ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Software
DOMINA EL MUNDO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA DE SOFTWARE

PROYECTO DE TITULACÍON, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SOFTWARE

TEMA:

SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES ENFOCADO A ATAQUES DE INGENIERÍA SOCIAL DISEÑADO ESPECÍFICAMENTE PARA SU APLICACIÓN EN ENTORNOS DE TRANSACCIONES EN LÍNEA, A TRAVÉS DEL USO DE INTELIGENCIA DE AMENAZAS.

AUTORAS:

NACIMBA CAIZA, MELANY VANESA

SANTAMARIA ZAMBRANO, LISSETTE HELENA

DIRECTOR:

Ing. Navas Moya, Milton Patricio, Msc.

LATACUNGA AGOSTO, 2024



Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Problema

- El internet y la tecnología han transformado la forma en que las personas se comunican, interactúan, trabajan y viven.
- Las transacciones en línea se han convertido en una parte esencial de la vida cotidiana, pero han traído consigo un aumento exponencial de los ciberataques.
- El phishing se ha consolidado como una de las técnicas más utilizadas por ciberdelincuentes, causando daños financieros y robos de identidad.
- Los sistemas tradicionales de detección y prevención de intrusos (IDS/IPS) son vulnerables a nuevas y sofisticadas amenazas, debido a su dependencia de firmas y patrones de ataque predefinidos.



Solución

- Se plantea la creación de un IDPS especializado en proteger entornos de transacciones en línea frente a ataques de ingeniería social, como el phishing.
- Se emplearán modelos y/o algoritmos de Machine Learning(ML) para este propósito. Los modelos serán entrenados con datos de ataques de phishing para identificar patrones sospechosos y mejorar la precisión en la detección de amenazas.
- El Sistema IDPS integra inteligencia de amenazas para optimizar la capacidad del mismo, reduciendo falsos positivos y adaptándose dinámicamente a nuevas tácticas de ataque.



Objetivo General

Desarrollar un sistema de detección y prevención de intrusiones enfocado a ataques de ingeniería social específicamente diseñado para su aplicación en entornos de transacciones en línea, mediante el uso de inteligencia de amenazas.

Objetivos Específicos

Investigar y analizar las definiciones, conceptos clave y terminología específica sobre sistemas de detección y prevención de intrusos, machine learning, ataques de ingeniería social, y el uso de inteligencia de amenazas en la ciberseguridad.

Desarrollar prototipos iniciales de un sistema de detección y prevención de intrusos, en un ambiente controlado para ataques de ingeniería social, usando inteligencia de amenazas.

Optimizar un servidor que gestione datos de correos maliciosos para mejorar la eficiencia del sistema.

Analizar la eficiencia del sistema desarrollado mediante la aplicación de métricas de evaluación.

Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Transacciones en Línea

- Intercambio de información entre dos o más usuarios a través de medios electrónicos conectados a internet.



- La ingeniería social es una de las amenazas más destacadas en la actualidad.

- Malware, ransomware, botnets, cryptojacking, y phishing.

Ingeniería social - Phishing (Ciber-ataque)

- La Ingeniería social se ha convertido de una de las técnicas más utilizadas por los ciberdelincuentes.

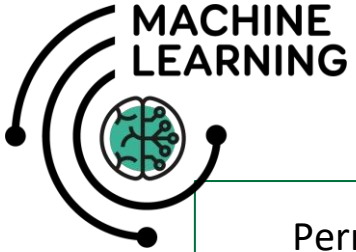
- Habilidades sociales y técnicas piscologías para manipular el comportamiento humano.



- Haciéndose pasar por entidades legítimas, logran que el usuario revele información personal como: contraseñas, nombre de usuarios, correo electrónico, entre otros.

- El objetivo principal del phishing es manipular al usuario para que revele información confidencial.

Modelos y/o algoritmos de Machine Learning



Permite que los ordenadores "aprendan" a partir de los datos, desarrollando algoritmos que reconocen patrones sin necesidad de programar cada solución como en la programación tradicional.

Modelos y/o algoritmos de Machine Learning

Decision Tree

Modelo de aprendizaje supervisado que utiliza un árbol de decisiones para realizar predicciones basadas en características de entrada.

Recuperado de Su, J., & Zhang, H. (2006, July). A fast decision tree learning algorithm. In Aaai (Vol. 6, pp. 500-505).

Random Forest

Es una versión extendida del árbol de decisiones donde cada árbol es entrenado con una muestra aleatoria del dataset y las decisiones finales se toman por mayoría de votos.

Recuperado de Shaik, A. B., & Srinivasan, S. (2019). A brief survey on random forest ensembles in classification model. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 2 (pp. 253-260). Springer Singapore.

Support Vector Machines

Modelo supervisado que encuentra el hiperplano óptimo que separa las clases en un espacio de características de alta dimensión.

Recuperado de Mammone, A., Turchi, M., & Cristianini, N. (2009). Support vector machines. Wiley Interdisciplinary Reviews: Computational Statistics, 1(3), 283-289.

