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

ING. SERGIO ANDRÉS RODRIGUEZ RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ – COLOMBIA
2023

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

SERGIO ANDRÉS RODRIGUEZ RODRIGUEZ

INFORME TÉCNICO DEL SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM PARA OPTAR AL TÍTULO DE:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

MG. JOHN FREDDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ - COLOMBIA
2023

AGRADECIMIENTOS

Mi más profundo agradecimiento a mi familia, en especial a mi madre, quien, aunque ya no está a mi lado, sigue siendo mi fuente de inspiración y fortaleza. A mi novia, gracias por ser mi fuente de alegría y apoyo constante. Y a la universidad por proporcionarme las herramientas necesarias para alcanzar esta meta académica.

CONTENIDO

pág.

LISTA DE DIAGRAMAS

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

RESUMEN

Este documento constituye un informe técnico que resume los resultados alcanzados durante la ejecución de las tareas llevadas a cabo en el "Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team". Durante el proceso se abordó el escenario de una organización hipotética denominada 'HackerHouse', donde se llevó a cabo una evaluación exhaustiva de su infraestructura y necesidad de seguridad informática. Este análisis se basó en la implementación de la estrategia de equipos Red Team y Blue Team. Incluyendo un examen detallado del panorama tecnológico actual y una revisión de la legislación vigente en Colombia relacionada con la ciberseguridad.

Se abordan las capacidades técnicas, legales y de gestión esenciales para los equipos Blue Team y Red Team en el contexto de ciberseguridad en Colombia. Se enfatiza la importancia de la legislación colombiana en cuanto a protección de datos (Ley 1581 de 2012) y cómo los especialistas en seguridad deben cumplirlas durante pruebas de infraestructuras informáticas.

Se describen los roles y objetivos de los equipos Red Team y Blue Team, subrayando su colaboración para fortalecer la seguridad a través de pruebas simuladas de ataque y defensa. Se complementa esto con una investigación de las herramientas y técnicas clave para mejorar la seguridad en infraestructuras informáticas.

Se evalúa la necesidad de la implementación de profesionales y herramientas especializadas para abordar la creciente amenaza de ciberataques. Se presentan etapas clave y mejores prácticas, incluyendo consideraciones legales, pruebas de penetración y evaluación de los acuerdos necesarios para la realización de las mismas.

Finalmente se resalta la importancia de una cultura organizacional de mejora continua de la infraestructura y de las políticas de seguridad para garantizar la protección de la información y los sistemas de una organización, que debe darse articuladamente con auditorías y monitoreo constante para asegurar su implementación y mitigar los riesgos de ciberataques, para una protección integral tanto de la información de la organización como de sus clientes y colaboradores.

GLOSARIO

ANTIVIRUS: Programa informático diseñado con el propósito de reconocer, prevenir y erradicar virus, así como otros tipos de software perjudiciales, de un sistema informático o una red.

ATAQUE INFORMÁTICO: Es la acción de comprometer la integridad de la seguridad de un sistema o red informática, aprovechando las debilidades o vulnerabilidades presentes en el entorno digital.

CARGA ÚTIL (PAYLOAD): Parte de un malware o código malicioso que realiza una acción específica una vez que ha infectado un sistema objetivo. Puede incluir cualquier acción maliciosa diseñada para cumplir los objetivos del atacante.

CIBERDELINCUENTE: Individuo o grupo que participan en ataques cibernéticos, robo de datos, distribución de malware, fraude en línea y otras acciones maliciosas destinadas a causar daño, obtener ganancias ilegales o comprometer la seguridad de sistemas informáticos.

CIS (Center for Internet Security): Organización internacional de carácter no lucrativo enfocada en la Seguridad en Internet, cuya misión radica en la mejora de la seguridad cibernética a escala mundial.

COPNIA: Entidad colombiana que regula y supervisar la práctica profesional de la ingeniería.

