PROPUESTA TFG MARIO A. 2DAM

masenper@myuax.com

Fecha: 9 de Febrero 2026

Plataforma de Pre-Explotación y Análisis Ofensivo de Binarios

Enfoque del producto:

El producto se centra en la fase de pre-explotación dentro de una auditoría ofensiva, entendida como el proceso de análisis previo a cualquier intento de explotación, cuyo objetivo es identificar, estructurar y priorizar la superficie de ataque de un binario ejecutable.

La plataforma no incluye funcionalidades de explotación automática, persistencia ni post-explotación, manteniendo un enfoque ético y profesional orientado a la evaluación y análisis de seguridad.

Descripción general:

Se propone el desarrollo de una plataforma software capaz de analizar binarios ejecutables (inicialmente ELF sobre Linux) mediante la combinación de:

1. Análisis estático, sin ejecución del binario, para extraer información estructural y de mitigaciones de seguridad.
2. Análisis dinámico controlado, ejecutando el binario en un entorno monitorizado para observar su comportamiento real.
3. Correlación de evidencias y sistema de puntuación, que permita priorizar hallazgos dfesde un punto de vista ofensivo.
4. Generación de informes estructurados, orientados a facilitar la revisión técnica posterior.

La solución se diseña como un producto real, multiusuario, extensible y preparado para escalar, separando claramente la interfaz de usuario, la lógica de negocio y los componentes de análisis.

Problema real que resuelve:

En auditorías ofensivas reales, la fase inicial de análisis suele realizarse mediante el uso de herramientas independientes (por ejemplo strings, checksec, ldd, strace), lo que produce:

- Resultados dispersos y difíciles de correlacionar.
- Falta de trazabilidad sobre quién realizo el análisis y cuándo.
- Ausencia de priorización clara de riesgos.
- Dependencia excesiva del criterio manual del auditor.

La plataforma propuesta centraliza este proceso, proporcionando:

- Un análisis inicial estructurado y reproducible.
- Priorización automática de hallazgos.
- Trazabilidad completa de las acciones realizadas.
- Informes consistentes y reutilizables.

Objetivo General:

Diseñar e implementar una plataforma modular para la fase de pre-explotación, capaz de realizar análisis estático y dinámico de binarios ejecutables, correlacionar los resultados obtenidos y generar informes con priorización de riesgos orientados a auditorías ofensivas.

Alcance:

MVP:

- Soporte completo para binarios ELF en Linux.
- Análisis estático y dinámico.
- Sistema de puntuación básico justificable.
- Interfaz web con visualización por pestañas y filtros.
- Autenticación de usuarios y auditoría de acciones.
- Persistencia de resultados e informes.

Alcance opcional:

- Análisis estático de binarios PE.
- Políticas de sandboxing avanzadas.
- Escalado de análisis mediante workers distribuidos.

Arquitectura y Tecnologías:

Backend:

- Java + Spring Boot
- Arquitectura Hexagonal
- API Rest
- Autenticación y autorización mediante JWT.
- Auditoría de acciones (append-only)

Frontend:

- Aplicación web (SPA)
- Comunicación con backend mediante HTTPS
- Visualización avanzada de resultados (tabs, filtros, dashboards)

Análisis:

- Python: ejecución de pipelines de análisis, correlación y scoring.
- C: agente de análisis dinámico basado en ptrace y/o seccomp.

Persistencia:

- PostgreSQL
- Uso de JSONB para resultados de análisis
- Modelo relacional para usuarios, auditoría y metadatos.

Capa Ética:

La plataforma se limita a tareas de análisis y evaluación de seguridad, excluyendo explícitamente cualquier funcionalidad orientada a explotación automática o persistencia. Su diseño y uso están orientados a entornos controlados de auditoría y laboratorio.

Atentamente,

Mario Asenjo