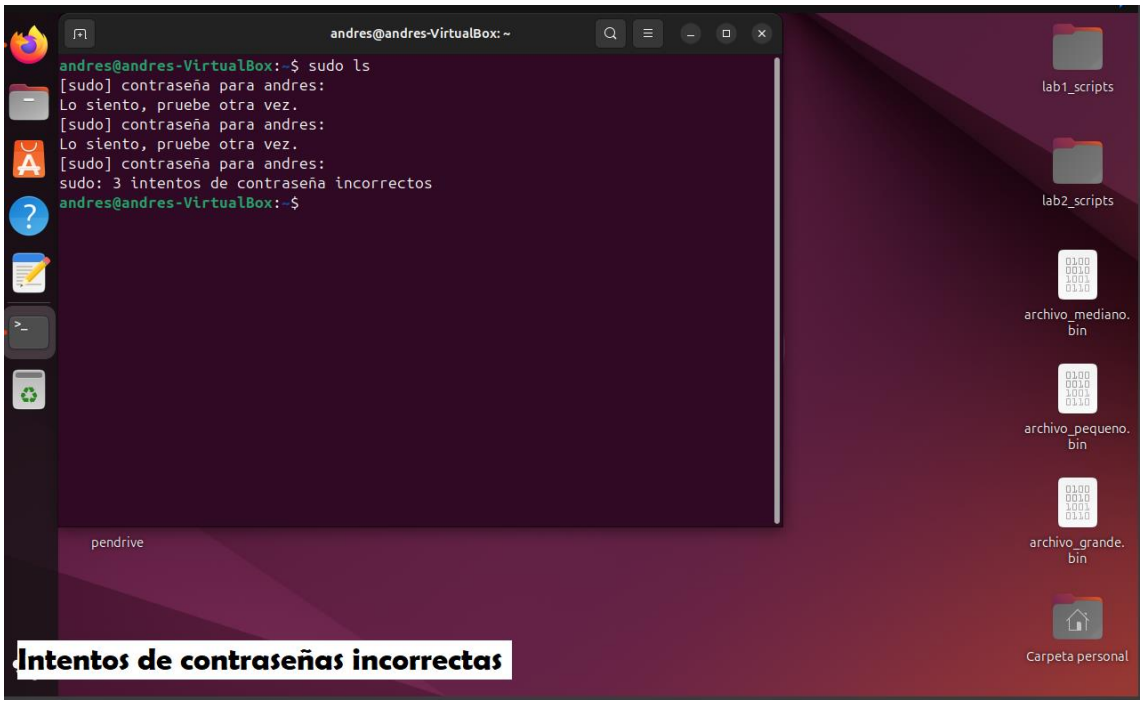
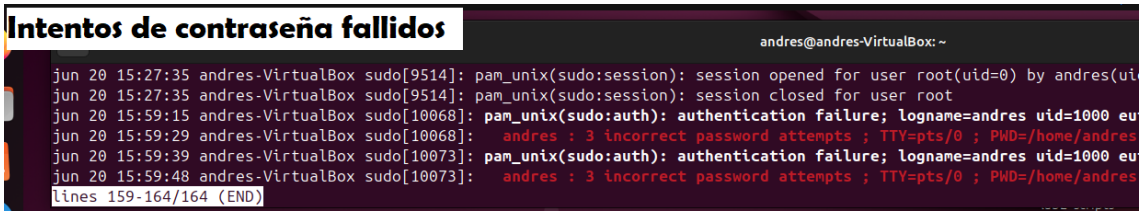
Informe Laboratorio 4

1. Auditoría de logs de Seguridad

La auditoría de logs es fundamental para la seguridad informática porque permite registrar, analizar y responder a actividades que ocurren en un sistema. Los logs (o registros) contienen información detallada sobre acciones de usuarios, procesos del sistema, accesos, errores, y más.

La prueba realizada fue ejecutar el comando “sudo ls” y luego errar las solicitudes de contraseña.

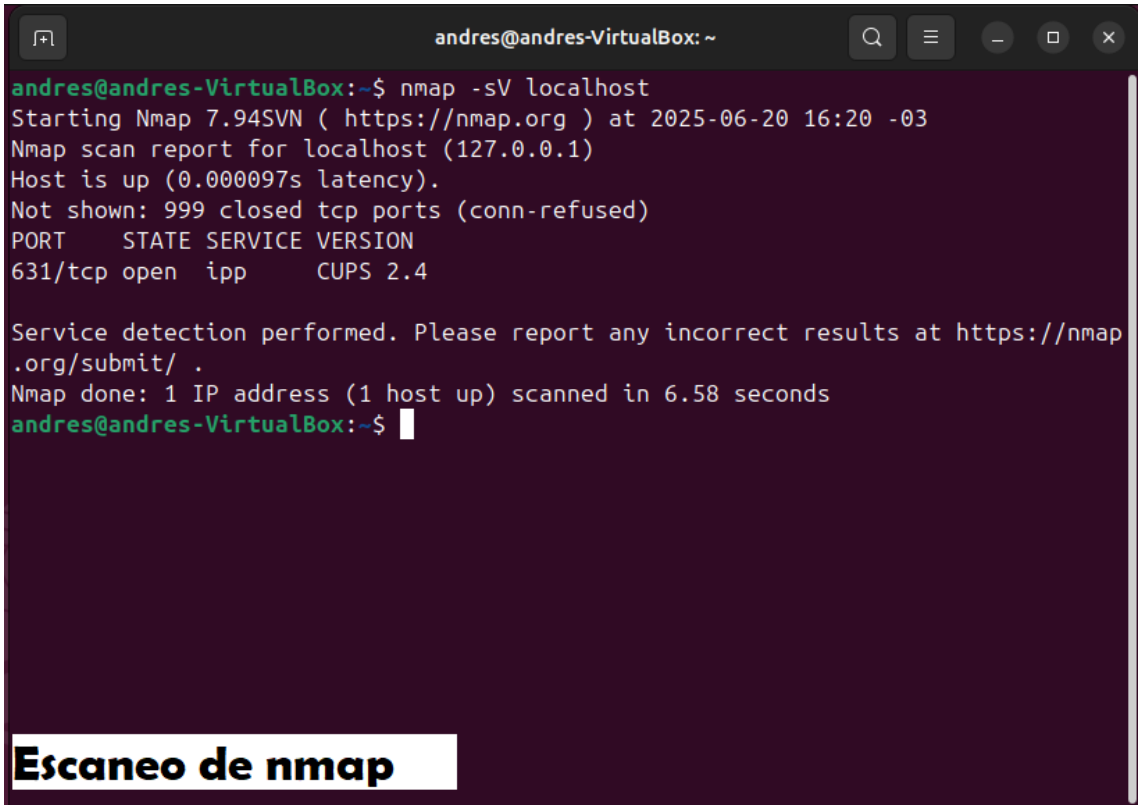




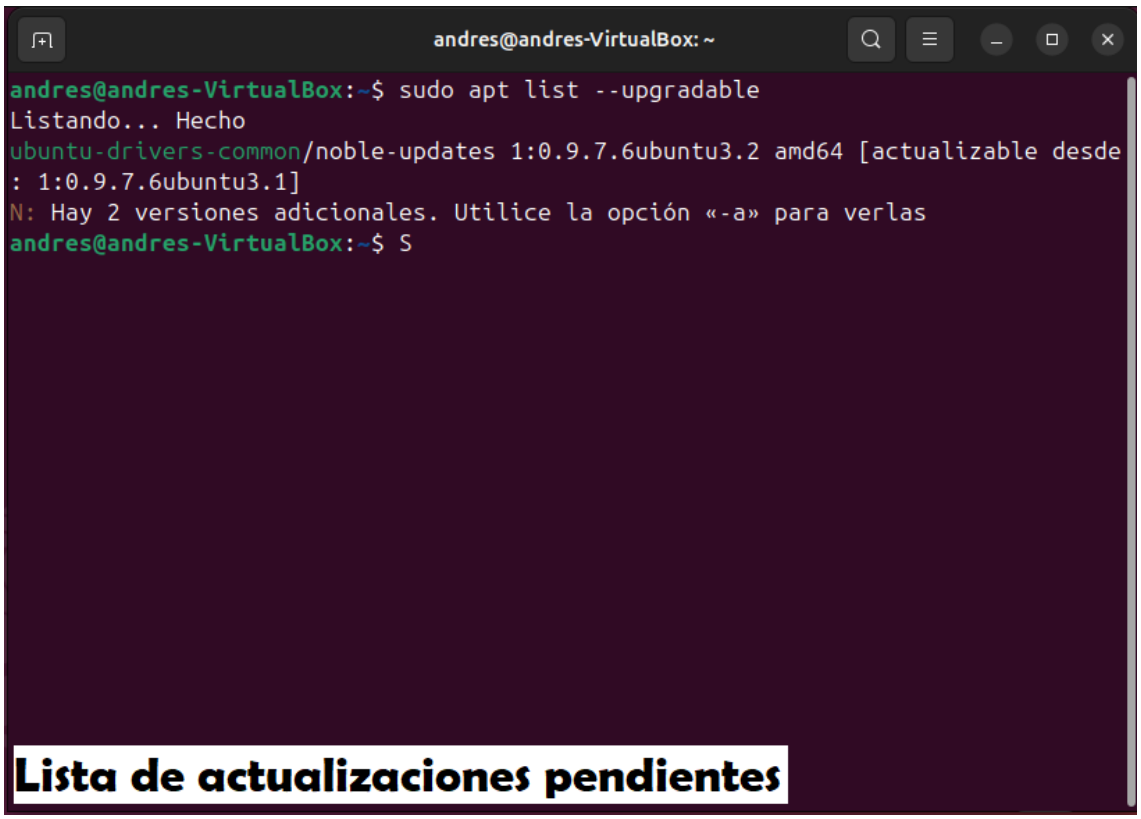
La imagen muestra el log generado por un intento fallido de autenticación con sudo. El sistema registra el usuario (andres) y el terminal (tty) desde donde se originó el intento. Este tipo de logs son esenciales para detectar intentos de escalada de privilegios no autorizados.

2. Análisis de vulnerabilidades

Para evaluar la seguridad del sistema, se verificó la lista de actualizaciones de software pendientes y se escanearon los puertos de red para identificar servicios en ejecución.

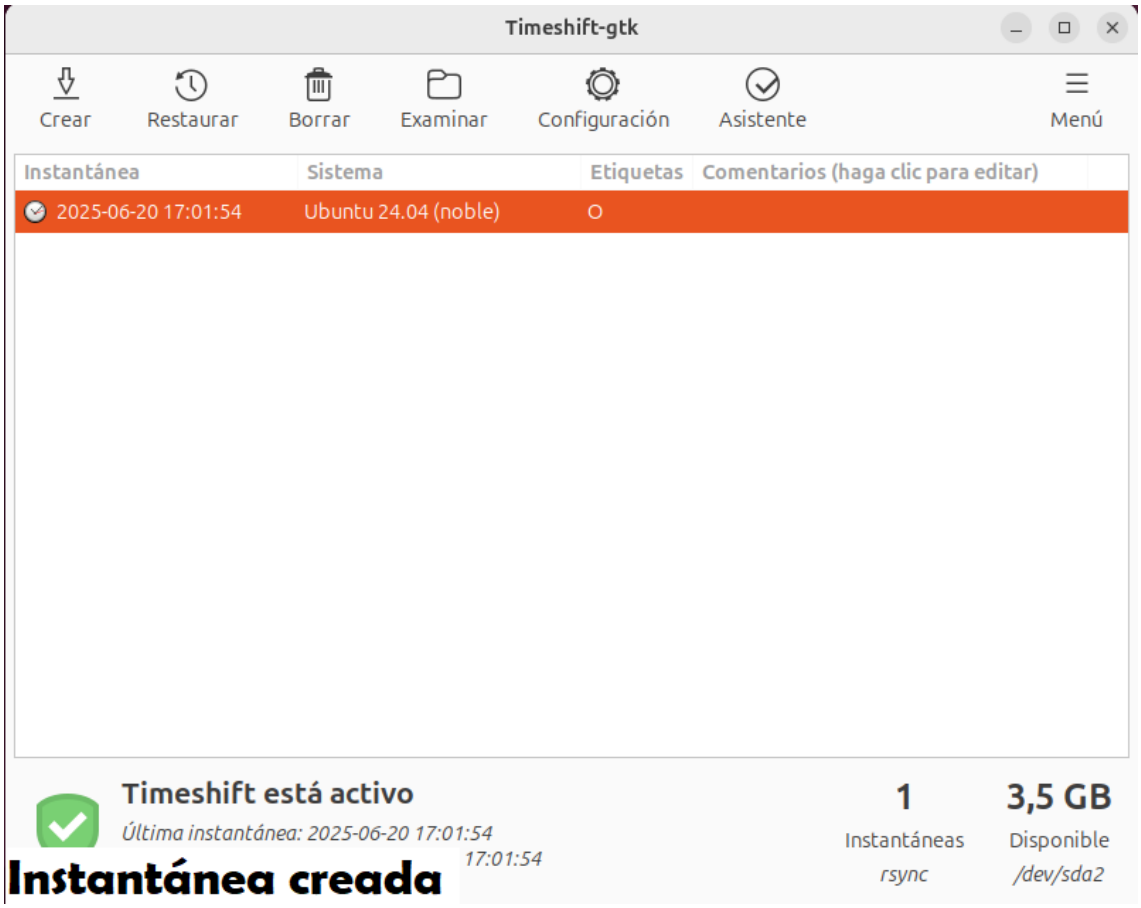


Se utilizó el comando sudo apt list --upgradable para listar los paquetes que tienen actualizaciones pendientes. Mantener el sistema actualizado es importante para corregir vulnerabilidades conocidas.



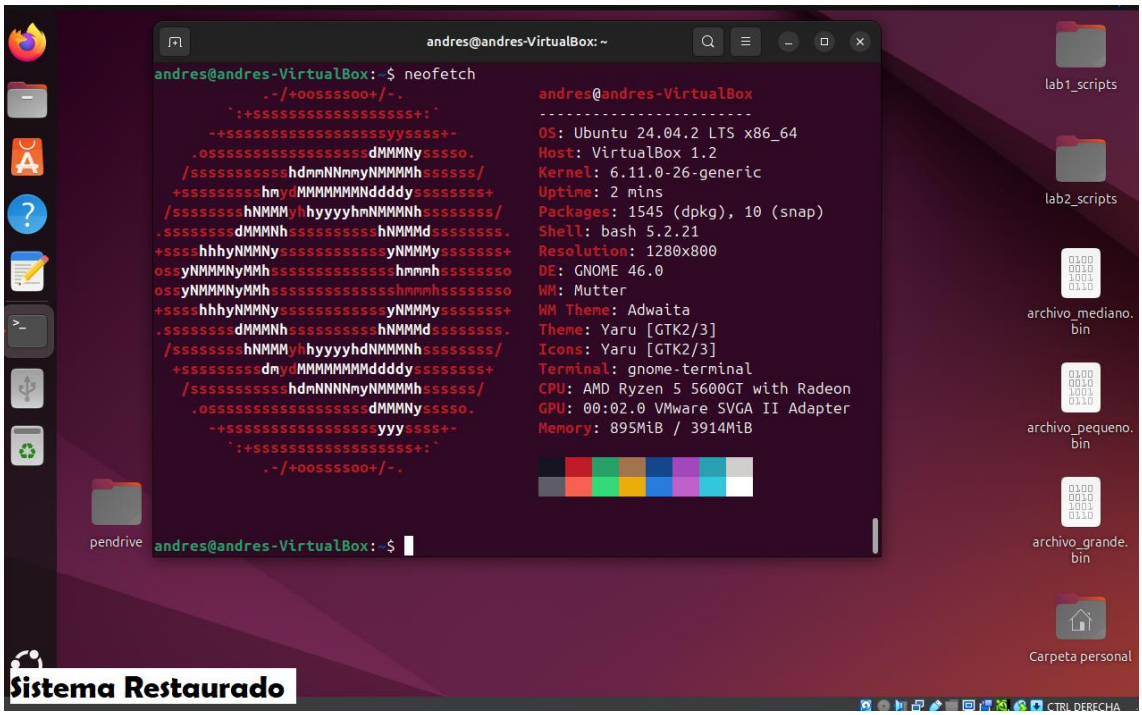
3. Estrategia de Respaldo y Recuperación

Los puntos de restauración son importantes porque permiten volver el sistema operativo a un estado anterior en caso de que ocurra un problema, sin afectar los archivos personales del usuario.



El procedimiento seguido fue crear una instantánea del SO utilizando timeshift, luego eliminar neofetch, para luego restaurar el SO con la instantánea creada y verificar que neofetch siga funcionando.


andres@andres-VirtualBox: ~
andres@andres-VirtualBox:~$ sudo apt remove neofetch
[sudo] contraseña para andres:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete «neofetch» no está instalado, no se eliminará
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
andres@andres-VirtualBox:~$ neofetch
No se ha encontrado la orden «neofetch», pero se puede instalar con:
sudo apt install neofetch
andres@andres-VirtualBox:~$
desinstalando neofetch


andres@andres-VirtualBox: ~
andres@andres-VirtualBox:~$ neofetch
andres@andres-VirtualBox
OS: Ubuntu 24.04.2 LTS x86_64
Host: VirtualBox 1.2
Kernel: 6.11.0-26-generic
Uptime: 2 mins
Packages: 1545 (dpkg), 10 (snap)
Shell: bash 5.2.21
Resolution: 1280x800
DE: GNOME 46.0
WM: Mutter
WM Theme: Adwaita
Theme: Yaru [GTK2/3]
Icons: Yaru [GTK2/3]
Terminal: gnome-terminal
CPU: AMD Ryzen 5 5600GT with Radeon
GPU: 00:02.0 VMware SVGA II Adapter
Memory: 895MiB / 3914MiB
andres@andres-VirtualBox:~$
pendrive
lab1_scripts
lab2_scripts
archivo_mediano.bin
archivo_pequeno.bin
archivo_grande.bin
Carpeta personal
Sistema Restaurado