**ANTEPROYECTO DEL**

**TRABAJO DE FIN DE GRADO**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **INFORMACIÓN GENERAL** | | | | | |
| **Alumno/a** | Álvaro Valencia Villalón | | | | |
| **Titulación:** | Graduado en Ingeniería del Software | | | | |
| **Tutor/es:** | Gabriel Jesús Luque Polo | | | | |
| **Título** | ***SecurAI: Una aplicación inteligente para la detección de ataques en tu red*** | | | | |
| **Subtítulo** *(solo si en grupo)* |  | | | | |
| **Título en inglés** | ***SecurAI: A smart app to detect attacks on your network*** | | | | |
| **Subtítulo en inglés** *(solo si en grupo)* |  | | | | |
| **Trabajo en grupo:** | **Sí** |  | **No** | X |  |
| **Otros integrantes del grupo:** |  | | | | |

|  |
| --- |
| **INTRODUCCIÓN** |
| *Contextualización del problema a resolver. Describir claramente de dónde surge la necesidad de este TFG y el dominio de aplicación. En caso de que el TFG se base en trabajos previos, debe aclararse cuáles son las aportaciones del TFG.* |
| Es poco común que los hogares o pequeñas empresas tengan una protección avanzada de sus redes. No es trivial el uso de herramientas IDS/IPS (Sistema de Detección/Prevención de Intrusos) y requieren de un conocimiento avanzado para su instalación y utilización. En un contexto social en el que los sistemas informáticos cada vez son más frecuentes y manejan información cada vez más importante, es crucial tener un escudo ante, por lo menos, los ataques más comunes que podemos recibir.  Destacar también que la complejidad de los ataques cibernéticos está en claro aumento, por lo que las técnicas de protección y prevención que hasta ahora han funcionado están en camino de ser ineficaces, por eso es muy importante mantener el desarrollo de tecnologías punteras, accesibles y al nivel de los atacantes, para garantizar que la infraestructura digital de nuestro hogar o negocio no se verá comprometida.  La tecnología de detección o prevención de intrusos no es nueva. Un ejemplo de las plataformas ya existentes es Suricata [1], un proyecto open source que basa su funcionamiento en la definición de reglas que detecten y/o frenen ciertos tipos de ataques. Aun siendo una herramienta extremadamente potente, sus usuarios se quejan de la complejidad que supone su uso ya que por ejemplo no posee interfaz gráfica oficial [2], lo cual aleja esta herramienta de muchísimos usuarios potenciales. Otro punto de mejora de Suricata es que funciona con reglas predefinidas, y no contempla por ahora el uso de herramientas de inteligencia artificial que pueden ser claves para el futuro desarrollo de este tipo de herramientas ante ataques cada vez más sofisticados [3-4]. |

|  |
| --- |
| **OBJETIVOS** |
| *Descripción detallada de en qué consistirá el TFG. En caso de que el objeto principal del TFG sea el desarrollo de software, además de los objetivos generales deben describirse sus funcionalidades a alto nivel.* |
| En este trabajo fin de grado (TFG) se plantea desarrollar una aplicación que incorpora un IDS que **se ejecutará localmente en tiempo real** para **varios sistemas operativos**, de forma que **la instalación será sencilla** para todos los usuarios, generando instaladores en caso necesario para que el usuario final no tenga que tener conocimientos avanzados de informática.  El IDS analizará el tráfico de la red para estimar la probabilidad de que estemos siendo atacados. Para ello se estudiará el uso de algunas técnicas de **inteligencia artificial** y se implementarán diversos algoritmos para **notificar al usuario del ataque**. En la literatura científica actual ya se han observado casos de éxito en la información de la IA en la detección de ataques [5] que valida la viabilidad de este TFG.  Se considera la posibilidad de implementar sugerencias para el usuario sobre qué medidas tomar o incluso el sistema podría tomarlas de manera autónoma dependiendo del escenario en cuestión.  Se contemplará el desarrollo de un **visionado de estadísticas**, que ayude al usuario a estudiar y entender ciertos aspectos de la seguridad de su red, con el fin de acercar la seguridad de las redes a un mayor público, mejorando la seguridad estándar que suelen tener todos los usuarios: un firewall preinstalado en el ordenador personal.  Otro pilar importante del proyecto es la **escalabilidad**, ya que la aplicación se construirá con intención de poder ser ampliada, considerando más tipos de ataques de los que implementaremos inicialmente a modo de demostración. De esta forma garantizamos que el proyecto no quede desfasado rápidamente y favorecemos la investigación de nuevas técnicas de seguridad de red en un campo de rápido crecimiento como lo es la inteligencia artificial, ya que proporcionamos la plataforma sobre la que trabajar. De hecho, consideramos que la estructura y su modularidad son los grandes puntos fuertes de este del proyecto, facilitando implementar en el futuro nuevos modelos de detección. |

|  |
| --- |
| **ENTREGABLES** |
| *Listado de resultados que generará el TFG (aplicaciones, estudios, manuales, etc.)* |
| Aplicación para Windows. |
| Aplicación para MacOS. |
| Manual de usuario. |
| Documentación del proyecto. |
| Código fuente del proyecto. |
| Datasets utilizados para el entrenamiento de los algoritmos de defensa. |

|  |
| --- |
| **MÉTODOS Y FASES DE TRABAJO** |
| **METODOLOGÍA:** |
| *Descripción de la metodología empleada en el desarrollo del TFG. Especificar cómo se va a desarrollar. Concretar si se trata de alguna metodología existente y, en caso contrario, describir y justificar adecuadamente los métodos que se aplicarán.* |
| Vamos a seguir una metodología ágil como Scrum adaptada para una sola persona. Haremos periodos de desarrollo y luego periodos de prueba para nuestra aplicación, de forma que nos vamos asegurando de que el proyecto va por el buen camino.  El tutor tendrá el rol de Product Owner, y para un mejor control del progreso del proyecto y del tiempo invertido usaremos una herramienta de control de trabajo, TooglTrack [6], que nos permitirá observar en qué dedicamos nuestros esfuerzos. |
| **FASES DE TRABAJO:** |
| *Enumeración y breve descripción de las fases de trabajo en las que consistirá el TFG.* |
| **Para la realización de este TFG se han identificado las siguientes fases que hemos agrupado en cuatro bloques:**  **Recopilación de información y especificación de la herramienta:**  **1ª Fase: Investigación inicial sobre el funcionamiento de los IDS existentes, ataques y formas de prevenirlos**  **2ª Fase: Análisis de requisitos y especificación**  **Desarollo de la herramienta:**  **3ª Fase: Creación de los archivos del proyecto, estructuración inicial**  **4ª Fase: Implementación de prueba del primer algoritmo de defensa para prevenir el primer tipo de ataque**  **5ª Fase: Desarrollo inicial de la interfaz**  **6ª Fase: Integración de la interfaz con el primer algoritmo de defensa**  **7ª Fase: Pruebas del sistema hasta este punto**  **8ª Fase: Desarrollo, implementación e integración del segundo algoritmo de defensa**  **9ª Fase: Pruebas del sistema hasta este punto**  **10ª Fase: Desarrollo, implementación e integración del tercer algoritmo de defensa**  **11ª Fase: Pruebas del sistema hasta este punto**  **12ª Fase: Desarrollo, implementación e integración del cuarto algoritmo de defensa**  **13º Fase: Pruebas del sistema hasta este punto**  **Despliegue de la herramienta:**  **14ª Fase: Empaquetar la aplicación, crear los instaladores para los diversos sistemas operativos**  **15ª Fase: Probar los instaladores en los diversos sistemas operativos**  **Documentación:**  **16ª Fase: Finalizar la documentación**  **17ª Fase: Crear el manual de usuario**  **Se realizarán sprints de 2 semanas y cada uno de ellos abarcará entre una y tres fases de las mostradas previamente atendiendo a su dificultad.** |
| **TEMPORIZACIÓN:** |
| *La siguiente tabla deberá contener una fila por cada una de las fases enumeradas en la sección anterior. En caso de tratarse de un trabajo en grupo, se añadirá una columna HORAS por cada miembro del equipo. Debe especificarse claramente el número de horas dedicado por cada alumno/a y la suma de horas individual deberá ser también de 296.* |
| |  |  | | --- | --- | | **FASE** | **HORAS** | | *Nombre Apellidos* | | **1ª Investigación inicial** | **20** | | **2ª Análisis de requisitos y especificación** | **10** | | **3 ª Creación de los archivos del proyecto** | **5** | | **4 ª Desarrollo del primer algoritmo de defensa** | **30** | | **5 ª Desarrollo inicial de la interfaz** | **35** | | **6 ª Integración de la interfaz con el primer algoritmo** | **20** | | **7 ª Pruebas del sistema hasta este punto** | **10** | | **8 ª Desarrollo e integración del segundo algoritmo de defensa** | **30** | | **9 ª Pruebas del sistema hasta este punto** | **10** | | **10 ª Desarrollo e integración del tercer algoritmo de defensa** | **30** | | **11 ª Pruebas del sistema hasta este punto** | **10** | | **12 ª Desarrollo e integración del cuarto algoritmo de defensa** | **30** | | **13 ª Pruebas del sistema hasta este punto** | **10** | | **14 ª Crear los instaladores** | **11** | | **15 ª Probar los instaladores** | **10** | | **16 ª Finalizar la documentación** | **20** | | **17 ª Crear el manual de usuario** | **5** | |  | **296** | |

