

# TRABAJO PRÁCTICO INTEGRADOR

## Escaneo de Vulnerabilidades en Sistemas

**Materia:** Arquitectura y Sistemas Operativos

**Profesor/a:** Diego Lobos

**Alumnos/as:** Chiappone Michael  
Campana Jonatan

**Fecha de entrega:** 05/06/25

## INDICE

- 1. Introducción**
- 2. Marco Teórico**
- 3. Caso Práctico**
- 4. Metodología Utilizada**
- 5. Resultados Obtenidos**
- 6. Conclusiones**
- 7. Bibliografía**
- 8. Anexos**

## 1. Introducción

La seguridad en los sistemas operativos es clave para prevenir vulnerabilidades que pueden ser explotadas por atacantes.

Este trabajo tiene como enfoque el escaneo de vulnerabilidades utilizando herramientas especializadas como Lynis, con el objetivo de identificar debilidades del sistema y tomar conciencia sobre la importancia del monitoreo constante en la protección de la infraestructura informática.

## 2. Marco Teórico

El escaneo de vulnerabilidades es una técnica utilizada para detectar fallos de seguridad potenciales en un sistema.

Herramientas como Lynis permiten realizar auditorías de seguridad, revisando configuraciones, permisos, servicios activos, y otros aspectos del sistema.

Entre los conceptos clave se encuentran:

- Seguridad proactiva vs. reactiva
- Auditoría del sistema: revisión de logs, configuraciones y permisos
- Herramientas de escaneo: Lynis, ClamAV, Rkhunter
- Principios de hardening: reducción de superficie de ataque, cierre de servicios innecesarios
- Reportes de seguridad: interpretación de hallazgos y recomendaciones

## 3. Caso Práctico

Se instaló la herramienta Lynis en un entorno Ubuntu y se ejecutó un escaneo completo del sistema.

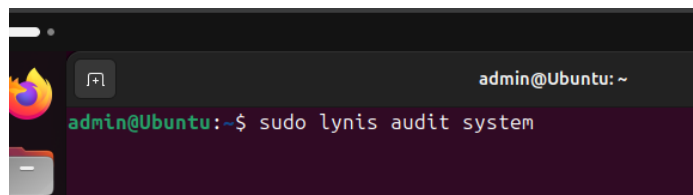
El comando principal utilizado fue:

```
sudo lynis audit system
```

El análisis arrojó un informe detallado con advertencias (WARN), sugerencias (SUGGESTION) y un puntaje de seguridad general. Se identificaron configuraciones débiles, servicios innecesarios activos, y ausencia de algunas prácticas recomendadas de seguridad.

