Solicitud Beca ciberseguridad

Asier Muñoz Villanueva

Desarrollo de una herramienta automatizada de análisis de vulnerabilidades para PYMES y estudiantes con generación de informes asistida por inteligencia artificial.

26 de Junio de 2025

Universidad Pública de Navarra

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

ÍNDICE

Resumen y objetivos

Resumen

El proyecto consiste en el desarrollo de una herramienta de escaneo de vulnerabilidades orientada a pequeñas y medianas empresas (PYMES) y estudiantes, con el objetivo de permitirles realizar auditorías básicas de seguridad de forma autónoma.
Esta herramienta integrará diferentes motores de escaneo ampliamente utilizados (GoBuster, Wfuzz, Nikto, OpenVAS, Nessus, Metasploit, entre otros) y contará con un sistema de detección de versiones de servicios y tecnologías utilizadas en aplicaciones web, servidores y sistemas expuestos.
Posteriormente, realizará una consulta a una inteligencia artificial externa (mediante API) que analizará los resultados del escaneo, ayudará a priorizar las vulnerabilidades según su criticidad y generará un informe tanto técnico como ejecutivo.
De esta forma, la herramienta ofrecerá una solución asequible y automatizada para mejorar la seguridad de las pequeñas empresas, facilitando la detección temprana de fallos y mitigación de riesgos.

Objetivos

- Desarrollar una herramienta de escaneo de vulnerabilidades fácil de usar para PYMES y estudiantes.
- Integrar y automatizar herramientas de escaneo como GoBuster, Wfuzz, Nikto, OpenVAS, Nessus, Metasploit y otras.
- Detectar versiones de servicios, CMS y tecnologías, y consultar bases de datos públicas de vulnerabilidades (CVE, NVD, ExploitDB...).
- Implementar un módulo de integración con una inteligencia artificial externa a través de API, para que esta analice los resultados y ayude a priorizar los hallazgos.
- Generar informes automáticos que incluyan la descripción de las vulnerabilidades, su nivel de criticidad y recomendaciones para su mitigación.
- Diseñar la herramienta de manera modular para facilitar futuras mejoras, como añadir nuevas técnicas de escaneo o bases de datos de vulnerabilidades.

Metodología y planificación

Se plantea dividir el proyecto tanto en fases y en meses, teniendo en cuenta que la duración del proyecto será de 5 meses.

Fases

- **Fase 1:** Análisis y selección de las mejores herramientas de escaneo.
- **Fase 2:** Desarrollo de un sistema que permita ejecutar de manera centralizada estas herramientas y recoger sus resultados en un formato unificado (JSON o CSV).
- **Fase 3:** Implementación de un módulo de fingerprinting para identificar tecnologías, versiones y servicios activos.
- **Fase 4:** Creación de un sistema que consulte bases de datos públicas (CVE, NVD, ExploitDB, Vulners API) para mapear versiones con vulnerabilidades conocidas.
- **Fase 5:** Integración con modelos de inteligencia artificial mediante API (como OpenAI o similares), para que la IA: Analice los resultados, clasifique las vulnerabilidades según su criticidad y genere explicaciones y recomendaciones en lenguaje natural.
- **Fase 6:** Desarrollo del generador de informes automáticos en formatos PDF y HTML, con un resumen ejecutivo y un apartado técnico detallado.
- **Fase 7:** Pruebas, validación en entornos controlados y ajustes finales.

Meses

Mes	Actividades principales
Mes 1	Análisis de requisitos, diseño de la herramienta y planificación. Preparación de máquinas vulnerables para pruebas.
Mes 2	Desarrollo del motor de escaneo e integración de herramientas. Implementación del sistema de detección de servicios y versiones.
Mes 3	Desarrollo del módulo de consulta a bases de datos de vulnerabilidades. Integración de la IA para análisis y priorización. Despliegue de máquinas vulnerables avanzadas.
Mes 4	Desarrollo del generador de informes automáticos. Pruebas completas del sistema sobre los entornos vulnerables. Ajustes y mejoras.
Mes 5	Validación final, documentación, generación de la memoria y preparación de la presentación del proyecto.

Herramientas y resultados

Herramientas a utilizar

Lenguajes: Python (principalmente), Bash, y posiblemente Go o Rust para partes específicas donde se requiera mayor rendimiento.

Herramientas de escaneo: GoBuster, Wfuzz, Nikto, OpenVAS, Nessus, Metasploit y herramientas de Sectools seleccionadas.

Detección de versiones: Servicios como WhatWeb, Nmap (con scripts NSE), y fingerprinting personalizado.

Bases de datos de vulnerabilidades: CVE, NVD, Vulners API, ExploitDB, entre otras.

IA externa vía API: OpenAI (ChatGPT), Azure OpenAI o equivalentes, para realizar análisis del riesgo y generación automática de texto.

Generación de informes: Librerías como ReportLab, WeasyPrint o generación de HTML con posterior conversión a PDF.

Resultados esperados

Se desarrollará una herramienta orientada a PYMES y entornos educativos, capaz de realizar análisis de seguridad de forma automatizada. Permitirá identificar servicios, versiones y vulnerabilidades mediante la integración de motores de escaneo y consultas a bases de datos como CVE.

El sistema generará informes con dos niveles: un **informe ejecutivo**, para perfiles no técnicos, que resumirá los riesgos principales; y un **informe técnico**, con detalle de vulnerabilidades, servicios afectados, nivel de criticidad, evidencias y recomendaciones.

La herramienta estará diseñada con una arquitectura modular, facilitando su futura ampliación y la incorporación de nuevos motores o mejoras. La validación se realizará mediante entornos controlados con máquinas vulnerables para comprobar su capacidad de detección y precisión.

Impacto del proyecto

Este proyecto está orientado tanto a mejorar la seguridad de pequeñas y medianas empresas, que con frecuencia carecen de recursos para contratar auditorías profesionales o servicios de pentesting, como a servir como herramienta formativa para estudiantes interesados en iniciarse en el ámbito del pentesting y la ciberseguridad. Al ofrecer una solución automatizada y asistida por inteligencia artificial, se contribuye a democratizar el acceso a la ciberseguridad, permitiendo a las PYMES identificar y mitigar vulnerabilidades antes de que puedan ser explotadas.

Adicionalmente, el proyecto tiene un impacto académico significativo, ya que permite aplicar de forma práctica conocimientos en ciberseguridad, automatización, análisis de datos y uso responsable de inteligencia artificial, consolidando mi formación técnica y profesional de cara a mi futura trayectoria en el sector.