DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA DE SOFTWARE

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

TEMA:

SISTEMA DE DETECCIÓN DE INTRUSOS EN SITIOS WEB, USANDO MODELOS Y/O ALGORITMOS DE MACHINE LEARNING: CASO PRÁCTICO PHISHING GOOGLE CHROME

AUTORES:
CASTILLO VELOZ, MISHELL ESTEFANÍA
CHUQUITARCO VELASCO, KEVIN JAIR

DIRECTOR:
Dr. CARRILLO MEDINA, JOSÉ LUIS, (mCL)

LATACUNGA FEBRERO, 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

- Con el crecimiento exponencial del Internet, han surgido un sin numero de amenazas a la información.
- Estas amenazas han llegado a afectar instituciones y/o empresas como Facebook, Microsoft, Sony, gobiernos de todo el mundo y hasta millones de usuarios.
- Existen diferentes tipos de ataques en el internet (Cyber-Ataques), entre los más conocidos son los ataques Malware, Botnes, Ramsomware, Brute Force Attack y Phishing. Para el año 2021, se tuvo un total de $4,65 millones de dólares en pérdidas económicas.

Solución

- Se propone desarrollar un Sistema de Detección de Intrusos (IDS) para sitios web con Phishing.
- EL IDS se lo desarrollará en forma de una extensión para el navegador Google Chrome.
- Se utilizarán modelos y/o algoritmos de Machine Learning, los cuales aprenderán en base a un conjunto de características que son usadas con frecuencia para detectar sitios web con phishing y así implementar la extensión IDS.

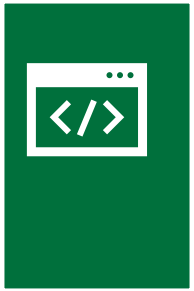
PHISHING

Objetivo General

Desarrollar un sistema de detección de intrusos en sitios web, usando modelos y/o algoritmos de Machine Learning: Caso Práctico Phishing Google Chrome

Objetivos Específicos

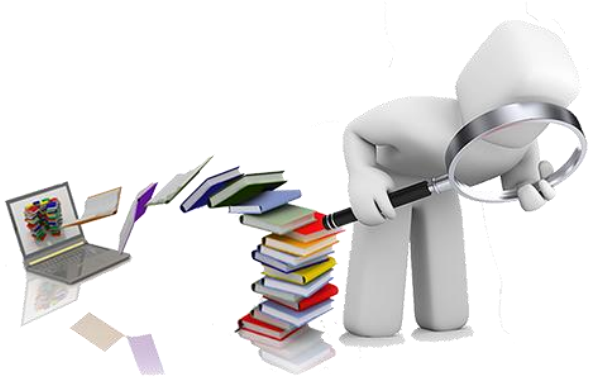
Conocer el estado del arte sobre métodos y técnicas para la detección de intrusos en sitios web, basado en phishing por motores de búsqueda - Google Chrome.



Implementar un sistema de detección de intrusos en sitios web, a través del desarrollo de una extensión para Google Chrome, empleando técnicas de Machine Learning.

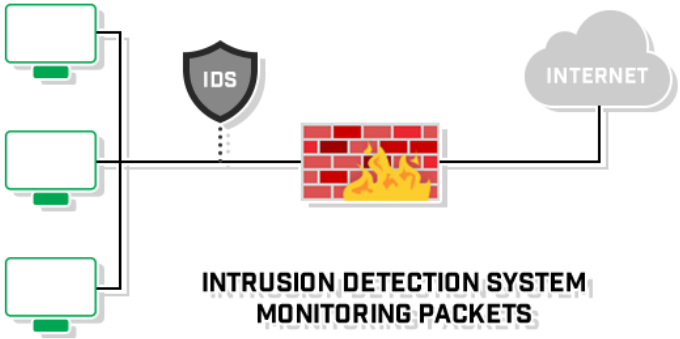
Validar los resultados, analizar los errores y ajustar los modelos del sistema de detección de intrusos.

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



Sistema de Detección de Intrusos (IDS)

- Sistema de software o hardware que identifica actividades maliciosas.
- Un IDS requiere de una o varias entradas para poder detectar algún tipo de ataque.



- Sistema de detección de intrusos basados en firmas (SIDS).
- Sistema de detección de intrusos basado en anomalías (AIDS).

Phishing (Ciber-ataque)

- Pretende robar información privada, posiblemente con fines ilegales.
- Los sitios web con phishing se han ido perfeccionando con el tiempo.

