UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

APLICACIÓN DE MEDIDAS DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA SECCIÓN ACADÉMICA DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA (UPSE) – FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD

AUTOR

ALAY MEREJILDO BYRON ALEXANDER

MODALIDAD DE TITULACIÓN

EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Ing. Jaramillo Infante Mónica Karina Mgt.

Santa Elena, Ecuador

Año 2024

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino Mgt.
DIRECTOR DE LA CARRERA

Ing. Mónica Jaramillo Infante Mgt.
TUTOR

Ing. Carlos Castillo Yagual, Mgt.
DOCENTE ESPECIALISTA

Ing. Mónica Jaramillo Infante Mgt.
DOCENTE GUÍA UIC

UPSE

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Alay Merejildo Byron Alexander, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 18 dias del mes de junio del año 2024

TUTOR

Ing. Mónica Karina Jaramillo Infante, Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **ALAY MEREJILDO BYRON ALEXANDER**

DECLARO QUE:

El trabajo de Titulación APLICACIÓN DE MEDIDAS DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA SECCIÓN ACADÉMICA DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA (UPSE) – FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 18 días del mes de junio del año 2024

EL AUTOR

Byron Alexander Alay Merejildo

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado (Titulo del ensayo), presentado por el estudiante, ALAY MEREJILDO BYRON ALEXANDER fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 4%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

CERTIFICADO DE ANÁLISIS
magister

PROYECTO DE TITULACION BYRON ALAY MEREJILDO

4% Textos sospechosos

4% Similitudes
< 1% similitudes entre comillas
< 1% entre las fuentes mencionadas
2% Idiomas no reconocidos (ignorado)

Nombre del documento: PROYECTO DE TITULACION BYRON ALAY MEREJILDO.docx
ID del documento: 7c09cb0f375ded4834ee4d432144adfbf4a11cf8
Tamaño del documento original: 7,63 MB

Depositante: MÓNICA KARINA JARAMILLO INFANTE
Fecha de depósito: 18/6/2024
Tipo de carga: interface
fecha de fin de análisis: 18/6/2024

Número de palabras: 12.371
Número de caracteres: 85.758

TUTOR

Ing. Mónica Karina Jaramillo Infante, Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **ALAY MEREJILDO BYRON ALEXANDER**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del trabajo de titulación con fines de difusión pública, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

La Libertad, a los 18 días del mes de junio del año 2024

EL AUTOR

Byron Alexander Alay Merejildo

AGRADECIMIENTO

En primer lugar, quiero expresar mi profunda gratitud a Dios por brindarme la fortaleza y la sabiduría necesarias para culminar con éxito este proyecto de investigación. Asimismo, deseo hacer patente mi más sincero agradecimiento a mis padres, Ángel Alay Yépez y Lizzie Merejildo Cruz, por su amor incondicional, su apoyo constante y sus valiosos consejos que me han permitido crecer como profesional y como ser humano.

A mi tutora, Mónica Jaramillo Infante, por su valiosa guía académica, sus acertadas recomendaciones y su permanente motivación durante todo el proceso de elaboración de este trabajo, a todos los docentes que me han formado a lo largo de mi carrera universitaria, inculcándome el compromiso y la responsabilidad con la profesión elegida.

A mis compañeros y amigos mas cercanos por su apoyo emocional y por las palabras de aliento que me brindaron en los momentos difíciles. Finalmente, mi gratitud a todas aquellas personas que de una u otra manera contribuyeron para que este sueño se hiciera realidad.

Byron Alexander, Alay Merejildo

DEDICATORIA

A Dios, por ser mi guía espiritual y bríndame la sabiduría y fortaleza necesarias para nunca desistir en este arduo camino. A mis padres Ángel Alay y Lizzie Merejildo, por su amor incondicional, sus sabios consejos y su apoyo inquebrantable durante todas las etapas de mi vida. Este logro es tan mío como de ustedes.

A mis Hermanos Lesslie Alay y Adrián Alay, por su cariño fraternal y por creer siempre en mí y ser ese apoyo incondicional en todo momento. A mis compañeros y amigos más cercanos que Dios me ha brindado y durante mi vida académica en la universidad, especialmente a Mirian Mateo y Bryan del Pezo, por su apoyo emocional y por las palabras de aliento que me brindaron en los momentos difíciles.

A todos aquellos seres queridos que ya no se encuentran físicamente conmigo, especialmente a mi gran amigo que me mira desde el cielo, José Douglas Orrala Ramos. Este logro que se suma a mi vida va dedicado a ti, amigo, por tu amistad, por las enseñanzas y los recuerdos que permanecen grabados en mi mente y corazón.

A todos ustedes dedico esta meta alcanzada. ¡Gracias Infinitas!

Byron Alexander, Alay Merejildo

1 INDICE GENERAL

ÍNDICE TABLAS

ÍNDICE IMÁGENES

RESUMEN

La protección de datos personales en el ámbito académico es una prioridad crítica y fundamental para las instituciones educativas modernas. La Universidad Estatal Península de Santa Elena (UPSE), particularmente en la Facultad de Ciencias Sociales y de la Salud, maneja una gran cantidad considerable de información sensible que requiere medidas de seguridad rigurosas y robustas. Los ataques de ingeniería social maliciosas, como phishing, spear-phishing y vishing, representan amenazas significativas y perjudiciales que pueden comprometer la integridad y confidencialidad de los datos personales. Este manual técnico exhaustivo aborda la aplicación efectiva de medidas de seguridad informática para proteger los datos personales en la UPSE, centrándose en la concienciación adecuada, la capacitación, la implementación de tecnologías de seguridad y la formulación de políticas y procedimientos adecuados. Al comprender y mitigar estos riesgos cibernéticos, la UPSE puede fortalecer significativamente su postura de seguridad y proteger eficazmente la información valiosa de sus estudiantes y personal académico.

Palabras claves: Phishing, Spear-Phishing, Vishing

ABSTRACT

The protection of personal data in academia is a critical and fundamental priority for modern educational institutions. The Santa Elena Peninsula State University (UPSE), particularly in the Faculty of Social and Health Sciences, handles a considerable amount of sensitive information that requires rigorous and robust security measures. Malicious social engineering attacks, such as phishing, spear-phishing, and vishing, represent significant and damaging threats that can compromise the integrity and confidentiality of personal data. This comprehensive technical manual addresses the effective application of cybersecurity measures to protect personal data at UPSE, focusing on appropriate awareness, training, implementation of security technologies, and formulation of appropriate policies and procedures. By understanding and mitigating these cyber risks, UPSE can significantly strengthen its security posture and effectively protect the valuable information of its students and academic staff.

Keywords: Phishing, Spear-Phishing, Vishing

INTRODUCCIÓN

En la era digital actual, la seguridad informática se ha convertido en un componente esencial para la protección de los datos personales. Las instituciones educativas, como la Universidad Estatal Península de Santa Elena (UPSE), enfrentan el desafío de garantizar la integridad, confidencialidad y disponibilidad de la información académica y personal de sus estudiantes, docentes y personal administrativo. Este desafío es especialmente crítico en la Facultad de Ciencias Sociales y de la Salud, donde la gestión de datos sensibles requiere un enfoque riguroso y actualizado en materia de seguridad informática.

La creciente dependencia de las tecnologías de la información y la comunicación (TIC) en los procesos académicos y administrativos ha incrementado la exposición a amenazas cibernéticas, como el robo de datos, el acceso no autorizado y los ataques de malware. Estos riesgos no solo comprometen la privacidad de los individuos, sino que también pueden afectar la reputación y el funcionamiento de la institución.

Este trabajo se enfoca en la aplicación de medidas de seguridad informática para la protección de datos personales en la sección académica de la UPSE. Se analizarán las políticas de seguridad actuales, las vulnerabilidades existentes y las mejores prácticas a implementar para fortalecer la seguridad de la información. El objetivo es desarrollar un marco de referencia que permita a la UPSE no solo cumplir con las normativas legales vigentes, sino también establecer una cultura de seguridad que proteja de manera proactiva los datos personales de toda la comunidad universitaria.

Mediante la implementación de controles de seguridad efectivos, la capacitación continua del personal y la adopción de tecnologías avanzadas, se espera que la UPSE pueda mitigar los riesgos asociados a la gestión de datos personales y garantizar un entorno académico seguro y confiable. Este estudio contribuirá a

sentar las bases para un manejo adecuado de la información y a fomentar una conciencia de seguridad informática en la comunidad universitaria

A continuación, se detalla la estructura y organización del presente proyecto de Investigación:

Capítulo 1, se describe todo lo esencial de los orígenes del problema enmarcado en los antecedentes del proyecto, a su vez la descripción del proyecto, los objetivos del proyecto, Justificación y alcance

Capítulo 2, El proyecto describe el marco teórico y metodología de desarrollo, aquí ingresa la parte de la recolección de información, el estudio de temas relacionado al proyecto, conceptualización de términos referentes y sobre todo la importancia de los beneficiarios del proyecto.

Capítulo 3, El proyecto describe los componentes de desarrollo del proyecto, aquí se presenta todo el desarrollo de las fases de estudio seleccionado por la metodología base, a su vez se desarrolla la elaboración de un manual técnico para la protección de datos personales

Finalmente, se presenta las conclusiones y recomendaciones

CAPÍTULO I

2 FUNDAMENTACIÓN

2.1 ANTECEDENTES DEL PROYECTO

La creciente digitalización en las instituciones educativas ha generado una demanda imperante y un reconocimiento contundente sobre la necesidad de asegurar los datos personales de estudiantes, docentes y personal administrativo, subrayando así la importancia crucial de la seguridad informática en este entorno educativo en constante evolución. Este énfasis en la seguridad informática se justifica por la naturaleza sensible de la información manejada en el ámbito académico, donde la confidencialidad y la integridad de los datos son fundamentales para garantizar la privacidad y el buen funcionamiento de las operaciones educativas [1].

Institución

Actualmente en las actividades diarias se exponen la identidad personal, que en ocasiones sin darnos cuenta se da la apertura que se roben la información para ejercer la clonación y posteriormente aprovechar la acción ilegal ya sea con fines educativo, por venganza, entre otros. En este contexto dinámico, se observa la proliferación de nuevas herramientas digitales que, si bien pueden fortalecer la protección de datos, también introducen riesgos significativos de explotación mediante técnicas de ingeniería social, incrementando la vulnerabilidad ante el robo de identidad digital y el acceso no autorizado a la información confidencial. [2].

El robo de identidad digital sucede cuando alguien asume la identidad de otra persona física o jurídica en plataformas digitales o en sus perfiles de redes sociales. Dependiendo de las acciones realizadas por el impostor, esta suplantación puede constituir un delito. Usualmente, la suplantación de identidad en línea tiene como objetivo cometer fraudes, como contratar servicios o adquirir productos, con el fin de obtener ganancias o causar daños. En consecuencia, el infractor puede enfrentar cargos por delitos relacionados con el uso indebido de identidades falsas [3].

La tesis de maestría titulada **Modelo de Gestión de la Información para la Protección de Datos Personales en la Carrera de Ciencias Policiales de la Universidad Central del Ecuador** desarrollada por Ing. Ángel Calle A., menciona la importancia de usar modelo de protección de datos de carácter personal de los docentes de la Carrera de Ciencias Policiales y Seguridad de la Universidad Central del Ecuador en donde imparte los problemas presente como robo de identidad, huellas digitales, entre otros que proporciona gran cantidad de datos que pueden ser vulnerables mediante ataques informáticos [4].

La tesis de maestría titulada **Medidas de Seguridad de Protección de Datos Personales en mi lugar de trabajo** desarrollada por Esteban Rodríguez Jiménez en la ciudad de México, menciona como es de importante la seguridad de los datos personales tanto para individuos como para las misma instituciones públicas, privadas, educativas u organizaciones debido que se rigen datos relevantes y de suma delicadeza obligado a tener derecho por su rigurosidad. Por ende, la falta de consciencia respecto a mecanismos y controles es de solución emergente para garantizar la seguridad adecuada [5].

La tesis titulada **Ingeniería Social en una institución de educación superior aplicando técnicas computacionales y no computacionales** de la Universidad Estatal Península de Santa Elena presentada por Marcelo Peñafiel S., menciona como el aumento de nuevas formas tecnológicas en plena pandemia Covid-19 ha permitido crear el teletrabajo y la educación virtual de forma contundente y solución óptima, sin embargo, así mismo como se presenta nuevas herramientas también llegan nuevas formas de atacar sistemas informáticos, aplicaciones, servidores de instituciones públicas o privadas. Por ende, la propuesta de ejercer el conocimiento de ingeniería social como factor partida rige el papel de comprender y entender como una simple acción computacional o no computacional permite aludir la forma de robo de datos personales sin ser descubierto [6].

Por consiguiente, el infractor puede enfrentar cargos por delitos relacionados con el uso indebido de identidades falsas. Este escenario subraya la necesidad imperante de implementar y fortalecer medidas de seguridad informática en la sección académica de la Universidad Estatal Península de Santa Elena (UPSE) –

Facultad de Ciencias Sociales y de la Salud, con el fin de proteger los datos personales y preservar la integridad de la comunidad educativa en un entorno cada vez más digitalizado y complejo.

2.2 DESCRIPCIÓN DEL PROYECTO

En la actualidad, se requiere desarrollar medidas de seguridad informática efectivas en la sección académica de la Universidad Estatal Península de Santa Elena (UPSE) - Facultad de Ciencias Sociales y de la Salud, debido a la carencia de una adecuada protección de los datos personales de estudiantes, docentes y personal administrativo. Esta necesidad surge en un contexto donde la creciente digitalización y el uso de nuevas tecnologías aumentan la vulnerabilidad ante posibles ataques cibernéticos y el robo de identidad digital.

La premisa fundamental de esta investigación es que la implementación efectiva de medidas de seguridad informática en la sección académica de la UPSE - Facultad de Ciencias Sociales y de la Salud impacta directamente en la percepción de seguridad de los usuarios respecto a la protección de sus datos personales. Este aspecto puede influir significativamente en su participación en actividades académicas en línea y en la utilización de recursos digitales proporcionados por la universidad.

El presente proyecto para el desarrollo

La metodología de desarrollo del proyecto contara de cinco fases correspondiente para el cumplimiento del objetivo propuesto sobre la seguridad informática en la protección de datos personales en la identidad digital, que son los siguientes:

Fase de Estudio

- Explorar las técnicas más comunes usadas para ingeniería social para el robo de identidad digital
- Ejercer un cuadro comparativo de todas las técnicas encontradas más comunes

- Emplear clasificación de criticidad, sistemas que afectan, datos comprometidos y descripción

Fase de desarrollo de escenarios

- Preparación de escenarios de pruebas para comprometer objetivo
- Herramientas de desarrollo de vector de ataque
- Seleccionar el sistema de objeto real y personal a vulnerar

Fase de prueba de penetración

- Explotar brecha de seguridad mediante el uso de las técnicas seleccionada para la intrusión
- Conocer el nivel de seguridad que se encuentran protegido los datos del objeto
- Extraer la información encontrada a través de la prueba de penetración

Fase de análisis de resultados

- Desarrollar fichas descriptivas sobre el proceso de ataque, resultado encontrado y tiempo de ejecución
- Clasificar los resultados de bajo, medio y alto nivel en base a la seguridad
- Analizar e interpretar resultados
- Observaciones técnicas

Fase de manual

- Identificar requisitos y objetivos
- Recopilar información relevante de la ley de protección de datos personales
- Emplear políticas y procedimientos en base a los resultados
- Brindar recomendaciones

Kali Linux: Es una distribución de Linux personalizada, diseñada, desarrollada de forma exclusiva con el objetivo de realizar pruebas de intrusión y evaluaciones de ciberseguridad. Incluye una amplia gama de herramientas informática que permiten a los profesionales evaluar la seguridad de sistemas y redes [7].

Exitools: Exitools es un conjunto de herramientas de seguridad informática que se utilizan para realizar pruebas de penetración y auditorías de seguridad en sistemas informáticos. Estas herramientas están diseñadas para ayudar a identificar y explotar vulnerabilidades en sistemas y redes [8].

Virus Informático: Un virus informático es un programa malicioso diseñado para infectar y dañar sistemas informáticos. Los virus pueden propagarse a través de archivos ejecutables, documentos infectados o enlaces maliciosos, y pueden causar una amplia gama de problemas, desde la pérdida de datos hasta el robo de información personal [9].

Msfvenom: Msfvenom es una herramienta incluida en el marco de explotación Metasploit que se utiliza para crear payloads maliciosos. Estos payloads pueden ser utilizados para comprometer sistemas informáticos y redes durante pruebas de penetración y auditorías de seguridad [10].

Social Engineering Toolkit: El Social Engineering Toolkit (SET) es una herramienta de código abierto diseñada para realizar ataques de ingeniería social. Permite a los atacantes crear escenarios de ataque realistas para engañar a las víctimas y obtener acceso a información confidencial [11].

RAT (Troyano de acceso remoto): Un RAT, o troyano de acceso remoto, es un tipo de malware que permite a un atacante tomar el control completo de un sistema informático de forma remota. Los RATs pueden utilizarse para robar información, instalar otros tipos de malware o incluso controlar la cámara y el micrófono del dispositivo infectado [12].

2.3 OBJETIVOS DEL PROYECTO

2.3.1 OBJETIVO GENERAL

Evaluar las técnicas de ingeniería social utilizadas para el robo de identidad digital en entornos controlados, con el fin de proteger los datos personales en la Facultad de Ciencias Sociales y de la Salud de la UPSE.

2.3.2 OBJETIVO ESPECÍFICOS

- Analizar técnicas de ingeniería social para comprender el robo de identidad digital
- Desarrollar escenarios de pruebas usando entornos controlados para evaluar el nivel de protección de datos personales.
- Elaborar un manual de estrategias y políticas de seguridad informáticas para el fortalecimiento de protección de datos personales

2.4 JUSTIFICACIÓN DEL PROYECTO

En la era digital actual, la seguridad informática desempeña un papel vital al proporcionar una amplia gama de servicios esenciales que garantizan la protección y la privacidad de los datos personales tanto para individuos como para organizaciones. En un entorno digital cada vez más complejo y conectado, la exposición de la información personal a diversas amenazas es una realidad omnipresente. Es por ello que se vuelve crucial contar con medidas de seguridad sólidas y adaptables, capaces de salvaguardar la integridad y confidencialidad de los datos en todo momento [13].

En el ámbito educativo, tal como se observa en la Universidad Estatal Península de Santa Elena (UPSE) – Facultad de Ciencias Sociales y de la Salud, la digitalización ha revolucionado la manera en que se gestionan los datos y se accede a los recursos educativos. Esta evolución ha traído consigo numerosos beneficios, como una mayor eficiencia en la administración de información y una ampliación del acceso a recursos educativos en línea. No obstante, esta transformación también ha introducido nuevos desafíos, entre los que destaca la necesidad imperante de proteger de manera efectiva la integridad y confidencialidad de la información sensible de estudiantes, profesores y personal administrativo [14].

La implementación de medidas de seguridad informática se convierte, entonces, en un aspecto crucial para salvaguardar la privacidad y confidencialidad de los datos en la UPSE. Estas medidas no solo están diseñadas para prevenir el acceso no autorizado a la información, sino que también tienen como objetivo fortalecer la

integridad de los sistemas y procesos de protección de datos, garantizando así un entorno digital seguro y protegido [15].

Por lo tanto, es imperativo desarrollar e implementar estrategias efectivas de seguridad informática en la Facultad de Ciencias Sociales y de la Salud de la UPSE. Estas estrategias deben abordar tanto la prevención de ataques cibernéticos como la detección y respuesta ante posibles incidentes de seguridad, asegurando así la protección integral de la información sensible y la continuidad de las operaciones educativas.

El tema propuesto esta alineado a los objetivos del Plan de Creación de Oportunidades 2021-2025, específicamente en:

Objetivos del eje social

Objetivo 5. Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social. [16]

Políticas.

5.5 Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población. [16]

Pol. 5.4.

A4. Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios. [16]

2.5 ALCANCE DEL PROYECTO

El alcance del proyecto abarca un análisis exhaustivo de la infraestructura tecnológica y los sistemas de información actualmente en uso en la sección académica de la Universidad Estatal Península de Santa Elena (UPSE) - Facultad de Ciencias Sociales y de la Salud. Este análisis se centrará en identificar las debilidades y vulnerabilidades existentes que puedan comprometer la seguridad de los datos personales de estudiantes, docentes y personal administrativo. Además, se evaluará la eficacia de las medidas de seguridad existentes y se determinarán las áreas que requieren mejoras o actualizaciones. Este proceso permitirá establecer

una base sólida para el diseño e implementación de estrategias de seguridad informática adecuadas y específicas para las necesidades de la institución.

En la fase de estudio, se realizará una exploración exhaustiva de las técnicas más comunes utilizadas en ingeniería social para el robo de identidad digital. Esto implicará la investigación y comparación de estas técnicas, así como la clasificación de su criticidad, los sistemas que afectan, los datos comprometidos y una descripción detallada de cada una.

Posteriormente, en la fase de desarrollo de escenarios, se prepararán escenarios de pruebas realistas para comprometer los objetivos de seguridad. Esto incluirá la selección de herramientas adecuadas para el desarrollo de vectores de ataque y la identificación de sistemas y personal objetivo a vulnerar.

La fase de prueba de penetración implicará la explotación de las brechas de seguridad identificadas mediante el uso de las técnicas seleccionadas para la intrusión. Se buscará conocer el nivel de seguridad de los datos del objeto y se extraerá la información encontrada a través de la prueba.

Luego, en la fase de análisis de resultados, se desarrollarán fichas descriptivas sobre el proceso de ataque, los resultados obtenidos y el tiempo de ejecución. Se clasificarán los resultados en base a su nivel de seguridad y se realizarán análisis e interpretaciones detalladas, así como observaciones técnicas relevantes.

Finalmente, en la fase de manual, se identificarán requisitos y objetivos, se recopilará información relevante de la ley de protección de datos personales, se emplearán políticas y procedimientos basados en los resultados obtenidos, y se proporcionarán recomendaciones para mejorar la seguridad informática en la sección académica de la UPSE

El alcance del proyecto no incluye la gestión de incidentes de seguridad cibernética ni la resolución de problemas relacionados con la seguridad de hardware específico, como servidores o dispositivos individuales. Sin embargo, se puede considerar la integración de protocolos de respuesta a incidentes como parte de las medidas de seguridad implementadas.

CAPÍTULO II

3 MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

3.1.1 MARCO CONCEPTUAL

SEGURIDAD INFORMATICA

El campo de la seguridad informática es considerado una disciplina con el objetivo de proteger los sistemas informáticos que se encuentran almacenado en el mismo, para establecer una abrigada en garantizar la integridad, confiabilidad y disponibilidad. La extensa protección de los sistemas informática se establece mediante la implementación y creación de política y normas que den el régimen sobre el buen flujo de información que se encuentra en la organización.

La seguridad informática es un campo que se dedica a proteger la privacidad y la integridad de los datos almacenados en sistemas informáticos, basándose en las normas internas y externas de una organización. El objetivo de proteger esta información de cualquier tipo de amenaza es reducir al mínimo los riesgos físicos y lógicos que puedan afectarla [17].

CONFIDENCIALIDAD: Como principio fundamental de la seguridad informática, la confidencialidad establece que la información debe ser accesible únicamente para las personas autorizadas. Esto significa que solo las personas con los permisos adecuados pueden acceder a ciertos datos o programas. El objetivo es evitar que se divulguen datos personales o comerciales. El principio de privacidad, también conocido como principio de privacidad, es la base de otros aspectos de la seguridad informática [18].

AUTENTICIDAD: El principio de autenticidad se utiliza para verificar que la información que posee la organización es verdadera. Este es un componente crucial de la ciberseguridad que garantiza que el origen del documento o información es auténtico. En cualquier momento, asegúrese de que el creador del mensaje es efectivamente la persona indicada como remitente para los consultantes [18].

INTEGRIDAD: Se refiere a asegurarse de que terceros no alteren la información almacenada en dispositivos o transmitida a través de cualquier canal de comunicación. Esto garantiza que las personas no autorizadas no alteren la información [19].

DISPONIBILIDAD: Se refiere a la necesidad de que la información esté siempre disponible para las personas autorizadas para acceder a ella y gestionarla, y que pueda ser recuperada en caso de una pérdida o corrupción de la información debido a un incidente de seguridad. En otras palabras, garantiza la disponibilidad de la información cuando sea necesario [19].

¿CUÁLES SON LOS TIPOS MAS COMUNES DE CIBERATAQUES Y QUE MEDIDAS PODEMOS TOMAR PARA PROTEGERNOS?

El phishing y el malware son dos de los ciberataques más comunes. El phishing es un método utilizado por los atacantes para engañar a las víctimas y obtener información confidencial, como contraseñas o datos personales. Es fundamental capacitar a los usuarios para que reconozcan correos electrónicos y mensajes sospechosos, utilizar filtros avanzados de correo electrónico para detectar y bloquear intentos de phishing, y implementar la autenticación multifactor (MFA) para añadir una capa adicional de seguridad a los accesos para protegerse contra el phishing. Por otro lado, el malware es un software malicioso que incluye virus, troyanos, ransomware, spyware y adware y está diseñado para dañar, interrumpir o tomar el control de sistemas y redes [20].

ENTRE LAS RECOMENDACIONES DE PROTECCIÓN PODRÍAN ESTAR

- Usa contraseñas que solo tú conozcas y evita usar combinaciones fáciles de adivinar de letras y números. No utilices contraseñas como «12345678” [20].
- Cambia tus contraseñas regularmente y evita reutilizarlas en diferentes cuentas [20].
- Mantén tus dispositivos y programas actualizados con las últimas versiones de seguridad [20].

- Sé cauteloso al hacer clic en enlaces o al descargar archivos adjuntos. Es más, evita las plataformas desconocidas o sospechosas [20].
- Mira que el sitio web sea seguro antes de ingresar información confidencial [20].
- Verifica que comience con «https://» y tenga un candado de seguridad [20].
- Utiliza software antivirus y antimalware confiables [20].

INGENIERIA SOCIAL

Este ataque utiliza métodos que hacen que los usuarios legítimos de un sistema revelen datos confidenciales, lo que les permite acceder a los recursos e información de una empresa. En otras situaciones, tiene como objetivo persuadir a los usuarios para que tomen medidas que van más allá de sus responsabilidades habituales. Con frecuencia se debe a la falta de precaución al revelar información confidencial; por ejemplo, un usuario podría revelar sus datos al registrarse para un servicio. En el peor de los casos, un atacante podría recurrir al chantaje o incluso al secuestro de familiares cercanos [21].

Los ataques de ingeniería social son comunes y peligrosos, ya que se aprovechan de la confianza y vulnerabilidad de las personas. Por lo general, los hackers planifican estos ataques con anticipación, investigando a la persona o empresa objetivo, seleccionando el método de ataque más adecuado y finalmente llevándolo a cabo [22].

TIPOS DE TECNICAS DE INGENIERÍA SOCIAL

PHISHING

Es un tipo de ingeniería social en la que un atacante envía comunicaciones fraudulentas, como suplantaciones de identidad de una institución financiera, con el fin de engañar y obtener información confidencial de una persona. El ataque también podría tener como objetivo instalar software malicioso en el equipo de la víctima con el fin de secuestrar sus datos [23].

En la actualidad es un tipo de ataque muy común y conocido por los ciberdelincuentes, sin embargo, es bastante fácil ser víctima de esta técnica si no

tienes cuidado. Los conocidos ataques de suplantación de identidad intentan robar información sensible a través de correos electrónicos, sitios web, mensajes de texto u otras formas de comunicación electrónica [23].

FUNCIONAMIENTO

La naturaleza del engaño depende del ingenio y la habilidad del atacante. Los phishers ahora tienen acceso a una cantidad sin precedentes de información personal sobre sus objetivos gracias a la omnipresencia de las redes sociales. Con estos datos, pueden hacer propuestas mucho más atractivas ajustando sus ataques a las necesidades, deseos y circunstancias específicas de la víctima. En estas situaciones, las redes sociales facilitan el uso de la ingeniería social para llevar a cabo ataques de phishing [24].

PHARMING

El pharming, una combinación de las palabras phishing y farming, es una estafa en línea que redirige a las personas a sitios web fraudulentos que imitan a los legítimos. Estas estafas buscan engañar a los usuarios para que interactúen con estos sitios falsos, con el objetivo de recopilar sus datos personales, como correos electrónicos y contraseñas, o de infectar sus dispositivos con malware [25].

FUNCIONAMIENTO

El pharming explota la forma en que los navegadores traducen una URL en una dirección IP mediante servidores DNS. Los servidores DNS realizan esta conversión y almacenan la información en caché, evitando la necesidad de contactar al servidor en cada visita al sitio. Los ataques de pharming interrumpen este proceso, redirigiendo a los usuarios a direcciones IP falsificadas que llevan a sitios web fraudulentos. Los atacantes de pharming emplean tácticas de ingeniería social para hacer que sus direcciones maliciosas parezcan legítimas, de modo que las víctimas no sospechen nada. Existen dos tipos principales de pharming: el pharming de malware, que introduce software malicioso en los dispositivos, y el envenenamiento de DNS, que manipula la caché del DNS. Ambos métodos buscan el mismo objetivo: recopilar datos personales de las víctimas [25].

VISHING

El Vishing, también conocido como phishing por voz, ocurre cuando alguien o una organización aparentemente respetable llama a las víctimas por teléfono o utiliza mensajería de voz para convencerlas de revelar información personal. Los estafadores, también conocidos como vishers, realizan ataques de engaño haciéndose pasar por fuentes confiables para obtener datos confidenciales, como números de tarjetas de crédito o identificaciones gubernamentales. Estos ataques suelen usar técnicas de ingeniería social para ganarse la confianza de las víctimas y frecuentemente utilizan tecnologías como la suplantación de identidad de llamadas (caller ID spoofing) para parecer más creíbles. Para evitar el engaño, se debe ser escéptico ante las solicitudes inesperadas de información personal y verificar la autenticidad de la fuente antes de compartirla [26].

FUNCIONAMIENTO

Los estafadores pueden realizar estafas de varias maneras. En ocasiones, envían mensajes a la víctima para alertarla sobre intentos no autorizados de acceso a su cuenta o compras fraudulentas con su tarjeta. Se proporciona un número de atención al cliente para resolver el problema en el mensaje. El estafador se hace pasar por un empleado de la entidad y solicita información personal a la víctima. Los delincuentes pueden utilizar esta información para suplantar la identidad de la víctima y cometer fraudes adicionales. Para evitar este tipo de estafas, es crucial verificar la autenticidad de las comunicaciones antes de proporcionar cualquier información personal [27].

SHISHING

Smishing es una táctica de ingeniería social que emplea mensajes de texto móviles falsos para engañar a las personas para que descarguen software malicioso, divulguen información confidencial o envíen dinero a los cibercriminales. El término "sms" proviene de las palabras "sms" y "phishing", que son las palabras técnicas detrás de los mensajes de texto [28].

EJEMPLOS

- Entidad bancaria: El mensaje parecerá provenir de un banco, solicitando los datos de la tarjeta de crédito o las claves de acceso a la banca en línea de la víctima [29].
- Familiar en apuros: El mensaje se hará pasar por un familiar o alguien cercano, afirmando que esta persona necesita ayuda y pidiendo dinero a la víctima para asistirla [29].
- Lotería falsa: El mensaje parecerá provenir de una administración de lotería, anunciando que la víctima ha ganado un gran premio en efectivo. Solicitará sus datos bancarios para posterior hacer transferencia del dinero [29].
- Empresa de mensajería: El mensaje se hará pasar por una empresa de envíos que afirma tener retenido uno de nuestros paquetes, solicitando de una u otra manera un pago para posterior liberar la entrega[29].

¿CUÁLES SON LOS BENEFICIOS DERIVADOS DE LA IMPLEMENTACION DE UN PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES?

En la actualidad, la información personal se ha convertido en un recurso valioso para las empresas, que mediante el uso de tecnología avanzada pueden recopilar, analizar y utilizar datos para tomar decisiones más informadas [30].

El manejo apropiado de la información personal conduce a una reputación corporativa positiva, lo que se traduce en la confianza de los stakeholders en las empresas que adoptan un enfoque empresarial que protege los derechos fundamentales de las personas y a su vez aumenta la competitividad en el mercado [30].

¿CUAL ES LA RELEVANCIA DE PRESERVAR LA CONFIDENCIALIDAD DE LA INFORMACION PERSONAL Y PRIVADA?

En la era actual, la importancia de la privacidad de los datos abarca una amplia gama de datos personales e información que se puede almacenar en nuestros dispositivos digitales personales, en centros de datos corporativos e incluso en la

nube. Además, la complejidad se incrementa con la inclusión de la perspectiva del cliente respecto a la privacidad, las regularizaciones específicas de la industria y las dinámicas geopolíticas en constante evolución. Las empresas deben alinearse y cumplir con todo esto si desean evitar sanciones por mal manejo de la privacidad, que van desde multas importantes hasta clientes furiosos [31].

Así como las sanciones por falta de cumplimiento y el abandono de clientes representan el lado punitivo de la privacidad, también hay un lado positivo, los clientes tienen mayor disposición a establecer relaciones comerciales e incluso incrementar sus transacciones con aquellas empresas que les inspiran confianza. Esto significa que la privacidad no solo representa un deber, sino que es un componente estratégico clave dentro del modelo de negocios, capaz de potenciar significativamente el posicionamiento de marca y los ingresos de la compañía [31].

¿Cómo Acatar la Ley Orgánica de Protección de Datos (LOPD)?

Todas las entidades que manejen datos personales en un ámbito profesional o comercial están obligadas a cumplir con la normativa de protección de datos personales establecidas en dicha ley ya estas sean en organizaciones, empresas, administraciones públicas y autónomos [32].

¿QUÉ HACER PARA CUMPLIR LA LOPD, LEY DE PROTECCIÓN DE DATOS? 12 PASOS

- Determinar qué datos personales tratas [32].
- Definir que tratamiento de datos vas a realizar [32].
- Análisis de riesgos [32].
- Implantar las medidas de seguridad adecuada [32].
- Elaborar el registro de actividades de tratamiento [32].
- Ceder datos a terceros [32].
- Designar un DPO [32].
- Deber informar [32].
- Recabar y registrar el consentimiento expreso [32].
- Textos legales de la página web [32].
- Gestionar brechas de seguridad [32].
- Auditorias periódicas [32].

3.2 MARCO TEÓRICO

ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN CIBER ATAQUES DE INGENIERÍA SOCIAL PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN, DE LA UNIVERSIDAD TÉCNICA DE AMBATO

La Ingeniería Social es un conjunto de técnicas utilizadas para obtener información confidencial a través de la manipulación de personas. En este proyecto, se emplea la plataforma DigitalOcean para servicios virtualizados en la nube, el framework Gophish para la planificación y ejecución de simulaciones de ataques de phishing, y la herramienta Hunter.io para la recolección de correos electrónicos. Se busca evaluar la seguridad de los sistemas informáticos de la institución, considerando que el componente humano puede ser una vulnerabilidad. Por lo tanto, se realiza un estudio sobre el nivel de concicia en ciberseguridad entre estudiantes y docentes. El objetivo principal es fortalecer la seguridad de la información en la institución, aumentando la conciencia de seguridad entre estudiantes y docentes para prepararlos ante posibles ataques reales [33].

DESARROLLO DE CAMPAÑA DE ATAQUE DE INGENIERÍA SOCIAL

El proyecto se centra en evaluar cómo la ingeniería social afecta la seguridad de la información confidencial de las personas y los riesgos asociados. Se realizó un ataque de phishing controlado para crear una campaña de ingeniería social, identificando la falta de conocimiento como la principal causa de caer en este tipo de ataques. La metodología descriptiva reveló que la fase de investigación es crucial para el éxito del ataque. Se observó que las personas suelen usar contraseñas débiles al no establecer restricciones, y la concientización enviada a cada correo electrónico registrado contribuyó al éxito de la campaña. Se sugiere realizar investigaciones futuras sobre otros tipos de ataques de ingeniería social para evaluar su impacto, evaluación de la efectividad de concientización de ciberseguridad para prevenir ataques, investigaciones sobre el uso de la inteligencia artificial para detectar y prevenir intentos de ingeniera social, análisis comparativo de políticas y procedimientos de seguridad en diferentes organizaciones y su resistencia ante

técnicas de manipulación psicológica, estudios del impacto psicológicos en víctimas y desarrollo de estrategias. [34].

IMPLEMENTACIÓN DE INGENIERÍA SOCIAL PARA LA DETECCIÓN DE VULNERABILIDADES EN LOS SISTEMAS DE INFORMACIÓN UTILIZADOS EN LA UNIVERSIDAD AUTÓNOMA DE ZACATECAS, CENTRO EDUCATIVO ROTAY Y LA COORDINACIÓN DE LA SECRETARÍA DE SEGURIDAD PÚBLICA, BASADOS EN METODOLOGÍAS DE PENTESTING

La tesis aborda el creciente riesgo de cibercrimen para las organizaciones, independientemente de su sector, debido a los constantes ataques a los sistemas informáticos y la falta de énfasis en la seguridad durante su implementación. Se destaca que cualquier dispositivo conectado a internet está expuesto a diversas amenazas, comprometiendo la integridad de la información. Se argumenta que invertir en la capacitación del personal en seguridad informática y establecer políticas de seguridad es más rentable que enfrentar incidentes costosos. El trabajo revisa y compara diferentes metodologías, seleccionando la más adecuada para evaluar las vulnerabilidades en instituciones como la Universidad Autónoma de Zacatecas, el Centro Educativo Rotary y la Secretaría de Seguridad Pública. Se utilizan herramientas actuales para detectar fallas en los servicios proporcionados por estas organizaciones, identificando vulnerabilidades que afectan desde el recurso humano hasta los sistemas de información críticos [35].

3.3 METODOLOGÍA DEL PROYECTO

3.3.1 METODOLOGÍA DE INVESTIGACIÓN

El proyecto propuesto se basa en una metodología de investigación experimental, ya que implica el análisis de una variable de medición que facilitará la evaluación de los resultados antes y después de la investigación. En este caso, la variable de medición se centra en la percepción de protección de datos en la Facultad de Ciencias Sociales y de la Salud de la UPSE. Esta percepción se evaluará a través de indicadores que reflejen el nivel de seguridad y protección que los miembros de la comunidad académica perciben en relación con sus datos personales en el entorno digital. Esta investigación se relaciona directamente con el tema de mi tesis, ya que

se enfoca en comprender y mejorar la percepción de protección de datos mediante la implementación de medidas específicas de seguridad informática [36].

En cuanto al alcance de la investigación, se identifica como explicativo. En este contexto, el enfoque se centra en la comprensión de las causas y consecuencias relacionadas con un fenómeno particular, en este caso, la percepción de protección de datos en la Facultad de Ciencias Sociales y de la Salud de la UPSE. Mediante este estudio, se busca elucidar los motivos subyacentes detrás de la percepción de protección de datos y su conexión con las medidas de seguridad informática aplicadas. Este enfoque explicativo posibilitará una comprensión más profunda de los factores que influyen en la percepción de protección de datos y proporcionará información valiosa para mejorar las prácticas de seguridad en el ámbito académico [37].

En lo que respecta al tipo de investigación, se clasifica como cualitativo. Este enfoque se enfoca en explorar y comprender las percepciones, experiencias y significados asociados con la protección de datos en la Facultad de Ciencias Sociales y de la Salud de la UPSE [38].

Mediante el uso de métodos cualitativos, como entrevistas en profundidad, grupos focales y análisis de contenido, se buscará obtener una comprensión profunda y detallada de las perspectivas de los participantes en relación con este tema específico. Este enfoque cualitativo permitirá capturar la riqueza y complejidad de las percepciones de los individuos, así como también proporcionará insights significativos para abordar la protección de datos desde una perspectiva más holística [39].

En cuanto a los métodos de investigación, se adoptará un enfoque deductivo. Este enfoque implica partir de principios generales y teorías existentes para analizar datos específicos y llegar a conclusiones. Se llevará a cabo un proceso de recolección y análisis de datos para validar o refutar las afirmaciones generales. Este método facilitará la exploración de relaciones causales entre las variables de interés y contribuirá a la generación de conclusiones respaldadas por evidencia empírica [40].

BENEFICIARIOS

La población objeto de estudio comprende exclusivamente a los estudiantes matriculados en la Facultad de Ciencias Sociales y de la Salud de la Universidad Estatal Península de Santa Elena (UPSE). Esta población, diversa en cuanto a perfiles y procedencias, representa el núcleo fundamental de la comunidad académica de la institución. Su participación en el estudio será crucial para obtener una comprensión completa de las percepciones y experiencias relacionadas con la protección de datos en el entorno universitario.

BENEFICIARIOS	CANTIDAD
DOCENTES	5
ESTUDIANTES	18
TOTAL	23

Tabla 1: Tabla de beneficiarios del Proyecto

VARIABLE

Nivel de Conciencia de Seguridad". Esta variable se refiere al grado de conciencia que tienen los usuarios y el personal de la institución sobre las prácticas de seguridad informática y la importancia de proteger los datos personales.

3.3.2 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Técnicas

- Estado del arte, entrevista, fuentes bibliográficas

Instrumento

Para la recopilación de datos, se emplearán entrevistas y métodos de observación enfocados en obtener información relevante sobre los procesos relacionados con la seguridad informática en la Facultad de Ciencias Sociales y de la Salud de la UPSE.

Se indagará sobre aspectos como la gestión y protección de datos personales, los procedimientos de acceso a la información, así como cualquier otro proceso relacionado con la seguridad y privacidad de los datos en el entorno académico.

3.3.3 METODOLOGÍA DE DESARROLLO

OSSTMM, abreviatura de Manual de Metodología de Pruebas de Seguridad de Código Abierto, es una completa metodología desarrollada por ISECOM para realizar análisis exhaustivos, pruebas y mediciones de la seguridad operativa real. Funciona como un marco metodológico para llevar a cabo auditorías técnicas de seguridad, siendo diseñada para ser consistente y repetible en su aplicación. Al ser un proyecto de código abierto, permite la contribución de profesionales en auditoría de seguridad para mejorar los métodos de prueba, lo que garantiza evaluaciones más precisas y eficientes. Además, su naturaleza de código abierto facilita la libre difusión de la documentación sin preocupaciones por temas de propiedad intelectual [41].

Fase 1: Lanzamiento del Proyecto, es crucial, ya que implica obtener la aprobación de los recursos necesarios y concienciar a todos los involucrados sobre los posibles efectos adversos no previstos que la auditoría puede tener en los sistemas de información. Aunque los ejecutores intenten minimizar estos efectos, es importante que la organización reconozca y acepte explícitamente esta posibilidad.

La Fase 2: Inductiva, según la metodología establecida, marca el inicio de la ejecución de la auditoría. Aquí, el analista se concentra en comprender los requisitos, alcance y limitaciones de la auditoría para determinar el tipo de pruebas que se llevarán a cabo.

La Fase 3: Interactiva, se centra en planificar la auditoría una vez que se ha definido su alcance y se han determinado los tipos de pruebas necesarios para cada elemento a auditar.

En la Fase 4: Investigación, se analizan los aspectos organizativos y de gestión de la organización, y se realiza un análisis técnico inicial, utilizando fuentes abiertas, sobre los elementos objeto de la auditoría.

La Fase 5: Intervención, constituye el núcleo de la auditoría, donde se realizan las pruebas técnicas sobre los elementos del alcance. Estas pruebas pueden implicar modificaciones, sobrecargas o bloqueos de elementos para provocar una penetración o interrupción. Esta etapa suele ser la fase final de una prueba de seguridad y puede ocasionar disfunciones no previstas en los sistemas de información auditados.

La Fase 6: Reporte, se elabora el informe de la auditoría, evaluando los resultados objetivos y registrando la valoración correspondiente en base a los hallazgos identificados durante todo el proceso de auditoría.

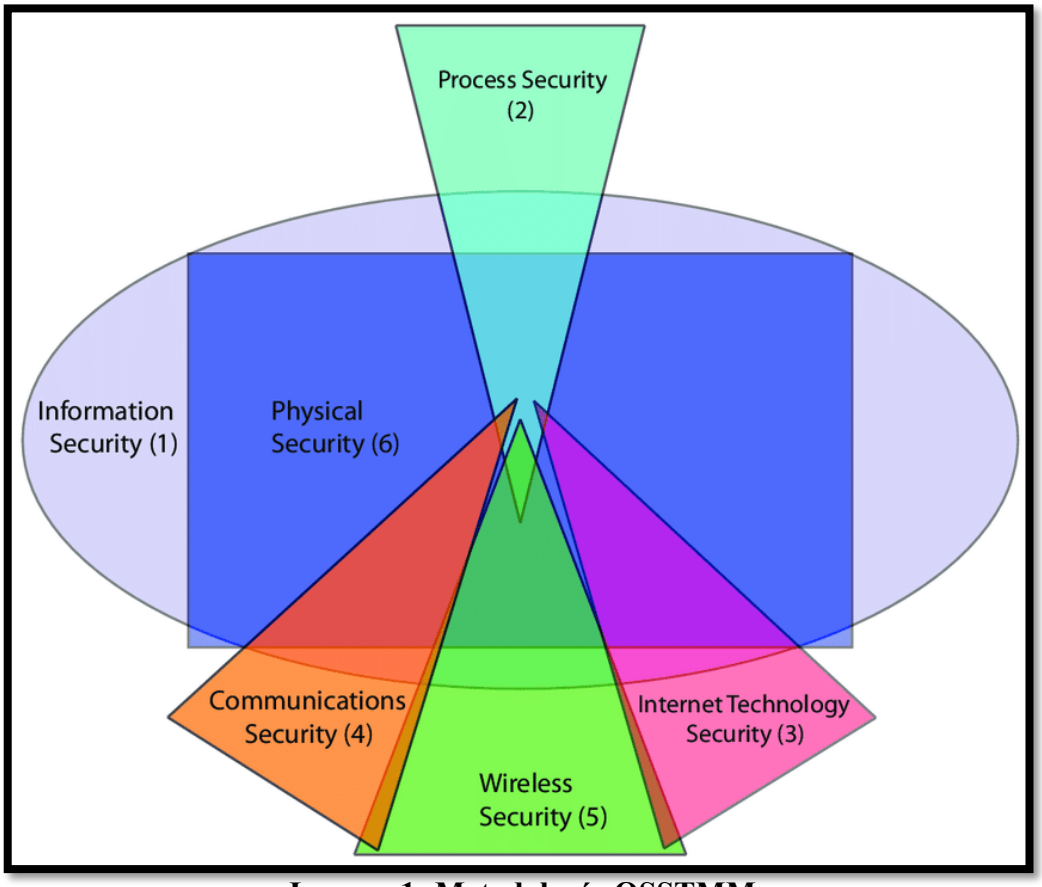

Imagen 1: Metodología OSSTMM

CAPÍTULO III

4 PROPUESTA

4.1 DESARROLLO

4.2 FASE DE ESTUDIO

En esta fase de estudio se desglosa la investigación pertinente de las diversas técnicas de ingeniería social que cuentan como pauta para el entendimiento de como un ciberdelincuente doblega la ley de protección de datos personales y saca beneficioso propio con la finalidad de usar la data recolectada para ofértalas en la red o pedir un rescate

TÉCNICA DE INGENIERÍA SOCIAL	CLASIFICACIÓN DE CRITICIDAD	SISTEMAS AFECTADOS	DATOS COMPROMETIDOS	DESCRIPCIÓN	MÉTODOS DE PREVENCIÓN
Phishing	Alta	Correo electronicos, Plataformas Web	Credenciales de inicio de sesión, Información financiera	Los atacantes envían correos electrónicos fraudulentos que imitan a entidades confiables para engañar a las víctimas y hacer que revelen información confidencial.	- Capacitación de los usuarios para identificar correos electrónicos sospechosos. - Antes de suministrar datos sensibles, es fundamental corroborar que los sitios

					web sean legítimos y auténticos.
Spear-Phishing	Alta	Correo Electronico, Mensajeria instantanea, Sistema de gestión de información	Datos personales Archivos confidenciales Credenciales de Usuarios	Los atacantes envían mensajes personalizados, dirigidos a individuos específicos con la finalidad de engañar para que revelen información confidencial o permitan un consentimiento no autorizado sin darse cuenta para comprometer la seguridad	-Educación y concienciación sobre seguridad para los empleados. -Implementación de autenticación multifactor (MFA). -Uso de filtros de correo electrónico avanzados para detectar y bloquear intentos de spear-phishing. -Verificación de la autenticidad de las comunicaciones antes de proporcionar cualquier información confidencial.
Vishing	Media	Telefonía, VoIP	Números de tarjeta de crédito, Información de cuentas bancarias	Los atacantes utilizan llamadas telefónicas fraudulentas para engañar a	- Desconfiar de llamadas no solicitadas y verificar la identidad del interlocutor. - No proporcionar

				las víctimas y obtener información confidencial.	información personal o financiera a través de llamadas telefónicas no verificadas.
Smishing	Media	Mensajería de texto, Aplicaciones de Mensajería	Información personal, Contraseñas	Los atacantes envían mensajes de texto fraudulentos para engañar a las víctimas y obtener información confidencial.	- No hacer clic en enlaces ni responder mensajes de texto no solicitados. - Verificar la autenticidad de los remitentes antes de compartir información confidencial.
Ingeniería Social en Redes Sociales	Baja	Redes Sociales	Información personal, Fotos, Amigos y familiares	Los atacantes crean perfiles falsos o utilizan información engañosa en redes sociales para manipular a las víctimas y obtener información confidencial.	- Revisar la configuración de privacidad en las redes sociales y limitar la información compartida públicamente. - Ser cauteloso al aceptar solicitudes de amistad o interactuar con perfiles desconocidos.

Ataques de Ingeniería Social en Persona	Alta	Interacciones físicas, Llamadas telefónicas	Documentos de identificación, Información confidencial	Los atacantes interactúan directamente con las víctimas para obtener información confidencial a través de conversaciones en persona o llamadas telefónicas.	- Verificar la identidad de las personas antes de compartir información confidencial en persona o por teléfono. - No proporcionar información personal a personas no autorizadas o desconocidas.

Tabla 2: Cuadro Descriptivo de técnicas de Ingeniería Social

4.3 FASE DE DESARROLLO DE ESCENARIOS

En la fase de desarrollo de escenarios se describe el contexto de prueba seleccionada con su respectiva técnica de ingeniería social a evaluar para enfatizar la importancia y el origen de como los delincuentes informáticos operan para saltarse la seguridad en la información y cumplir con los objetivos planeados para usar en beneficioso propio

TÉCNICA DE INGENIERÍA SOCIAL	DESCRIPCIÓN DEL ESCENARIO	OBJETIVO DEL ATAQUE
Phishing	Un usuario recibe un mensaje de un link camuflado sobre soporte técnico o verificación de seguridad de plataformas tecnológicas como Facebook, Twitter, Gmail, entre otros	Obtener credenciales de inicio de sesión.

Spear-Phishing	El usuario recibe un mensaje de correo electrónico de un personal ya sea institución financiera, educativa o personal que cuenta con un archivo camuflado con un virus que tiene la capacidad de comprometer la integridad del sistema operativo y explorar la información de la víctima en el computador.	Encontrar datos confidenciales del usuario en la maquina victima
Vishing	Un individuo recibe una llamada telefónico sobre un familiar o persona de institución financiera, educativo u ofertas de operadoras con el fin de extraer datos personal básicos o muy sensibles para engañar y utilizarlas para beneficiosos propio	Obetener informacion sensible sober el usurario victima a suplantar
Smishing	Un usuario recibe un mensaje de texto que aparenta ser de su banco, solicitando hacer clic en un enlace para evitar el bloqueo de su cuenta. Al hacerlo, es redirigido a una página falsificada para ingresar sus credenciales bancarias.	Obtener credenciales de acceso a la cuenta bancaria.
Ingeniería Social en Redes Sociales	Un usuario acepta una solicitud de amistad de un desconocido en una red social. Este nuevo "amigo" solicita información personal, como fecha de nacimiento	Obtener información de seguridad personal.

	y nombre de soltera de la madre, bajo la apariencia de un cuestionario divertido.	
Ataques de Ingeniería Social en Persona	Un atacante se hace pasar por un empleado de mantenimiento y solicita acceso al área de servidores de una empresa para realizar una revisión de rutina. Una vez dentro, instala dispositivos de espionaje para robar información confidencial.	Obtener acceso físico a los sistemas de la empresa.

Tabla 3 Fase de Desarrollo de Escenarios

4.4 FASE DE PRUEBA DE PENETRACIÓN

Para desarrollar pruebas de penetración, se seleccionan técnicas esenciales de ingeniería social comúnmente utilizadas en el proceso de atacar la confidencialidad, integridad y disponibilidad de la información. La ingeniería social implica la manipulación de personas para obtener datos relevantes que beneficien al atacante. Se emplea ampliamente en ciberseguridad para obtener acceso no autorizado a sistemas informáticos, pero también se utiliza en contextos como estafas telefónicas, phishing por correo electrónico, pharming, entre otros.

Una técnica comúnmente seleccionada para iniciar el proceso y comprender mejor el arte de la ingeniería social es el phishing. Esto permite relacionarlo con otras técnicas y profundizar en su estudio.

PHISHING

- Utilizar herramienta de phishing
- Seleccionar el sitio de clonación
- Establecer las credenciales de usuario a robar
- Establecer link malicioso de la prueba
- Probar la funcionalidad del link
- Archivo de almacenamiento de datos
- Pescando victima con contexto engañoso

Estos son los principales puntos para tomar en cuenta para emplear el proceso de intrusión de la técnica phishing para imponer una página de inicio de sesión falsa para robar credenciales de usuario sin que sepan, para entender más de la prueba (Ver anexo 1: Manual Prueba Penetración – Phishing)

Para el siguiente proceso de prueba se seleccionó la técnica spear-phishing que permite enviar un archivo malicioso anexado al correo electrónico de la víctima, con la finalidad de tomar control de su máquina y visualizar los datos que presenta.

SPEAR-PHISHING

- Utilizar herramienta msfvenom
- Utilizar herramienta winrar
- Utilizar Proto Mail para envio de correos electrónicos de cualquier SMTP
- Onedrive para subir el archivo y recuperar un enlace compartido
- Visulizar archivos
- Crear Carpetas
- Ver variables de sesión
- Ver la información actual de la sesión victima

Estos son los principales puntos para tomar en cuenta para emplear el proceso de intrusión de la técnica spear - phishing para imponer un contexto de engañar a una persona a través de un archivo pdf enviado a su correo y tomar posesión en su máquina (Ver anexo 1: Manual Prueba Penetración – SpearPhishing)

4.5 FASE DE ANÁLISIS DE RESULTADOS

En esta fase se desarrolla el análisis de los resultados obtenidos en la fase anterior de explotación de las técnicas seleccionadas para la ingeniería social

La herramienta Zphisher captura la información de la ip, las credenciales a continuación se presenta el detalle en las plataformas de estudio “FACEBOOK” Y “GMAIL” – Técnica Phishing

HERRAMIENTA ZPHISHER - PHISHING						
FECHA	**DIRECCION IP**	**USUARIO**	**CONTRASEÑA**	**PLATAFORMA**	**COMENTARIOS**	**DETALLE**
1/06/2024 00:00 am	186.178.**.**	098424****	Loki********	Facebook	La victima cayo en el ataque Phishing sin sospecha – Cuenta sin seguridad Factor	Detalle 1
06/06/2024 14:20 pm	181.263.**.**	Quinde*****@hotmail.com	Carrilo*****	Facebook	La victima hace sin problema alguno al ataque de con el contexto planteado – No contaba con seguridad de factor	Detalle 2
06/06/2024 14:35 pm	200.7.**.***	09859******	May****	Facebook	El usuario tuvo la sospecha de que algo raro	Detalle 3

					acontecia con el link, pero acorde al contexto planteado del estudio accedió – No contaba con seguridad de factor	
06/06/2024 14: 50 pm	190.15.***.**	danna.******.*****@gmail.com	Dnp******	Facebook	La credenciales de la víctima fueron capturados de la mejor forma y la seguridad de factor no tenia	Detalle 4
06/06/2024 15:05 pm	190.63.**.**	Belen*********	Pe*****	Facebook	Las credenciales fueron capturadas de la mejor forma – La cuenta tiene seguridad de factor	Detalle 5
06/06/2024 15:20 pm	45.263.***.***	Lesslei**********@outlook.com	Xiini*******	Facebook	Las credenciales fueron capturadas de la mejor forma, pero no dieron facilidad de ingreso al login manifestaba	Detalle 6

					error de contraseña	
06/06/2024 15:35 pm	186.66.**.**	Carlaca********@outlook.com	Carla*****	Facebook	Las credenciales fueron capturadas de la mejor forma – No fueron las correctas para ingresar a la cuenta	Detalle 7
06/06/2024 15:50 pm	45.187.***.***	Byron_alaya****@hotmail.com	09*******	Facebook	Las credenciales del usuario fueron capturadas de la mejor forma – la cuenta no tiene seguridad de factor	Detalle 8

Tabla 4 Fase de Análisis de Resultados, Pruebas en Facebook

HERRAMIENTA ZPHISHER – PHISHING						
FECHA	**DIRECCION IP**	**USUARIO**	**CONTRASEÑA**	**PLATAFORMA**	**COMENTARIOS**	**DETALLE**
807/2024 10:36 am	45.96.**.**	Palber**@gmail.com	PAL******	Gmail	Credenciales de usuarios capturado exitosamente – No se dio el inicio de Gmail	Detalle G1
10/07/2024 11:08 PM	190.63.97.12	Carla*********@gmail.com	Carla*******	Gmail	Credenciales de usuarios capturado exitosamente – No se dio el inicio de Gmail	Detalle G2
10/07/2024 11:08 PM	190.155.158.150	Katita*******@gmail.com	Flow*****	Gmail	Credenciales de usuarios capturado exitosamente – No se dio el inicio de Gmail	Detalle G3

10/07/2024 11:18 PM	190.63.241.71	Ferphon*******@gmail.com	Ferc*****	Gmail	Credenciales de usuarios capturado exitosamente – No se dio el inicio de Gmail	Detalle G4
10/07/2024 00:20 PM	181.78.****.***	Pacruz*******@gmail.com	0928*****	Gmail	Credenciales de usuarios capturado exitosamente – No se dio el inicio de gmail	Detalle G5

Tabla 5 Fase de Análisis de Resultados, Pruebas en Gmail

En este cuadro se describe el proceso de identificación y análisis a través de la técnica SPEAR-PHISHING, un método sofisticado de ingeniería social Esta táctica implica el envío de correos electrónicos aparentemente legítimos pero personalizados, que contienen archivos o enlaces maliciosos. El objetivo es engañar a la victima para que revele información sensible o instale software malicioso inadvertidamente. Es crucial comprender como funciona esta técnica para desarrollar estrategias de defensa efectivas. Esto incluye la implementación de filtros de correos avanzados, programas de concientización para empleados, y protocolos de seguridad robustos. También es importante considerar el impacto potencial en la privadcidad y seguridad de los datos, asi como la implicaciones legales y éticas de tales ataques.

COMANDO	DESCRIPCIÓN	SALIDA
SET	Muestra las variables de entorno.	ALLUSERSPROFILE=C:\ProgramData APPDATA=C:\Users\Hacking\AppData\Roaming CommonProgramFiles=C:\Program Files\Common Files CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files ProgramW6432=C:\Program Files COMPUTERNAME=HACKING-PC ComSpec=C:\Windows\system32\cmd.exe HOMEDRIVE=C: HOMEPATH=\Users\Hacking LOCALAPPDATA=C:\Users\Hacking\AppData\Local LOGONSERVER=\HACKING-PC NUMBER_OF_PROCESSORS=2 OS=Windows_NT Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\WindowsPowerShell\v1.0;...
DIR	Lista los archivos en el directorio Downloads.	Directory of C:\Users\Hacking\Downloads 12/06/2024 11:24 <DIR> . 12/06/2024 11:24 <DIR> .. 12/06/2024 09:32 302.161 AcroRdrDC2400220759_es_ES.exe 12/06/2024 09:04 61 Contra4.txt 12/06/2024 11:22 52.893.344 firefox-esr-78.8.0-installer.exe 12/06/2024 10:30 222.720 icono.ico 12/06/2024 10:29 188.084 Notas.pdf 12/06/2024 10:20 51.236.765 NotaImportante.pdf.exe 12/06/2024 11:37 7.168 pruebaIng.exe 7 File(s) 356.293.496 bytes 2 Dir(s) 257.860.952.064 bytes free

CAT CONTRA.TXT	Intenta mostrar el contenido de Contra.txt (pero falla porque 'cat' no es un comando reconocido).	'cat' is not recognized as an internal or external command, operable program or batch file.
MORE CONTRA.TXT	Muestra el contenido del archivo Contra.txt usando el comando 'more'.	alexanderalay1995@gmail.com contra- alexanderalaymerejildo23
DEL CHROMESETUP.EXE	Elimina el archivo ChromeSetup.exe del directorio Downloads.	Directory of C:\Users\Hacking\Downloads 12/06/2024 11:24 <DIR> . 12/06/2024 11:24 <DIR> .. 12/06/2024 09:32 302.161 AcroRdrDC2400220759_es_ES.exe 12/06/2024 11:22 52.893.344 firefox-esr-78.8.0-installer.exe 12/06/2024 10:30 222.720 icono.ico 12/06/2024 10:29 188.084 Notas.pdf 12/06/2024 10:20 51.236.765 NotaImportante.pdf.exe 12/06/2024 11:37 7.168 pruebaIng.exe 6 File(s) 356.290.242 bytes 2 Dir(s) 257.862.688.768 bytes free

Tabla 6 Detalle de Comandos y Efectos en Ataque SPEAR-PHISHIN

4.6 FASE DE MANUAL

En esta fase del manual se proporciona una guía detallada para implementar medidas de seguridad informática con el objetivo de proteger los datos personales contra ataques de ingeniería social. Se destacan programas continuos de formación para empleados, incluyendo simulaciones de ataques para mejorar la capacidad de respuesta. Además, se promueve el uso de tecnologías de seguridad como filtros de correo electrónico, autenticación multifactor (MFA) y software de seguridad actualizado. También se establecen políticas robustas de gestión de contraseñas y uso aceptable de recursos tecnológicos. Para la respuesta a incidentes, se sugiere la creación de un equipo especializado y el desarrollo de un plan de respuesta detallado. La fase incluye la evaluación de riesgos mediante la identificación de activos y vulnerabilidades, el análisis de impacto y la mitigación de riesgos con controles de seguridad adecuados. Finalmente, se recomiendan prácticas de seguridad personal y procedimientos de reporte de incidentes para mantener una protección continua (Ver Anexo: Manual).

CONCLUSIONES

- El análisis exhaustivo de las técnicas de ingeniería social, como phishing, spear-phishing y vishing, ha demostrado que estos métodos son extremadamente efectivos para engañar a los usuarios y obtener información confidencial. Comprender cómo operan estos ataques es crucial para desarrollar estrategias de defensa eficaces. La educación y concienciación continua sobre estas amenazas son fundamentales para prevenir el robo de identidad digital.

- El desarrollo e implementación de escenarios de pruebas en entornos controlados han permitido evaluar de manera efectiva el nivel de protección de los datos personales. Estas han resaltado la importancia de simular ataques reales para identificar vulnerabilidades en los sistemas de seguridad existentes y mejorar las defensas en función de los resultados obtenidos. Las simulaciones han mostrado ser una herramienta valiosa para medir la eficacia de las políticas y controles de seguridad.

- La creación de un manual detallado de estrategias y políticas de seguridad informática ha proporcionado una guía integral para fortalecer la protección de datos personales. Este manual incluye medidas técnicas, políticas organizacionales y procedimientos de respuesta a incidentes, ofreciendo un marco estructurado para proteger la información confidencial contra amenazas internas y externas.

RECOMENDACIONES

- Es esencial implementar programas de capacitación continua para estudiantes y personal sobre las técnicas de ingeniería social, como phishing, spear-phishing y vishing. Estas sesiones deben incluir simulaciones de ataques para que los participantes puedan aprender a identificar y responder a amenazas reales de manera efectiva.

- La facultad debe adoptar filtros avanzados de correo electrónico para detectar y bloquear mensajes sospechosos. Además, es crucial implementar la autenticación multifactor (MFA) para el acceso a sistemas sensibles y mantener actualizados los antivirus y sistemas de detección de amenazas en todos los dispositivos utilizados en la facultad.

- Establecer y comunicar claramente políticas para el uso de contraseñas seguras y el cambio regular de las mismas. También, es importante definir una política de uso aceptable de recursos tecnológicos y desarrollar un plan de respuesta a incidentes que incluya procedimientos específicos para gestionar ataques de ingeniería social de manera efectiva y rápida.

BIBLIOGRAFÍAS

[1] José Roa B., «Seguridad informática,» Mc Graw Hill Education, Madrid - España, 2013.

[2] Javier Guaña M., «La importancia de la seguridad informática en la educación digital: retos y soluciones,» ReciMundo, Quito, 2023.

[3] UNIR, «Unir - La Universidad en Internet,» El robo de la identidad digital: tipos y legislación vigente, 20 02 2023. [En línea]. Available: https://www.unir.net/derecho/revista/robo-identidad-digital/. [Último acceso: 06 09 2023].

[4] Ing. Angel Calle A., «Modelo de gestion de la información para la protección de datos personales en la carrera de ciencias policiales de la universidad central del Ecuador,» Universidad Regional Autónoma de los Andes "UNIADES", Ambato - Ecuador , 2018.

[5] Esteban Rodríguez J., «Medidas de Seguridad de Protección de Datos Personales en mi Lugar de Trabajo,» Infotec Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, Ciudad de México, 2020.

[6] Marcelo Peñafiel S., «Ingenieria Social en una Institución de Educación Superior aplicando técnicas computacionales y no computacionales,» Universidad Estatal Peninsula de Santa Elena, La Libertad - Ecuador, 2022.

[7] Kali Linux, «Kali Linux,» 2020. [En línea]. Available: https://www.kali.org/. [Último acceso: 27 03 2024].

[8] IBM, «¿Qué son las pruebas de penetración?,» 2022. [En línea]. Available: ¿Qué son las pruebas de penetración?. [Último acceso: 27 03 2024].

[9] Nica Latto, «¿Qué es un virus informático y cómo funciona?,» Avast, 12 02 2020. [En línea]. Available: https://www.avast.com/es-es/c-computer-virus. [Último acceso: 27 03 2024].

[10] Daniel Cunha B., «Metasploit Framework: Explotar vulnerabilidades puede ser bastante fácil,» WeliveSecurity, 27 10 2023. [En línea]. Available: https://www.welivesecurity.com/es/recursos-herramientas/metasploit-framework-explotar-vulnerabilidades/. [Último acceso: 07 03 2024].

[11] QUORA, «¿Qué es el SEToolkit, y qué tipo de ataques de ingeniería social facilita crear y lanzar?,» Quora, 21 02 2023. [En línea]. Available: https://es.quora.com/Qu%C3%A9-es-el-SEToolkit-y-qu%C3%A9-tipo-de-ataques-de-ingenier%C3%ADa-social-facilita-crear-y-lanzar. [Último acceso: 21 03 2024].

[12] Fernando Tavella, «WSHRAT: troyano de acceso remoto capaz de realizar múltiples acciones en un equipo infectado,» WeliveSecurity, 25 10 2021. [En línea]. Available: WSHRAT: troyano de acceso remoto capaz de realizar múltiples acciones en un equipo infectado. [Último acceso: 20 03 2024].

[13] Katherine Ramirez, «Conexion Puce,» Ciberseguridad: protege tus datos personales en la era digital, 08 06 2023. [En línea]. Available: https://conexion.puce.edu.ec/ciberseguridad-protege-tus-datos-personales-en-la-era-digital/. [Último acceso: 20 12 2023].

[14] Marlon Calle, Nery Chiliquinga, «IMPACTO DE LA ENSEÑANZA EN LÍNEA EN LA EDUCACIÓN PRESENCIAL DE LA UNIDAD EDUCATIVA PATRIMONIO DE LA HUMANIDAD DESDE LA PERSPECTIVA DOCENTE,» *Qualitas - Revista Ciéntifica,* vol. 1, nº 1, pp. 50-75, 2023.

[15] ESGinnova Group, «ESGinnova Group,» Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad, 01 02 2018. [En línea]. Available: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/. [Último acceso: 15 03 2024].

[16] S. PLANIFICACION, «Plan de Creacion de Oportunidades 2021-2025,» Quito, 2021-2025.

[17] Gabriel Baca U. , Introducción a la Seguridad Informática, México : Grupo Editorial Patria, 2016.

[18] UNIR, «Los 4 principios de la seguridad informática y su implementación,» UNIR, 04 Enero 2023. [En línea]. Available: https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/. [Último acceso: 18 Mayo 2024].

[19] Unir , «rincipios de la seguridad informática: consejos para la mejora de la ciberseguridad,» UNIR, 30 Abril 2020. [En línea]. Available: https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/. [Último acceso: 18 Mayo 2024].

[20] Katherine Ramírez, «Ciberseguridad: protege tus datos personales en la era digital,» ConexionPuce, 08 Junio 2023. [En línea]. Available: https://conexion.puce.edu.ec/ciberseguridad-protege-tus-datos-personales-en-la-era-digital/. [Último acceso: 18 Mayo 2024].

[21] Alexander Verdesoto G., «Utilización de Hacking Ético para diagnosticas, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones,» Escuala Politécnica Nacional, Quito - Ecuador , 2007.

[22] Banco Pichincha, «Qué son los ataques de ingeniería social y cómo evitarlos,» 01 Diciembre 2020. [En línea]. Available: https://www.pichincha.com/blog/ataques-ingenieria-social. [Último acceso: 18 Mayo 2024].

[23] Juanjo Ramos, Cómo protogerte del phishing - Evita que te roben tu información y tu dinero, E-Book Distribution: Xinxii, 2022.

[24] Ivan Belcic, «¿Qué es exactamente el phishing?,» Avast Academy, 06 Octubre 2023. [En línea]. Available: https://www.avast.com/es-es/c-phishing#topic-3. [Último acceso: 18 Mayo 2024].

[25] Danielle Bodnar, «¿Qué es el pharming y cómo puede protegerse de él?,» 07 Octubre 2016. [En línea]. Available: https://www.avast.com/es-es/c-pharming. [Último acceso: 18 Mayo 2024].

[26] Danielle Bodnar, «Qué es el vishing: una definición,» AVG, 27 Mayo 2022. [En línea]. Available: https://www.avg.com/es/signal/what-is-a-vishing-attack. [Último acceso: 18 Mayo 2024].

[27] UNIR, «¿Qué es el vishing telefónico y cómo detectarlo?,» La Universidad en Internet, 01 Enero 2024. [En línea]. Available: https://www.unir.net/derecho/revista/vishing/. [Último acceso: 18 Mayo 2024].

[28] IBM, «¿Qué es el smishing?,» 2022. [En línea]. Available: https://www.ibm.com/es-es/topics/smishing. [Último acceso: 18 Mayo 2024].

[29] Ruth Matthews, «¿Qué es el smishing y cómo funciona?,» NordVPN, 09 Marzo 2021. [En línea]. Available: https://nordvpn.com/es/blog/que-es-el-smishing/. [Último acceso: 18 Mayo 2024].

[30] E. Andrea, Interviewee, *Retos empresariales para garantizar derechos en materia de protección de datos personales.* [Entrevista]. 15 marzo 2023.

[31] I. Security, «Por qué es importante la privacidad de los datos,» Estados Unidos de America, 2018.

[32] G. Atico34, «¿Cómo cumplir la LOPD (Ley de Protección de Datos)?,» 2024.

[33] Shirley Flores L. , «ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN CIBER ATAQUES DE INGENIERÍA SOCIAL PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN, DE LA UNIVERSIDAD TÉCNICA DE AMBATO,» Universidad Tecnica de Ambato, Ambato - Ecuador , 2023.

[34] Sofia Villacís M., «Diseño de una campaña de ataques de ingeniería social,» Pontificia Universidad Católica del Ecuador, Quito - Ecuador , 2023.

[35] Pedro Morales G., «Implementación de ingeniería social para la detección de vulnerabilidades en los sistemas de información utilizados en la Universidad Autónoma de Zacatecas, Centro Educativo Rotary y la Coordinación de la Secretaría de Seguridad Pública, basados en metodo,» Universidad Autónoma de Zacatecas, Zacatecas, 2020.

[36] S. Campbell, DISEÑOS EXPERIMENTALES Y CUASIEXPERIMENTALES EN LA INVESTIGACION SOCIAL, AMMORRORTU, Ed., BUENOS AIRES, 2002.

[37] Carlos Ramos G., «LOS ALCANCES DE UNA INVESTIGACIÓN,» CienciAmerica, Quito - Ecuador, 2020.

[38] Sampieri, Metodología de la Investigación, México: McGRAW-HILL, 2010.

[39] Fernández Pita, «INVESTIGACIÓN CUANTITATIVA Y CUALITATIVA,» ESPAÑA, CAD ATEN PRIMARIA, 2002, pp. 9:76-78.

[40] P. CORBETTA, «METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN CUALITATIVAS,» MADRID, MC GRAW HILL, 2007.

[41] CyberZaintza, «Open Source Security Testing Methodology Manual (OSSTMM),» 2022. [En línea]. Available: https://www.ciberseguridad.eus/ciberpedia/vulnerabilidades/open-source-security-testing-methodology-manual-

osstmm#:~:text=%C2%BFQu%C3%A9%20es%3F,de%20la%20seguridad%20operativa%20real.. [Último acceso: 04 04 2024].

ANEXOS

ANEXO 1 – ENTREVISTA

UPSE – UNIVERSIDAD ESTAL PENINSULA DE SANTA ELENA
Entrevistador
Objetivo
¿Cómo perciben los estudiantes y el personal académico de la UPSE la importancia de proteger los datos personales?
¿Cuál es su nivel de confianza en la seguridad de los datos personales dentro de la facultad?
¿Han experimentado alguna vez algún incidente relacionado con la seguridad de la información en la facultad?
¿Cómo creen que podrían mejorar la protección de los datos personales en la UPSE - Facultad de Ciencias Sociales y de la Salud?
¿Qué preocupaciones tienen sobre la seguridad de la información en un entorno académico?
¿Cómo afectaría una violación de seguridad de datos a la confianza y reputación de la facultad?
¿Qué medidas creen que podrían implementarse para aumentar la conciencia sobre la seguridad de la información entre los estudiantes y el personal académico?
¿Qué impacto tendría la pérdida o compromiso de datos personales en la facultad y en la comunidad estudiantil?
¿Qué valoran más en términos de seguridad de la información dentro de la facultad?
¿Qué papel creen que debería desempeñar la UPSE en la protección de los datos personales de sus estudiantes y personal académico?

ANEXO

PRUEBA DE PENETRACIÓN

PHISHING

Herramienta: ZPHISHER **Tiempo: 15 minutos**

Objetivo: Obtener credenciales de usuario mediante una página falsificada de Facebook

1. Se procede la clonación del repositorio de github de ZPHISHER tras el siguiente link https://github.com/htr-tech/zphisher

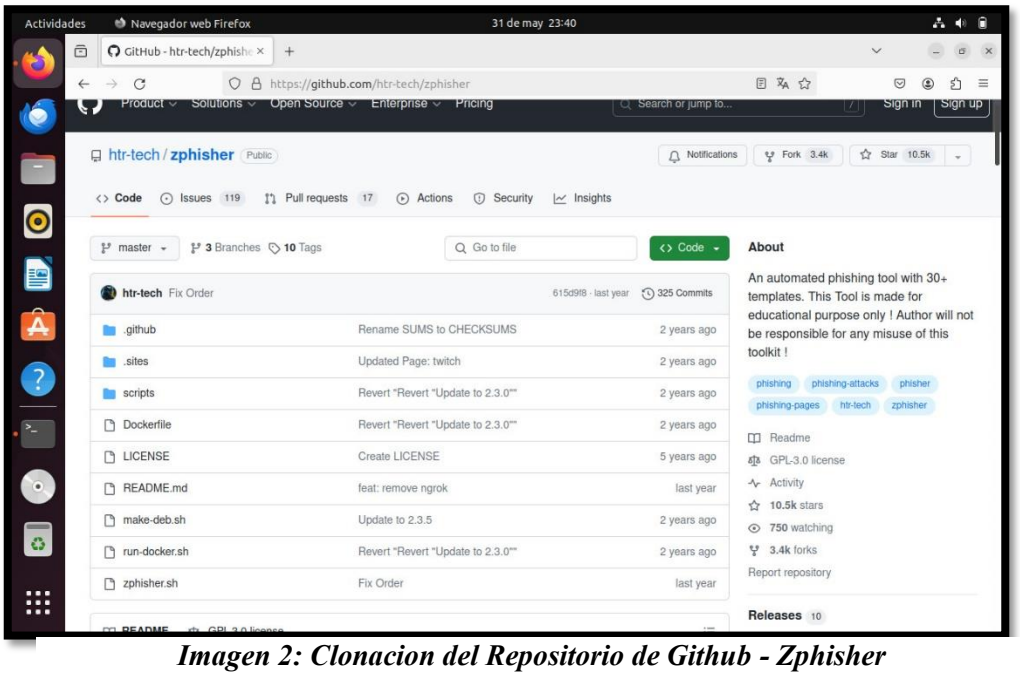

Imagen 2: Clonacion del Repositorio de Github - Zphisher

2. Se procede a copiar la dirección del repositorio para desarrollar la clonación en la maquina atacante

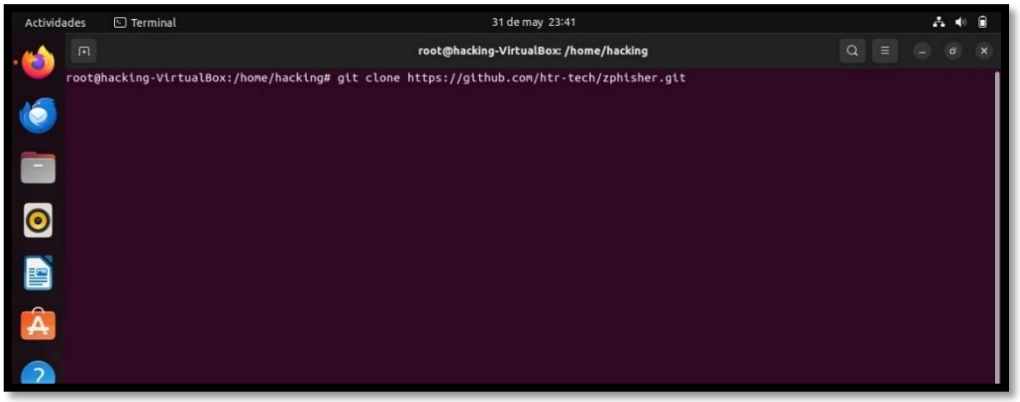

Imagen 3 Copia del Repositorio en la Máquina Virtual – Ubuntu 22.04

3. Repositorio Clonado a la perfección

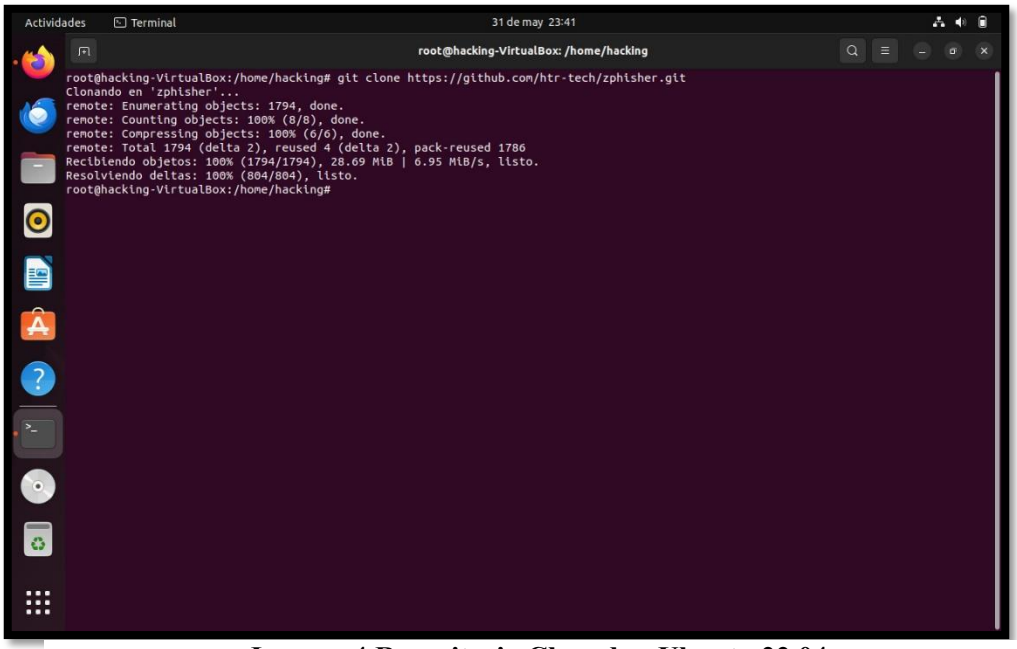

Imagen 4 Repositorio Clonado - Ubuntu 22.04

4. Se ingresa a la direccion de Zphisher para ejecutar el archivo zphisher.sh

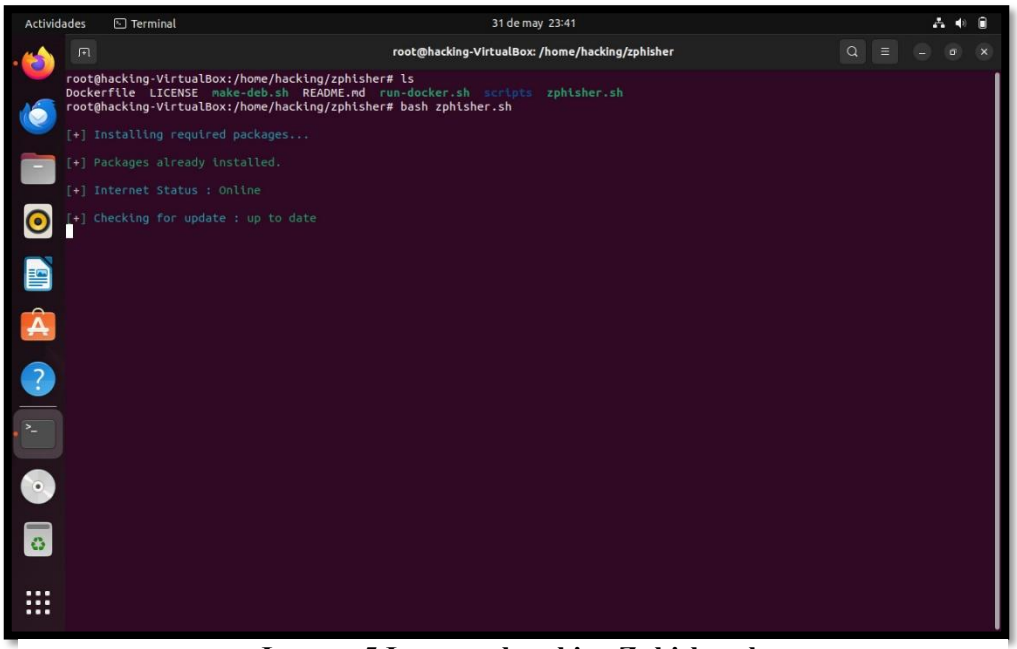

Imagen 5 Ingreso al archivo Zphisher.sh

5. Se carga completamente el script con diversas plantillas para ejercer el phishing de la red social Facebook

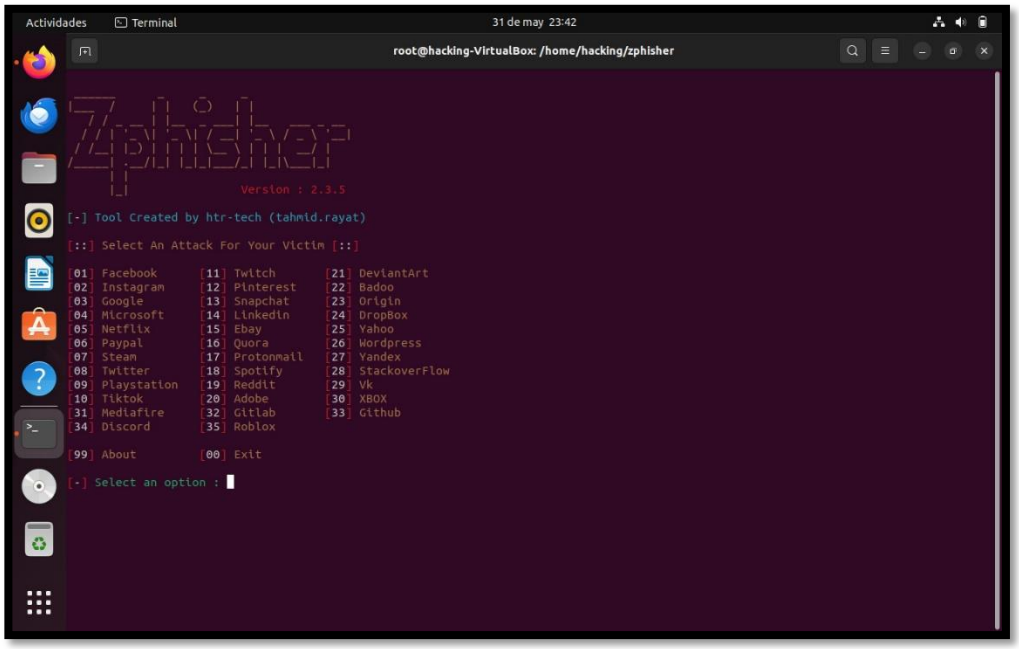

Imagen 6 Script con Diversas Plantillas -Zphisher

6. Seleccionar el número del sitio a clonar en este caso 1 para Facebook

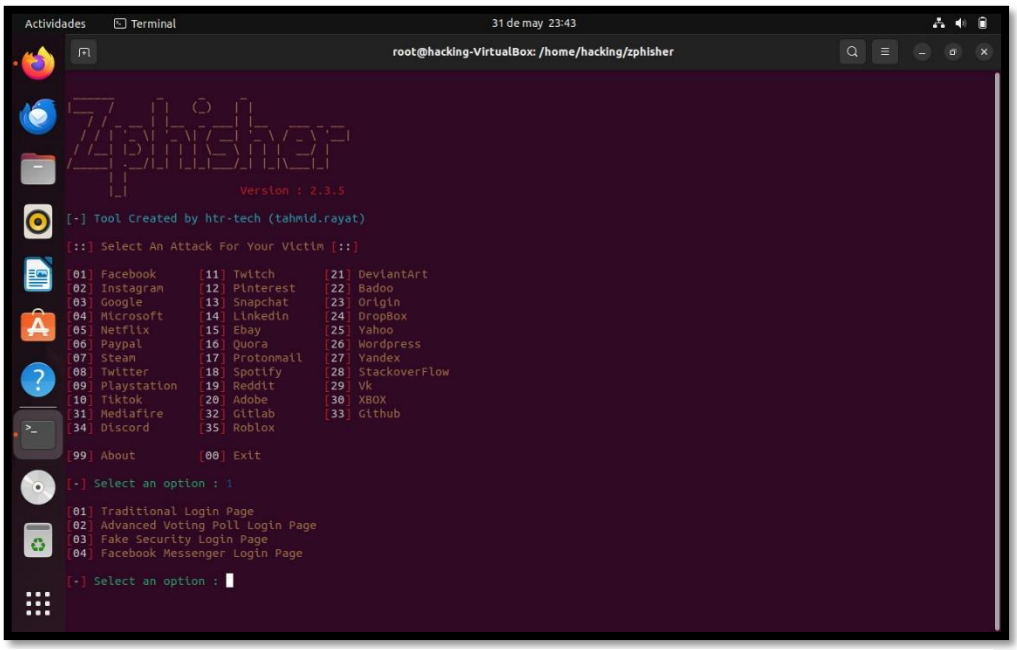

Imagen 7 Selección del Sitio a Clonar - Facebook (01)

7. Aparece unas opciones para ejercer la clonación, seleccionar 1 para ejercer la clonación del portal Facebook tradicional y habitual que se ve hoy en día

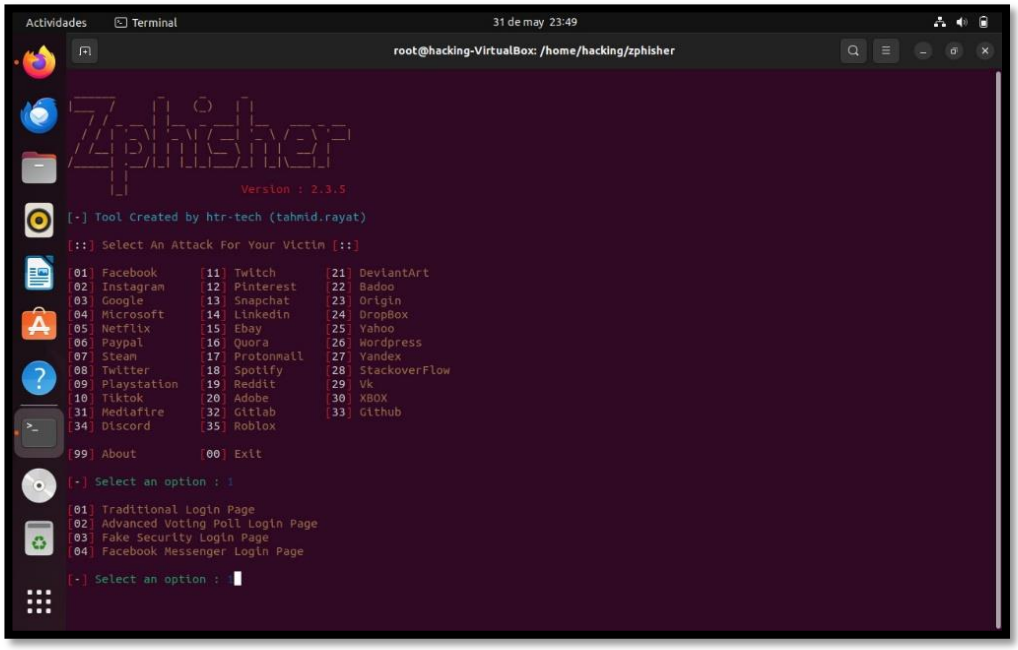

Imagen 8 Selección Tradicional Login Page - Facebook (01)

8. Una vez seleccionado la plantilla a clonar, nos da tres opciones de ejecutar el sitio de URL, por ejemplo el localhost corresponde a usar nuestra propia dirección de la máquina y emplear una dirección diferente de la local pero establecida en la propia red, la opción de Cloudflared permite crea la dirección de manera local en nuestra propia red pero no es capaz de expandirse en su totalidad, la opción LocalXpose es una alterativa interesante debida que permite ejercer una url local dentro de la red para que sea compartido para todos. Pero tiene un valor de duración de 15 minutos, aquellos 15 minutos para el hackear a la victima.

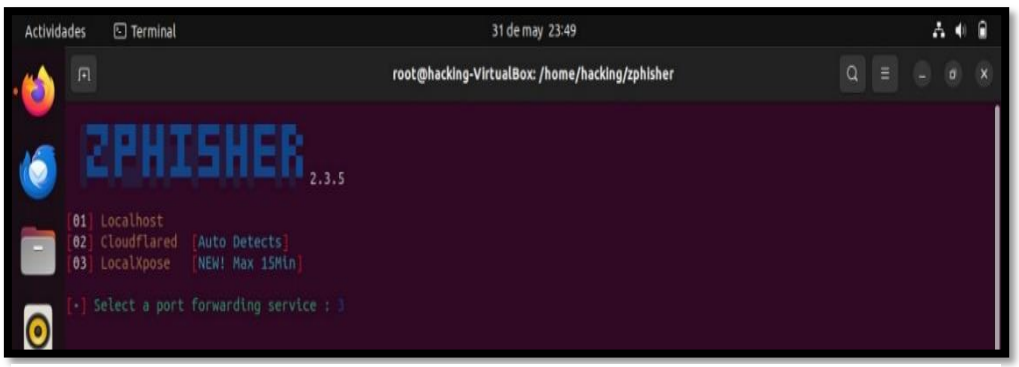

Imagen 9 Selección (03), LocalXpose - Tiempo Max 15Min

9. Se selecciona la opción 3 para que la clonación de Facebook sea de manera general y se capture la info necesaria de la víctima.

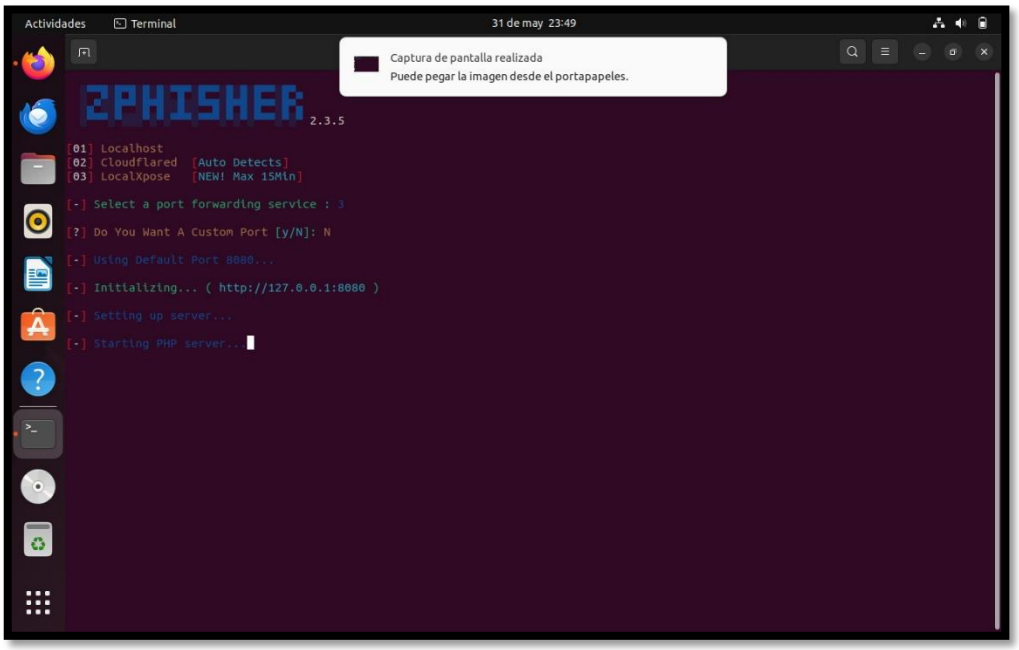

Imagen 10 Inicialización de la clonación de Facebook

10. Para que se ejerza una url con dirección local se necesita tener una cuenta en LocalXpose para tener una Token de acceso a la cuenta y asi crear la dirección.

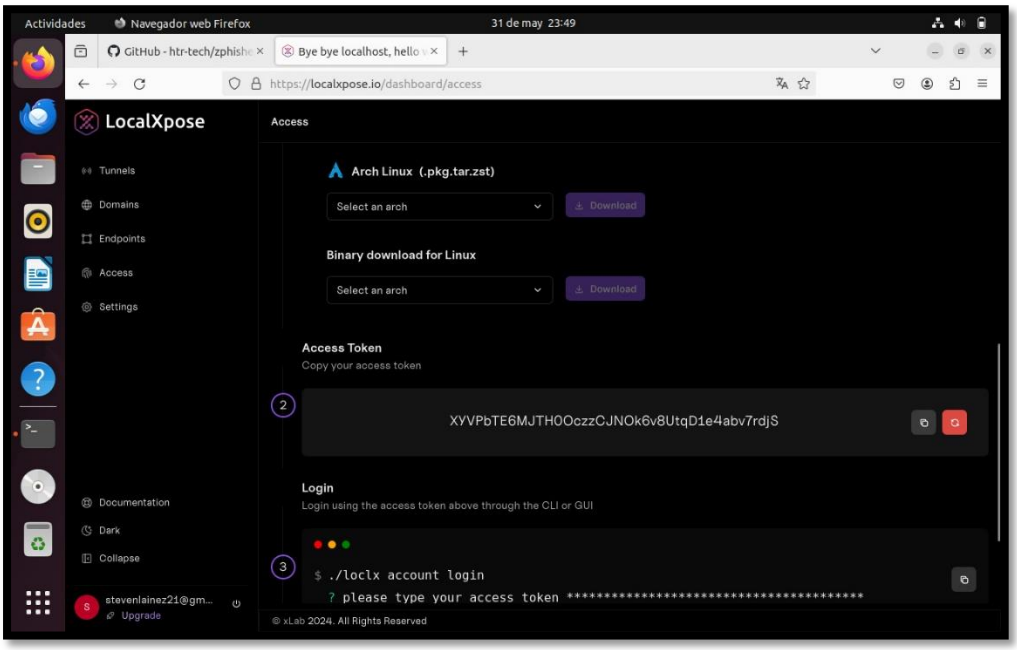

Imagen 11 Pagina de LocalXpose con Acceso al Token

11. Se inserta el token en el input que el script Solicita.

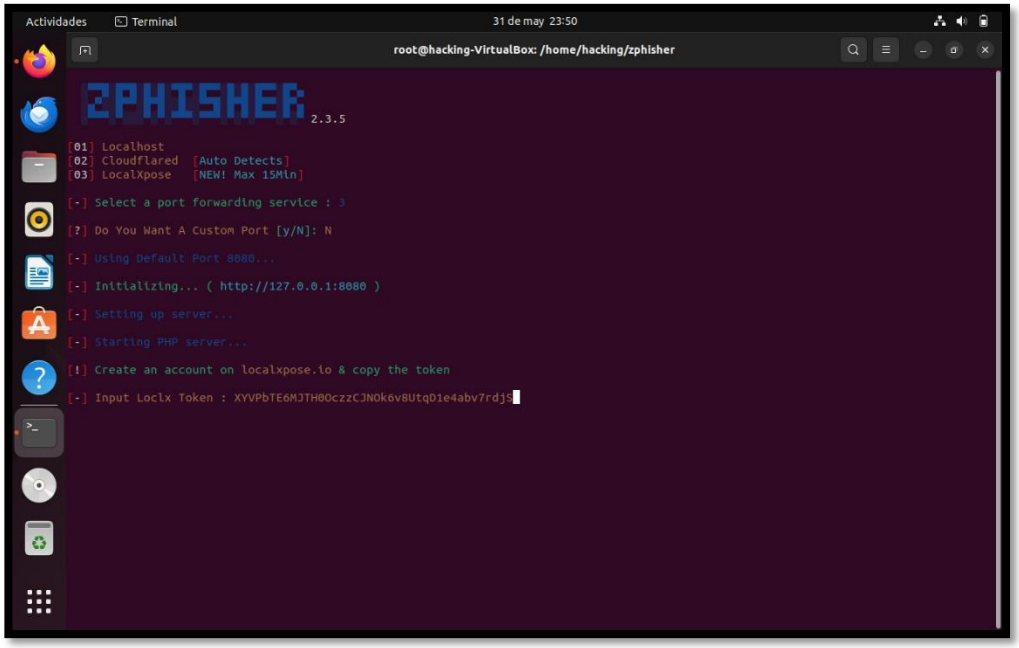

Imagen 12 Copiamos el Token que nos brindó LocalXpose en el Script - Zphisher

12. Dar “Y” como un “Si” para crear un link server en una región fuera de lo habitual de nuestro local.

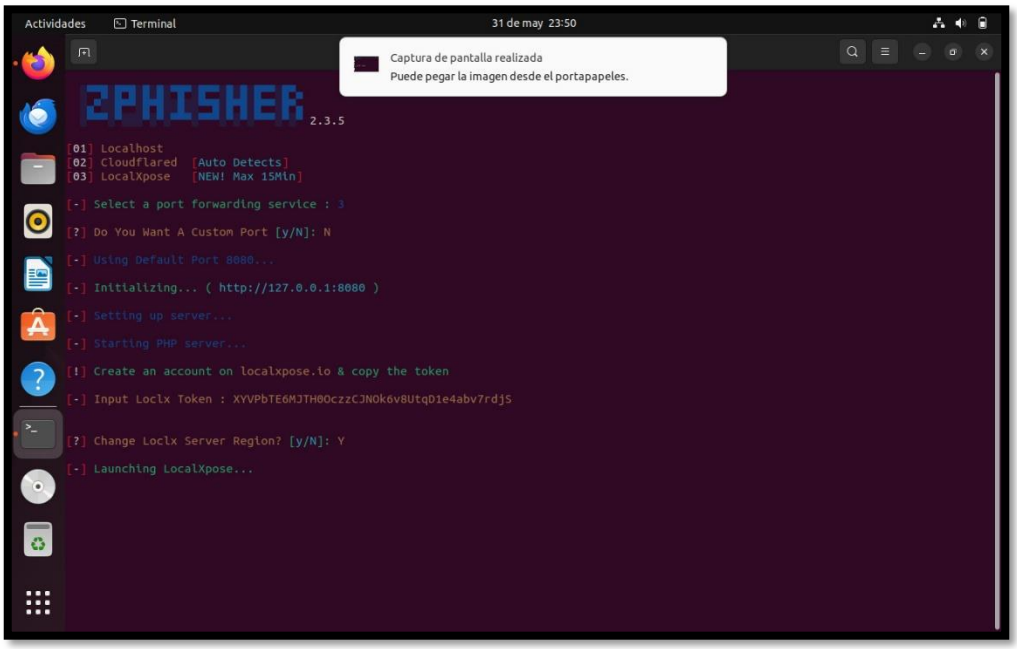

Imagen 13 Cambiamos el Server Región - Zphisher

13. Se genera la dirección y tener en cuenta solo el link que esta de color verde

    URL 1: https://iyrbmmhmfq.eu.loclx.io

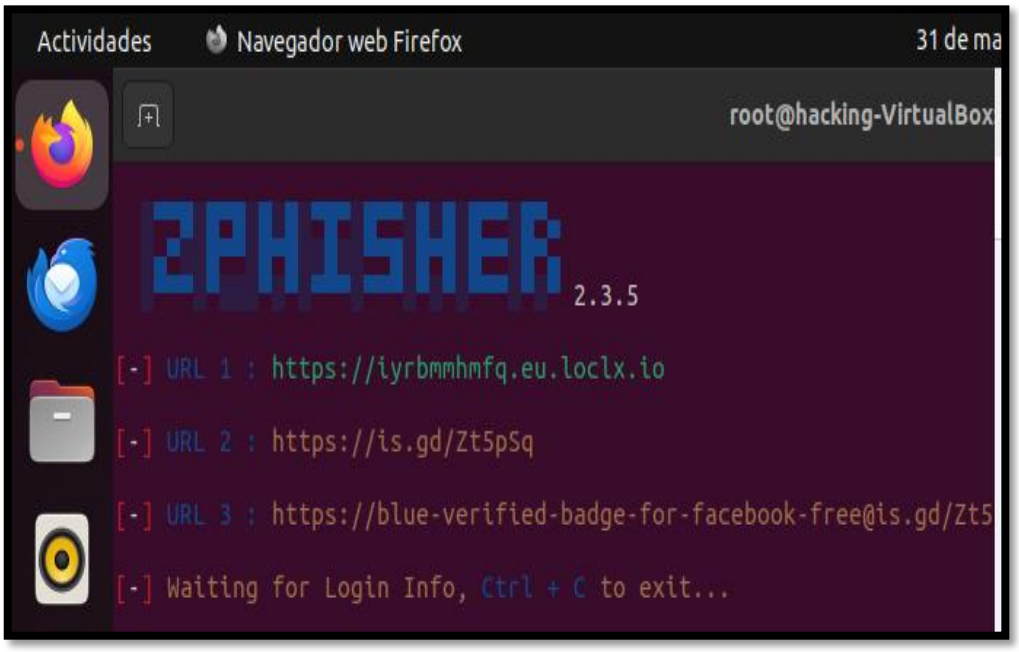

Imagen 14 Link Generado en Zphisher - Https://iyrbmmhmfq.eu.loclx.io

14. Se procede a corta la dirección en una página de short links.

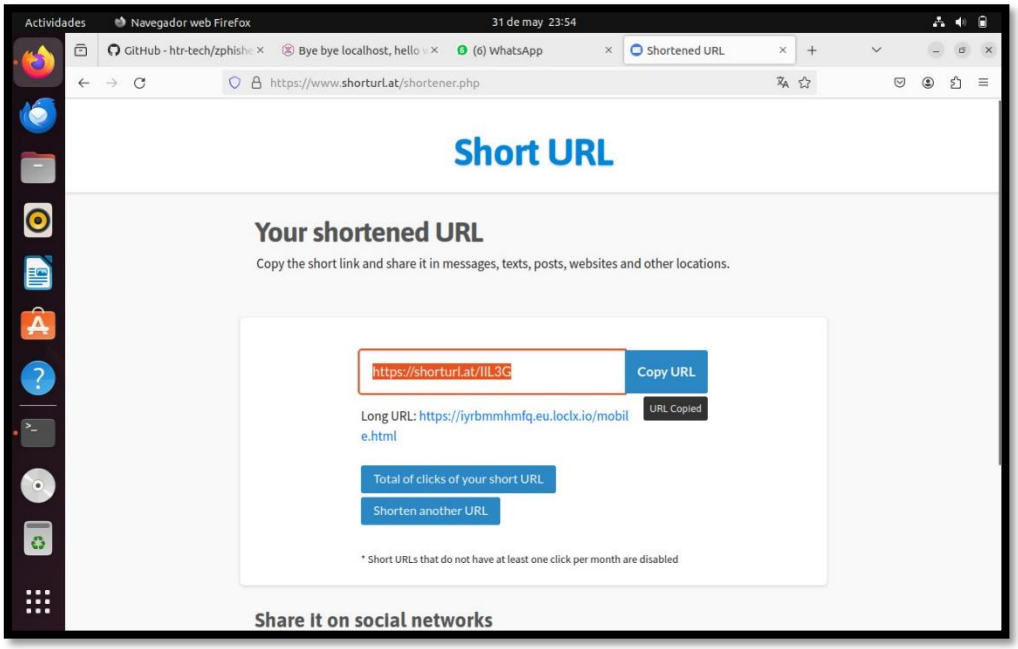

Imagen 15 Ingreso Pagina Short Links

15. Se envía el link o enlace a la víctima por WhatsApp.

Imagen 16 Link enviado mediante la Aplicación WhatsApp

16. La victima ingresa y se captura su dirección local, y una vez que esté en el formulario se captura también las credenciales el login.

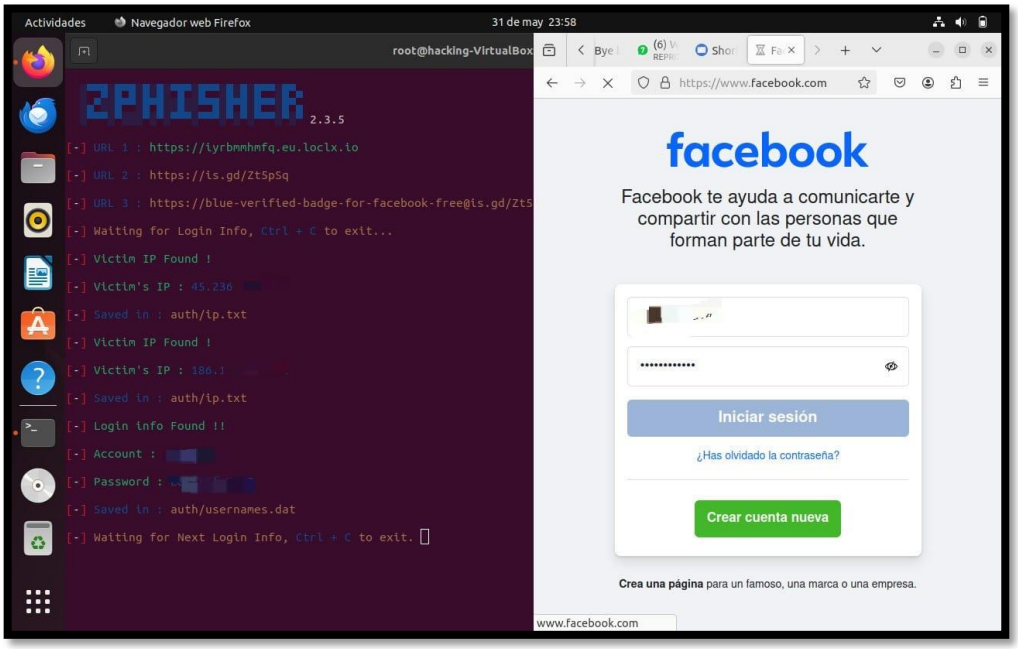

Imagen 17 Capturando datos de la Victima una vez de haber ingresado sus datos en Facebook

17. Se logra obtener el ingreso de sesión de manera correcta. Usuario Hackeado exitosamente.

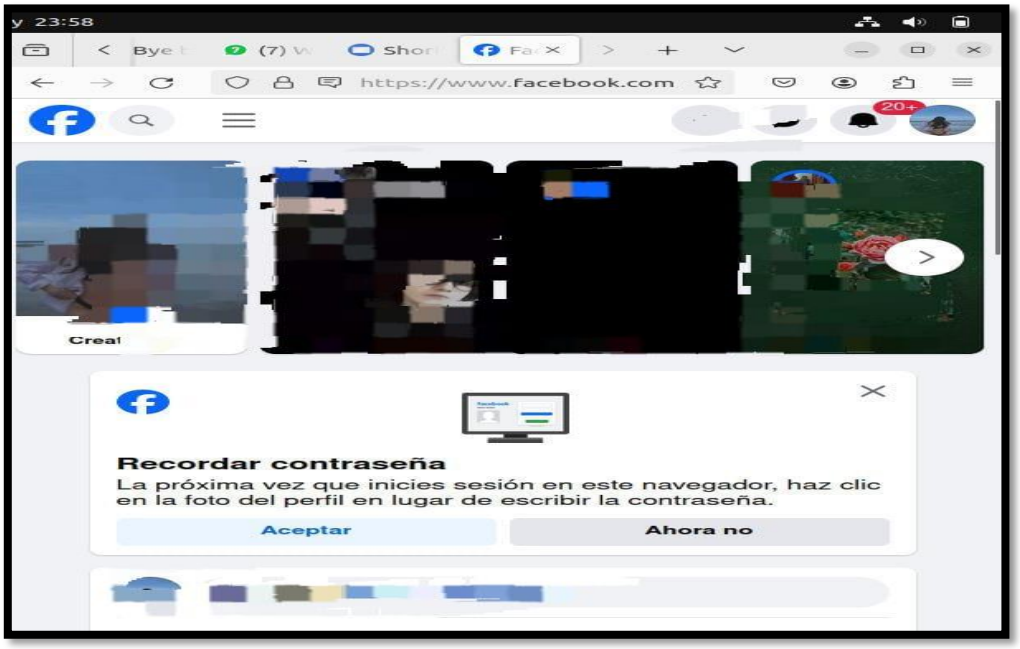

Imagen 18 Acceso a la cuenta del usuario hackeado en Facebook.

Manipulación Digital 2

18. Usuario 2 se le envía el enlace o link mediante el aplicativo WhatsApp

Imagen 19 Enlace o Link enviado al Usuario 2 mediante WhatsApp

19. Se procede a tomar las credenciales del usuario 2 que nos aparece en Zphisher.

Imagen 20 Acceso a las credenciales, Usuario 2

20. Login Usuario 2.

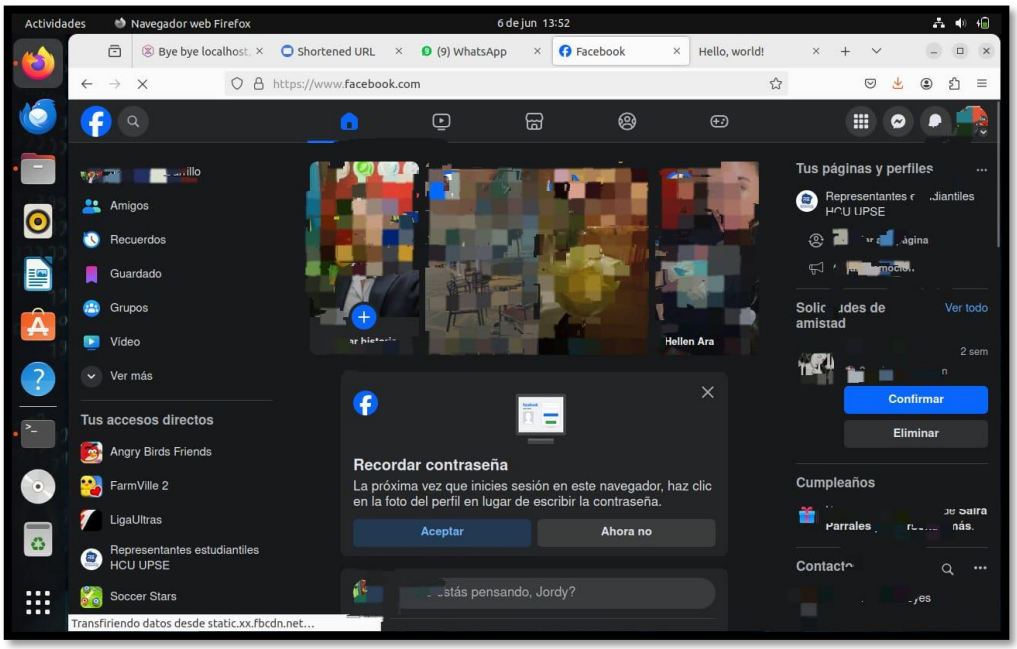

Imagen 21 Acceso no autorizado o acceso ilegitimo - Usuario 2

Manipulación Digital 3

21. Credenciales del Usuario 3.

Imagen 22 Acceso a las credenciales, Usuario 3

22. Login o Acceso cuenta del usuario 3.

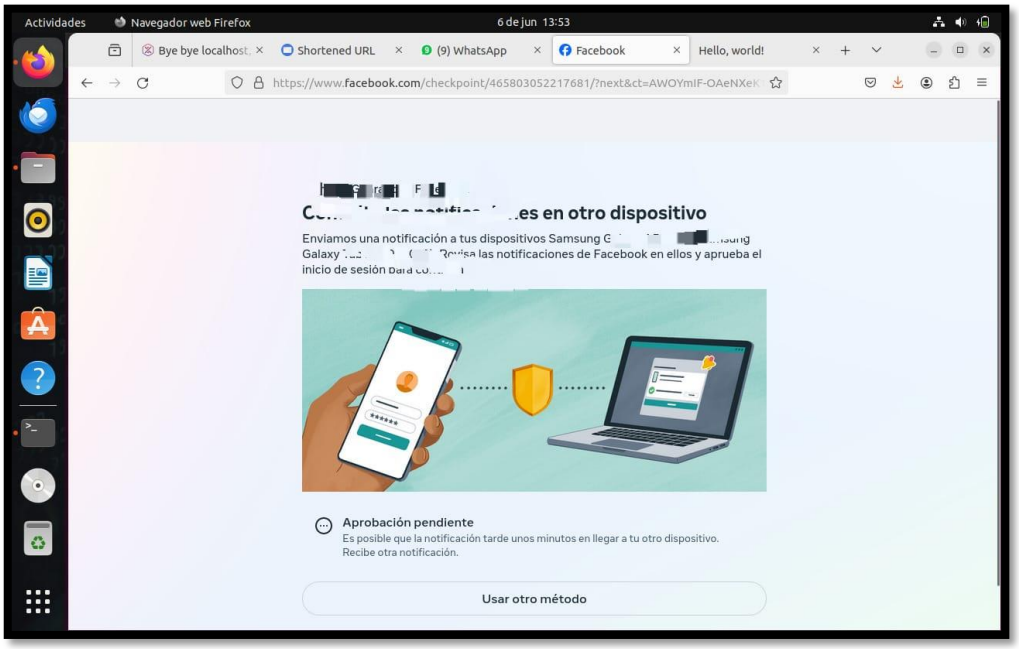

Imagen 23 Acceso no autorizado o acceso ilegitimo - Usuario 3

Manipulación Digital 4

23. Se toma las credenciales del usuario 4.

Imagen 24 Acceso a las credenciales, Usuario 4

24. Login o Acceso cuenta del usuario 4

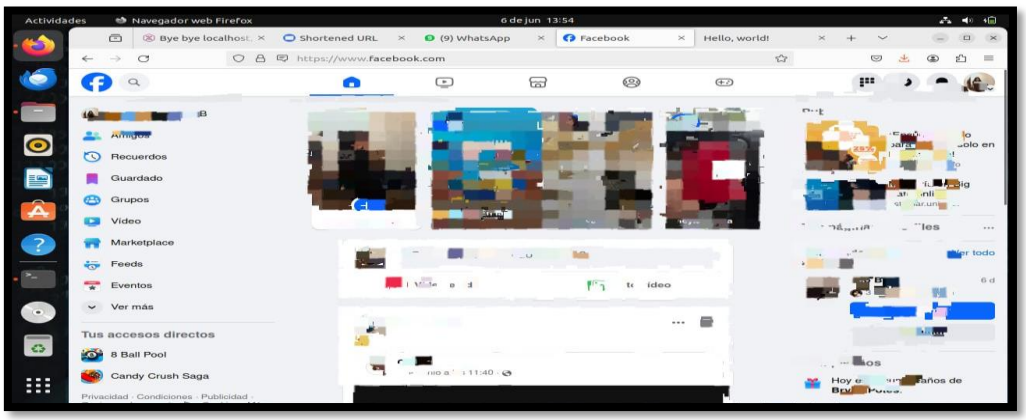

Imagen 25 Acceso no autorizado o acceso ilegitimo - Usuario 4

Manipulación Digital 5

25. Credenciales de Usuario Capturadas.

Imagen 26 Acceso a las credenciales, Usuario 5

26. Login o Acceso cuenta del usuario 5.

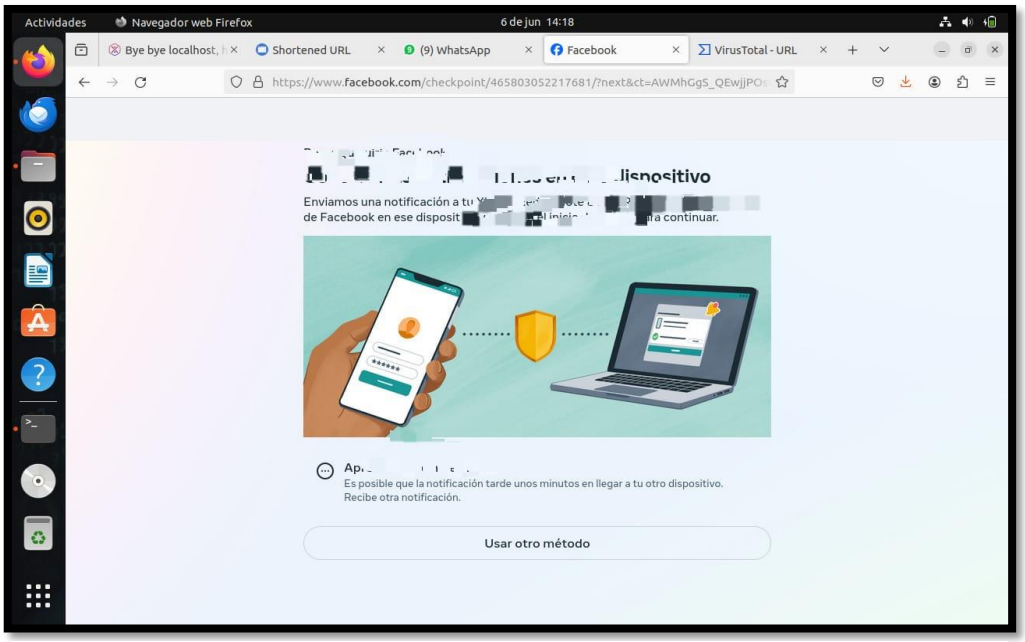

Imagen 27 Acceso no autorizado o acceso ilegitimo - Usuario 5

Manipulación Digital 6

27. Credenciales de Usuario Capturadas.

Imagen 28 Acceso a las credenciales, Usuario 6

28. Login o Acceso cuenta del usuario 6.

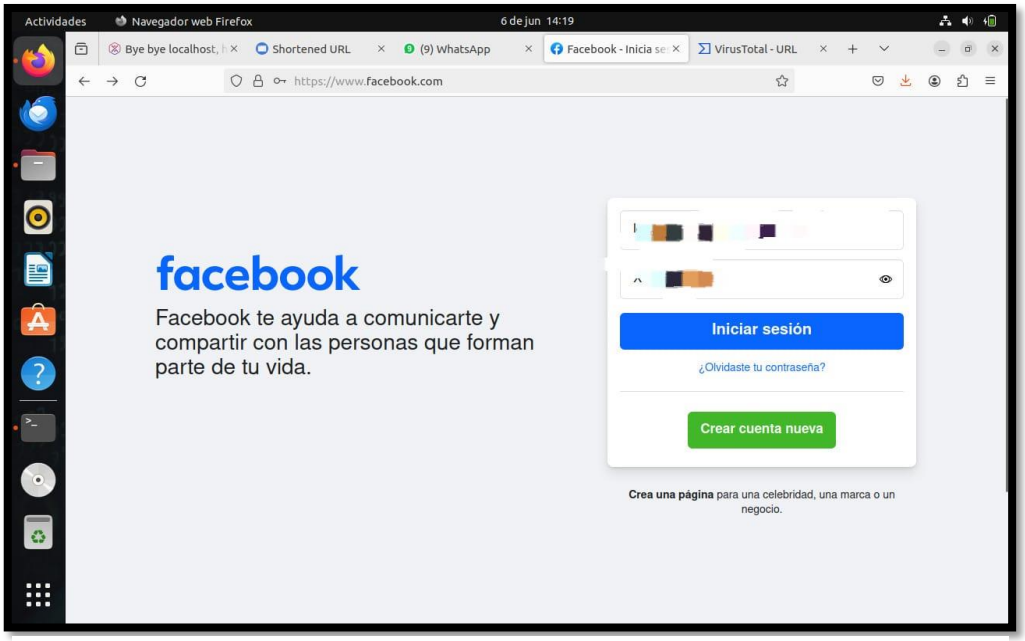

Imagen 29 Acceso no autorizado o acceso ilegitimo - Usuario 6

Manipulación Digital 7

29. Credenciales de usuario.

Imagen 30 Acceso a las credenciales, Usuario 7

30. Login o Acceso cuenta del usuario 7

Imagen 31 Acceso no autorizado o acceso ilegitimo - Usuario 7

Manipulación Digital Gmail.

31. Credenciales de usuario

Imagen 32: Credenciales Capturados – Usuario 8

32. Login de victima 8

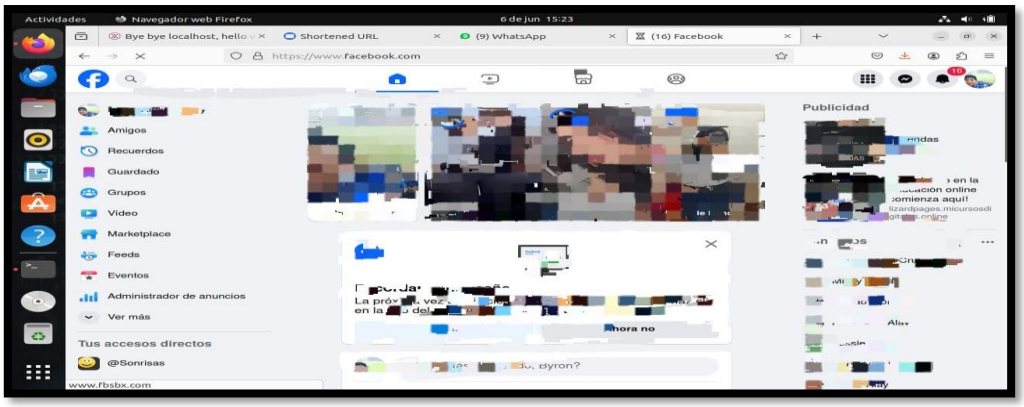

Imagen 33: Acceso no autorizado o acceso ilegitimo – Usuario 8

PLATAFORMA GMAIL

1. Comando bash Zphisher.sh para ejecutar el script

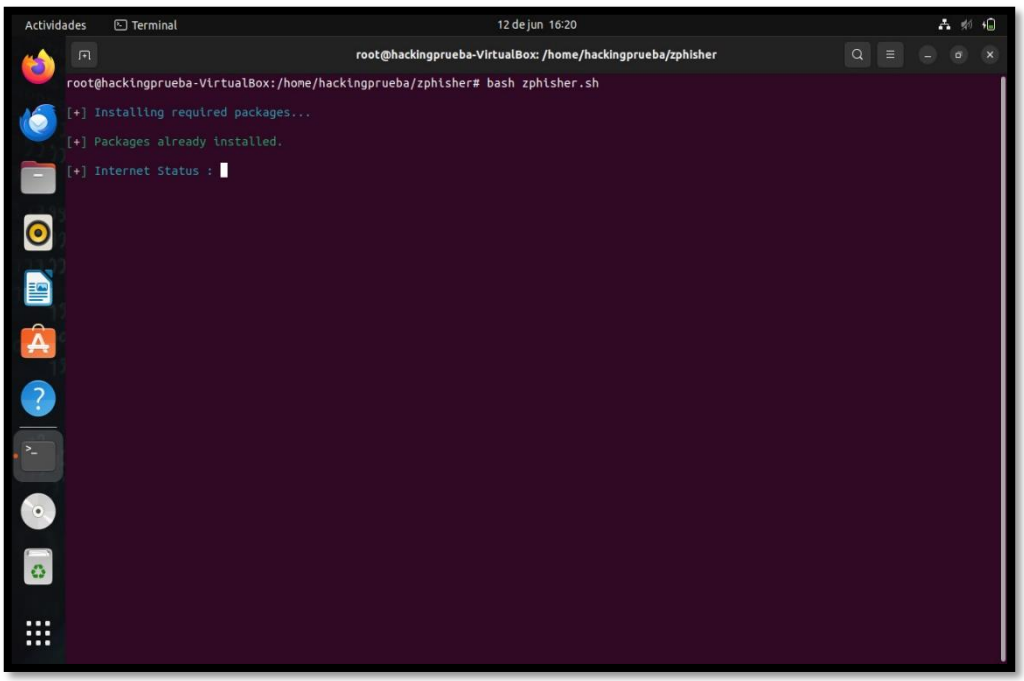

Imagen 34: Comando Bash zhpisher.sh para ejecutar con la plataforma GMAIL

2. Se ejecutó la herramienta Zphisher

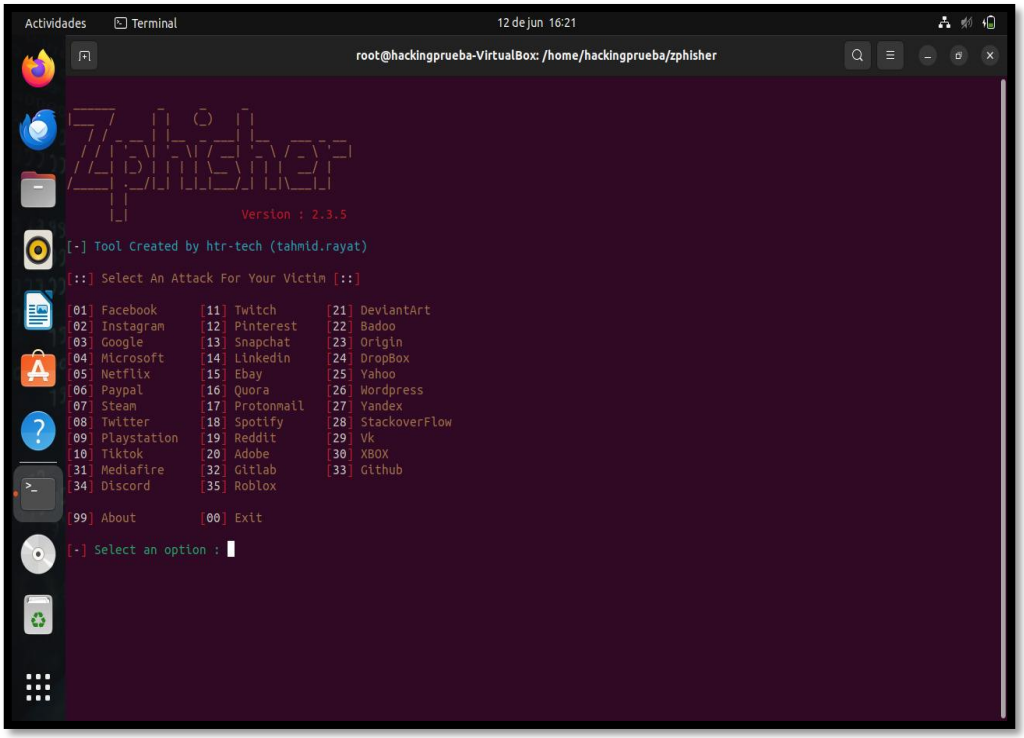

Imagen 35: Herramienta Zphisher – Inicio

3. Se selecciona la plantilla de Gmail Opcion 3

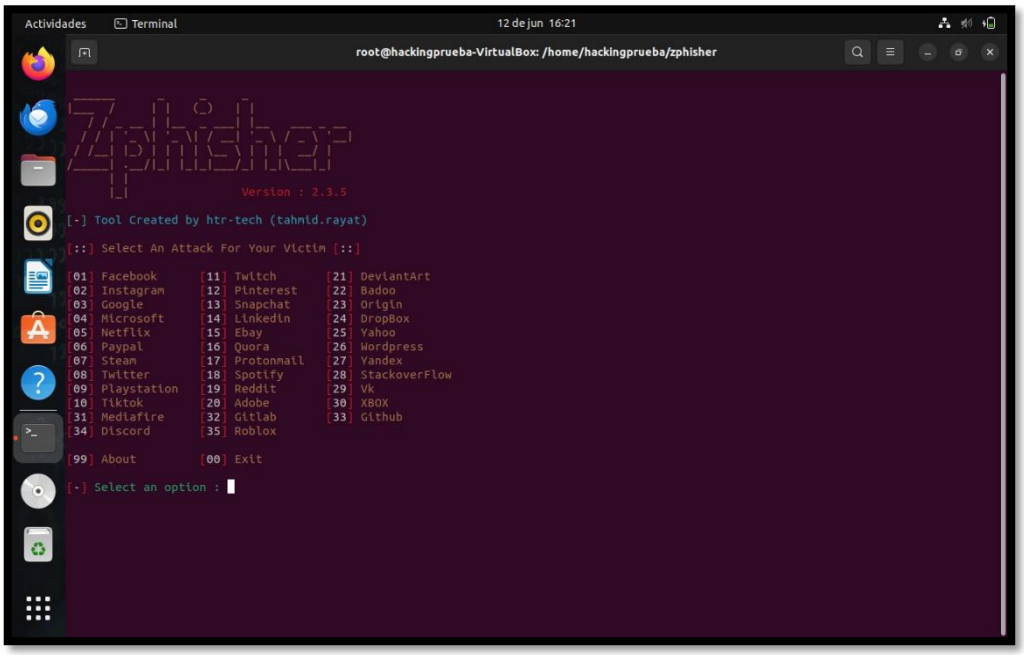

Imagen 36: Opción 3 – GMAIL

4. Se toma la opción 2 de la plantilla avanzada de Gmail

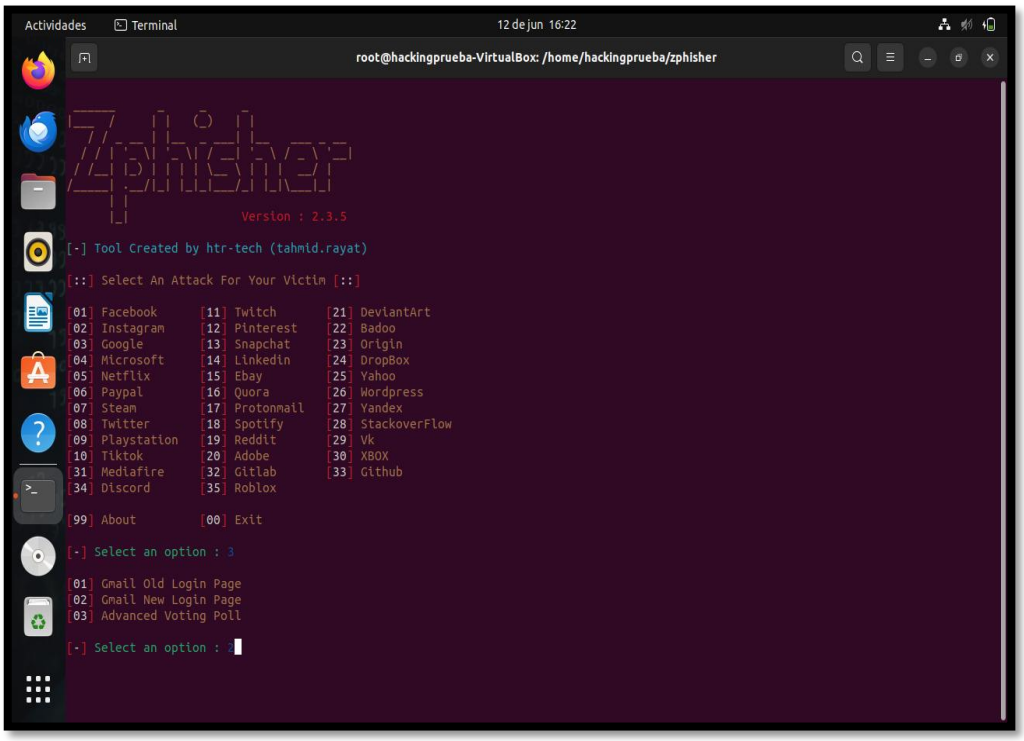

Imagen 37: Seleccionar 2 – Plantilla GMAIL

5. Seleccionar la opción LocalXpose

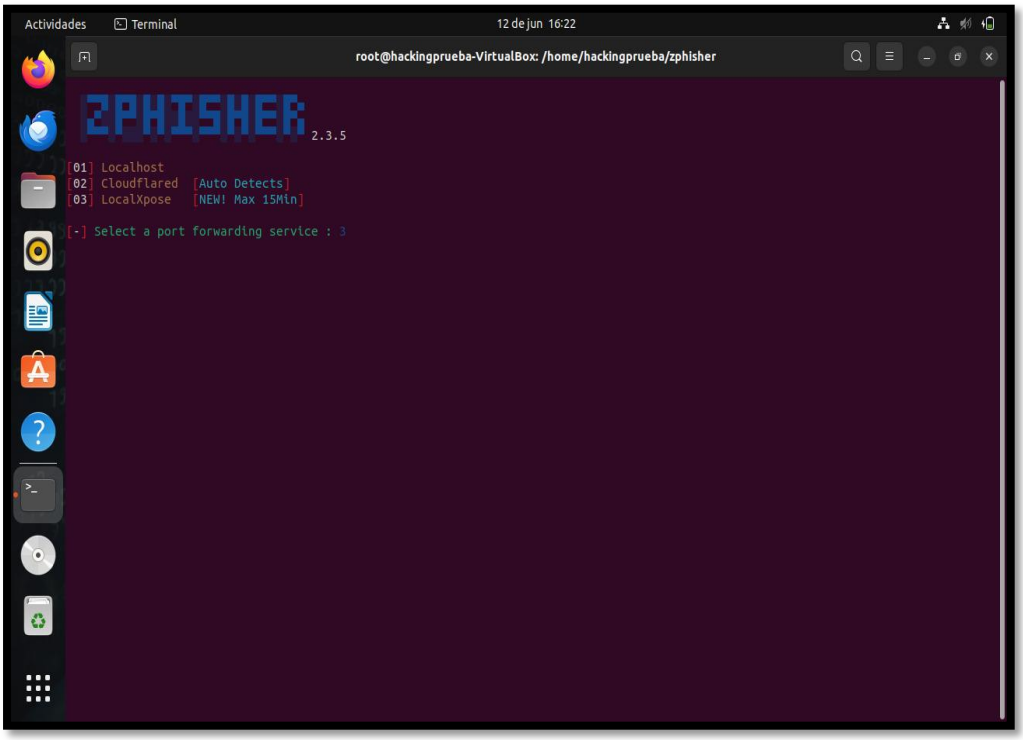

Imagen 38: Opción LocalXpose

6. Generar Link

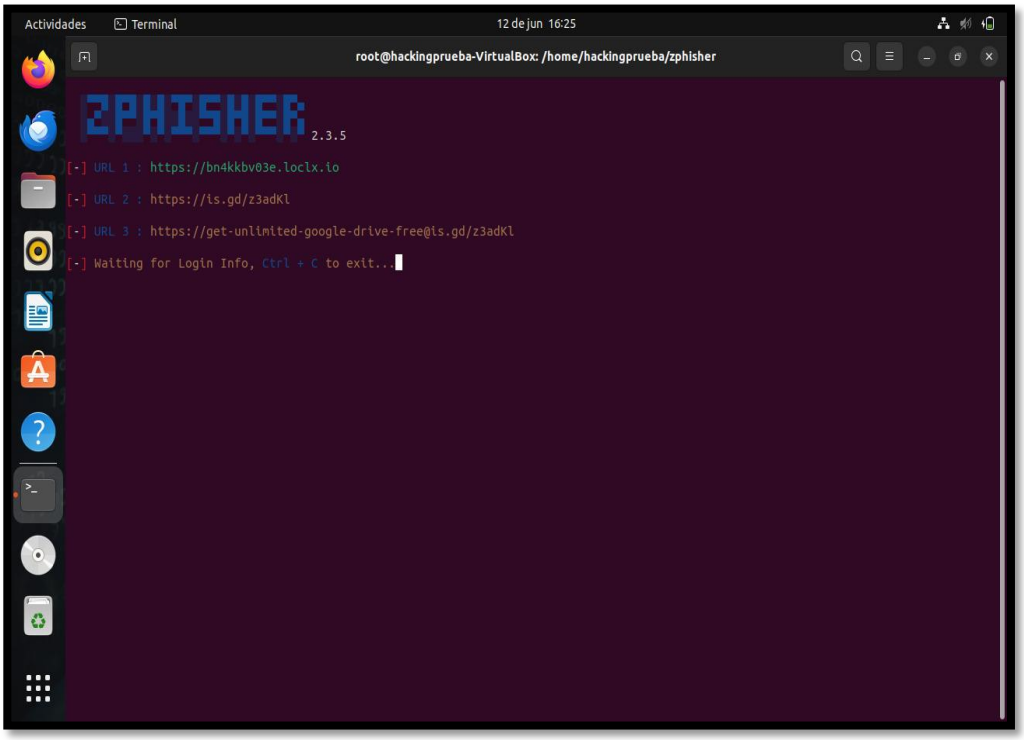

Imagen 39: Link Generado

7. Corta el link generado con short link

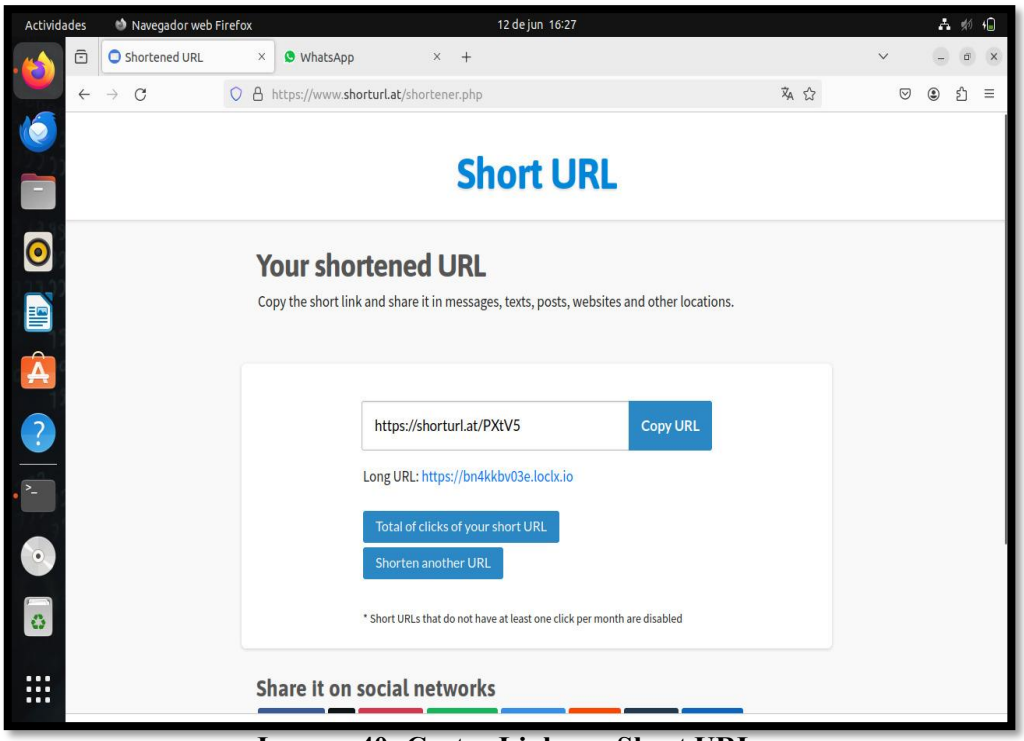

Imagen 40: Cortar Link por Short URL

8. Enviar link a las víctimas por WhatsApp

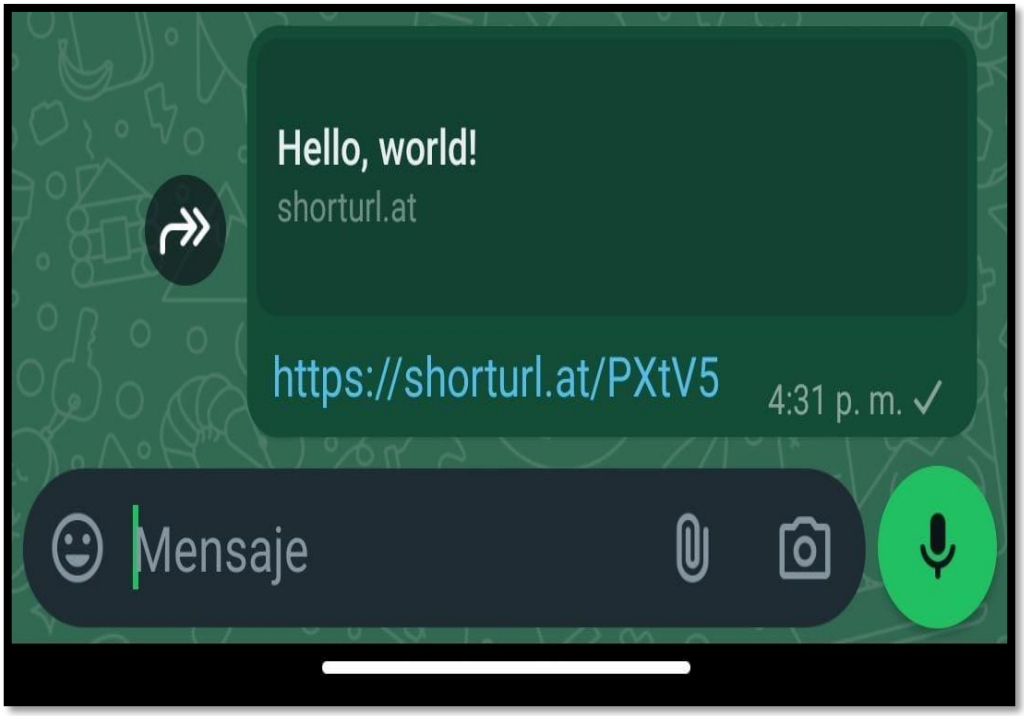

Imagen 41: Link enviado a las victimas

Manipulación Digital / GMAL -1

9. Credenciales de usuario

Imagen 42: Credenciales Capturados Usuario 1 - GMAIL

10. Login Victima 1

Imagen 43: Acceso no permitido GMAIL - Usuario 1

Manipulación Digital/GMAIL - 2

11. Credenciales de Usuario

Imagen 44: Credenciales Capturados Usuario 2 - GMAIL

12. Login Victima 2

Imagen 45: Acceso no permitido GMAIL - Usuario 2

Manipulación Digital/GMAIL - 3

13. Credenciales de Usuario

Imagen 46: Credenciales Capturados Usuario 3 - GMAIL

14. Login Victima 3

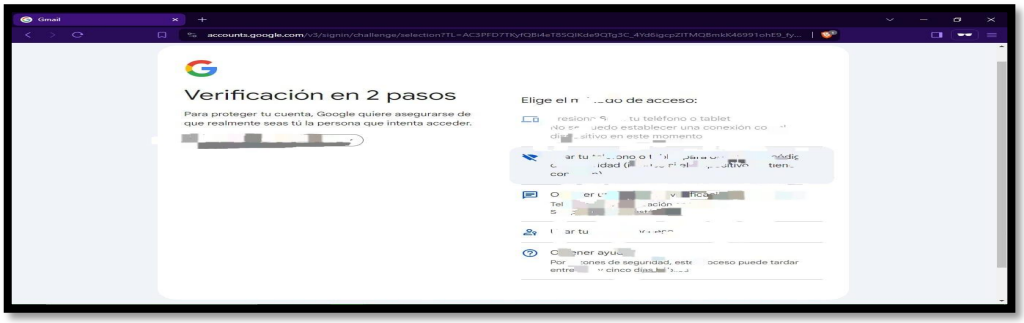

Imagen 47: Acceso no permitido GMAIL – Usuario 3

Victima Engaño - 4

15. Credenciales de Usuario

Imagen 48: Credenciales Capturados Usuario 4 - GMAIL

16. Login Victima 4

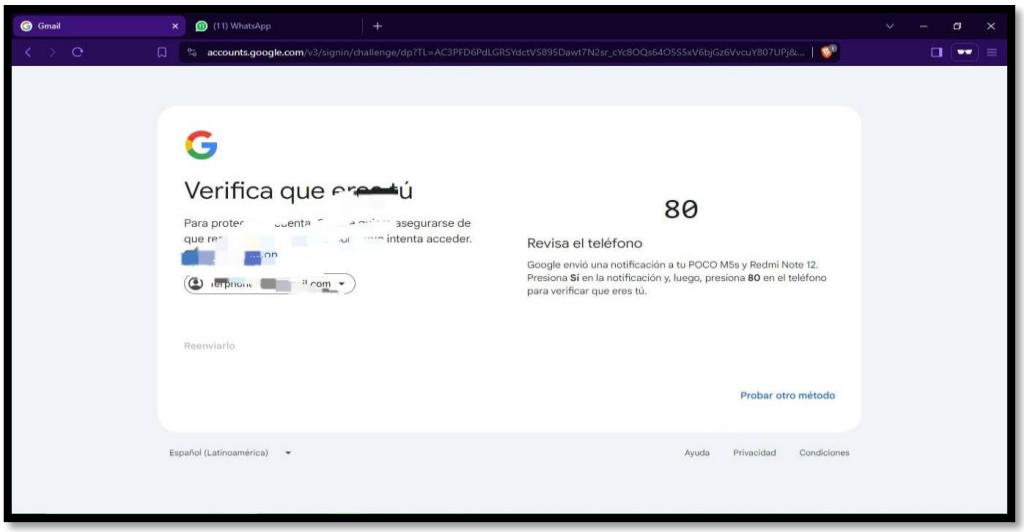

Imagen 49: Acceso no permitido GMAIL – Usuario 4

Manipulación Digital/GMAIL - 5

17. Credenciales de Usuario

Imagen 50: Credenciales Capturados Usuario 5 - GMAIL

18. Login Victima 5

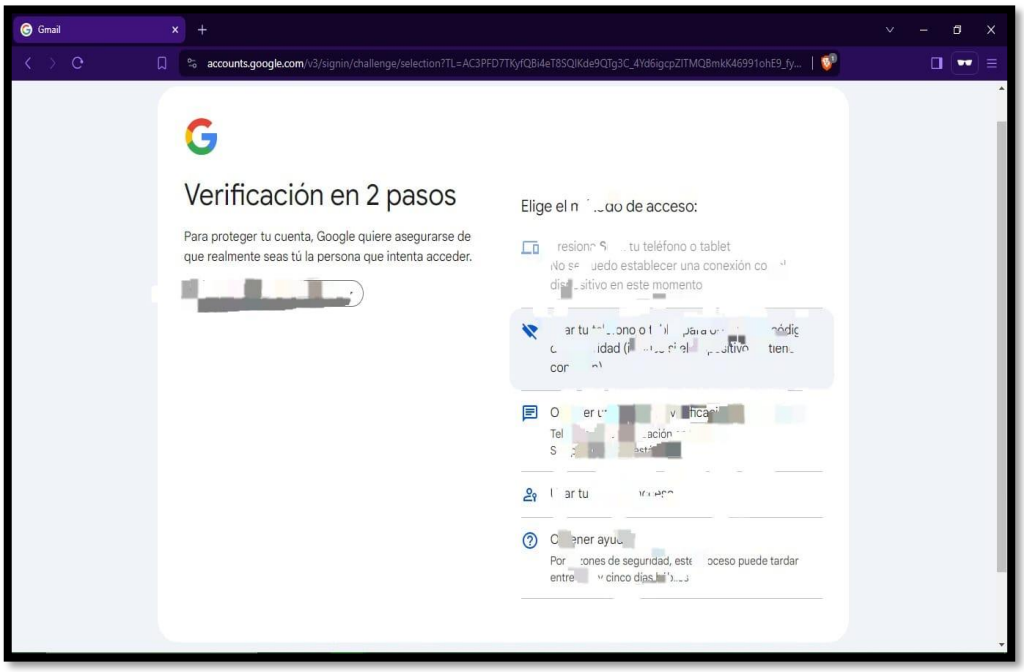

Imagen 51: Acceso no permitido GMAIL – Usuario 5

SPEAR – PHISHING

Herramientas: Proton Mail, Msfvenom, winrar, Abobe PDF , Net **Tiempo:** 30 minutos

Objetivo: Obtener privilegio de la maquina victima a través de un archivo ejectuable malicioso camuflado en pdf y observas configuraciones y archivos

1. Se ejecuta el siguiente comando para crear el payload malicioso desde la maquina Kali Linux con las configuraciones necesarias como la dirección de relación y el puerto de escucha

Imagen 52: Máquina Kali Iniciada

2. Se obtiene el formato del payload malicioso como PruebaIng.exe un ejecutable para máquina Windows

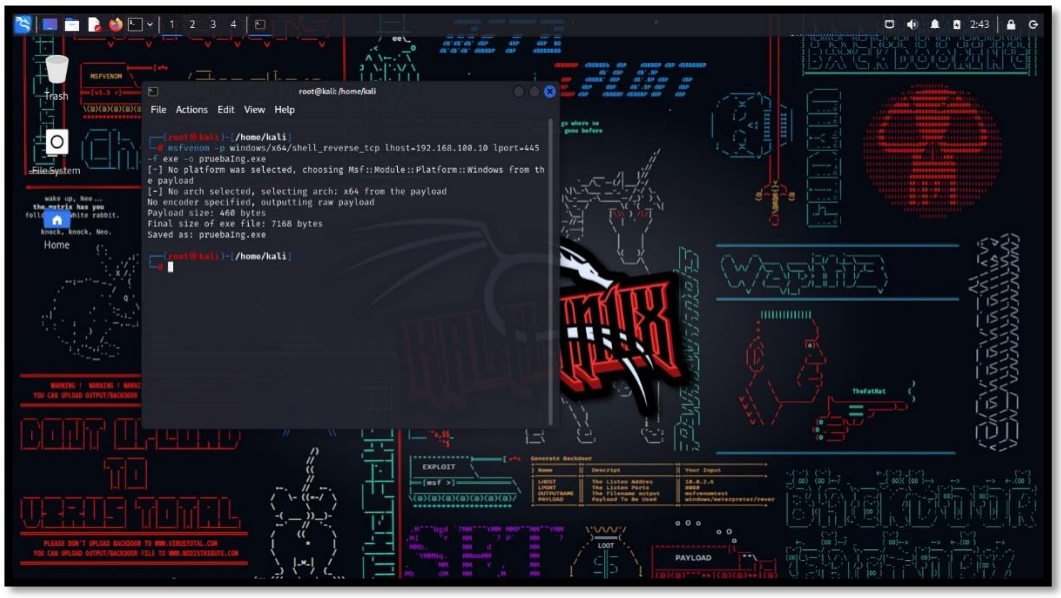

Imagen 53: Comando de creación de Payload para Windows

3. Seleccionar los archivos esenciales para la camuflar la carga útil maliciosa para la victima

Imagen 54: Archivos necesarios para camuflar el payload malicioso

4. Convertir la imagen del pdf en icono en el siguiente link

Imagen 55: Convertir la imagen pdf a icono

5. Seleccionar la imagen pdf a convertir

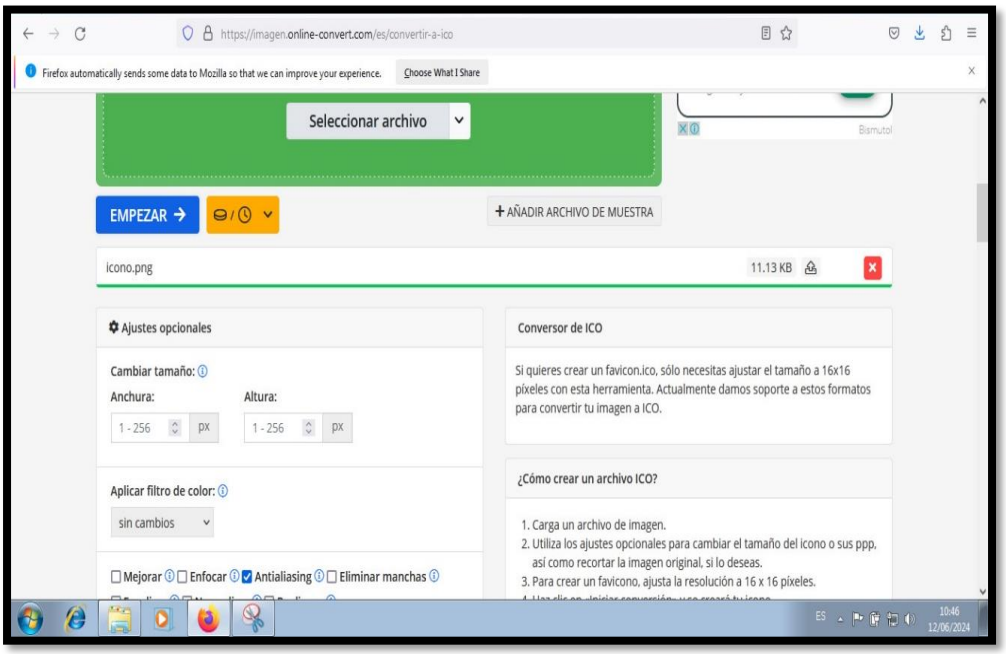

Imagen 56: Imagen cargada para convertir

6. Descargar el archivo final

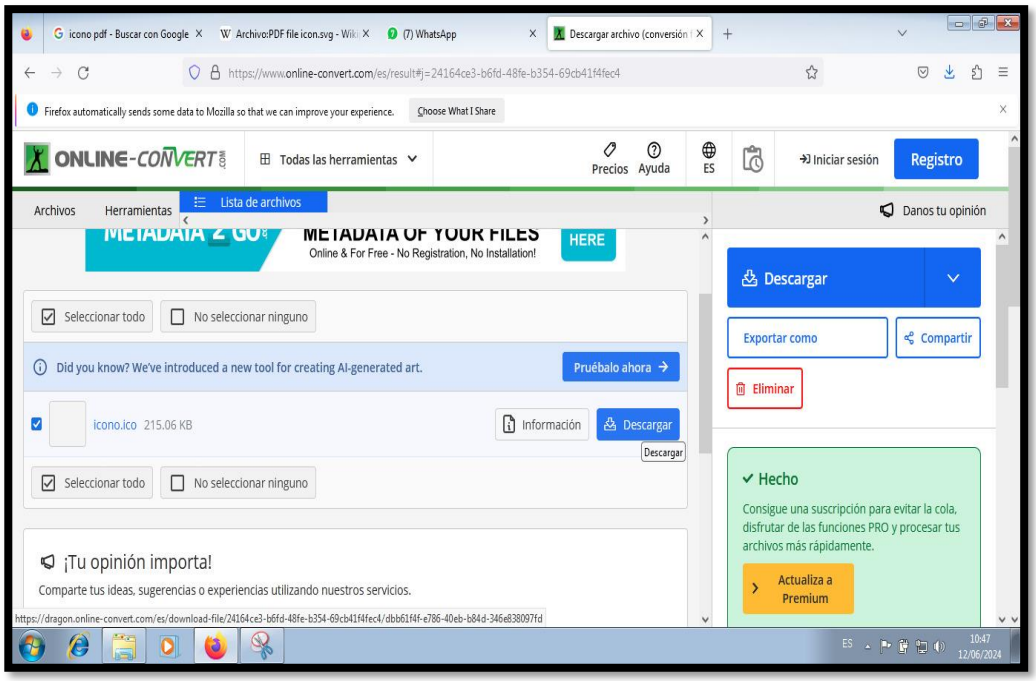

Imagen 57: Icono listo para descargar

7. Una vez teniendo todos los archivos necesarios para camuflar el payload/carga útil malicioso se comienza el proceso

Imagen 58: Archivos completos para el proceso de camuflaje del Payload

8. Seleccionar el archivo notas.pdf y el archivo ejecutable pruebaIng.exe para crear un nuevo archivo mediante la herramienta Winrar, dar clic en añadir archivo

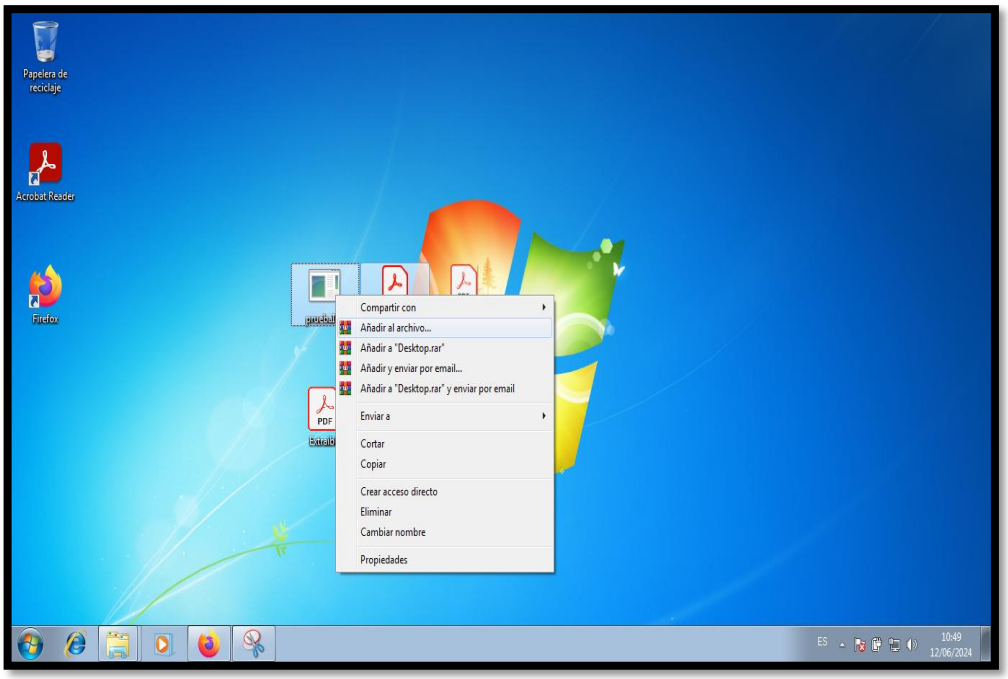

Imagen 59: Crear un nuevo archivo extraíble con el payload y el documento muestra

9. Configurar el archivo final por notasImportante.pdf, seleccionar la casilla de crear un archivo ejecutable, y en método de comprensión tener en la mejor. Como resultado se presenta notasImportantes.pdf.exe

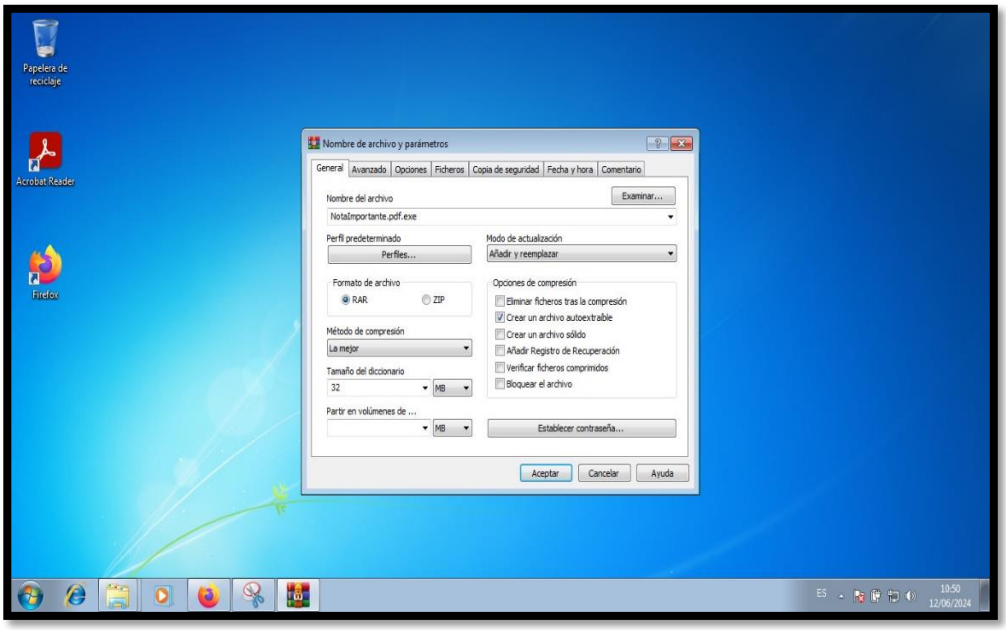

Imagen 60: Cambiar formato de salida a pdf.exe

10. En la sección avanzado dar clic en AutoExtraible

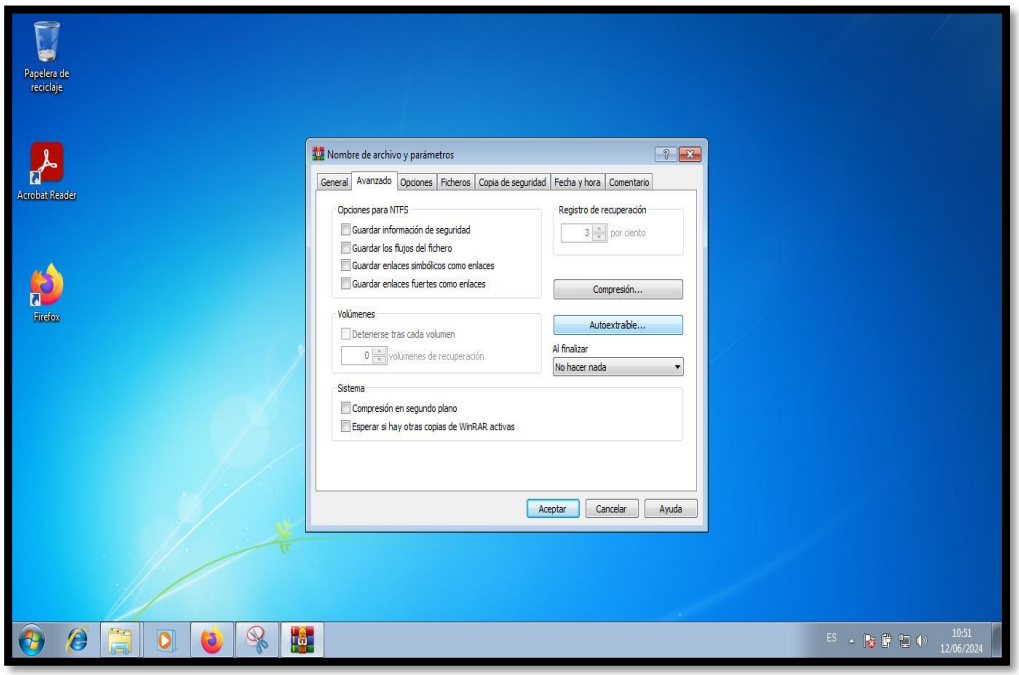

Imagen 61: Seleccionar AutoExtraible

11. Una vez en el apartado AutoExtraible, en la sección instalación se configura los archivos a combinar; primero va notas.pdf y luego va pruebaIng para que una vez se ingrese el archivo se ejecute de una vez el ejecutable igual

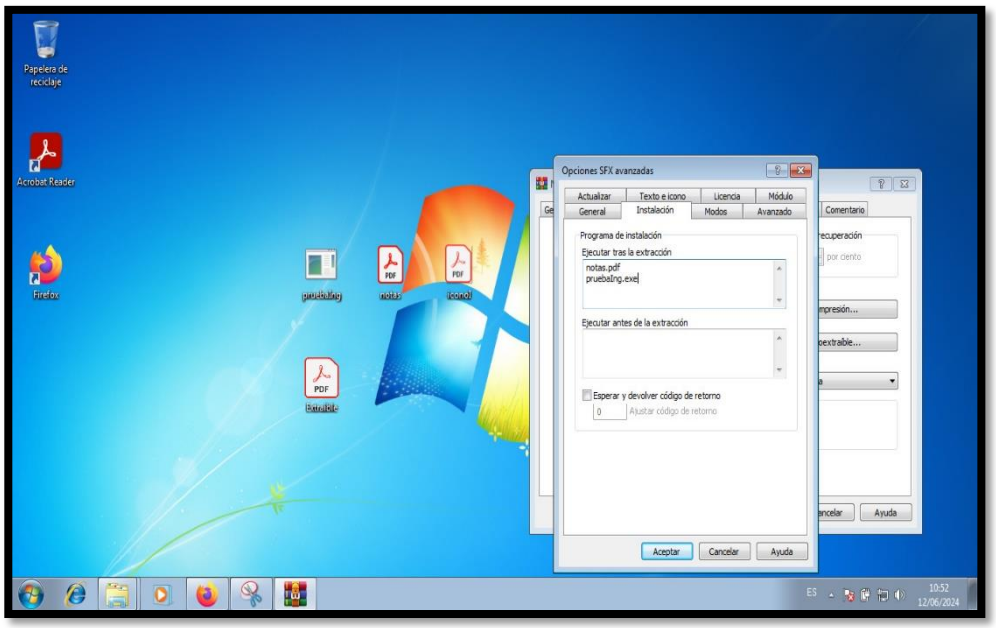

Imagen 62: Insertar el payload y el pdf en instalación

12. En la sección de texto e icono se carga el icono convertido de la imagen pdf

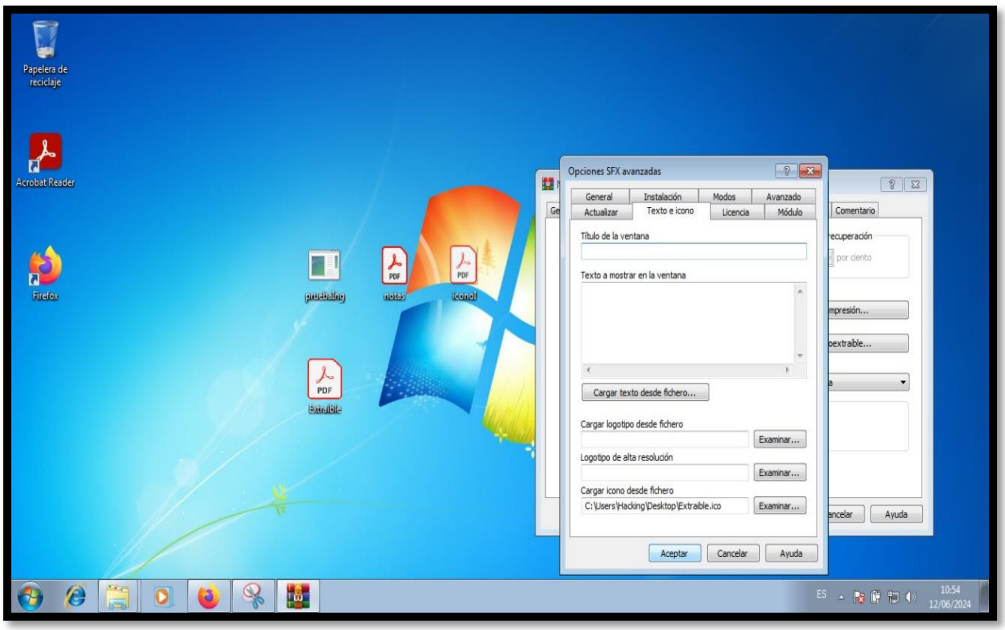

Imagen 63: Insertar el icono resultante en texto e icono

13. En la sección Actualizar, en la parte de modo actualización deja la casilla extraer y reemplazar fichero marcada, pero en modo sobreescritura, marca la parte de sobreescribir todos los ficheros con la finaliza que se ejerza la aceptación de cualquier proceso adicional como de instalación y no estar sobreescribiendo a cada rato. Sino a dar clic al archivo de uno se desarrolle el proceso y listo

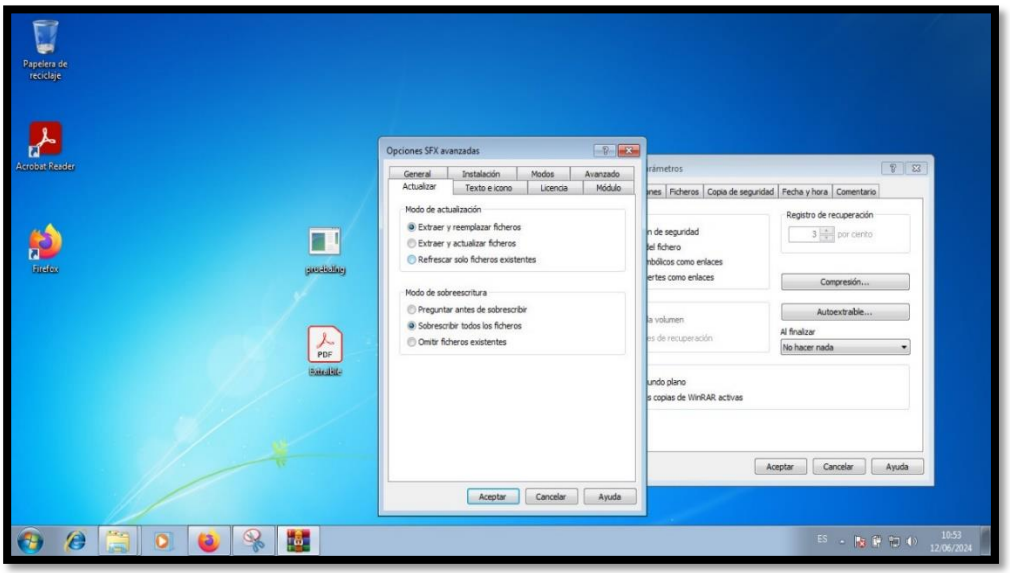

Imagen 64: En actualización dar en sobreescribir

14. Una vez finalizado la configuración correspondiente, se da en aceptar para finalización del archivo camuflado con el payload malicioso

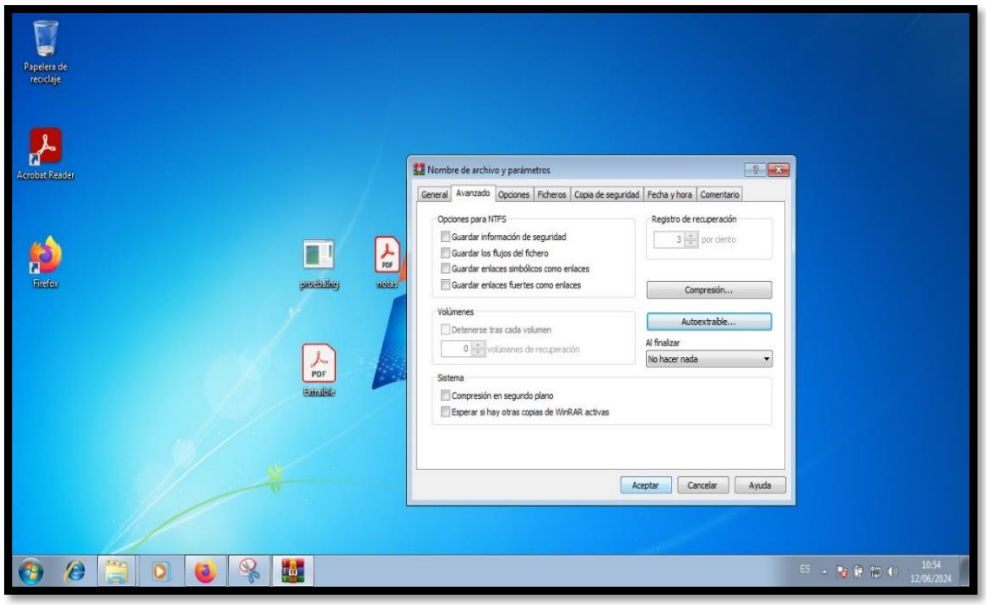

Imagen 65: Aceptar configuración y aceptar

15. Archivo Creado exitosamente

Imagen 66: Archivo final

16. Se sube el archivo en OneDrive para ejercer una ruta compartida para enviar a la víctima como link de descarga

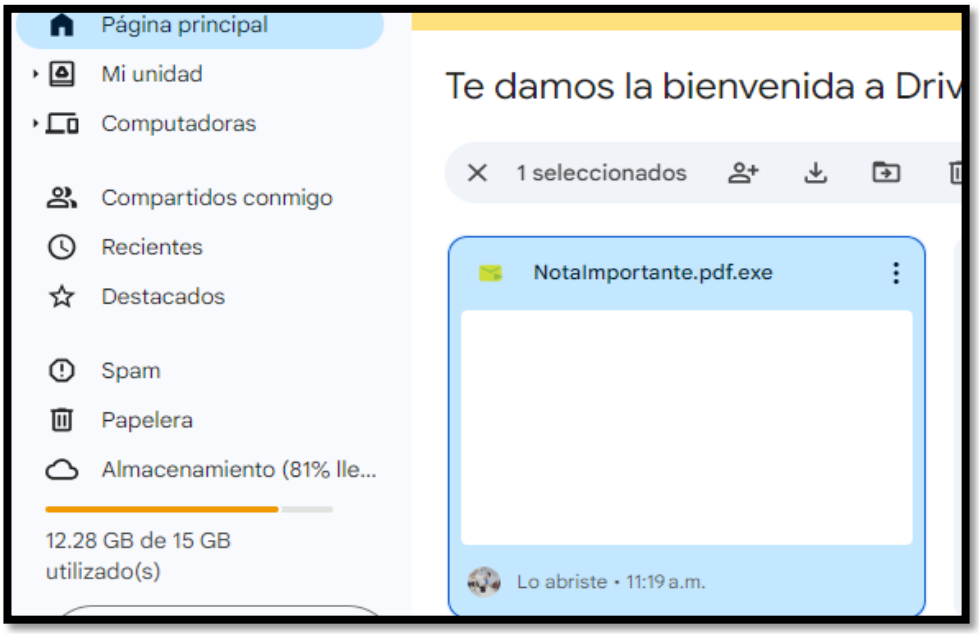

Imagen 67: Subir el archivo en Drive para crear link compartido

17. A través de la herramienta Proto Mail se envía el mensaje al correo victima con el siguiente formato de estructura de mensaje

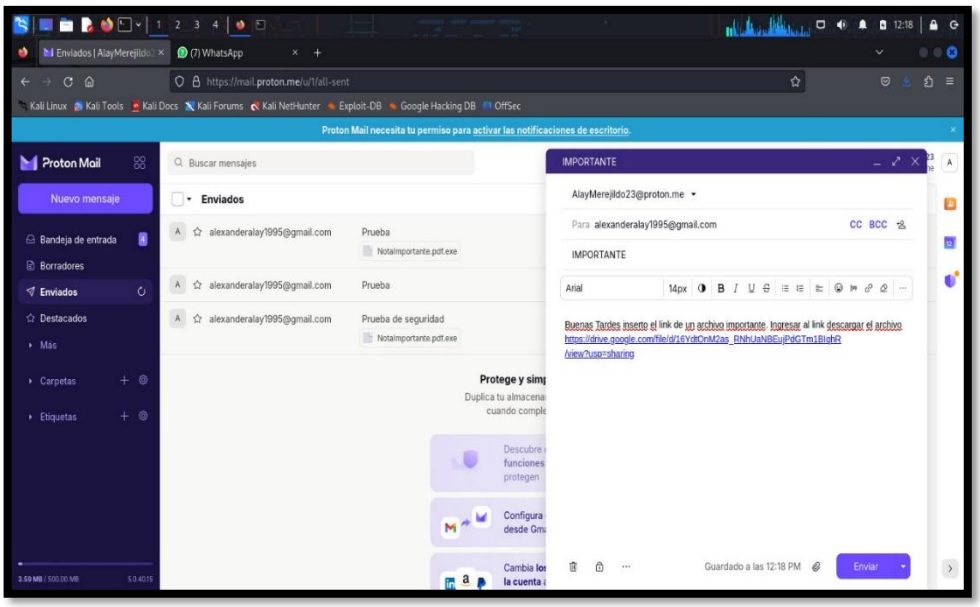

Imagen 68: Tecnología Proton MAIL – Enviar correo a diferentes SMTP

18. Mensaje enviado a la víctima y receptado

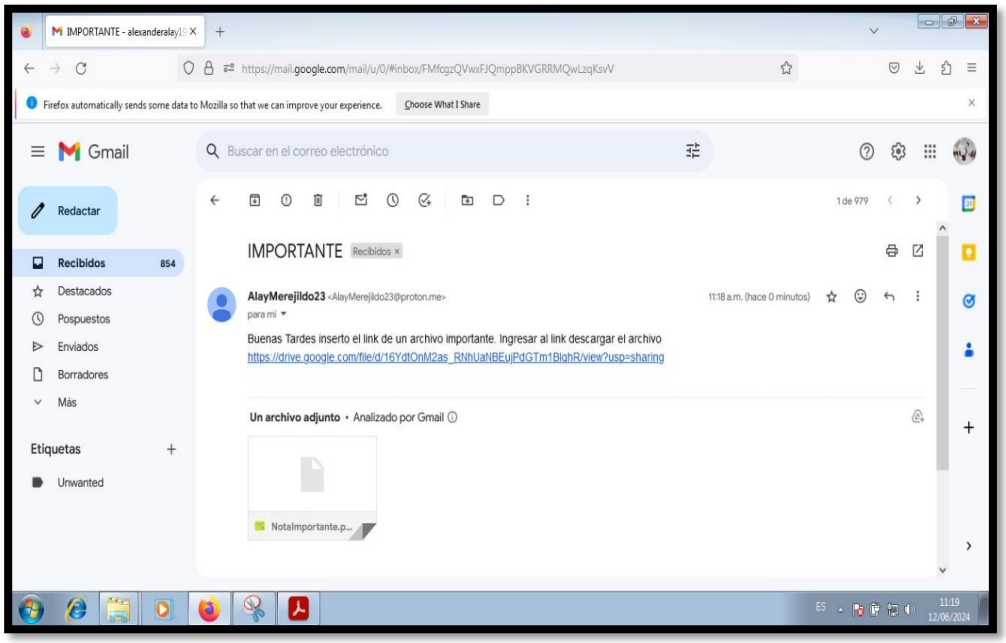

Imagen 69: Correo recibido a la victima

19. La victima da clic en el enlace compartido y le direcciona para descargar el archivo

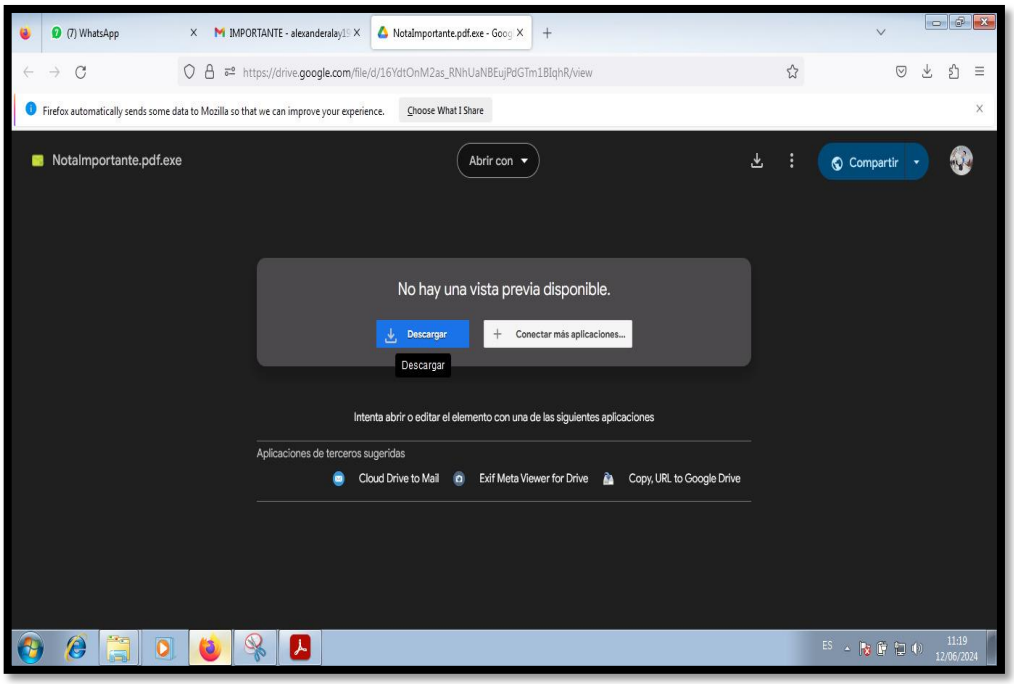

Imagen 70: La victima ingresa – Descargar

20. Se pasa el ultimo filtro para descargar de todos modos, y el archivo se descarga

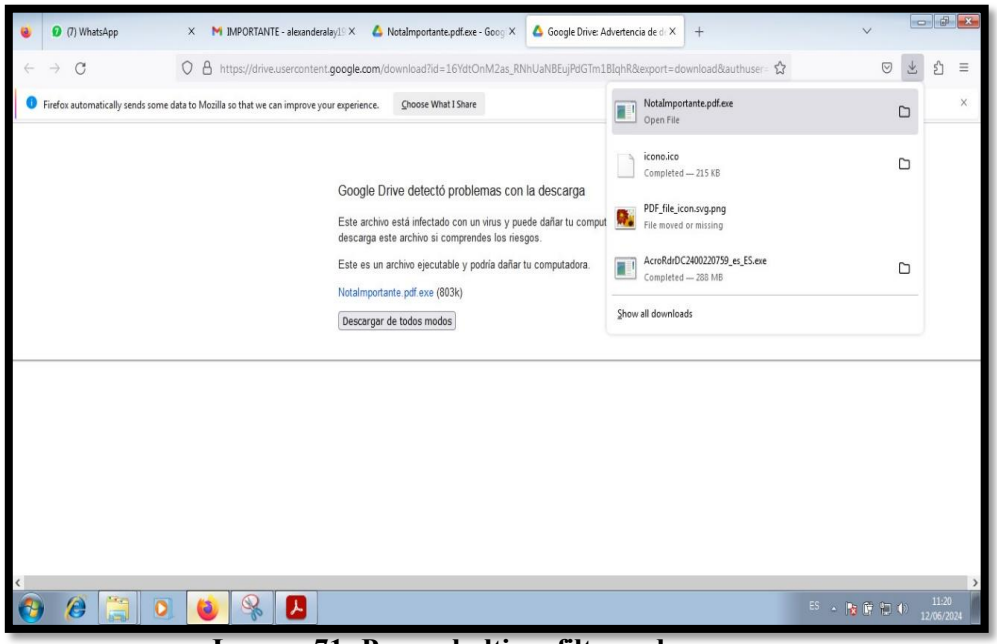

Imagen 71: Pasar el ultimo filtro y descargar

21. Se presenta en la carpeta el archivo descargado para ser ejecutado

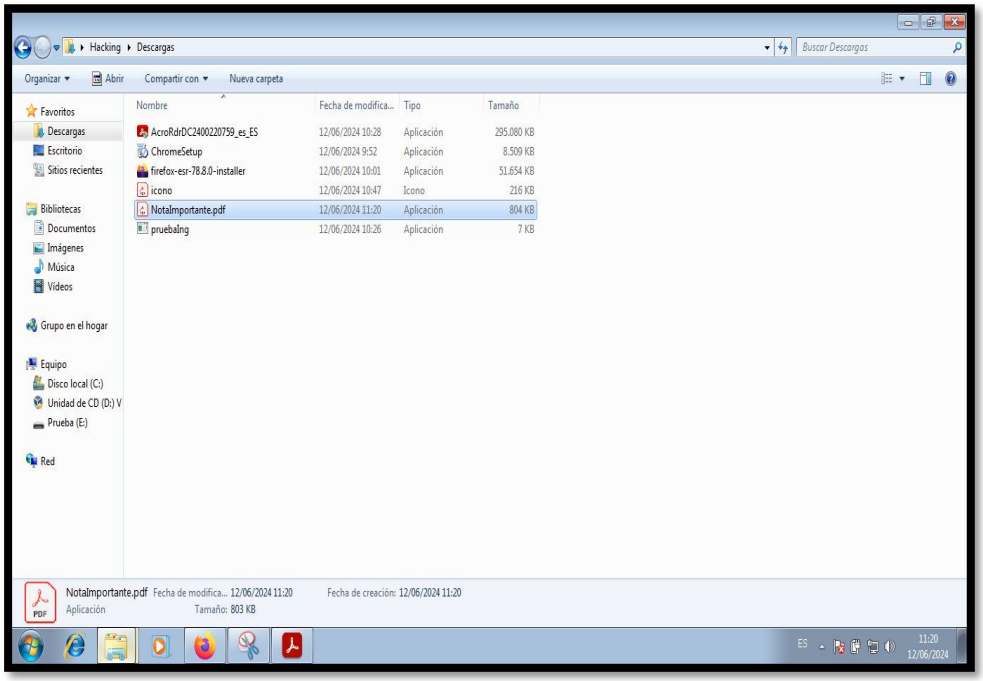

Imagen 72: Archivo descargado en el panel de descarga de la máquina victima

22. Se presenta un mensaje de instalación en dependencia a la ruta de ejecución

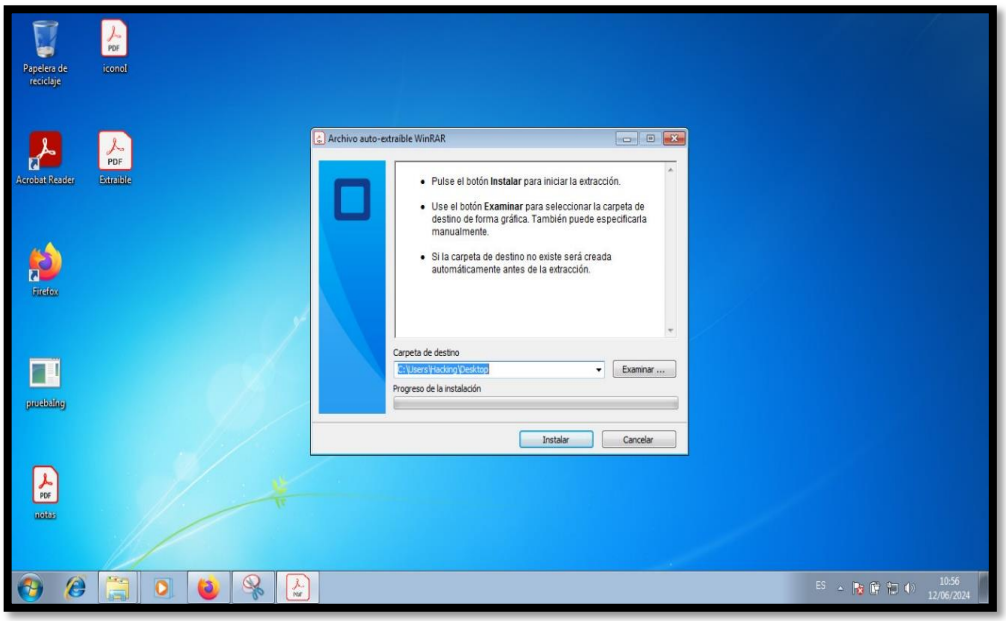

Imagen 73: Dar en Instalar

23. Pdf ejecutado correctamente

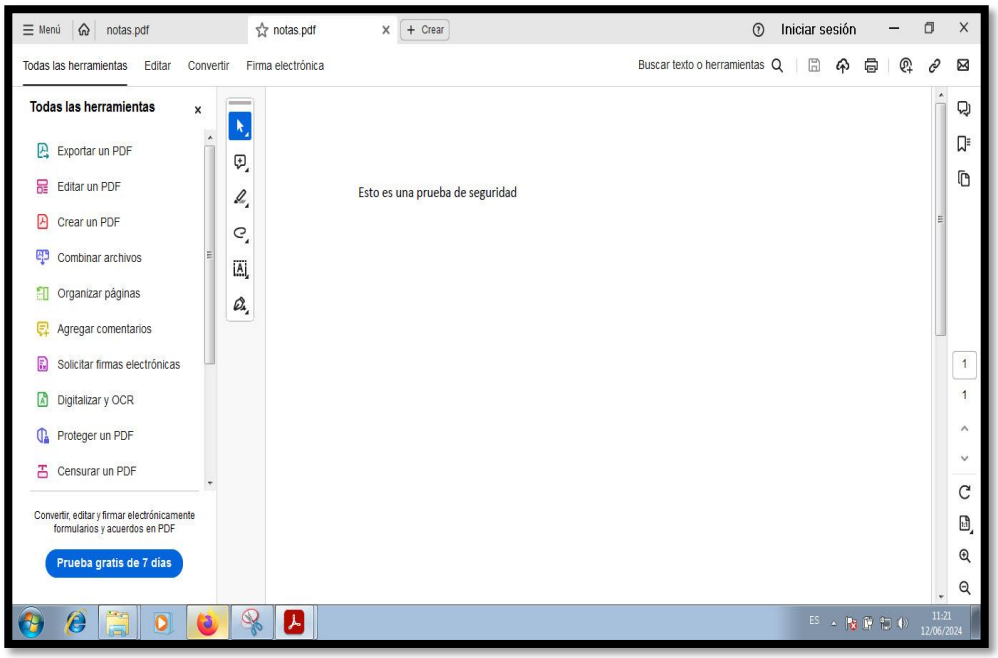

Imagen 74: Pdf Ejecutado exitosamente

24. En la maquina atacante se logra la conexión retoma a través del puerto de escucha configurado Port 445

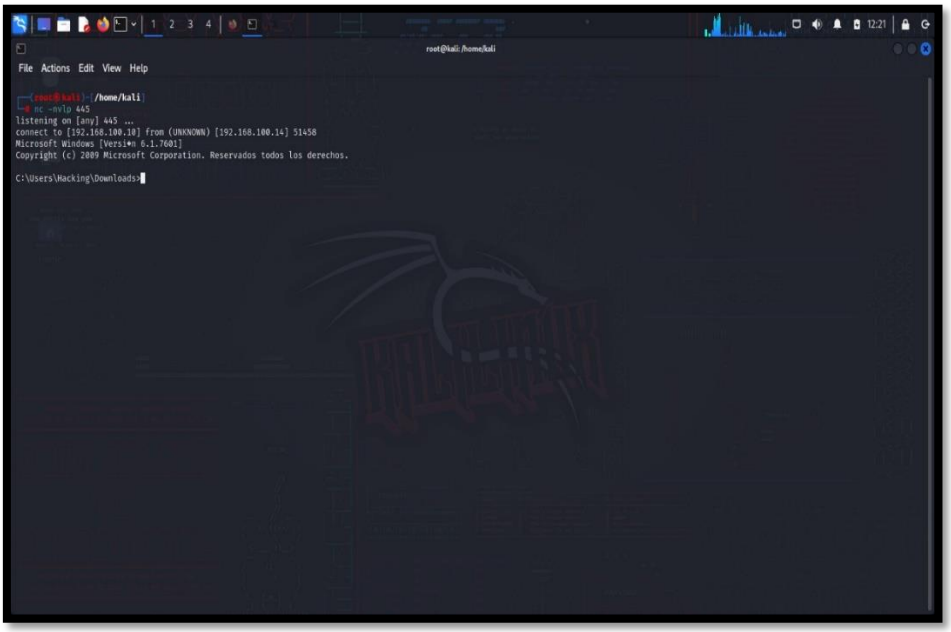

Imagen 75: Comando de esccuha en máquina Kali

25. Lista de archivos en la carpeta Downloands y borrar un archivo con el comando del

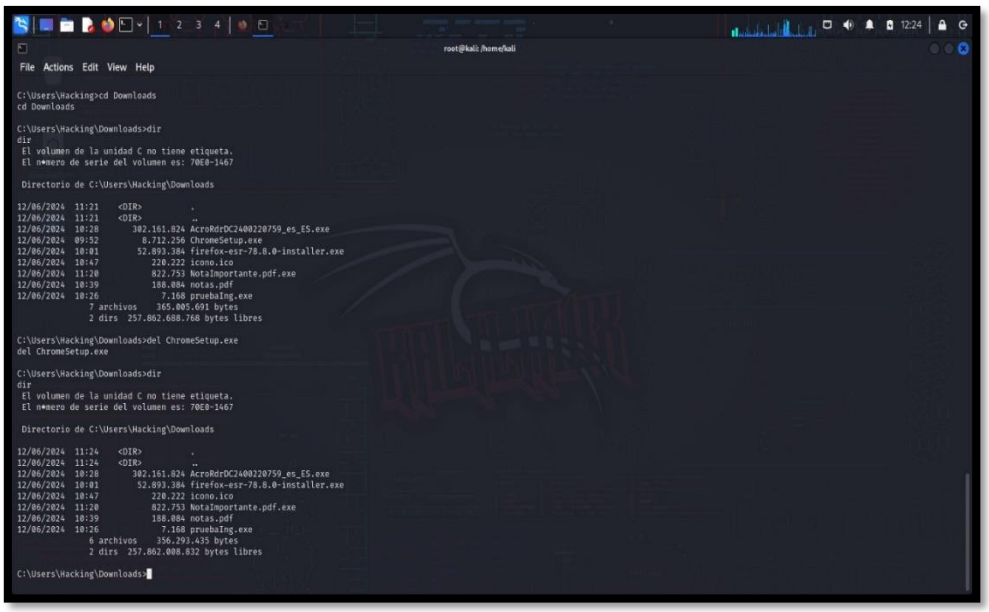

Imagen 76: Elevación de privilegio de la máquina victima

26. Con el comando more visualizar información de archivos como contra.txt

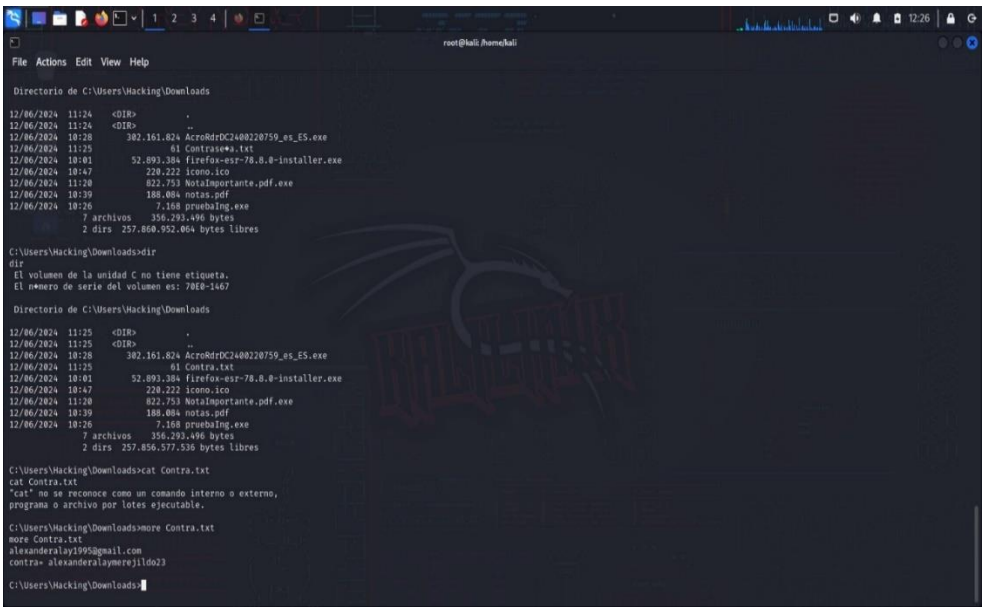

Imagen 77: Comando More para visualizar formato en específico .txt

27. Con el comando ser permite ver todas las variables de entorno de la sesión actual

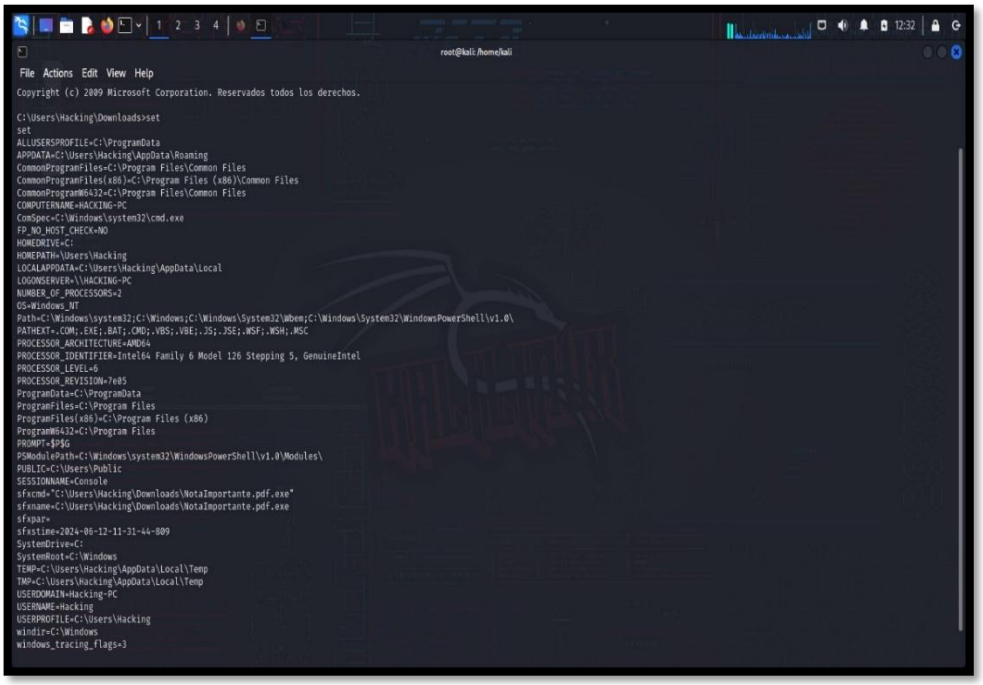

Imagen 78: Resultados del comando

28. El comando net user permite ver toda la información del usuario actual

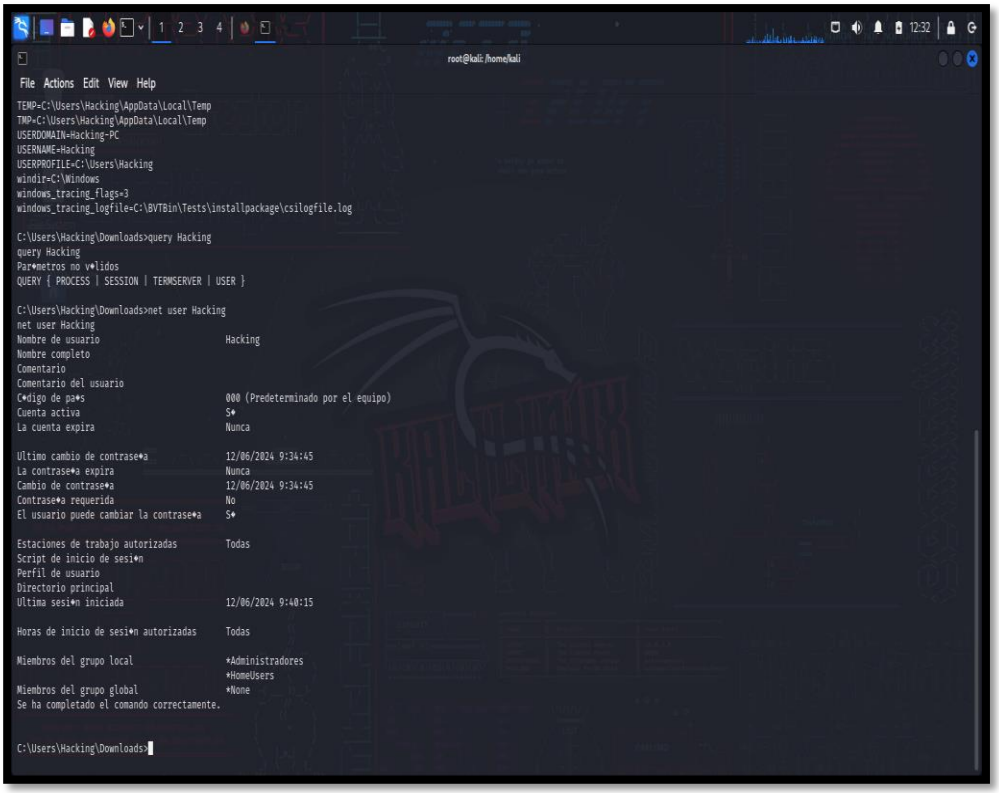

Imagen 79: Resultados del comando- net user

ANEXO MANUAL

MANUAL TÉCNICO DE APLICACIÓN DE MEDIDAS DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE DATOS PERSONALES

Introducción

La protección de datos personales es esencial en el entorno digital actual. Los ataques de ingeniería social, como phishing, spear-phishing y vishing, representan amenazas significativas para la seguridad de la información. Este manual técnico proporciona una guía detallada para implementar medidas de seguridad informática destinadas a proteger los datos personales frente a estos tipos de ataques.

1. Conceptos Fundamentales

1.1 Datos Personales

Información que permite la identificación directa o indirecta de una persona física, como nombre, dirección, número de teléfono, correo electrónico, entre otros.

1.2 Ingeniería Social

Técnica de manipulación psicológica utilizada por atacantes para obtener información confidencial mediante el engaño.

2. Tipos de Ataques de Ingeniería Social

2.1 Phishing

Método de fraude mediante el envío de correos electrónicos que parecen provenir de fuentes confiables, con el objetivo de que los destinatarios revelen información personal o financiera.

2.2 Spear-Phishing

Variante del phishing donde los correos electrónicos están altamente personalizados y dirigidos a individuos específicos dentro de una organización.

2.3 Vishing

Uso de llamadas telefónicas fraudulentas para engañar a otros y obtener información confidencial.

3. Medidas de Seguridad Informática

3.1 Concienciación y Capacitación

- **Programa de Capacitación Continua**: Implementar programas de capacitación periódica para empleados sobre la identificación de correos electrónicos sospechosos y llamadas telefónicas fraudulentas.
- **Simulaciones de Ataques**: Realizar simulaciones regulares de phishing y vishing para evaluar la capacidad de respuesta de los empleados.

3.2 Implementación de Tecnologías de Seguridad

- **Filtros de Correo Electrónico**: Configurar y mantener filtros avanzados de correo electrónico que detecten y bloqueen mensajes de phishing. Utilizar soluciones de filtrado como SPF, DKIM y DMARC.
- **Autenticación Multifactor (MFA)**: Implementar MFA para el acceso a sistemas y datos sensibles, utilizando aplicaciones de autenticación, tokens de hardware o biometría.
- **Software de Seguridad**: Mantener actualizados los sistemas de antivirus, antimalware y firewalls. Utilizar EDR (Endpoint Detection and Response) para una mayor protección.

3.3 Políticas de Seguridad

- **Política de Gestión de Contraseñas**: Establecer políticas de contraseñas robustas que incluyan requisitos de longitud, complejidad, y cambios periódicos. Implementar herramientas de gestión de contraseñas.
- **Política de Uso Aceptable**: Definir y comunicar claramente las políticas de uso aceptable de recursos tecnológicos dentro de la organización, incluyendo el acceso a redes, dispositivos y aplicaciones.

3.4 Procedimientos de Respuesta a Incidentes

- **Equipo de Respuesta a Incidentes**: Formar un equipo especializado en la respuesta a incidentes de seguridad informática, compuesto por expertos en TI, legales y de comunicación.
- **Plan de Respuesta a Incidentes**: Desarrollar y mantener un plan detallado para responder rápidamente a los incidentes de seguridad, incluyendo procedimientos de contención, erradicación y recuperación.

4. Proceso de Evaluación de Riesgos

4.1 Identificación de Activos y Vulnerabilidades

- **Inventario de Activos**: Crear y mantener un inventario detallado de todos los activos de información, clasificándolos por niveles de sensibilidad y criticidad.
- **Evaluación de Vulnerabilidades**: Realizar evaluaciones regulares de vulnerabilidades utilizando herramientas automatizadas de escaneo y pruebas de penetración.

5 4.2 Análisis de Impacto

- **Evaluación del Impacto en la Privacidad (PIA)**: Realizar PIAs para evaluar el impacto potencial de las brechas de seguridad en la privacidad de los datos personales. Utilizar metodologías estándar como ISO/IEC 29134.

6 4.3 Mitigación de Riesgos

- **Implementación de Controles de Seguridad**: Basado en los resultados del análisis de impacto, implementar controles de seguridad adecuados para mitigar los riesgos identificados, siguiendo marcos de referencia como ISO/IEC 27001 y NIST.

5. Recomendaciones para los Usuarios

5.1 Prácticas de Seguridad Personal

Verificación de Fuentes: Verificar la autenticidad de los correos electrónicos y llamadas telefónicas antes de proporcionar información personal. Utilizar mecanismos como la verificación de remitentes y la autenticación de llamadas.

Uso de Contraseñas Seguras: Utilizar contraseñas fuertes y únicas para diferentes cuentas. Implementar el uso de gestores de contraseñas.

Actualización de Software: Mantener todos los dispositivos y software actualizados con los últimos parches de seguridad, siguiendo un ciclo regular de gestión de parches.

Uso de Autenticación Multifactor (MFA): Habilitar la autenticación multifactor en todas las cuentas críticas para añadir una capa adicional de seguridad. Esto incluye el uso de métodos como códigos enviados a través de SMS o aplicaciones de autenticación.

Cuidado con los Enlaces y Archivos Adjuntos: Evitar hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos o mensajes no solicitados. Utilizar herramientas de análisis de enlaces para verificar su seguridad antes de interactuar con ellos.

Educación Continua: Participar en programas de capacitación y mantenerse informado sobre las últimas amenazas de seguridad cibernética. La educación es clave para reconocer tácticas de ingeniería social y otros métodos de ataque.

Desconexión de Redes Públicas: Evitar acceder a información sensible o realizar transacciones financieras en redes Wi-Fi públicas. Si es necesario, usar una red privada virtual (VPN) para asegurar la conexión.

Monitoreo Regular de Cuentas: Revisar periódicamente las actividades de las cuentas en línea para detectar cualquier actividad sospechosa. Configurar alertas automáticas para recibir notificaciones sobre intentos de acceso no autorizados.

Copia de Seguridad de Datos: Realizar copias de seguridad regulares de datos importantes en un medio seguro y desconectado de la red principal para evitar la pérdida de información en caso de incidentes de seguridad.

Gestión de Permisos y Accesos: Limitar los permisos de acceso a la información sensible solo a aquellos usuarios que lo necesiten para su trabajo. Revisar y actualizar los permisos de manera periódica.

Cierre de Sesiones: Asegurarse de cerrar sesión en todas las cuentas y aplicaciones cuando ya no se necesiten, especialmente en dispositivos compartidos o públicos.

5.2 Reporte de Incidentes

- **Procedimiento de Reporte**: Establecer un procedimiento claro y eficiente para reportar posibles incidentes de phishing, spear-phishing o vishing a los responsables de seguridad de la organización, utilizando canales de comunicación seguros y monitorizados.