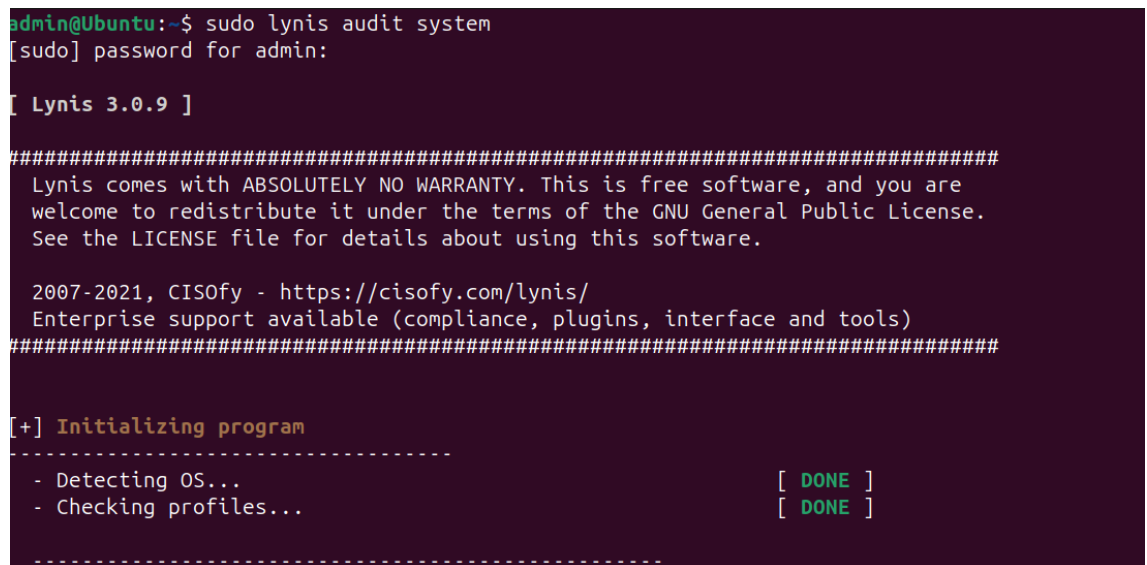
#### 4. Metodología Utilizada

- Investigación de herramientas de escaneo disponibles en sistemas Linux.
- Instalación de Lynis desde repositorios oficiales.



```
admin@Ubuntu: ~  
admin@Ubuntu:~$ sudo lynis audit system
```

- Ejecución del comando de auditoría general.



```
admin@Ubuntu:~$ sudo lynis audit system  
[sudo] password for admin:  
  
[ Lynis 3.0.9 ]  
  
#####  
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are  
welcome to redistribute it under the terms of the GNU General Public License.  
See the LICENSE file for details about using this software.  
  
2007-2021, CISOfy - https://cisofy.com/lynis/  
Enterprise support available (compliance, plugins, interface and tools)  
#####  
  
[+] Initializing program  
-----  
- Detecting OS... [ DONE ]  
- Checking profiles... [ DONE ]  
-----
```

- Análisis e interpretación de resultados.

- Captura de pantalla del informe generado.

```
Lynis security scan details:

Hardening index : 59 [#####          ]
Tests performed : 255
Plugins enabled : 1

Components:
- Firewall           [V]
- Malware scanner    [X]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status [?]
- Security audit    [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data                : /var/log/lynis-report.dat
```

- Reparto de tareas: Chiappone Michael se encargó del entorno y pruebas, Campana Jonatan redactó el informe y armó el video.

## 5. Resultados Obtenidos

- Se generó un informe de auditoría detallado.
- Se detectaron vulnerabilidades comunes como servicios innecesarios activos o configuraciones por defecto.
- El sistema recibió un puntaje de seguridad intermedio (dependiendo del estado del entorno).
- Se entendió la importancia de revisar regularmente la seguridad del sistema operativo incluso si no se detectan incidentes visibles.

## 6. Conclusiones

El escaneo de vulnerabilidades es una práctica fundamental para la administración segura de sistemas operativos.

Herramientas como Lynis permiten anticipar problemas antes de que ocurran, mejorando la postura de seguridad de un sistema.

Este trabajo permitió explorar una técnica real utilizada por profesionales, reforzando la importancia de auditar sistemas de forma regular.

## 7. Bibliografía

- Center for Internet Security. (s. f.). CIS Controls.  
<https://www.cisecurity.org/controls/>
- Arch Linux. (2025, mayo). Lynis - ArchWiki.  
<https://wiki.archlinux.org/title/Lynis>
- CISOfy. (s. f.). Lynis [Repositorio GitHub].  
<https://github.com/CISOfy/lynis>
- Canonical. (s. f.). Ubuntu server - Security.  
<https://ubuntu.com/server/docs/security>
- man lynis. (2025, mayo). Página de manual consultada desde la terminal de Linux.

## 8. Anexos

- Capturas de pantalla del informe de Lynis
- Fragmento del log generado (/var/log/lynis.log)
- Enlace al video explicativo: <https://youtu.be/VdU9cLnqW0>
- Enlace repositorio en GitHub con todo el contenido:  
[https://github.com/CampanaJ/proyect\\_integrador-AySO](https://github.com/CampanaJ/proyect_integrador-AySO)