UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS Y SIMULACIÓN DE ATAQUE DE MALWARE CON EL USO DE LA HERRAMIENTA COBALT STRIKE PARA LA EMPRESA PC SOLUCIONES

ESTUDIANTE:

ENZO ALDAHIR TAMAQUIZA MURILLO

TUTOR:

ING. JOSÉ DANILO VILLARES PAZMIÑO, MG.

AÑO 2023

INDICE

RESUMEN

El propósito de este caso de estudio es simular un ataque informático a través de con el uso de la herramienta Cobalt Strike sobre el sistema testeo Kali Linux y, establecer los procedimientos que se pueden implementar para detectar que se continúa atacando a los sistemas y así evitar que esto suceda. es decir, para mantener la estabilidad del sistema, por tanto, se realizarán pruebas para tomar las acciones oportunas que se puedan realizar, evitando así posibles ataques informáticos y contrarrestando posibles y futuras amenazas.

Con esta simulación como ejemplo, se identificarán las formas en que la información de la empresa puede protegerse desde los servidores domésticos hasta los servidores organizacionales, evitando y reduciendo las altas tasas de delitos informáticos.

El propósito de este caso de estudio es simular un ataque informático a través de con el uso de la herramienta Cobalt Strike sobre el sistema testeo Kali Linux y, establecer los procedimientos que se pueden implementar para detectar que se continúa atacando a los sistemas y así evitar que esto suceda. es decir, para mantener la estabilidad del sistema, por tanto, se realizarán pruebas para tomar las acciones oportunas que se puedan realizar, evitando así posibles ataques informáticos y contrarrestando posibles y futuras amenazas.

Con esta simulación como ejemplo, se identificarán las formas en que la información de la empresa puede protegerse desde los servidores domésticos hasta los servidores organizacionales, evitando y reduciendo las altas tasas de delitos informáticos.

En conclusión, se pudo identificar la importancia de utilizar herramientas de Hacking Ético para mejorar la seguridad de la red empresarial y prevenir posibles ataques.

Palabras claves: Simulación, Ciberseguridad, vulnerabilidades.

ABSTRACT

The purpose of this case study is to simulate a computer attack through the use of the Cobalt Strike tool on the Kali Linux testing system and, establish the procedures that can be implemented to detect that the systems continue to be attacked and thus prevent this from happening. i.e., to maintain system stability, therefore, tests will be performed to take the appropriate actions that can be performed, thus avoiding possible computer attacks, and counteracting possible and future threats.

With this simulation as an example, ways in which the company's information can be protected from home servers to organizational servers will be identified, avoiding, and reducing the high rates of computer crimes.

The purpose of this case study is to simulate a computer attack through the use of the Cobalt Strike tool on the Kali Linux testing system and, establish the procedures that can be implemented to detect that the systems continue to be attacked and thus prevent this from happening. i.e., to maintain system stability, therefore, tests will be performed to take the appropriate actions that can be performed, thus avoiding possible computer attacks and counteracting possible and future threats.

With this simulation as an example, ways in which the company's information can be protected from home servers to organizational servers will be identified, avoiding and reducing the high rates of computer crimes.

In conclusion, it was possible to identify the importance of using Ethical Hacking tools to improve the security of the business network and prevent possible attacks.

Key words: Simulation, Cybersecurity, vulnerabilities.

PLANTEAMIENTO DEL PROBLEMA

"PC soluciones" es un local sencillo que actualmente se encuentra en etapa de desarrollo y crecimiento comercial, la cantidad de clientes va en aumento, se sabe que ningún sistema es totalmente seguro, "PC soluciones" se preocupa por la integridad de sus clientes por lo cual se emplea medidas de seguridad de la información, como el cifrado de datos, el uso de contraseñas seguras para tener más respaldo a posibles hackeos.

Cabe mencionar que el establecimiento se dedica a ofrecer una amplia gama de servicios para ayudar a las personas y a la empresa a aprovechar al máximo la tecnología. Por ejemplo, servicios de reparación y mantenimiento de computadoras, software de análisis de datos, servicios de soporte técnico, consultoría en tecnología de la información para ayudar a las empresas a identificar las mejores soluciones tecnológicas para sus necesidades específicas.

La problemática principal presentada en la empresa es la creciente amenaza de los ataques de malware, los cuales pueden comprometer la seguridad de su infraestructura y su información. En particular, la herramienta Cobalt Strike es una herramienta que es utilizada comúnmente por los atacantes para llevar a cabo los ataques de malware. La falta de una estrategia efectiva de seguridad cibernética y herramientas adecuadas para protegerse contra los ataques de malware lo cual ocasiona la pérdida de datos confidenciales y la violación de la seguridad.

Estos ataques pueden tener graves consecuencias, reflejada en la pérdida de datos confidenciales como nombres completos, direcciones, correos electrónicos y números telefónicos, listas de clientes, precios y otros detalles comerciales, también el robo de propiedad intelectual, la interrupción de los servicios en línea, el daño a la reputación y la pérdida financiera. Aunque la empresa cuenta con medidas de seguridad como el

cifrado de datos y el uso de contraseñas seguras, estos ataques continúan siendo un problema en crecimiento.

El propósito de este caso de estudio es simular un ataque informático a través de con el uso de la herramienta Cobalt Strike sobre el sistema testeo Kali Linux y establecer los procedimientos que se pueden implementar para detectar que se continúa atacando a los sistemas y así evitar que esto suceda. es decir, para mantener la estabilidad del sistema, por tanto, se realizarán pruebas para tomar las acciones oportunas que se puedan realizar, evitando así posibles ataques informáticos y contrarrestando posibles y futuras amenazas.

Con esta simulación como ejemplo, se identificarán las formas en que la información de la empresa puede protegerse desde los servidores domésticos hasta los servidores organizacionales, evitando y reduciendo las altas tasas de delitos informáticos.

JUSTIFICACIÓN

La investigación propuesta tiene como objetivo destacar la importancia de contar con un respaldo de auditoría de seguridad para la empresa "PC Soluciones" y proponer la aplicación de Pentesting mediante el uso de la herramienta Cobalt Strike. La realización de este tipo de pruebas permite garantizar la seguridad e integridad de la información tanto de los clientes como de la empresa, detectando y evaluando posibles vulnerabilidades en los sistemas informáticos.

La herramienta Cobalt Strike es fundamental para garantizar la seguridad y la integridad de la información de la empresa "PC Soluciones", así como para cumplir con los requisitos de seguridad y privacidad de los clientes. Además, la realización de esta actividad permite detectar y corregir posibles vulnerabilidades, prevenir posibles ataques y garantizar la continuidad de las operaciones en caso de una amenaza informática.

El beneficio que conlleva tener a la mano un respaldo de seguridad, la gestión de las actividades diarias de la empresa lo tendrá los administrativos de forma directa y los clientes aprovecharan de la garantía que genera contar con un respaldo de auditoría de pentesting. aportará un progreso significativo en el cumplimiento de las actividades administrativas de la empresa

Como idea principal se pretende ejecutar ataques a computadoras con un malware e identificar sus vulnerabilidades con el propósito de establecer herramientas que permitan neutralizar el hackeo y, además, saber qué información se puede robar a través del malware y determinar el impacto en las personas y organizaciones por este tipo de piratería informática. El trabajo tendrá como fundamento los principios de Hacking Ético y Ciberseguridad estudiados en la carrera y que encuentran su aplicación práctica en el mundo real.

OBJETIVOS DEL ESTUDIO

Objetivo general:

Analizar el uso de la herramienta Cobalt Strike a través de una simulación de ataque malware en la red de PC Soluciones.

Objetivos específicos:

- Fundamentar las bases teóricas sobre el uso de las herramientas de Hacking Ético y su relación con la seguridad de la red empresarial.
- Identificar las vulnerabilidades y escalar privilegios mediante la ejecución del exploits con ataque de penetración mediante la herramienta de Cobalt Strike.
- Definir puntos o soluciones a las debilidades encontradas en la red de PC mediante simulación de ataque malware realizada.

LÍNEAS DE INVESTIGACIÓN

Para el desarrollo de la presente investigación se basó en las líneas de investigación de la Universidad Técnica de Babahoyo reconociendo como pertinente tema de "Análisis y Simulación de ataque de malware con el uso de la herramienta Cobalt Strike para la empresa pc soluciones".

- **Línea de investigación**

Sistemas de información y comunicación, emprendimiento e innovación.

- **Sub línea de investigación**

Redes y tecnologías inteligentes de software y hardware.

MARCO CONCEPTUAL

Seguridad informática

Afirma (Lowe, 2017). que la seguridad informática es un conjunto de métodos, herramientas y procedimientos diseñados para proteger la información y los sistemas informáticos de posibles amenazas y ataques externos. La atención se centra en la protección de los recursos informáticos, incluidos el hardware, el software, los datos y las redes. Los peligros asociados a la estabilidad informática continúan creciendo debido al mayor uso de las tecnologías de la información y la comunicación, la digitalización de los procesos de negocio y la interconexión de sistemas. También se reúne para tratar temas de gestión de incidentes, incluida la detección y respuesta a incidentes de estabilidad, recuperación ante desastres y gestión de crisis. (pag.4)

Según Martha Romero et at. (2018) que la seguridad informática es importante por muchas razones. Primero, los ataques cibernéticos son cada vez más comunes y sofisticados, lo que significa que los sistemas informáticos a menudo se ven comprometidos o comprometidos. En segundo lugar, los datos personales y comerciales se han vuelto cada vez más valiosos, y la pérdida o el robo pueden tener consecuencias graves y costosas. En tercer lugar, la seguridad de TI es para mantener la confidencialidad, la integridad y la disponibilidad de los datos. (pag.7)

Por lo tanto, las empresas y los usuarios individuales deben tomar medidas para proteger su información y sus sistemas informáticos, como usar contraseñas seguras, implementar medidas de autenticación de múltiples factores, actualizar regularmente el software y los sistemas, y educar a los usuarios sobre los riesgos de seguridad informática, además los profesionales deben estar capacitados en seguridad de la información. (pag.7)

Ciberseguridad

Explica (García A. A., 2019) que la ciberseguridad es el conjunto de medidas y prácticas que se implementan para proteger los sistemas, dispositivos y redes informáticas de ataques malintencionados, fraudes, espionaje y cualquier otro tipo de ciberdelito. La ciberseguridad se enfoca en la protección de la información y los activos digitales, para garantizar la disponibilidad, integridad y confidencialidad de los mismos.