Inteligencia de Amenazas

Inteligencia de amenazas estratégica

- Ofrece a la alta dirección información sobre riesgos y amenazas cibernéticas de alto nivel para apoyar la toma de decisiones y mitigar impactos en los activos tecnológicos.

Inteligencia de amenazas operacional

- Dirigida al personal de defensa de infraestructuras tecnológicas, se centra en ataques inminentes y en los actores y métodos usados para las intrusiones.

Inteligencia de amenazas técnica

- Proporciona IOCs como IPs, URLs, hashes y dominios, para integrarlos en herramientas de seguridad y monitorear posibles ataques.

Inteligencia de amenazas tácticas

- Se enfoca en las TTPs de los ciberataques, ayudando a establecer defensas y actualizar políticas de seguridad según las amenazas actuales.

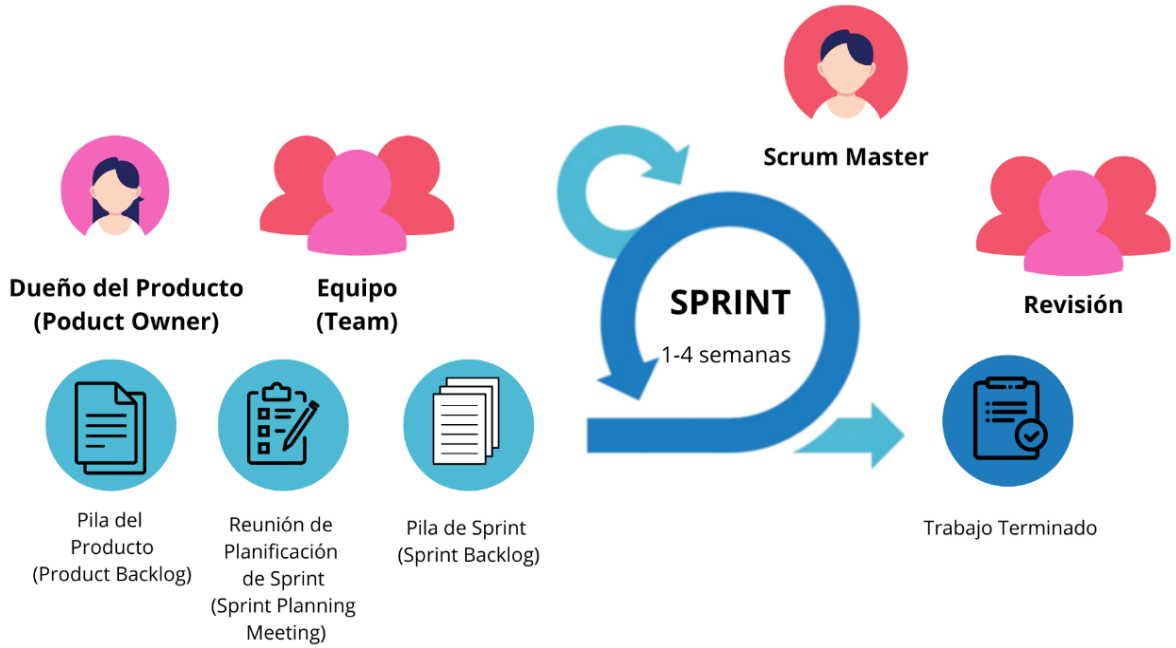
Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Metodología de desarrollo

- Metodología Scrum



Elaboración propia basado en (*Deemer, P., Benefield, G., Larman, C., & Vodde, B. (2009). Información básica de SCRUM. California: Scrum Training Institute, 1-20.)*

Análisis del sistema

- Historias de Usuario:



Historia de usuario 01

Quiero un sistema de detección y prevención de intrusos que por medio del entrenamiento de un modelo de machine learning pueda detectar ataques de phishing.

Para tener un medio que sea capaz de identificar y analizar ataques de phishing, mejorando la seguridad en entornos de transacciones en línea.

Historia de usuario 02

Quiero que el sistema se apoye en APIs de inteligencia de amenazas para respaldar el modelo.

Para mejor la precisión de la detección de phishing con datos sobre amenazas actualizadas.

Historia de usuario 03

Quiero un dashboard que permita la visualización de la información adquirida sobre ataques de phishing.

Para lograr supervisar y analizar las amenazas, permitiendo una mejor toma de decisiones.

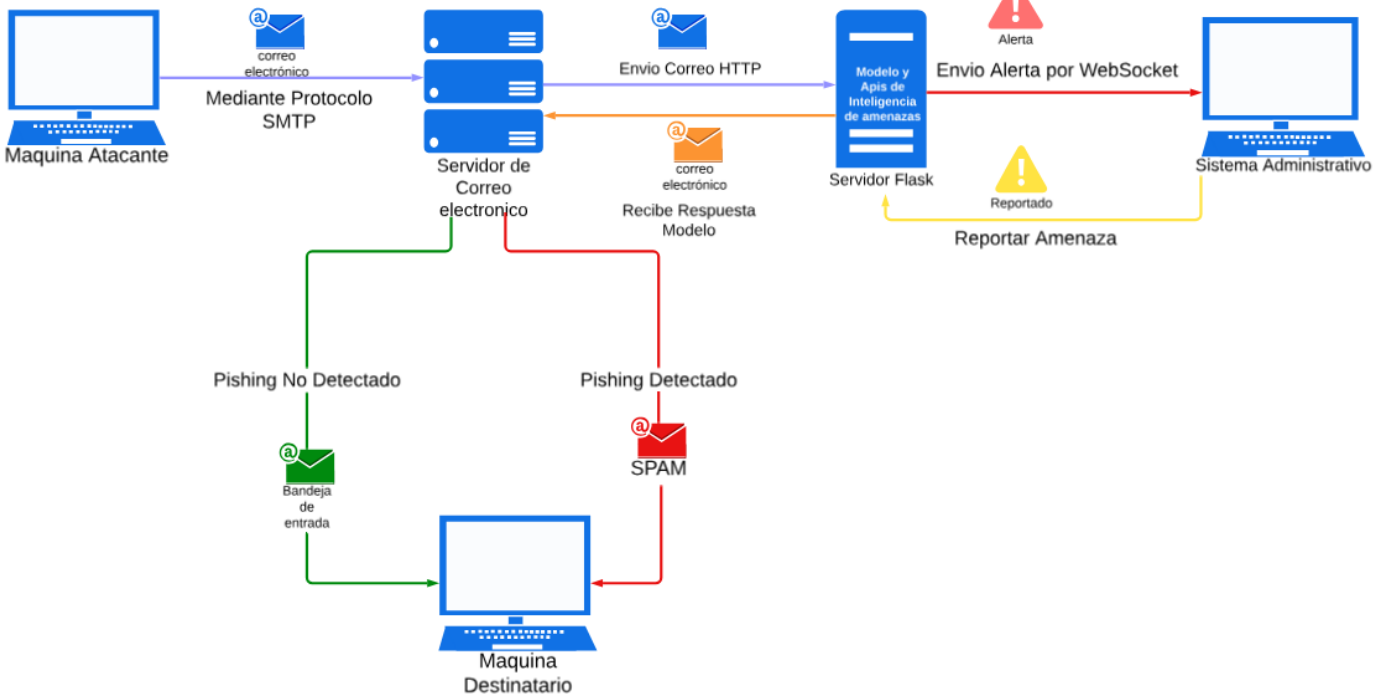
Historia de usuario 04

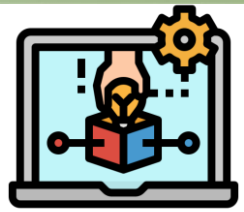
Quiero recibir alertas y/o notificaciones sobre posibles ataques de phishing detectados.

Para poder reaccionar ante las diferentes amenazas y tomar las medidas necesarias, con el fin de proteger la integridad del sistema. .

Diseño del sistema

- Arquitectura Física del sistema





Desarrollo del Sistema

- Resultados del Sprint 01: Entrenamiento y selección del modelo machine learning para URL

Modelo y/o algoritmo	Recall	Precision	Accuracy	F1 Score
Decision Tree	96.36%	96.43%	96.36%	96.38%
Random Forest	96.39%	96.47%	96.39%	96.40%
Support Vector Machine	95.34%	95.48%	95.34%	95.37%

Resultados de evaluación de los modelos y/o algoritmos machine learning para URL

Desarrollo del Sistema

- Resultados del Sprint 01: Entrenamiento y selección del modelo machine learning para el cuerpo del correo

Modelo y/o algoritmo	Recall	Precision	Accuracy	F1 Score
Decision Tree	92.28%	92.34%	92.28%	92.30%
Random Forest	97.03%	97.04%	97.03%	97.03%
Support Vector Machine	97.54%	97.62%	97.54%	97.55%

Resultados de evaluación de los modelos y/o algoritmos machine learning para el cuerpo del correo

Desarrollo del Sistema

- Resultados del Sprint 02: Integración con las APIs de inteligencia de amenazas.

VIRUSTOTAL	ABUSEIPDB	APIVOID
Sospechoso	Porcentaje de abuso	Puntuación de riesgo
No detectado	País	Suspensión de página
Malicioso	Dominio	Lista negra de dominios
Inofensivo		
Reputación		
Último análisis		
Categoría		

VIRUSTOTAL

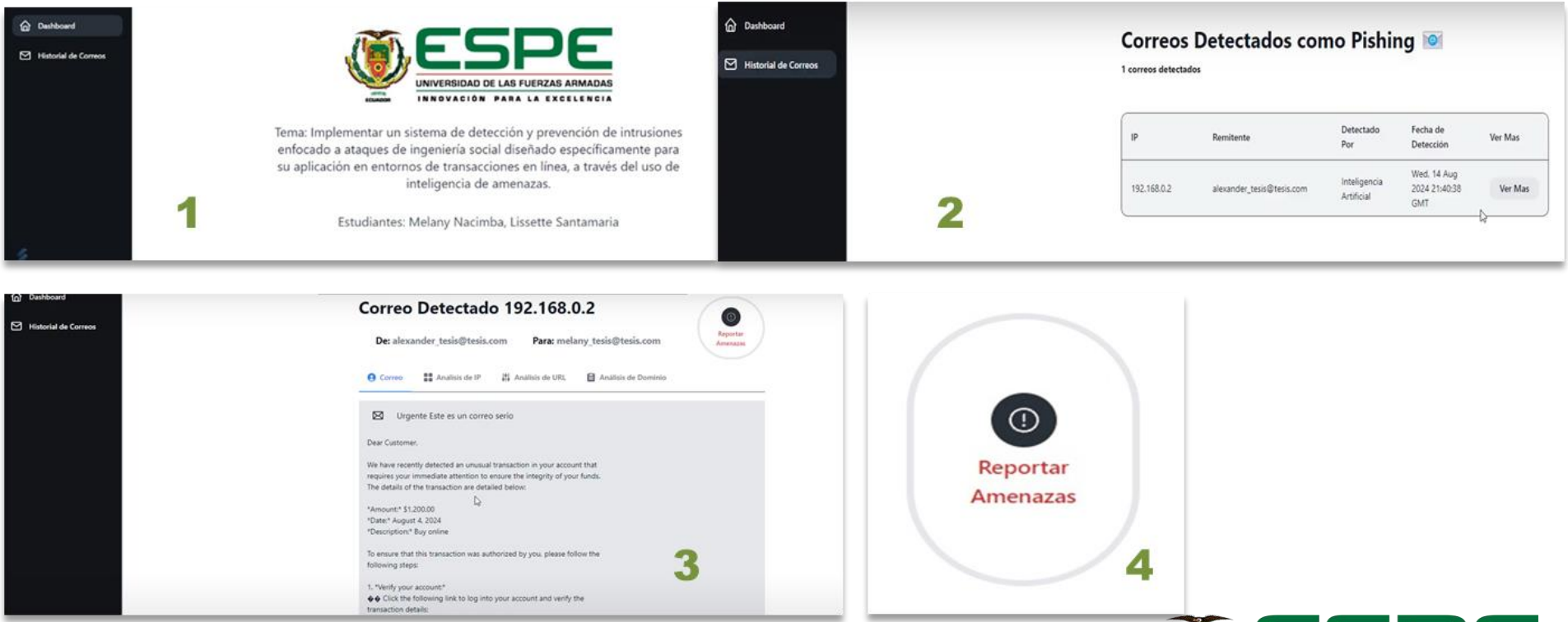
AbuseIPDB

apivoid
Threat Analysis APIs

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Desarrollo del Sistema

- Resultados del Sprint 03: Creación del Dashboard



Desarrollo del Sistema

- Resultados del Sprint 04: Alertas y Notificaciones

```
    socketio.init_app(self.app)
    self.register_blueprints()

def register_blueprints(self):
    self.app.register_blueprint(controller, url_prefix="/api/v1")

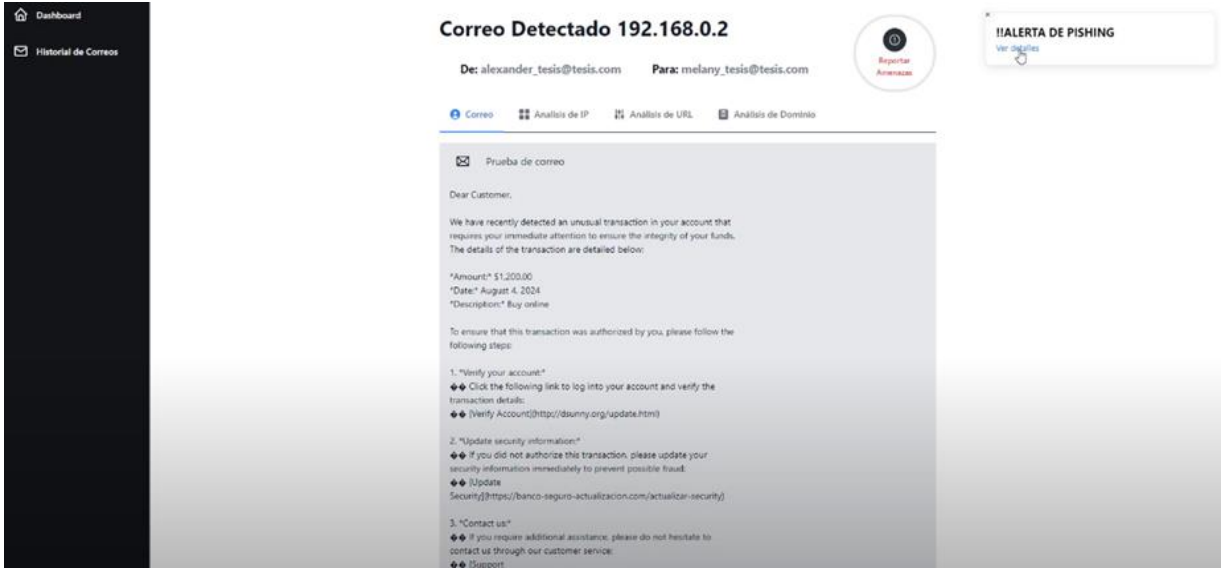
def run(self):
    socketio.run(self.app, port=5000, debug=True, host='0.0.0.0')
```

```
# Emitir evento de alerta si se detecta phishing
socketio.emit('phishing_alert', {'data': email_data})
```

- Websocket permite tener una conexión bidireccional entre el backend y el frontend.
- Librería socketIO permite realizar las configuraciones

Desarrollo del Sistema

- Resultados del Sprint 04: Alertas y Notificaciones

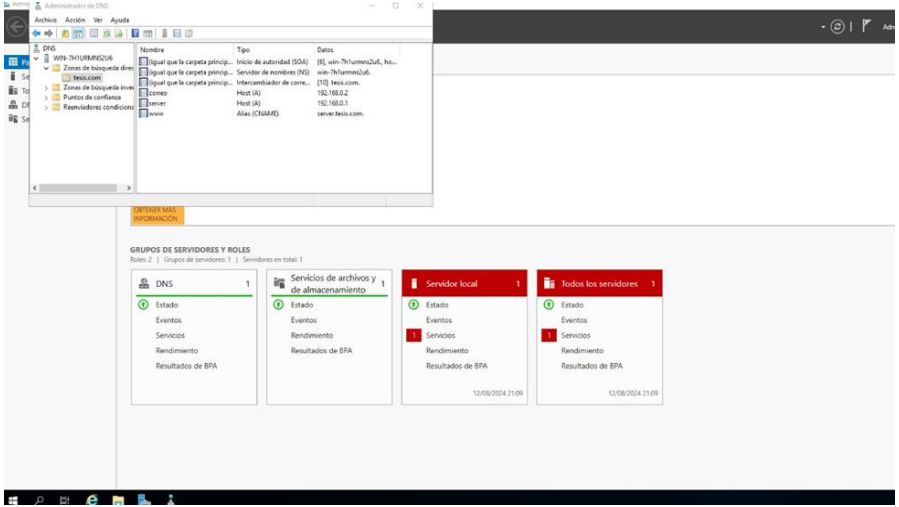


Orden del día

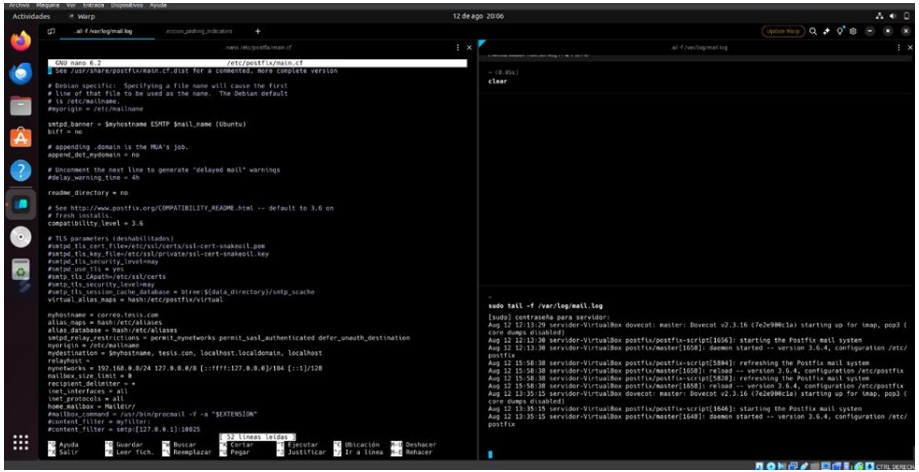
- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Validación del Sistema

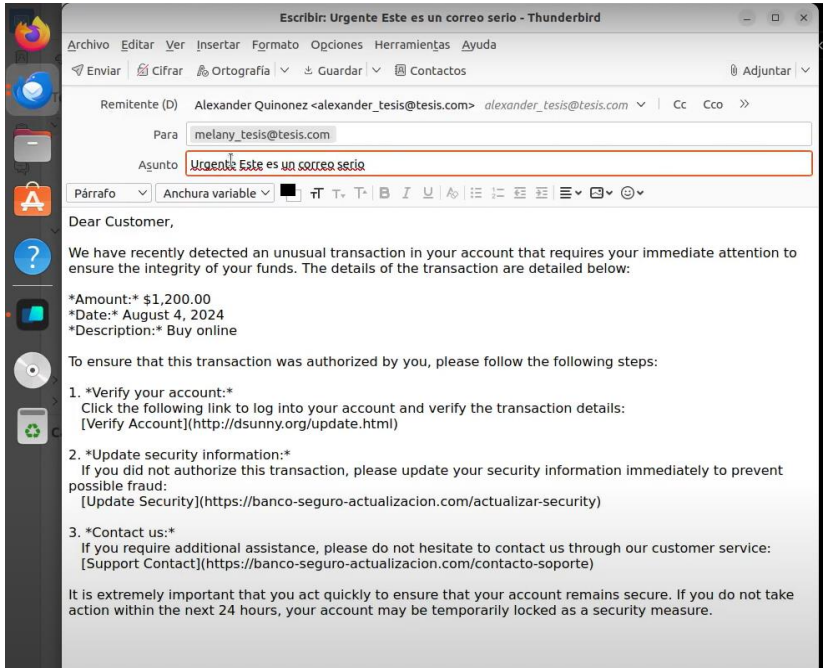


Windows Server 2019, configuración del servidor DNS.



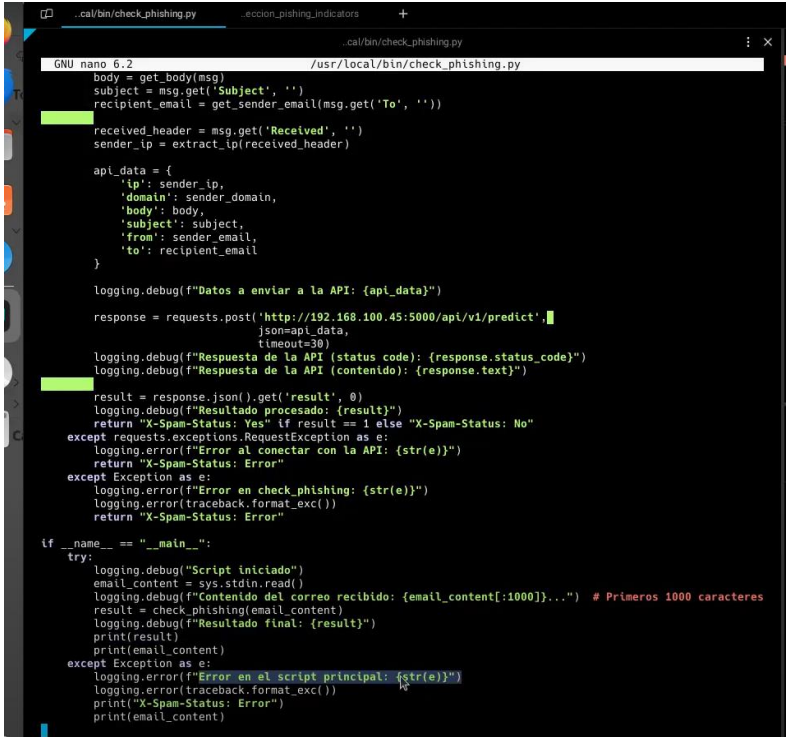
Ubuntu, configuración de Postfix como servidor de correo electrónico

Validación del Sistema

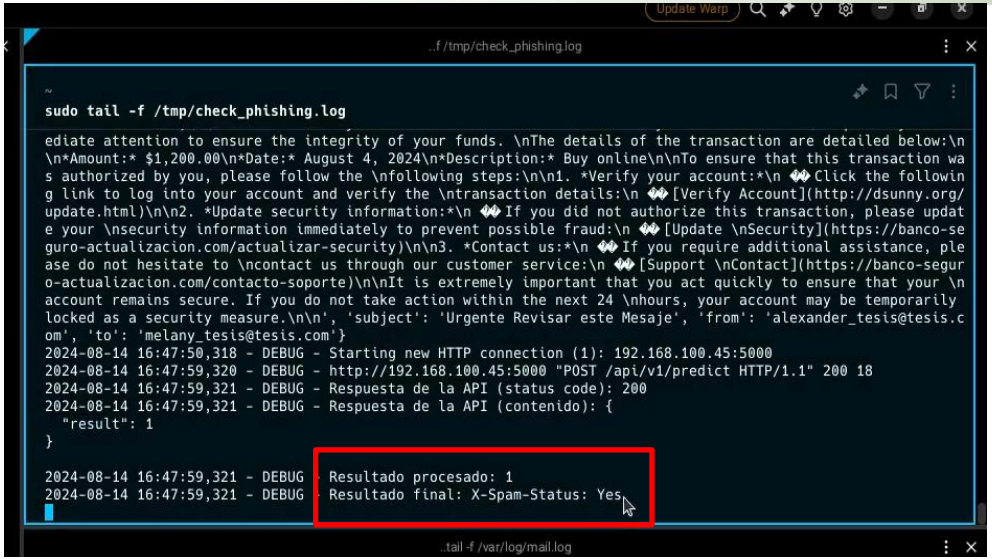


Envío del correo al servidor de Postfix

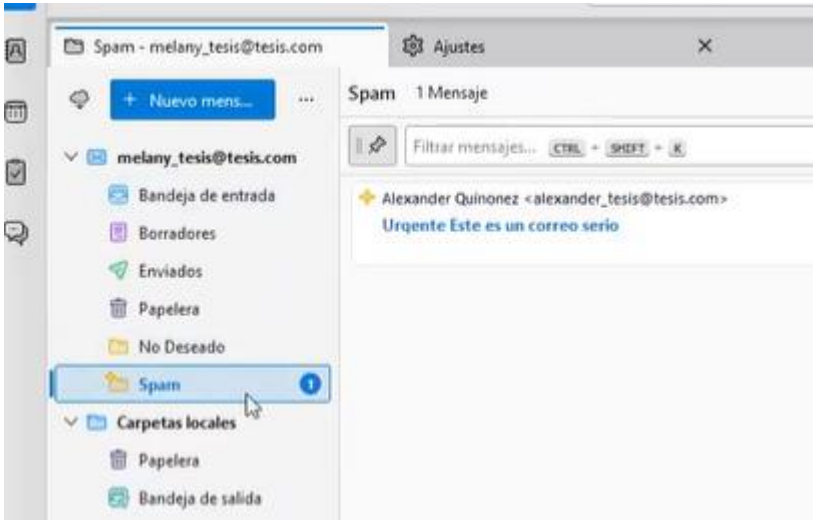
Análisis preliminar del script en python



Validación del Sistema



Análisis en el servidor Flask

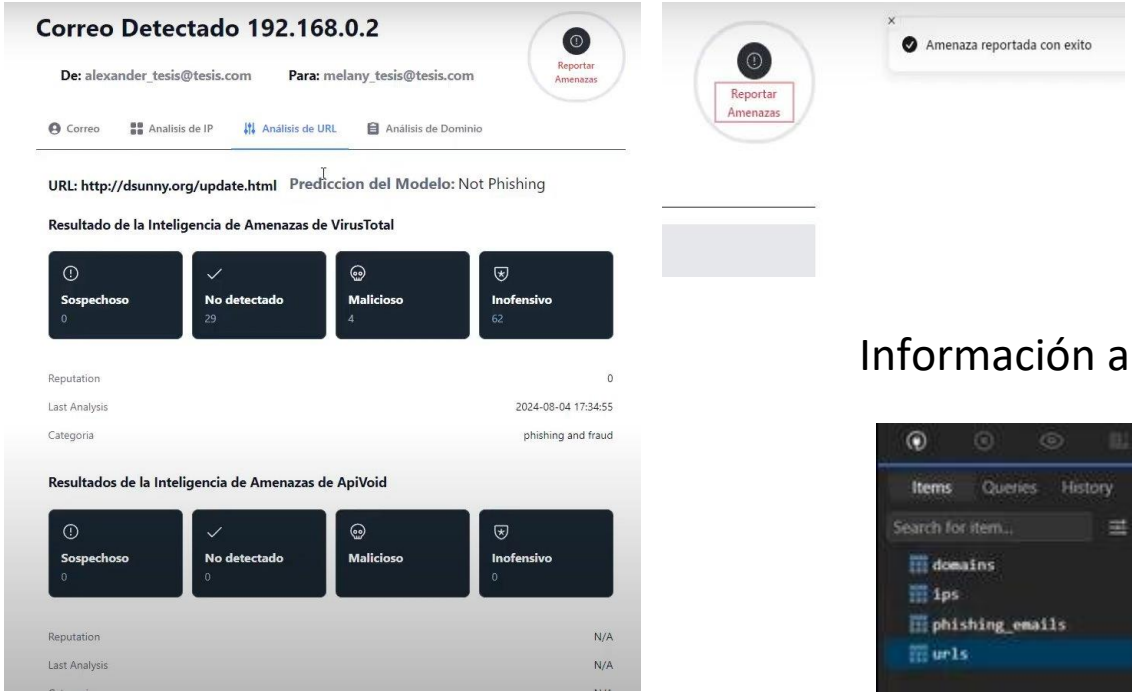


Correo enviado a Spam

Validación del Sistema

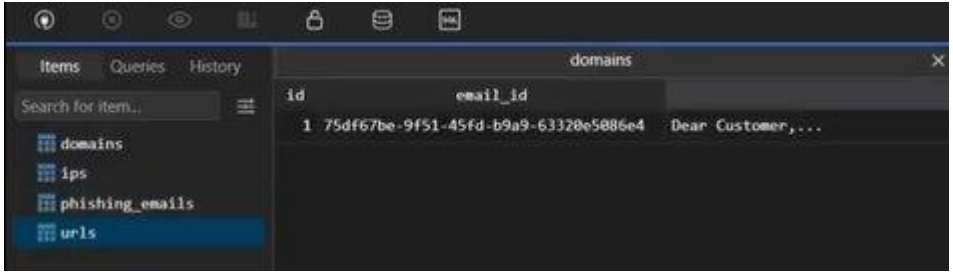


Notificación de un ataque de phishing



Información del ataque de phishing y reporte de la amenaza

Información almacenada en la base de datos



Validación del Sistema

- Resultados Generales: Matriz de confusión

	POSITIVO	NEGATIVO
POSITIVO	159	11
NEGATIVO	7	223

- Resultados de las pruebas individuales del cuerpo del correo: 400 cuerpos de correo

MÉTRICA DE EVALUACIÓN	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5	Promedio
Accuracy	97.47%	94.05%	96.20%	96.25%	95.00%	95.50%
Precision	96.97%	91.67%	96.97%	94.12%	91.43%	93.53%
Recall	96.97%	94.29%	94.12%	96.97%	96.97%	95.78%
F1 score	96.97%	92.96%	95.52%	95.52%	94.12%	94.64%

Validación del Sistema

- Resultados Generales: Matriz de confusión

	POSITIVO	NEGATIVO
POSITIVO	223	5
NEGATIVO	6	191

- Resultados de las pruebas individuales de las URLs: 425 URLs

MÉTRICA DE EVALUACIÓN	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5	Promedio
Accuracy	96.50%	95.80%	96.80%	96.30%	95.00%	96.08%
Precision	97.30%	96.90%	97.70%	97.10%	97.44%	97.28%
Recall	95.10%	94.20%	95.70%	94.90%	96.36%	95.25%
F1 score	96.20%	95.50%	96.60%	96.00%	96.20%	96.10%

Validación del Sistema



- Obtención de las métricas de evaluación de las Apis de Inteligencia de Amenazas

Resultados Generales: Matriz de confusión

	POSITIVO	NEGATIVO
POSITIVO	31	4
NEGATIVO	2	54

Métricas de evaluación

MÉTRICA DE EVALUACIÓN	Resultado
Accuracy	93.41%
Precision	93.94%
Recall	88.57%
F1 score	91.18%

Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Conclusiones

En la investigación realizada sobre técnicas de detección de phishing e inteligencia de amenazas, se seleccionó y adoptó tres modelos de machine learning adecuados para el análisis de cuerpos de correos y URLs: Random Forest, SVM y Decision Tree. Esta investigación previa, permitió una fluida integración de los modelos con las APIs de inteligencia de amenazas.

La metodología Scrum demostró ser una metodología ágil y eficaz para desarrollar sistemas de detección y prevención de intrusos en ciberseguridad. Permite a los equipos adaptarse rápidamente a cambios, priorizar tareas clave y mejorar la colaboración. Con roles bien definidos, se optimiza la comunicación y la eficiencia, acelerando el proceso y garantizando un producto final de alta calidad que responde a las amenazas en evolución.

Conclusiones

En los modelos y/o algoritmos de machine learning, Random Forest presenta una superioridad según la métrica F1 Score, donde muestra un mayor porcentaje en la evaluación de las predicciones de URLs. Aunque, en la evaluación del cuerpo del correo el modelo SVM presenta mayor porcentaje en las métricas, se sigue prefiriendo el modelo Random Forest ya que el tiempo de respuesta es significativamente más rápido, lo que ayuda a optimizar el sistema.

El uso de inteligencia de amenazas técnica, que proporciona datos cruciales como IPs, URLs, hashes de archivos y dominios maliciosos, enriquece las herramientas de seguridad al ofrecer indicadores de compromiso (IOCs) para el monitoreo de posibles ataques. Sin embargo, al integrar estos datos con modelos de machine learning, se ha evidenciado la necesidad de ajustes adicionales para mejorar la precisión en la clasificación de amenazas.

Conclusiones

El dashboard permite al administrador reportar amenazas, lo que alimenta una base de datos que almacena información sobre correos maliciosos en un servidor Flask. Este servidor utiliza los datos previamente guardados para comparar características de nuevos correos, evitando la necesidad de analizar la información repetidamente, lo que reduce el tiempo de análisis y a su vez mejora la eficiencia del sistema IDPS en la detección y prevención de ataques de phishing.

En un ambiente controlado para las pruebas, se implementó las tecnologías Postfix, Devecot y Thunderbird para desarrollar un sistema que sea capaz de analizar e interceptar correos electrónicos; con la incorporación del modelo de machine learning e inteligencia de amenazas se facilitó la identificación de ataques de phishing basado en la información proporcionada sobre IPs, dominios y URLs reportadas. Demostrando la fiabilidad del sistema en un entorno de transacciones en línea, protegiendo a los usuarios de posibles robos de información.

Bibliografía

- C. E. L. Grande y R. S. Guadrón, «Ingeniería Social: El Ataque Silencioso», 2015
- J. Bobadilla, *Machine Learning y Deep Learning: Usando Python, Scikit y Keras*. Ediciones de la U, 2021.
- «INFORMACIÓN BÁSICA DE SCRUM». Accedido: 8 de agosto de 2024. [En línea]. Disponible en: https://goodagile.com/scrumprimer/scrumprimer_es.pdf
- W. Drzewiecki, «Thorough statistical comparison of machine learning regression models and their ensembles for sub-pixel imperviousness and imperviousness change mapping», *Geod. Cartogr.*, vol. 66, dic. 2017, doi: 10.1515/geocart-2017-0012.
- M. Cohn, «User Stories and User Story Examples by Mike Cohn», Mountain Goat Software. Accedido: 8 de agosto de 2024. [En línea]. Disponible en: https://www.mountaingoatsoftware.com/agile/user-stories

Software
DOMINA EL MUNDO

Gracias por su atención

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA