-client unban 192.168.122.197
1
debian@lab04:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
    |- Currently banned: 0
    |- Total banned: 1
    \- Banned IP list:
debian@lab04:~$
```

Figura 9: Aplicando el unban.



The image shows a terminal window with three tabs: 'debian@lab04: ~', 'pedrolab04@lab0...', and 'peter@mark-5: ~/...'. The active tab is 'pedrolab04@lab0...'. The terminal output shows a series of SSH login attempts from 'pedrolab04@192.168.122.59' to a server. The first three attempts fail with 'Permission denied, please try again.' and 'Permission denied (publickey,password).' respectively. The fourth attempt, initiated by 'debian@fail2ban', also fails with 'ssh: connect to host 192.168.122.59 port 22: Connection refused'. The fifth attempt, also initiated by 'debian@fail2ban', succeeds, displaying the system version 'Linux lab04 6.1.0-9-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.27-1 (2023-05-08) x86\_64', followed by a disclaimer about free software and warranty, and the last login time 'Mon Aug 7 12:52:40 2023 from 192.168.122.50'. The prompt then changes to 'pedrolab04@lab04: \$'.

```
pedrolab04@192.168.122.59's password:
Permission denied, please try again.
pedrolab04@192.168.122.59's password:
Permission denied, please try again.
pedrolab04@192.168.122.59's password:
pedrolab04@192.168.122.59: Permission denied (publickey,password).
debian@fail2ban:~$ ssh pedrolab04@192.168.122.59
ssh: connect to host 192.168.122.59 port 22: Connection refused
debian@fail2ban:~$
debian@fail2ban:~$
debian@fail2ban:~$ ssh pedrolab04@192.168.122.59
ssh: connect to host 192.168.122.59 port 22: Connection refused
debian@fail2ban:~$ ssh pedrolab04@192.168.122.59
ssh: connect to host 192.168.122.59 port 22: Connection refused
debian@fail2ban:~$ ssh pedrolab04@192.168.122.59
pedrolab04@192.168.122.59's password:
Linux lab04 6.1.0-9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1 (2023-05-08) x86_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.
Last login: Mon Aug 7 12:52:40 2023 from 192.168.122.50
pedrolab04@lab04:~$
```

Figura 10: El cliente después de estar baneado puede autenticarse correctamente.