

Trabajo Práctico – Seguridad en Sistemas Operativos

Alumnos:

- Federico Garcia – garcia.federico@outlook.com
- Federico Garcia Bengolea - feddericogarciaa@gmail.com

Materia:

Arquitectura y Sistemas Operativos

Profesor: Diego Lobos

Tutor: Nicolas Carcaño

Fecha de Entrega: 05 de junio de 2025

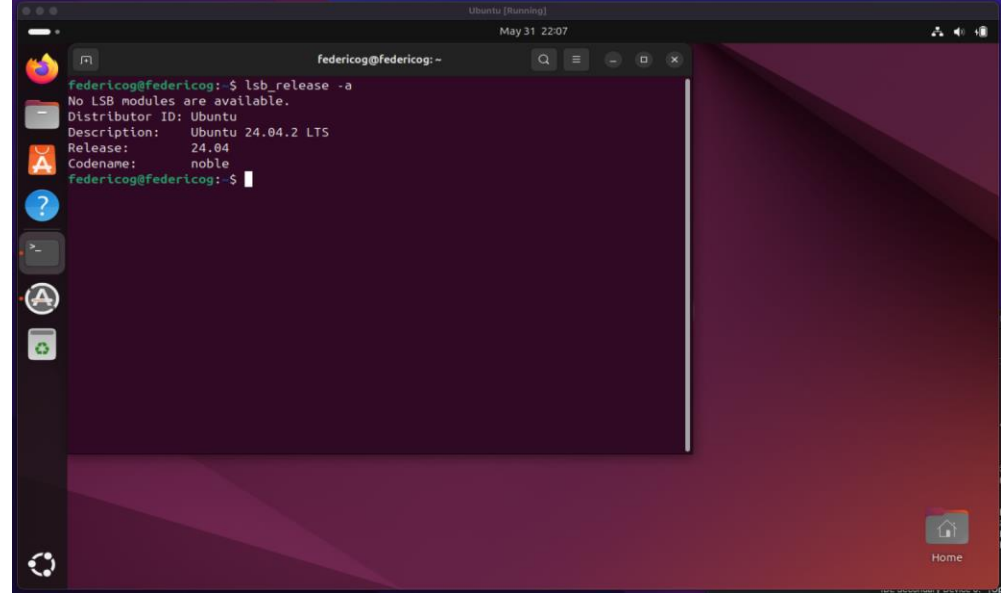
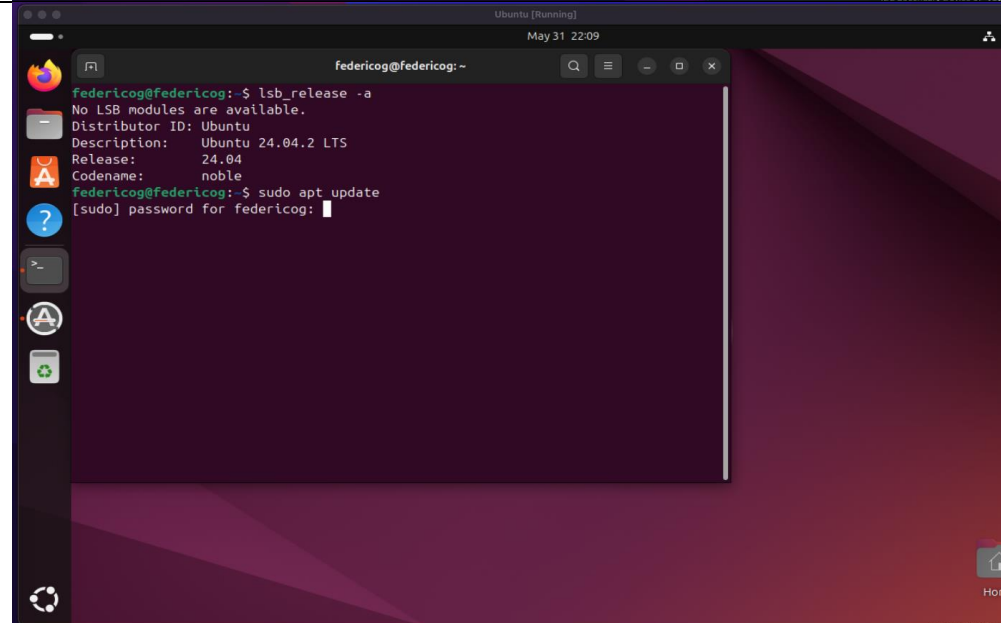
Índice:

Introducción	1
Anexo	2

Introducción

La información detallada a continuación es un anexo y complemento al trabajo práctico integrador. Aquí se detallan las operaciones realizadas en el caso práctico del trabajo, acompañado de capturas de pantalla.

Anexo

	<p>Sistema operativo utilizado para el caso práctico. Linux Ubuntu virtualizado en una VM con Virtual Box.</p>
	<p>Realizamos un update de los repositorios, para asegurarnos que está todo up to date.</p>

```

523 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en
[185 kB]
Get:16 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Component
s [52.2 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Compone
nts [212 B]
Get:18 http://ar.archive.ubuntu.com/ubuntu noble-updates/main i386 Packages [473
kB]
Get:19 http://ar.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [23
5 kB]
Get:20 http://ar.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [
161 kB]
Get:21 http://ar.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Compon
ents [212 B]
Get:22 http://ar.archive.ubuntu.com/ubuntu noble-updates/universe i386 Packages
[645 kB]
Get:23 http://ar.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages
[1068 kB]
Get:24 http://ar.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en
[271 kB]
Get:25 http://ar.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Componen
ts [377 kB]
97% [25 Components-amd64 219 kB/377 kB 58%] 1168 kB/s 0s

```

Se actualiza la lista de repositorios disponibles antes de hacer las instalaciones necesarias.

```

[645 kB]
Get:23 http://ar.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages
[1068 kB]
Get:24 http://ar.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en
[271 kB]
Get:25 http://ar.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Componen
ts [377 kB]
Get:26 http://ar.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Compon
ents [948 B]
Get:27 http://ar.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components
[7076 B]
Get:28 http://ar.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Comp
onents [216 B]
Get:29 http://ar.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Compon
ents [16.4 kB]
Get:30 http://ar.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Comp
onents [212 B]
Reading package lists... Done
E: The repository 'file:/cdrom/noble/Release' no longer has a Release file.
N: Updating from such a repository can't be done securely, and is therefore disa
bled by default.
N: See apt-secure(8) manpage for repository creation and user configuration deta
ils.
federicog@federicog:~$ sudo apt install firewall

