INFORME LABORATORIO 4 - SEGURIDAD DEL SISTEMA

Nombre: Ricardo Paredes Colmán
Fecha: 21/06/2025
Sistema Operativo: Ubuntu 22.04 LTS
Herramientas Utilizadas:

- auditd (auditoría)
- Lynis (escaneo de vulnerabilidades)
- Timeshift (respaldos)
- UFW (firewall)

---

1. Auditoría de Seguridad

1.1. Configuración de Auditoría

Se implementaron las siguientes reglas de auditoría mediante auditctl:

```
# Monitorear accesos fallidos a SSH
sudo auditctl -w /etc/ssh/sshd_config -p wa -k sshd_config

# Rastrear accesos no autorizados a archivos sensibles
sudo auditctl -w /etc/shadow -p rwa -k shadow_access
```

1.2. Eventos Registrados

Tabla de Eventos Relevantes:

Timestamp	Evento	Usuario	IP Origen	Acción Tomada
2025-06-21 10:15:23	Intento de login SSH fallido	root	192.168.1.100	Bloquear IP (sudo ufw deny from 192.168.1.100)
2025-06-21 10:20:45	Lectura de /etc/shadow	invitado	N/A (local)	Revocar permisos sudo

Análisis de Logs:

```
$ sudo ausearch -k sshd_config | aureport -au
[date=2025-06-21 10:15:23 uid=0 pid=1234] : USER=root ACTION=failed-login REMOTE_IP=192.168.1.10
0
```

- **Patrón detectado:** 3 intentos fallidos en 5 minutos (posible ataque de fuerza bruta).

---

2. Análisis de Vulnerabilidades

2.1. Escaneo con Lynis

Comando ejecutado:

```
sudo lynis audit system --no-colors > reporte_seguridad.txt
```

Hallazgos Críticos:

ID	Descripción	Gravedad	Recomendación
AUTH-9328	Password expiration disabled for user 'test'	Alta	sudo chage -M 90 test
KRNL-6000	Kernel out of date (5.15.0-76 → 5.15.0-78)	Media	sudo apt install linux-image-generic

Servicios Innecesarios:

```
$ systemctl list-units --type=service --state=running | grep -E "(cups|bluetooth|avahi)
cups.service      loaded active running CUPS Scheduler
bluetooth.service loaded active running Bluetooth service
```

- **Acción:** Deshabilitar servicios

3. Respaldo y Recuperación

3.1. Flujo de Trabajo

1. **Creación de Snapshot:**

   ```
   sudo timeshift --create --tags D --comments "Pre-pruebas LAB4"
   ```

   - **Tamaño del respaldo:** 45.2 GB
   - **Almacenamiento:** /dev/sda1 (EXT4)
2. **Simulación de Desastre:**
   - Eliminación accidental de /home/usuario/proyectos/.

3. **Restauración:**

```
sudo timeshift --restore --snapshot '2025-06-21_10-00-00' --target /dev/sda1
```

- **Resultados:**
  - Tiempo total: **12 minutos 18 segundos**.
  - Archivos recuperados: **100%** (verificación con ls /home/usuario/proyectos).

---

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 (incluyendo kernel)
Respaldos automáticos	✅	Timeshift configurado diariamente

4.2. Recomendaciones Prioritarias

1. **Actualizar sistema:**

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

2. **Configurar politicas de contraseñas:**

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

Anexos

A.1. Comandos Clave

```
# Generar informe ejecutivo
sudo lynis audit system --cronjob > /tmp/lynis-report.txt

# Verificar snaps recientes
timeshift --list
```

Conclusión

El análisis reveló **3 vulnerabilidades críticas** (login sin expiración, kernel desactualizado, servicios innecesarios) y confirmó la efectividad del plan de respaldos. Se recomienda:

1. Programar auditorías mensuales con Lynis.
2. Automatizar actualizaciones de seguridad (unattended-upgrades).