Trabajo Práctico – Seguridad en Sistemas Operativos

Alumnos:
Martina López – martinalopez@gmail.com
Julián Álvarez – julianalvarez@gmail.com

Materia: Sistemas Operativos
Profesor: Ing. Ricardo Martínez
Fecha de Entrega: 05 de junio de 2025

Índice

Introducción

La seguridad en sistemas operativos es un aspecto fundamental para proteger la información y los recursos del sistema. Este trabajo analiza las principales técnicas de protección y muestra un ejemplo práctico de aplicación de permisos y auditoría en Linux.

Marco Teórico

Los sistemas operativos modernos incorporan mecanismos para controlar el acceso a archivos, usuarios, procesos y dispositivos. Entre los conceptos clave se incluyen:

- **Permisos de archivos**: lectura, escritura y ejecución para usuario, grupo y otros.
- **Usuarios y grupos**: segmentación de acceso por identidad.
- **Control de acceso basado en roles (RBAC)**.
- **Auditoría de eventos** mediante herramientas como `auditd`.
- **Manejo de privilegios** mediante `sudo` y `setuid`.

Caso Práctico

Se configuró un entorno Linux con múltiples usuarios para probar:

1. Restricciones de acceso a archivos mediante `chmod`.
2. Auditoría de accesos usando `auditctl`.
3. Uso seguro de `sudo`.

Comandos utilizados:

```
bash
CopyEdit
# Crear usuario y archivo protegido
sudo useradd usuario1
sudo touch /seguro/datos.txt
sudo chmod 600 /seguro/datos.txt

# Agregar regla de auditoría
sudo auditctl -w /seguro/datos.txt -p rwxa -k acceso_datos

# Consultar logs
sudo ausearch -k acceso_datos
```

Metodología Utilizada

- Se investigaron conceptos en manuales oficiales.
- Se configuró un entorno Linux (Ubuntu Server).
- Se realizaron pruebas controladas con distintos usuarios.
- Se documentaron los comandos, resultados y errores.

Resultados Obtenidos

- Se validó el bloqueo de acceso a archivos protegidos.
- Se registraron exitosamente intentos de acceso no autorizados.
- Se verificó la correcta delegación de privilegios con `sudo`.

Conclusiones

El control de acceso y la auditoría son herramientas claves para prevenir y detectar incidentes. La práctica permitió observar cómo pequeñas configuraciones refuerzan la seguridad de un sistema operativo.

Bibliografía

- The Linux Command Line (William Shotts)
- https://wiki.archlinux.org/title/Security
- https://linux.die.net/man/

Anexos

- Captura de pantalla de logs de auditoría
- Script de automatización de configuración