**Guía3. Informe final Proyecto APT**

**Asignatura Capstone**

|  |
| --- |
| **1. Informe final Proyecto APT** |
| El objetivo de este informe es que describas los aspectos más relevantes de tu Proyecto APT. Es importante que fundamentes las decisiones que tuviste que tomar a lo largo del proceso.  A continuación, encontrarás distintos campos que deberás completar con la información solicitada, los que dan cuenta del resumen de tu proyecto APT y sus principales resultados. |

|  |  |
| --- | --- |
| Nombre del proyecto | ***RobotPentester*** |
| Área (s) de desempeño(s) | *Ciberseguridad, control de calidad y automatizaciones de procesos.* |
| Competencias | *Análisis y planificación de requerimientos informáticos, calidad de software, gestión de proyectos informaticos, programacion de software, arquitectura de software* |

|  |  |
| --- | --- |
| **Contenidos del informe final** | |
| 1. Relevancia del proyecto APT | *Problema abordado: RobotPentester busca optimizar la ciberseguridad en el desarrollo de software, detectando y mitigando vulnerabilidades antes de que el software entre en producción. Esto es esencial en el campo de la ciberseguridad, donde los ataques y las amenazas se vuelven cada vez más sofisticados.*  *Relevancia para el campo laboral: La ciberseguridad es crítica en cualquier industria que dependa de sistemas de información. Este proyecto tiene especial importancia en el desarrollo de software, ya que garantiza una protección proactiva y minimiza el riesgo de ataques en los sistemas.*  *Este proyecto se implementa con un enfoque general que puede aplicarse a empresas de desarrollo de software en Chile, especialmente aquellas que manejan datos sensibles o tienen una amplia base de usuarios, a lo cual, RobotPentester beneficiará tanto a los equipos de desarrollo de software como a los usuarios finales, ya que garantiza aplicaciones más seguras y confiables.*  *Nuestro aparto de valor con RobotPentester es una herramienta que proporciona una evaluación continua, genera informes detallados y permite actuar rápidamente en la corrección de fallas, lo que reduce costos y tiempos de respuesta.* |
| 2. Objetivos | *Desarrollar una herramienta automatizada que detecte y mitigue riesgos en el desarrollo de software, optimizando tiempos y costos, y asegurando la calidad mediante la identificación temprana de vulnerabilidades en flujos web.*  *Objetivos específicos:*  *Implementar un sistema de pruebas de seguridad automatizadas que permita la evaluación continua de vulnerabilidades en frontend y backend.*  *Integrar herramientas de ciberseguridad como OWASP ZAP y Metasploit para mejorar la detección y mitigación de fallos en el software.*  *Desarrollar scripts personalizados en JMeter para analizar y simular diferentes escenarios de seguridad en aplicaciones web.*  *Generar informes detallados que proporcionen recomendaciones accionables para la corrección de vulnerabilidades detectadas.* |
| 3. Metodología | *Se utilizó la metodología cascada, que asegura un avance estructurado y una documentación exhaustiva, esenciales en proyectos de ciberseguridad.*  *Las fases y procedimientos empleadas con esta metodología fueron las siguientes:*   * *Análisis de requerimientos: Identificación de las necesidades de seguridad.* * *Diseño de arquitectura: Configuración de una estructura en Docker que permite ejecutar herramientas como JMeter y OWASP ZAP.* * *Implementación de pruebas: Uso de JMeter para pruebas de carga, con OWASP ZAP interceptando el tráfico y ejecutando análisis de seguridad.* * *Generación de informes: Producción de un informe en HTML que detalla vulnerabilidades encontradas.*   *La metodología fue escogida ya que nos permite una ejecución ordenada y sistemática, cumpliendo los objetivos de identificar y corregir vulnerabilidades en un entorno controlado y replicable.* |
| 4. Desarrollo | *Las etapas con las que abordamos el proyecto fueron tapas:*   * *Análisis de requerimientos.* * *Configuración de contenedores Docker.* * *Pruebas de rendimiento y carga.* * *Escaneo de vulnerabilidades y análisis de tráfico.* * *Generación de informes y recomendaciones.* * *Documentar el proyecto (La cual fue llevada a través de todo el proceso)*   *Lo que nos facilitó el proyecto fue el acceso a herramientas de código abierto y la estructura clara de las fases.*  *Y una dificultad que tuvimos que llevar a cabo fue La complejidad de integrar múltiples herramientas en Docker y asegurar la compatibilidad entre ellas.* |
| 5. Evidencias | *Se mostraran una serie de imágenes en la cual mostraremos como íbamos aprendiendo y ejecutando el desarrollo del proyecto en el cual, mostramos como íbamos usando las herramientas para aprender y ejecutar el proyecto.*  *Por temas de privacidad no podemos poner el código completo o un esquema general de nuestro git o proyecto.*  *Pruebas de JMeter a una página de la achs, por temas de seguridad y datos no se puede mostrar el resultado.*  *A screenshot of a computer  Description automatically generated*  *Levantamiento del robot pentester, el cual ejecuta un Docker compose, en el cual se generan todas las imágenes creadas con Docker y sus configuraciones para que le robot pueda ser utilizado a posterior.*  *A screenshot of a computer  Description automatically generated*  *Resultado de las imágenes levantadas*  *A screenshot of a computer  Description automatically generated* |
| 6. Intereses y proyecciones profesionales | *RobotPentester refuerza nuestros intereses en la automatización de pruebas de seguridad y el desarrollo de soluciones*  *Después de este proyecto, nos interesa explorar más sobre la integración de herramientas de ciberseguridad y optimizar procesos de auditoría en entornos corporativos.* |