```

Comenzamos la instalación de firewalld, una vez finalizada la actualización.

```

Get:28 http://ar.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Comp
onents [216 B]
Get:29 http://ar.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Compon
ents [16.4 kB]
Get:30 http://ar.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Comp
onents [212 B]
Reading package lists... Done
E: The repository 'file:/cdrom/noble/Release' no longer has a Release file.
N: Updating from such a repository can't be done securely, and is therefore disa
bled by default.
N: See apt-secure(8) manpage for repository creation and user configuration deta
ils.
federicog@federicog:~$ sudo apt install firewalld
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ipset libipset13 python3-cap-ng python3-firewall python3-nftables
The following NEW packages will be installed:
  firewalld ipset libipset13 python3-cap-ng python3-firewall python3-nftables
0 upgraded, 6 newly installed, 0 to remove and 120 not upgraded.
Need to get 686 kB of archives.
After this operation, 4507 kB of additional disk space will be used.
Do you want to continue? [Y/n]

```

Se realiza la instalación del firewall.

```

federicog@federicog:~$ sudo dpkg --get-selections | grep firewall
federicog@federicog:~$ sudo dpkg --get-selections | grep ipset
federicog@federicog:~$ sudo dpkg --get-selections | grep python3
federicog@federicog:~$ sudo dpkg --get-selections | grep nftables
federicog@federicog:~$ sudo dpkg --get-selections | grep firewalld
federicog@federicog:~$ sudo systemctl start firewalld

```

Se startea el servicio de firewalld.

```

federicog@federicog:~$ sudo systemctl start firewalld
federicog@federicog:~$ sudo systemctl enable firewalld

```

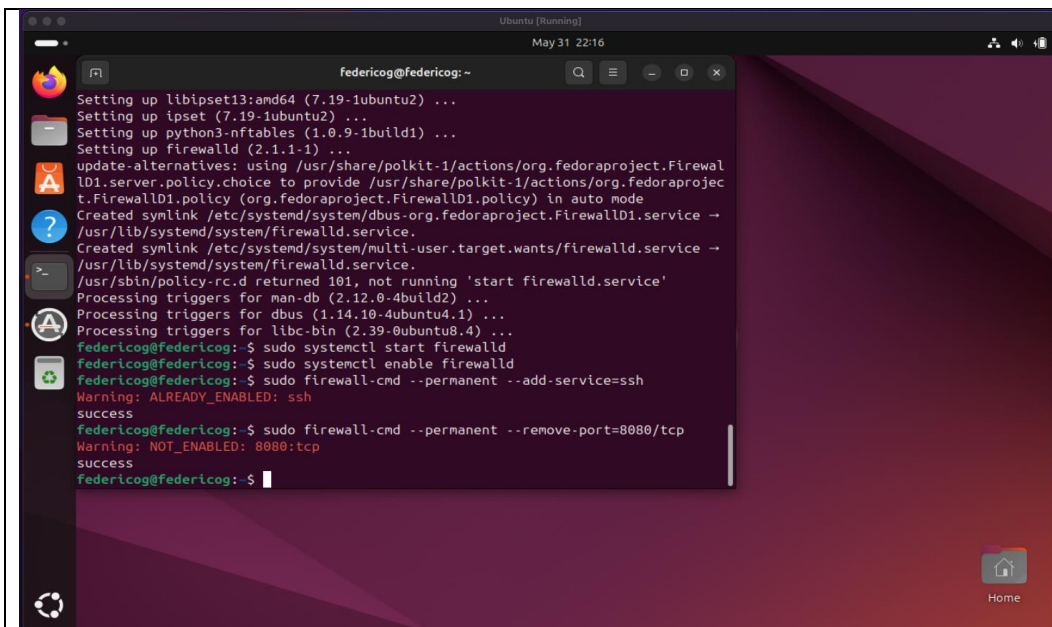
Se activa el servicio de firewalld.

```

federicog@federicog:~$ sudo firewall-cmd --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
federicog@federicog:~$

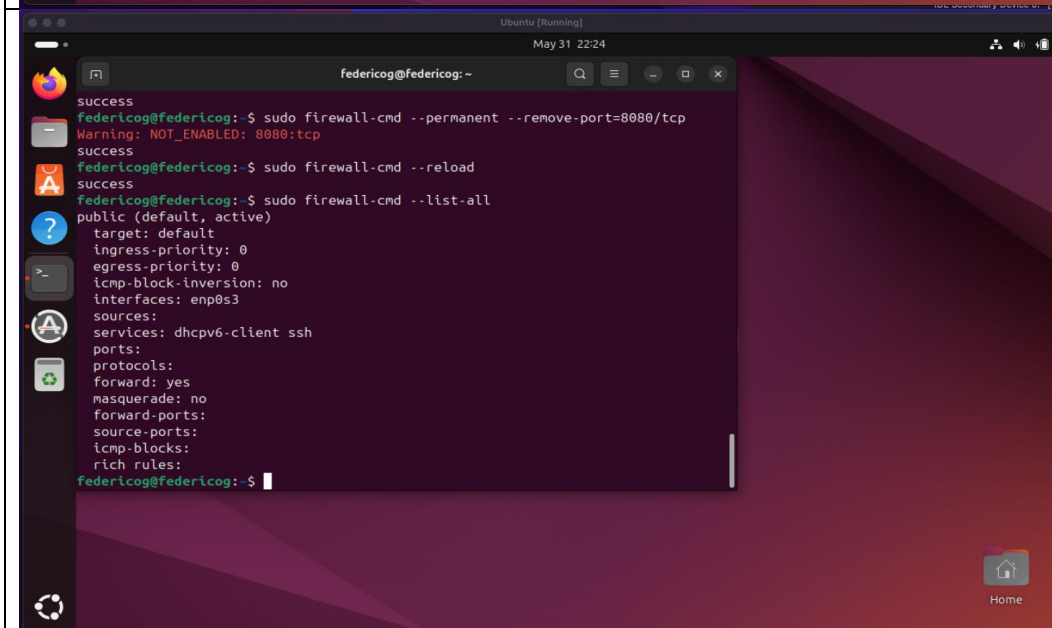
```

Por medio del comando correspondiente realizamos la habilitación del servicio ssh. Vemos un mensaje de “warning” porque el servicio estaba habilitado, pero de todas formas la habilitación es exitosa.

A terminal window titled 'Ubuntu [Running]' with the date 'May 31 22:16'. The user 'federicog' is at the prompt. The terminal shows the setup of libipset, ipset, python3-nftables, and firewall. It then shows the creation of symlinks for the firewall service, starting and enabling the firewall, and finally removing port 8080/tcp from the firewall rules.

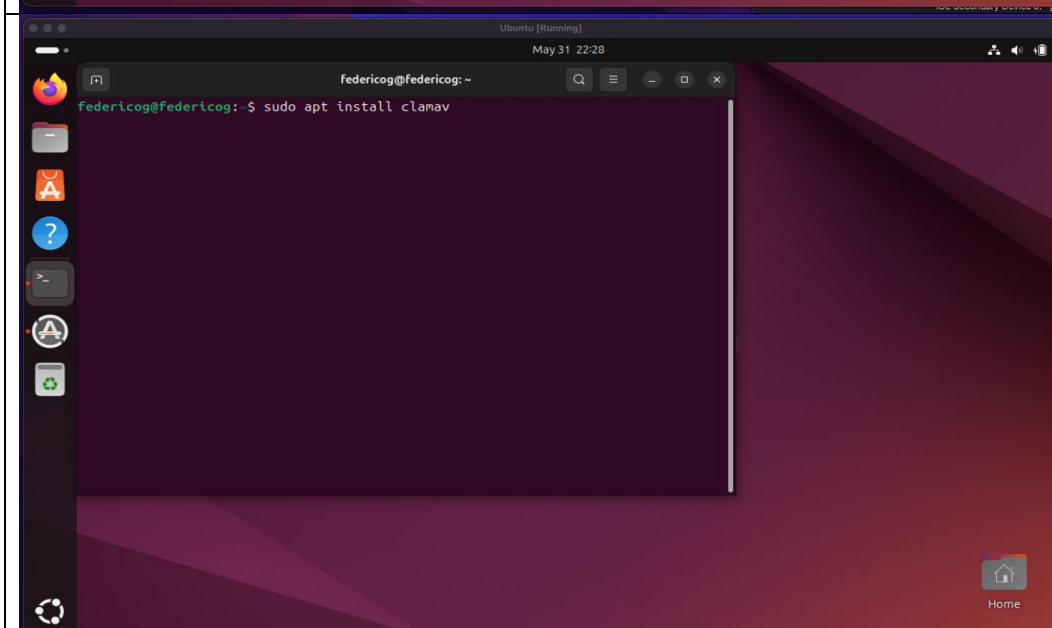
```
federicog@federicog:~$ sudo apt install libipset1:amd64 (7.19-1ubuntu2) ...
Setting up ipset (7.19-1ubuntu2) ...
Setting up python3-nftables (1.0.9-1build1) ...
Setting up firewall (2.1.1-1) ...
update-alternatives: using /usr/share/polkit-1/actions/org.fedoraproject.Firewal
ld1.server.policy.choice to provide /usr/share/polkit-1/actions/org.fedoraprojec
t.FirewallD1.policy (org.fedoraproject.FirewallD1.policy) in auto mode
Created symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service ->
/usr/lib/systemd/system/firewalld.service.
Created symlink /etc/systemd/system/multi-user.target.wants/firewalld.service ->
/usr/lib/systemd/system/firewalld.service.
/usr/sbin/policy-rc.d returned 101, not running 'start firewalld.service'
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for dbus (1.14.10-4ubuntu4.1) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
federicog@federicog:~$ sudo systemctl start firewalld
federicog@federicog:~$ sudo systemctl enable firewalld
federicog@federicog:~$ sudo firewall-cmd --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
federicog@federicog:~$ sudo firewall-cmd --permanent --remove-port=8080/tcp
Warning: NOT_ENABLED: 8080:tcp
success
federicog@federicog:~$
```

Deshabilitamos la conexión a través del puerto 8080. Al igual que en el caso anterior este puerto estaba deshabilitado, pero, de todas formas, hay una deshabilitación exitosa.

A terminal window titled 'Ubuntu [Running]' with the date 'May 31 22:24'. The user 'federicog' is at the prompt. The terminal shows the reload of the firewall rules and the listing of all rules, which shows the 'public' target with various settings and the 'ssh' service added to the allowed services.

```
success
federicog@federicog:~$ sudo firewall-cmd --permanent --remove-port=8080/tcp
Warning: NOT_ENABLED: 8080:tcp
success
federicog@federicog:~$ sudo firewall-cmd --reload
success
federicog@federicog:~$ sudo firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
federicog@federicog:~$
```

Luego listamos la configuración de firewalld para asegurarnos que la misma esté como queremos.

A terminal window titled 'Ubuntu [Running]' with the date 'May 31 22:28'. The user 'federicog' is at the prompt. The terminal shows the command to install ClamAV using apt.

```
federicog@federicog:~$ sudo apt install clamav
```

Iniciamos la instalación de ClamAV.

```
Ubuntu [Running]
May 31 22:28

federicog@federicog: ~
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamav-freshclam libclamav11t64 libmspack0t64
Suggested packages:
  libclamunrar clamav-docs libclamunrar11
The following NEW packages will be installed:
  clamav clamav-base clamav-freshclam libclamav11t64 libmspack0t64
0 upgraded, 5 newly installed, 0 to remove and 120 not upgraded.
Need to get 12.6 MB of archives.
After this operation, 55.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ar.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-base a
ll 1.0.8+dfsg-0ubuntu0.24.04.1 [93.5 kB]
Get:2 http://ar.archive.ubuntu.com/ubuntu noble/main amd64 libmspack0t64 amd64 0
.11.1.1build1 [40.0 kB]
Get:3 http://ar.archive.ubuntu.com/ubuntu noble-updates/main amd64 libclamav11t6
4 amd64 1.0.8+dfsg-0ubuntu0.24.04.1 [6714 kB]
Get:4 http://ar.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-freshc
lam amd64 1.0.8+dfsg-0ubuntu0.24.04.1 [97.6 kB]
Get:5 http://ar.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav amd64
1.0.8+dfsg-0ubuntu0.24.04.1 [5684 kB]
67% [5 clamav 1118 kB/5684 kB 20%]
```

Se realiza la instalación correctamente.

```
Ubuntu [Running]
May 31 22:30

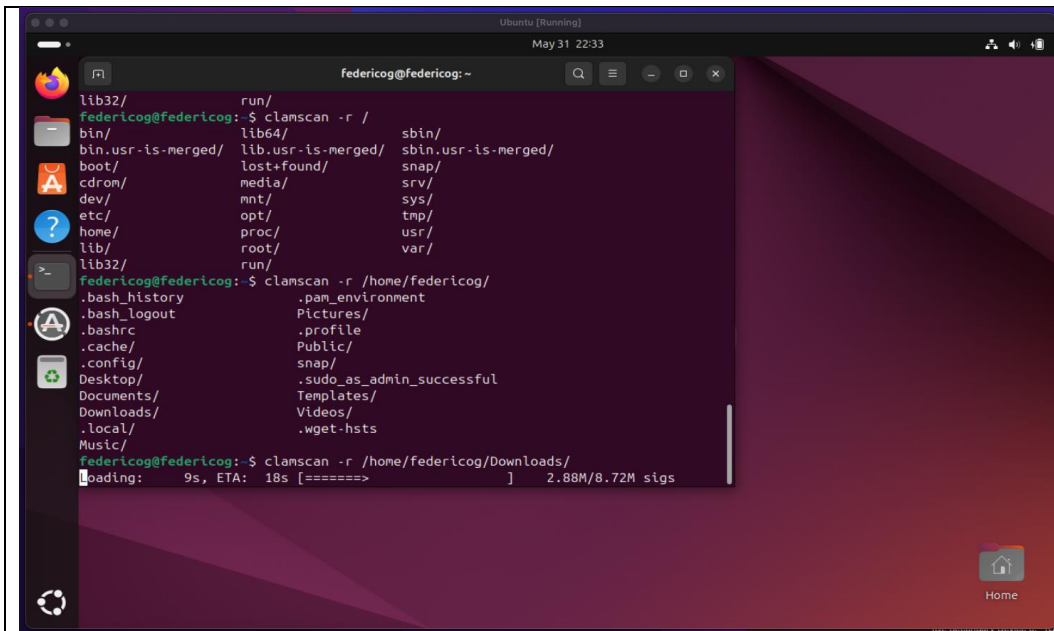
federicog@federicog: ~
Unpacking libmspack0t64:amd64 (0.11.1.1build1) ...
Selecting previously unselected package libclamav11t64:amd64.
Preparing to unpack .../libclamav11t64_1.0.8+dfsg-0ubuntu0.24.04.1_amd64.deb ...
Unpacking libclamav11t64:amd64 (1.0.8+dfsg-0ubuntu0.24.04.1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../clamav-freshclam_1.0.8+dfsg-0ubuntu0.24.04.1_amd64.deb ...
Unpacking clamav-freshclam (1.0.8+dfsg-0ubuntu0.24.04.1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../clamav_1.0.8+dfsg-0ubuntu0.24.04.1_amd64.deb ...
Unpacking clamav (1.0.8+dfsg-0ubuntu0.24.04.1) ...
Setting up libmspack0t64:amd64 (0.11.1.1build1) ...
Setting up libclamav11t64:amd64 (1.0.8+dfsg-0ubuntu0.24.04.1) ...
Setting up clamav-base (1.0.8+dfsg-0ubuntu0.24.04.1) ...
Setting up clamav-freshclam (1.0.8+dfsg-0ubuntu0.24.04.1) ...
invoke-rc.d: policy-rc.d denied execution of start.
Setting up clamav (1.0.8+dfsg-0ubuntu0.24.04.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
federicog@federicog: ~$ sudo freshclam
ClamAV update process started at Sat May 31 22:30:19 2025
Sat May 31 22:30:19 2025 -> daily database available for download (remote versio
n: 27654)
Time: 8.1s, ETA: 35.8s [====>] 11.42MiB/61.67MiB
```

Actualizamos la base de datos de ClamAV.

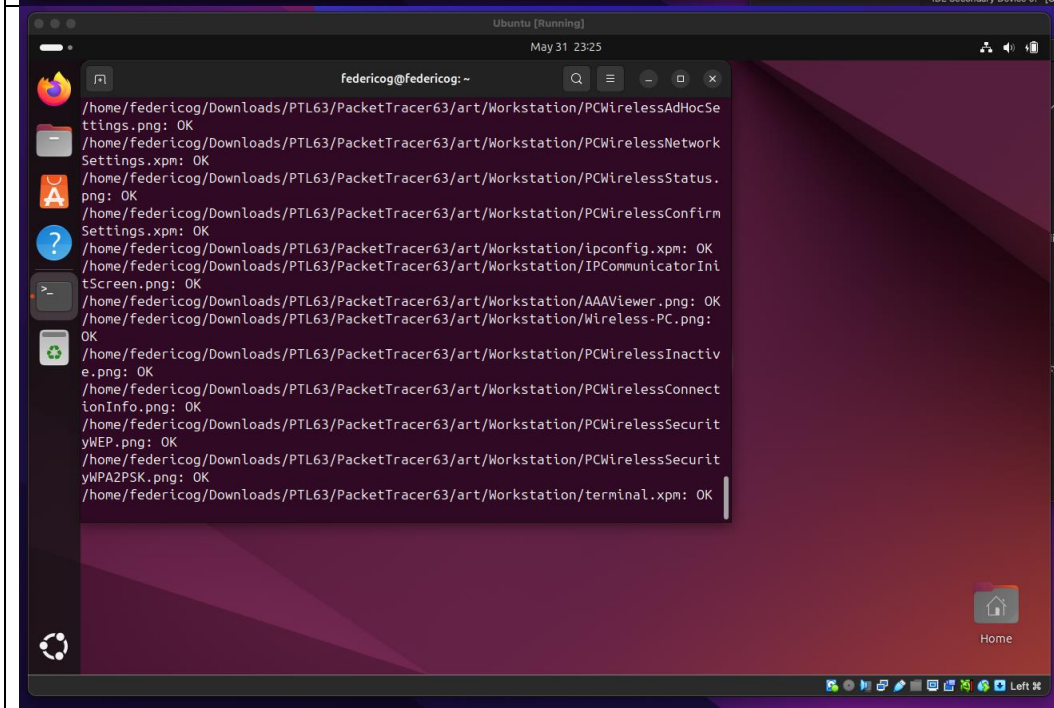
```
Ubuntu [Running]
May 31 22:33

federicog@federicog: ~
lib/          root/          var/
lib32/        run/
federicog@federicog: ~$ clamscan -r /
bin/          lib64/         sbin/
bin usr-is-merged/ lib usr-is-merged/ sbin usr-is-merged/
boot/         lost+found/    snap/
cdrom/        media/         srv/
dev/          mnt/           sys/
etc/          opt/           tmp/
home/         proc/          usr/
lib/          root/          var/
lib32/        run/
federicog@federicog: ~$ clamscan -r /home/federicog/
.bash_history      .pam_environment
.bash_logout       Pictures/
.bashrc            .profile
.cache/            Public/
.config/           snap/
Desktop/           .sudo_as_admin_successful
Documents/          Templates/
Downloads/          Videos/
.local/             .wget-hsts
Music/
federicog@federicog: ~$ clamscan -r /home/federicog/Downloads/
```

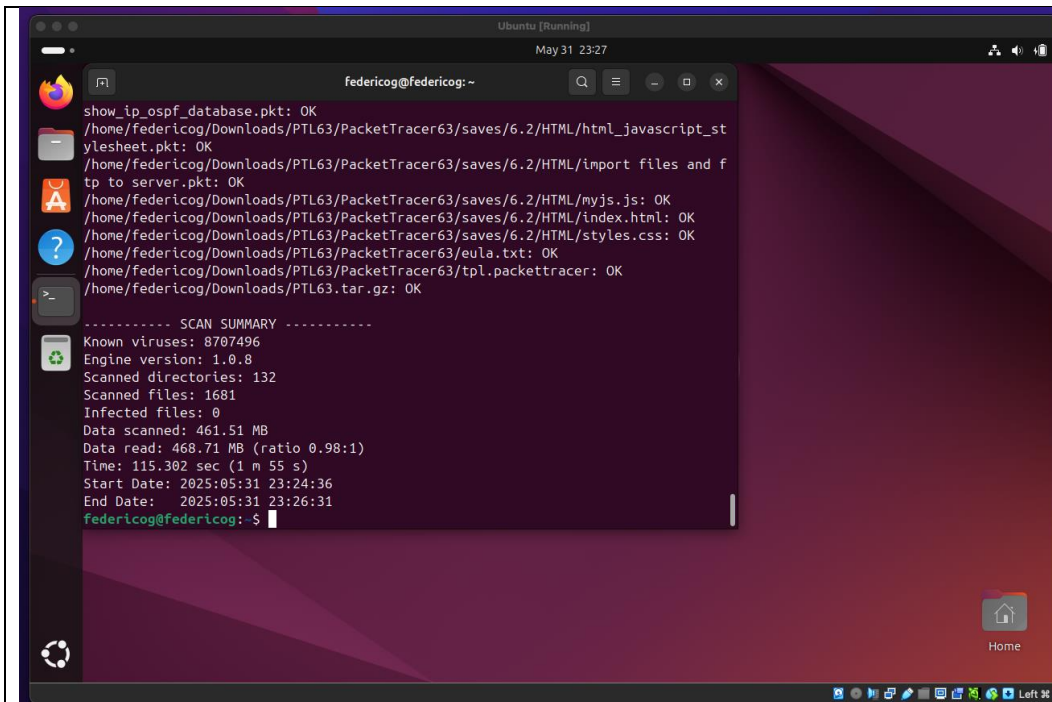
Iniciamos el escaneo de una carpeta con ClamAV.



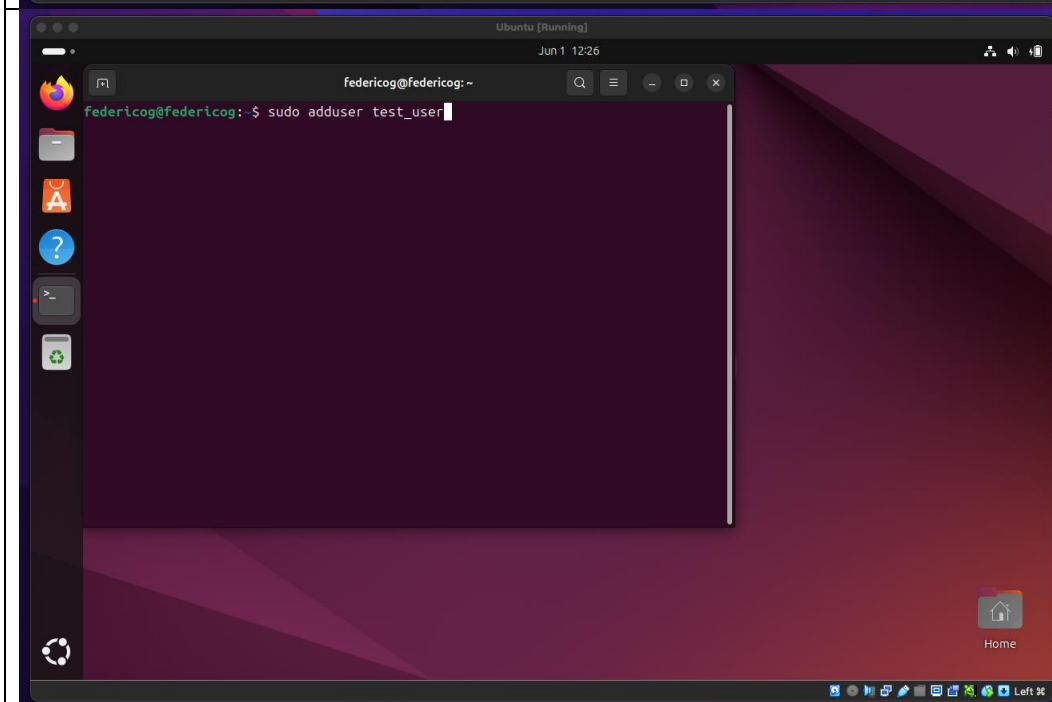
Parte del proceso de escaneo.



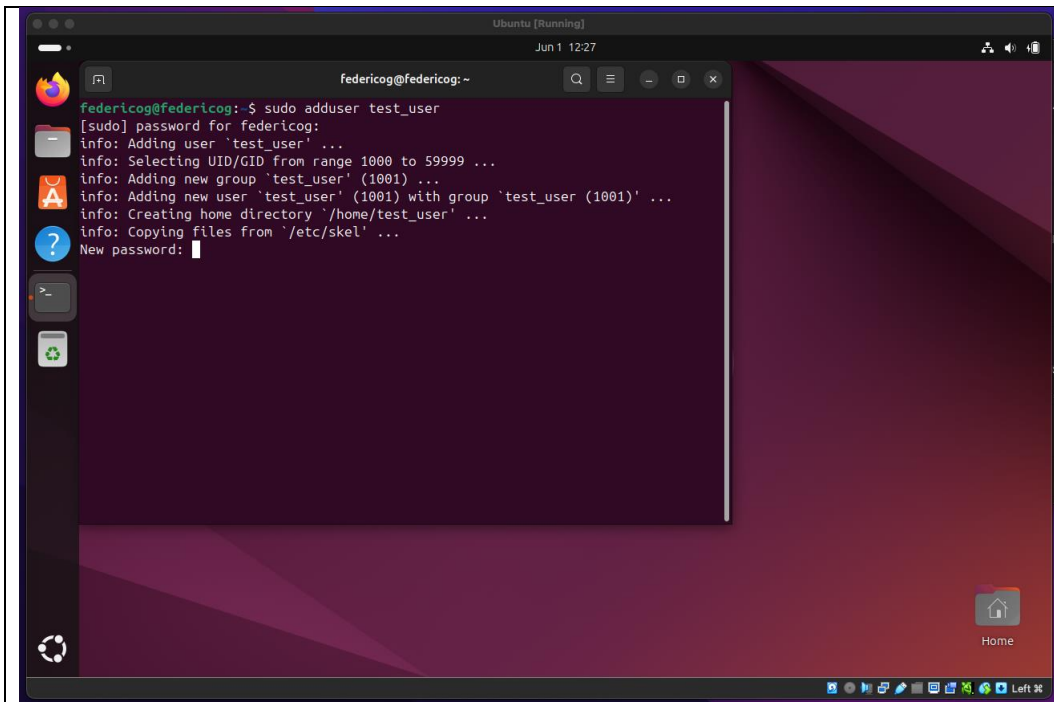
Continuamos escaneando.



Finalmente, una vez que se concluye con el escaneo, podemos ver los resultados obtenidos del mismo. Podemos observar la cantidad de archivos analizados y la cantidad de archivos infectados.



Creamos un usuario llamado test_user.

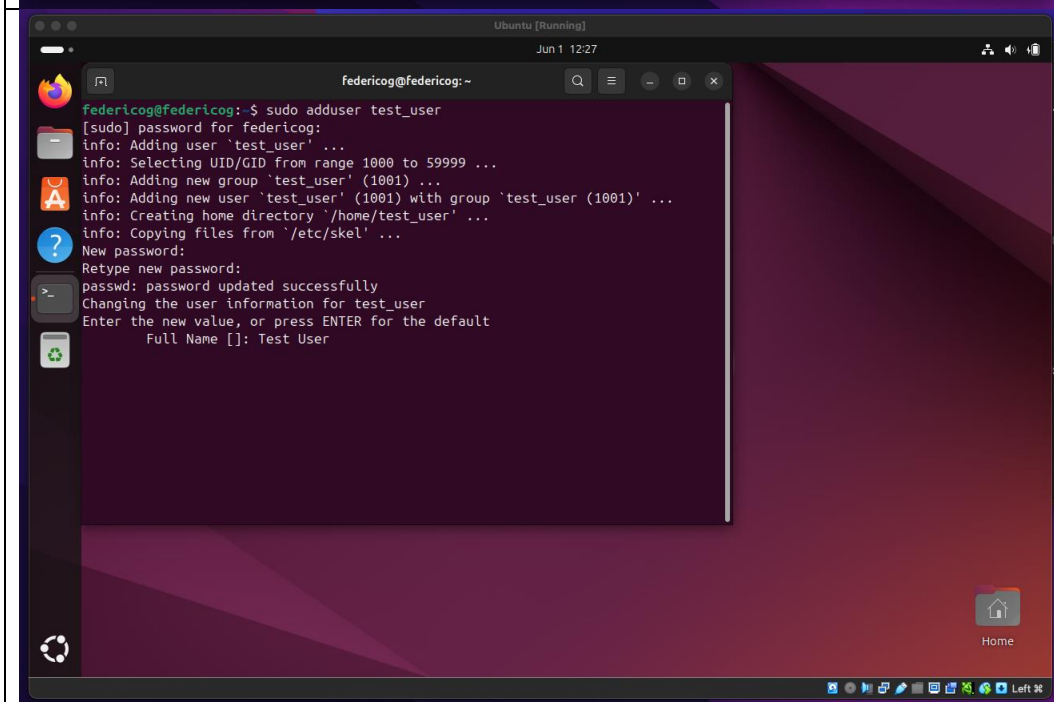


```

federicog@federicog: ~
federicog@federicog:~$ sudo adduser test_user
[sudo] password for federicog:
info: Adding user 'test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'test_user' (1001) ...
info: Adding new user 'test_user' (1001) with group 'test_user (1001)' ...
info: Creating home directory '/home/test_user' ...
info: Copying files from '/etc/skel' ...
New password:

```

Le otorgamos una contraseña.



```

New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
Full Name []: Test User

```

Y agregamos un poco de información.

```
Ubuntu [Running]
Jun 1 12:27

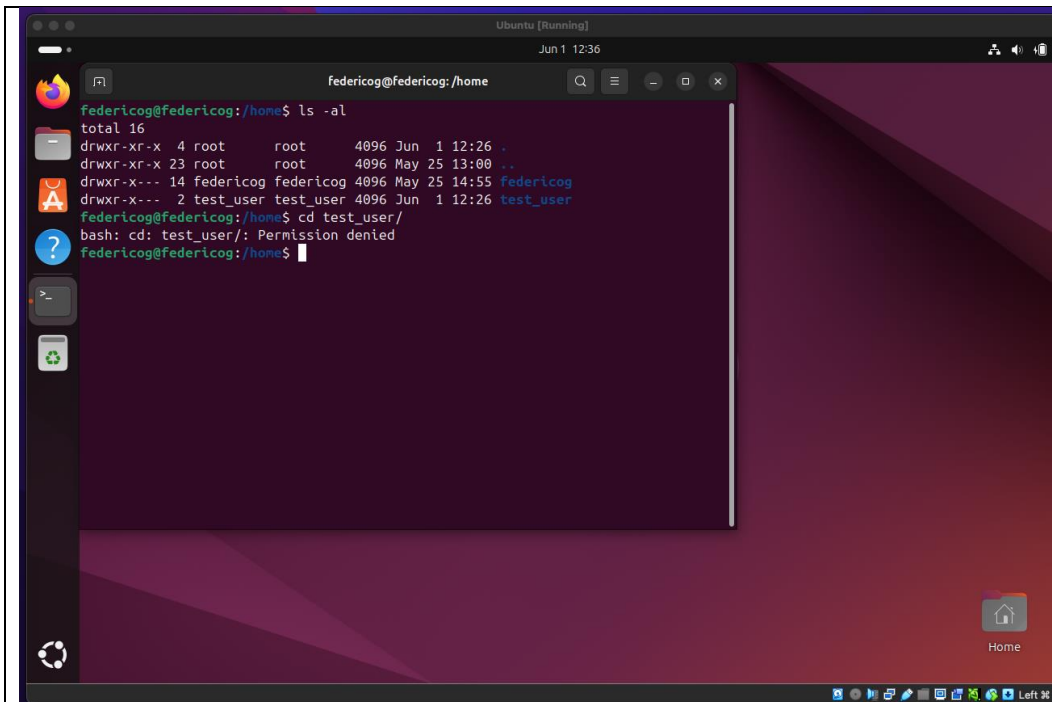
federicog@federicog:~$ sudo adduser test_user
[sudo] password for federicog:
info: Adding user 'test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'test_user' (1001) ...
info: Adding new user 'test_user' (1001) with group 'test_user (1001)' ...
info: Creating home directory '/home/test_user' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
  Full Name []: Test User
    Room Number []:
    Work Phone []:
    Home Phone []:
      Other []:
Is the information correct? [Y/n] y
info: Adding new user 'test_user' to supplemental / extra groups 'users' ...
info: Adding user 'test_user' to group 'users' ...
federicog@federicog:~$
```

Ya tenemos el usuario correctamente creado.

```
Ubuntu [Running]
Jun 1 12:35

federicog@federicog:/home$ ls -al
total 16
drwxr-xr-x  4 root    root      4096 Jun  1 12:26 .
drwxr-xr-x 23 root    root      4096 May 25 13:00 ..
drwxr-x--- 14 federicog federicog 4096 May 25 14:55 federicog
drwxr-x---  2 test_user test_user 4096 Jun  1 12:26 test_user
federicog@federicog:/home$ cd test_user/
```

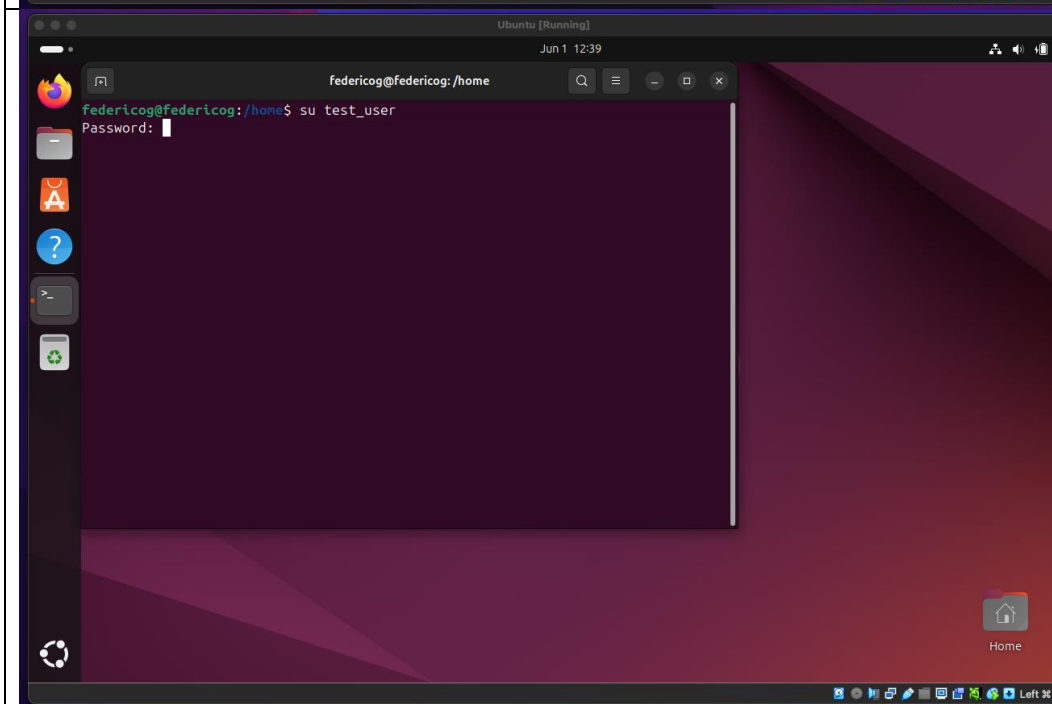
Intentamos ingresar al directorio del usuario recientemente creado, estando logueados con el usuario que lo creo.



The terminal window shows the user 'federicog' at the prompt 'federicog@federicog:/home'. They run 'ls -al' and see a directory listing. Then they run 'cd test_user/' and receive the error 'bash: cd: test_user/: Permission denied'.

```
federicog@federicog:/home$ ls -al
total 16
drwxr-xr-x  4 root    root      4096 Jun  1 12:26 .
drwxr-xr-x 23 root    root      4096 May 25 13:00 ..
drwxr-x--- 14 federicog federicog 4096 May 25 14:55 federicog
drwxr-x---  2 test_user test_user 4096 Jun  1 12:26 test_user
federicog@federicog:/home$ cd test_user/
bash: cd: test_user/: Permission denied
federicog@federicog:/home$
```

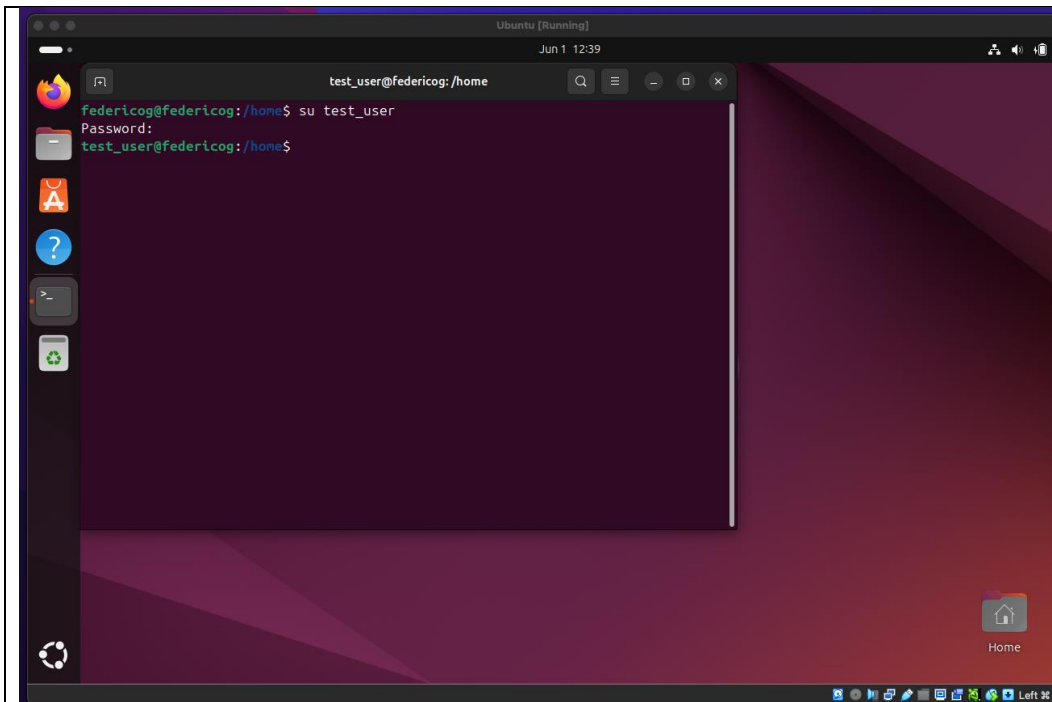
Y recibimos un rechazo por no tener permisos correctos para poder ingresar al directorio solicitado.



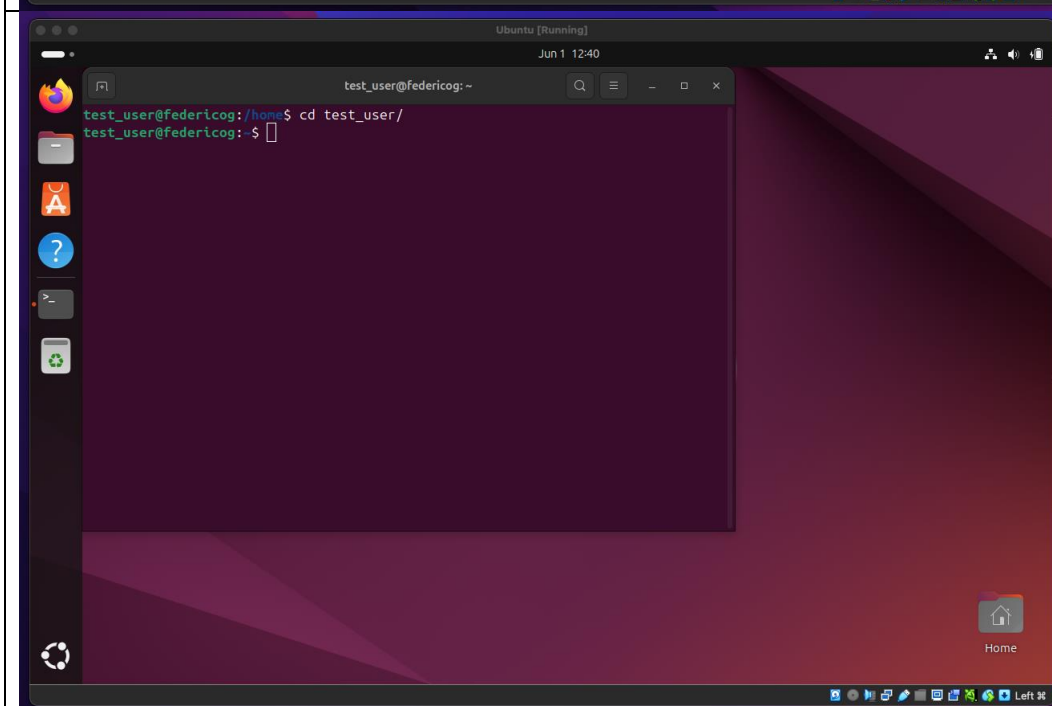
The terminal window shows the user 'federicog' at the prompt 'federicog@federicog:/home'. They run 'su test_user' and enter a password, successfully switching to the 'test_user'.

```
federicog@federicog:/home$ su test_user
Password:
```

Cambiamos de usuario al usuario creado recientemente.



Nos logueamos correctamente.



Y sin problemas podemos ingresar ahora si al directorio del usuario creado.