- Técnica de Ingeniería social

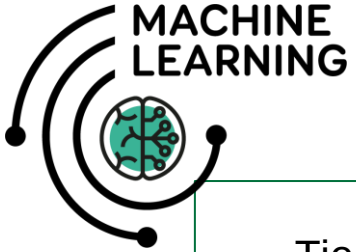
Características para la detección de intrusos – Phishing

- Se determinaron los recursos de comprobación con la ayuda de una revisión de la literatura.
- Se seleccionaron 30 características: basadas en el contenido del sitio web y en la URL

Sitio web con Phishing

Estructura de una URL

Modelos y/o algoritmos de Machine Learning



Tiene como objetivo hacer que las computadoras tengan la capacidad de aprender, basándose en un conjunto de datos, para después poder tomar decisiones (predecir) por si sola sin la necesidad de estar programándolas.

Modelos y/o algoritmos de Machine Learning

Decision Tree

Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima de 96,60% en la detección de phishing.

Random Forest

Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima de 99,33% en la detección de phishing.

Ada Boost

Clasificador meta-estimador. Alcanza una precisión máxima del 99,81% en la detección de phishing.

Neural Networks

Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima del 97% en la detección de phishing.

Support Vector Machines

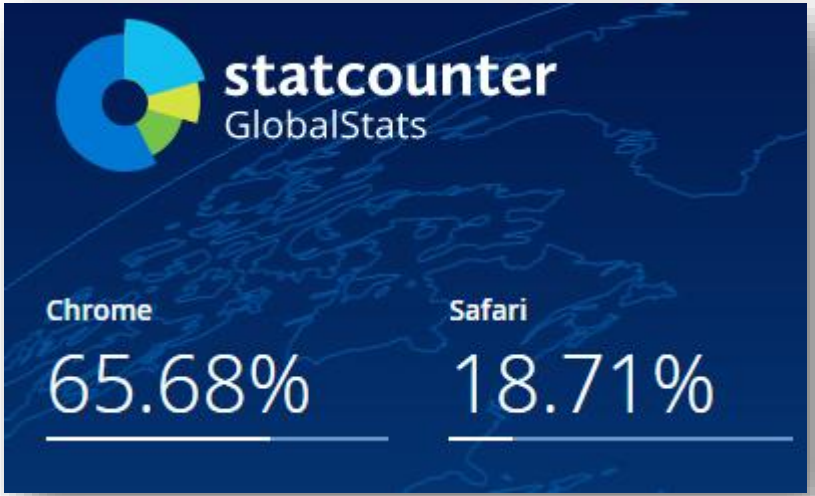
Algoritmo de aprendizaje supervisado. Alcanza el 96,5% en la detección de phishing.

Bagging

Algoritmo optimizador. Alcanza el 98,3% en la detección de phishing.

Extensiones Google Chrome

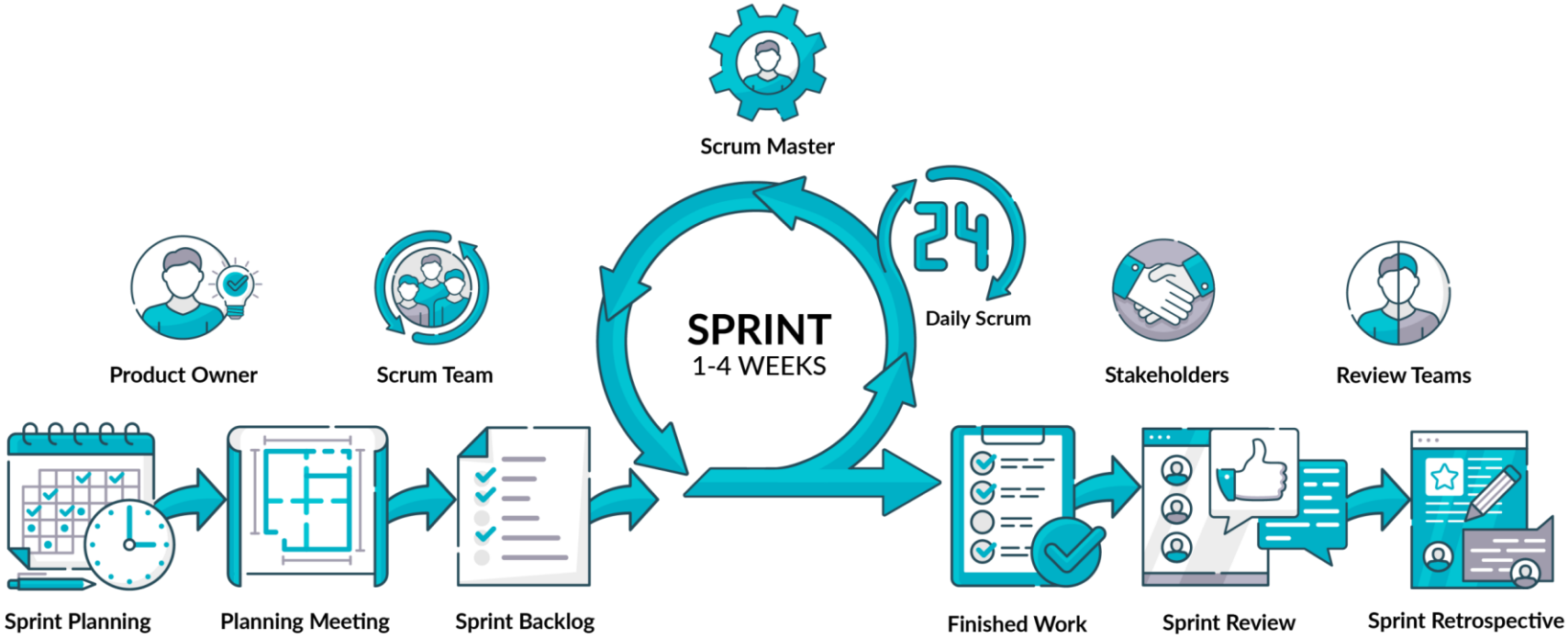
- Son aplicaciones que se ejecutan dentro del entorno de un Sitio Web.
- Google Chrome es el navegador más usado.
- El navegador Google Chrome implementó este tipo de funcionalidades desde el año 2010, es decir, a partir de la cuarta versión se pudo crear extensiones.



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

Metodología de desarrollo

- Metodología Scrum



Recuperado de What is Scrum. (2022). App Inlet. https://appinlet.com/what-is-scrum/

Análisis del sistema

- Historias de Usuario:

Historia de usuario 01
Quiero que la extensión utilice el mejor algoritmo y/o modelo de Machine Learning para la detección de phishing en sitios web.
Para que la extensión realice predicciones con una buena precisión

Historia de usuario 02
Quiero un dataset que contenga características que permitan identificar sitios web con phishing de los legítimos.
Para entrenar el modelo de Machine Learning

Análisis del sistema

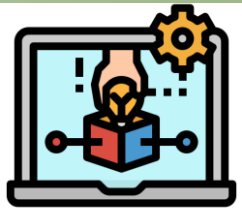
- Historias de Usuario:

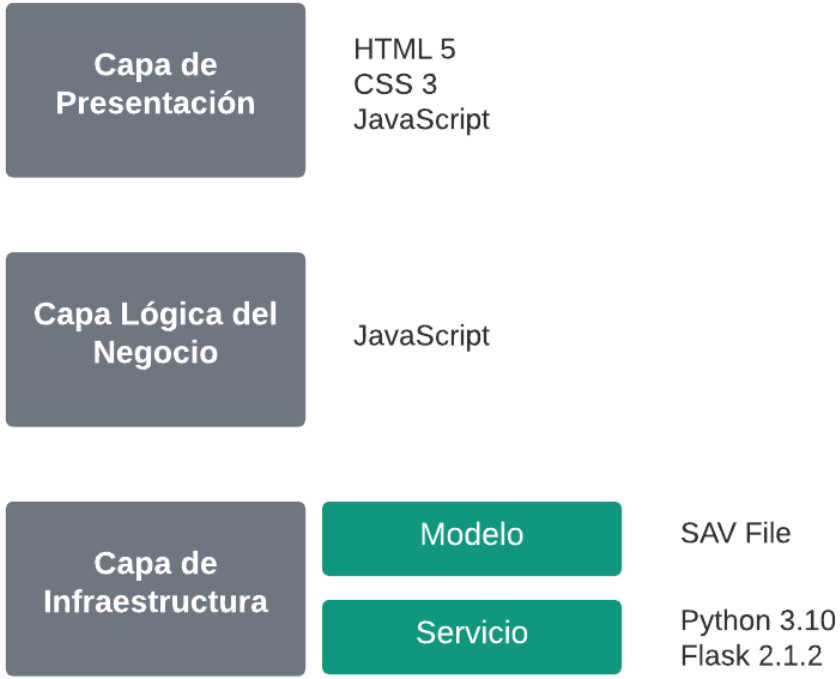
Historia de usuario 03
Quiero que el modelo de Machine Learning se encuentre almacenado en un servidor y pueda realizar predicciones a través de un servicio
Para tener un servicio que pueda ser utilizado en otras aplicaciones

Historia de usuario 04
Quiero una extensión para el navegador Google Chrome que me informe si un sitio web contiene phishing
Para determinar si estoy en un sitio web seguro mientras estoy navegando en la red con Google Chrome

Diseño del sistema

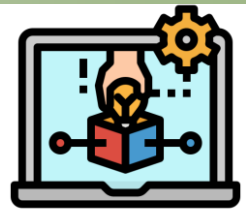
- Arquitectura Lógica con las tecnologías a usar.

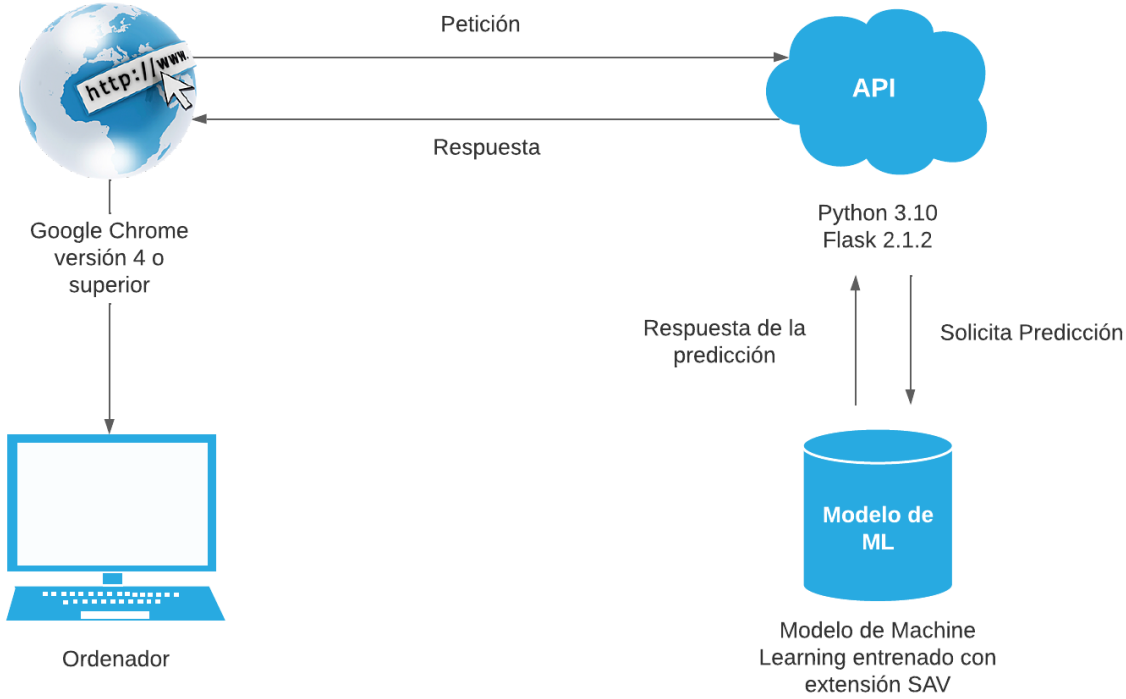




Diseño del sistema

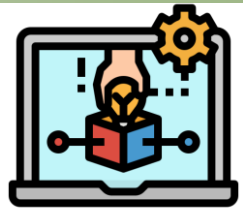
- Arquitectura Física

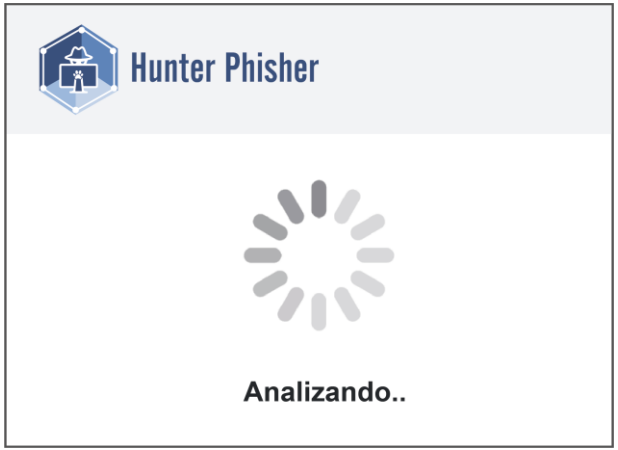




Diseño del sistema

- Mockups





Desarrollo del Sistema

- Resultado del Sprint 1: Selección del mejor modelo de Machine Learning

Algoritmos/Modelos	Accuracy	Precision	Recall
Random Forest	0,9725	0,9691	0,9821
Multi-layer Perceptron classifier	0,9688	0,9649	0,9797
Decision Tree	0,9617	0,9645	0,9670
Ada Boost	0,9325	0,9276	0,9534
SVM	0,9511	0,9444	0,9693
Bagging Random Forest	0,9708	0,9656	0,9828
Bagging Decision Tree	0,9688	0,9661	0,9784
Bagging Ada Boost	0,9326	0,9269	0,9544
Bagging SVM	0,9514	0,9470	0,9569

Dataset utilizado: Phishing Detection Using Machine Learning Techniques

https://github.com/fafal-abnir/phishing_detection/blob/master/dataset.csv

Desarrollo del Sistema

- Resultado del Sprint 2: Creación del Dataset

-1
Phishing

0
Sospechoso

1
Legítimo

Ord.	haveIp	lengthUrl	haveAtSymbol	sslState	domainAge
1	-1	1	1	-1	-1
2	1	1	1	1	-1
3	1	0	1	-1	1
4	1	0	1	-1	-1
5	1	0	1	1	-1

Características

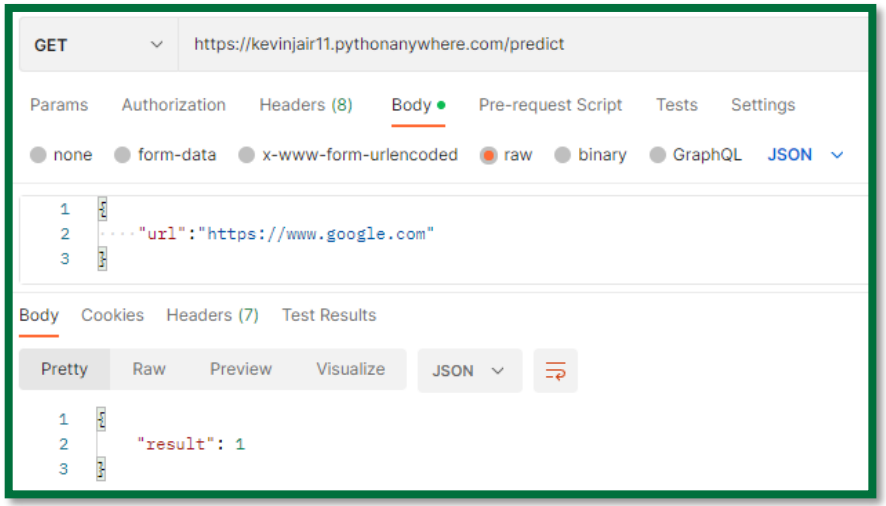
Dataset creado:

https://drive.google.com/file/d/1BEE9-4bGuQYk9M40JzqNGZJxUINjAM60/view?usp=sharing

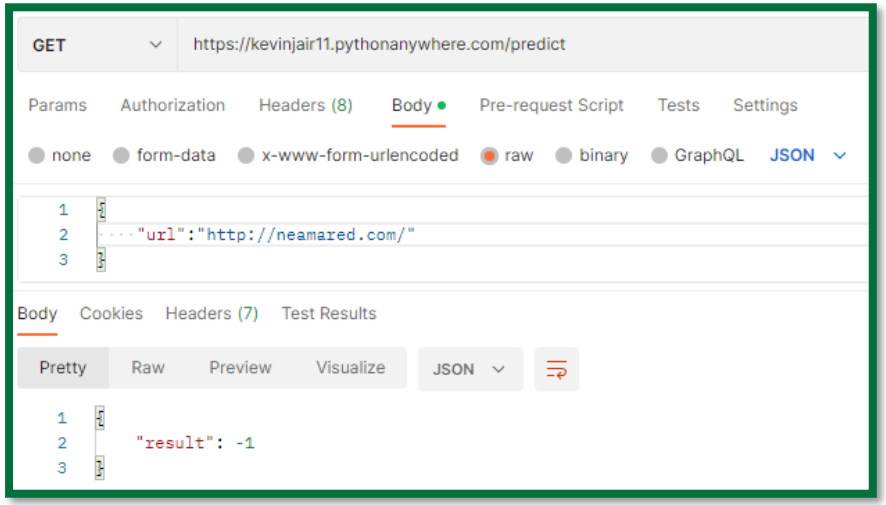
Desarrollo del Sistema

- Resultado del Sprint 3: Creación de la API

Sitio web con Phishing

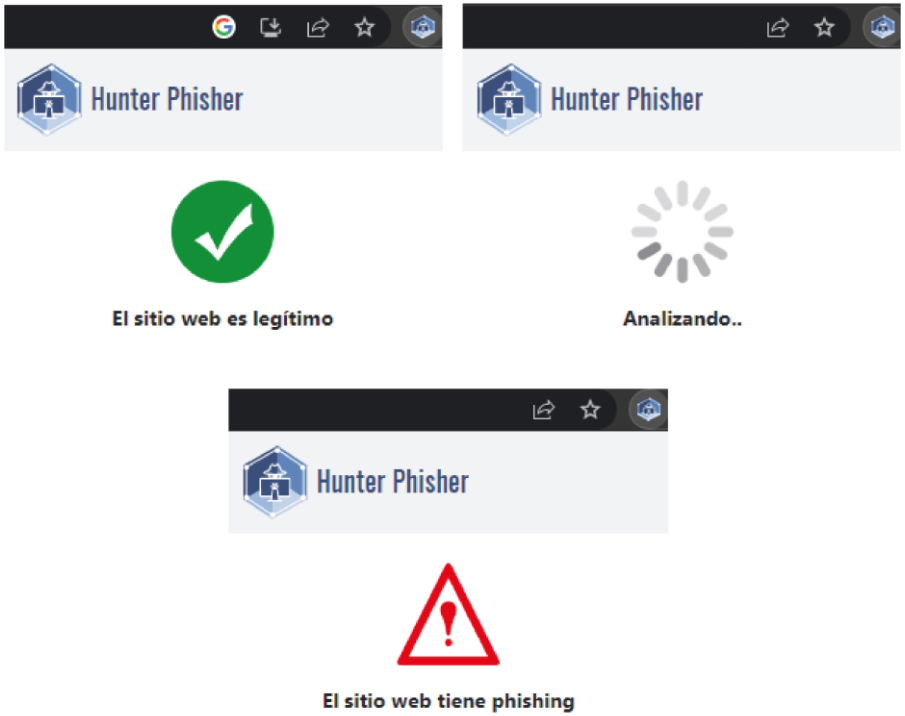


Sitio web Legítimo

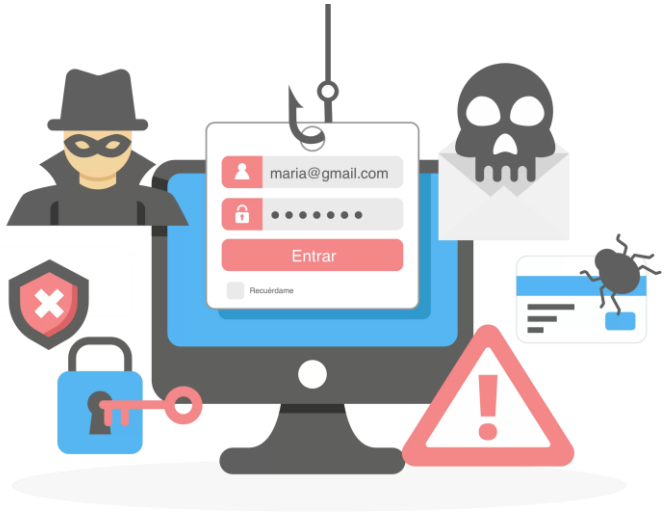


Desarrollo del Sistema

- Resultado del Sprint 4: Desarrollo de la Extensión de Google Chrome



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

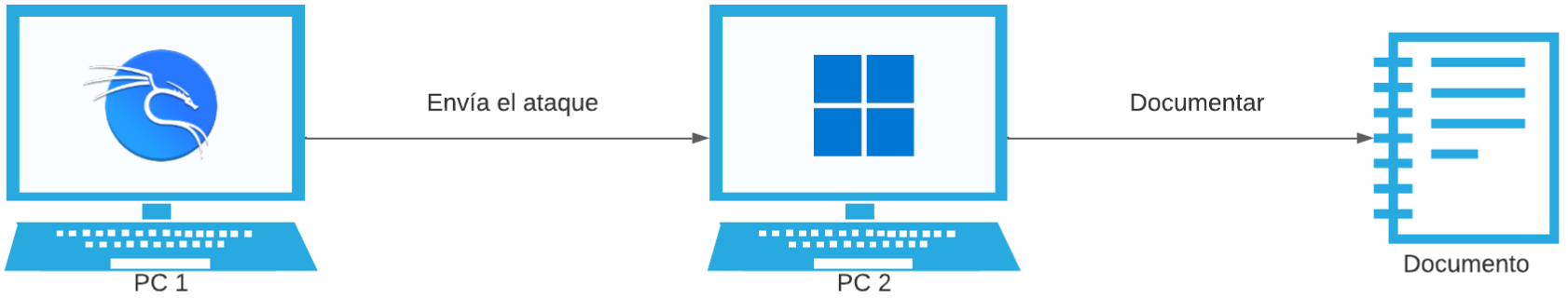


Validación del Sistema

- Uso de la herramienta Zphisher (ambiente simulado)

Validación del Sistema

- Proceso de ejecución de pruebas



Genera el sitio web con phishing con ayuda de la herramienta Zphisher

Escanea el sitio web con la extención de Google Chrome desarrollada (Hunter Phisher)

Se documenta el resultado obtenido para validar el sistema

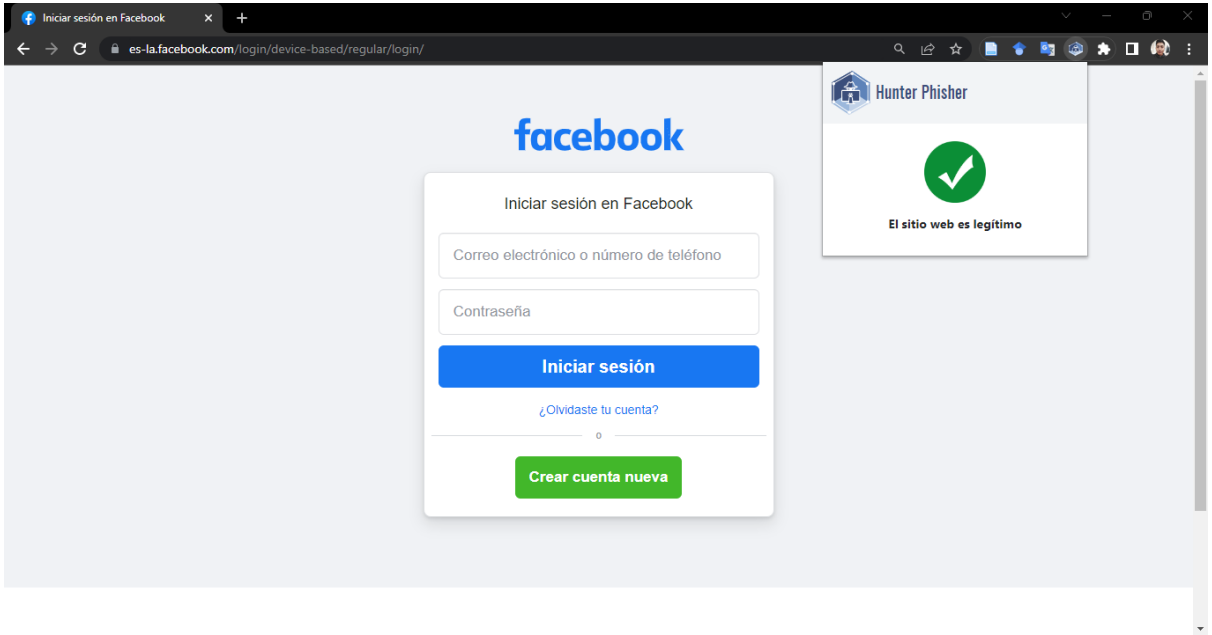
Validación del Sistema

- Se probó con 86 sitios web: 43 sitios web con phishing y 43 sitios web legítimos.

SITIO WEB	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING		PRUEBAS SITIOS WEB LEGÍTIMOS	
		RESULTADO ESPERADO	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Facebook	*Traditional Login Page*	Phishing	Phishing	Legítimo	Phishing
	Advanced Voting Poll Login Page	Phishing	Phishing	Legítimo	Phishing
	Fake Security Login Page	Phishing	Phishing	Legítimo	Phishing
	Facebook Messenger Login Page	Phishing	Phishing	Legítimo	Phishing

Validación del Sistema

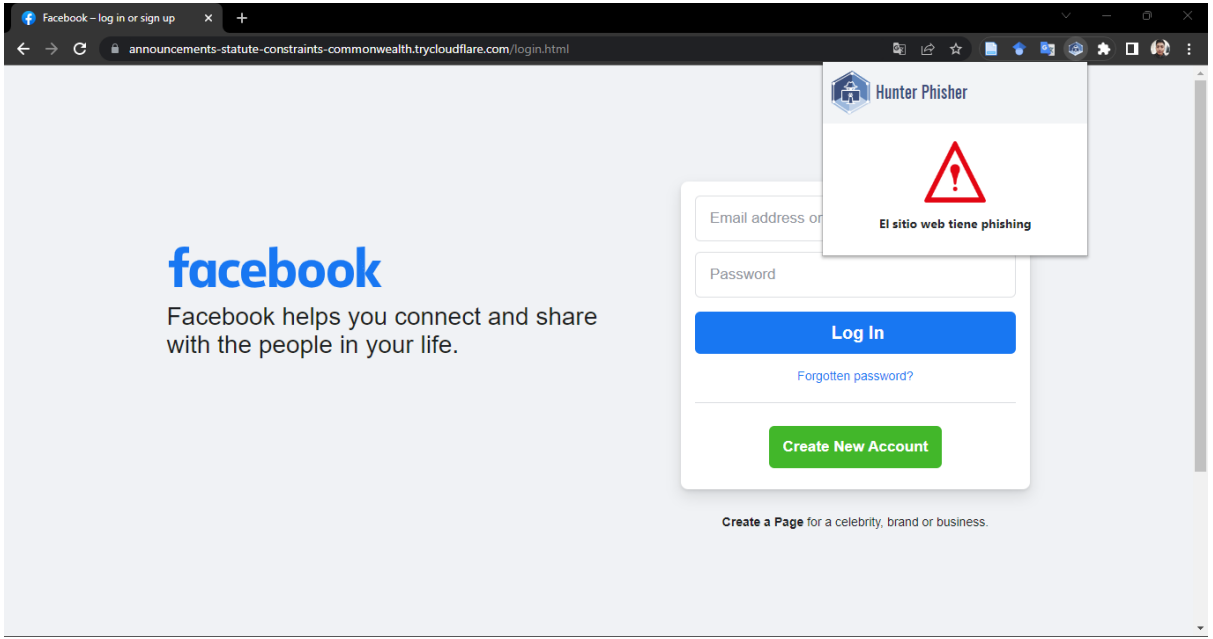
- Se muestra un análisis de un sitio web cuando es legítimo



URL: https://es-la.facebook.com/login/device-based/regular/login/

Validación del Sistema

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



URL: https://announcements-statute-constraints-commonwealth.trycloudflare.com

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	$accuracy = \frac{VP + VN}{VP + VN + FP + FN}$
PRECISION	$precision = \frac{VP}{VP + FP}$
RECALL	$recall = \frac{VP}{VP + FN}$

Validación del Sistema

- Obtención de las métricas de evaluación en los 3 modelos

	ETAPA DE ENTRENAMIENTO			CAMPO SIMULADO/REAL		
	ACCURACY	PRECISION	RECALL	ACCURACY	PRECISION	RECALL
Modelo Implementado	91,39% ±0,0853	93,88% ±0,0767	95,21% ±0,0770	50% ±0	50% ±0	100% ±0
Modelo primer Ajuste	94,25% ±0,0429	95,16% ±0,0554	96,38% ±0,0422	85,23% ±1,94	88,96% ±1,88	80,47% ±3,32
Modelo Segundo Ajuste	98,52% ±0,0484	98,43% ±0,0670	98,88% ±0,1761	91,98% ±0,8140	96,42% ±1,2092	87,21% ±1,1628

Análisis de resultados

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

- Se obtuvo en la métrica Accuracy el valor más alto de 93,02% y el más bajo con 90,70%, valores que están aproximadamente dentro de los valores encontrados en la literatura (92,18% y 91,46%) de Accuracy (Sönmez et al., 2018) (Chapla et al., 2019) respectivamente. Por lo tanto, el IDS implementado para evitar ataques Phishing presenta resultados que están dentro del rango aceptable de predicciones.

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

Conclusiones

El IDS desarrollado (Hunter Phishing) se entrenó con un dataset de 22.796 sitios web (7.444 sitios web con Phishing (32,65%) y 15.352 sitios web legítimos (67,35%)).

Se diseñó e implementó un sistema de detección de Phishing.

Para validar el IDS (Hunter Phisher) implementado se utilizó la herramienta Zphisher.

Conclusiones

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

La extensión desarrollada puede ser puesta en marcha en un entorno real, siempre y cuando exista un mecanismo que se encargue de recolectar en forma periódica nuevos ciber-ataques phishing para alimentar el dataset.

Referencias

- What is Scrum. (2022). *App Inlet*. https://appinlet.com/what-is-scrum/
- Chapla, H., Kotak, R., & Joiser, M. (2019). *A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifier.* 383-388. Scopus. https://doi.org/10.1109/ICCES45898.2019.9002145
- Sönmez, Y., Tuncer, T., Gökal, H., & Avci, E. (2018). *Phishing web sites features classification based on extreme learning machine. 2018-January*, 1-5. Scopus. https://doi.org/10.1109/ISDFS.2018.8355342

Software
DOMINA EL MUNDO

Gracias por su atención

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA