UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMA DE INFORMACIÓN

TEMA:

ANÁLISIS DE LA EVOLUCIÓN DE LAS TÉCNICAS DE PHISHING PARA LA CLONACIÓN DE PÁGINAS WEB

ESTUDIANTE:

EVA AZUCENA VACA ANGULO

TUTOR:

ING. LEON ACURIO JOFFRE VICENTE

MAYO 2023 - SEPTIEMBRE 2023

Contenido

Resumen

El propósito de este caso de estudio es estudiar y analizar la evolución de las diferentes técnicas de phishing empleadas en el web spoofing y para engañar a usuarios inadvertidos, debido a que el phishing es un ciberataque que tiene como objetivo obtener información confidencial haciéndose pasar por entidades legítimas, razón por la cual los diferentes ciberdelincuentes han adaptado sus estrategias para conseguir un mayor éxito en sus campañas de phishing a medida que avanza la tecnología.

El objetivo principal de este estudio es analizar la constante evolución de los métodos de phishing para la clonación de páginas web y cómo los ciberdelincuentes obtienen datos confidenciales de los usuarios, también se revisarán investigaciones previas en las que se evaluarán las herramientas y tácticas empleadas por los atacantes, así como cómo la ingeniería social y la personalización han sido utilizadas para incrementar la efectividad de los ataques.

Este caso de estudio proporcionará una completa visión de cómo han cambiado las técnicas de phishing para la clonación de páginas web permitiendo una mejor comprensión de las amenazas actuales, además de brindar información para así mejorar las estrategias de seguridad y concientizar a los usuarios sobre los riesgos asociados con el phishing.

Palabras claves: Phishing, Clonación de páginas web, Ciberataque, Spoofing

Summary

The purpose of this case study is to study and analyze the evolution of the different phishing techniques used in web spoofing and to deceive unaware users, because phishing is a cyber-attack that aims to obtain confidential information by pretending to be legitimate entities, which is why the different cybercriminals have adapted their strategies to greater success in their phishing campaigns as technology advances.

The main objective of this study is to analyze the constant evolution of phishing methods for cloning web pages and how cybercriminals obtain sensitive user data; it will also review previous investigations in which the tools and tactics used by attackers will be evaluated, as well as how social engineering and customization have been used to increase the effectiveness of attacks.

This case study will provide a comprehensive overview of how phishing techniques for cloning web pages have changed, allowing a better understanding of current threats, as well as providing information to improve security strategies and raise user awareness about the risks associated with phishing.

Keywords: Phishing, Web page cloning, Cyber-attack, Spoofing

Planteamiento del Problema

Los métodos de phishing empleados para llevar a cabo el spoofing web dentro del entorno de Kali Linux han experimentado un aumento y transformación en su enfoque, debido al incremento significativo en el riesgo al que se enfrentan los usuarios y la confidencialidad de sus datos personales, estos métodos de ataque han demostrado su capacidad para provocar a los usuarios a revelar inadvertidamente información confidencial como contraseñas y datos privados de diversas índoles.

La gravedad de esta problemática aumenta debido a la continua sofisticación de las técnicas empleadas por los ciberdelincuentes, ya que estos se tornan más astutos en sus enfoques, la probabilidad de que los usuarios caigan víctimas de estos engaños fraudulentos se incrementa, por lo que los resultados de estos ataques pueden llevar a diferentes consecuencias que van desde el robo de identidad hasta la pérdida irrecuperable de información valiosa.

Kali Linux es una distribución de Linux ampliamente utilizada en el ámbito de las pruebas de seguridad y el hacking ético la cual ha generado un nuevo conjunto de desafíos en la lucha contra el phishing y el spoofing web, puesto que originalmente estaba diseñada para actividades de ciberseguridad legítimas, esta ha sido aprovechada por diversos ciberdelincuentes para mejorar sus técnicas de ataque, debido a que Kali provee una base versátil y potente para la ejecución de este tipo de acciones maliciosas, dificultando así su detección por parte de las soluciones de seguridad convencionales.

Además, gracias al carácter de código abierto de Kali Linux es posible crear y modificar scripts y herramientas dentro de esta plataforma lo que significa que los diferentes métodos de phishing pueden evolucionar rápidamente, como resultado esta facilidad en la creación de nuevas técnicas de ataque mantiene a los proveedores de seguridad y a los usuarios en una constante

carrera para mantenerse actualizados e informados acerca de las amenazas y vulnerabilidades más recientes, exigiendo así una adopción de medidas preventivas adecuadas para enfrentar los diversos retos que presenta el panorama de la seguridad en línea.

Justificación

Debido al aumento de ciberataques refiriéndose especialmente al phishing y la clonación de páginas web también conocida como spoofing, la seguridad informática se ha convertido en una preocupación importante dentro del contexto actual, es por esta razón que este estudio se justifica por su gran importancia para comprender las diversas estrategias empleadas por los ciberdelincuentes en estos ataques y cómo Kali Linux puede potenciar y dificultar su detección.

La evolución constante de las tácticas de phishing requiere un análisis exhaustivo para mantenerse al tanto sobre sus nuevas variantes y técnicas, permitiendo desarrollar contramedidas más efectivas para prevenir y mitigar dichos ataques maliciosos, puesto que los diversos expertos en seguridad informática pueden reforzar las defensas y desarrollar soluciones adecuadas para detectar y contrarrestar estas acciones maliciosas al comprender cómo los ciberdelincuentes explotan esta plataforma para mejorar sus tácticas.

Este estudio va más allá del ámbito académico porque sus datos serán útiles para la industria de la seguridad informática, los proveedores de servicios y las organizaciones que buscan mejorar sus estrategias de protección y educación frente al phishing, ya que es importante concientizar a los usuarios sobre las tácticas de los delincuentes y las medidas preventivas necesarias en un entorno digital cada vez más amenazante.

Objetivos

Objetivo General

- Analizar la evolución de los métodos de phishing para la clonación de páginas web y cómo los ciberdelincuentes obtienen datos confidenciales de los usuarios.

Objetivos Especifico

- Realizar un análisis de las técnicas utilizadas por los ciberdelincuentes en el spoofing web.
- Examinar las herramientas empleadas por los criminales informáticos en ataques de phishing para la clonación de páginas web.
- Evaluar el papel de Kali Linux como una herramienta de seguridad informática en la potenciación de ataques de phishing y la clonación de páginas web.

Línea de Investigación

La línea de investigación a la que corresponde es Sistemas de información y comunicación, emprendimiento e innovación, sublínea Redes y tecnologías inteligentes de software y hardware porque aborda la evolución de los métodos de phishing y clonación de páginas web que dependen de tecnologías avanzadas y se propagan a través de redes de comunicación, estos métodos engañan a los usuarios y roban sus datos confidenciales utilizando técnicas sofisticadas como el cifrado de sitios web y la ingeniería social, ya que debido a que estos ataques se propagan a través de redes de comunicación como correo electrónico, SMS y redes sociales, es fundamental investigar cómo se propagan e interactúan en el mundo digital.

También es relevante analizar cómo se es posible fortalecer la resiliencia de las redes y la infraestructura de comunicación mediante medidas de ciberseguridad avanzadas, como la encriptación y la autenticación segura, para así evitar el acceso no autorizado a sitios web y datos confidenciales, facilitando la identificación de intentos de phishing de manera más efectiva dentro de la sublínea de redes y tecnologías inteligentes.

Marco Conceptual

Ciberataques

Como afirma Páez (2020) debido a la gran expansión que han tenido las TICs a lo largo del tiempo estas han influenciado significativamente en la difusión de información y datos a través de rede gracias a la utilización del internet y sus diferentes protocolos, este incremento de datos da paso a un crecimiento de riesgo para los diversos activos críticos de las diferentes organizaciones o Estados ya sea la integridad, confidencialidad y disponibilidad de los datos a través de ataques de TICs, dirigidos por intrusiones no autorizadas, los cuales van incrementando a la par del mismo desarrollo tecnológico afectando directamente a los administradores de aplicaciones, como lo son los servicios financieros, entidades gubernamentales, proveedores de servicios de salud, entre otros (p.117).

Como señala Cano (2020) la información está compuesta por un conjunto de datos organizados los cuales forman parte de uno de los principales activos de todas las organizaciones en general y esto a su vez convierte su seguridad en un punto crítico, debido a que la mayoría de datos que la componen se encuentran alojadas en el ciberespacio, el cual se representa como un entorno virtual, fuera de la naturaleza física y gran aporte al desarrollo es realmente indiscutible pero en consecuencia su mal uso es posible y evidente actualmente razón por la cual han aparecido medidas conocidas como ciberdefensa, técnicas que tienen como objetivo la seguridad y defensa de activos fundamentales de algún estado u organización (p.70).

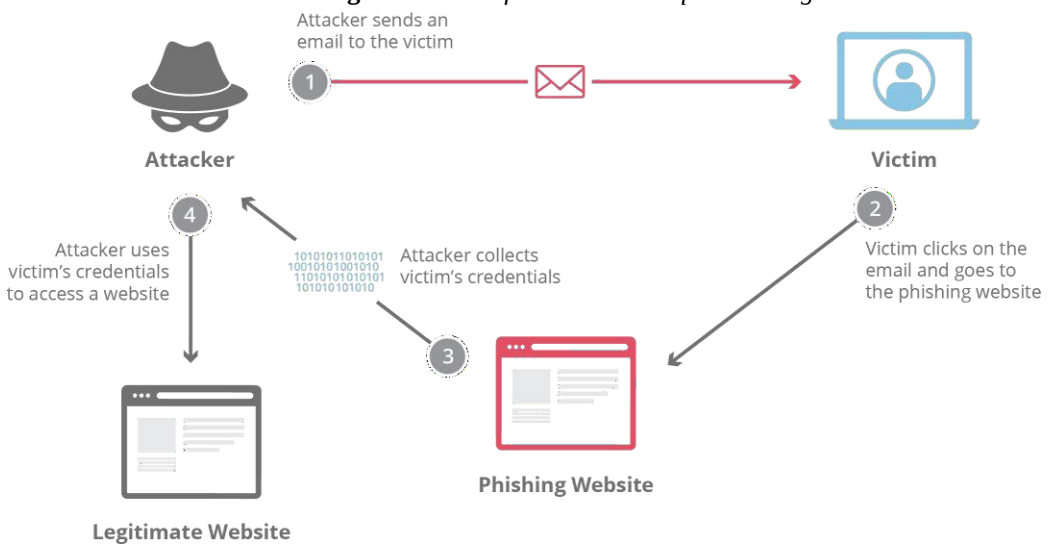
Phishing

Como mencionó Amo (2022) el phishing es uno de los ataques de ingeniería social más comunes utilizados por los ciberdelincuentes de todo el mundo para engañar a los usuarios, obtener información confidencial, privada y personal, especialmente información bancaria, por esta razón,

existen innumerables estudios y literaturas científicas sobre tipos de phishing, métodos de análisis, detección, prevención de ataques, casos de estudio específicos, trabajos futuros y posibles soluciones en la actualidad.

Estas formas de prevención están en constantes cambios, por lo que los investigadores deben analizarlos detalladamente, ya que los atacantes, además del aumento del número de computadoras en internet, utilizan cada vez más nuevas tecnologías que dificultan la prevención o reducen el riesgo de daño, dispositivos móviles e Internet de las Cosas, lo que hace que los datos y las credenciales de los usuarios sean más vulnerables a ataques en infraestructuras y organizaciones potencialmente vulnerables. (p. 27).

Figura 1. *Como funciona un Ataque Phishing.*



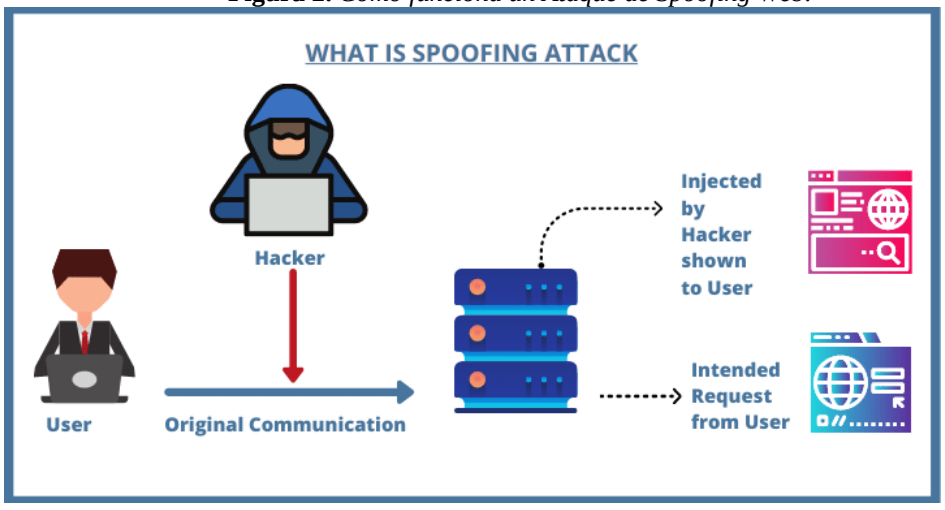
Clonación de Páginas Web

Como señala Castro (2022) la tecnología ha sido un factor determinante para el desarrollo de la humanidad, debido a que ha permitido poder resolver necesidades muy complejas como dispositivos que reemplazan órganos humanos o procesos un poco más sencillos como las tecnologías que facilitan las interacciones entre personas sin importar su ubicación, pero asi como

estos avances han traido ventajas a la actulidad, tambien, han desembocado varias vulnerabilidades las cuales han sido desarrolladas y perfeccionas por los ciberdelincuentes para buscar beneficios económicos o simplemente generar afectaciones en organizaciones y personas, por estas razon es fundamental que las personas y diferentes organizaciones comprendan las consecuencias que pueden sucitar al ser victima de un Domain Spoofing attack para asi tomar precauciones y lograr prevenirlas.

Uno de los ataques de Phishing más reconocidos actualmente por su fácil ejecución y explotación son los Domain Spoofing Attack los cuales consisten en la suplantacion de un sitio web real buscando que la víctima ingrese información sensible que permita al ciberdelincuente obtenerla, explotarla y aprovechada para sus fechorías, entre los más destacados, extorsiones por información sensible y accesos no autorizados a plataformas o bancos.

Figura 2. *Como funciona un Ataque de Spoofing Web.*



Kali Linux

Según Elizalde (2021) Kali Linux es una distribución de código abierto cuyo objetivo principal es realizar pruebas de penetración y auditoría informática, además dispone de

herramientas para realizar todo de manera integral, desde pruebas de penetración, análisis forense, seguridad de la información, ingeniería inversa y auditoría informática.

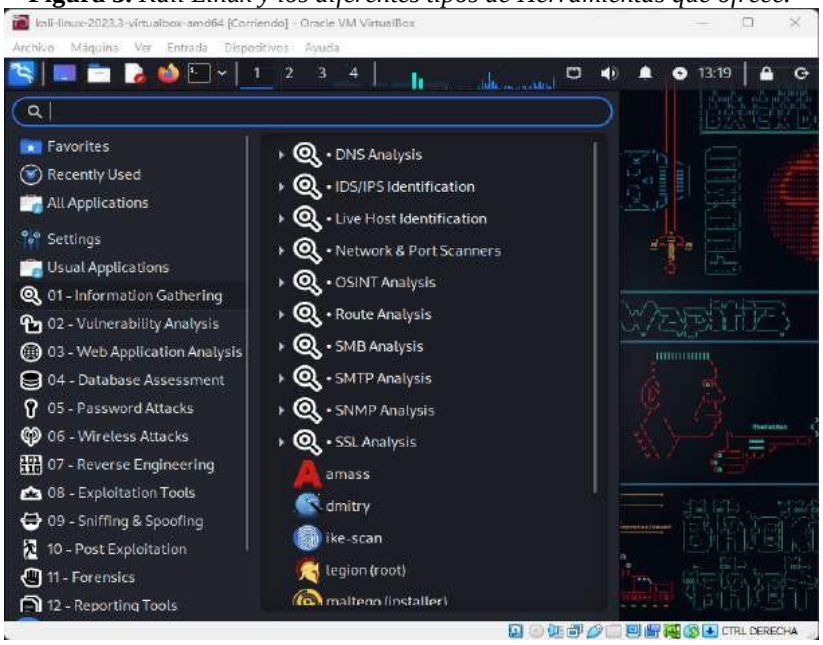
Ha recorrido un largo camino, basado en un proceso de muchos años lleno de conocimiento y experiencia para adaptar las bases de un sistema operativo dedicado al hacking ético, logrado a través de varios proyectos, sin casi ningún cambio entre los desarrolladores ya que el equipo ha sido muy pequeño, en el transcurso de tiempo con la experiencia obtenida, construyeron con éxito Kali Linux utilizando Debian como motor y lo desarrollaron desde cero hasta que hicieron la transición exitosa a las pruebas de Debian y convirtieron a Kali en un sistema operativo rodante. (p. 38)

Tabla 1. *Categorías de Herramientas de Kali Linux.*

Categoría	**Herramientas**
Recopilación de Información	Recopilar información de DNS, IDS/IPS, escáner de redes, análisis de ruteo, SMB, SSL, SMTP, SNMP, OSINT.
Análisis de Vulnerabilidades	Analizar vulnerabilidades en general, evalúa redes Cisco, vulnerabilidad en diversos servidores de base de datos y herramientas de fuzzing.
Análisis de Aplicaciones Web	Escáner de vulnerabilidades Web, identificador Web y CMS, rastreadores web, explotación de base de datos, los proxies de aplicaciones web.
Evaluación de Base de Datos	Probar la seguridad de las bases de datos SQL.
Ataques de contraseñas	Realiza ataques de contraseña Online u Offline y genera diccionarios para vulnerar los hosts.
Ataques Wireless	Realiza ataques a redes Bluetooth y dispositivos inalámbricos.

Ingeniería Inversa	Depurar un programa o desensamblar un archivo ejecutable.
Herramientas de Explotación	Explotar vulnerabilidades en una red, web o base de datos. También realiza ataques de ingeniería social.
Sniffing & Spoofing	Capturar tráfico de red y web. También incluye Spoofing de red como Ettercap.
Post Exploitación	Mantiene el acceso a la máquina destino. También cuenta con tunelización y backdooring.
Análisis forense	Actividades de forenses digitales como la recopilación y exhaustivo peritaje de datos.

Figura 3. *Kali Linux y los diferentes tipos de Herramientas que ofrece.*



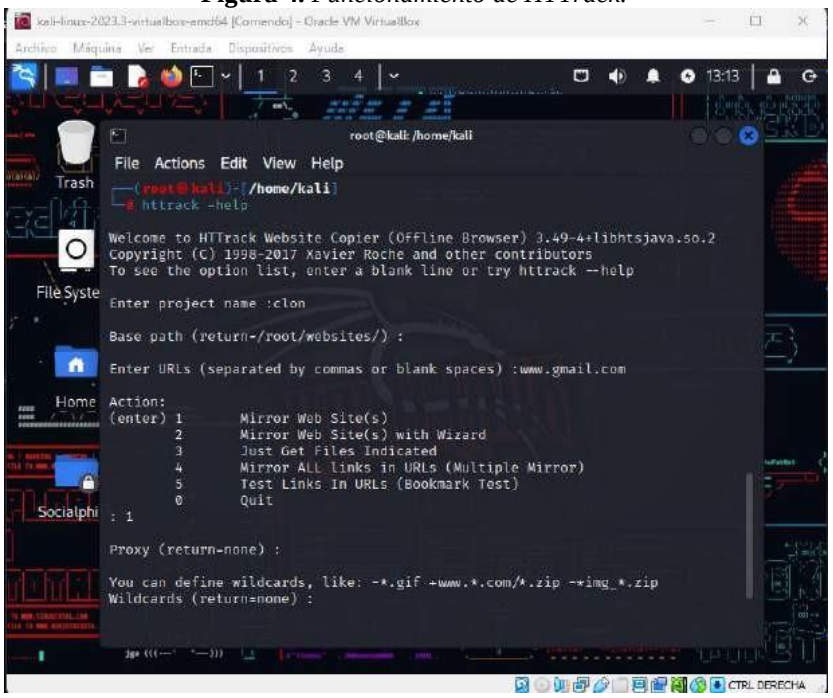
HTTrack

Desde el punto de vista de Leite et al (2023) HTTrack es un rastreador web y un navegador sin conexión de código abierto y gratuito que permite a los usuarios descargar sitios World Wide

Web desde computadora a través de internet, esta herramienta se encarga de ordenar todos los sitios descargados según su estructura de enlaces relativa al sitio original, donde los sitios web reflejados se pueden ver abriendo las páginas del sitio en un navegador.

También ofrece la posibilidad de actualizar las páginas espejo existentes y reanudar las descargas interrumpidas, además esta es ampliamente configurable con opciones y filtros (incluir/excluir), existiendo varias versiones diferentes de la misma como una versión básica de línea de comandos y dos versiones de GUI (WinHTTrack y WebHTTrack) (p.8).

Figura 4. *Funcionamiento de HTTrack.*

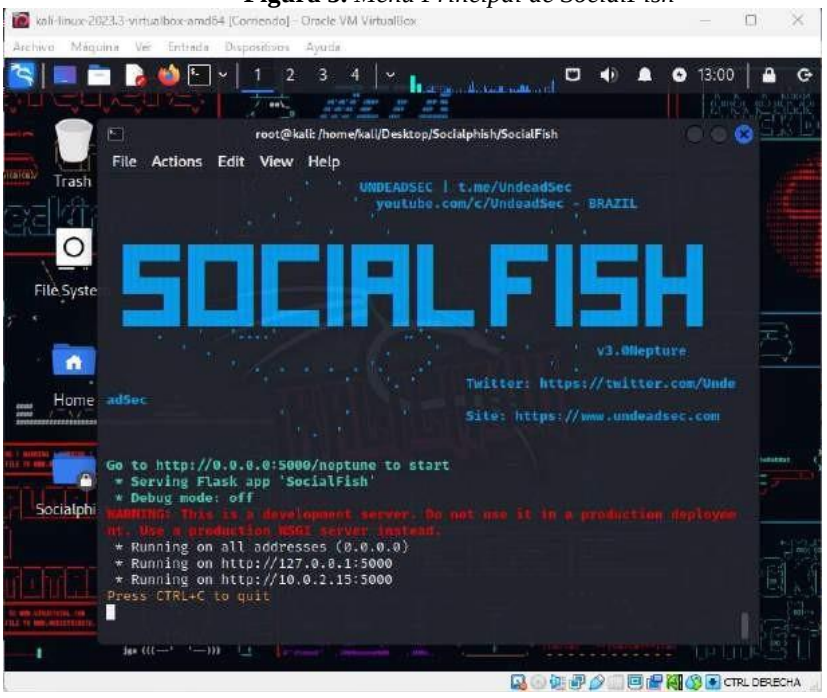


SocialFish

Como señalan Ariani & Jayanti (2023) SocialFish es una poderosa herramienta de código abierto encargada en el phishing, la cual se ha convertido en una alternativa muy popular para hacer ataques de phishing en Target, puesto que SocialFish ofrece un amplio kit de herramientas basadas en la ingeniería social haciéndola más fácil de usar, debido a que contiene algunas plantillas generadas por otras herramientas para phishing y páginas web.

Esta potente herramienta es capaz de generar más de 33 sitios populares como Facebook, Instagram, Google, Snapchat, Github, Yahoo, Protonmail, Spotify, Netflix, Linkedin, WordPress, Origin, Steam, Microsoft, etc. Además de esto SocialFish ofrece la opción de emplear plantillas personalizadas si alguien lo desea, facilitando la realización de un ataque de phishing debido a que los atacantes disponen de mucha creatividad para que el correo electrónico parezca lo más legítimo posible. (p.24).

Figura 5. *Menú Principal de SocialFish*

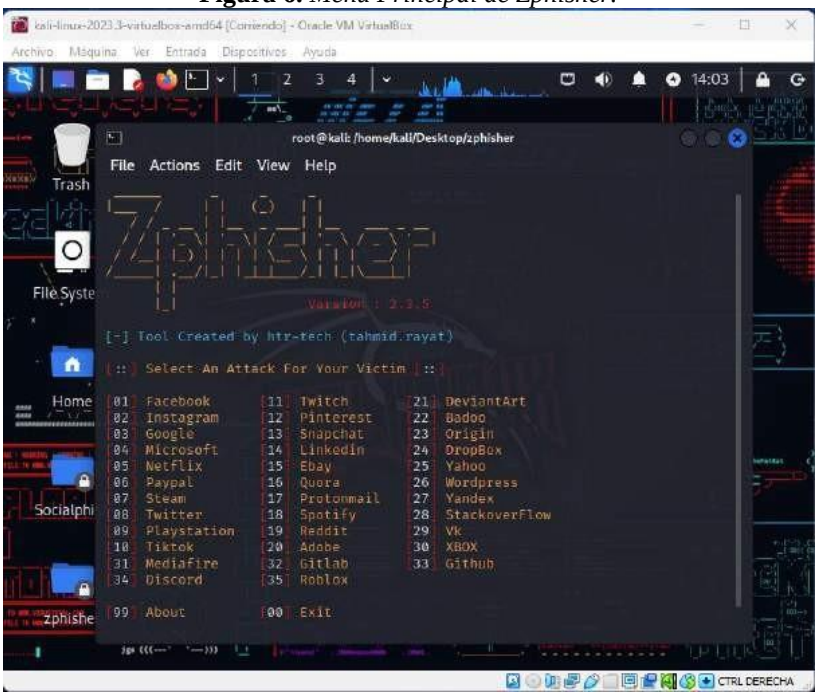


Zphisher

Zphisher es una potente herramienta de phishing de código abierto, la cual se esta haciendo muy conocida hoy en día debido a su facilidad para realizar ataques de phishing en comparación al Social Engineering Toolkit, esta dispone de varias plantillas para realizar diversosn ataques a paginas web conocidas como los son Facebook, Instagram, Google, Snapchat, GitHub, etc, esta a su vez ofrece la posiblidad de emplear plantillas personalizadas si el susario lo desea.

Desde el punto de vista de Wahyuni et al (2023) esta herramienta favorece la realización de ataques de phishing, a traves del uso de sus diferentes opciones o funcionalidades, permitiendo obtener credenciales como IDs o contraseñas, funcionando eficazmente al momento de realizar pruebas o experimentos de phishing debido a su practicidad y facil manejo, ademas de su rapida respuesta en cada solicitud realizada tardando alrededor de 14,14 segundos en mostrar un enlace de phishing (p.25).

Figura 6. *Menú Principal de Zphisher.*

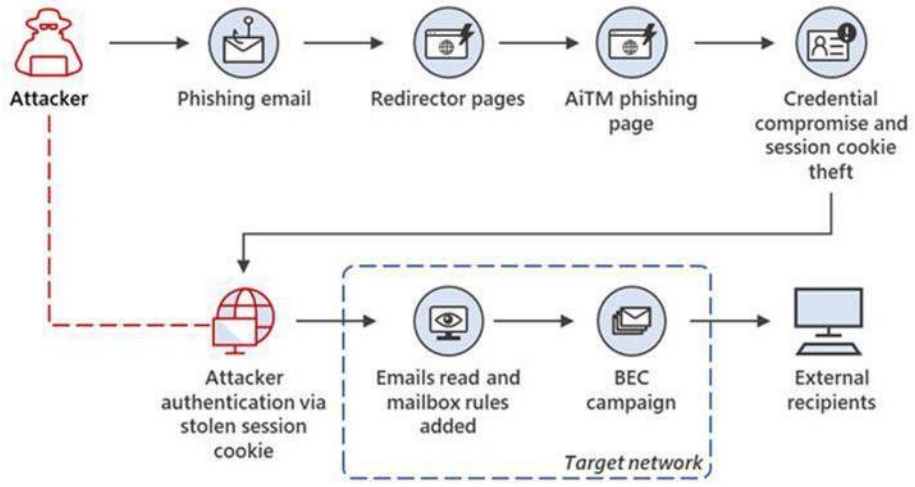


Ingeniería Social en Ataques de Phishing.

Como señalan Benavides et al (2020) la ingeniería Social es el acto de obtener información importante de las personas fraudulentamente con la finalidad de usar esa misma información en contra de ellas o de sus organizaciones, actualmente existen diversas maneras de realizar este ataque pero la manera más utilizada es mediante el uso de Phishing, puesto que este es un ataque de Ingeniería Social, el cual busca obtener esta información sensible por medios electrónicos, popularmente a través de Phishing Emails y por Phishing Websites (p.98).

El objetivo principal del Phisher (Persona que realiza el Phishing) según Bogantes (2020) es estafar a una persona para así poder obtener una retribución económica, debido a que en la actualidad no existe un estudio completo, que permita conocer todo sobre los ataques de Phishing, sus características y las maneras para mitigarlos, es importante promover programas de capacitación y concientización en la comunidades para poder aplicar buenas prácticas tecnológicas y minimizar el impacto de la reincidencia de estos delitos informáticos (p.25).

Figura 7. *Proceso del Phishing.*



Detección de Phishing

Etapas de detección

Como opinan Starov et al (2019) el phishing no es un tema especialmente nuevo debido a que este siempre se encuentra en constante evolución por esta razón se han venido desarrollando e implementando diferentes tipos de mecanismos que buscan identificar y bloquear posibles ataques de phishing, donde incluso se han creado comunidades que tratan de luchar contra el fraude como es el caso de APWG, las cuales cada trimestre están publicando reportes del comportamiento de los ataques de phishing donde al compararlo con lo que era el phishing en el 2005 se observa como

el crecimiento tecnológico ha complicado en diferentes maneras el panorama del análisis de phishing (p.221).

Estudios como Yang et al (2019) se enfocan en corroborar los ataques de phishing a través de las URL implementadas debido a que son un medio de ataque existente y popular actualmente, debido a que es posible que muchas personas hayan recibido el mismo URL o enlace, mientras que otras han recibido instrucciones para evitar caer en esta estafa, mientras que otras investigaciones a su vez se enfocan en desarrollar algoritmos de generación de dominios las cuales pueden funcionar en tiempo cero identificando posibles ataques de phishing incluso antes de que se implemente dicho acceso, aunque en realidad existen diversos métodos de detección al final todos están diseñados para detectar la fuente y las técnicas utilizadas (p.15197).

Etapa de prevención

Desde el punto de vista de Nakamura & Dobashi (2019) esta etapa es perfecta para las diversas aplicaciones que realmente desean evitar que el phishing se propague antes de que llegue a los usuarios, fomentando una cultura de la seguridad informática para proteger la información confidencial y la seguridad de los datos, debido a que estos participan dentro de los dominios recientemente registrados además de dominios generados a partir de palabras clave (p.446).

Etapa de difusión

Como opinan Balim & Gunal (2019) esta etapa esta estrechamente relacionada con los diferentes metodos por los cuales el phishing llega a los usuarios finales como por ejemplo posria ser cuando algun atacante envía un SMS haciendose pasar por un banco o alguna institución a cientos de personas tras haber obtenido sus números comprando alguna base de datos robada ya con eso el atacante pueda robar datos bancarios o mas información sensible (p.2).

Etapa de mitigación

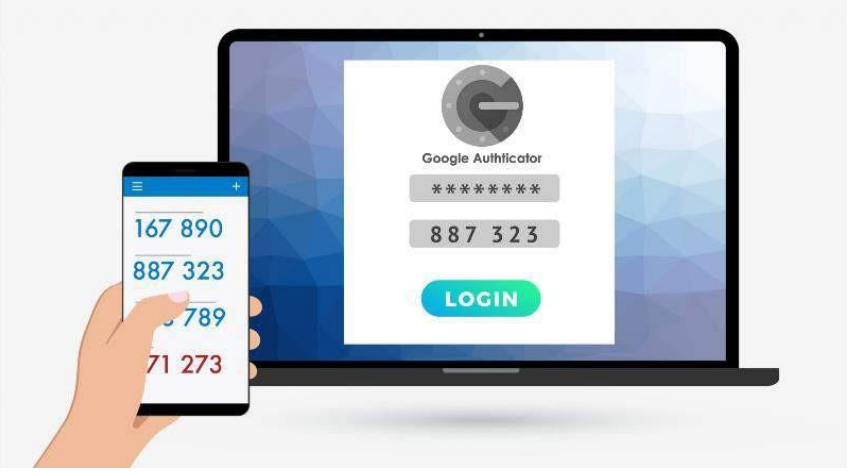
De acuerdo con Eshmawi & Nair (2019) en esta etapa participan todos los procesos cuyos modelos se basan en bases de datos comunitarias o URL informadas puesto que actúan sobre enlaces ya desplegados o reportadas previamente por usuarios para así poder instaurar políticas de seguridad que ayuden a la detección y bloqueo de diferentes archivos adjuntos maliciosos lo cuales muchas veces propagan el ataque (p.3).

Autenticación de Dos Factores (2FA)

Como señalan Vaca et al (2019) se conoce que actualmente la autenticación a través de nombre de usuario y contraseña es lo más común en los sistemas o aplicaciones, pero esta manera de protección contiene una inmensa brecha de seguridad ya sea por contraseñas no tan robustas, repetidas o suplantaciones de identidad, por todas estas razones es que se han buscado nuevas formas para que los usuarios se autentiquen de una manera rápida y segura, por lo que surgió la autenticación de dos factores la cual se ha convertido en un estándar de protección en internet, debido a que genera un elevado nivel de seguridad (p.24).

Puesto que la autenticación de dos factores no es un método infalible, de acuerdo con Sciarretta et al (2020) es una muy buena alternativa para prevenir los accesos no deseados en las cuentas online, ya que es de público conocimiento que las contraseñas tienen un doble filo puesto que las más débiles son fáciles de recordar pero muy fáciles de descifrar, mientras las más fuertes pueden ser difíciles de adivinar, pero son difíciles de recordar, por estas razones la autenticación de dos factores esencialmente logra que un atacante no solo tenga que descubrir la contraseña de los usuarios sino también tenga que acceder a segundo factor el cual es mucho más difícil de conseguir o replicar (p.21).

Figura 8. *Autenticación de Dos Factores de Google.*



Regulaciones y Cumplimiento en Ciberseguridad

Teniendo en cuenta a Coulombie (2020) debido a que la digitalización de los diferentes sistemas de gestión son algo constante dentro de las organizaciones, esto obliga cada vez más a garantizar el cumplimiento en ciberseguridad para así prevenir diferentes amenazas las cuales siempre se encuentran en constante evolución, puesto que hoy en día el cumplimiento de ciberseguridad es una necesidad para todas las empresas, debido a que les ofrece una mayor defensa contra amenaza, además de proteger todo su ecosistema digital y ofrecer una ventaja competitiva.

Como medida de protección para los datos e información sobre los clientes, las empresas optan por implementar diferentes medidas de ciberseguridad, como lo son la adopción de políticas de seguridad y la implementación de tecnologías de protección, además de realizar auditorías de seguridad para así detectar posibles vulnerabilidades en el entorno, por esta razón es importante que todas las organizaciones estén al tanto de los avances en las prácticas de ciberseguridad para así garantizar estén al día y sean efectivos (p.383).

Marco Metodológico

El desarrollo de este estudio sobre la evolución de las técnicas de phishing para la clonación de páginas web se basa en una metodología integral que combina enfoques cualitativos y comparativos. Inicialmente, se realizará una recopilación exhaustiva de información a través de informes de seguridad, investigaciones y estudios de casos relacionados con ataques de phishing y clonación de páginas web. Este proceso permitirá obtener una visión detallada y actualizada de las tácticas utilizadas por los ciberdelincuentes.

Una vez recopilada la información, se llevará a cabo un análisis cualitativo de casos reales de ataques de phishing. Estos casos se seleccionarán cuidadosamente de fuentes confiables y se analizarán en profundidad para identificar patrones, técnicas y enfoques utilizados por los atacantes a lo largo del tiempo. Este enfoque cualitativo permitirá comprender las estrategias subyacentes y las adaptaciones realizadas por los ciberdelincuentes.

Además, se realizarán entrevistas con expertos en seguridad informática y ciberseguridad. Estas entrevistas aportarán perspectivas valiosas sobre las tendencias actuales y la evolución de las técnicas de phishing. Los comentarios y opiniones de estos expertos enriquecerán la comprensión de cómo los ciberdelincuentes han cambiado sus enfoques y cómo esto ha afectado la seguridad informática en general.

La metodología también incluirá un análisis comparativo, donde se contrastarán los resultados obtenidos del análisis cualitativo de casos, las entrevistas con expertos y la revisión de la literatura especializada. Esto permitirá identificar convergencias y discrepancias en las tendencias observadas, brindando una imagen completa de la evolución de las técnicas de phishing.

En última instancia, basándose en la información recopilada y los análisis realizados, se propondrán recomendaciones concretas y medidas de seguridad efectivas para prevenir y mitigar los ataques de phishing y clonación de páginas web. Esta metodología integrada garantizará una comprensión holística de cómo las tácticas de phishing han evolucionado y cómo enfrentar adecuadamente esta creciente amenaza en el mundo digital.

Resultados

Después de realizar un exhaustivo análisis detallado de las técnicas de clonación de páginas web empleadas por los ciberdelincuentes se encontró que hacen uso de la identificación y documentación de métodos específicos como la manipulación de URLs, la creación de formularios falsos, redirecciones engañosas y otros enfoques empleados para engañar a los usuarios y así obtener información sensible.

Tabla 2. T*écnicas utilizadas por los ciberdelincuentes en la clonación de páginas web.*

Técnica	Descripción
Manipulación de URLs	Modificación de la dirección URL de la página para que se parezca a la de un sitio legítimo.
Creación de Formularios Falsos	Creación de formularios que imitan los campos de inicio de sesión o detalles personales.
Redirecciones Engañosas	Utilización de redirecciones falsas para llevar a los usuarios desde sitios legítimos a réplicas falsas.
Ataques Man-in-the-Middle (MITM)	Intercepción de la comunicación entre el usuario y el sitio legítimo para redirigirla a servidores falsos.
Uso de Contenido Falso	Rellenar las páginas falsas con contenido convincente, como logotipos y elementos de diseño similares.

Dentro de las herramientas más recientes utilizadas por los ciberdelincuentes en ataques de phishing y spoofing web, se encontró que las más relevantes eran "SocialFish", “HTTrack” y "Zphisher", debido a que cada una ofrece una funcionalidad diferente, características adicionales, además de capacidades particulares, las cuales contribuyen a la sofisticación de los ataques.

Tabla 2. *Comparación de las herramientas de phishing y spoofing web estudiadas.*

Característica	**SocialFish**	**HTTrack**	**Zphisher**
Tipo de Herramienta	Phishing y Clonación de Redes Sociales	Descarga de Sitios Web	Phishing y Clonación de Páginas Web
Interfaz de Usuario	Interfaz de línea de comandos y web	Interfaz de línea de comandos	Interfaz de línea de comandos
Fácil de Usar	Sí	Sí	Sí
Phishing de Redes Sociales	Sí	No	No
Clonación de Páginas Web	No	Sí	Sí
Personalización	Amplia gama de plantillas personalizables	Personalizable	Plantillas personalizables
Seguridad	Herramienta de hacking ético, debe usarse legalmente	Herramienta de descarga legítima	Herramienta de hacking ético, debe usarse legalmente
Comunidad de Usuarios	Comunidad activa en GitHub	Comunidad activa en el foro	Comunidad activa en GitHub

Se descubrió que el papel de Kali Linux dentro de la potenciación de ataques de phishing y spoofing web es muy importante debido a que debido a sus características y herramientas las cuales fueron originalmente diseñadas para pruebas de seguridad también pueden ser empleadas por los ciberdelincuentes, facilitando la realización de ataques y dificultando su detección por parte de sistemas de seguridad.

Tabla 3. *Puntos claves de la potenciación de ataques de phishing y spoofing web por parte de Kali Linux*

Puntos claves	**Descripción**
Versatilidad	Es una distribución de Linux diseñada para pruebas de seguridad, pero también la hace atractiva para ciberdelincuentes.
Amplia Gama de Herramientas	Incluye una amplia variedad de herramientas de hacking y pruebas de penetración las cuales pueden ser utilizadas en ataques de phishing.
Acceso a Herramientas de Clonación	Herramientas como "HTTrack" pueden ser instaladas en Kali Linux para clonar páginas web con fines maliciosos.

Facilita la Creación de Ataques	Kali Linux proporciona un entorno propicio para desarrollar y ejecutar ataques de phishing y clonación de páginas web con facilidad.
Dificulta la Detección	Algunas herramientas en Kali Linux pueden eludir las defensas de seguridad tradicionales, lo que dificulta la detección de ataques.
Actualización Constante	Se actualiza regularmente con nuevas herramientas y exploits, lo que mantiene a los ciberdelincuentes al día con las vulnerabilidades más recientes.
Uso Ético vs. Malicioso	Aunque Kali Linux está diseñada para el hacking ético, su disponibilidad pública significa que también puede ser utilizada de manera maliciosa.
Responsabilidad del Usuario	La ética del uso de Kali Linux recae en el usuario; es crucial utilizarla de manera legal y ética con permiso explícito.

Discusión de Resultados

La evolución de las técnicas de clonación de páginas web en el contexto de Kali Linux refleja una transformación significativa en la forma en que los ciberdelincuentes abordan el proceso de crear réplicas falsas de sitios web legítimos, debido a que a medida que la tecnología ha avanzado y las herramientas disponibles en Kali Linux se han vuelto más accesibles, la clonación de páginas web se ha vuelto más sofisticada y peligrosa en términos de su potencial para engañar a los usuarios y comprometer la seguridad en línea.

En sus inicios, las técnicas de clonación de páginas web en Kali Linux se centraban en la duplicación básica de contenido y la modificación manual de enlaces para dirigir a los usuarios a sitios fraudulentos, sin embargo, con el tiempo, se observa un cambio hacia la utilización de herramientas más avanzadas que permiten la replicación completa de la estructura y funcionalidad de sitios web legítimos, por lo que esto ha resultado en la creación de páginas falsas que son visualmente indistinguibles de sus contrapartes genuinas, lo que aumenta la probabilidad de éxito en los ataques.

La clonación de páginas web también se ha vuelto más personalizada y adaptativa, debido a que las herramientas disponibles en Kali Linux facilitan la creación de páginas de phishing que imitan plataformas populares, como redes sociales o servicios bancarios, lo que aprovecha la familiaridad de los usuarios con esas interfaces, además de la incorporación de elementos de ingeniería social, como imágenes personalizadas y contenido convincente, aumenta la autenticidad percibida de las páginas falsas y dificulta aún más la detección por parte de los usuarios.

En consonancia con la tendencia general en la ciberseguridad, la automatización ha desempeñado un papel esencial en la evolución de las técnicas de clonación de páginas web en

Kali Linux, puesto que los scripts y herramientas automatizadas permiten a los atacantes replicar páginas web en poco tiempo y con un grado de detalle que habría sido difícil de lograr manualmente agilizando el proceso de creación de sitios fraudulentos y aumenta el volumen de ataques potenciales.

No obstante, esta evolución no está exenta de desafíos, ya que a medida que las tácticas de clonación de páginas web se vuelven más avanzadas, también lo hacen los diversos métodos de seguridad y detección, donde las organizaciones y los proveedores de seguridad están tomando medidas para educar a los usuarios, implementar sistemas de detección avanzados y adoptar prácticas de autenticación más sólidas para mitigar los riesgos asociados con la clonación de páginas web.

Conclusiones

En el transcurso de este proyecto, se ha llevado a cabo un análisis exhaustivo de las técnicas de clonación de páginas web utilizando herramientas disponibles en Kali Linux, a través de esta experiencia, se ha podido constatar cómo estas técnicas han evolucionado de manera significativa en respuesta a los avances tecnológicos y las necesidades de los ciberdelincuentes.

Al trabajar directamente con herramientas como SocialFish, Zphisher y otras presentes en Kali Linux, se ha observado cómo la clonación de páginas web ha pasado de simples imitaciones a métodos mucho más elaborados y convincentes, debido a que la capacidad de replicar la funcionalidad de sitios legítimos ha aumentado sustancialmente, lo que hace que estos ataques sean aún más difíciles de identificar para los usuarios.

En este proyecto también se ha puesto de manifiesto la importancia de la educación en ciberseguridad y la concienciación de los usuarios, puesto que el conocimiento sobre cómo identificar posibles señales de phishing y cómo verificar la autenticidad de los sitios web antes de compartir información confidencial se vuelve cada vez más crucial en un panorama donde las técnicas de clonación se vuelven más refinadas.

Recomendaciones

Implementación de Autenticación de Dos Factores (2FA): La implementación del 2FA constituye un paso significativo para reforzar la seguridad, debido a que la autenticación de dos factores añade una capa adicional de protección al requerir una segunda forma de autenticación, lo que reduce considerablemente las posibilidades de acceso no autorizado.

Validación Rigurosa de Enlaces y URL: Antes de hacer clic en enlaces en correos electrónicos o mensajes, es esencial validar su autenticidad, puesto que esto se logra al verificar la dirección URL y asegurarse de que corresponda al sitio legítimo lo puede prevenir la exposición a páginas falsas.

Promoción de Buenas Prácticas de Seguridad Web: Los propietarios de sitios web deben implementar prácticas sólidas de seguridad, incluyendo la utilización de certificados SSL y la aplicación regular de actualizaciones de software para mitigar las vulnerabilidades y prevenir la clonación no autorizada.

Formación en Ingeniería Social: Proporcionar formación específica en ingeniería social es fundamental para mejorar la capacidad de los usuarios para identificar los indicios de técnicas de clonación de páginas web que utilizan la manipulación psicológica para obtener información confidencial.

Referencias

Amo, C. M. (Septiembre de 2022). *Análisis y técnicas de prevención, detección y ataques de phishing*. Obtenido de Universidad Nacional de Educación a Distancia (España). Escuela Técnica Superior de Ingeniería Informática: http://e-spacio.uned.es/fez/view/bibliuned:master-ETSInformatica-II-Cmayo

Ariani, P. C., & Jayanti, K. S. (2023). Comparative Analysis of Phishing Tools on Social Media Sites. *Ultimatics : Jurnal Teknik Informatika*, 22-27.

Balim, C., & Gunal, E. S. (2019). Automatic Detection of Smishing Attacks by Machine Learning Methods. *Conference: 2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 1-3.

Benavides, E., Fuertes, W., & Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología*, 97-104.

Bogantes, A. (2020). El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados. *Revista Sistemas, Cibernética e Informática*, 24-29.

Cano, J. (2020). Ciberataques. *Sistemas*, 67-74.

Castro, J. (01 de Diciembre de 2022). *Domain Spoofing Attack*. Obtenido de Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12276/Domain%20Spoofing%20Attack.pdf?sequence=1&isAllowed=y

Elizalde, R. E. (27 de Septiembre de 2021). *Laboratorio de Ethical Hacking con herramientas del sistema operativo Kali Linux como apoyo al aprendizaje de seguridad en redes de la Carrera Telemática*. Obtenido de Universidad de Guayaquil : http://repositorio.ug.edu.ec/handle/redug/55991

Eshmawi, A., & Nair, S. (2019). The Roving Proxy Framewrok for SMS Spam and Phishing Detection. *Conference: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 1-6.

Leite, C. M., Saccardo, E. S., & Gonzaga, F. B. (28 de Febrero de 2023). *A study about migrating from HTTrack to Apache Nutch*. Obtenido de Universidade Federal de Alfenas: https://www.unifal-mg.edu.br/dcc/wp-content/uploads/sites/221/2023/03/TCC_CaioLeite_e_EduardoSaccardo.pdf

Nakamura, A., & Dobashi, F. (2019). Proactive Phishing Sites Detection. *IEEE/WIC/ACM International Conference on Web Intelligence*, 443–448.

Páez, W. A. (2020). Ciberataques: Desafíos en el Ciberespacio. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, 116-128.

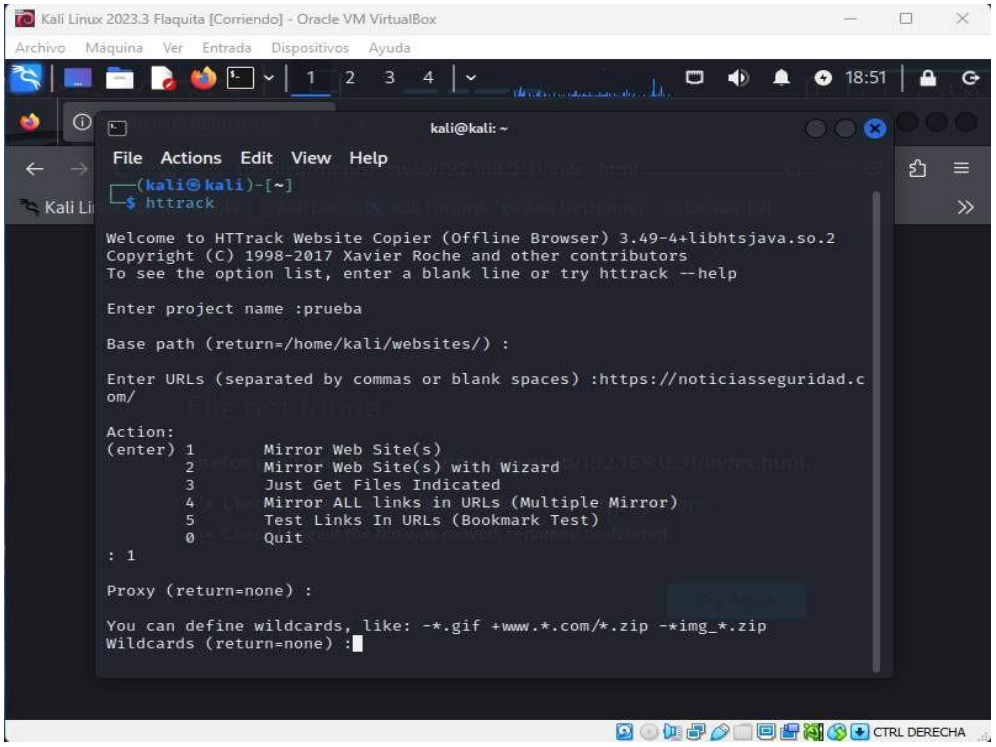
Starov, O., Wang, J., & Zhou, Y. (2019). Detecting Malicious Campaigns in Obfuscated JavaScript with Scalable Behavioral Analysis. *IEEE Security and Privacy Workshops (SPW)*, 218-223.

Wahyuni, N. K., Cahayani, P. P., Wicaksana, I. G., & Wijayanti, I. A. (2023). Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zphisher, Shellphish Dan Whphisher. *Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, 23-31.

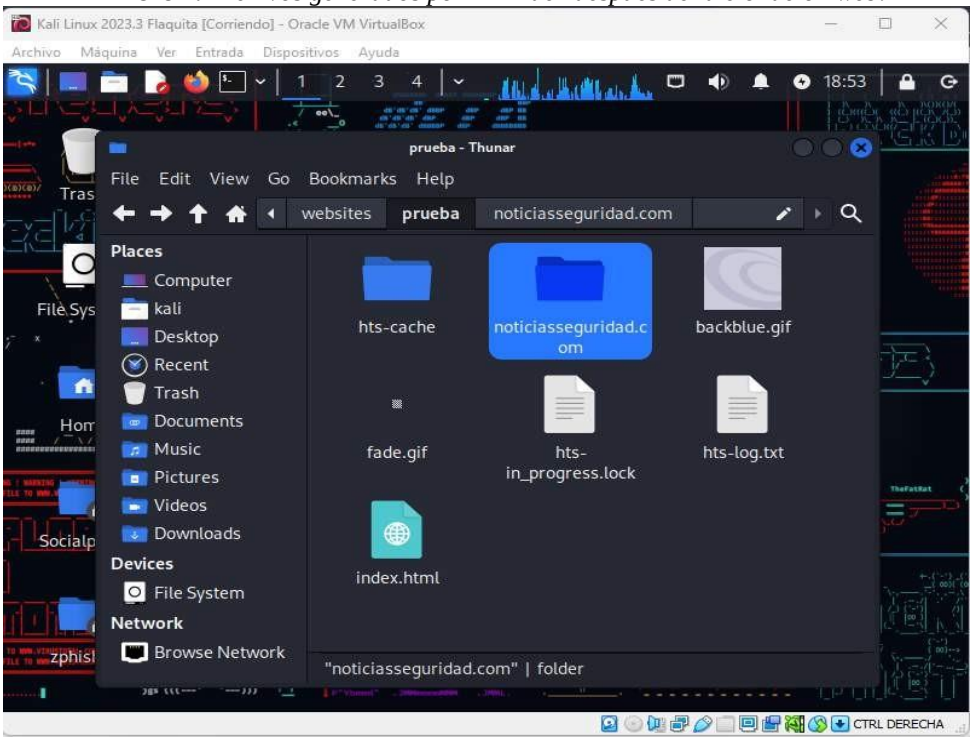
Yang, P., Guangzhen, Z., & Peng, Z. (2019). Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning. *IEEE Access*, 15196-15209.

Anexos

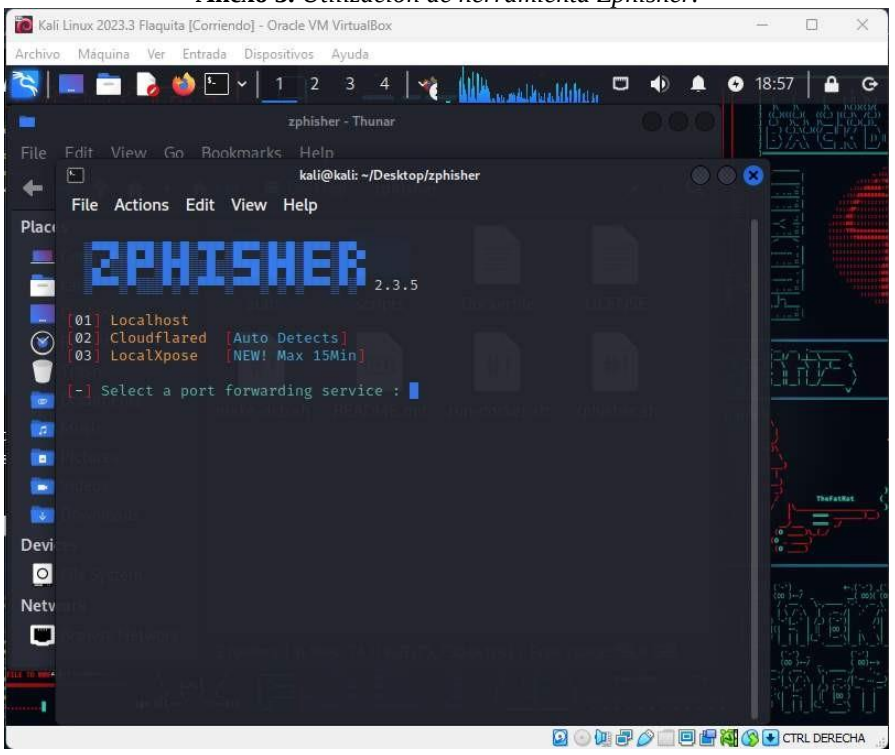
Anexo 1. *Utilización de herramienta HTTrack.*



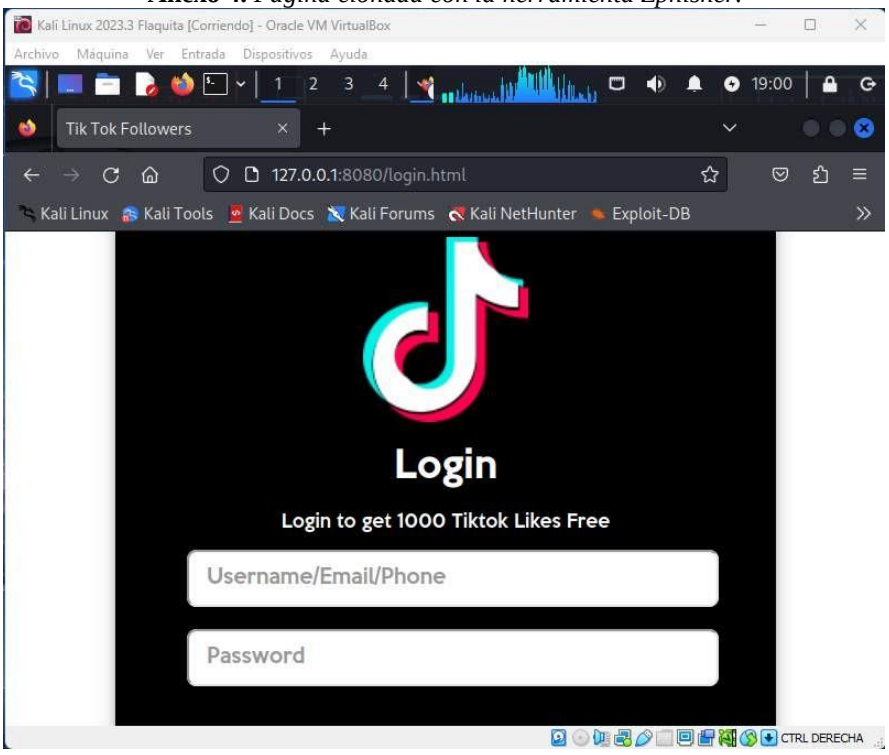
Anexo 2. *Archivos generados por HTTrack despues de la clonación web.*



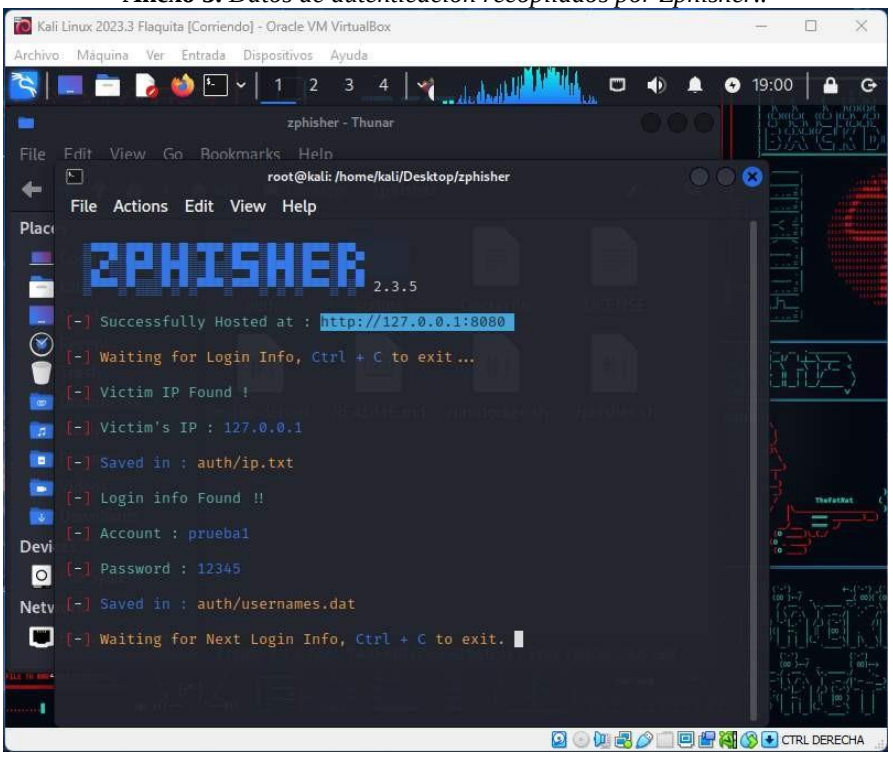
Anexo 3. *Utilización de herramienta Zphisher.*



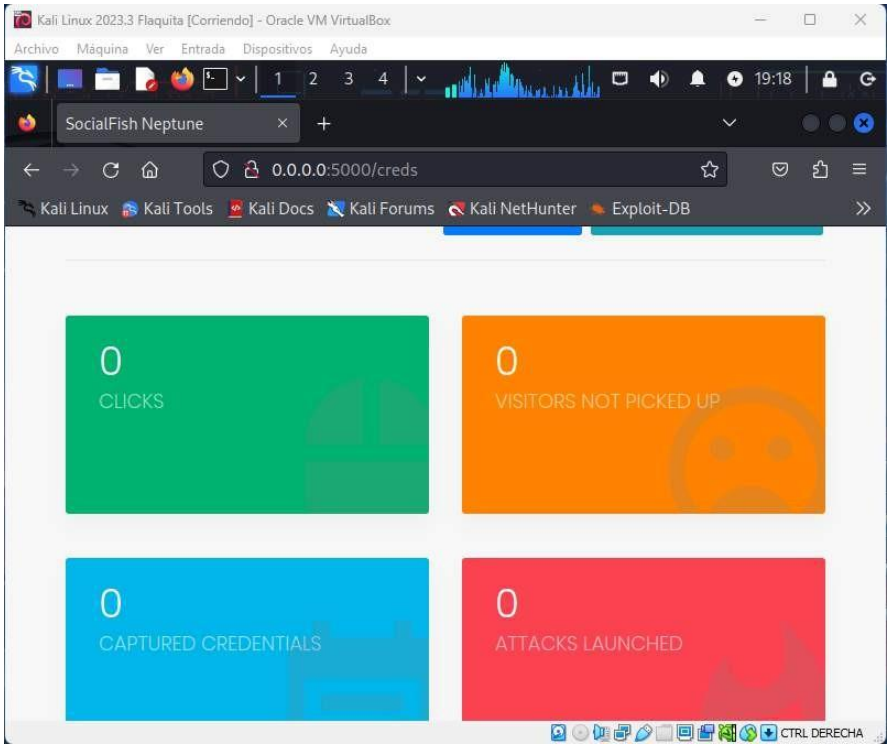
Anexo 4. *Pagina clonada con la herramienta Zphisher.*



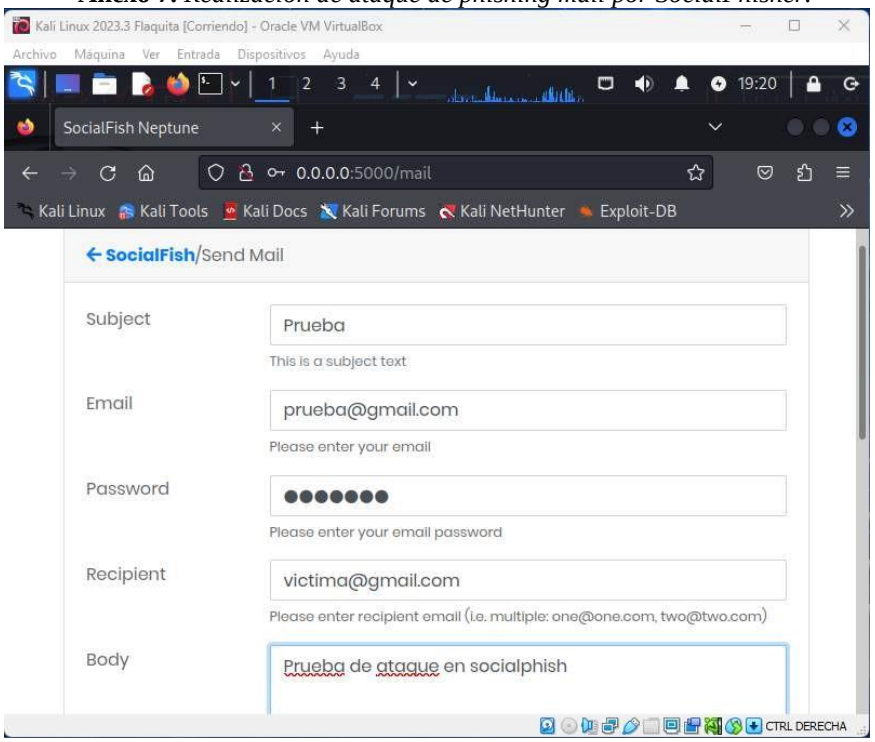
Anexo 5. *Datos de autenticación recopilados por Zphisher..*



Anexo 6. *Utilización de herramienta SocialPhisher.*



Anexo 7. *Realización de ataque de phishing mail por SocialPhisher.*



Anexo 8. *Entrevista Realizada al Ingeniero Harry Saltos.*

Formulario Caso de Estudio

Este formulario busca recopilar información clave de diferentes especialistas en el área, puesto que su experiencia es esencial para abordar los desafíos actuales en la seguridad digital. Las respuestas serán confidenciales y se utilizarán con fines de investigación académica.
Agradezco su valiosa contribución.

Se ha registrado el correo del encuestado (**hsaltos@utb.edu.ec**) al enviar este formulario.

¿Qué papel cree que juegan las herramientas de seguridad informática, como Kali Linux, en la evolución de los ataques de phishing y la clonación de páginas web? *

Juegan un papel de tener al alcance de poner herramientas pre elaboradas por personas con experiencia a personas de básicos conocimientos

Desde su experiencia, ¿Qué recomendaciones prácticas daría a las personas para proteger sus datos personales en línea?

utiliza contraseñas sólidas y únicas, activa la autenticación de dos factores, mantén tu software actualizado y emplea software de seguridad. Evita redes Wi-Fi públicas no seguras, configura la privacidad en redes sociales y sé cauteloso con correos electrónicos sospechosos. Realiza copias de seguridad, educa a tus hijos sobre la seguridad en línea y supervisa tus cuentas regularmente. La conciencia constante y la prudencia en línea son clave para mantener tus datos seguros.

¿Cree que la industria tecnológica está haciendo lo suficiente para proteger a los usuarios de los ataques de phishing y spoofing web?

La industria tecnológica ha avanzado en la protección contra ataques de phishing y spoofing web, implementando medidas como la autenticación de dos factores y filtros de correo electrónico. Sin embargo, la evolución constante de las tácticas de los atacantes presenta desafíos. Aunque se hacen esfuerzos, la educación de los usuarios y la vigilancia siguen siendo vitales para una protección efectiva.

¿Cree que la educación sobre seguridad cibernética debería ser una parte obligatoria del currículo escolar en la actualidad? *

no, solamente alguna charla básica de prevención, no todo lo nuevo que se nos ocurra debe ser parte de una educación con los jóvenes, seria desaprovechar el tiempo en enseñar temas mas urgentes

¿Tiene alguna experiencia personal con un intento de phishing o con la clonación de una página web? *

Si, cuando entró en auge un equipo de hackers contra instituciones publicas y no tenia buenas medidas de seguridad, sin embargo restitui el servicio en 2 minutos, pues tenia respaldos dinámicos automatizados y virtualizados, fue cuestión de apagar una virtual y encender otra

¿Cómo evalúa el impacto de las técnicas de ingeniería social en la efectividad de los ataques de phishing y spoofing web a lo largo del tiempo? *

Pues han demostrado ser cruciales en el éxito continuo de ataques de phishing y spoofing web. A medida que los atacantes refinan sus tácticas y utilizan información personal fácilmente disponible en línea, el impacto de estos ataques sigue siendo significativo. La concienciación y la educación son esenciales para mitigar este riesgo en constante evolución, además de la implementación de medidas tecnológicas de seguridad robustas.

Este formulario se creó en Facultad de Administración Finanzas e Informatica.

Google Formularios

Anexo 9. *Entrevista Realizada al Ingeniero Omar Montece.*

Formulario Caso de Estudio

Este formulario busca recopilar información clave de diferentes especialistas en el área, puesto que su experiencia es esencial para abordar los desafíos actuales en la seguridad digital. Las respuestas serán confidenciales y se utilizarán con fines de investigación académica.
Agradezco su valiosa contribución.

Se ha registrado el correo del encuestado (**omontece@utb.edu.ec**) al enviar este formulario.

¿Qué papel cree que juegan las herramientas de seguridad informática, como Kali Linux, en la evolución de los ataques de phishing y la clonación de páginas web? *

Este tipo de sistema operativo nos permite la recopilación de información, mediante el uso de herramientas para obtener todos los datos posibles sobre el sistema objetivo, admeas nos provee de un análisis de vulnerabilidades: escaneo e identificación de fallos de seguridad, los cuales pueden ser aprovechados para iniciar un ciberataque.

Desde su experiencia, ¿Qué recomendaciones prácticas daría a las personas para proteger sus datos personales en línea?

Usá contraseñas seguras con mayúsculas, minúsculas, números y símbolos.
Usá el modo incógnito para que no se guarden tus contraseñas y tu historial de navegación.
No uses la misma contraseña para los sitios a los que accedés y para las redes sociales.

¿Cree que la industria tecnológica está haciendo lo suficiente para proteger a los usuarios de los ataques de phishing y spoofing web?

no

¿Cree que la educación sobre seguridad cibernética debería ser una parte obligatoria del currículo escolar en la actualidad? *

Dentro del enterno de aprendizaje y crecimiento personal de los alumnos, es fundamental promover su integridad física, emocional y social.

¿Tiene alguna experiencia personal con un intento de phishing o con la clonación de una página web? *

Si

¿Cómo evalúa el impacto de las técnicas de ingeniería social en la efectividad de los ataques de phishing y spoofing web a lo largo del tiempo? *

No son al cien por ciento segura, se deberian crear politicas de seguridad mas drasticas que permitan mitigar este tipo de ataques.

Este formulario se creó en Facultad de Administración Finanzas e Informatica.

Google Formularios

Anexo 10. *Entrevista Realizada al Ingeniero Joffre León.*

Formulario Caso de Estudio

Este formulario busca recopilar información clave de diferentes especialistas en el área, puesto que su experiencia es esencial para abordar los desafíos actuales en la seguridad digital. Las respuestas serán confidenciales y se utilizarán con fines de investigación académica.
Agradezco su valiosa contribución.

Se ha registrado el correo del encuestado (**jvleon@utb.edu.ec**) al enviar este formulario.

¿Qué papel cree que juegan las herramientas de seguridad informática, como Kali Linux, en la evolución de los ataques de phishing y la clonación de páginas web? *

Un papel muy importante, ya que es cuenta con un sin numero de herramientas que nos permiten tanto atacar como contrarrestar ataques

Desde su experiencia, ¿Qué recomendaciones prácticas daría a las personas para proteger sus datos personales en línea?

Verificar que los sitios de conexión sean seguros, no dejar datos colgados en la web, usar sw antivirus apropiados, firewall de seguridad

¿Cree que la industria tecnológica está haciendo lo suficiente para proteger a los usuarios de los ataques de phishing y spoofing web?

Sin duda alguna existen mecanismos apropiados, pero lamentablemente no existe una verdadera cultura informática y una inversión en mecanismos de seguridad

¿Cree que la educación sobre seguridad cibernética debería ser una parte obligatoria del currículo escolar en la actualidad? *

Completamente de acuerdo

¿Tiene alguna experiencia personal con un intento de phishing o con la clonación de una página web? *

Phissing es una técnica muy usada hoy en día y lo podemos vivir en nuestros correos electrónicos a diario, en si una experiencia de haber sido victima no

¿Cómo evalúa el impacto de las técnicas de ingeniería social en la efectividad de los ataques de phishing y spoofing web a lo largo del tiempo? *

A nivel global han mitigado algunos ataques, sin embargo no ha sido posible contrarrestar los diversos procedimientos que se han dado

Este formulario se creó en Facultad de Administración Finanzas e Informatica.

Google Formularios