PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

TRABAJO DE TITULACIÓN

“CONCIENTIZACIÓN Y PREVENCIÓN DE RIESGOS EN ESTUDIANTES UNIVERSITARIOS MEDIANTE SIMULACIÓN DE ATAQUES DE PHISHING”

AUTOR:

ANGIE MICAELA ESPARZA GALARZA

DIRECTOR:

GUAÑA MOYA EDISON JAVIER

QUITO DM, 2023

DEDICATORIA

A lo largo de esta travesía académica, he sido bendecida con el amor, el apoyo y la guía de personas excepcionales que han sido mi fortaleza en los momentos de dificultad y mi alegría en los momentos de triunfo. Hoy, al llegar al final de esta etapa tan significativa, quiero dedicar esta tesis con todo mi corazón a aquellos que han sido mi inspiración y mi sostén.

A mis queridos padres Segundo Esparza y Wilma Galarza, quienes con su amor incondicional y sacrificios interminables me han mostrado el verdadero significado de la perseverancia y la dedicación. Gracias por ser mis pilares inquebrantables, por creer en mis sueños incluso cuando yo dudaba de ellos, y por su apoyo constante en cada paso del camino. Este logro es tanto suyo como mío.

Finalmente, a todos aquellos que han dejado una huella en mi vida académica y personal. Sus consejos, su aliento y su compañía han sido fundamentales para alcanzar este sueño.

Con todo mi amor y gratitud, dedico esta tesis a ustedes, quienes han sido mi luz y mi fortaleza en este viaje. Este trabajo marca el inicio de una nueva etapa llena de retos y oportunidades, y no podría haberlo logrado sin su apoyo incondicional.

AGRADECIMIENTO

A lo largo de este arduo y maravilloso viaje, he aprendido que los logros más significativos no se alcanzan en solitario, sino que son el resultado del apoyo incondicional y el amor de aquellos que nos rodean. Con el corazón lleno de gratitud, quiero expresar mis más sinceros agradecimientos.

En primer lugar, agradezco a Dios por darme la fortaleza y sabiduría necesarias para superar los desafíos a lo largo de este proceso.

A mis padres Segundo Esparza y Wilma Galarza, quienes han sido mi roca y mi inspiración. Gracias por su amor incondicional, sus sacrificios silenciosos y por enseñarme que con esfuerzo y dedicación se pueden alcanzar los sueños más grandes. Sin ustedes, nada de esto sería posible.

A mi hermano Alejandro, por su constante apoyo y amor. Sus palabras de aliento y su fe en mí me han dado la fuerza para superar los momentos más difíciles. Gracias por estar siempre a mi lado.

A mis amigos, mi segunda familia, por su amistad sincera y su apoyo incondicional. Gracias por los momentos de risas, por su compañía en los días difíciles y por ser una fuente constante de alegría y esperanza. Gracias por su apoyo emocional y por hacer de este viaje algo mucho más llevadero y significativo.

A mi tutor de tesis, Javier Guaña, por su invaluable orientación, paciencia y consejos. Su experiencia y conocimientos han sido fundamentales para la realización de este trabajo.

RESUMEN

El presente trabajo propone una metodología general para realizar un ataque de phishing dirigido de manera controlada en un entorno universitario. esta metodología se implementa con un enfoque estrictamente educativo y académico, asegurando que no se vulneren cuentas ni se realicen accesos no autorizados, a fin de cumplir con todas las normativas legales.

Se plantean cuatro tipos diferentes de ataques de phishing: la creación de una página web falsa, phishing por correo electrónico, smishing (phishing mediante SMS) y vishing (phishing mediante llamadas telefónicas).

Para poder realizar los ataques mencionados anteriormente, se plantean cuatro fases importantes.

La fase inicial es la de investigación y selección de objetivos, en la cual el atacante investiga y selecciona a las víctimas, recolectando información relevante para realizar el ataque dirigido.

La segunda fase es la de depuración de información, aquí la información recopilada se depura y se guarda. Esta fase asegura que únicamente se utilice información pertinente para maximizar la efectividad del ataque.

La tercera fase es la realización del ataque, en la cual se llevan a cabo los diferentes ataques de phishing utilizando herramientas como Zphisher, spoofcheck, espoofer y TBomb. estas herramientas se emplean para realizar ataques a las víctimas previamente seleccionadas, aprovechando las técnicas y estrategias específicas de cada tipo de phishing.

Finamente la cuarta fase de obtención de resultados y uso de la información se enfoca en la obtención de resultados y el análisis de la información recopilada. Dado que este trabajo tiene un propósito educativo, no se generan consecuencias graves para las víctimas. los resultados permitirán evaluar el nivel de conocimiento de los estudiantes sobre el phishing.

La conclusión de este estudio incluirá una charla de concientización y prevención sobre los ataques de phishing, destinada a mejorar la conciencia y la preparación de los estudiantes frente a estas amenazas.

En resumen, este trabajo no solo busca entender y demostrar cómo se realizan los ataques de phishing, sino también educar a los estudiantes universitarios sobre cómo reconocer y prevenir estos ataques, fortaleciendo así la seguridad de la información en el entorno universitario.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I: INTRODUCCIÓN

1.1 Tema

Concientización y prevención de riesgos en estudiantes universitarios mediante simulación de ataques de phishing

1.2 Justificación

La seguridad informática es un aspecto fundamental en el ámbito de la tecnología de la información, especialmente en entornos universitarios donde se manejan grandes cantidades de datos sensibles y se utilizan sistemas de información para diversas actividades académicas y administrativas. En este contexto, el phishing se ha convertido en una de las amenazas más comunes y peligrosas, afectando tanto a instituciones como a individuos.

El phishing es una técnica de ingeniería social utilizada por ciberdelincuentes para engañar a las personas y obtener información sensible, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por entidades confiables en comunicaciones electrónicas. Este método ha crecido exponencialmente con la expansión del uso de internet y las tecnologías digitales. (Antonsen, 2017)

La simulación de ataques de phishing se presenta como una herramienta efectiva para sensibilizar a los estudiantes sobre esta amenaza y capacitarlos para reconocer y responder adecuadamente a posibles intentos de phishing. Al exponer a los estudiantes a escenarios simulados de phishing, se les brinda la oportunidad de experimentar de manera segura cómo funcionan estos ataques, identificar señales de alerta y practicar buenas prácticas de seguridad.

En conclusión, el presente trabajo de titulación busca contribuir al desarrollo de habilidades clave en seguridad informática entre los estudiantes de un entorno universitario, promoviendo la

concientización y la adopción de medidas preventivas para mitigar los riesgos asociados al phishing.

1.3 Planteamiento del problema

En el contexto de un entorno universitario, la falta de concientización y prevención de riesgos en relación con los ataques de phishing representa una vulnerabilidad significativa

En función de la problemática planteada se propone la siguiente pregunta principal:

- ¿Qué impacto tienen los ataques de phishing en la seguridad de los sistemas y la privacidad de la información en entornos universitarios?

Y las siguientes preguntas secundarias:

- ¿Cuál es el nivel de concientización de los estudiantes universitarios respecto a los riesgos asociados con los ataques de phishing?
- ¿Cuáles son las principales técnicas de phishing que afectan a los estudiantes en entornos universitarios?
- ¿Cuáles son las consecuencias más frecuentes de caer en un ataque de phishing para los estudiantes universitarios?

1.4 Objetivo general

Concientizar a los estudiantes universitarios sobre los riesgos de pérdida de información que se obtienen mediante ataques de phishing

1.5 Objetivo especifico

- Identificar las principales técnicas de phishing utilizadas por los atacantes informáticos.
- Analizar el impacto de los ataques de phishing en la privacidad de la información en estudiantes universitarios.

- Implementar un ataque de Phishing a estudiantes universitarios en un entorno controlado.
- Proponer recomendaciones y medidas de seguridad para el fortalecimiento de la seguridad de la información y concientización en entornos universitarios.

1.6 Antecedentes

El phishing en Ecuador, al igual que en muchos otros países, ha sido una amenaza creciente a medida que la digitalización avanza y más personas y empresas utilizan servicios en línea.

Con el comienzo de la pandemia de COVID-19, los criminales han aprovechado el cambio del modelo laboral, el teletrabajo, que permite a los empleados conectarse remotamente a los sistemas de sus organizaciones. (Rosero, 2021)

Debido al incremento del uso de e-commerce y los servicios bancarios en línea, las oportunidades para los ciberdelincuentes aumentaron. Las tácticas de phishing han evolucionado para incluir no solo correos electrónicos, sino también mensajes de texto (smishing) y llamadas telefónicas fraudulentas (vishing).

Uno de los incidentes más relevantes ocurrió en 2018, cuando un ataque de phishing afectó a varios clientes de bancos ecuatorianos, resultando en la sustracción de información confidencial y pérdidas financieras significativas. Las tácticas utilizadas incluyeron correos electrónicos fraudulentos y sitios web falsos diseñados para parecerse a los de instituciones bancarias legítimas. (Martínez, 2019)

En 2022, Ecuador fue el país con más detecciones de ataques phishing en toda América Latina, según el informe “Security Report latinoamérica 2023” realizado por la firma Ciberseguridad ESET. En el cual se compara los países de Latinoamérica y el número de ataques

de phishing recibidos, donde podemos observar que Ecuador tiene un 8, encabezando así la lista. (Ver figura 1)

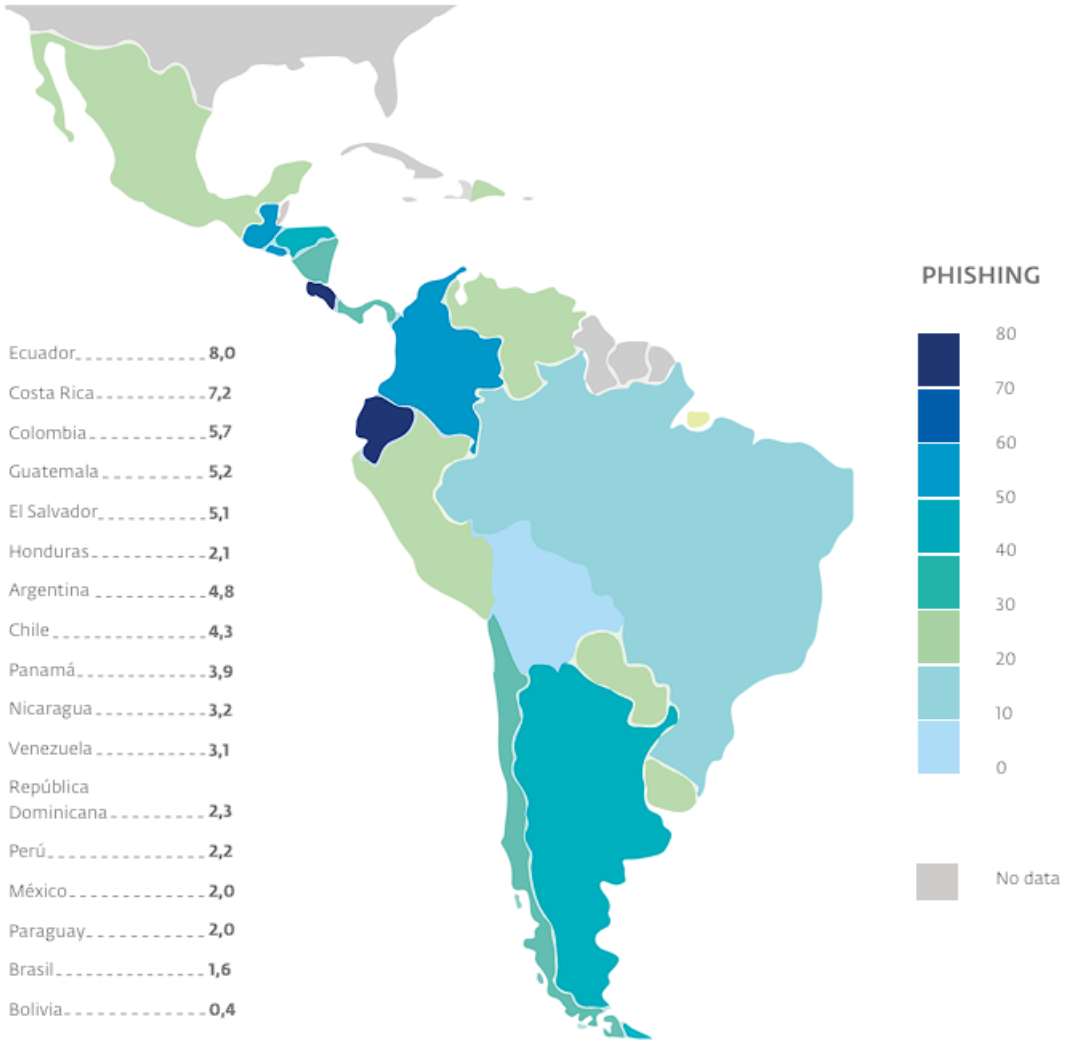

Figura 1. *Países de América Latina con mayor cantidad de detecciones de phishing en 2022*

Nota: Los datos corresponden al índice de detección, que toma valores entre 1 y 10 y que es calculado a partir de la relación entre la cantidad de detecciones de campañas de phishing y la cantidad de detecciones por territorio, normalizado de acuerdo con el tamaño de cada país. Teniendo este tipo de medición, Adaptado de ESET. (2023). ESET Security Report 2023: Estado de la ciberseguridad en América Latina. ESET Latinoamérica. https://www.eset.com/latam.

De acuerdo con el "ESET Security Report 2023", Ecuador es uno de los países de América Latina con el mayor porcentaje de detecciones de phishing, con un índice del 8%. Este porcentaje lo coloca por delante de otros países como Costa Rica (7.2%) y Colombia (5.7%). La alta prevalencia de este tipo de ataques sugiere que los ciberdelincuentes ven a los usuarios ecuatorianos como objetivos viables debido a una combinación de factores, que pueden incluir menores niveles de concienciación sobre seguridad digital y la implementación de medidas de protección insuficientes en comparación con otros países.

Las organizaciones en Ecuador están empezando a tomar medidas más proactivas para combatir el phishing. Sin embargo, según el reporte de ESET, un 65% de los encuestados señaló que el presupuesto asignado a ciberseguridad es insuficiente, lo que representa un desafío significativo para implementar soluciones de seguridad eficaces. A pesar de esto, ha habido un aumento en la adopción de soluciones de seguridad para dispositivos móviles, pasando del 10% al 21% en un año, lo que indica una creciente concienciación sobre la importancia de proteger estos dispositivos que son frecuentemente blanco de ataques de phishing.

1.7 Alcance

El presente proyecto tiene como finalidad determinar el nivel de vulnerabilidad en los estudiantes universitarios de diversas disciplinas y niveles académicos, abarcando una muestra representativa de la población estudiantil.

En donde se analizarán las técnicas más comunes de phishing utilizadas por ciberdelincuentes, así como las señales de alerta que indican posibles intentos de phishing. Para realizarlo se realizarán las siguientes actividades:

- Se realizará un estudio exhaustivo sobre los conocimientos básicos que tienen los estudiantes sobre los ataques de ciberseguridad y si son conscientes de las consecuencias de estos.
- Se verificará el nivel de seguridad que tiene la universidad para ataques de ciberdelincuentes y si tiene el protocolo necesario para abarcar estos problemas.
- Se recopilará información necesaria para realizar el ataque como por ejemplo direcciones de correo electrónico, nombres de administrativos, nombres de profesores, nombres de estudiantes e información relevante para empezar la simulación.
- Se diseñará correos electrónicos persuasivos, páginas web que sean idénticos a los originales con el objetivo de engañar a las personas que lo reciban.
- Se realizarán pruebas internas con un grupo selecto de personas, antes de ya empezar con el ataque real con el objetivo de identificar si existen problemas, los errores que pueden presentarse y así poder mejorar la efectividad del ataque
- Se enviarán los correos electrónicos falsos a los estudiantes y se monitorearán las respuestas.
- Se analizarán las respuestas de los usuarios como cuántos hicieron clic en los enlaces falsos, cuántos proporcionaron información sensible, etc.
- Una vez realizada la simulación, se procederá a realizar una capacitación sobre la concienciación phishing a los usuarios de la universidad.
- Se preparará un informe detallado que resuma los resultados de la simulación, incluyendo estadísticas, áreas de mejora y recomendaciones para fortalecer la seguridad en la universidad.

CAPITULO II: FUNDAMENTOS TEÓRICOS

2.1 Ciberseguridad

La ciberseguridad consiste en proteger computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra ataques malintencionados. También se le conoce como seguridad de la tecnología de la información o seguridad de la información electrónica. Este concepto se aplica en diversos ámbitos, desde el empresarial hasta la informática móvil, y puede subdividirse en varias categorías comunes.

En el ámbito de la seguridad de la información, esta está encargada de proteger la privacidad, así como la integridad de los datos, desde el tránsito de estos hasta su almacenamiento.

Aunque a menudo se confunden los términos seguridad de la información y ciberseguridad, cabe destacar que la seguridad de la información se enfoca en proteger la información en todas sus formas, incluyendo la impresa y la transmitida verbal o visualmente. Por otro lado, la ciberseguridad se especializa en la protección integral de los activos digitales, abarcando la información que se procesa, se guarda o se envía a través de redes de sistemas de información, así como de la infraestructura crítica de información. (Solleiro et al, 2022)

Un tema importante por tratar es la capacitación al usuario final, que para este caso de estudio serán los estudiantes universitarios, este factor en la ciberseguridad es indispensable, dado que de ellos depende tener conocimiento sobre las buenas prácticas de seguridad para así poder evitar el robo de información.

2.2 Riesgos de seguridad informática en entornos universitarios

La seguridad informática es esencial en la educación digital para proteger la información y garantizar su integridad, confidencialidad y disponibilidad. (Guaña-Moya, 2023)

En cuanto a los entornos universitarios, la seguridad informática enfrenta diversos desafíos debido a la naturaleza abierta y colaborativa de estos espacios. Las universidades manejan una gran cantidad de datos sensibles, incluidos registros académicos, información personal de estudiantes, profesores, administrativos, etc. así como datos de investigación. La presencia de múltiples dispositivos y usuarios conectados a la red universitaria aumenta el riesgo de accesos no autorizados y posibles brechas de seguridad. Los estudiantes y el personal pueden ser objetivos de ataques de phishing, donde los atacantes intentan engañarlos para que revelen información confidencial.

Asimismo, las redes universitarias son vulnerables a ataques de malware y ransomware, que pueden infiltrarse en los sistemas mediante correos electrónicos de phishing o enlaces comprometidos. Estos tipos de ataques pueden cifrar datos críticos y exigir un rescate para su liberación, afectando gravemente las operaciones universitarias (White, 2021). La constante rotación de usuarios y la falta de recursos dedicados a la ciberseguridad complican la implementación de medidas de protección adecuadas. Por ello, es esencial que las universidades desarrollen políticas de seguridad robustas y lleven a cabo campañas de concienciación para educar a los usuarios sobre las mejores prácticas de seguridad informática. (Miller & Davis, 2020)

Es importante reconocer que todos los usuarios pueden ser blanco de un ataque de phishing, dado que todos los días se recibe diferentes tipos de correo electrónico y es necesario tener el conocimiento necesario para detectar cuando estos sean reales, así como también cuando estén diseñados para robar contraseñas. (Kaspersky, Cómo reconocer y evitar correos electrónicos de phishing, 2024)

Otra parte fundamental que en la mayoría de los casos es algo que los estudiantes no le ponen mucha atención es a las redes Wi-Fi, cuando estas pueden ser entradas fáciles para hackers

que desean robar información. La incorporación de dispositivos personales como laptops y celulares en el ámbito universitario ha transformado significativamente la manera en que estudiantes, docentes y personal administrativo desarrollan sus actividades académicas y cotidianas. (McAfee, 2021)

2.3 Ataques cibernéticos

Los ataques cibernéticos han evolucionado significativamente en los últimos años, convirtiéndose en una amenaza persistente para organizaciones de todo tipo. Los ciberdelincuentes utilizan una variedad de métodos para infiltrarse en sistemas informáticos, incluyendo el phishing, el malware y los ataques de denegación de servicio (DDoS). Estos ataques no solo buscan robar información confidencial, sino también interrumpir las operaciones y causar daños financieros y reputacionales. Las tácticas empleadas son cada vez más sofisticadas, lo que dificulta su detección y prevención.

El phishing es una de las formas más prevalentes de ataque, donde los atacantes envían correos electrónicos que aparentan ser de fuentes confiables. Estos mensajes suelen contener enlaces o archivos adjuntos maliciosos que, al abrirse, instalan malware en el sistema del usuario. Este tipo de ataque se basa en la ingeniería social para manipular a las víctimas y obtener acceso a sus credenciales y datos sensibles. Es crucial que las empresas eduquen a sus empleados para reconocer y evitar estos correos fraudulentos. (Jones, 2019)

2.4 Técnicas de ataques cibernéticos

Los ataques cibernéticos avanzan con el tiempo y cada vez evolucionan constantemente para lograr evadir las defensas de seguridad. Existen diferentes tipos de ataques, los cuales se enfocan en conseguir específicamente la información deseada. A continuación, se mencionan las técnicas de ataques más comunes:

1. **Phishing**: El phishing es un método para intentar obtener detalles potencialmente valiosos, como nombres de usuario, contraseñas o datos médicos, por motivos maliciosos, mediante comunicaciones dirigidas, como correos electrónicos o mensajes, en los que la parte atacante anima a los destinatarios a hacer clic en enlaces a sitios web que ejecutan código malicioso para descargar o instalar malware. (Guaña-Moya et al., 2022)
2. **Malware**: Es el nombre común para muchas versiones maliciosas de un programa, suele ser un código informático destinado a destruir datos o procesos, así como adquirir accesos no autorizados a una red, generalmente se proporciona como un enlace o archivo por correo electrónico para que el usuario haga clic en este o abra el archivo de malware. (Guaña-Moya et al., 2022)
3. **DDoS**: También conocido como ataque de denegación de servicio, representa uno de los tipos de ataques más peligrosos que afectan a las computadoras. El objetivo principal de este ataque es derribar la máquina objetivo y hacer que los servicios no estén disponibles para los usuarios legales, lo que se logra, principalmente, dirigiendo muchos equipos para que envíen una gran cantidad de paquetes hacia el computador especifico con el fin de consumir los recursos y hacer que deje de funciona. (Guaña-Moya et al., 2022)
4. **Ingeniería Social:** La ingeniería social se basa en explotar la psicología humana y averiguar sus vulnerabilidades para obtener acceso a datos o sistemas. "La ingeniería social implica la manipulación psicológica de las personas para obtener acceso a información o sistemas. Los atacantes explotan cualidades humanas como la

curiosidad, la codicia y la autoridad para engañar a sus víctimas". (Computerworld, 2023)

5. **Man in the Middle:** En un ataque de intermediario, el atacante intercepta y posiblemente altera la comunicación entre dos partes que creen que están comunicándose directamente entre sí. "Un ataque MitM ocurre cuando un atacante intercepta y potencialmente altera la comunicación entre dos partes sin que estas se den cuenta". (Norton, 2018)
6. **Fuerza Bruta:** Estos ataques tratan de adivinar las contraseñas probando todas las combinaciones posibles hasta encontrar la correcta. "Los ataques de fuerza bruta implican probar todas las combinaciones posibles de contraseñas hasta encontrar la correcta". (Kaspersky, 2020)

2.5 Phishing

El phishing es una técnica de ciberdelincuencia diseñada para engañar a los usuarios y hacer que revelen información personal y confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito. Este tipo de ataque suele realizarse a través de correos electrónicos, mensajes instantáneos o sitios web falsificados que aparentan ser entidades legítimas. (Abawajy, 2014)

El phishing es una técnica de ciberdelincuencia que busca engañar a las personas para que revelen información confidencial, como contraseñas, números de tarjetas de crédito, y otros datos personales sensibles. Los atacantes se hacen pasar por entidades confiables mediante el uso de correos electrónicos, mensajes de texto, o sitios web falsos, diseñados para parecer legítimos. El término "phishing" deriva de "fishing" (pesca en inglés), ya que los atacantes "pescan" información sensible de sus víctimas utilizando técnicas de señuelo.

La persona que lleva a cabo este tipo de ataques es conocida como "phisher", el objetivo principal de la persona es obtener una retribución económica a expensas de sus víctimas. Una vez que obtiene la información confidencial, el ciberdelincuente puede realizar diversas acciones delictivas, como robo de identidad, fraude financiero, venta de datos en la web oscura o incluso la instalación de malware en los dispositivos de las víctimas.

2.5.1 Tipos de ataques de phishing

En su estudio, Ángel Herrera (2016), propone una clasificación detallada de los ataques de phishing tomando en cuenta dos dimensiones principales:

- Según el servicio que atacan:
    - Servicios financieros: Bancos, cajas de ahorro, pasarelas de pago en línea, criptomonedas.
    - Redes sociales: Facebook, X, Instagram, LinkedIn.
    - Comercio electrónico: Tiendas online, subastas, plataformas de compraventa.
    - Entretenimiento: Juegos en línea, plataformas de streaming.
    - Soporte técnico: Mesas de ayuda, sitios web de soporte de marcas tecnológicas.
    - Almacenamiento en la nube: Dropbox, Google Drive, iCloud.
    - Servicios públicos: Impuestos, seguridad social, servicios de salud.
    - Mensajería instantánea: WhatsApp, Telegram.
    - Ofertas de empleo: Falsos anuncios de trabajo, sitios web fraudulentos de reclutamiento
- Según el modus operandi:

- Phishing engañoso: Correos electrónicos o mensajes de texto que imitan la identidad de organizaciones legítimas para inducir a la víctima a revelar información confidencial.
- Software malicioso: Instalación de malware en el dispositivo de la víctima para capturar información personal o financiera.
- Envenenamiento de DNS (DNS o pharming): Redireccionamiento del tráfico web de la víctima a un sitio web falso que simula la página legítima.
- Introducción de contenido: Inyección de código malicioso en sitios web legítimos para capturar información de los usuarios.
- Ataques "Man in the middle": Interceptación de la comunicación entre la víctima y un sitio web legítimo para robar información confidencial.
- Search Engine Phishing (SEP): Posicionamiento de sitios web falsos en los resultados de búsqueda para engañar a los usuarios que buscan información específica.

Es importante destacar que esta clasificación no es exhaustiva y que los ciberdelincuentes están en constante evolución, creando nuevas técnicas y combinando métodos existentes para llevar a cabo sus ataques. (Herrera, 2016)

Existen diversos tipos de ataques de phishing:

- **Phishing Tradicional:** El phishing tradicional implica el envío masivo de correos electrónicos fraudulentos que aparentan ser de fuentes confiables, como bancos o proveedores de servicios, para engañar a los destinatarios y que proporcionen información personal. (Hong, 2012)

Estos correos a menudo contienen enlaces a sitios web falsos que recopilan las credenciales de los usuarios

- **Spear Phishing:** El spear phishing es un ataque más dirigido y personalizado. A diferencia del phishing tradicional, estos ataques se centran en individuos específicos, utilizando información personal para hacer que los correos electrónicos sean más convincentes. (Sysmantec, 2018)

  Los atacantes suelen investigar a sus víctimas para crear mensajes altamente personalizados.

- **Whaling**: El whaling, o phishing dirigido a altos ejecutivos, se enfoca en miembros de la alta dirección de una organización, como CEOs y CFOs. Estos ataques son cuidadosamente diseñados para parecer correos electrónicos legítimos relacionados con asuntos empresariales importantes, aprovechando la autoridad y acceso a información crítica de estos ejecutivos. (Parrish et al., 2009)

- **Vishing**: El vishing, o phishing por voz, utiliza llamadas telefónicas para engañar a las víctimas y obtener información personal. Los atacantes se hacen pasar por representantes de empresas o instituciones confiables para convencer a las personas de que revelen datos sensibles. (Abraham & Chengalur-Smith, 2010)

- **Smishing**: El smishing es una variante de phishing que utiliza mensajes de texto (SMS) para dirigir a las víctimas a sitios web fraudulentos o para que llamen a números de teléfono controlados por los atacantes. (Oliviera et al., 2017)

  Este método se aprovecha de la confianza que los usuarios tienen en los mensajes de texto.

Clone Phishing: El clone phishing implica la creación de una copia de un correo electrónico legítimo previamente enviado a la víctima. Los atacantes clonan el correo y reemplazan los enlaces o archivos adjuntos con versiones maliciosas, engañando a la víctima para que piense que está interactuando con un mensaje auténtico. (Jansson & Von Solms, 2013)

2.6 Comparación ataques de phishing

Una vez analizados los diferentes tipos de ataques de phishing que existen y las principales características, se plantea una comparativa de los mismos para enfatizar en el objetivo que tiene cada uno de los ataques. (Ver tabla 1)

Tabla 1*.Comparativa de ataques de phishing*

Tipos de ataque de phishing	Descripción	Eficacia	Vulnerabilidades	Objetivo
Phishing tradicional	Envío masivo de correos electrónicos fraudulentos que aparentan ser de fuentes confiables.	Moderada	Usuarios confiados y falta de conocimiento sobre correos electrónicos fraudulentos	Obtener información personal y financiera
Spear phishing	Ataques dirigidos y personalizados utilizando información específica de la víctima	Alta	Información específica y personal de la víctima	Obtener acceso a datos específicos y comprometer sistemas
Whaling	Ataques dirigidos a altos ejecutivos con correos electrónicos relacionados con asuntos empresariales importantes	Alta	Acceso a información crítica y autoridad de los ejecutivos	Acceder a información crítica y confidencial de la empresa
Vishing	Uso de llamadas telefónicas para engañar a las víctimas y obtener información personal	Moderada	Falta de verificación visual y confianza en llamadas telefónicas	Obtener información personal y financiera
Smishing	Uso de mensajes de texto (SMS) para dirigir a las víctimas	Moderada	Confianza en mensajes de texto y falta de verificación	Dirigir a las víctimas a sitios web maliciosos para

	a sitios web fraudulentos			obtener datos personales.
Clone Phishing	Creación de una copia de un correo electrónico legítimo previamente enviado a la víctima con enlaces o archivos adjuntos maliciosos	Alta	Confianza en correos electrónicos legítimos previamente recibidos.	Engañar a la víctima para que interactúe con contenido malicioso

Al analizar la tabla anterior, se enfatiza en la eficiencia, en las vulnerabilidades y el objetivo que tiene cada tipo de ataque, llegando así a que todos los tipos de phishing son importantes y se pueden usar de diferente manera.

2.7 Herramientas para desarrollar phishing

2.7.1 Open source

El término "Open Source" se refiere a un enfoque de desarrollo de software en el que el código fuente está disponible públicamente para su visualización, modificación y distribución. Este modelo promueve la colaboración abierta y la participación de la comunidad, lo que a menudo resulta en un software de mayor calidad y más innovador que el producido mediante métodos tradicionales de desarrollo cerrado. (Raymond, 1999)

Open Source, también conocido como código abierto, se define como un modelo de desarrollo de software y tecnología en el que el código fuente está disponible y es compartido de manera pública. Este enfoque permite que los usuarios puedan ver, modificar y redistribuir el software a su antojo, promoviendo así la colaboración y la transparencia dentro de la comunidad. (Red Hat, 2023)

El movimiento Open Source se basa en principios de libertad y transparencia. Los desarrolladores pueden utilizar el código fuente de otros proyectos como base para sus propios trabajos, lo que facilita la reutilización y la interoperabilidad entre diferentes sistemas y

aplicaciones. Además, este modelo de desarrollo promueve la educación y la capacitación, ya que los estudiantes y profesionales pueden estudiar y aprender de códigos reales utilizados en aplicaciones comerciales y académicas. Esta apertura también permite que se identifiquen y corrijan errores de manera más eficiente, gracias a la colaboración de una comunidad global de desarrolladores.

El software de código abierto promueve la colaboración y la innovación en el desarrollo de programas, ya que al hacer el código fuente públicamente accesible, permite que cualquier persona pueda estudiar, modificar, mejorar e incluso eliminar partes del software. Esta apertura conduce a una mayor diversidad de ideas y soluciones, lo que contribuye a la transparencia, la seguridad y la flexibilidad del desarrollo. Además, permite realizar adaptaciones y personalizaciones específicas de acuerdo con las necesidades de los usuarios.

Para las empresas, el software Open Source ofrece beneficios significativos, incluidos costos reducidos y una mayor flexibilidad. Al no depender de licencias costosas y actualizaciones de proveedores específicos, las organizaciones pueden adaptar el software a sus necesidades particulares y contribuir activamente a su mejora. Esto no solo reduce los costos operativos, sino que también impulsa la innovación y la competitividad. (Feller & Fitzgerald, 2002)

2.7.2 Kali-Linux

Kali Linux es una distribución de Linux basada en Debian, creada por Offensive Security. Se caracteriza por estar específicamente diseñada para pruebas de penetración, seguridad informática y hacking ético. Como una herramienta preinstalada en el sistema operativo Linux, Kali Linux destaca por su alta seguridad y configuraciones avanzadas, y cuenta con múltiples herramientas para proteger y asegurar la información almacenada en el sistema operativo. (Castro, 2023)

Kali Linux se destaca por su amplia variedad de herramientas de seguridad y pruebas de penetración. Esta característica, junto con su compatibilidad para interactuar con otras herramientas y aplicaciones tanto de su propio entorno como de otros sistemas operativos, lo convierte en una elección preferida. Además, sus robustas medidas de seguridad lo hacen especialmente adecuado para tareas relacionadas con la ciberseguridad.

2.7.3 Python

Python es un lenguaje de programación orientado a objetos, interpretado y de uso general, reconocido por su código claro y estructurado. Se distingue por su licencia de código abierto, lo que permite su uso gratuito en una variedad de aplicaciones. Este lenguaje es ampliamente utilizado en el desarrollo web, la informática científica, el análisis de datos y la automatización de tareas, y es conocido por su versatilidad, capacidad multiplataforma y soporte para múltiples paradigmas de programación. Python es empleado en plataformas de alto tráfico como Google, YouTube o Facebook, destacándose por su eficiencia y facilidad de aprendizaje. (ORACLE, 2022)

La elección de Python para realizar phishing se debe en gran parte a su facilidad de uso y su sintaxis legible. Python es conocido por su sintaxis clara y legible, lo que facilita la escritura y comprensión de scripts complejos, incluso para aquellos que no son programadores avanzados. (Van Rossum, 1995)

Entre las razones principales para elegir Python en este trabajo está su versatilidad, ya que se puede aplicar en una amplia gama de proyectos, y su extensa comunidad, que proporciona numerosos recursos, bibliotecas y frameworks. Además, Python se destaca por su capacidad para integrarse con otros lenguajes de programación y tecnologías, lo que lo hace especialmente útil.

Python es una herramienta poderosa para la automatización, lo que es crucial para realizar campañas de phishing a gran escala. Con Python, los atacantes pueden escribir scripts que

automáticamente envían correos electrónicos a miles de destinatarios, personalizan los mensajes para aumentar la efectividad del engaño, y gestionan respuestas de manera automática. Esta capacidad de automatización permite a los atacantes ejecutar operaciones de phishing con mínima intervención manual, aumentando la eficiencia y el alcance de sus ataques.

2.7.4 Github

GitHub es una plataforma ampliamente utilizada por desarrolladores de todo el mundo para compartir y colaborar en proyectos de software. Esto significa que hay una gran cantidad de scripts disponibles que han sido probados y utilizados por otros, lo que aumenta la probabilidad de encontrar código funcional y efectivo para realizar phishing. Clonar estos scripts ahorra tiempo y esfuerzo, ya que no es necesario desarrollar soluciones desde cero.

GitHub proporciona un sistema robusto de control de versiones basado en Git, lo que permite a los desarrolladores colaborar eficazmente, realizar un seguimiento de los cambios y gestionar diferentes versiones de sus scripts de phishing. (Chacon & Straub, 2014)

GitHub no solo es una plataforma de código, sino también una comunidad activa de desarrolladores. La posibilidad de documentar proyectos y obtener retroalimentación de la comunidad mejora la calidad y seguridad de las herramientas desarrolladas. (GitHub, Inc., 2021)

Finalmente, la capacidad de recibir actualizaciones y mejoras continuas es una ventaja significativa de clonar scripts de GitHub. A medida que la comunidad de desarrolladores contribuye con nuevas características y correcciones de errores, los scripts clonados se mantienen al día con las últimas tecnologías y técnicas de seguridad, lo que mejora la efectividad de los ataques de phishing. (Loeliger & McCullough, 2012)

2.7.5 Zphisher

Zphisher es una herramienta de phishing de código abierto ampliamente utilizada en la comunidad de hacking ético. Desarrollada para facilitar la creación de páginas de phishing, Zphisher permite a los usuarios generar páginas web que imitan la apariencia de sitios legítimos con el objetivo de engañar a las víctimas y obtener información sensible como contraseñas y datos personales. La herramienta ofrece una interfaz sencilla y soporta una variedad de plantillas preconfiguradas para servicios populares, lo que la hace accesible incluso para usuarios con conocimientos técnicos limitados.

Esta herramienta es especialmente conocida por su facilidad de uso y su capacidad para automatizar la creación de múltiples páginas de phishing, lo que la hace accesible incluso para aquellos con conocimientos técnicos limitados. (Doe, 2020)

Sin embargo, el uso de Zphisher, como el de cualquier herramienta de phishing, es ilegal y altamente ético, y su uso está estrictamente prohibido en la mayoría de los entornos profesionales y académicos. (Smith, 2021)

2.7.6. Spoofcheck

Spoofcheck es una herramienta esencial para mejorar la seguridad del correo electrónico. Según el proyecto Sender Policy Framework, "SPF es una técnica para prevenir la falsificación de direcciones de remitente" (SPF Project, 2021). Esta herramienta verifica la correcta configuración de los registros SPF para asegurar que solo los servidores autorizados pueden enviar correos electrónicos en nombre del dominio.

Spoofcheck analiza las configuraciones de los registros DNS relacionados con el correo electrónico de un dominio específico, tales como SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting &

Conformance). Estos registros son cruciales para validar la autenticidad de los correos electrónicos enviados desde un dominio y prevenir que sean falsificados por atacantes maliciosos.

- SPF es un protocolo que permite a los propietarios de dominios especificar qué servidores de correo tienen permiso para enviar correos electrónicos en nombre de su dominio
- DKIM añade una firma digital a los correos electrónicos, permitiendo a los receptores verificar que un correo realmente proviene del dominio especificado y que no ha sido alterado durante el tránsito.
- DMARC utiliza las políticas de SPF y DKIM para proporcionar una capa adicional de protección.

2.7.7 Espoofer

Espoofer es una herramienta versátil que se utiliza para la suplantación de identidad en redes. Aunque su principal uso es la evaluación de la seguridad de la red al probar su vulnerabilidad a ataques de suplantación de IP, también puede ser utilizada en el contexto de ataques de phishing. Los atacantes pueden emplear espoofer para falsificar la dirección IP de origen en los paquetes de red, haciendo que los correos electrónicos o mensajes enviados parezcan provenir de fuentes confiables.

Espoofer es una herramienta valiosa para evaluar la seguridad de la red frente a ataques de suplantación de IP. Según el equipo de CAIDA (Center for Applied Internet Data Analysis), "Spoofer ayuda a identificar y mitigar las vulnerabilidades de suplantación de IP en redes globales" (CAIDA, 2021). Esta capacidad es esencial para cualquier organización que busque fortalecer sus defensas contra ataques potenciales.

Este tipo de ataque implica falsificar la dirección IP de origen en paquetes de red, lo que permite a un atacante hacerse pasar por otra máquina en la red.

Espoofer realiza una serie de pruebas para determinar si una red permite el envío de paquetes con direcciones IP falsificadas. La herramienta puede generar informes detallados que ayudan a los administradores a comprender las debilidades en sus configuraciones de red y a tomar medidas correctivas.

2.7.8 TBomb

TBomb es una herramienta valiosa para realizar pruebas de resistencia en sistemas de comunicación. Según la documentación de su desarrollador, "TBomb permite a los usuarios enviar un gran volumen de mensajes o realizar llamadas repetidas, evaluando así la capacidad del sistema para manejar el tráfico masivo" (TBomb Project, 2021). Esta funcionalidad es esencial para identificar posibles puntos de falla en los sistemas de comunicación.

TBomb es una herramienta diseñada para realizar bombardeos de mensajes SMS y llamadas telefónicas. Utilizada tanto para fines educativos como para pruebas de resistencia en sistemas de comunicación, TBomb puede enviar una gran cantidad de mensajes o realizar llamadas repetidas en un corto período de tiempo. Esta herramienta es principalmente utilizada por profesionales de seguridad y desarrolladores para probar la resistencia de sistemas y aplicaciones frente a este tipo de ataques.

Entre sus funcionalidades principales se incluyen:

- Bombardeo de SMS: La herramienta puede enviar una gran cantidad de mensajes SMS a un número de teléfono específico, saturando la capacidad de recibir mensajes.
- Bombardeo de Llamadas: Similar al bombardeo de SMS, TBomb puede realizar múltiples llamadas telefónicas en rápida sucesión, lo que puede bloquear la línea telefónica del objetivo.

- Interfaz de Uso Sencillo: TBomb cuenta con una interfaz sencilla que facilita su uso, permitiendo a los usuarios configurar rápidamente los parámetros del bombardeo y ejecutar las pruebas.
- Personalización de Parámetros: Los usuarios pueden personalizar varios parámetros, como el número de mensajes o llamadas, la frecuencia y la duración, lo que permite realizar pruebas específicas y controladas.

2.8 Importancia de la concientización y prevención en seguridad informática

La concientización y la prevención en seguridad informática son fundamentales para proteger la integridad, confidencialidad y disponibilidad de la información en el entorno digital. La creciente sofisticación de las amenazas cibernéticas, como el phishing, el malware y los ataques de denegación de servicio, exige una preparación constante y una comprensión profunda de los riesgos asociados.

La concientización en seguridad informática implica educar a los usuarios sobre las amenazas cibernéticas y las mejores prácticas para evitar ser víctimas de ataques. Esto incluye reconocer correos electrónicos sospechosos, utilizar contraseñas fuertes y únicas, y mantener el software actualizado.

Además, la formación regular y las campañas de concientización pueden reducir significativamente la susceptibilidad a los ataques de ingeniería social y phishing. (Anderson & Moore, 2018)

Mientras que la prevención en seguridad informática se refiere a la implementación de medidas técnicas y administrativas para proteger los sistemas y la información. Esto abarca el uso de firewalls, sistemas de detección de intrusos, cifrado de datos y políticas de gestión de acceso. La prevención también incluye la creación de planes de respuesta a incidentes y la realización de

auditorías de seguridad periódicas para identificar y corregir vulnerabilidades. (Whitman & Mattord, 2019)

La combinación de concientización y prevención en seguridad informática ofrece varios beneficios. En primer lugar, ayuda a minimizar los riesgos de seguridad y a proteger los activos de la organización. En segundo lugar, fomenta una cultura de seguridad entre los empleados, lo que puede llevar a una mayor adherencia a las políticas de seguridad. Por último, la concientización y la prevención pueden mejorar la reputación de una organización al demostrar su compromiso con la protección de datos. (Pfleeger & Pfleeger, 2020)

CAPITULO III: METODOLOGÍA

Para realizar el desarrollo de este trabajo, se empleó una metodología de investigación, cuyo propósito es indagar las causas o razones del problema planteado, respondiendo a cómo y por qué podrían ocurrir las situaciones presentadas.

El trabajo tiene como objetivo demostrar que es posible robar información de los estudiantes universitarios mediante un ataque de phishing utilizando la información que las personas compartan en sitios web falsos, correos electrónicos, mensajes de texto y llamadas. Aunque no existe una metodología estándar para llevar a cabo este tipo de ataque, se basará en las metodologías empleadas en ataques de phishing previos y en técnicas de recolección de información.

Se considerarán los recursos de hardware disponibles para la realización del trabajo, teniendo en cuenta que, si resultan insuficientes, se realizarán ajustes en la metodología planteada. Además, se evaluarán las limitaciones de las herramientas a utilizar y las políticas de seguridad de la institución educativa, implementando cambios necesarios para cumplir con el objetivo del trabajo.

Para el desarrollo del trabajo se optó por open source, basándose en Kali Linux, GitHub, phyton, Zphisher, spoofcheck, espoofer y TBomb.

3.1 Metodología para un ataque de phishing

Existen varios métodos para realizar un ataque de phishing, que dependen de la finalidad que se tenga, si el objetivo es robar información personal, tarjetas de crédito, etc. Si bien no hay una metodología exacta a seguir, se proponen 4 fases para poder realizar cualquier tipo de ataque de phishing.

Fase 1: Investigación y Selección de Objetivos

- Seleccionar la víctima, que puede ser un individuo o una empresa.
- Recolección de datos sobre las víctimas potenciales
- Selección de la herramienta de ataque
- Extracción y almacenamiento de la información

Fase 2: Depurar la información

- Analizar la información extraída
- Decidir si es necesario depurar la información, de ser necesario se puede hacer manualmente o con el uso de una herramienta.
- Guardar la información depurada.

Fase 3: Realizar el ataque

- Seleccionar herramientas existentes o crear una herramienta para conseguir un ataque.
- Ingresar la información para empezar el ataque
- Desarrollar el ataque de phishing, verificar si este tuvo éxito o si es necesario buscar un nuevo método que se acople al objetivo.
- Guardar la información obtenida

Fase 4: Resultados y uso de información

- Monitorear la actividad y registrar la información
- Definir la finalidad que va a tener la información que se obtuvo
- Borrar rastros del ataque

Para un mejor entendimiento sobre el tema y la metodología que pueden usar los ciberdelincuentes para realizar el ataque, se realiza una propuesta de un diagrama de flujo que contiene las 4 fases mencionadas anteriormente. (Ver Figura 2)

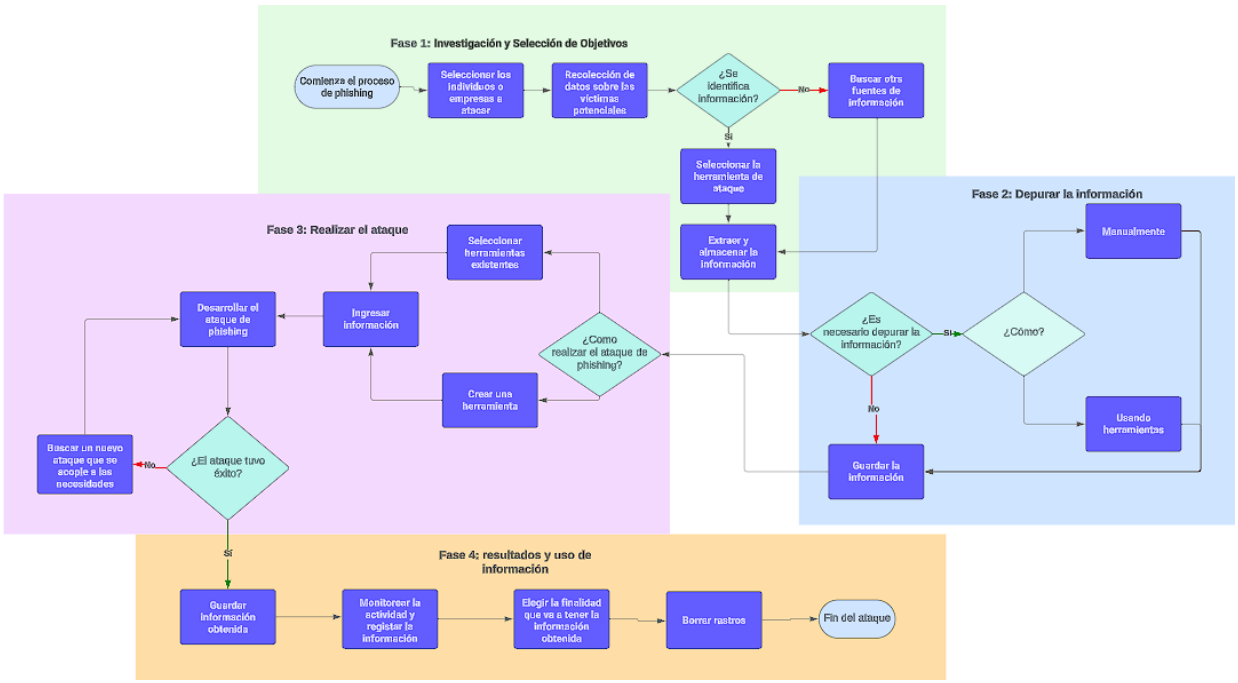

Figura 2. *Fases para realizar un ataque de phishing*

Nota: Este diagrama detalla el proceso sistemático y meticuloso que los ciberdelincuentes pueden seguir para llevar a cabo un ataque de phishing exitoso, desde la identificación y recolección de datos hasta la explotación y uso de la información obtenida.

3.2 Fases de metodología utilizada

Para el presente proyecto, se utilizó una metodología estructurada basada en prácticas aceptadas en el campo de la ciberseguridad, dividida en 6 fases principales que son:

Fase 1. Planificación y Preparación

- Identificación de Objetivos: Seleccionar a las víctimas potenciales mediante la recopilación de información inicial, para este caso de estudio se consideró a estudiantes universitarios.

Fase 2. Creación del Ataque

- Diseño del Mensaje de Phishing: Crear correos electrónicos, mensajes de texto o llamadas telefónicas convincentes que parezcan legítimos. Este paso incluye la utilización de técnicas de ingeniería social para que los mismo parezcan enviados por la universidad.
- Desarrollo de Sitios Web Falsos: Crear páginas web que imiten a las legítimas para engañar a las víctimas y recolectar sus credenciales. Para el estudio se utilizó redes sociales personales para evitar problemas legales.

Fase 3. Implementación del Ataque

- Envío de Mensajes de Phishing: Utilizar herramientas automatizadas como Zphisher, Spoofcheck, Espoofer y TBomb para enviar correos electrónicos y mensajes de texto, o para realizar llamadas telefónicas (smishing y vishing).
- Monitorización del Ataque: Supervisar las respuestas de las víctimas y registrar la información recopilada.

Fase 4. Recolección y Análisis de Datos

- Recolección de Credenciales: Recopilar la información ingresada por las víctimas en los sitios web falsos.
- Análisis de Resultados: Evaluar la efectividad del ataque mediante el análisis de la tasa de respuesta y el tipo de información obtenida.

Fase 5. Simulación y Evaluación en Entornos Controlados

- Realización de Simulaciones: Ejecutar ataques de phishing en un entorno controlado para educar a los usuarios (estudiantes) y medir su susceptibilidad.
- Evaluación y Retroalimentación: Proporcionar retroalimentación a los estudiantes sobre cómo reconocer y evitar ataques de phishing. (Ver Anexo A)

CAPITULO IV: SIMULACIÓN PARA ATAQUE DE PHISHING

4.1 Planteamiento para ataque de phishing

Los ataques de phishing se llevan a cabo principalmente porque son altamente efectivos para obtener información confidencial de las víctimas de manera rápida y con relativamente poco esfuerzo. Los ciberdelincuentes los prefieren debido a la simplicidad en la implementación y la alta tasa de éxito, ya que aprovechan la falta de conocimiento y la confianza de los usuarios en la legitimidad de los correos electrónicos y sitios web falsificados. (Jakobsson & Myers, 2007)

Además, los ataques de phishing pueden ser altamente lucrativos, proporcionando acceso a datos sensibles como credenciales de cuentas bancarias, información personal y detalles de tarjetas de crédito, que pueden ser vendidos en el mercado negro o utilizados para cometer fraudes financieros. (Hadnagy & Fincher, 2015)

4.2 Extracción de información del ataque

Existen varios tipos de ataques para realizar phishing, sin embargo, el presente proyecto se enfocará en cuatro tipos de ataques diferentes para demostrar la efectividad de estos. Los mismos que serán una página web para obtener credenciales de la víctima con la herramienta Zphisher, un correo electrónico para extorsionar por medio de Spoofcheck y Espoofer, mensajes de texto y llamadas con la ayuda de TBomb. Todas estas aplicaciones serán aplicadas en Kali Linux.

Se detalla un resumen de las herramientas a utilizar:

1. Zphisher: Página web
2. Spoofcheck y Espoofer: Correo electrónico
3. TBomb: mensajes de texto y llamadas

A continuación, se describirá la guía de instalación y configuración de cada herramienta:

1. Zphisher

Es una herramienta de phishing que facilita la creación de páginas web que imitan la apariencia de sitios legítimos con el objetivo de engañar a las víctimas y obtener información sensible como contraseñas y datos personales. Seguidamente, se detalla la guía de instalación y configuración de Zphisher para empezar con el ataque.

Paso 1: Clonación del Repositorio

Para comenzar, se debe clonar el repositorio Zphisher desde GitHub. Esto se logra ejecutando el comando **git clone https://github.com/htr-tech/zphisher.git** mostrado en la Figura 3. Antes de clonar el repositorio, es importante ejecutar el comando sudo su para cambiar al usuario root (superusuario), lo que permite ejecutar comandos con privilegios elevados.

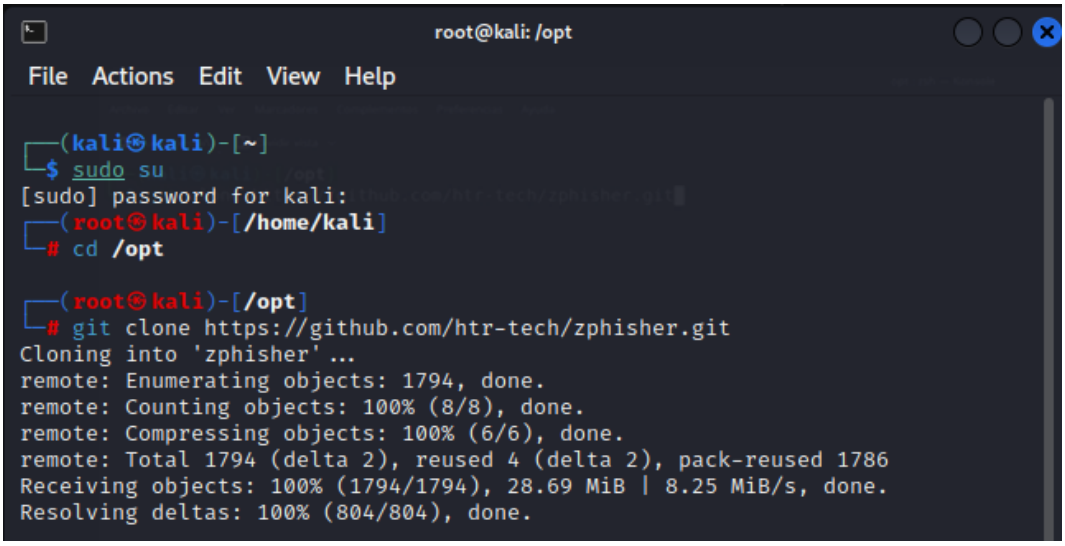

***Figura 3**. Clonación del Repositorio zphisher desde GitHub*

Paso 2: Exploración del Directorio

Una vez clonado el repositorio, con el comando **ls** se puede verificar que en el directorio **/opt** hay dos subdirectorios: **microsoft y zphisher**. Como siguiente paso se debe cambiar al directorio zphisher utilizando **cd zphisher**. Dentro de este directorio, otro comando ls mostrará los archivos y directorios que contiene el repositorio zphisher, como se indica en la Figura 4.

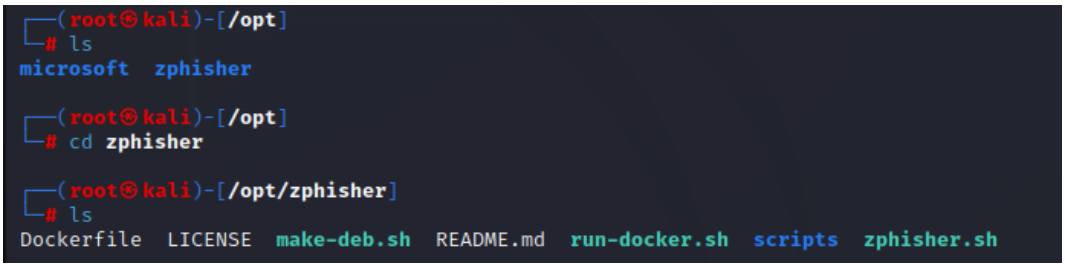

Figura 4. *Listar Contenidos del Directorio zphisher*

Paso 3: Ejecución del Script de Instalación

Para instalar y configurar zphisher, se debe ejecutar el script principal **zphisher.sh**. Esto se hace con el comando **bash zphisher.sh**, como se muestra en la Figura 5. Este script comienza instalando los paquetes necesarios, verificando si ya están instalados, comprobando el estado de la conexión a Internet y buscando actualizaciones.

Figura 5. *Ejecución del Script zphisher.sh*

Paso 4: Selección del Tipo de Ataque

Una vez que el script de instalación ha completado su configuración inicial, zphisher presenta una interfaz para seleccionar el tipo de ataque de phishing que se desea realizar. En la Figura 6 se puede ver la pantalla de selección donde se listan múltiples plataformas populares como Facebook, Instagram, Google, y muchas más. Se selecciona una opción introduciendo el número correspondiente. Por ejemplo, para seleccionar Facebook, se introduce 01 y se presiona Enter. A continuación, se elige el tipo de página de inicio de sesión falsa que se quiere utilizar.

En este paso, se muestran las opciones de ataques disponibles y se permite al usuario configurar y personalizar el ataque según sus necesidades específicas. Esto asegura que la herramienta esté lista para simular ataques de phishing en diversas plataformas y escenarios.

***Figura 6**. Interfaz de usuario de la herramienta zphisher*

Paso 5: Selección del Servicio de Redirección de Puertos

Después de seleccionar el tipo de ataque y la página de inicio de sesión falsa, zphisher ofrece varias opciones para el servicio de redirección de puertos, como se muestra en la Figura 7. Aquí, el usuario puede elegir entre opciones como Localhost, Cloudflared, y LocalXpose. En este caso, se selecciona Cloudflared introduciendo 02 y presionando Enter.

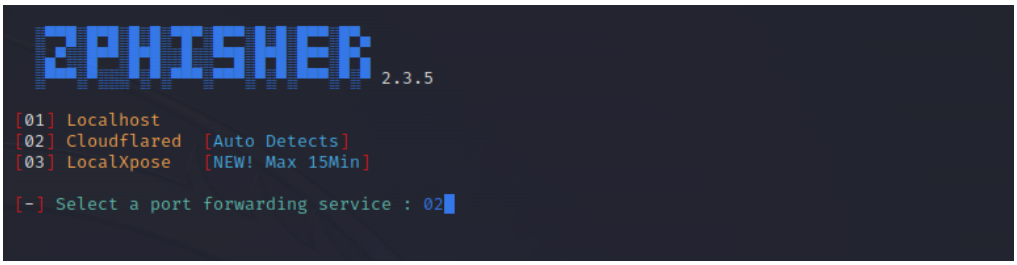

***Figura 7**. Selección del Servicio de Redirección de Puertos*

La herramienta ofrece tres opciones para la redirección de puertos:

- [01] Localhost: Redirección local.
- [02] Cloudflared: Detección automática (seleccionado por el usuario en este caso).
- [03] LocalXpose: Una nueva opción con un límite de 15 minutos.

En este paso, se configura la redirección de puertos necesaria para que el ataque de phishing sea accesible a través de Internet, utilizando el servicio elegido. Esto asegura que la página falsa creada esté disponible para los objetivos en línea.

Paso 6: Generación y Configuración del Enlace de Phishing

Una vez seleccionado el servicio de redirección de puertos, zphisher genera una URL que se puede utilizar para llevar a cabo el ataque de phishing. En la Figura 8 se muestra la URL generada por Cloudflared. Esta URL debe ser compartida con el objetivo para que acceda a la página falsa. Además, se generan múltiples URLs para mayor flexibilidad. La herramienta se queda esperando la entrada de credenciales, y se puede salir del proceso utilizando Ctrl + C.

Figura 8. *URLs Generadas que redirigen al sitio de phishing*

Paso 7: Página de Phishing Activa

Finalmente, cuando la víctima accede a la URL generada, se le presenta una página de inicio de sesión falsa que simula ser de una plataforma popular, como Instagram. En la Figura 9 se muestra un ejemplo de la página de phishing para Instagram. Esta página solicita las

credenciales de inicio de sesión de la víctima, las cuales, una vez ingresadas, son capturadas por la herramienta zphisher.

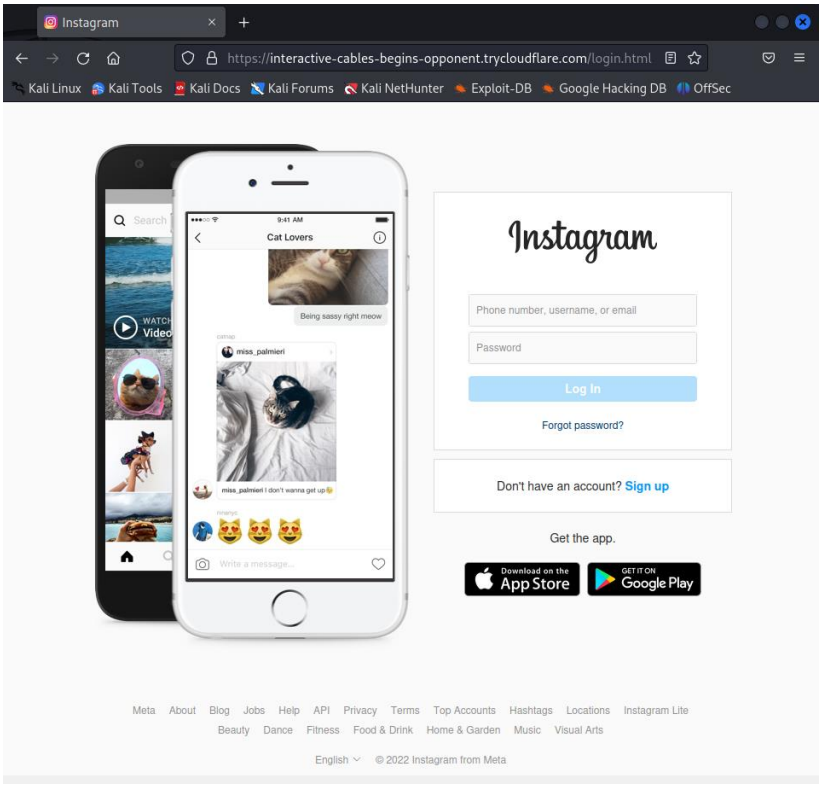

Figura 9. *Página de Inicio de Sesión de Phishing*

La interfaz de usuario de la página de phishing es prácticamente idéntica a la página real de inicio de sesión de Instagram. Incluye campos para que el usuario ingrese su número de teléfono, nombre de usuario o correo electrónico, y su contraseña. También incluye botones como "Log In", "Forgot password?", "Sign up", y enlaces para descargar la aplicación desde Google Play y App Store.

El objetivo es engañar a las víctimas para que ingresen sus credenciales de inicio de sesión en esta página falsa, creyendo que es la página auténtica de Instagram. Cuando la víctima ingresa sus datos y hace clic en "Log In", la información se envía al atacante a través de la herramienta Zphisher.

Paso 8: Captura de Credenciales

Una vez que la víctima introduce sus credenciales en la página de phishing, zphisher captura esta información y la muestra en la terminal. En la Figura 10 se puede ver cómo zphisher notifica que se ha encontrado información de inicio de sesión, incluyendo el nombre de usuario y la contraseña, y guarda esta información en un archivo (auth/usernames.dat). La herramienta queda esperando la siguiente entrada de credenciales.

***Figura 10**. Información de Inicio de Sesión Encontrada*

La herramienta ha capturado credenciales de una víctima: Login info Found!!.

- Cuenta: La dirección de correo electrónico capturada es angie.micaela@hotmail.com.
- Contraseña: La contraseña capturada es A1234E566.

En este último paso, zphisher ha capturado las credenciales ingresadas por la víctima, permitiendo al atacante obtener acceso a la cuenta comprometida. La herramienta sigue en espera de más credenciales hasta que el proceso sea detenido manualmente.

2. Espoofer

Espoofer permite enviar paquetes con direcciones IP de origen falsificadas. En un ataque de phishing, esto puede ser utilizado para enviar correos electrónicos que parezcan venir de una fuente legítima, como una institución financiera o una empresa conocida.

Los atacantes pueden utilizar espoofer para crear entornos simulados que imiten sistemas seguros, engañando a las víctimas para que proporcionen información confidencial como contraseñas y detalles bancarios.

A continuación, se detallan la guía de instalación y configuración de Spoofcheck para empezar con el ataque, debido a que este es un requerimiento previo para ejecutar la aplicación Espoofer.

Paso 1: Clonación del Repositorio

Para comenzar, se debe clonar el repositorio spoofcheck desde GitHub. Esto se logra ejecutando el comando **git clone https://github.com/BishopFox/spoofcheck.git** mostrado en la Figura 11. Antes de clonar el repositorio, es importante ejecutar el comando sudo su para cambiar al usuario root (superusuario), lo que permite ejecutar comandos con privilegios elevados.

Paso 2: Instalación de Dependencias

Una vez clonado el repositorio, es necesario instalar las dependencias requeridas para ejecutar spoofcheck. En este caso, se necesita instalar Python 3.11. Para hacerlo, se ejecuta el comando **sudo apt install python3.11**. Este comando actualizará el sistema e instalará las versiones necesarias de Python y sus dependencias. (Ver figura 11)

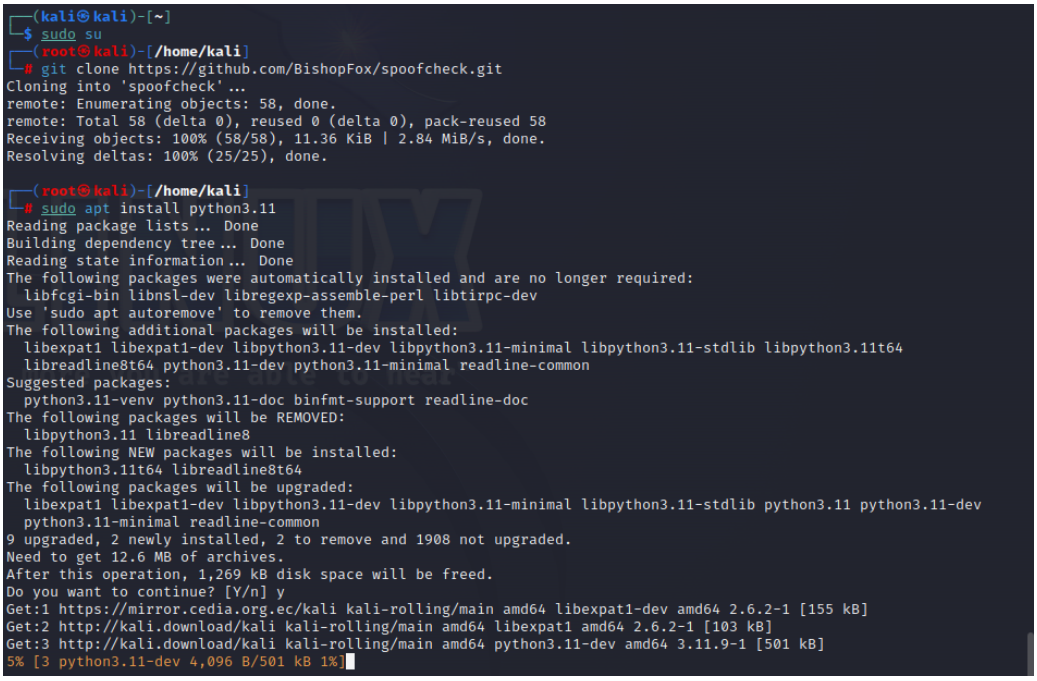

***Figura 11**. Clonación del Repositorio Spoofcheck desde GitHub e instalación de Python 3.11*

Paso 3: Instalación de Dependencias del Proyecto

Luego de instalar Python 3.11, se deben instalar las dependencias específicas del proyecto spoofcheck. Esto se realiza ejecutando el comando **pip install -r requirements.txt**, como se muestra en la Figura 12. Este comando lee el archivo requirements.txt y descarga e instala todas las librerías y paquetes necesarios para que spoofcheck funcione correctamente.

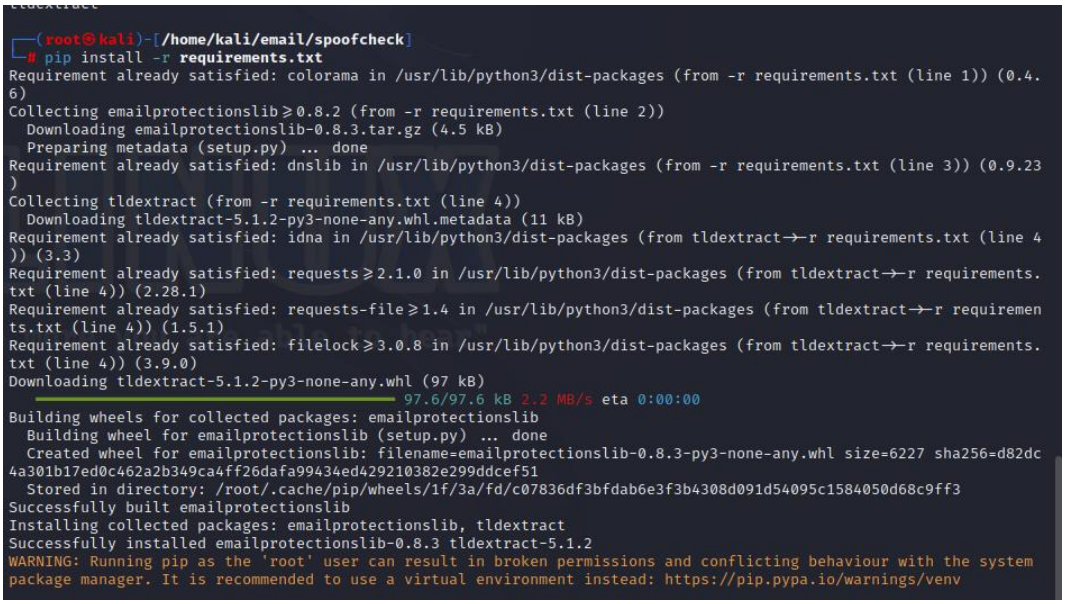

***Figura 12**. Instalación de Dependencias con pip*

Paso 4: Clonación del Repositorio espoofer

Para ampliar las herramientas disponibles, también se debe clonar el repositorio espoofer desde GitHub. Esto se realiza ejecutando el comando **git clone https://github.com/chenjj/espoofer.git desde el directorio home/kali/email**, como se muestra en la Figura 13. Después de clonar el repositorio, se utiliza el comando ls para verificar que los directorios espoofer y spoofcheck están presentes.

***Figura 13**. Clonación del Repositorio Espoofer desde GitHub*

Paso 5: Instalación de Dependencias del Proyecto Espoofer

Una vez clonado el repositorio espoofer, se deben instalar las dependencias específicas del proyecto. Esto se realiza ejecutando el comando **pip install -r requirements.txt**, como se muestra en la Figura 14. Este comando lee el archivo requirements.txt y descarga e instala todas las librerías y paquetes necesarios para que espoofer funcione correctamente.

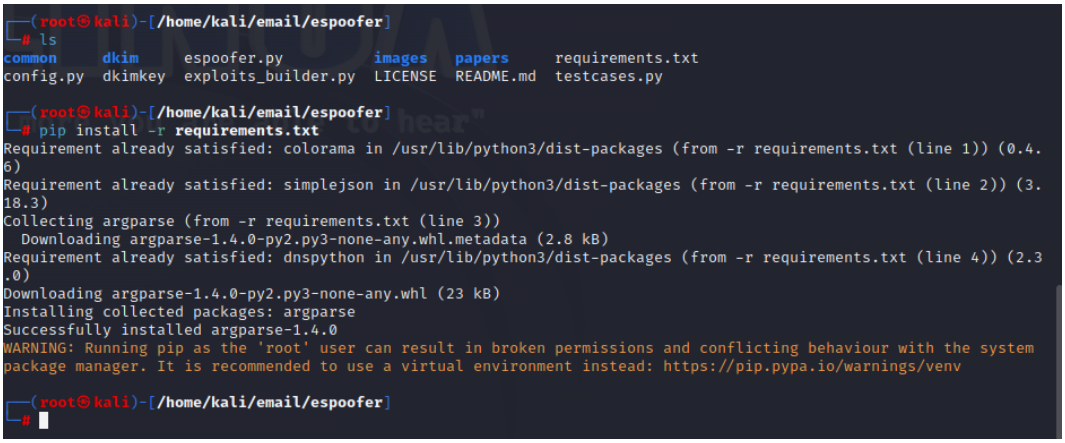

***Figura 14**. Listado de Contenidos del Directorio espoofer e Instalación de Dependencias con pip*

En este paso, se aseguran todas las dependencias necesarias para la correcta ejecución de las herramientas spoofcheck y espoofer, permitiendo así su utilización sin problemas de compatibilidad o faltantes.

Paso 6: Configuración de Entorno Virtual

Para evitar problemas de permisos y compatibilidad, se recomienda utilizar un entorno virtual de Python. Si al ejecutar spoofcheck.py se encuentra el error **ModuleNotFoundError: No**

module named 'Resolver', se debe instalar el entorno virtual utilizando el comando **sudo apt-get install python3-venv**, como se muestra en la Figura 15.

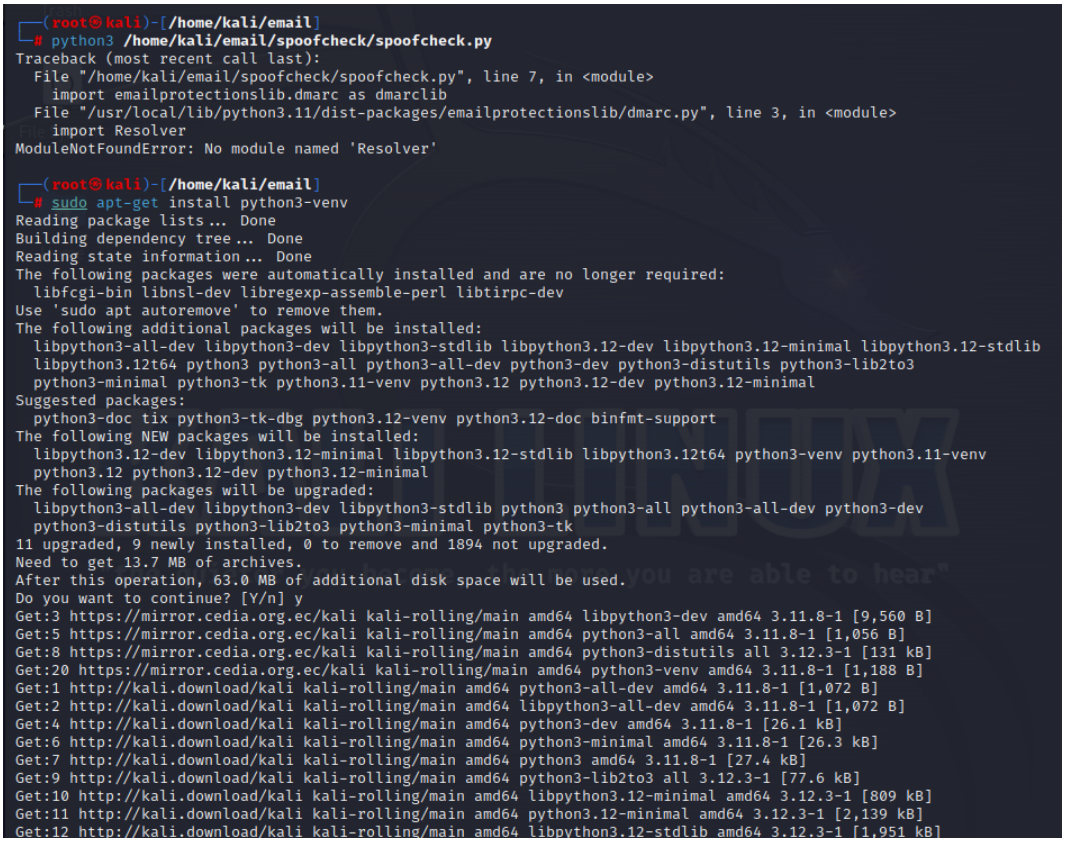

***Figura 15**. Ejecución de spoofcheck e instalación de un entorno virtual*

En este paso, se asegura que todas las dependencias necesarias para la correcta ejecución de las herramientas spoofcheck y espoofer están instaladas, y se configura un entorno virtual para evitar problemas de permisos y conflictos de librerías.

Paso 7: Creación y Activación del Entorno Virtual

Una vez instalado **python3-venv**, se crea un entorno virtual utilizando **python3 -m venv spoofcheck_env** y se activa con **source spoofcheck_env/bin/activate**, como se muestra en la Figura 16. Dentro del entorno virtual, se instalan las dependencias necesarias con **pip3 install emailprotectionslib dnspython.**

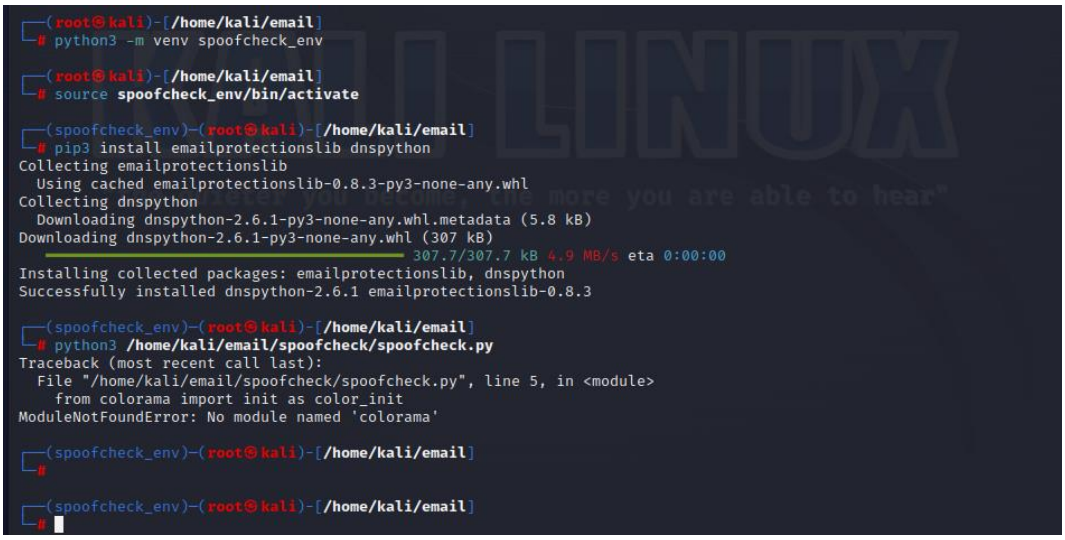

***Figura 16**. Creación y activación del entorno virtual*

Paso 8: Ejecución de SpoofCheck

Finalmente, para verificar si un dominio es vulnerable a ataques de spoofing, se ejecuta **spoofcheck.py** con el dominio de interés. En la Figura 17 se muestra la ejecución del comando **python3 /home/kali/email/spoofcheck/spoofcheck.py puce.edu.ec**, que verifica la configuración del dominio puce.edu.ec y confirma si es susceptible a spoofing al no tener registros SPF o DMARC.

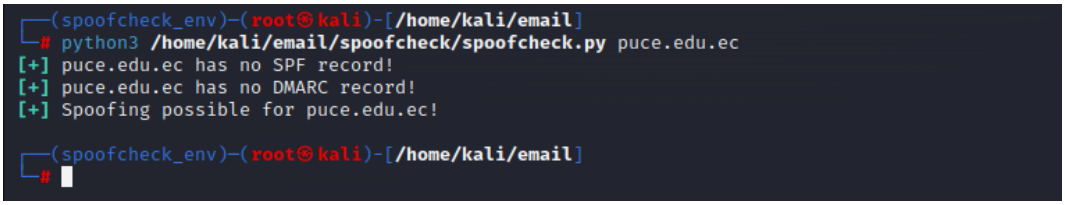

***Figura 17**. Ejecución de spoofcheck*

Paso 9: Ejecución de Espoofer

Para realizar un ataque de spoofing, se utiliza espoofer. En la Figura 18 se muestra la ejecución del comando **python3 espoofer.py -m c -id client_a1 --helo puce.edu.ec --mfrom**

jjcedeno@puce.edu.ec --rcptto jjcedeno@puce.edu.ec. Este comando envía un correo electrónico falsificado utilizando las credenciales y configuración especificadas.

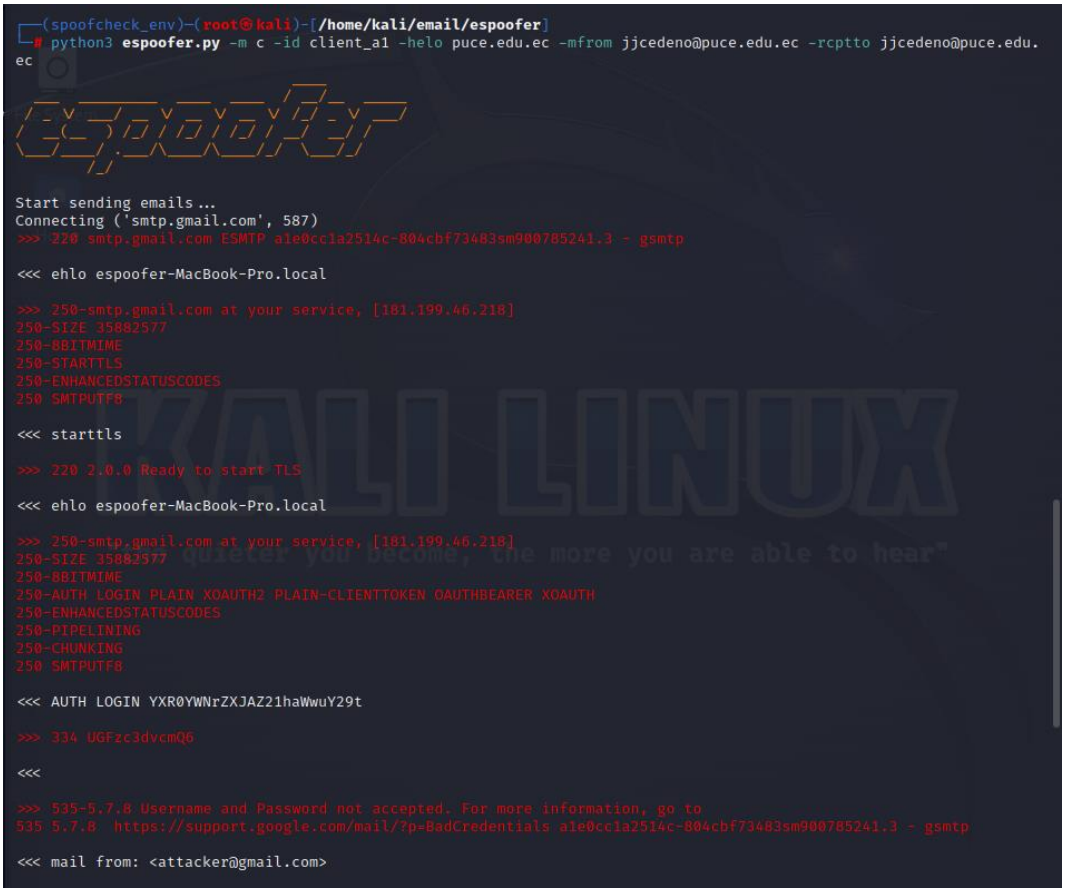

Figura 18. *Ejecución de espoofer*

Los parámetros incluyen:

-m c: Modo de envío de correo.

-id client_al: Identificación del cliente.

-helo puce.edu.ec: El comando HELO, que identifica el dominio del remitente.

-mfrom jjcedeno@puce.edu.ec: Dirección de correo del remitente falsificado.

-rcptto jjcedeno@puce.edu.ec: Dirección de correo del destinatario.

Paso 10: Verificación del Correo de Spoofing

Finalmente, se verifica que el correo electrónico falsificado ha sido enviado correctamente y aparece en la bandeja de entrada o en el correo no deseado del destinatario (Ver Figura 19). En la Figura 20 se muestra un ejemplo de un correo electrónico falsificado recibido en la cuenta de destino.

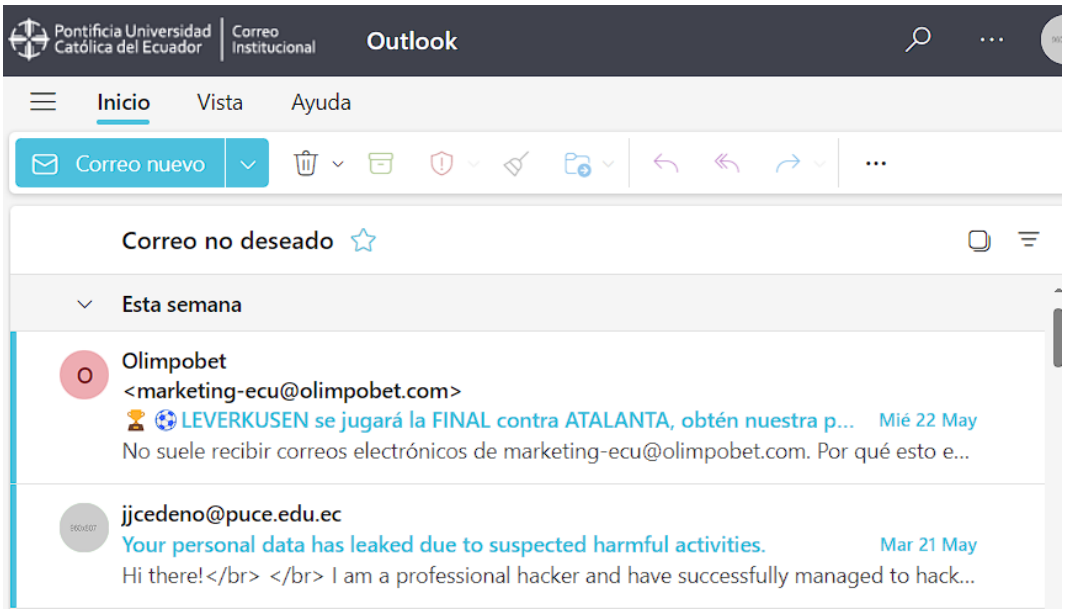

Figura 19.*Interpretación del correo*

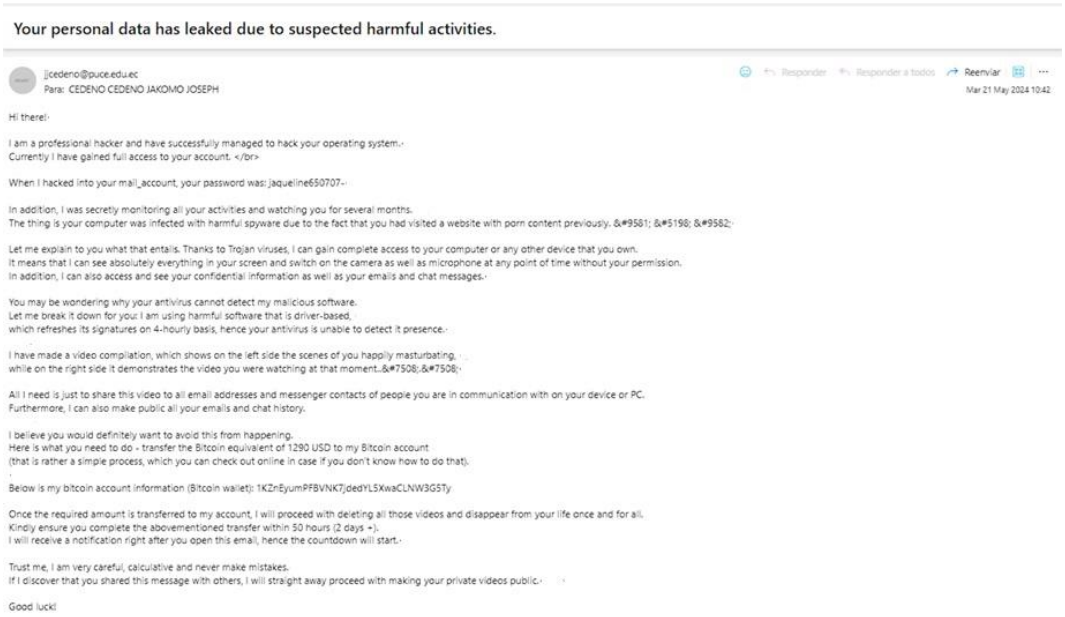

Figura 20. *Descripción del correo*

Este correo es un claro ejemplo de un intento de phishing o de extorsión. El remitente afirma ser un hacker y trata de asustar al destinatario mencionando una supuesta filtración de datos personales. Este tipo de correos suelen intentar engañar a los usuarios para que proporcionen información sensible o realicen pagos.

3. TBomb

TBomb es conocida por su capacidad para enviar una gran cantidad de mensajes de texto o realizar llamadas telefónicas en poco tiempo. Esto puede ayudar a evaluar cómo los sistemas de comunicación manejan el tráfico masivo y a identificar posibles puntos de falla o debilidad.

A continuación, se detallan la guía de instalación y Configuración de TBomb para empezar con el ataque.

Paso 1: Clonación del Repositorio

Para comenzar, se debe clonar el repositorio TBomb desde GitHub. Esto se logra ejecutando el comando **git clone https://github.com/TheSpeedX/TBomb.git**, como se muestra en la Figura 21. Antes de clonar el repositorio, es importante ejecutar el comando sudo su para cambiar al usuario root (superusuario), lo que permite ejecutar comandos con privilegios elevados.

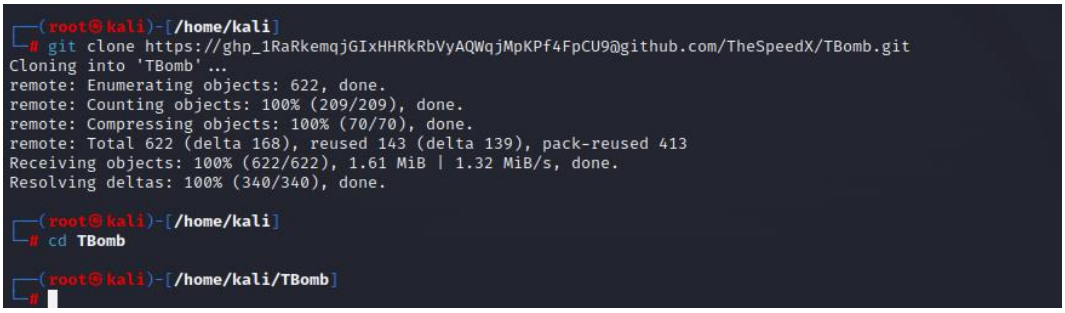

Figura 21*.Clonación del Repositorio TBomb desde GitHub*

El comando mostrado en la imagen se utiliza para clonar el repositorio Tbomb desde GitHub con un token personal.

Paso 2: Inicio de TBomb

Al iniciar TBomb, se presenta una pantalla de bienvenida, como se muestra en la Figura 22. En esta pantalla se recomienda moverse a la versión PIP de TBomb para una mayor estabilidad. Se indica presionar cualquier tecla para continuar.

Figura 22. *Pantalla de bienvenida de TBomb*

Paso 3: Menú Principal de TBomb

Después de la pantalla de bienvenida, TBomb muestra el menú principal con varias opciones, como se muestra en la Figura 23. Las opciones disponibles son:

- Iniciar SMS Bomber
- Iniciar Call Bomber
- Iniciar Mail Bomber (aún no disponible)
- Actualizar (funciona en Linux y emuladores de Linux)
- Salir

Figura 23. *Menú principal de Tbomb*

Paso 4: Configuración del SMS Bomber

Al seleccionar la opción de SMS Bomber, se pide al usuario que ingrese varios parámetros para configurar el ataque, como se muestra en la Figura 24. Los parámetros incluyen:

- Código del país (sin el símbolo +).
- Número de teléfono del objetivo.
- Número de SMS a enviar (máximo 100).
- Tiempo de retardo entre mensajes (en segundos).
- Número de hilos (se recomienda 1).

Figura 24. *Ingreso de Configuraciones para el Ataque de SMS*

Una vez ingresados estos parámetros, TBomb comenzará a enviar los mensajes SMS al número de teléfono especificado.

En este último paso, se completa la configuración y ejecución de TBomb para realizar ataques de SMS Bomber, permitiendo al usuario definir los parámetros específicos del ataque.

Paso 5: Ejecución del SMS Bomber

Después de ingresar los parámetros de configuración, TBomb muestra un resumen de la configuración y comienza el ataque, como se muestra en la Figura 25 y en la Figura 26. Se recomienda mantenerse conectado a internet durante el ataque. El usuario puede suspender el bomber presionando CTRL+Z o reanudarlo presionando ENTER.

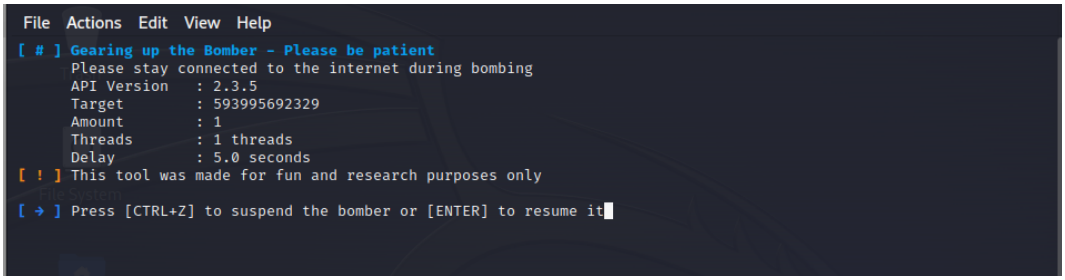

Figura 25*.Ataque por SMS*

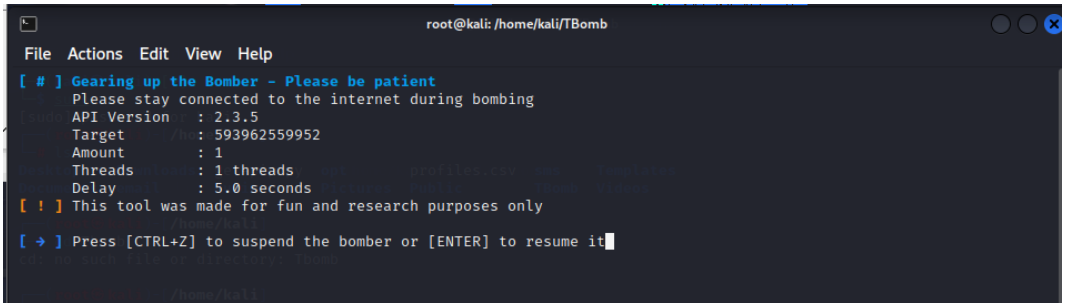

Figura 26*. Ataque por llamada*

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

A través de la simulación de ataques de phishing, que incluyeron páginas web falsas, correos electrónicos engañosos, mensajes de texto y llamadas, se logró aumentar la conciencia de los estudiantes universitarios sobre los riesgos de pérdida de información. La participación en estas simulaciones ha permitido a los estudiantes identificar las señales de alerta y las estrategias empleadas en los ataques de phishing, mejorando significativamente su capacidad para prevenir estos incidentes.

El estudio ha identificado las principales técnicas de phishing utilizadas por los atacantes informáticos, revelando que estos métodos incluyen la creación de páginas web falsas que imitan sitios legítimos, el envío de correos electrónicos fraudulentos que aparentan ser de fuentes confiables, y el uso de mensajes de texto y llamadas para obtener información sensible. Esta identificación ha sido fundamental para diseñar simulaciones realistas y efectivas que han permitido a los estudiantes comprender el impacto potencial de estos ataques en su privacidad y seguridad.

Asimismo, la implementación de ataques de phishing en un entorno controlado proporcionó a los estudiantes una experiencia segura y educativa, permitiéndoles aplicar los conocimientos adquiridos en un escenario práctico sin riesgo real. Esta metodología demostró ser efectiva para educar a los estudiantes sobre las amenazas de phishing y fortalecer su capacidad para proteger su información personal y académica.

5.2 Recomendaciones

Es fundamental que las universidades implementen programas de capacitación continua en ciberseguridad para estudiantes y personal. Estos programas deben incluir módulos específicos

sobre phishing y otras amenazas cibernéticas, proporcionando a los participantes las habilidades necesarias para identificar y prevenir ataques. Estas campañas pueden incluir simulaciones de phishing, talleres interactivos y materiales educativos.

Proporcionar y fomentar el uso de herramientas de seguridad, como software antivirus, filtros de correo electrónico y extensiones de navegador que bloqueen sitios web maliciosos, puede ayudar a proteger a los estudiantes contra los ataques de phishing.

Fomentar una cultura de colaboración y reporte de incidentes en la que los estudiantes se sientan cómodos informando sobre intentos de phishing y otros incidentes de seguridad a las autoridades universitarias. Un sistema de reporte efectivo puede ayudar a identificar y mitigar amenazas de manera más rápida y eficiente.

Bibliografía

(s.f.).

Abawajy, J. (2014). *User preference of cyber security awareness delivery methods.* (Vol. 33(3)). Behaviour & Information Technology,. doi:10.1080/0144929X.2013.781637

Abraham, S., & Chengalur-Smith, I. (2010). *An overview of social engineering malware: Trends, tactics, and implications.* (Vol. 32(3)). Technology in Society. doi:10.1016/j.techsoc.2010.07.001

Anderson, R., & Moore, T. (2018). *Information Security Economics: Lessons Learned and Unanswered Questions* (Vol. 16(3)). IEEE Security & Privacy. doi:10.1109/MSP.2018.2701177

Antonsen, R. (2017). *Understanding Cybercrime: A Guide for Developing Countries.* International Telecommunication Union.

Castro, A. (15 de septiembre de 2023). *Internetizado*. Obtenido de Internetizado: https://www.internetizado.com/linux/kali

Center for Applied Internet Data Analysis (CAIDA). (2021). Obtenido de Spoofer Project.: https://www.caida.org/projects/spoofer/

Chacon, S., & Straub, B. (2014). *Pro Git (2nd ed.).* Apress. doi:https://doi.org/10.1007/978-1-4842-0076-6

Computerworld. (2023). *Ingeniería social: definición, ejemplos y técnicas*. Obtenido de Computerworld: https://cso.computerworld.es/articulo/ingenieria-social

Doe, J. (2020). *Introduction to Ethical Hacking Tools.* . Cybersecurity Publishing.

Feller, J., & Fitzgerald, B. (2002). *Understanding Open Source Software Development.* . Addison-Wesley.

GitHub, I. (2021). *Features*. Obtenido de https://github.com/features

GitHub, Inc. (2021). *Features*. Obtenido de https://github.com/features

Guaña-Moya, J. (2023). *La importancia de la seguridad informática en la educación digital: retos y soluciones.* Quito: Saberes del conocimiento. doi:10.26820/recimundo/7.(1).enero.2023.609-616

Guaña-Moya, J., Chiluisa-Chiluisa, M. A., Jaramillo-Flores, P., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022, June). Ataques de phishing y cómo prevenirlos Phishing attacks and how to prevent them. *IEEE*, (pp 1-6). doi:10.23919/CISTI54924.2022.9820161

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 87-100.

Hadnagy, C., & Fincher, M. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails.* . Wiley.

Herrera, E. (2016). *El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal.* Quito: UCE.

Hong, J. (2012). *The state of phishing attacks* (Vol. 50(10)). Communications of the ACM. doi:10.1145/2063176.2063197

Jakobsson, M., & Myers, S. (2007). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.* . Wiley.

Jansson, K., & Von Solms, R. (2013). *Phishing for phishing awareness.* (Vol. 32(6)). Behaviour & Information Technology. doi:10.1080/0144929X.2011.632650

Jones, A. (2019). *Understanding Phishing Attacks and Their Impact on Security.* (Vol. 22(3)). Journal of Cybersecurity.

Kaspersky. (2020). *10 Consejos para protegerte del phishing*. Obtenido de Kaspersky: https://latam.kaspersky.com/blog/10-consejos-para-protegerte-del-phishing/

Kaspersky. (2024). *Cómo reconocer y evitar correos electrónicos de phishing*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Loeliger, J., & McCullough, M. (2012). *Version Control with Git (2nd ed.).* O'Reilly Media.

Martínez, P. (2019). *Incidencia del Phishing en el Sector Bancario Ecuatoriano.* (Vol. 10(2)). Revista de Seguridad Informática.

McAfee. (2021). *Cómo evitar las estafas de phishing por correo electrónico.* Obtenido de McAfee: https://www.mcafee.com/blogs/phishing-email-how-to-avoid/

Miller, C., & Davis, E. (2020). *Implementing comprehensive security policies in higher education.* (Vol. 12(4)). Cybersecurity Review.

Norton. (2018). *¿Qué es la ingeniería social?* Obtenido de Norton: https://co.norton.com/blog/que-es-la-ingenieria-social

Oliviera, D., Sabt, M., Ben Othmane, L., & El-Moussaoui, M. (2017). *SMiShing attacks and mitigation methods.* (Vol. 70). Computers & Security. doi:10.1016/j.cose.2017.07.008

ORACLE. (31 de MAYO de 2022). *ORACLE*. Obtenido de ORACLE: https://developer.oracle.com/es/learn/technical-articles/what-is-python

Parrish, J. L., Bailey, J. L., & Courtney, J. F. (2009). *A personality-based model for determining susceptibility to phishing attacks.* Proceedings of the Southern Association for Information Systems Conference,.

Pfleeger, C. P., & Pfleeger, S. L. (2020). *Security in Computing (5th ed.).* . Prentice Hall.

Raymond, E. S. (1999). *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary.* O'Reilly Media.

Red Hat. (24 de Enero de 2023). *Red Hat*. Obtenido de Red Hat: https://www.redhat.com/es/topics/open-source/what-is-open-source

Rosero, L. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático.* Quito: Universidad Politécnica Salesiana. Obtenido de http://dspace.ups.edu.ec/handle/123456789/21699

Ruiz, F. C. (2023). Herramientas digitales para fomentar la alfabetización mediática en la era digital. *Revista Ingenio global*, 2(1), 35-45.

Sender Policy Framework Project. (2021). *SPF*. Obtenido de Protect Against E-mail Address Forgery: https://www.open-spf.org

Smith, A. (2021). *Cybersecurity Practices and Legal Implications.* . TechLaw Publications.

Solleiro Rebolledo, J. L., Castañón Ibarra, R., Guillén Valencia, Á. D., Hernández Molina, T. Y., & Solís Mérida, N. (2022). *Vigilancia tecnológica en ciberseguridad: Tendencias tecnológicas (Boletín No. 2).* Universidad Nacional Autónoma de México, Instituto de Ciencias Aplicadas y Tecnología. Obtenido de https://www.redinnovagro.in/pdfs/cyber.pdf

Sysmantec. (2018). *nternet Security Threat Report*. Obtenido de https://www.symantec.com/security-center/threat-report

TBomb Project. (2021). *TBomb*. Obtenido de SMS and Call Bomber: https://github.com/TheSpeedX/TBomb

Tigselema-Egre, S., Villarroel-Molina, R., Guaña-Moya, J., & Sánchez Paredes, W. I. (2024). Análisis de Vulnerabilidades de Ciberseguridad Mediante Técnicas de Ciencia de Datos. *Revista Científica y Tecnológica VICTEC*, 5(8), 95-104.

Van Rossum, G. (1995). *Python Tutorial.* Centrum voor Wiskunde en Informatica (CWI).

White, K. (2021). *The impact of ransomware on educational institutions.* (Vol. 18(1)). Journal of Computer Security.

Whitman, M. E., & Mattord, H. J. (2019). *Principles of Information Security (6th ed.).* . Cengage Learning.

ANEXOS

Anexo A: Capacitación a Estudiantes Universitarios

Durante el desarrollo de esta tesis, se realizó una capacitación sobre concientización y prevención de riesgos relacionados con ataques de phishing a un grupo de estudiantes universitarios. Esta capacitación tuvo como objetivo principal sensibilizar a los participantes sobre las técnicas utilizadas en los ataques de phishing y proporcionarles herramientas para protegerse contra estas amenazas.

La capacitación incluyó una sesión teórica sobre la naturaleza de los ataques de phishing, seguida de una demostración práctica de cómo se realizan estos ataques en un entorno controlado con la herramienta de Zphisher. Se discutieron las mejores prácticas de seguridad y se respondieron preguntas de los participantes para asegurar una comprensión profunda del tema.

Anexo B: Encuesta a Estudiantes Universitarios

Al finalizar la capacitación, se realizó una encuesta a los 18 estudiantes participantes para evaluar el impacto de la capacitación y su nivel de conocimiento sobre los ataques de phishing antes y después de la sesión. A continuación, se presentan las preguntas de la encuesta y un resumen de los resultados obtenidos.

Encuesta de Evaluación

- ¿Cuántos estudiantes entendieron donde estaba la documentación de los repositorios en Github para la clonación del script de Zphisher?

  Todos (18)

- ¿Tuvieron los estudiantes problemas con la clonación de los repositorios en Github?

  Sí: 3 estudiantes

No: 15 estudiantes

- ¿Cuántos estudiantes tuvieron problemas con la instalación?

  Ningún estudiante

- ¿Cuántos estudiantes consiguieron abrir la aplicación?

  Si: 15 estudiantes

  No: 3 estudiantes

- ¿Cuántos estudiantes seleccionaron el servicio de redirección de puertos “Local Host”?

  12 estudiantes

- ¿Cuántos estudiantes seleccionaron el servicio de redirección de puertos “Cloudflared”?

  3 estudiantes

Resultados de la Encuesta

Los resultados de la encuesta muestran que la capacitación fue efectiva en aumentar el conocimiento y la comprensión de los estudiantes sobre los ataques de phishing. La mayoría de los participantes indicó que ahora se sienten más capacitados para identificar y protegerse contra estos ataques.

Anexo C: Materiales Utilizados en la Capacitación

Presentación de la Capacitación

Figura 27. *Presentación de la capacitación*

Figura 28. *Presentación de la demostración gráfica*

Se adjunta la presentación utilizada durante la capacitación, que incluye diapositivas con la teoría sobre phishing, ejemplos de correos electrónicos de phishing y demostraciones prácticas.

Esparza, A. (2024). Concientización y prevención de riesgos en universitarios mediante simulación de ataques de phishing [Diapositivas de PowerPoint]. Presentación interna. https://www.canva.com/design/DAGHC8ydmRk/CjbDvDaQWozlALyKTPSUrw/edit