La ciberseguridad implica el uso de tecnologías, políticas, prácticas y procedimientos para proteger la información y los sistemas informáticos, y suele involucrar la utilización de herramientas y soluciones de seguridad como software antivirus, firewalls, sistemas de detección de intrusiones, cifrado de datos y copias de seguridad. La implementación de medidas de ciberseguridad efectivas ayuda a proteger la información y los activos digitales (pag.9)

Ciberdelito

Menciona (Atienza, 2022) que es cualquier actividad delictiva que utiliza tecnologías de la información y la comunicación, como computadoras, dispositivos móviles y redes en línea. Incluye el acceso no autorizado, la difusión de malware, el robo de información. Además, se ha convertido en una amenaza cada vez más común en la era digital.

Es importante que tanto los individuos como empresas tomen medidas de seguridad para protegerse de los ataques, como utilizar contraseñas seguras, actualizar regularmente su software, estar atentos a correos y sitios web fraudulentos, y tener un plan de respuesta a incidentes en caso de sufrir un ataque. (pag.15)

(Mahecha, 2022) Argumenta que existen diversas categorías en las que se pueden clasificar los ciberdelitos. Algunas de ellas son:

Ciberespionaje: Se refiere a la obtención ilegal de información clasificada o sensible por parte de personas o gobiernos extranjeros.

Ciberterrorismo: Es la utilización de técnicas informáticas para cometer actos de terrorismo, tales como la alteración de sistemas críticos, la interrupción de servicios esenciales, o la difusión de propaganda violenta.

Fraude en línea: Se trata de delitos en los que se utilizan medios electrónicos para realizar actividades fraudulentas, tales como la falsificación de documentos, el engaño en la venta de bienes o servicios, o la utilización de tarjetas de crédito o cuentas bancarias robadas.

Acoso en línea: Incluye conductas agresivas o intimidatorias realizadas en el ámbito virtual, tales como el ciberbullying, la difamación, el acoso sexual, o la suplantación de identidad.

Robo de identidad: Es el acto de utilizar la información personal de un individuo sin su consentimiento para cometer fraudes, adquirir bienes o servicios, o realizar actividades ilegales en línea.

Hacking: Consiste en la obtención no autorizada de información o acceso a sistemas informáticos, con el fin de realizar actividades malintencionadas, tales como el robo de datos, la distribución de malware, o el sabotaje de sistemas.

Cada una de estas categorías tienen un gran impacto, por lo que es importante tomar medidas de seguridad para protegerse de estas amenazas en línea. (pag.67)

Aspectos de seguridad que compromete un ataque

La seguridad de la información se basa en tres principios básicos: confidencialidad, integridad y disponibilidad. Estos principios, conocidos como los tripletes CID, se consideran los pilares de la seguridad de la información

La confidencialidad: Explica (Huerta, 2020) que se relaciona con la protección de la información contra la intrusión de personas o empresas no autorizadas que no tienen derecho a acceder a la información. Entonces, estamos hablando de garantizar que solo las personas autorizadas tengan acceso a la información Esto se logra mediante la implementación de medidas de seguridad que protegen la información en tránsito y en reposo, como el cifrado de datos, la autenticación y la autorización de usuarios. (pag.11)

La integridad Menciona (Kleppmann, 2022) que este término se refiere a la seguridad y confianza en que los datos no han sido alterados de manera no autorizada o accidental. Por lo tanto, nos esforzamos por garantizar que la información permanezca sin cambios desde su construcción hasta su almacenamiento y transmisión. Para lograr esto, se utilizan técnicas y herramientas de verificación de datos, como firmas digitales, códigos hash y controles de variantes. (pag.22)

La disponibilidad Según (Santos, 2020) que se relaciona con garantizar que los sistemas que almacenan y procesan datos estén continuamente accesibles y funcionen de manera óptima para los usuarios autorizados. Además, insistir en un inicio de sesión sin problemas para los usuarios autorizados también es un aspecto crucial. Se utilizan técnicas de redundancia como sistemas de copia de estabilidad y replicación de datos. De esta forma se evitan fallos en el acceso a la información y se garantiza una disponibilidad continua y fiable. (pag.31)

Ataque Informático

Comenta (Audit, 2018) que un ataque informático es un acto malicioso en el que alguien intenta obtener acceso no autorizado o dañar un sistema informático. Es un tipo de robo digital donde un atacante intenta acceder a información valiosa almacenada en un sistema informático. Dichos ataques pueden tener graves consecuencias, especialmente para las empresas y las personas afectadas. Un ataque a un banco puede resultar en la pérdida de información financiera y personal de los clientes, y el banco puede perder dinero. Por esta razón, es fundamental que las empresas y las personas tomen medidas para proteger sus sistemas informáticos. (pag.56)

Dependiendo del ataque que afecte se pueden provocar distintos daños los cuales son:

Daños menores: Afirma (Gargallo, 2017) que los ataques que causan daños menores pueden causar ciertos problemas, pero generalmente no tienen secuelas significativas a largo plazo. Además, puede causar errores en su sistema operativo, eliminar archivos no esenciales o interrumpir temporalmente su acceso a Internet. Estos efectos nocivos se pueden resolver restaurando el sistema o reinstalando el programa. (pag.72)

Daños moderados: Dice (Gargallo, 2017) que los ataques que provocan daños moderados pueden tener consecuencias más graves que uno que hace poco daño. Esto puede provocar la pérdida de datos importantes, interrupciones del servicio a largo plazo o daños en los sistemas o bases de datos. Estas infracciones pueden requerir la restauración de datos de copias de seguridad, la eliminación y reinstalación de programas y la implementación de medidas de seguridad adicionales. (pag.75)

Daños mayores: Menciona **Fuente especificada no válida.** que los ataques que provocan daños mayores pueden ser muy graves y tener un impacto significativo en los sistemas y en la empresa. Puede ser muy grave y tener un impacto en los sistemas y negocios. Pueden provocar la pérdida total de datos, interrupciones prolongadas del servicio, violaciones de la privacidad del usuario y daños en los sistemas críticos. Estos compromisos pueden requerir la reconstrucción de sistemas y bases de datos, la implementación de nuevas medidas de seguridad y la evaluación de daños financieros. (pag.78)

Daños severos: Explica (Briceño, 2020) que los ataques que provocan daños severos pueden ser catastróficos y amenazar la seguridad de su empresa. Pueden provocar la pérdida completa de datos y la interrupción prolongada del servicio, así como la exposición de la información personal y financiera de los usuarios. Estas infracciones pueden requerir la intervención de expertos en seguridad informática, la eliminación y restauración de sistemas críticos y pueden tener graves consecuencias financieras y legales. (pag.67)

Daños triviales: Argumenta (Briceño, 2020) que los ataques que causan daños intrascendentes generalmente tienen poco efecto y no tienen consecuencias graves. Esto podría ser, por ejemplo, un virus que ralentiza su sistema o anuncios no deseados en su navegador. Aunque estos ataques no son graves, es importante evitar que se agraven.

Daños ilimitados: Según (Briceño, 2020) que los ataques que provocan daños ilimitados tienen un impacto masivo y son difíciles de contrarrestar. Pueden provocar la pérdida de la reputación y la confianza del cliente, así como graves daños financieros y legales. Estos ataques pueden ser muy complejos y requieren la intervención de expertos en seguridad informática para resolverlos. (pag.72)

Fases del Ciberataque

Ilustración # 1. Fases del ciberataque.

Fuente: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces Autor: (INCIBE, 2020).

Reconocimiento.

(Kim, 2021) En esta fase, los ciberdelincuentes recopilan información sobre sus objetivos, analizan la información de la empresa publicada públicamente, buscan encontrar en las redes sociales e incluso desarrollan colaboraciones a través de la comunicación electrónica. Con esta información, los atacantes evalúan qué procedimientos de ataque funcionan y la probabilidad de que funcionen. Para evitar que los atacantes cibernéticos accedan a dichos datos, es imperativo que los empleados conozcan y desarrollen planes de estabilidad proactivos y puedan identificar la información compartida principalmente a través de Internet y las redes sociales. (pag.75)

Preparación.

Afirma (Kim, 2021) que, en esta etapa, el ataque es específico del objetivo: por ejemplo, un atacante puede crear un documento de Microsoft Office e insertarlo en un correo electrónico haciéndose pasar por una persona legítima con la que la empresa interactúa normalmente, es decir, la suplantación. Por ello, es sumamente importante estar atento a este tipo de ataques y así poder evitarlos. (pag.77)

Distribución.

En esta fase se realiza la difusión del ataque, por ejemplo, abriendo un documento infectado enviado por correo electrónico, accediendo a un phishing, etc.

Explotación.

Según (Ismail, 2021) que después de que el ataque es generalizado, sigue lo que se conoce como la "detonación" del ataque, infectando las computadoras y sus redes. Esto generalmente se hace explotando vulnerabilidades conocidas que ya tienen parches de seguridad, como vulnerabilidades de escritorio remoto, que de otro modo permitirían la entrada remota, por lo que es importante parchear la seguridad y mantener actualizados todos los sistemas incluido el software antivirus. (pag.87)

Instalación.

Explica (Ismail, 2021) que esto se refiere cuando el malware se instala en la víctima. También puede haber situaciones en las que la instalación no sea deseable, como el robo de credenciales o algún tipo de fraude, por lo que debemos estar atentos y tomar

medidas, como monitorear el estado del sistema a través de nuestra propia infraestructura o seguridad administrada, o subcontratar personas o servicios. (pag.89)

Comando y control.

Argumenta (Ismail, 2021) que comando y control (C2) se refiere a un grupo de herramientas y métodos que utiliza un atacante para comunicarse con un sistema comprometido. En otras palabras, el objetivo es permitir que un atacante obtenga el control remoto completo sobre un sistema comprometido. C2 se puede omitir a través de varios métodos, como correo electrónico, mensajería instantánea o servidores web maliciosos. (pag.90)

Acciones sobre los objetivos.

Esta es la fase final donde la atacante toma el control de los datos e intenta extender su acción maliciosa a objetivos más peligrosos.

Tipos de ataques.

Malware.

Menciona (Bottini, 2021) que el malware es un tipo de software que está especialmente diseñado para causar daños o realizar acciones no deseadas en los sistemas informáticos de los usuarios. Este término cubre una amplia gama de malware, incluidos virus, troyanos, gusanos, spyware y ransomware. Además, puede propagarse a través de correos, descargas de archivos infectados o visitas a sitios web. Cuando el malware infecta un sistema, puede causar varios daños, como el robo de datos confidenciales, la corrupción de archivos, el bloqueo del sistema o la reducción del rendimiento. Para protegerse del malware, es importante tener instalado un antivirus actualizado, mantener

sus sistemas operativos y aplicaciones actualizados con actualizaciones de seguridad y evitar descargar archivos sospechosos o hacer clic en enlaces desconocidos. (pag.41)

Troyano

Comenta (Snyder, 2021) que un troyano es un tipo de malware que se utiliza para obtener acceso no autorizado a un sistema informático. Las actividades que puede realizar un troyano incluyen la recopilación de información confidencial, como contraseñas y datos bancarios, la instalación de software adicional, el robo de información personal, el espionaje y el uso de una computadora infectada para lanzar ataques a otros sistemas. Cuando un usuario ejecuta un troyano, instala malware en el sistema infectado, lo que permite que el atacante tome el control del sistema.

Los troyanos se dividen en tres categorías principales:

Troyanos de puerta trasera (backdoor Trojan): Permite a un atacante mantener el control de un sistema infectado de forma remota sin el conocimiento del cliente. Los atacantes pueden usar estas puertas traseras para robar información, instalar más malware o tomar el control de un sistema.

Troyanos de descarga (downloader Trojan): Estos troyanos descargan e instalan malware adicional en el sistema infectado sin el conocimiento del usuario. Pueden descargar cualquier tipo de malware, incluyendo virus, gusanos, ransomware y spyware.

Troyanos de caballo de Troya (Trojan horse): Esta amenaza se hace pasar por software legítimo y se distribuyen a través de descargas ilegales o correos electrónicos con archivos adjuntos maliciosos. Una vez instalado, los atacantes pueden tomar el control del sistema infectado, robar información o instalar más malware. Es importante

que tenga un software antivirus actualizado y realice análisis de seguridad regulares para detectar y eliminar cualquier posible infección por troyanos. (pag.77)

Virus informático.

Explica (Rubenking, 2022) que es un programa que infecta las computadoras sin el permiso de los usuarios. También se clasifica como un mecanismo parasitario porque ataca archivos o sectores de arranque y se replica a sí mismo para propagarse aún más de una manera que incluye la pérdida no solo de datos sino también de imágenes y videos incluso a los sistemas operativos, causando aún más graves daños entre otros. Es importante instalar y mantener actualizado el software antivirus. (pag.52)

Phishing.

Según (Nguyen, 2018) que el phishing se usa comúnmente para robar datos de usuario, como números de tarjeta y contraseñas. Este delito informático intenta engañar a las personas para que accedan a información personal. El ataque está diseñado mediante el envío de mensajes escritos o correos electrónicos destinados a hacerse pasar por una persona de confianza para asustar y engañar a la víctima para que abra un enlace. Al hacer clic en este enlace, se llevará a la víctima al mismo enlace que el original, donde se le pedirá que ingrese el cliente y la contraseña. (pag.59)

Ransomware.

Argumenta (García H. A., 2018) que el ransomware es un tipo de malware que impide que los usuarios accedan a sistemas o archivos individuales y exige un rescate para volver a iniciar sesión Los ataques de ransomware pueden lanzarse de diversas formas, como a través de correos electrónicos de phishing, enlaces o archivos adjuntos maliciosos o aprovechando vulnerabilidades en el software o los sistemas operativos. Una

vez que el malware infecta un ordenador, comienza a cifrar archivos o bloquear al usuario para que no pueda acceder a sus datos. (pag.125)

Tipos de ransomware.

(García H. A., 2018) Comento que son conocidos tres tipos de ransomware, mismos que están definidos por la gravedad de estos:

Scareware: es un tipo de software que se hace pasar por un programa de seguridad legítimo con el fin de asustar al usuario y hacer que realice acciones innecesarias o incluso perjudiciales para su computadora. Los creadores utilizan tácticas engañosas, como mensajes de alerta falsos que parecen provenir de un programa antivirus o mensajes de error que parecen indicar que la computadora está infectada con virus.

Bloqueadores de pantalla: Su nivel de ejecución es formidable, pues bloquea la pantalla de un ordenador, impidiendo por completo el uso del ordenador. Al intentar encender nuevamente el ordenador se mostrará una ventana en toda la pantalla, generalmente usan emblemas o logos.

Ransomware de cifrado: Considerado como el peor de todos, este retiene archivos y los cifra, exigiendo un monto monetario para descifrarlos y posteriormente devolverlos. Es considerado como el peor debido a que no hay software de seguridad que pueda recuperar la información retenida por el ciberdelincuente.

Cómo protegerse del ransomware.

Para protegerse del ransomware, es importante tomar medidas de seguridad proactivas, como realizar copias de seguridad de los archivos importantes, utilizar software antivirus, mantener el software actualizado, utilizar contraseñas seguras y

desconfiar de los mensajes de alerta sospechosos. Además, es recomendable evitar abrir correos electrónicos de remitentes desconocidos y utilizar una (VPN). (pag.127)

Medidas de seguridad para ataques C&C.

(Candel, 2021)dice que las empresas corren un mayor riesgo de sufrir ataques de servidor C&C porque puede haber miles de dispositivos que pertenecen a una sola red, o varias redes a menudo sufren de rendimiento. Varias medidas para garantizar un buen nivel de protección:

- **Actualice sus sistemas regularmente:** Los sistemas y aplicaciones deben actualizarse regularmente para garantizar que estén protegidos contra vulnerabilidades conocidas. Los fabricantes de software lanzan actualizaciones de seguridad para solucionar vulnerabilidades, errores y brechas de seguridad, por lo que mantener los sistemas actualizados puede prevenir ataques.
- **Instale software antivirus y antimalware**: Un software antivirus y antimalware es esencial para detectar y eliminar software malicioso en un sistema. La mayoría de los programas antivirus y antimalware contienen bases de datos actualizadas de amenazas conocidas y patrones de comportamiento sospechosos que pueden ayudar a prevenir ataques.
- **Filtre el tráfico de red:** La filtración de tráfico de red implica el uso de cortafuegos y otros dispositivos de seguridad para bloquear el acceso a sitios web y direcciones IP conocidos por ser utilizados por servidores C&C. Un cortafuegos puede identificar y bloquear el tráfico de red no autorizado y reducir el riesgo de que los dispositivos en su red se conecten a servidores maliciosos.

- **Monitoree el tráfico de red:** Las herramientas de monitoreo de red pueden detectar patrones de tráfico inusual y actividad sospechosa que pueden indicar la presencia de un ataque. Estas herramientas pueden identificar conexiones maliciosas, tráfico de red cifrado para detectar amenazas. (pag.47)

Cobalt Strike

Explica (Yuri Diogenes, 2022)que la herramienta RedTeam Cobalt Strike es ampliamente utilizada por varios ciberdelincuentes para explotar y entregar las denominadas balizas, que permiten el inicio de sesión remoto persistente en dispositivos infectados. Luego, los atacantes pueden usar estas balizas para obtener acceso a los servidores infectados para recopilar datos o distribuir malware adicional.

En un nuevo informe de la firma de seguridad Intezer, los investigadores argumentan cómo los actores de amenazas pueden hacer que sus balizas de Linux Cobalt Strike sean compatibles a voluntad. Con estas balizas, los actores de amenazas ahora tienen la capacidad de lograr resiliencia e instalaciones de ejecución de comandos. Se postula que Cobalt Strike tiene una desventaja, ya que solo es compatible con dispositivos Windows y no contiene balizas de Linux. El atacante modificó una versión de Cobalt Strike con nombre en código "Vermilion" para que fuera compatible con Linux. Al mismo tiempo, también se considera una herramienta flexible y robusta, ya que puede reutilizarse para diferentes cargas útiles, como ransomware o keylogger.

La capacidad de proporcionar un marco para controlar los datos o archivos involucrados en el ataque. Esto significa que los usuarios pueden definir cómo se almacenan, cifran y transfieren los datos a través de la red. Esto hace que Cobalt Strike sea una herramienta muy flexible y robusta contra cargas útiles de ransomware o

keylogger, ya que permite a los usuarios personalizar el comportamiento de estas cargas útiles para adaptarse a las necesidades del ataque. Sin embargo, es importante destacar que, como cualquier herramienta de software, Cobalt Strike no es infalible. A pesar de los resguardos y papeles adicionales para evitar abusos, siempre existe la posibilidad de que la herramienta sea modificada o descifrada por ciberdelincuentes. (pag.112)

MARCO METODOLÓGICO

En este caso de estudio se construyó utilizando el método deductivo e inductivo. En la fase deductiva se realizará una revisión bibliográfica exhaustiva para comprender los conceptos fundamentales sobre la ciberseguridad, los ataques de malware y el uso de la herramienta Cobalt Strike. Esta revisión permitirá establecer una base teórica sólida para la investigación y plantear hipótesis iniciales sobre el impacto del uso de la herramienta en la seguridad informática de la empresa PC soluciones.

En la fase inductiva se llevará a cabo un estudio de caso en la empresa, con el objetivo de recopilar datos empíricos y analizar la situación actual de seguridad informática en la empresa. Para ello, se utilizará una encuesta dirigida a los miembros de la empresa que tengan conocimientos en seguridad informática, con el fin de conocer la percepción que tienen sobre la seguridad actual y su experiencia en la detección y prevención de ataques de malware.

A continuación, se visualizará el listado de las preguntas realizadas en la encuesta:

RESULTADOS

1. ¿Ha sufrido su empresa pérdidas de datos importantes debido a un ataque de malware?

Se puede concluir que el total de personas encuestadas mencionan que si han tenido problemas donde se ha comprometido y perdido información.

Tabla 1: Resultados de la pregunta 1.

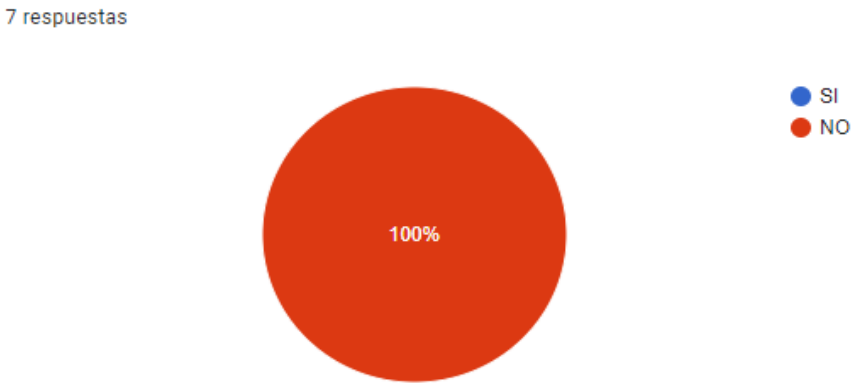
Fuente: Encuesta a la empresa Pc soluciones

Autor: Tamaquiza 2023

2. ¿Ha utilizado alguna vez la herramienta Cobalt Strike en su trabajo?

Como resultado se obtuvo que el total de personas encuestadas afirman que no han utilizado la herramienta Cobal Strike si la han escuchado, pero no han hecho efectivo si utilización

Tabla 2: Resultados de la pregunta 2.



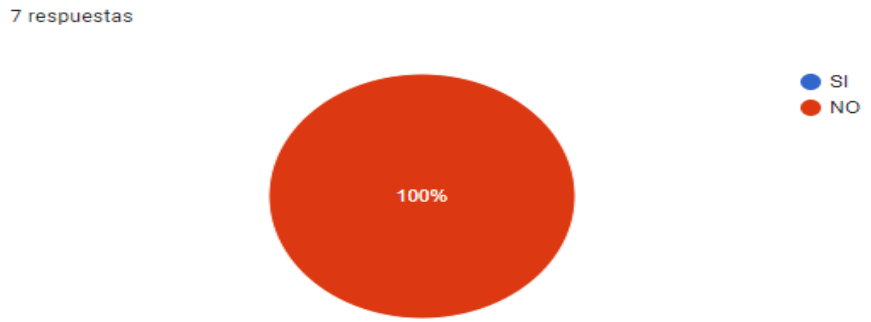
Fuente: Encuesta a la empresa Pc soluciones

Autor: Tamaquiza 2023

3. ¿Ha recibido capacitación formal sobre el uso de la herramienta Cobalt Strike?

Como resultado se obtuvo que el total de personas encuestadas afirman que no cuenta con el conocimiento necesario para la utilización de la herramienta Cobal Strike.

Tabla 3: Resultados de la pregunta 3.



Fuente: Encuesta a la empresa Pc soluciones

Autor: Tamaquiza 2023

4. ¿Ha notado algún comportamiento sospechoso en los sistemas de su empresa que podría indicar un posible ataque de malware?

Se puede concluir que el total de personas encuestadas mencionan que si han notado comportamientos extraños en su sistema debido ataques realizados diferentes medios.

Tabla 4: Resultados de la pregunta 4.

Fuente: Encuesta a la empresa Pc soluciones

Autor: Tamaquiza 2023

5. ¿Cree que la herramienta Cobalt Strike es necesaria para mantener la seguridad de su empresa?

Como resultado se obtuvo que el total de personas encuestadas afirman que esta herramienta es esencial para evitar estos ataques a la seguridad del sistema de su empresa.

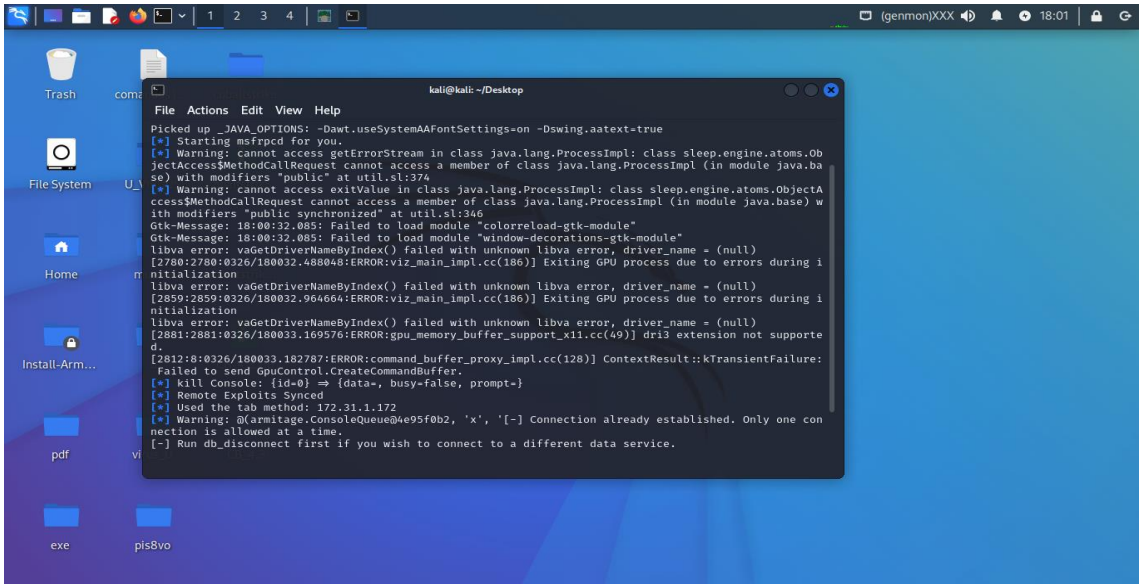
Tabla 5: Resultados de la pregunta 5.

Fuente: Encuesta a la empresa Pc soluciones

Autor: Tamaquiza 2023

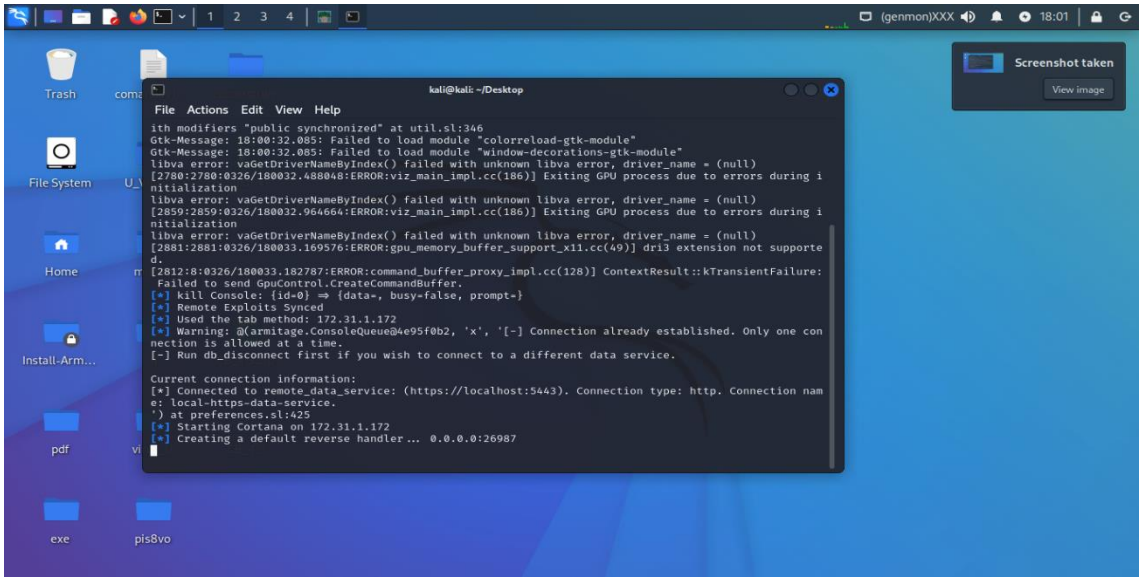
En las siguientes imágenes se puede observar el proceso de la simulación de un ataque malware en la empresa PC Soluciones por lo cual resultaron de manera eficiente y eficaz, en el efecto del desconocimiento sobre seguridad hace que la empresa PC Soluciones sean muy vulnerables en este tipo de ataques.

Ilustración 1. Ejecución del Cobalt strike



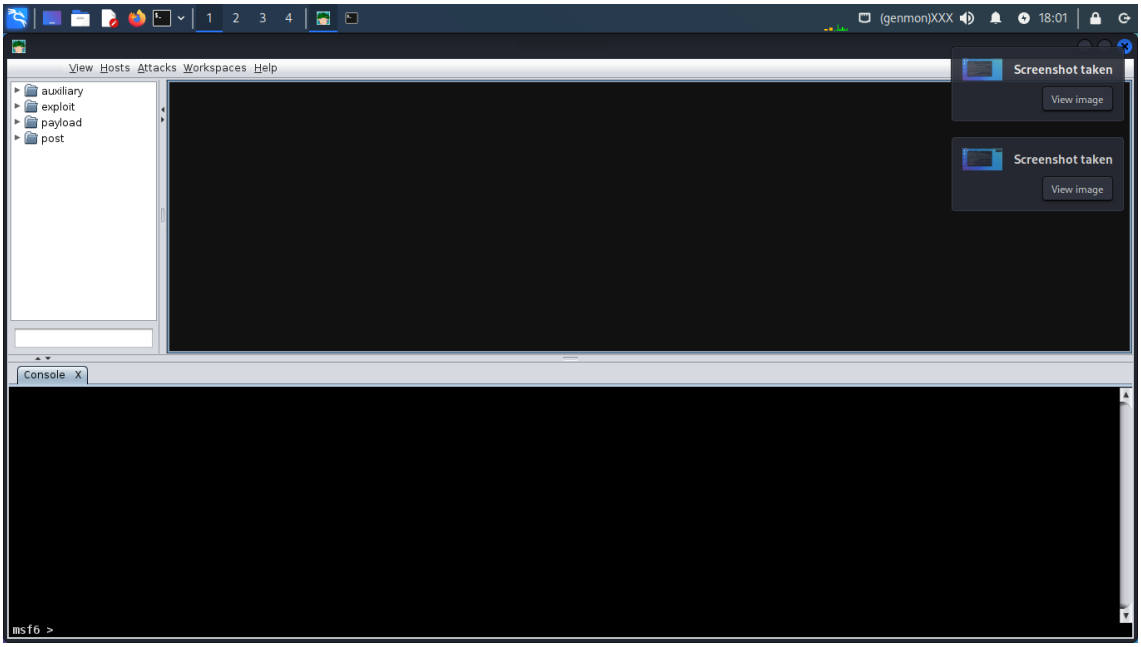
Elaborado por: Enzo Aldahir Tamaquiza Murillo.

Ilustración 2. El puerto que está en escucha en la red cuando un puerto está abierto para que entren conexiones tcp, Pueda conectarse el virus A la herramienta



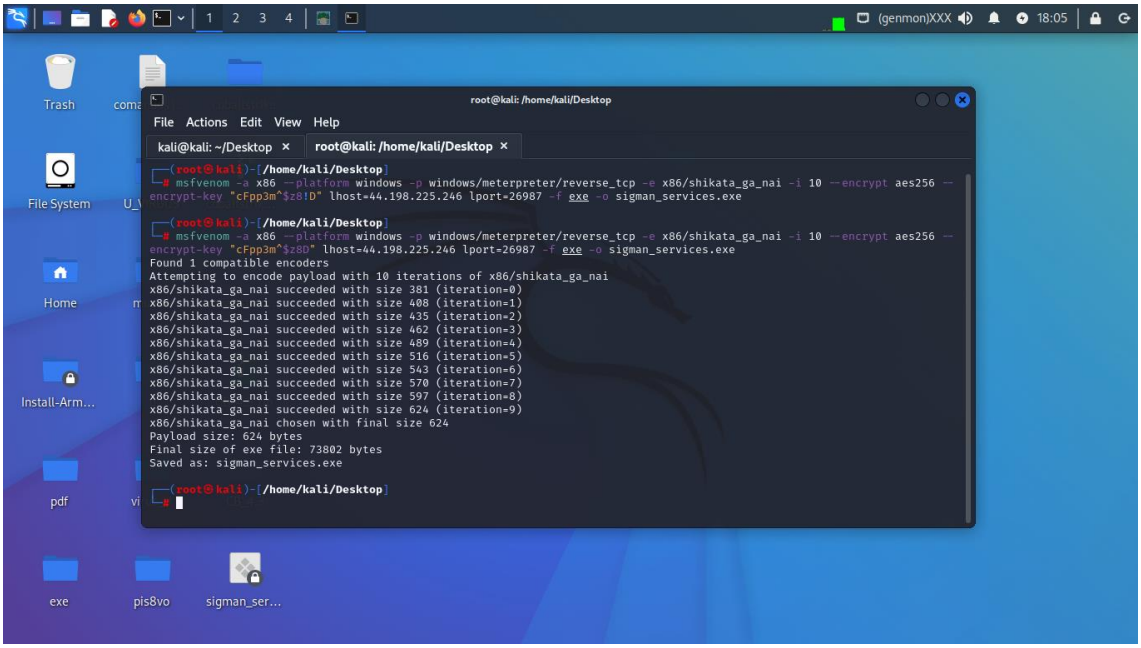
Elaborado por: Enzo Aldahir Tamaquiza Murillo.

Ilustración 3. Visualización de la interfaz gráfica de Cobal Strike



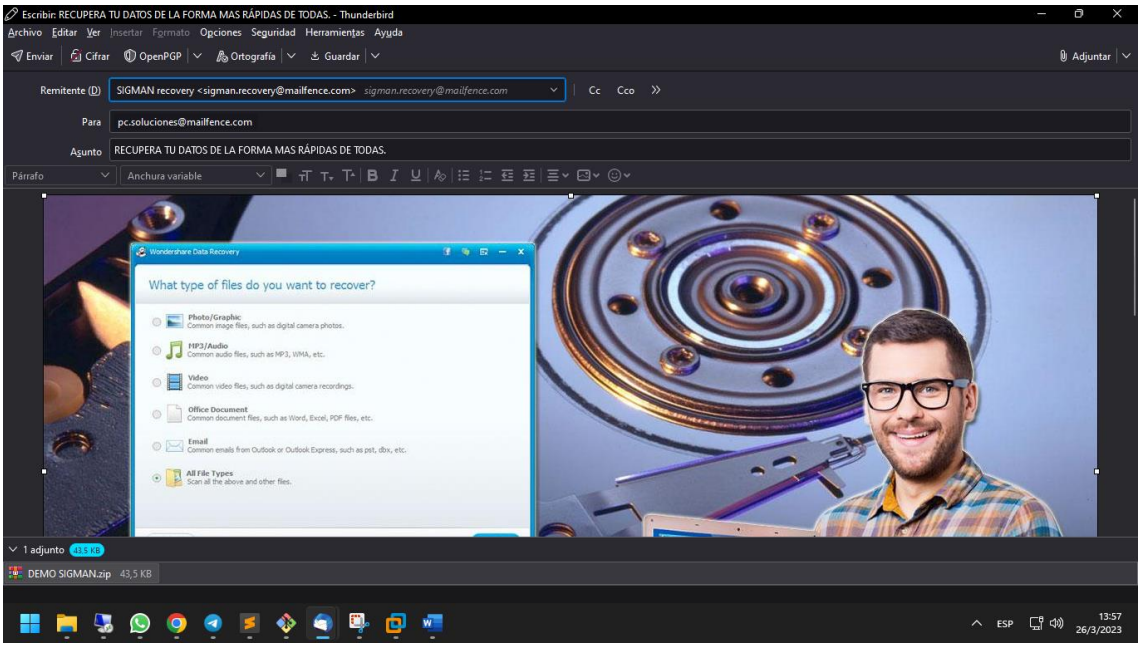
Elaborado por: Enzo Aldahir Tamaquiza Murillo.

Ilustración 4. Aquí se puso una línea de código con la ip del servidor y el puerto en escucha, por la cual genere un virus sigman_services.exe.



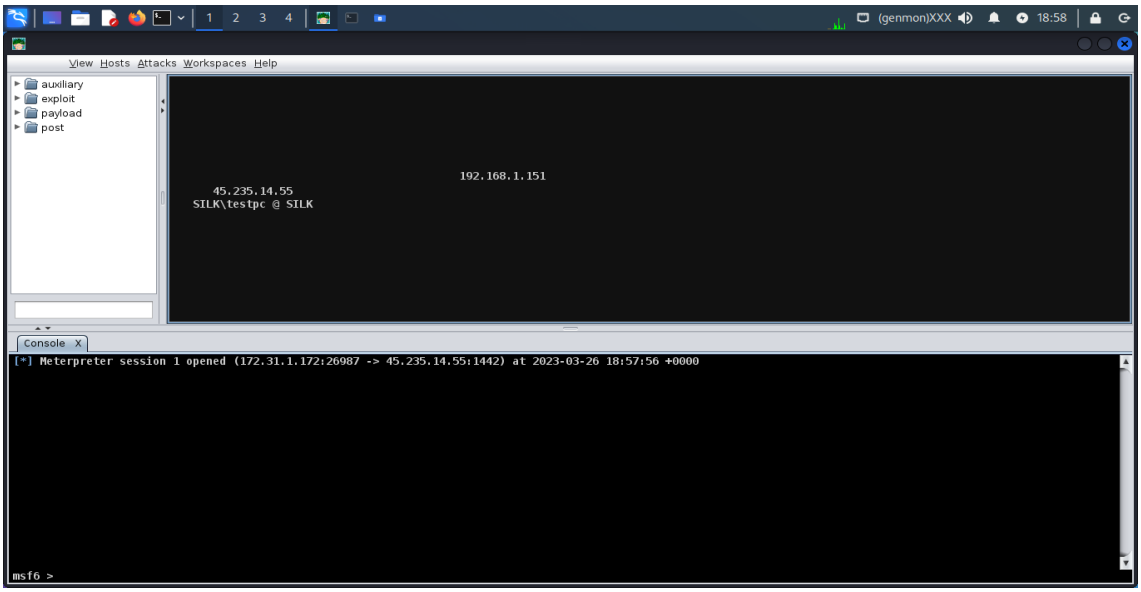
Elaborado por: Enzo Aldahir Tamaquiza Murillo.

Ilustracion 5. Aquí el virus fue envío a la empresa PC Soluciones por un servidor de correo privado promocionando un programa de recuperación de información.



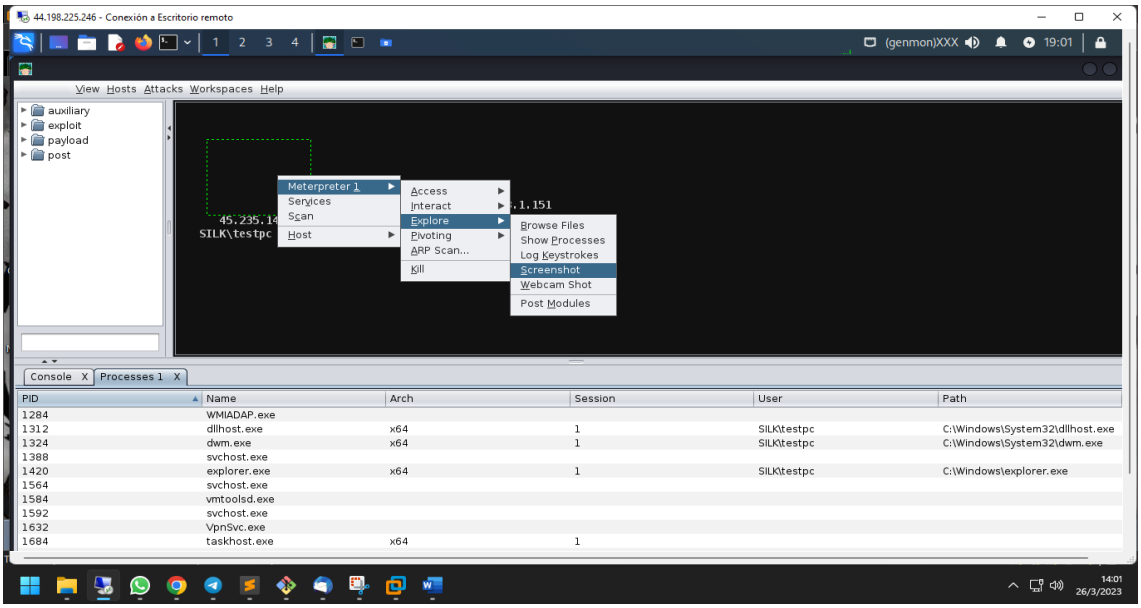
Elaborado por: Enzo Aldahir Tamaquiza Murillo.

ilustración 6. En esta parte se muestra que la víctima cayó en la ingeniería social y ahora tenemos acceso a todo su pc



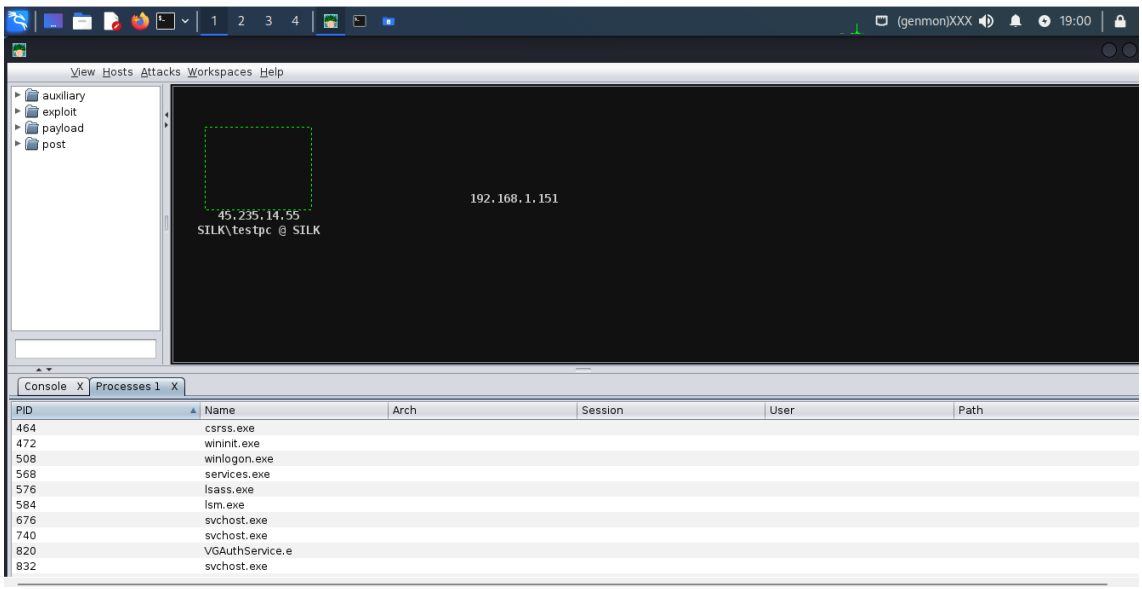
Elaborado por: Enzo Aldahir Tamaquiza Murillo.

Ilustración 7. En la computadora víctima tenemos una sesión abierta meterpreter dónde hay muchas opciones para espiar sus computadoras, en la parte de Explorer podemos ver qué tenemos la opción de ver sus procesos de la Pc, Archivos, tomar captura a la pantalla, espirar por la cámara de esa máquina.



Elaborado por: Enzo Aldahir Tamaquiza Murillo.

Ilustración 8. En esta parte podemos ver los procesos que está haciendo la pc.



Elaborado por: Enzo Aldahir Tamaquiza Murillo.

A continuación, se muestra un cuadro donde se muestra puntos o soluciones a las debilidades encontradas en la red de PC mediante simulación de ataque malware realizada.

Vulnerabilidades	Soluciones
• Autenticación débil o inexistente puede permitir que los atacantes ingresen a los sistemas y redes de la empresa. Si no se implementa la autenticación de dos factores (2FA) o contraseñas fuertes.	• Si se detecta un ataque de malware, es crucial aislar rápidamente los sistemas afectados de la red, Desconecta los sistemas infectados de la red y apártalos hasta que puedan ser analizados y limpiados adecuadamente.
• Software sin parches o desactualizado puede dejar abiertas vulnerabilidades conocidas que los atacantes pueden explota	• Identificar correos electrónicos de phishing, enlaces sospechosos y descargas no autorizadas. Anima a los empleados a informar cualquier actividad sospechosa y establece un canal de comunicación claro para que puedan hacerlo de manera segura.
• Descargas y ejecución de archivos no autorizado aumentan el riesgo de introducir malware en la empresa.	• Mantener copias de seguridad actualizadas y almacenadas de manera segura en ubicaciones fuera de línea. En caso de un ataque de malware que cifre o dañe los datos, contar con copias de seguridad te permitirá restaurar la información importante y minimizar la pérdida de datos.
• Si no se educa al personal sobre los riesgos del malware, como hacer clic en enlaces o abrir archivos adjuntos sospechosos, podrían caer en trampas y permitir la entrada del malware a la red corporativa.	• Actualizar todos los sistemas operativos, aplicaciones y antivirus actualizados con los últimos parches de seguridad.

DISCUSIÓN DE RESULTADOS

En primer lugar, se ejecutó la herramienta Cobalt Strike, la cual fue capaz de aprovechar la vulnerabilidad en el puerto abierto en la red de la empresa para conectarse al virus y obtener acceso a la interfaz gráfica de Cobalt Strike.

Posteriormente, se generó un virus con la dirección IP y el puerto en escucha y se envió a la empresa PC Soluciones por medio de un servidor de correo privado. La ingeniería social utilizada fue eficaz, lo que permitió a los atacantes obtener acceso a toda la PC de la víctima.

Una vez dentro de la PC de la víctima, los atacantes pudieron espiar los procesos, archivos y tomar capturas de pantalla. También tuvieron la capacidad de espiar a través de la cámara de la máquina.

La simulación de un ataque de malware con el uso de Cobalt Strike en la empresa PC Soluciones ha demostrado que la empresa es muy vulnerable a este tipo de ataques. Los resultados obtenidos indican que la empresa debe mejorar sus medidas de seguridad, incluyendo la actualización de sus sistemas de seguridad, la implementación de herramientas avanzadas de detección y respuesta de seguridad, y la educación y concienciación del personal sobre las mejores prácticas de seguridad.

Los resultados obtenidos de esta simulación de ataque de malware con el uso de la herramienta Cobalt Strike en la empresa PC Soluciones son preocupantes, ya que demostraron una alta vulnerabilidad ante este tipo de ataques debido al desconocimiento en seguridad. Es necesario que la empresa tome medidas para mejorar sus sistemas de seguridad y concientizar a su personal sobre las mejores prácticas de seguridad para evitar futuros ataques.

CONCLUSIONES

Una vez finalizado el respectivo caso de estudio gracias a los métodos deductivos como inductivos se pudo recolectar información muy esencial sobre la problemática suscitada en la empresa, respecto a la creciente amenaza de los ataques de malware. Además, cabe destacar que estos métodos permitieron obtener una visión completa de la red y sus debilidades, lo que permitió proponer alternativas de solución específicas y adecuadas a las necesidades de la empresa PC Soluciones.

La simulación de un ataque de malware en la empresa PC Soluciones utilizando la herramienta Cobalt Strike ha demostrado una alta vulnerabilidad en la seguridad de la empresa. es importante destacar que la falta de medidas de seguridad adecuadas en una empresa puede poner en riesgo su reputación y su capacidad para mantener la confianza de sus clientes. Un ataque exitoso de malware puede tener graves consecuencias para la empresa, incluyendo la pérdida de datos importantes, la interrupción de la actividad empresarial y el daño a la reputación de la empresa.

El análisis de la información obtenida a través de esta investigación se llegó a la conclusión de que el uso de herramientas de Hacking Ético, como Cobalt Strike, es una práctica importante para la evaluación de la seguridad de la red de la empresa PC Soluciones. Además, se demostró que el uso de esta herramienta puede ayudar a identificar vulnerabilidades en la red y prevenir posibles ataques.

RECOMENDACIONES

- Se sugiere que empresa PC Soluciones implemente medidas de seguridad adicionales para proteger su red empresarial contra posibles ataques de malware.
- Se recomienda capacitar y sensibilizar al personal en materia de seguridad de la información.
- Se recomienda que la empresa evalúe sus sistemas y procesos de seguridad actuales, identifique las debilidades y las fortalezas, y luego implemente medidas adecuadas para mejorar la seguridad

REFERENCIAS

Atienza, G. M. (2022). *Ciberdelitos. Instrucción y prueba.* Madrid. Obtenido de https://www.google.com.ec/books/edition/Ciberdelitos_Instrucci%C3%B3n_y_prueba/I72hEAAAQBAJ?hl=es&gbpv=1&dq=Ciberdelito++Atienza,+2022&pg=PP1&printsec=frontcover

Audit, c. i. (2018). *Seguridad informática.* France. Obtenido de https://www.google.com.ec/books/edition/Seguridad_inform%C3%A1tica/efAmg9f8XtQC?hl=es&gbpv=1&dq=ataque+informatico+(Audit,+2018&pg=PA205&printsec=frontcover

Bottini, C. (2021). *Elimina el malware sin instalar programas.* Madrid. Obtenido de https://www.google.com.ec/books/edition/Elimina_el_malware_sin_instalar_programa/W3JEEAAAQBAJ?hl=es-419&gbpv=1&dq=Malware+que+es&printsec=frontcover

Briceño, E. V. (2020). *Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking.* Madrid. Obtenido de https://www.google.com.ec/books/edition/Planificaci%C3%B3n_y_ejecuci%C3%B3n_de_evaluacio/D9DWDwAAQBAJ?hl=es-419&gbpv=1&dq=ataque+informatico+Brice%C3%B1o,+2020&printsec=frontcover

Candel, O. (2021). *Ciberseguridad. Manual práctico.* España. Obtenido de https://www.google.com/search?q=Medidas+de+seguridad+para+ataques+C%26C.+que+es&biw=905&bih=864&tbm=bks&sxsrf=AJOqlzV3x_9BpV6xi-XdXMpQk21clMZCJw%3A1679240696396&ei=-C0XZM7hF7WIwbkPo-

q46AQ&ved=0ahUKEwjOvc2Jq-j9AhU1RDABHSM1Dk0Q4dUDCAk&uact=5&oq=Medidas+de+s

García, A. A. (2019). *Ciberseguridad.* Mexico. Obtenido de https://www.google.com.ec/books/edition/Ciberseguridad/ZqHDDwAAQBAJ?hl=es&gbpv=1&dq=Ciberseguridad++Garc%C3%ADa,+2019&pg=PT4&printsec=frontcover

García, H. A. (2018). *Neutralización del ransomware criptográfico mediante un sistema de almacenamiento sincrónico versionado.* Madrid. Obtenido de https://www.google.com.ec/books/edition/Neutralizaci%C3%B3n_del_ransomware_criptogr/Zk9HDwAAQBAJ?hl=es-419&gbpv=1&dq=ransomware+que+es&printsec=frontcover

Gargallo, E. d. (2017). *La seguridad para los menores en internet.* Madrid. Obtenido de https://www.google.com.ec/books/edition/La_seguridad_para_los_menores_en_interne/dY5ODwAAQBAJ?hl=es&gbpv=1&dq=Ataque+Inform%C3%A1tico++Da%C3%B1os+menores&pg=PT30&printsec=frontcover

Huerta, A. V. (2020). *Seguridad en Unix y redes. Versión 2.1'.* Madrid. Obtenido de https://www.google.com.ec/books/edition/Seguridad_en_Unix_y_redes_Versi%C3%B3n_2_1/i-LTDwAAQBAJ?hl=es&gbpv=1&dq=inauthor:%22Antonio+Villal%C3%B3n+Huerta%22&printsec=frontcover

Ismail, N. (25 de Agosto de 2021). *"5 Steps to Better Cybersecurity Preparedness"*. Obtenido de https://www.information-age.com/5-steps-better-cybersecurity-preparedness-123496709/

Kim, P. (10 de febrero de 2021). *Reconnaissance in Cybersecurity: What It Is, Why It Matters, and How to Prevent It"*. Obtenido de https://securityboulevard.com/2021/02/reconnaissance-in-cybersecurity-what-it-is-why-it-matters-and-how-to-prevent-it/

Kleppmann, M. (2022). *Diseño de aplicaciones mediante el uso intensivo de datos.* España. Obtenido de https://www.google.com.ec/books/edition/Dise%C3%B1o_de_aplicaciones_mediante_el_uso/t3J6EAAAQBAJ?hl=es&gbpv=1&dq=lntegridad+Kleppmann,+2022&pg=PT761&printsec=frontcover

Lowe, R. G. (2017). *La seguridad informática es como el sexo seguro.* Madrid. Obtenido de https://www.google.com.ec/books/edition/La_seguridad_inform%C3%A1tica_es_como_el_sex/SfH0DAAAQBAJ?hl=es&gbpv=1&dq=seguridad+informatica+Lowe,+2017&pg=PT186&printsec=frontcover

Mahecha, L. H. (2022). *Auditoría Forense.* España. Obtenido de https://www.google.com.ec/books/edition/Auditor%C3%ADa_Forense/EvJ8EAAAQBAJ?hl=es&gbpv=1&dq=Ciberdelito++Mahecha,+2022&pg=PA187&printsec=frontcover

Martha Irene Romero Castro, G. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* España. Obtenido de https://www.google.com.ec/books/edition/INTRODUCCI%C3%93N_A_LA_SEGURIDAD_INFORM%C3%81TIC/5Z9yDwAAQBAJ?hl=es&gbpv=1&dq=s

eguridad+informatica+Martha+Romero+et+at.(2018)&pg=PA121&printsec=frontcover

Nguyen, N. H. (2018). *Manual esencial de seguridad cibernética en español.* España. Obtenido de https://www.google.com.ec/books/edition/Essential_Cyber_Security_Handbook_In_Spa/lUJKDwAAQBAJ?hl=es-419&gbpv=1&dq=phishing+que+es&printsec=frontcover

Rubenking, N. (17 de marzo de 2022). *What Is a Computer Virus? Definition, Types, Protection*. Obtenido de https://www.pcmag.com/encyclopedia/term/computer-virus

Santos, J. M. (2020). *Sistemas de información geográfica.* Madrid. Obtenido de https://www.google.com.ec/books/edition/SISTEMAS_DE_INFORMACI%C3%93N_GEOGR%C3%81FICA/xjbeDwAAQBAJ?hl=es&gbpv=0

Snyder, J. (01 de diciembre de 2021). *What is a Trojan Virus? Understanding Trojan Malware and How to Protect Against It*. Obtenido de https://www.businessinsider.com/what-is-a-trojan-virus

Yuri Diogenes, D. E. (2022). *Cybersecurity – Attack and Defense Strategies.* Madrid. Obtenido de https://www.google.com.ec/books/edition/Cybersecurity_Attack_and_Defense_Strateg/uQuMEAAAQBAJ?hl=es-419&gbpv=1&dq=Cobalt+Strike+que+es&pg=PA45&printsec=frontcover

ANEXO 1

ENCUESTAS

1. ¿Ha sufrido su empresa pérdidas de datos importantes debido a un ataque de malware?

SI ■ NO □

2. ¿Ha utilizado alguna vez la herramienta Cobalt Strike en su trabajo?

SI □ NO ■

3. ¿Ha recibido capacitación formal sobre el uso de la herramienta Cobalt Strike?

SI □ NO ■

4. ¿Ha notado algún comportamiento sospechoso en los sistemas de su empresa que podría indicar un posible ataque de malware?

SI ■ NO □

5. ¿Cree que la herramienta Cobalt Strike es necesaria para mantener la seguridad de su empresa?

SI ■ NO □

ANEXOS 2

OFICIO A EMPRESA

Babahoyo, 3 de abril del 2023

Magister

Eduardo Galeas Guijarro

DECANO DE LA FACULTAD DE ADMINISTRACIÒN FINANZAS E INFORMÀTICA

En su despacho.

Reciba un cordial saludo de quienes conformamos **PC SOLUCIONES QUE REALIZAMOS ACTIVIDADES DE MANTENIMIENTO Y REPARACIÒN DE MAQUINARIA DE INFORMÀTICA Y EQUIPO PERIFÉRICO CONEXO, VENTA AL POR MENOR DE COMPUTADORAS** de la ciudad de **BABAHOYO** provincia de **LOS RÌOS**

Por medio de la presente me dirijo a usted para comunicarle que se ha **AUTORIZADO** al estudiante **ENZO ALDAHIR TAMAQUIZA MORILLO** de la carrera de **SISTEMAS DE INFORMACION** de la Facultad de Administración Finanzas e Informática de la Universidad Técnica de Babahoyo para que realice el estudio de caso con el tema: **ANÀLISIS Y SIMULACIÒN DE ATAQUE DE MALWARE CON EL USO DE LA HERRAMIENTA COBALT STRIKE PARA LA EMPRESA PC SOLUCIONES,** el cual es requisito indispensable para poder titularse.

Sin otro particular me suscribo de usted

Atentamente

FRANCISCO JAVIER AVILES ARCOS

1716711435

pcsoluciones2005@hotmail.com . 0990640528

ANEXOS 3

OFICIO A DECANO

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD ADMINISTRACIÓN FINANZAS E INFORMÁTICA
DECANATO

Babahoyo, 03 de abril del 2023
D-FAFI-UTB-00177-2023

Ingeniero.
Francisco Avilés Arcos.
GERENTE GENERAL DE LA EMPRESA PC SOLUCIONES.
Ciudad. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El Señor, **TAMAQUIZA MURILLO ENZO ALDAHIR,** con cédula de identidad No. **120749698-3** Estudiante de la Carrera de SISTEMAS DE INFORMACIÓN, matriculado en el proceso de titulación en el periodo Diciembre 2022 – Mayo 2023, trabajo de titulación modalidad Estudio de Caso, previo a la obtención del grado académico profesional universitario de tercer nivel como Ingeniero en Sistemas de Información, solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar el Estudio de Caso, el cual titula: **"ANÁLISIS Y SIMULACIÓN DE ATAQUE DE MALWARE CON EL USO DE LA HERRAMIENTA COBALT STRIKE PARA LA EMPRESA PC SOLUCIONES".**

Atentamente,

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO

c.c: Archivo

Recibido
03/04/2023

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Ing. Marilyn Coloma Aguilar	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

ANEXOS 4

OFICIO AUTORIZACION DE EMPRESA

Babahoyo, 3 de abril del 2023

Sr(a)
FRANCISCO JAVTER AVILES ARCOS
GERENTE DE LA EMPRESA PC SOLUCIONES
En su despacho.

De mis consideraciones:

Yo: **TAMAQUIZA MURILLO ENZO ALDAHIR**, con cédula de identidad 120749698-3, estudiante de la Universidad Técnica de Babahoyo de la Facultad de Administración, finanzas e informática, carrera de **SISTEMAS DE INFORMACION**, matriculado(a) en el proceso de titulación periodo DICIEMBRE 2022 – ABRIL 2023, le solicito a usted de la manera más comedida se sirva autorizar a quien corresponda se proceda otorgarme el permiso respectivo para realizar mi estudio de caso denominado **ANÀLISIS Y SIMULACIÒN DE ATAQUE DE MALWARE CON EL USO DE LA HERRAMIENTA COBALT STRIKE PARA LA EMPRESA PC SOLUCIONES** ,el cual es requisito indispensable para poder titularme.

Esperando una respuesta favorable quedo de usted muy agradecido(a).

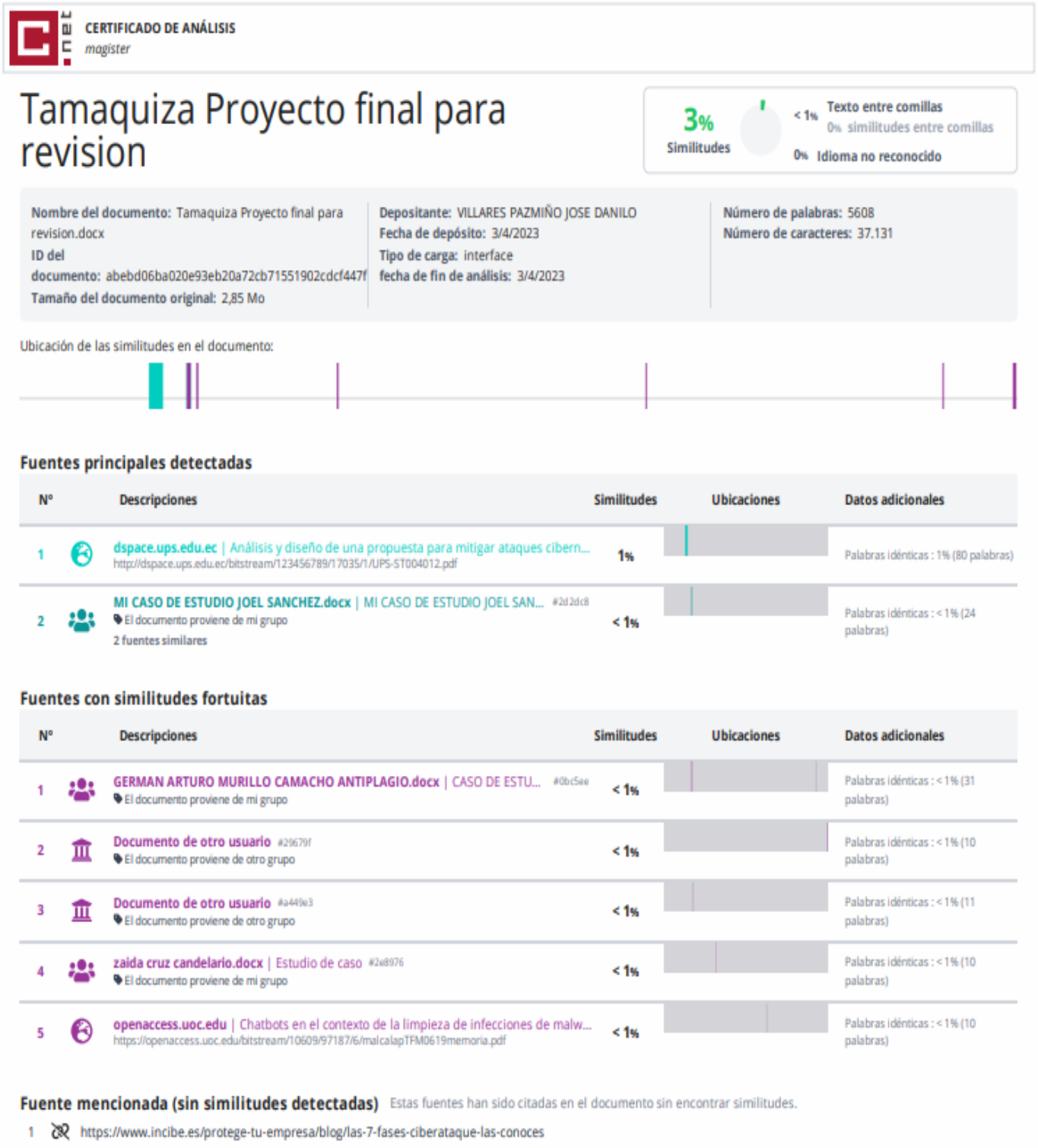
Muy atentamente

E——DAHIR TAMAQUIZA MURILLO
1207496983

Recibido
03/04/2023

ANEXOS 5

CERTIFICADO DE ANALISIS DE PLAGIO



CERTIFICADO DE ANÁLISIS
magister

Tamaquiza Proyecto final para revision

3% Similitudes
< 1% Texto entre comillas
0% similitudes entre comillas
0% Idioma no reconocido

Nombre del documento: Tamaquiza Proyecto final para revision.docx
ID del documento: abebd06ba020e93eb20a72cb71551902cdcf447f
Tamaño del documento original: 2,85 Mo

Depositante: VILLARES PAZMIÑO JOSE DANILO
Fecha de depósito: 3/4/2023
Tipo de carga: interface
fecha de fin de análisis: 3/4/2023

Número de palabras: 5608
Número de caracteres: 37.131

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.ups.edu.ec | Análisis y diseño de una propuesta para mitigar ataques cibern... http://dspace.ups.edu.ec/bitstream/123456789/17035/1/UPS-ST004012.pdf	1%		Palabras idénticas : 1% (80 palabras)
2	MI CASO DE ESTUDIO JOEL SANCHEZ.docx | MI CASO DE ESTUDIO JOEL SAN... #2d2dc8 El documento proviene de mi grupo 2 fuentes similares	< 1%		Palabras idénticas : < 1% (24 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	GERMAN ARTURO MURILLO CAMACHO ANTIPLAGIO.docx | CASO DE ESTU... #0bc5ee El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% (31 palabras)
2	Documento de otro usuario #29679f El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (10 palabras)
3	Documento de otro usuario #a449e3 El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (11 palabras)
4	zaida cruz candelario.docx | Estudio de caso #2e8976 El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% (10 palabras)
5	openaccess.uoc.edu | Chatbots en el contexto de la limpieza de infecciones de malw... https://openaccess.uoc.edu/bitstream/10609/97187/6/malcalapTFM0619memoria.pdf	< 1%		Palabras idénticas : < 1% (10 palabras)

Fuente mencionada (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces