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

TRABAJO DE INTEGRACIÓN CURRICULAR, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SOFTWARE

TEMA:

SISTEMA DE DETECCIÓN DE INTRUSOS EN SITIOS WEB, USANDO INDICADORES DE COMPROMISO APLICANDO MACHINE LEARNING: CASO PRÁCTICO ATAQUES PHISHING

AUTORES:
CAISA LLANO, DENNIS SEBASTIÁN
GUEVARA JIMÉNEZ, ADRIAN FERNANDO

DIRECTORA:
Ing. Corral Diaz, María Alexandra, Msc

LATACUNGA AGOSTO, 2023

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 Ascenso Exponencial de Internet: Desvelando las Amenazas Emergentes que Comprometen la Integridad de la Información.
- Las amenazas impactan de manera significativa a una amplia cantidad de individuos, destacando entre los más afectados tanto las empresas como las instituciones. Ejemplos notables incluyen a compañías prominentes como Meta y Tesla, así como a diversas organizaciones gubernamentales.
- Entre los casos más reconocidos de ataques en línea, encontramos el phishing, el malware, el wahling y el vishing. En el año 2022, se registró un total de pérdidas económicas a nivel global que ascendieron a 4,91 millones de dólares.

Solución

- Se plantea la creación de un Sistema de Detección de Intrusos (IDS) que emplee Indicadores de Compromiso (IOCs) con el fin de prevenir ataques de phishing dirigidos a sitios web.
- El Sistema de Detección de Intrusiones (IDS) se desarrolla mediante la implementación de Indicadores de Compromiso (IOCs), los cuales son presentados a través de una extensión para el navegador Google Chrome.
- Se emplearán modelos y/o algoritmos de Aprendizaje Automático para este propósito. Estos modelos serán entrenados utilizando conjuntos de datos que contienen las páginas web que han sido identificadas como phishing.

Objetivo General

Desarrollar un sistema de detección de intrusos en sitios web, usando indicadores de compromiso aplicando Machine Learning: Caso Práctico Phishing Google Chrome

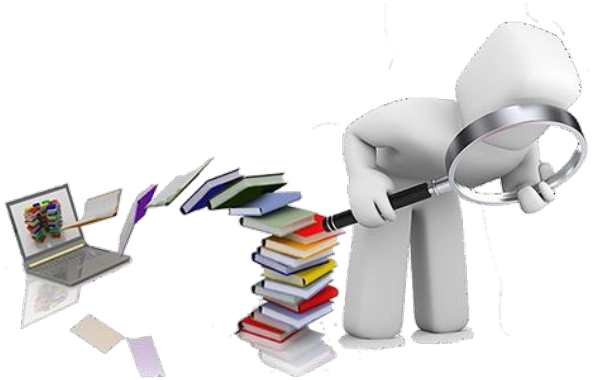
Objetivos Específicos

Entender la vanguardia en cuanto a los indicadores de compromiso y su utilidad en la detección de intrusos en sitios web mediante el uso de técnicas de phishing en el navegador Google Chrome.

Poner en marcha un sistema de detección de intrusos en páginas web mediante el desarrollo de una extensión para Google Chrome, empleando métodos de aprendizaje automático.

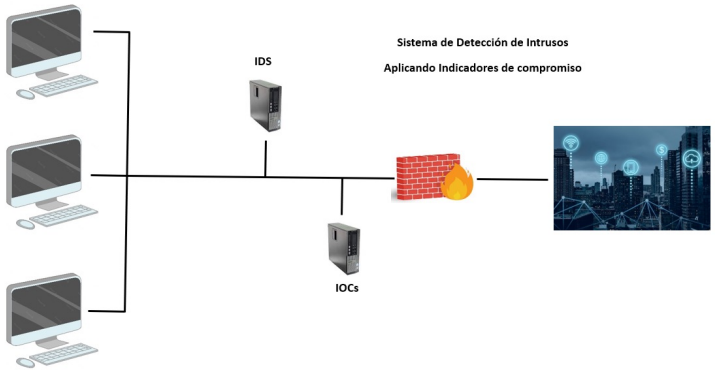
Evaluar los resultados obtenidos, analizar y corregir posibles errores identificados en los indicadores de compromiso del sistema de detección de intrusos.

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



Sistema de Detección de Intrusos (IDS) e Indicadores de Compromisos (IOCs)

- Sistema de software o hardware que identifica actividades maliciosas.



- Un IDS requiere de una o varias entradas para poder detectar algún tipo de ataque.
- Un IOCs un patrón de actividades o características para detectar ataques phishing.
- Sistema de detección de intrusos basados en firmas (SIDS).
- Indicadores de compromisos Basados en Ataques a Servicios Web.

Phishing (Ciber-ataque)

- Intenta obtener información confidencial de manera indebida, posiblemente con intenciones ilegales.

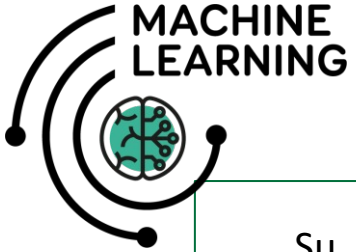
- Técnica de Ingeniería Social: Un Enfoque Persuasivo para la Interacción Humana

- Con el paso del tiempo, los sitios web de phishing han evolucionado y mejorado en su ejecución.

Características para la detección de intrusos – Phishing

- Se establecieron los medios de verificación mediante la realización de una revisión exhaustiva de la literatura de Indicadores de Compromiso.
- Se seleccionaron un total de 40 características: 30 que son extraidos del contenido de las URL y 10 de los indiacores de compromiso.

Modelos y/o algoritmos de Machine Learning



Su propósito radica en capacitar a las computadoras con la habilidad de aprendizaje, empleando conjuntos de datos como base, con el fin de permitirles tomar decisiones de manera autónoma (predicciones) sin requerir programación directa.

Modelos y/o algoritmos de Machine Learning

El algoritmo de aprendizaje supervisado logra una precisión máxima del 96,60% en la identificación de ataques de phishing.

Decision Tree

Algoritmo de aprendizaje supervisado logra una precisión máxima del 99,33% en la identificación de ataques de phishing.

Random Forest

El algoritmo de aprendizaje supervisado logra una precisión máxima del 97% en la identificación de ataques de phishing.

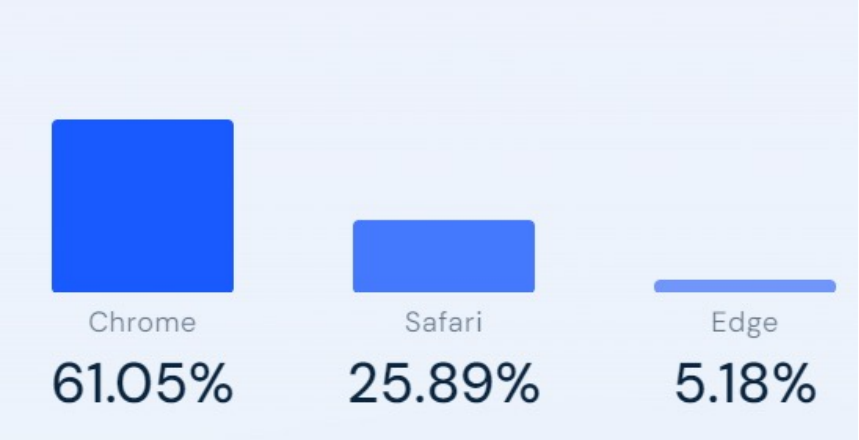
Neural Networks

El algoritmo de aprendizaje supervisado logra una precisión máxima del 96,5% en la identificación de ataques de phishing.

Support Vector Machines

Extensiones Google Chrome

- Son aplicaciones que se instalan en el navegador, cumpliendo funciones específicas que necesita el usuario.
- Google Chrome es el navegador más usado.
- El navegador Google Chrome introdujo este tipo de funcionalidades desde el año 2010. A partir de la cuarta versión, se volvió posible la creación de extensiones.

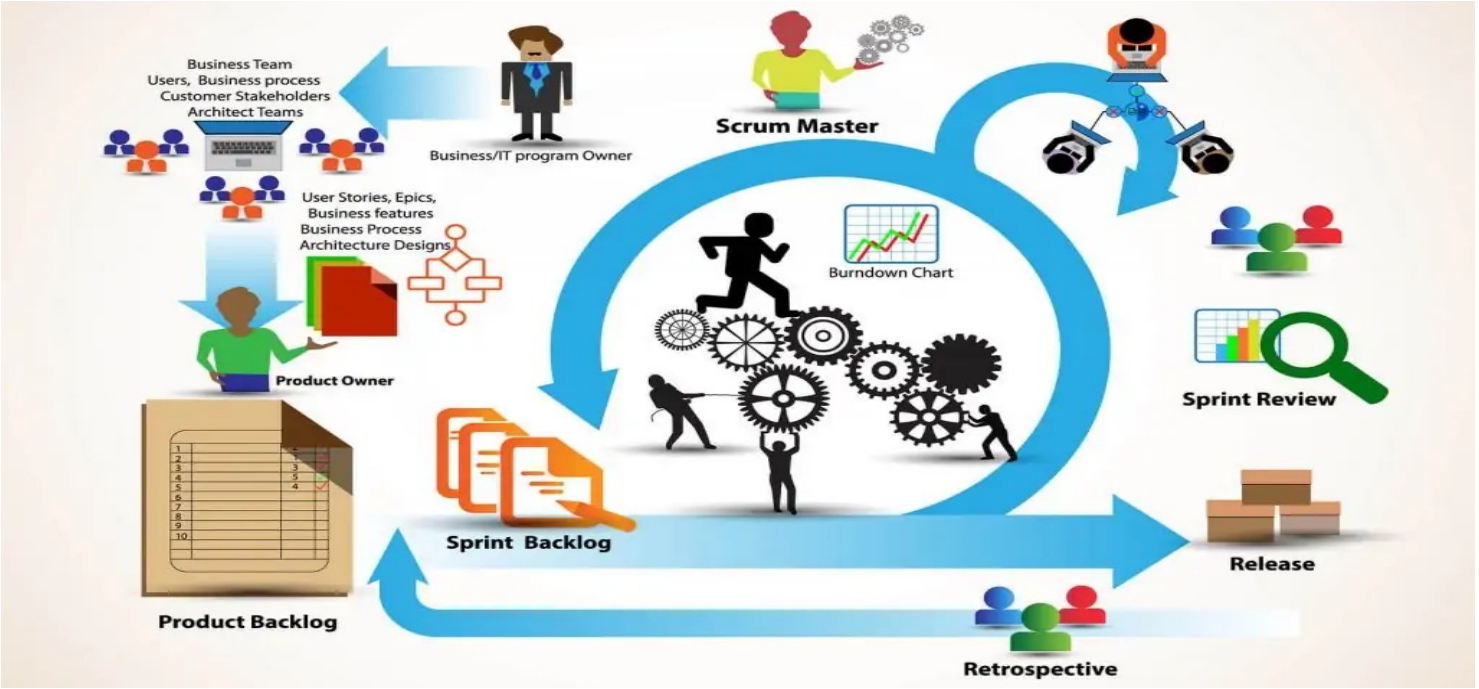


Navegadores más usados: Comparativa y estadísticas (2023). (2023, May 22). https://www.stackscale.com/es/blog/top-navegadores-caracteristicas-comparativa-estadisticas/

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

Metodología de desarrollo

- Metodología Scrum



Recuperado de ¿Qué Es La Metodología Scrum? Y Gestión De Proyectos Scrum. (2022, December 23). https://www.nimblework.com/es/agile/que-es-scrum/

Análisis del sistema

- Historia de Usuario:

Historia de usuario 01
Quiero una extensión de Google Chrome que pueda detectar y me diga si un sitio web contiene phishing.
Para disponer de un medio para detección si estoy navegando en un sitio web seguro de Internet con Google Chrome.

Análisis del sistema

- Lista de Tareas

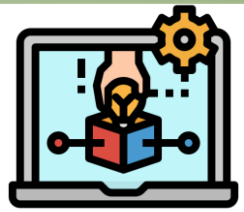
- LA EXTENSIÓN USA EL ALGORITMO Y/O MODELO MÁS EFECTIVO DE MACHINE LEARNING PARA DETECTAR EL PHISHING EN SITIOS WEB.
- EL COMPLEMENTO PUEDE HACER PREDICCIONES CON BUENA PRECISIÓN.

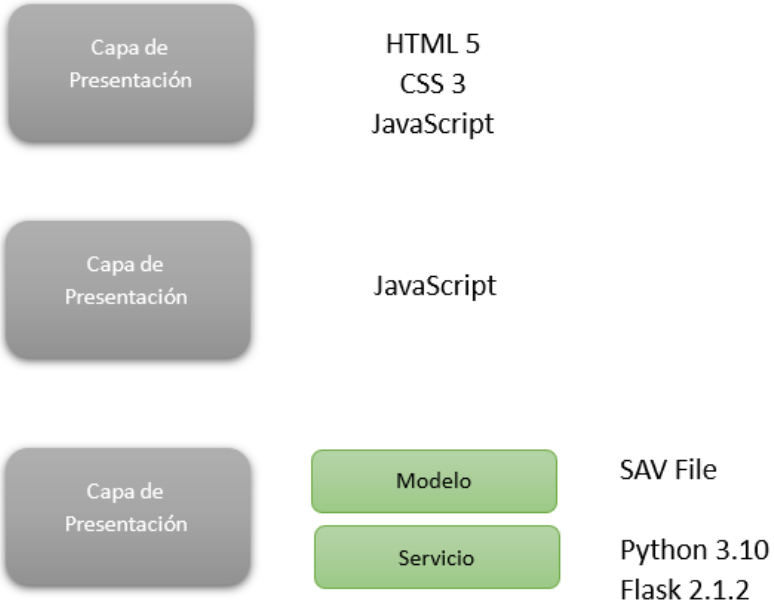
- SE CREA UN DATASET QUE CONTENGA FUNCIONES QUE PUEDAN IDENTIFICAR LOS SITIOS DE PHISHING DE LOS LEGÍTIMOS.
- NECESARIO PARA ENTRENAR EL MODELO DE MACHINE LEARNING

- IMPLEMENTAR UN MODELO DE MACHINE LEARNING, PARA SUBIR A UN SERVIDOR, PERMITIENDO LA REALIZACIÓN DE PREDICCIONES A TRAVÉS DE ESTE SERVICIO.
- OBTENGA UN SERVICIO QUE SE PUEDE UTILIZAR EN OTRAS APLICACIONES.

Diseño del sistema

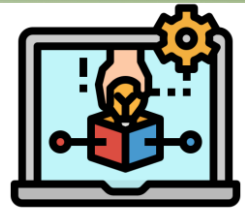
- Arquitectura Lógica del sistema con las tecnologías a usar.

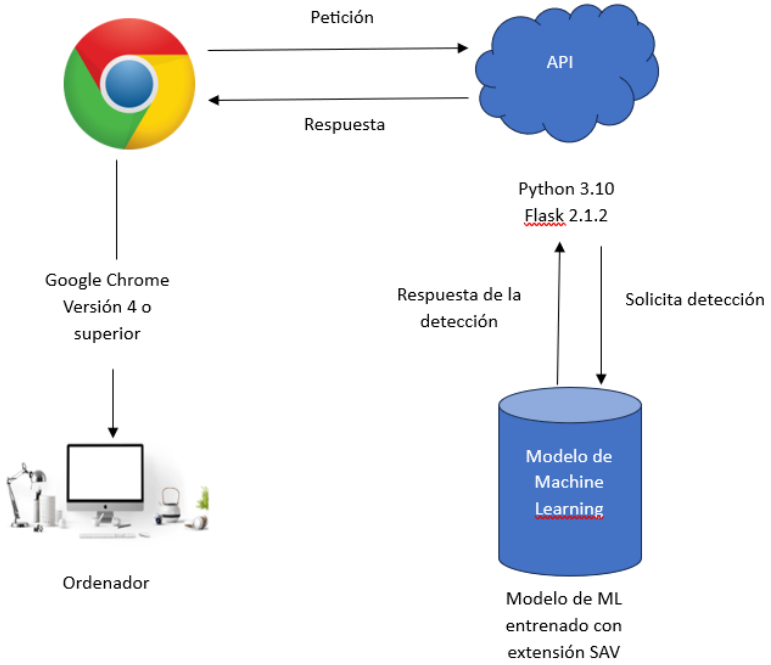




Diseño del sistema

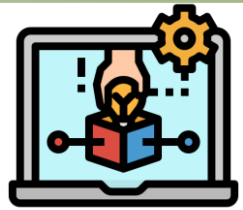
- Arquitectura Física del sistema





Diseño del sistema

- Mockups



Desarrollo del Sistema

- Resultado de la Tarea 1: Selección del mejor modelo/algoritmo para la detección de Phishing en Sitios Web

Algoritmos/Modelos	Accuracy	Recall	Precision	F1
Random Forest	0,8406	0,9642	0,8571	0,9060
Decision Tree	0.8140	0,9299	0,8517	0,8874
Ada Boost	0.7864	0,9096	0,8358	0,8678
SVM	0,7794	0,9088	0,8286	0,8607
Mezcla de Gaussianas	0,2096	0,0428	0,6677	0,0539
Bayesiano Ingenuos	0	0	0	0
Redes Bayesianas	0,2139	0,0330	0,6864	0,0489
Dummin Classifier	0,8069	1,0	0,8069	0,8931

Modelo seleccionado es el algoritmo Random Forest por mejores resultados.

Desarrollo del Sistema

- Resultado de la Tarea 1: Creación del Dataset

-1
Phishing

1
Legítimo

Ord.	linksToPage	hasMD5	hasSHA1	hasYara	hasSHA256	hasShort
0	1	-1	-1	-1	-1	-1
1	-1	1	-1	1	-1	-1
2	-1	1	1	-1	-1	-1
3	-1	-1	-1	-1	1	-1
4	-1	-1	-1	1	-1	-1
5	-1	1	-1	-1	-1	-1

Características

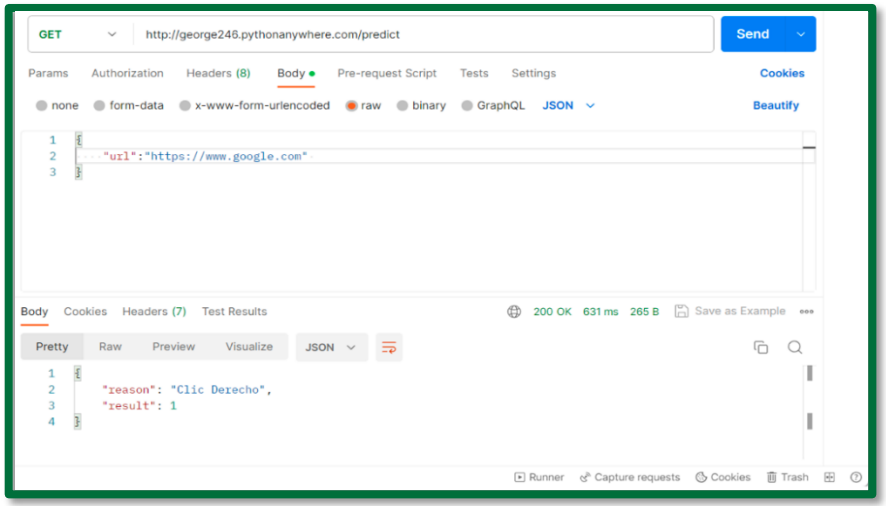
Dataset creado:

https://drive.google.com/drive/folders/1UsZfEZYrw0DnM6wOL3quS2q2uhXS8Bhx?usp=sharing

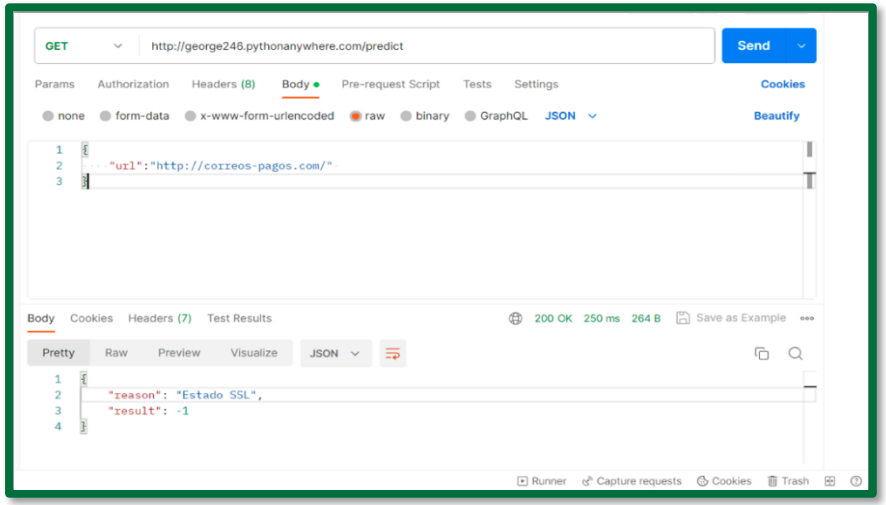
Desarrollo del Sistema

- Resultado de la Tarea 1: Selección del mejor modelo/algoritmo para la detección de Phishing en Sitios Web

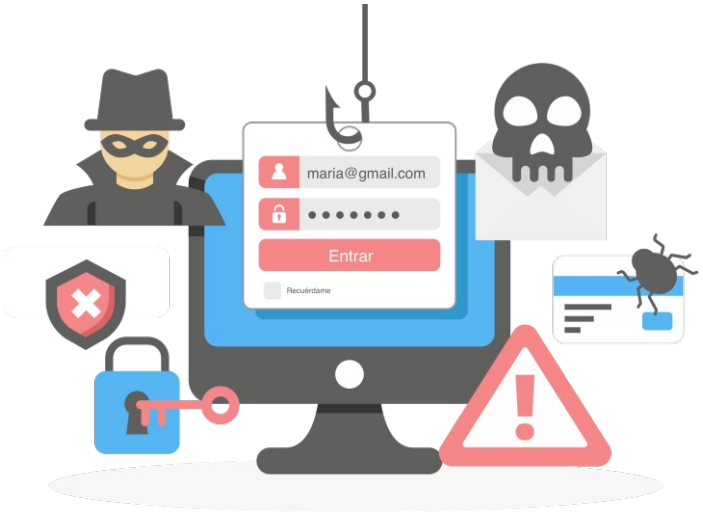
Sitio web con Phishing



Sitio web Legítimo

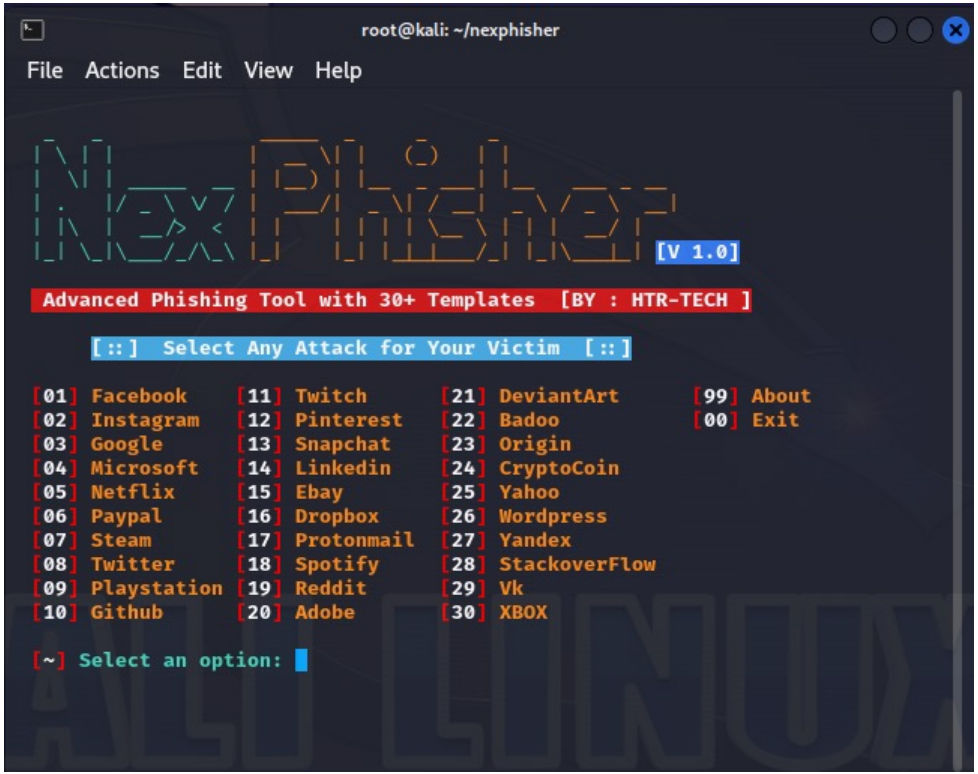


- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



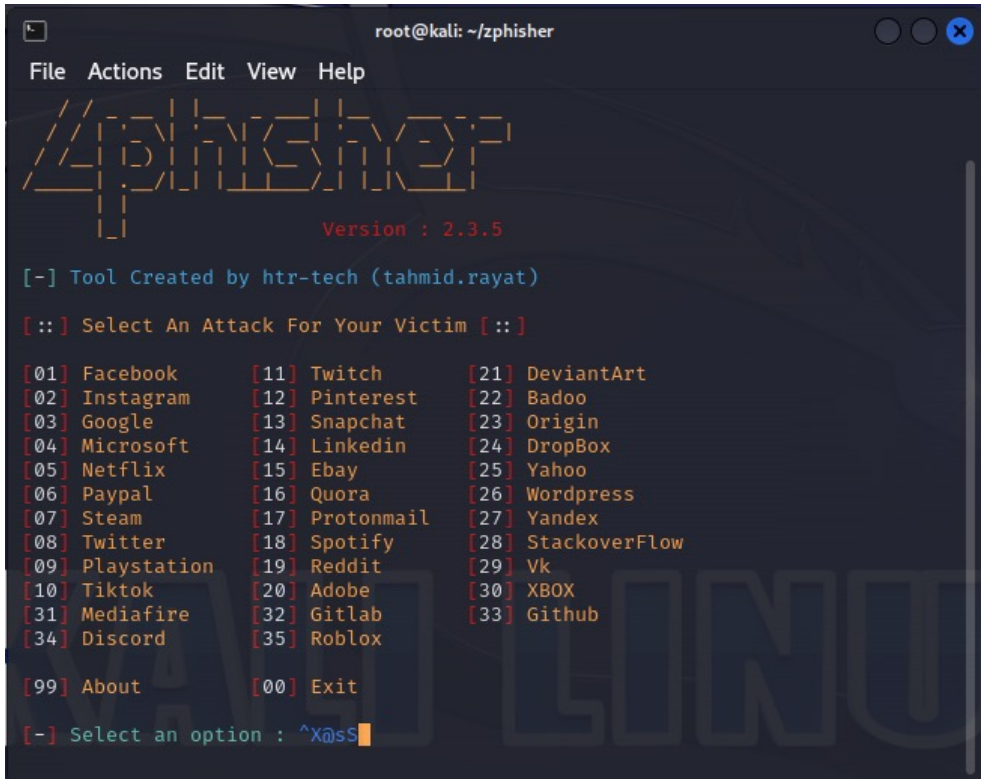
Validación del Sistema

- Uso de la herramienta NexPhisher (ambiente simulado)



Validación del Sistema

- Uso de la herramienta Zphisher (ambiente simulado)



Validación del Sistema

- Proceso de ejecución de pruebas

Envía un ataque

Documentar

Pc 1

PC2

Documento

Generar el sitio web con phishing con ayuda de la herramienta Zphisher y NexPhisher

Escáner el sitio web con la extensión de Google Chrome desarrollad (Phishing Impact)

Se documenta el resultado obtenido para validar el sistema

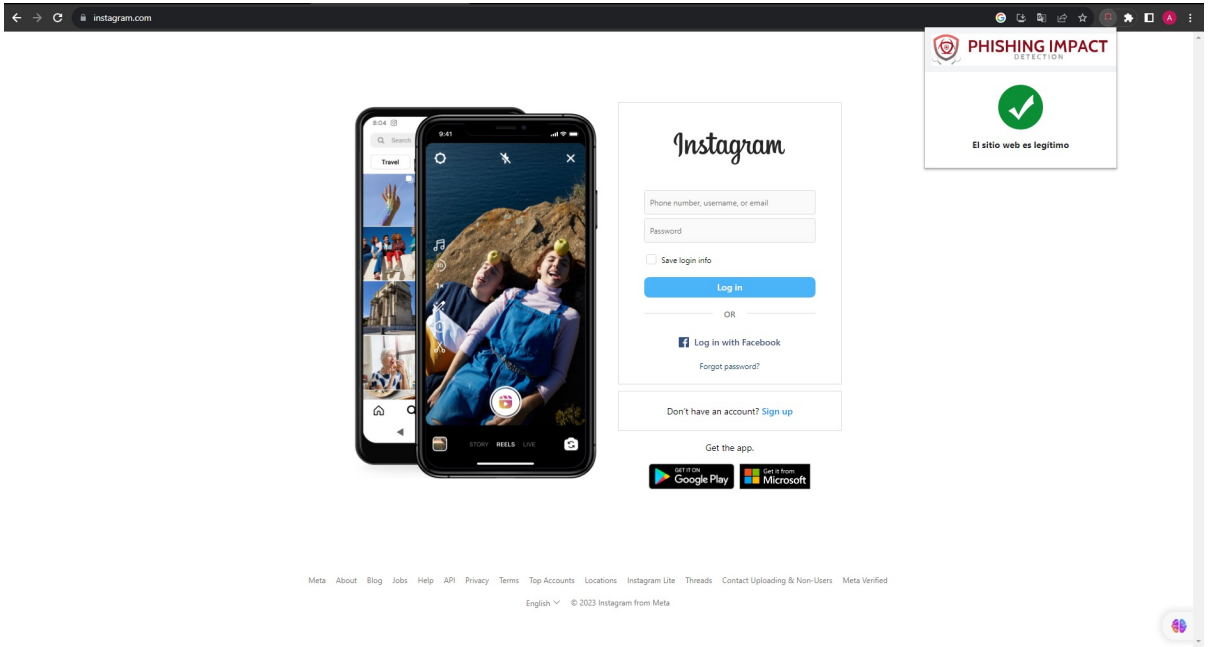
Validación del Sistema

- Resultados de pruebas de Phishing

SITIO WEB	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING		PRUEBAS SITIOS WEB LEGÍTIMOS	
Facebook	Traditional Login Page	Phishing	Phishing	Legitimo	Legitimo
Instagram	Traditional Login Page	Phishing	Legitimo	Legitimo	Legitimo
X	X Login Page	Phishing	Legitimo	Legitimo	Legitimo
TikTok	TikTok Login Page	Phishing	Legitimo	Legitimo	Legitimo
Pinterest	Pinterest Login Page	Phishing	Legitimo	Legitimo	Phishing

Validación del Sistema

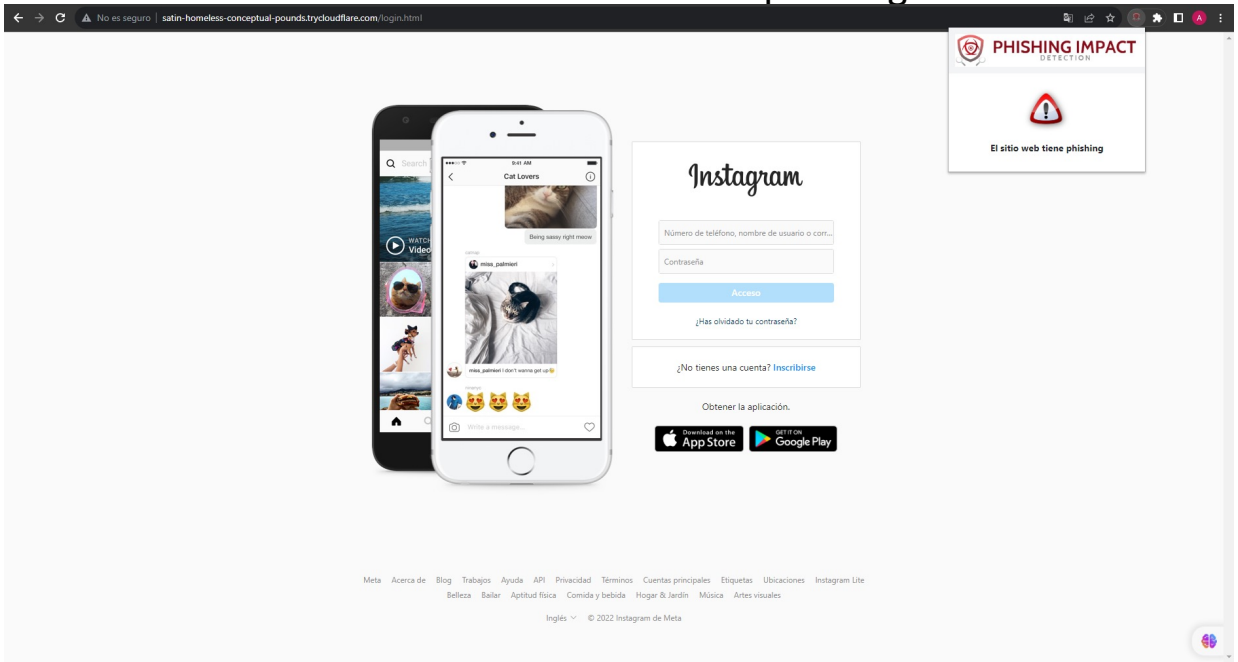
- Se muestra un análisis de un sitio web cuando es legítimo



URL: https://www.instagram.com/

Validación del Sistema

- Se muestra un análisis de un sitio web cuando tiene phishing



URL: http://satin-homeless-conceptual-pounds.trycloudflare.com/login.html

Validación del Sistema

- Obtención de datos para validar el sistema

Matriz de confusión

	POSITIVOS	NEGATIVOS
POSITIVOS	Phishing clasificados correctamente (VP)	Legítimos mal clasificados (FP)
NEGATIVOS	Phishing mal clasificados (FN)	Legítimos clasificados correctamente (VN)

Métricas de evaluación

MÉTRICA	FÓRMULA
Accuracy	$\text{accuracy} = \frac{\text{VP} + \text{VN}}{\text{VP} + \text{VN} + \text{FP} + \text{FN}}$
Precision	$precision = \frac{VP}{VP + FP}$
Recall	$recall = \frac{VP}{VP + FN}$
F1	$f1 = 2 * \frac{presicion * recall}{presicion + recall}$

Validación del Sistema

- Obtención de las métricas de evaluación en los 3 modelos

CAMPO SIMULADO/REAL					CAMPO SIMULADO/REAL			
ACCURACY	PRECISION	RECALL	F1		ACCURACY	PRECISION	RECALL	F1
84%	85%	96%	90%	Zphisher	84%	82%	85%	83%
				NexPhisher	86%	92%	82%	86%

Análisis de resultados

- Se probó en un campo simulado/real con Zphisher y NexPhisher.

- Se lograron niveles de precisión (Accuracy) en el rango más alto, alcanzando un 86%, y en el rango más bajo, con un 84%. Estos valores se encuentran cercanos a los resultados reportados en la literatura (93.14% y 91% respectivamente) por Garcia, E. A. (2009) en términos de precisión. Como resultado, el Sistema de Detección de Intrusiones (IDS) aplicando Indicadores de compromiso (IOCs), las técnicas utilizadas para mitigar los ataques de phishing muestran que el rendimiento cumple con las expectativas aceptables.

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

Conclusiones

El IDS desarrollado (Phishing Impact) se entrenó con un dataset de 13.190 sitios web (3.987 sitios web con Phishing (30,21%) y 9.205 sitios web legítimos (69,79%)).

Se diseñó e implementó un sistema de detección de Phishing.

Para validar el IDS e IOCs (Phishing Impact) implementado se utilizó las herramientas Zphisher y NexPhisher.

Conclusiones

La aplicación de la metodología Scrum, resulto de gran ayuda para cumplir con los objetivos de este proyecto.

La extensión de Google Chrome (Phishing Impact) está lista para su despliegue en un entorno práctico, siempre y cuando exista un mecanismo que se encargue de recolectar en forma periódica nuevos ciber-ataques phishing para alimentar el dataset.

Bibliografía

- Recuperado de ¿Qué Es La Metodología Scrum? Y Gestión De Proyectos Scrum. (2022, December 23). https://www.nimblework.com/es/agile/que-es-scrum/
- Navegadores más usados: Comparativa y estadísticas (2023). (2023, May 22). https://www.stackscale.com/es/blog/top-navegadores-caracteristicas-comparativa-estadisticas/
- He, H., Y Garcia, E. A. (2009). Learning from imbalanced data. IEEE Transactions on knowledge and data engineering, 21(9), 1263-1284.

Software
DOMINA EL MUNDO

Gracias por su atención

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA