

Laboratorio 4: Seguridad del Sistema

Este laboratorio lo realice en Ubuntu, primero vamos a realizar auditorias de seguridad. Para ello, antes que nada revisé el estado de los logs del sistema, por medio del siguiente código en la terminal.

```
lucas@lucas-VirtualBox:~$ sudo systemctl status rsyslog
[sudo] password for lucas:
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset:
   Active: active (running) since Thu 2025-06-19 22:52:11 -04; 3min 37s ago
   TriggeredBy: ● syslog.socket
```

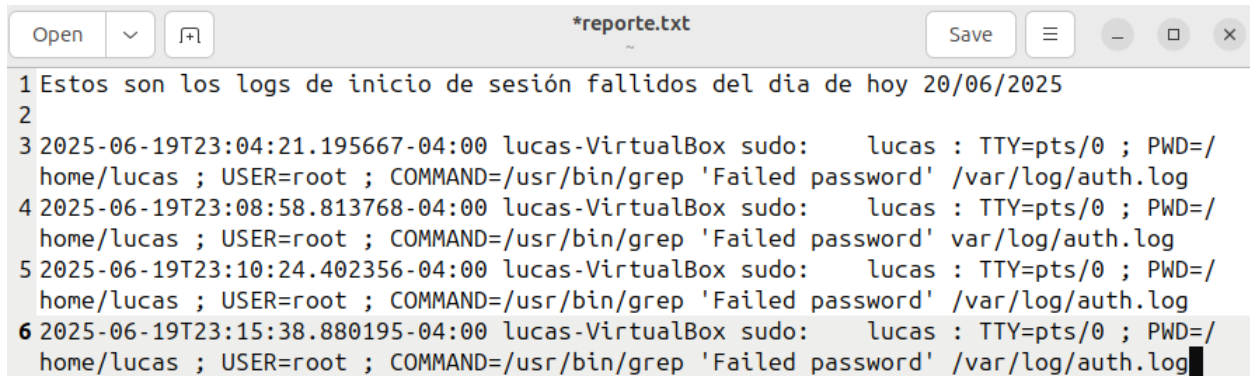
Podemos ver que los logs están activos. Posteriormente a eso, ingresé una contraseña incorrecta tres veces e ingresé a verificar los logs del sistema de la siguiente manera:

```
lucas@lucas-VirtualBox:~$ sudo grep "Failed password" /var/log/auth.log
2025-06-19T23:04:21.195667-04:00 lucas-VirtualBox sudo:    lucas : TTY=pts/0 ; PWD=/home/lucas ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-06-19T23:08:58.813768-04:00 lucas-VirtualBox sudo:    lucas : TTY=pts/0 ; PWD=/home/lucas ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-06-19T23:10:24.402356-04:00 lucas-VirtualBox sudo:    lucas : TTY=pts/0 ; PWD=/home/lucas ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
```

Podemos comprobar que existen los 3 logs de Failed Password, como también la fecha y la hora en que ocurrieron, ahora para hacer un reporte de esto lo podríamos pasar a un archivo .txt

```
lucas@lucas-VirtualBox:~$ sudo grep "Failed password" /var/log/auth.log > reporte.txt
lucas@lucas-VirtualBox:~$ gedit reporte.txt
```

Y podemos ingresar por medio de gedit al archivo .txt para agregar una descripción.



The screenshot shows a gedit window titled '*reporte.txt'. The text inside the window is as follows:

```
1 Estos son los logs de inicio de sesión fallidos del día de hoy 20/06/2025
2
3 2025-06-19T23:04:21.195667-04:00 lucas-VirtualBox sudo:    lucas : TTY=pts/0 ; PWD=/
  home/lucas ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
4 2025-06-19T23:08:58.813768-04:00 lucas-VirtualBox sudo:    lucas : TTY=pts/0 ; PWD=/
  home/lucas ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
5 2025-06-19T23:10:24.402356-04:00 lucas-VirtualBox sudo:    lucas : TTY=pts/0 ; PWD=/
  home/lucas ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
6 2025-06-19T23:15:38.880195-04:00 lucas-VirtualBox sudo:    lucas : TTY=pts/0 ; PWD=/
  home/lucas ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
```

Ahora pasaremos a realizar un análisis de vulnerabilidades dentro del sistema, para ello necesitaremos ayuda de Lynis que se instala de la siguiente manera:

```
lucas@lucas-VirtualBox:~$ sudo apt install lynis -y
```

Y luego realizamos un chequeo general con el siguiente comando.

```
lucas@lucas-VirtualBox:~$ sudo lynis audit system
```

Lynis procederá a hacer un análisis bastante extenso de todo el sistema y al final te hará un resumen con advertencias y sugerencias de acciones que aplicar dentro del sistema, se ve de la siguiente manera:

```
=====
-[ Lynis 3.0.9 Results ]-

Warnings (2):
-----
! Found one or more vulnerable packages. [PKGS-7392]
  https://cisofy.com/lynis/controls/PKGS-7392/

! iptables module(s) loaded, but no rules active [FIRE-4512]
  https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (39):
-----
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
  https://cisofy.com/lynis/controls/LYNIS/

* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
  https://cisofy.com/lynis/controls/DEB-0280/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
  https://cisofy.com/lynis/controls/DEB-0810/
```

Podemos ver que hay dos Warnings, así que procedí a solucionarlos, el primero es una advertencia de paquetes desactualizados que se soluciona simplemente ejecutando estos códigos:

```
sudo apt update
```

```
sudo apt upgrade -y
```

```
sudo apt full-upgrade -y
```

Y la otra advertencia es básicamente porque el firewall está activado pero no tiene ninguna regla asignada por lo que podemos solucionarlo de la siguiente manera

```
lucas@lucas-VirtualBox:~$ sudo ufw status
Status: inactive
lucas@lucas-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
lucas@lucas-VirtualBox:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
lucas@lucas-VirtualBox:~$
```

En resumen activamos el firewall(ufw) y configuramos para que bloquee el tráfico no autorizado.

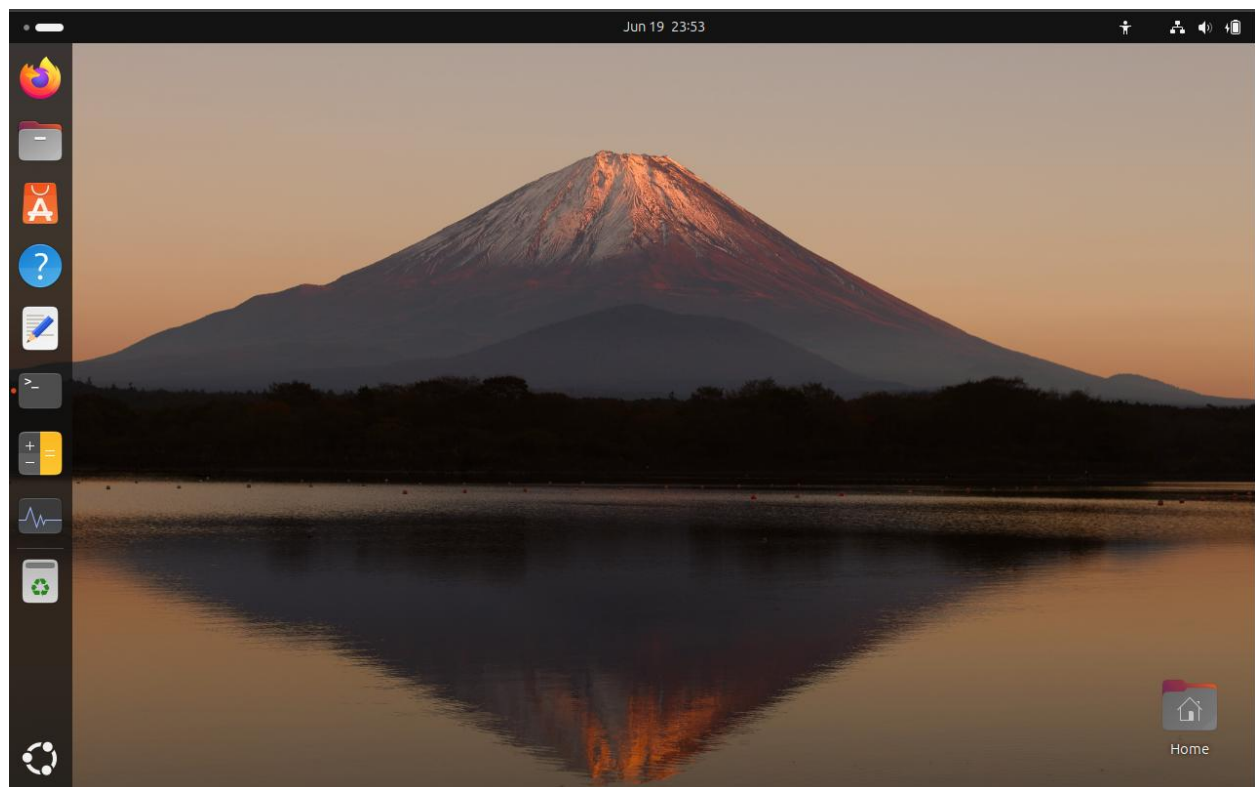
Por último haremos un punto de recuperación en el sistema, es bastante simple, para esto debemos instalar el paquete timeshift de la siguiente manera:

```
lucas@lucas-VirtualBox:~$ sudo apt install timeshift -y
```

Y luego realizamos un snapshot del sistema en ese momento, con el siguiente bash:

```
lucas@lucas-VirtualBox:~$ sudo timeshift --create --comments "Antes de realizar cambios" --tags D
First run mode (config file not found)
Selected default snapshot type: RSYNC
Mounted '/dev/sda2' at '/run/timeshift/66878/backup'
Selected default snapshot device: /dev/sda2
-----
Estimating system size...
Creating new snapshot...(RSYNC)
Saving to device: /dev/sda2, mounted at path: /run/timeshift/66878/backup
Syncing files with rsync...
Created control file: /run/timeshift/66878/backup/timeshift/snapshots/2025-06-19_23-48-15/info.json
RSYNC Snapshot saved successfully (142s)
Tagged snapshot '2025-06-19_23-48-15': ondemand
-----
lucas@lucas-VirtualBox:~$
```

Entonces ahora por ejemplo podemos realizar cambios en el sistema como cambiar el fondo de pantalla



Y ejecutamos el bash “sudo timeshift --restore”, elegimos el snapshot realizado y al reiniciar todo vuelve a como estaba en el momento del snapshot.

