

**Universidad de Sevilla**

**Grado en Ingeniería Informática – Ingeniería de Computadores**

**Seguridad en Sistemas Informáticos y en Internet**

**PRÁCTICA 3**

**Grupo 2**

**Alumnos: Silvia Castillo Ruiz, Amara Innocent Millán y Víctor Ramos Lara**

## Índice

[1. Resumen Ejecutivo 3](#_Toc212717806)

[2.1 Arquitectura 3](#_Toc212717807)

[2.2 Decisiones 3](#_Toc212717808)

[3. Pruebas 4](#_Toc212717809)

[3.1 Auditoría de Seguridad de Enpoints 4](#_Toc212717810)

[3.1.1 Análisis de un ordenador de sobremesa o portátil 4](#_Toc212717811)

[3.1.2 Análisis de un sistema móvil 5](#_Toc212717812)

[3.2 Auditoría de vulnerabilidades en aplicaciones Web 9](#_Toc212717813)

[4. Conclusiones 9](#_Toc212717814)

[5. Referencias 9](#_Toc212717815)

# Resumen Ejecutivo

El proyecto VULNAWEB tiene como finalidad realizar una auditoría de seguridad integral sobre los sistemas informáticos y las aplicaciones web de una empresa de comercio electrónico, con el objetivo de identificar vulnerabilidades y fortalecer su infraestructura tecnológica. La auditoría aborda tanto los endpoints como las aplicaciones web que soportan los servicios de la organización.

En la primera fase, se efectúan auditorías de sistemas utilizando herramientas como Lynis (para equipos Linux) y CONAN Mobile o Malwarebytes (para dispositivos Android), con el fin de calcular el hardening index y aplicar medidas de seguridad que permitan alcanzar los valores exigidos por la política corporativa. En la segunda fase, se lleva a cabo una auditoría de vulnerabilidades web mediante OWASP ZAP, analizando peticiones y respuestas HTTP/HTTPS y probando fallos de seguridad como inyecciones SQL, Cross-Site Scripting (XSS) o Path Traversal en entornos de prueba controlados.

El proyecto refuerza competencias prácticas en ciberseguridad ofensiva y defensiva, auditoría técnica, y el uso ético de herramientas de análisis de vulnerabilidades, aportando experiencia real en la protección de sistemas y aplicaciones web frente a amenazas modernas.

1. **Core**

## Arquitectura

La arquitectura del proyecto VULNAWEB integra los principales elementos informáticos de la empresa: equipos de sobremesa y portátiles con Kali Linux, dispositivos móviles Android y servidores web Apache. La auditoría se divide en dos fases; primero se verifica la seguridad y el nivel de hardening de todos los endpoints Linux y móviles mediante Lynis y CONAN Mobile/Malwarebytes; en la segunda fase, se analiza la seguridad de las aplicaciones web con OWASP ZAP, revisando las comunicaciones y detectando posibles vulnerabilidades en entornos de prueba controlados. Este enfoque modular permite auditar la infraestructura tecnológica clave de la organización y aplicar mejoras específicas en cada ámbito.

## Decisiones

Las decisiones tomadas en el desarrollo del proyecto VULNAWEB se sustentan en criterios de eficiencia, seguridad y alineación con las mejores prácticas del sector. En primer lugar, la elección de Lynis para la auditoría de sistemas Linux responde a su capacidad de realizar análisis detallados de configuración, cumplimiento de estándares y detección de errores, lo que facilita un diagnóstico integral y la implementación de medidas de mejora que eleven el Hardening Index del sistema según los requisitos de la política corporativa. Para los dispositivos móviles Android, la decisión de emplear CONAN Mobile y Malwarebytes se fundamenta en su enfoque especializado para la detección de configuraciones inseguras, aplicaciones maliciosas y problemas de permisos, permitiendo una recuperación y fortalecimiento efectivo de los activos móviles.

La fase dirigida a las aplicaciones web adopta OWASP ZAP como herramienta principal, lo que se justifica por su amplia aceptación en el ámbito de pruebas DAST y por la capacidad de interceptar y analizar peticiones y respuestas HTTP/HTTPS en profundidad. Esta aproximación permite identificar una amplia gama de vulnerabilidades, como inyecciones SQL, XSS y Path Traversal, posibilitando la aplicación de medidas concretas y traqueables según las advertencias y recomendaciones captadas por la herramienta.

Asimismo, todas las auditorías y pruebas de penetración se realizan en entornos de prueba controlados, con el objetivo de minimizar cualquier riesgo sobre los sistemas en producción y garantizar un ejercicio seguro, ético y conforme a la normativa vigente. La documentación exhaustiva de cada acción permite justificar la selección de herramientas, las configuraciones aplicadas y las medidas de mitigación adoptadas, facilitando la trazabilidad y el cumplimiento de los estándares profesionales que exige una auditoría técnica en ciberseguridad. Este enfoque integral asegura que las decisiones aportan coherencia y robustez al ciclo de mejora continua de la seguridad en la empresa auditada.

# Pruebas

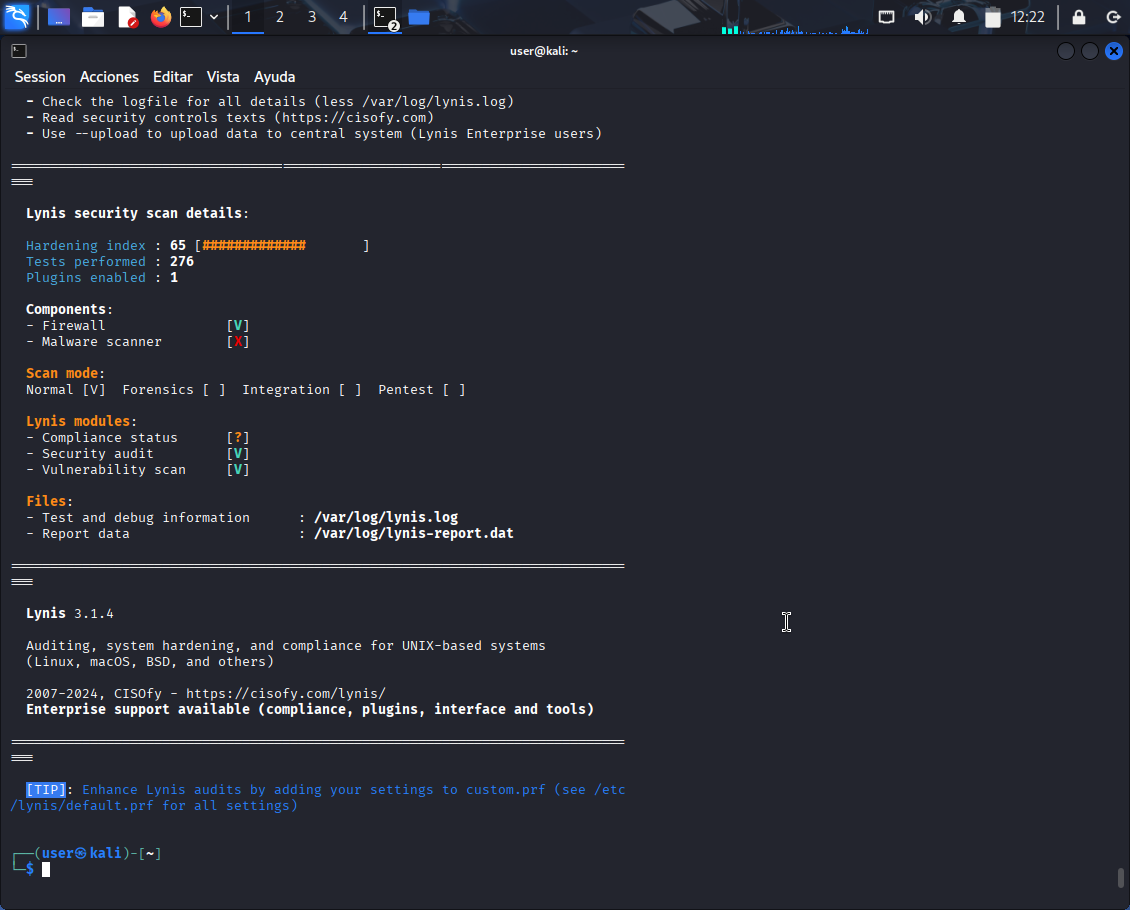
### **Auditoría de Seguridad de Enpoints**

### **Análisis de un equipo de sobremesa o portátil**

El análisis de los equipos de sobremesa constituye una fase esencial del proyecto, orientada a evaluar la robustez y el nivel de hardening de los sistemas operativos Linux empleados en la organización, en particular los basados en Kali Linux.

Para ello, se utilizó la herramienta Lynis, incluida en Kali Linux y reconocida por su capacidad de realizar auditorías exhaustivas de seguridad y cumplimiento en sistemas Linux. Esta combinación permite abordar el análisis desde una perspectiva técnica avanzada, aprovechando las funcionalidades y actualizaciones constantes que Kali Linux ofrece para fortalecer la seguridad de las estaciones de trabajo.

En primer lugar, se realizó una auditoría rápida utilizando Lynis, la cual arrojó un Hardening Index inicial de 65 tras la ejecución de 276 pruebas de control. Este resultado permitió identificar configuraciones mejorables y áreas en las que el sistema presentaba cierto margen de riesgo:



A continuación, se aplicaron una serie de mejoras y endurecimientos en el sistema, ajustando configuraciones, instalando utilidades recomendadas y revisando parámetros relevantes según las sugerencias de la herramienta. Posteriormente, se llevó a cabo una auditoría completa, obteniendo un Hardening Index elevado de 73 con la ejecución de 277 pruebas. Esto refleja un avance significativo en la robustez del sistema y evidencia la efectividad de las acciones correctivas implementadas:

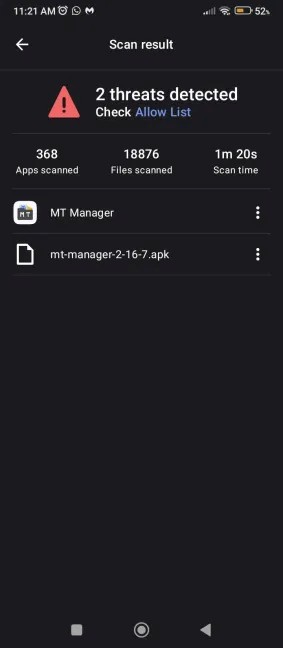


### **Análisis de un sistema móvil**

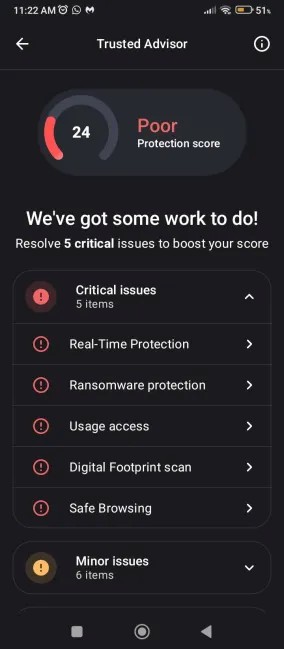
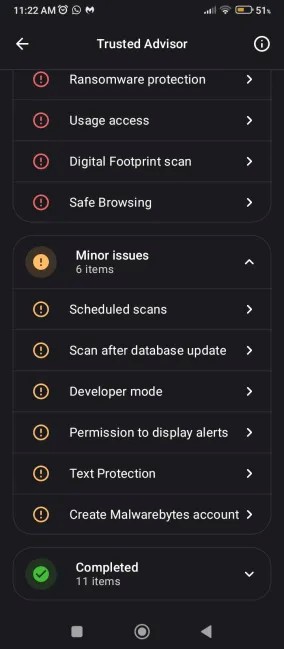
El análisis de dispositivos móviles en este proyecto se centra en evaluar la seguridad del entorno Android utilizado dentro de la empresa, con el propósito de identificar configuraciones vulnerables, aplicaciones potencialmente peligrosas y configuraciones de permisos que puedan comprometer la integridad y confidencialidad de la información.

Para ello, se utilizó la herramienta CONAN Mobile, específicamente diseñada para la detección de amenazas, análisis de configuración y evaluación del cumplimiento de políticas de seguridad en entornos móviles. El análisis se llevó a cabo sobre un dispositivo Xiaomi Redmi 10C que presentaba esta puntuación inicial de seguridad.

Tras realizar un escaneo encontró 2 archivos/aplicaciones peligrosas en el dispositivo, debido a presentar código malintencionado al haber sido descargado de una fuente no fiable.

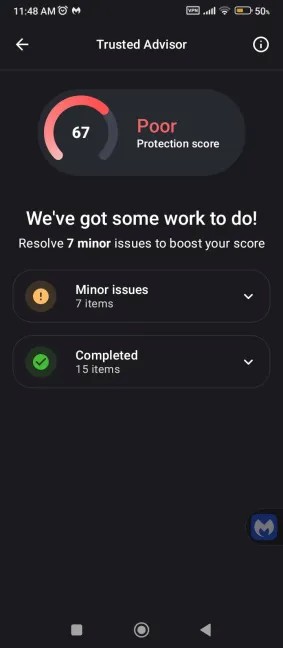


Tras el escaneo, pasamos al apartado de "Mejorar mi puntuación", donde podemos ver las distintas soluciones propuestas:

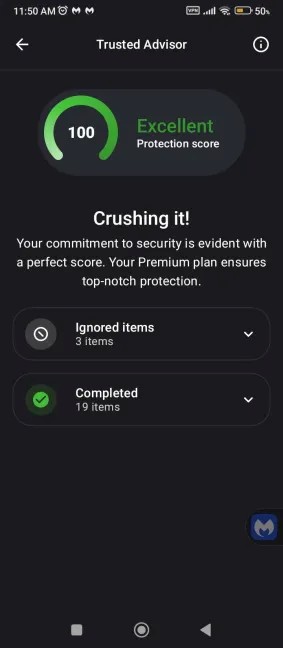
  

Estas soluciones principalmente son funciones en tiempo real dadas por la propia aplicación para tener un control de toda la información que llega al dispositivo, hacer uso de una VPN que nos proporciona la misma, algunos cambios de configuración para aumentar la seguridad, como deshabilitar el modo desarrollador, y escaneo de páginas web para darnos un índice de peligro.

Tras solucionar los problemas criticos nuestra puntuación aumenta en 40 puntos, acercándonos más a nuestra meta:



Al añadir solución a los problemas menores alcanzamos la puntuación máxima de seguridad:



### **Auditoría de vulnerabilidades en aplicaciones Web**

# Conclusiones

# Referencias