|  |
| --- |
| **ENTORNO TECNOLÓGICO** |
| **TECNOLOGÍAS EMPLEADAS:** |
| *Enumeración de las tecnologías utilizadas (lenguajes de programación, frameworks, sistemas gestores de bases de datos, etc.) en el desarrollo del TFG.* |
| Python |
| Librerías de Python para la recolección de paquetes de red, como Scapy |
| Librerías de Python para operaciones relacionadas con inteligencia artificial, como TensorFlow o Scikit-learn |
| React (JavaScript) |
| InnoSetup o aplicación para empaquetar ejecutables similar |
| **RECURSOS SOFTWARE Y HARDWARE:** |
| *Listado de dispositivos (placas de desarrollo, microcontroladores, procesadores, sensores, robots, etc.) o software (IDE, editores, etc.) empleados en el desarrollo del TFG.* |
| Mi ordenador personal |
| Visual Studio Code |

|  |
| --- |
| **REFERENCIAS** |
| *Listado de referencias (libros, páginas web, etc.)* |
| [1] The Open Information Security Foundation, "Web oficial de Suricata", URL: https://suricata.io/ Consultada: 16/2/2025 |
| [2] Suricata Forum, "Suricata web GUI", URL: https://forum.suricata.io/t/suricata-web-gui/2901 Consultada: 16/2/2025 |
| [3] Sergey, "Using AI in Suricata: Enhancing Intrusion Detection System Capabilities", URL: https://suri-oculus.com/using-ai-in-suricata-enhancing-intrusion-detection-system-capabilities/ Consultada: 16/2/2025 |
| [4] Madjiguene NDONG, "Autonomous Systems: The Power of IDS + AI", URL: https://www.linkedin.com/pulse/autonomous-systems-power-ids-ia-madjiguene-ndong/ Consultada: 16/2/2025 |
| [5] Ahuja, Nisha, et al. "Ascertain the efficient machine learning approach to detect different ARP attacks." Computers and Electrical Engineering 99 (2022): 107757 |
| [6] The toggl company, "Web oficial de toogltack", URL: https://toggl.com/ Consultada: 16/2/2025 |

Málaga, 17 de Febrero de 2025

|  |  |  |
| --- | --- | --- |
| Firma tutor/tutora: | Firma cotutor/a: | Firma tutor/a coordinador/a: |