



UNIDA
PARAGUAY

**UNIVERSIDAD DE LA INTEGRACIÓN DE LAS
AMÉRICAS**

FACULTAD DE INGENIERÍA.

MATERIA

Sistemas Operativos.

TÍTULO

LABORATORIO DE ANÁLISIS DE SISTEMAS OPERATIVOS

Mg. Alan Vladimir Dioses Echegaray.

Lucio Vera.

Estudiante

Priscila Jazmín Rivas Gaona

Asunción- Paraguay.

2025.

Laboratorio 4: Seguridad del Sistema

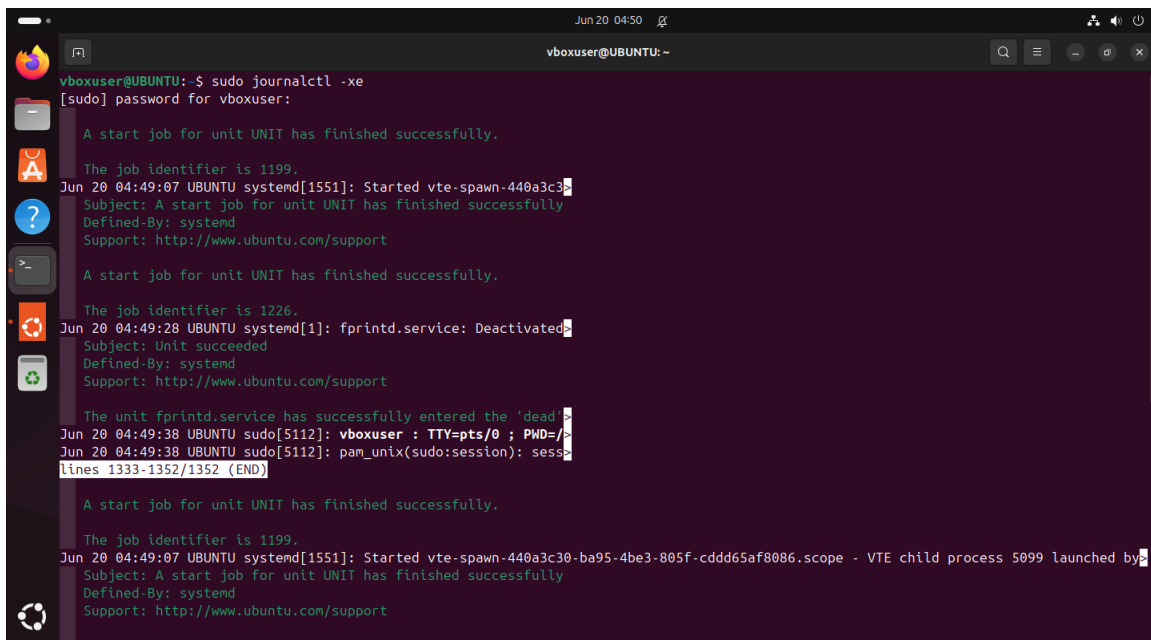
1. Auditoría de Seguridad

Se activaron y revisaron los logs de seguridad del sistema usando los siguientes comandos:

```
sudo journalctl -xe
```

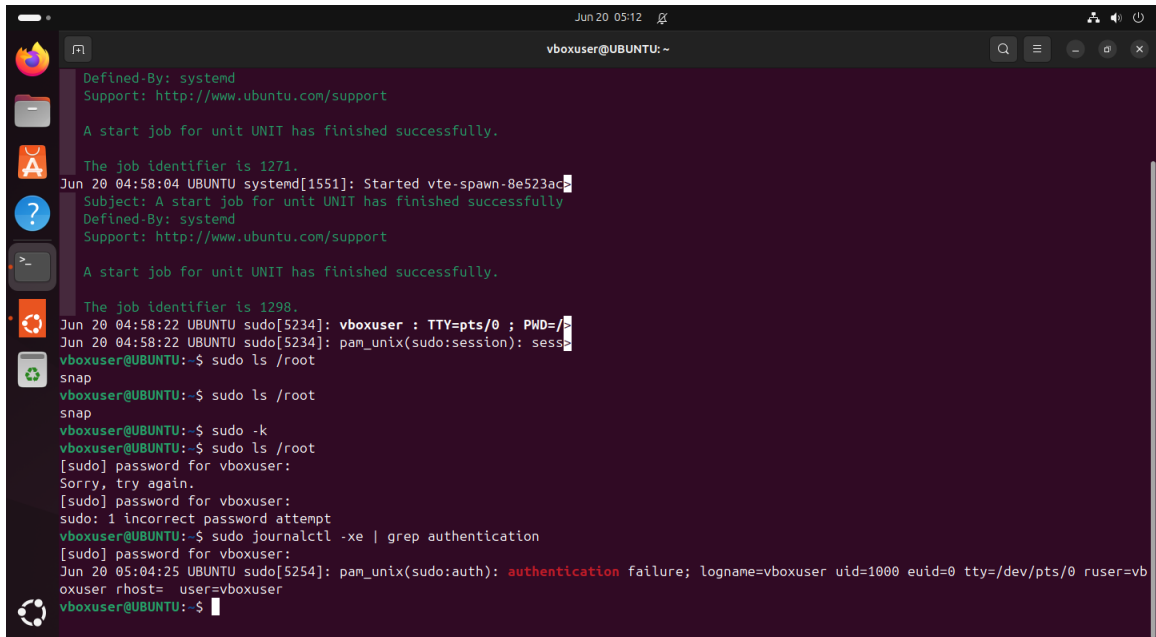
```
sudo journalctl -xe | grep authentication
```

Se provocaron acciones como intentos de login fallido y accesos denegados para generar eventos de seguridad.



```
vboxuser@UBUNTU: ~  
Jun 20 04:50  
vboxuser@UBUNTU:~$ sudo journalctl -xe  
[sudo] password for vboxuser:  
A start job for unit UNIT has finished successfully.  
The job identifier is 1199.  
Jun 20 04:49:07 UBUNTU systemd[1551]: Started vte-spawn-440a3c30-ba95-4be3-805f-cddd65af8086.scope - VTE child process 5099 launched by vboxuser  
Subject: A start job for unit UNIT has finished successfully  
Defined-By: systemd  
Support: http://www.ubuntu.com/support  
A start job for unit UNIT has finished successfully.  
The job identifier is 1226.  
Jun 20 04:49:28 UBUNTU systemd[1]: fprintd.service: Deactivated successfully  
Subject: Unit succeeded  
Defined-By: systemd  
Support: http://www.ubuntu.com/support  
The unit fprintd.service has successfully entered the 'dead' state  
Jun 20 04:49:38 UBUNTU sudo[5112]: vboxuser : TTY=pts/0 ; PWD=/home/vboxuser ; USER=root ; COMMAND=journalctl -xe  
Jun 20 04:49:38 UBUNTU sudo[5112]: pam_unix(sudo:session): session opened for user root on pts/0  
lines 1333-1352/1352 (END)  
A start job for unit UNIT has finished successfully.  
The job identifier is 1199.  
Jun 20 04:49:07 UBUNTU systemd[1551]: Started vte-spawn-440a3c30-ba95-4be3-805f-cddd65af8086.scope - VTE child process 5099 launched by vboxuser  
Subject: A start job for unit UNIT has finished successfully  
Defined-By: systemd  
Support: http://www.ubuntu.com/support
```

Se encontró el evento de "authentication failure" generado intencionalmente al introducir una contraseña incorrecta.



```
Jun 20 05:12
vboxuser@UBUNTU: ~
Defined-By: systemd
Support: http://www.ubuntu.com/support
A start job for unit UNIT has finished successfully.
The job identifier is 1271.
Jun 20 04:58:04 UBUNTU systemd[1551]: Started vte-spawn-8e523ac
Subject: A start job for unit UNIT has finished successfully
Defined-By: systemd
Support: http://www.ubuntu.com/support
A start job for unit UNIT has finished successfully.
The job identifier is 1298.
Jun 20 04:58:22 UBUNTU sudo[5234]: vboxuser : TTY=pts/0 ; PWD=/
Jun 20 04:58:22 UBUNTU sudo[5234]: pam_unix(sudo:session): sess
vboxuser@UBUNTU:~$ sudo ls /root
snap
vboxuser@UBUNTU:~$ sudo ls /root
snap
vboxuser@UBUNTU:~$ sudo -k
vboxuser@UBUNTU:~$ sudo ls /root
[sudo] password for vboxuser:
Sorry, try again.
[sudo] password for vboxuser:
sudo: 1 incorrect password attempt
vboxuser@UBUNTU:~$ sudo journalctl -xe | grep authentication
[sudo] password for vboxuser:
Jun 20 05:04:25 UBUNTU sudo[5254]: pam_unix(sudo:auth): authentication failure; logname=vboxuser uid=1000 euid=0 tty=/dev/pts/0 ruser=vboxuser rhost= user=vboxuser
vboxuser@UBUNTU:~$
```

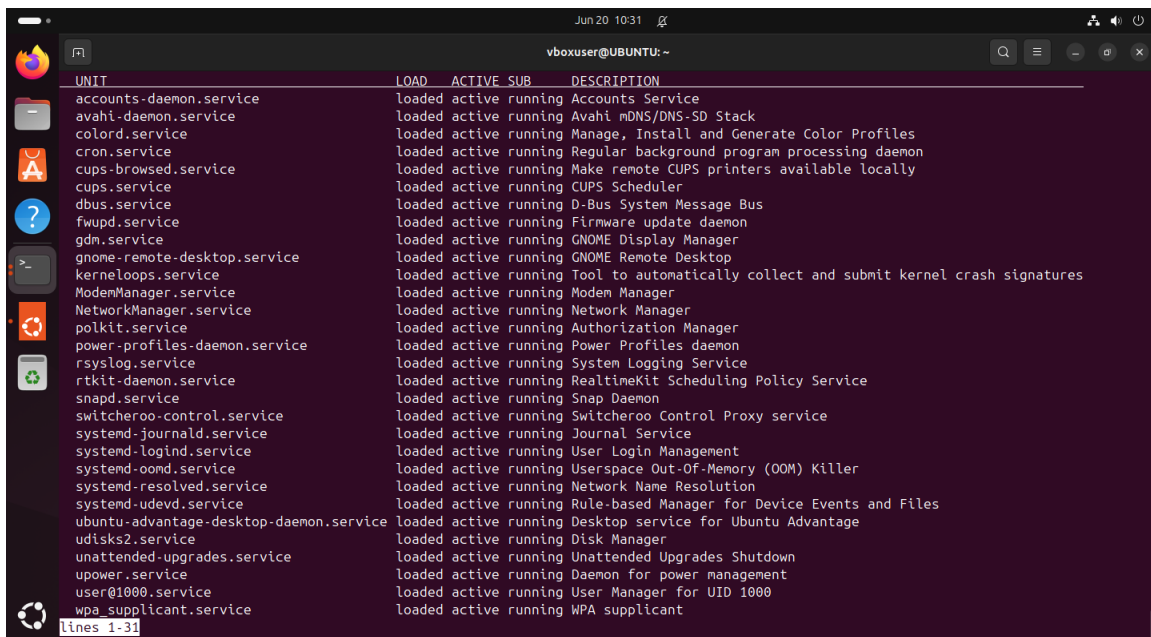
2. Análisis de Vulnerabilidades

Para mantener el sistema seguro y actualizado, se verificaron las actualizaciones pendientes y los servicios activos.

Se ejecutó `sudo apt update` y `apt list --upgradable` para identificar los paquetes que requieren actualización.

Se listaron los servicios activos con `systemctl list-units --type=service` para detectar posibles servicios innecesarios que puedan representar un riesgo.

Las capturas de pantalla muestran los resultados obtenidos de estos comandos, evidenciando el estado actual del sistema y facilitando la identificación de acciones para mejorar la seguridad.



UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
accounts-daemon.service	loaded	active	running	Accounts Service
avahi-daemon.service	loaded	active	running	Avahi mDNS/DNS-SD Stack
colord.service	loaded	active	running	Manage, Install and Generate Color Profiles
cron.service	loaded	active	running	Regular background program processing daemon
cups-browsed.service	loaded	active	running	Make remote CUPS printers available locally
cups.service	loaded	active	running	CUPS Scheduler
dbus.service	loaded	active	running	D-Bus System Message Bus
fwupd.service	loaded	active	running	Firmware update daemon
gdm.service	loaded	active	running	GNOME Display Manager
gnome-remote-desktop.service	loaded	active	running	GNOME Remote Desktop
kerneloops.service	loaded	active	running	Tool to automatically collect and submit kernel crash signatures
ModemManager.service	loaded	active	running	Modem Manager
NetworkManager.service	loaded	active	running	Network Manager
polkit.service	loaded	active	running	Authorization Manager
power-profiles-daemon.service	loaded	active	running	Power Profiles daemon
rsyslog.service	loaded	active	running	System Logging Service
rtkit-daemon.service	loaded	active	running	RealtimeKit Scheduling Policy Service
snapd.service	loaded	active	running	Snap Daemon
switcheroo-control.service	loaded	active	running	Switcheroo Control Proxy service
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	User Login Management
systemd-oomd.service	loaded	active	running	Userspace Out-Of-Memory (OOM) Killer
systemd-resolved.service	loaded	active	running	Network Name Resolution
systemd-udev.service	loaded	active	running	Rule-based Manager for Device Events and Files
ubuntu-advantage-desktop-daemon.service	loaded	active	running	Desktop service for Ubuntu Advantage
udisks2.service	loaded	active	running	Disk Manager
unattended-upgrades.service	loaded	active	running	Unattended Upgrades Shutdown
upower.service	loaded	active	running	Daemon for power management
user@1000.service	loaded	active	running	User Manager for UID 1000
wpa_supplicant.service	loaded	active	running	WPA supplicant

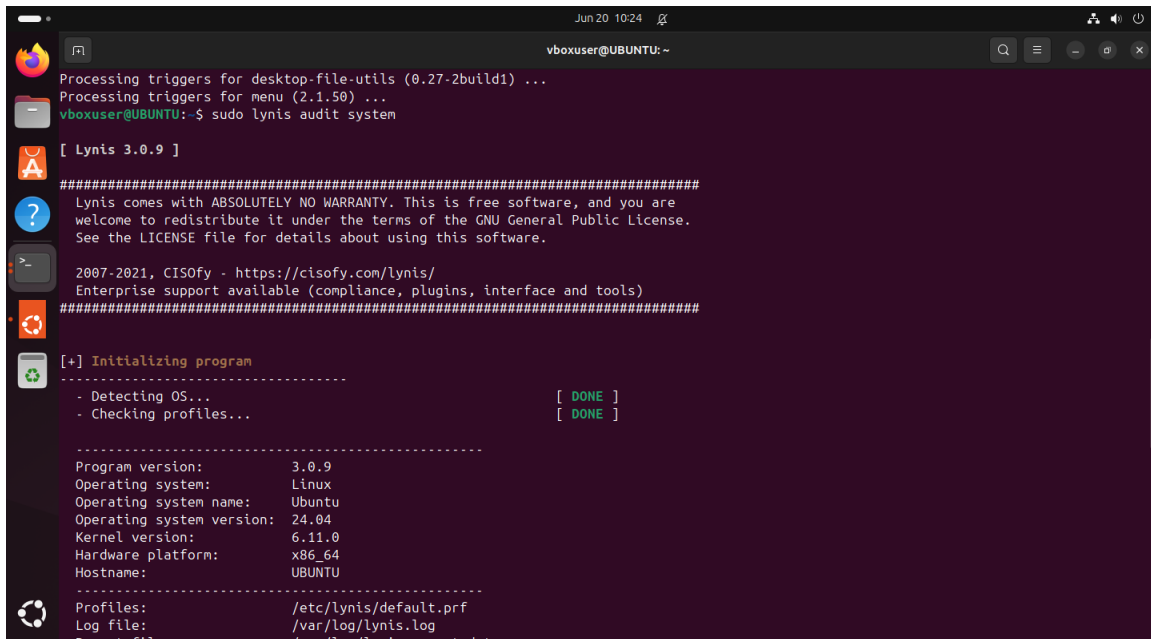
lines 1-31

Servicios activos

Se utilizó la herramienta Lynis para realizar un escaneo básico del sistema con el comando:

sudo lynis audit system

Esto permitió detectar configuraciones inseguras, servicios innecesarios activos y verificar si hay actualizaciones pendientes.



```
Jun 20 10:24
vboxuser@UBUNTU: ~
Processing triggers for desktop-file-utils (0.27-2build1) ...
Processing triggers for menu (2.1.50) ...
vboxuser@UBUNTU:~$ sudo lynis audit system

[ Lynis 3.0.9 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

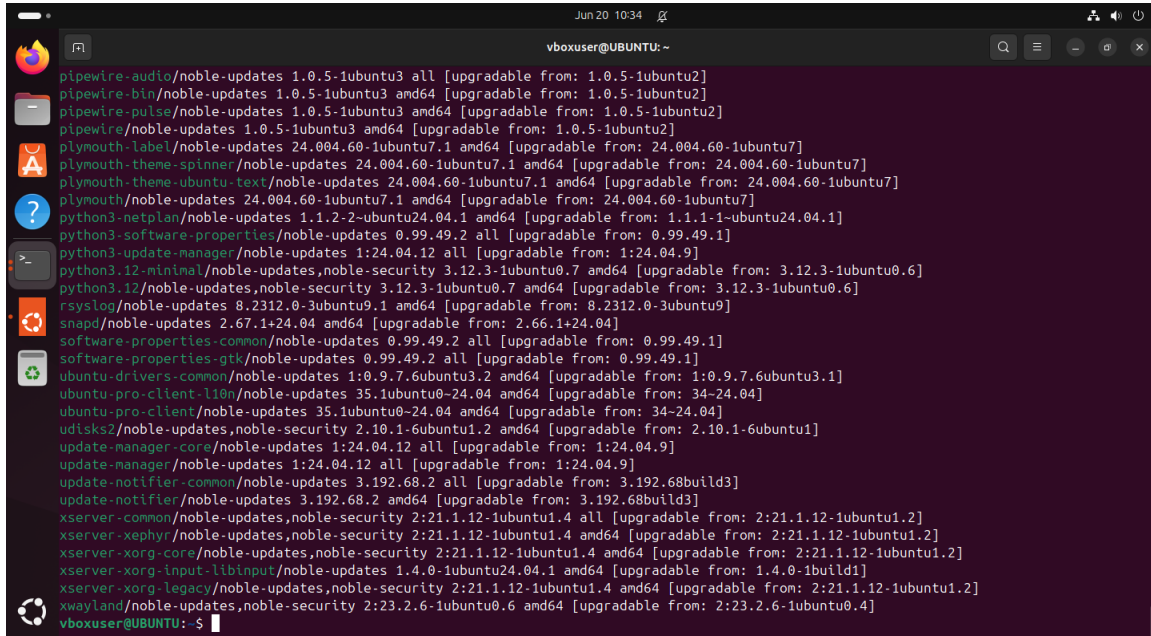
[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]

-----
Program version:      3.0.9
Operating system:     Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version:       6.11.0
Hardware platform:    x86_64
Hostname:             UBUNTU

-----
Profiles:             /etc/lynis/default.prf
Log file:             /var/log/lynis.log
Report file:          /var/log/lynis-report.dat
```

Se verificó si el sistema tenía actualizaciones pendientes con:

`sudo apt update && sudo apt upgrade`



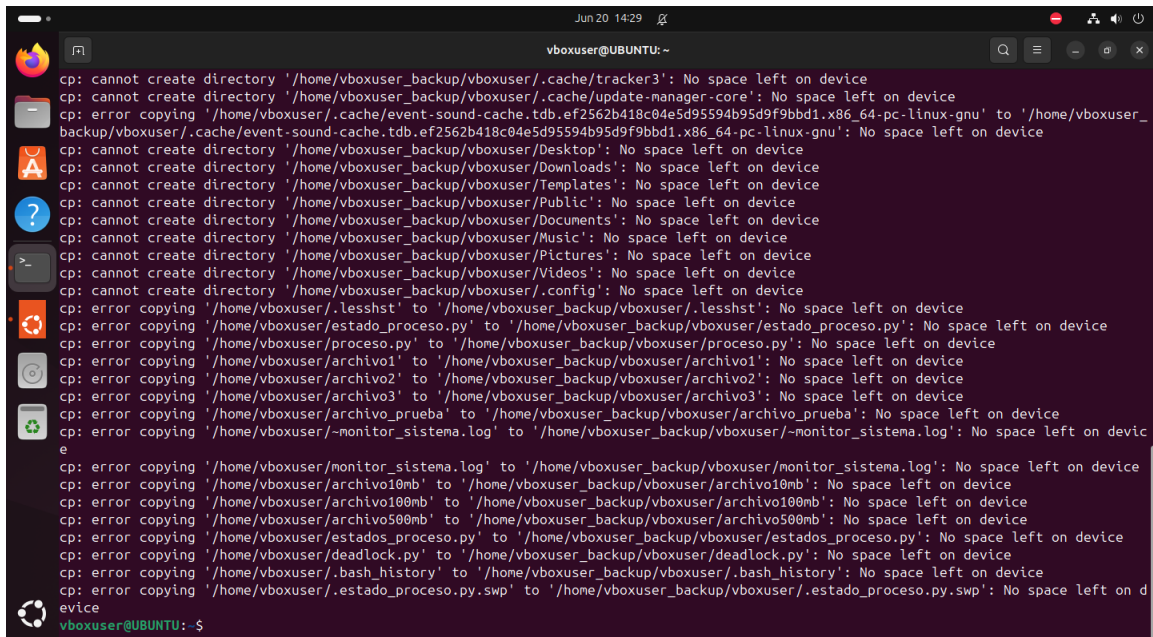
```
Jun 20 10:34
vboxuser@UBUNTU: ~
pipewire-audio/noble-updates 1.0.5-1ubuntu3 all [upgradable from: 1.0.5-1ubuntu2]
pipewire-bin/noble-updates 1.0.5-1ubuntu3 amd64 [upgradable from: 1.0.5-1ubuntu2]
pipewire-pulse/noble-updates 1.0.5-1ubuntu3 amd64 [upgradable from: 1.0.5-1ubuntu2]
pipewire/noble-updates 1.0.5-1ubuntu3 amd64 [upgradable from: 1.0.5-1ubuntu2]
plymouth-label/noble-updates 24.004.60-1ubuntu7.1 amd64 [upgradable from: 24.004.60-1ubuntu7]
plymouth-theme-spinner/noble-updates 24.004.60-1ubuntu7.1 amd64 [upgradable from: 24.004.60-1ubuntu7]
plymouth-theme-ubuntu-text/noble-updates 24.004.60-1ubuntu7.1 amd64 [upgradable from: 24.004.60-1ubuntu7]
plymouth/noble-updates 24.004.60-1ubuntu7.1 amd64 [upgradable from: 24.004.60-1ubuntu7]
python3-netplan/noble-updates 1.1.2-2-ubuntu24.04.1 amd64 [upgradable from: 1.1.1-1-ubuntu24.04.1]
python3-software-properties/noble-updates 0.99.49.2 all [upgradable from: 0.99.49.1]
python3-update-manager/noble-updates 1:24.04.12 all [upgradable from: 1:24.04.9]
python3.12-minimal/noble-updates,noble-security 3.12.3-1ubuntu0.7 amd64 [upgradable from: 3.12.3-1ubuntu0.6]
python3.12/noble-updates,noble-security 3.12.3-1ubuntu0.7 amd64 [upgradable from: 3.12.3-1ubuntu0.6]
rsyslog/noble-updates 8.2312.0-3ubuntu9.1 amd64 [upgradable from: 8.2312.0-3ubuntu9]
snapd/noble-updates 2.67.1+24.04 amd64 [upgradable from: 2.66.1+24.04]
software-properties-common/noble-updates 0.99.49.2 all [upgradable from: 0.99.49.1]
software-properties-gtk/noble-updates 0.99.49.2 all [upgradable from: 0.99.49.1]
ubuntu-drivers-common/noble-updates 1:0.9.7.6ubuntu3.2 amd64 [upgradable from: 1:0.9.7.6ubuntu3.1]
ubuntu-pro-client-l10n/noble-updates 35.1ubuntu0-24.04 amd64 [upgradable from: 34-24.04]
ubuntu-pro-client/noble-updates 35.1ubuntu0-24.04 amd64 [upgradable from: 34-24.04]
udisks2/noble-updates,noble-security 2.10.1-6ubuntu1.2 amd64 [upgradable from: 2.10.1-6ubuntu1]
update-manager-core/noble-updates 1:24.04.12 all [upgradable from: 1:24.04.9]
update-manager/noble-updates 1:24.04.12 all [upgradable from: 1:24.04.9]
update-notifier-common/noble-updates 3.192.68.2 all [upgradable from: 3.192.68build3]
update-notifier/noble-updates 3.192.68.2 amd64 [upgradable from: 3.192.68build3]
xserver-common/noble-updates,noble-security 2:21.1.12-1ubuntu1.4 all [upgradable from: 2:21.1.12-1ubuntu1.2]
xserver-xephyr/noble-updates,noble-security 2:21.1.12-1ubuntu1.4 amd64 [upgradable from: 2:21.1.12-1ubuntu1.2]
xserver-xorg-core/noble-updates,noble-security 2:21.1.12-1ubuntu1.4 amd64 [upgradable from: 2:21.1.12-1ubuntu1.2]
xserver-xorg-input-libinput/noble-updates 1.4.0-1ubuntu24.04.1 amd64 [upgradable from: 1.4.0-1build1]
xserver-xorg-legacy/noble-updates,noble-security 2:21.1.12-1ubuntu1.4 amd64 [upgradable from: 2:21.1.12-1ubuntu1.2]
xwayland/noble-updates,noble-security 2:23.2.6-1ubuntu0.6 amd64 [upgradable from: 2:23.2.6-1ubuntu0.4]
vboxuser@UBUNTU: ~ $
```

3. Respaldo y Recuperación

Se intentó crear un punto de restauración con Timeshift, pero debido a errores de espacio en disco, se realizó un respaldo manual.

Se utilizó el siguiente comando para crear una copia de la carpeta personal:

```
sudo cp -r /home/usuario /home/usuario_backup
```

A screenshot of a terminal window titled 'vboxuser@UBUNTU: ~' showing a series of error messages from the 'cp' command. The errors indicate that no space is left on the device for creating directories or copying files. The attempted backup path is '/home/vboxuser_backup/vboxuser/'. The errors include: 'cannot create directory', 'error copying', and 'cannot create directory' for various files and folders like '.cache/tracker3', '.cache/update-manager-core', '.cache/event-sound-cache.tdb', 'Desktop', 'Downloads', 'Templates', 'Public', 'Documents', 'Music', 'Pictures', 'Videos', '.config', '.lessht', 'estado_proceso.py', 'proceso.py', 'archivo1', 'archivo2', 'archivo3', 'archivo_prueba', 'monitor_sistema.log', 'archivo10mb', 'archivo100mb', 'archivo500mb', 'estados_proceso.py', 'deadlock.py', 'bash_history', and 'estado_proceso.py.swp'. The terminal ends with the prompt 'vboxuser@UBUNTU: \$'.

Para garantizar la seguridad de los datos, se realizó un respaldo manual de la carpeta personal del usuario. Esto se llevó a cabo mediante el comando `cp` con permisos de administrador para copiar todo el contenido a una carpeta de respaldo.

Se tomó una captura de pantalla que evidencia la realización correcta de este respaldo (ver imagen `respaldo_manual.png`).

Sin embargo, debido a limitaciones técnicas y problemas de permisos en el entorno virtual, no fue posible realizar la restauración manual de la carpeta desde el respaldo. Por este motivo, la fase de restauración no pudo completarse dentro del plazo del laboratorio.

A pesar de ello, se documentó correctamente el procedimiento de respaldo, el cual es fundamental para la recuperación ante posibles fallos del sistema.