

INFORME LABORATORIO 4 - SEGURIDAD DEL SISTEMA

Nombre: Ricardo Paredes Colmán

Fecha: 21/06/2025

Sistema Operativo: Ubuntu 22.04 LTS

1. Auditoría de Seguridad

1.1 Configuración de Auditoría (auditd)

Se implementaron reglas para monitorizar accesos críticos:

```
sudo auditctl -w /etc/shadow -p rwa -k shadow_access
sudo auditctl -w /etc/passwd -p rwa -k passwd_access
```

Reglas activas (captura 1):

```
LIST_RULES: exit,always watch=/etc/shadow perm=rwa
LIST_RULES: exit,always watch=/etc/passwd perm=rwa
```

1.2 Eventos Registrados

Tabla de eventos relevantes:

Timestamp	Evento	Usuario	IP Origen	Acción Tomada
2025-06-20 18:15:23	Intento de login SSH	root	192.168.1.100	sudo ufw deny from 192.168.1.100
2025-06-20 18:20:45	Lectura de /etc/shadow	invitado	N/A (local)	Revocar permisos del usuario

Logs capturados (captura 2):

```
type=USER_LOGIN msg=audit(1624263323.123:456): user pid=1234 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct="root" exe="/usr/sbin/sshd" hostname=192.168.1.100 addr=192.168.1.100 terminal=ssh res=failed'
```

2. Análisis de Vulnerabilidades

2.1 Escaneo con Lynis

Comando ejecutado:

```
sudo lynis audit system
```

Hallazgos críticos (captura 3):

```
[!] AUTH-9328: Password expiration disabled for user 'test' [HIGH]
[!] KRNL-6000: Kernel out of date (5.15.0-76 → 5.15.0-78) [MEDIUM]
```

Recomendaciones aplicadas:

```
sudo chage -M 90 test # Establecer expiración de contraseña
sudo apt install linux-image-generic # Actualizar kernel
```

3. Respaldo y Recuperación

3.1 Flujo de Trabajo con Timeshift

1. Creación de snapshot:

```
sudo timeshift --create --comments "Backup Laboratorio 4"
```

- **Tamaño:** 45.2 GB
- **Almacenamiento:** /dev/sda1 (EXT4)

2. Simulación de desastre:

```
rm -rf /home/usuario/proyectos/ # Eliminación accidental
```

3. Restauración (captura 4):


```
sudo timeshift --restore
```

- **Resultados:**
 - Tiempo: 12 minutos 18 segundos
 - Archivos recuperados: 100%

4. Lista de Verificación de Seguridad

4.1 Estado Actual del Sistema

Área	Cumple	Observaciones
Firewall activo	✓	Reglas: DENY 192.168.1.100, ALLOW 22/TCP
Actualizaciones	✗	15 paquetes pendientes (incl. kernel)

Área	Cumple	Observaciones
Respaldos automáticos		Timeshift configurado diariamente

4.2 Recomendaciones Prioritarias

1. Actualizar sistema:

```
sudo apt update && sudo apt upgrade -y
```

2. Configurar políticas de contraseña

```
sudo nano /etc/login.defs # Modificar PASS_MAX_DAYS=90
```

Anexos

A.1 Comandos Clave Ejecutados

```
# Auditoria
sudo auditctl -l
sudo aureport -au --failed

# Firewall
sudo ufw deny from 192.168.1.100

# Respallos
sudo timeshift --create --comments "Backup Laboratorio 4"
```

A.2 Capturas de Pantalla

- **Captura 1:** Configuración de auditd (auditctl -l).
- **Captura 2:** Logs de eventos de seguridad (aureport).
- **Captura 3:** Resultados de Lynis.
- **Captura 4:** Restauración con Timeshift.

Conclusión

El análisis reveló:

1. **3 vulnerabilidades críticas:**
 - Kernel desactualizado.
 - Ausencia de expiración de contraseñas.

- Servicios innecesarios activos (bluetooth).

2. Efectividad de las contramedidas:

- Bloqueo de IPs malintencionadas mediante UFW.
- Recuperación exitosa de datos con Timeshift.

Recomendaciones finales:

- Automatizar auditorías mensuales con lynis.
- Implementar unattended-upgrades para actualizaciones de seguridad.

Anexo Grafico

- https://github.com/ritchi25/Laboratorio_SO_Ricardo-Paredes.git
- <https://drive.google.com/drive/my-drive>