CORTAFUEGOS (FIREWALL): Componente fundamental en la seguridad informática que opera como una barrera protectora entre diferentes redes, analizando el flujo de datos de la red con el objetivo de discernir si se debe permitir o denegar el acceso a los paquetes de datos.

EQUIPO AZUL (BLUE TEAM): Equipo de profesionales de ciberseguridad que se encarga de proteger la infraestructura tecnológica y los sistemas de una organización contra ataques cibernéticos. Trabaja en la implementación de medidas de seguridad, la detección de amenazas y la respuesta a incidentes.

EQUIPO ROJO (RED TEAM): Equipo de profesionales de ciberseguridad que realiza pruebas de penetración y simulaciones de ataques en una organización con el objetivo de identificar vulnerabilidades en la infraestructura y sistemas.

HACKING ÉTICO: Acto de probar la seguridad de sistemas o redes de manera autorizada y con el propósito de identificar vulnerabilidades.

INFRAESTRUCTURA: Se refiere al conjunto de componentes, recursos y sistemas necesarios para el funcionamiento de una organización o una red. En el contexto de la ciberseguridad, abarca servidores, redes, dispositivos, sistemas operativos y software utilizados para respaldar las operaciones de una organización.

INFORMACIÓN: Conjunto estructurado y procesado de datos digitales, organizados de manera sistemática y destinados a ser utilizados para diversos fines, como el almacenamiento, la comunicación, el procesamiento y la toma de decisiones en sistemas informáticos y tecnológicos.

INGRESO NO AUTORIZADO: Se refiere a entrar en un sistema informático o red sin el permiso adecuado, una acción ilegal que puede ser castigada por la ley.

MALWARE: Software malicioso desarrollado para dañar, controlar o tomar control de sistemas o redes informáticas.

MÁQUINA VIRTUAL (VIRTUAL MACHINE): Entorno de virtualización que permite ejecutar sistemas operativos dentro de un sistema host.

SEGURIDAD CIBERNÉTICA: Conjunto de enfoques y acciones implementados con el fin de resguardar sistemas y redes informáticas frente a posibles ataques y amenazas.

SOFTWARE ANTIVIRUS: Programa diseñado con la finalidad de detectar, prevenir y eliminar virus y otros programas dañinos de un sistema informático o una red.

TÉCNICA DE EXPLOTACIÓN (EXPLOIT): Código o técnica diseñada para aprovechar una vulnerabilidad específica en un sistema o aplicación con el fin de comprometer la seguridad y obtener acceso no autorizado o realizar acciones maliciosas.

VULNERABILIDAD: Punto débil dentro de un sistema que podría ser explotado por un atacante para poner en riesgo su seguridad y funcionamiento.

INTRODUCCIÓN

La evolución de las TIC ha democratizado el acceso a la información, pero también ha dado origen a un desafío crítico: la protección de los datos, tanto a nivel personal como empresarial. Para las organizaciones la protección de los datos es esencial, ya que estos pueden ser objeto de manipulación, robo y acceso ilegal, entre otros incidentes. Dependiendo de la naturaleza de la información, las consecuencias pueden ser perjudiciales para la empresa, su reputación y sus asociados. Por lo tanto, resulta imperativo implementar estrategias y sistemas de seguridad que aseguren los fundamentos de la confidencialidad, integridad y disponibilidad de la información.

Los ciberdelincuentes constantemente desarrollan formas de realizar actos delictivos, buscando innovar en las técnicas de ataque y explotar vulnerabilidades antes desconocidas. Por tanto, los expertos en seguridad informática requieren de capacitación constante y estrategias sólidas para enfrentar amenazas en constante evolución. En este contexto, una de las mejores formas de evaluar los distintos sistemas de seguridad de la organización, es realizar una prueba de intrusión o "pentesting". Esta práctica permite identificar posibles vulnerabilidades en la infraestructura informática para corregirlas antes de que un ciberdelincuente las aproveche.

Por lo tanto, si un grupo de expertos en seguridad informática está a punto de simular un ataque a una infraestructura, lo ideal es que haya otro preparado para combatir dicho ataque. A estos equipos se les conoce como "Red Team" y "Blue Team", o Equipo Rojo y Equipo Azul, respectivamente. En este trabajo se analizan en detalle las normativas legales (para el contexto colombiano), técnicas y herramientas utilizadas por estos equipos para poder analizar la infraestructura de las organizaciones y establecer las debidas acciones de respuesta.

OBJETIVOS

OBJETIVO GENERAL

Analizar la implementación de la estrategia de equipos rojos y azules en contexto de la seguridad de la información, evaluando su implementación por medio de un caso de estudio. Esto considerando el status tecnológico actual, la legislación vigente en Colombia y los requerimientos de herramientas y metodologías necesarios para fortalecer la seguridad en la gestión de información y la infraestructura informática de las organizaciones.

OBJETIVOS ESPECÍFICOS

- Identificar las características de los equipos de seguridad informática, incluyendo las funciones y responsabilidades del Equipo Rojo y el Equipo Azul.
- Analizar los principios legales y éticos en Colombia que rigen la labor de los profesionales de seguridad informática para asegurar su actuación autorizada, ética y legal.
- Diseñar y ejecutar pruebas de intrusión simuladas (pentesting) utilizando las metodologías y herramientas para la detección de vulnerabilidades.
- Desarrollar estrategias y medidas efectivas para responder a los ataques informáticos simulados por el Equipo Rojo, asegurando la protección de los datos.
- Elaborar un informe técnico de los resultados de las pruebas de intrusión, las acciones tomadas por el Equipo Azul y las recomendaciones para robustecer la seguridad.
- Formular conclusiones y recomendaciones que guíen la toma de decisiones en ciberseguridad dentro de las organizaciones.

1 MARCO TEÓRICO

1.1 CONCEPTUALIZACIÓN

Tanto la información como el volumen de la misma, así como la forma en que se almacena reproduce y transmite ha manifestado una evolución muy acelerada en las últimas décadas. Esta transformación constante destaca la importancia crítica de que las organizaciones, independientemente de su escalla desarrollen y apliquen estrategias efectivas de seguridad de la información. Estas estrategias se vuelven fundamentales en el diseño de acciones de respuesta para proteger los activos digitales, garantizar la privacidad de los datos y mantener la integridad y disponibilidad de la información en un entorno tecnológico en constante cambio.

A continuación, se presenta la descripción de algunos conceptos necesarios para comprender y abordar los desafíos actuales de la seguridad de la información dentro de una organización y establecer una base sólida para el contenido del informe técnico.

1.1.1 Análisis de Amenazas (Threat Intelligence)

El análisis de amenazas, se refiere a datos que contienen conocimientos detallados sobre las amenazas de ciberseguridad que apuntan a una organización. Este tipo de inteligencia de amenazas ayuda a los equipos de seguridad a ser más proactivos, permitiéndoles tomar acciones efectivas basadas en datos para prevenir ataques cibernéticos antes de que ocurran. Además, puede ayudar a una organización a detectar y responder de manera más efectiva a los ataques en curso.

Esto se logra al recopilar información sobre amenazas de múltiples fuentes. Para luego, correlacionar y analizan los datos para descubrir tendencias, patrones y relaciones que proporcionen una comprensión profunda de las amenazas potenciales. La inteligencia resultante es específica de la organización, se enfoca en las vulnerabilidades específicas de la organización y sus activos[1].

[1] IBM. What is threat intelligence? IBM [página web]. [Consultado el 23, septiembre, 2023]. Disponible en Internet: <https://www.ibm.com/topics/threat-intelligence>.

1.1.2 Ataque de Ingeniería Social

Es una táctica de manipulación psicológica utilizada por ciberdelincuentes para obtener información confidencial o acceso no autorizado a sistemas. A menudo, los atacantes se valen de la confianza, la persuasión o el engaño para manipular a las víctimas a revelar información sensible o realizar acciones que comprometen la seguridad. Estos ataques pueden incluir la suplantación de identidad, el phishing por correo electrónico, las llamadas telefónicas fraudulentas y la exploración de redes sociales para obtener información personal. La generación de conciencia, cultura y la educación en seguridad son cruciales para protegerse contra estos ataques, ya que incluso las defensas técnicas más sólidas pueden ser vulnerables si los usuarios son engañados[2].

1.1.3 Autenticación y Autorización

La autenticación y autorización son componentes esenciales en la gestión de acceso y control de seguridad de los sistemas y recursos de una organización. La autenticación se refiere al proceso de verificar la identidad de un usuario o entidad, generalmente a través de contraseñas, tarjetas inteligentes, huellas dactilares o autenticación de dos factores. Por otro lado, la autorización determina los derechos de acceso de un usuario autenticado, lo que significa que define qué recursos o datos puede utilizar el usuario y en qué medida. Estos dos conceptos trabajan juntos para garantizar que solo los usuarios autorizados tengan acceso a la información y los sistemas necesarios para realizar sus funciones. Una implementación adecuada de autenticación y autorización es fundamental para prevenir el acceso no autorizado y salvaguardar la confidencialidad y la integridad de los datos [3] [4].

---

[2] GRANGER, Sarah. Social engineering fundamentals. Symantec Enterprise [página web]. (18, diciembre, 2001). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=891b1f29-e2e7-4484-89c0-a2137ee82f8b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.

[3] OWASP. Authentication. OWASP Cheat Sheet Series [página web]. (2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html>.

[4] OWASP. Authorization. Introduction - OWASP Cheat Sheet Series [página web]. (2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html>.

1.1.4 Cumplimiento Normativo

El cumplimiento normativo en seguridad de la información se refiere al conjunto de reglas, regulaciones y estándares que las organizaciones deben seguir para garantizar que están aplicando prácticas de seguridad adecuadas y protegiendo los datos y la privacidad de sus clientes. Estos requisitos pueden variar según la industria y la ubicación geográfica de la organización. No cumplir con estas normativas puede resultar en sanciones legales y daños a la reputación de la organización[5].

1.1.5 Educación y Concienciación en Seguridad

La educación y concienciación en seguridad se refieren a programas y actividades diseñados para capacitar a los empleados y usuarios finales sobre las mejores prácticas de seguridad de la información y para crear conciencia sobre las amenazas cibernéticas. Esto incluye la formación en la identificación de correos electrónicos de phishing, el uso seguro de contraseñas, la protección de datos personales y la importancia de mantener el software actualizado. La capacitación constante es fundamental, ya que los empleados pueden ser un eslabón débil en la cadena de seguridad si no están bien informados. Un personal bien educado y consciente puede ayudar a prevenir ataques y proteger los activos digitales de una organización[6].

1.1.6 Peritaje Forense Digital

El peritaje forense digital es un proceso especializado que implica la recopilación, análisis y presentación de evidencia digital en casos legales o investigaciones de seguridad. Los peritos forenses digitales utilizan técnicas y herramientas para recuperar datos de dispositivos y sistemas, preservando la cadena de custodia y asegurando que la evidencia sea admisible en un tribunal. Este proceso se utiliza

[5] ISO27K. ISO/IEC 27001 certification standard. ISO27k infosec [página web]. (2022). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.iso27001security.com/html/27001.html>.

[6] OSTEC. ¿Qué es security awareness? OSTEC [página web]. (1, agosto, 2022). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://ostec.blog/es/aprendizaje-descubrimiento/que-es-security-awareness/>.

para investigar delitos informáticos, fraudes, brechas de seguridad y otros incidentes relacionados con la tecnología[7].

1.2 LA NECESIDAD DE LA CULTURA DE LA CIBERSEGURIDAD

La Cultura de Ciberseguridad en las organizaciones abarca una serie de elementos que incluyen el conocimiento, las creencias, las percepciones, las actitudes, las suposiciones, las normas y los valores que las personas poseen en relación con la ciberseguridad, y cómo estos influyen en su comportamiento cuando interactúan con las tecnologías de la información.

La necesidad de apropiar esta cultura radica en la integración de las consideraciones de seguridad de la información como un componente integral de las actividades diarias de los empleados, impregnando sus rutinas y conductas cotidianas. Al adoptar el enfoque adecuado para abordar la seguridad de la información, se puede evolucionar de manera orgánica a partir de las actitudes y conductas de los empleados en su relación con los activos de información en el entorno laboral.

Dado que los entornos empresariales están en constante evolución, las organizaciones deben mantener y ajustar de manera proactiva sus políticas en respuesta a las nuevas tecnologías, amenazas emergentes y cambios en sus objetivos, procesos y estructuras para poder garantizar la seguridad de su información.

1.3 LA ESTRATEGIA DE EQUIPOS ROJOS Y AZULES

1.3.1 ¿Qué es un Equipo Rojo (Red team)?

Un equipo rojo se compone de expertos en seguridad con un enfoque ofensivo. Estos profesionales están encargados de simular ataques a la infraestructura de una organización. El objetivo principal de su labor es evaluar la postura de seguridad de la organización desde la perspectiva de un atacante malintencionado. Para esto

[7] LOPEZ DELGADO, Miguel. Análisis forense digital [en línea]. 2a ed. Bogotá: MinTIC, 2007 [consultado el 23, septiembre, 2023]. 40 p. Disponible en Internet: <https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf>.

se utilizan tácticas y técnicas del mundo real para identificar vulnerabilidades y debilidades ya sean en sus políticas, tecnologías o su implementación.

Durante las simulaciones, actúan de manera similar al atacante, siguiendo un enfoque sistemático para identificar las vulnerabilidades y posibles puntos de explotación. Para proponer la metodología de ataque a usar en la simulación se evalúan tácticas y técnicas de ataque comúnmente utilizadas entre las que se incluye el pentesting, la ingeniería social y la explotación de vulnerabilidades[8].

1.3.2 ¿Qué es un Equipo azul (Blue team)?

Es un equipo de profesionales de seguridad de la información que se dedica a la defensa y respuesta contra los ataques simulados por el equipo rojo. Se encarga de proteger la infraestructura, identificar intrusiones y tomar medidas correctivas para fortalecer la seguridad de la organización. Su objetivo principal es garantizar que las defensas cibernéticas de la organización estén adecuadamente preparadas y sean efectivas en la detección y mitigación de ataques.

El equipo azul sigue una metodología centrada en la detección y respuesta. Se utilizan tecnologías avanzadas de monitoreo y análisis para detectar comportamientos anómalos y posibles señales de intrusiones. Además, se llevan a cabo análisis forenses y revisión de registros para comprender la naturaleza y el alcance de un ataque[9]. La colaboración cercana con el equipo rojo y la aplicación de los hallazgos obtenidos durante las simulaciones son elementos clave en su metodología.

1.3.3 Motivación para usar esta estrategia

El proceso de retroalimentación entre equipos rojos y azules facilita la mejora continua de las defensas cibernéticas. Las organizaciones pueden aprender de las tácticas utilizadas por los equipos rojos y ajustar sus estrategias y tecnologías de seguridad en consecuencia. Ya que los escenarios simulados son cercanos a las

[8] TECHTARGET. What is red teaming? WhatIs.com [página web]. (21, abril, 2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.techtarget.com/whatis/definition/red-teaming>.

[9] KEEPCODING. ¿Qué es blue team en ciberseguridad? KeepCoding Bootcamps [página web]. (2023). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/>.

amenazas del mundo real, proporcionan una visión precisa de la preparación de la organización para enfrentar ataques reales y permiten una mejor respuesta a incidentes cibernéticos reales de manera efectiva.

2 MARCO HISTÓRICO

2.1 ORIGEN Y EVOLUCIÓN DEL CONCEPTO

El concepto de los equipos Blue Team y Red Team encuentra sus raíces en el ámbito militar, donde se utilizaban para llevar a cabo ejercicios de guerra simulada[10].

Los equipos Blue Team originalmente se encargaban de defender activos críticos, como instalaciones militares y redes de comunicación, de los ataques simulados del equipo rojo. Estos ejercicios eran esenciales para evaluar la preparación y capacidad de defensa frente a posibles amenazas. A medida que la tecnología avanzaba, la idea de un equipo azul se trasladó al ámbito de la seguridad informática, donde su enfoque principal se centró en la prevención y respuesta a incidentes cibernéticos.

Por otro lado, el Red Team se encargaban de simular las tácticas del enemigo en ejercicios de guerra para poner a prueba la preparación y la capacidad de respuesta de las fuerzas armadas. Con el tiempo se convirtieron en grupos de profesionales altamente capacitados que llevaban a cabo ataques simulados contra sistemas y redes con el propósito de identificar vulnerabilidades y evaluar la seguridad de una organización.

2.2 EVOLUCIÓN EN EL ÁMBITO EMPRESARIAL

Con el aumento de las amenazas cibernéticas en las décadas de 1990 y 2000, las organizaciones empresariales comenzaron a reconocer la importancia de implementar estrategias y equipos especializados en seguridad informática[11].

Los Blue Team se centraron en la detección temprana de amenazas, la implementación de medidas de seguridad proactivas y la respuesta efectiva a incidentes. Los equipos Red Team se convirtieron en una parte esencial de las evaluaciones de seguridad para descubrir vulnerabilidades antes de que los actores maliciosos puedan aprovecharlas.

---

[10] ROUSE, Margaret. Equipo rojo-Equipo azul. KW Foundation [página web]. (10, diciembre, 2020). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://kwfoundation.org/blog/2020/12/10/equipo-rojo-equipo-azul/#htoc-red-team-the-network>.

[11] DIOGENES, Yuri y OZKAYA, Erdal. Cybersecurity – attack and defense strategies: infrastructure security with red team and blue team tactics. [s.l.]: Packt Publishing, 2018. 384 p. ISBN 9781788475297.

2.3 IMPORTANCIA ACTUAL

En la actualidad, los equipos Blue Team y Red Team desempeñan un papel crítico en la seguridad de la información. Los Blue Team trabajan constantemente para fortalecer las defensas cibernéticas de sus organizaciones, mientras que los Red Team evalúan proactivamente la seguridad y ayudan a cerrar las brechas antes de que los atacantes reales las exploten[12].

La colaboración entre estos equipos, conocida como "ejercicio de adversarios" o "pruebas de penetración controladas," se ha convertido en una práctica estándar para mejorar la postura de seguridad de la información de las organizaciones.

[12] Ibid.

3 MARCO LEGAL Y NORMATIVO

3.1 LA ISO 27001 Y SU RELEVANCIA

La ISO 27001 es un estándar para la administración segura de la información y para la creación de sistemas de gestión de seguridad de la Información (SGSI). Por medio de la definición de esta norma se diseña el conjunto de requisitos que deben tenerse en cuenta para implementar y mantener controles de seguridad sólidos[13] [14].

Esta ISO se basa en varios principios clave, incluyendo: la identificación y evaluación de riesgos, la implementación de medidas de seguridad adecuadas, la gestión de incidentes y la mejora continua.

3.2 LEGISLACIÓN COLOMBIANA EN DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS

La Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales, es la legislación vigente que garantiza la seguridad y privacidad de la información en el país. Establece las obligaciones y responsabilidades de las organizaciones e individuos en el manejo de datos personales y busca garantizar la privacidad y seguridad de la información[15].

Se define en esta legislación una serie de disposiciones y deberes para los responsables del tratamiento de los datos. Se incluye la obtención de consentimiento para la recopilación y procesamiento de datos personales, la implementación de medidas de seguridad adecuadas y la notificación de brechas de seguridad a las autoridades y a los afectados. Así como también las consecuencias legales que pueden incluir multas y otras medidas correctivas.

---

[13] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Seguridad de la información. ISO/IEC 27001. [s.l.]: ISO, 2013.

[14] NORMAS ISO. ISO 27001 - seguridad de la información: norma ISO IEC 27001/27002. Normas ISO [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.normas-iso.com/iso-27001/>.

[15] COLOMBIA. CONGRESO DE COLOMBIA. Ley 1581 [en línea]. (17, octubre, 2012) [consultado el 25, septiembre, 2023]. Disposiciones generales para la protección de datos personales. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

Por otro lado, la Ley 1273 de 2009, también conocida como la " Protección de la información y de los datos"[16] en Colombia, desempeña un papel fundamental en la regulación de la seguridad de la información y la persecución de delitos informáticos en el país. Esta legislación establece un marco jurídico para la protección de datos personales y la prevención de actividades ilegales en el entorno digital. La Ley 1273 de 2009 aborda aspectos clave relacionados con la seguridad de la información y establece sanciones para delitos cibernéticos, lo que la convierte en un componente esencial para garantizar la integridad y la legalidad en el manejo de datos y sistemas informáticos en Colombia.

3.3 EL COPNIA

El Colegio Profesional Nacional de Ingenieros de Colombia (COPNIA) juega un papel fundamental en la vigilancia del accionar ético para ingenieros entre ellos los asociados al contexto de la seguridad informática. Como entidad reguladora avalada por el gobierno colombiano establece estándares éticos y profesionales que los ingenieros deben seguir al desempeñar sus funciones y define las sanciones a las cuales se pueden someter.

El papel del COPNIA en el ejercicio de los profesionales de la seguridad informática es fundamental, ya que garantiza que los ingenieros involucrados en la protección de sistemas y datos operen de manera ética y responsable. Los estándares definidos en el código de ética[17] ayudan a mantener la confianza de los ciudadanos en la profesión de ingeniería y en la seguridad de sus datos personales en un entorno tecnológico en constante evolución.

[16] COLOMBIA. CONGRESO DE COLOMBIA. Ley 1273. (5, enero, 2009). De la Protección de la información y de los datos.
[17] COPNIA. Código de ética |. COPNIA [página web]. (2023). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

4 CASO DE ESTUDIO

4.1 HACKERHOUSE: ORGANIZACIÓN EN SEGURIDAD INFORMÁTICA (CASO TEÓRICO)

HackerHouse es una destacada organización especializada en ciberseguridad e investigación en seguridad informática (Este es un caso teórico y solamente corresponde a una entidad ficticia). Su compromiso con la formación, capacitación y desarrollo de profesionales en este campo la ha convertido en un referente en la industria de la seguridad digital. La organización tiene su sede en Colombia y ha ganado reconocimiento internacional por su enfoque innovador y sus soluciones avanzadas en ciberseguridad.

4.2 SITUACIÓN PROBLEMA: MONTAJE DEL BANCO DE TRABAJO

Se requiere la creación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de HackerHouse. El banco de trabajo y las herramientas de software utilizadas a lo largo del proceso deben estar basadas en alternativas de software de código abierto.

4.3 ANÁLISIS LEGAL Y ÉTICO

Dada la importancia de la ética y el cumplimiento legal en el campo de la ciberseguridad, se da la necesidad de garantizar que sus prácticas y acuerdos estén en línea con los estándares éticos y legales. Esto incluye la elaboración y revisión de acuerdos de confidencialidad y la comprensión de los aspectos legales involucrados en la contratación de profesionales en seguridad informática.

4.4 ANÁLISIS TÉCNICO DEL RED TEAM

El análisis técnico es fundamental para comprender y abordar los desafíos de seguridad informática. HackerHouse, en su enfoque en equipos Red Team, se enfrenta a la necesidad de analizar escenarios específicos de seguridad y comprender cómo se llevan a cabo ataques informáticos. Por tanto, se plantea el siguiente escenario problemático:

“Se encontró que uno de los equipos de cómputo que contenía un Windows 10 x64 fue vulnerado de algún modo. El administrador de dicho equipo se percató de la presencia de un archivo inusual y sospechoso en el sistema. Esto plantea preguntas sobre cómo se realizó el ataque y cuáles fueron las técnicas utilizadas.”

4.5 ANÁLISIS TÉCNICO DEL BLUE TEAM

El análisis del equipo Blue Team es igualmente crucial para la detección y mitigación de amenazas cibernéticas. Se necesita contar con profesionales capaces de asegurar y proteger sus sistemas contra ataques informáticos. A este respecto se presenta la necesidad de tomar medidas respecto al ataque sufrido en el equipo Windows. El objetivo del equipo es por tanto el asegurar la máquina afectada y documentar el proceso utilizado para contener y eliminar la amenaza.

INFORME TÉCNICO

5 ETAPA 1: CONCEPTOS DE EQUIPOS DE SEGURIDAD Y CREACIÓN DEL BANCO DE PRUEBAS

En el ***marco legal y normativo*** previamente presentado se realizó una descripción detallada del contexto legal relacionado con los delitos informáticos en Colombia, centrándonos en la Ley 1273 de 2009 y la Ley 1581 de 2012. A continuación, se profundiza en la aplicación y las implicaciones prácticas de esta legislación en el caso de estudio.

5.1 DELITOS INFORMÁTICOS EN COLOMBIA, ANÁLISIS DEL MARCO LEGAL.

Como parte de la constante evolución mundo digital del siglo XXI, los delitos informáticos se han convertido en una preocupación creciente para gobiernos, empresas y ciudadanos por igual. Colombia no es una excepción. Se explora el panorama legal del país, se analizará la ley 1273 de 2009 y ley 1581 de 2012 así como su relevancia en la prevención y persecución de delitos informáticos. Se examina a continuación las disposiciones clave de esta legislación, las sanciones asociadas a los delitos cibernéticos y su impacto en la lucha contra el crimen en asociados a la seguridad digital. Como resultado de este análisis se destacarán los desafíos y oportunidades que enfrenta Colombia en la protección de su infraestructura digital y en la promoción de un ambiente en línea seguro y confiable.

5.2 DELITOS INFORMÁTICOS (LEY 1273 DE 2009)

La Ley 1273 de 2009, también conocida como la "Ley de Delitos Informáticos y Protección de Datos Personales" en Colombia. Aborda dos aspectos vitales para la sociedad digital: la protección de la información personal y la persecución de delitos informáticos. En primer lugar, la ley establece un marco jurídico sólido para la protección de datos personales, garantizando que los ciudadanos tengan control sobre su información y que esta sea tratada de manera ética y segura.

En cuanto a las penalizaciones se incluyen las sanciones acciones como el acceso no autorizado a sistemas informáticos, la difusión de programas maliciosos y la suplantación de identidad en línea. Si bien estas normas se cubren la mayoría de necesidades legales la implementación efectiva ha enfrentado desafíos, incluida la necesidad de fortalecer las capacidades de investigación y enjuiciamiento de delitos cibernéticos. Razón por la cual esta ley es importante para demarcar las responsabilidades legales de los profesionales de la seguridad de la información y las organizaciones.

5.3 PROTECCIÓN DE DATOS LEY 1581 DE 2012

En la Ley 1581 de 2012 se define la regulación de la privacidad y la gestión de la información personal en el Colombia. Esta legislación es esencial en un mundo donde la información personal se ha vuelto un activo valioso y su protección es fundamental para los derechos individuales y la confianza en las actividades en línea.

El objetivo principal de esta ley es otorgar a los ciudadanos el control sobre sus datos personales y establecer pautas claras para su recolección, tratamiento, almacenamiento y circulación. Esto se logra a través de la definición de principios clave, como el consentimiento informado, la finalidad legítima, la veracidad y calidad de la información, y la seguridad en el manejo de los datos. Adicionalmente establece la obligación de implementar políticas y procedimientos internos para el adecuado tratamiento de datos por parte de las organizaciones, así como la notificación de brechas de seguridad en caso de ser necesario.

Es de resaltar la figura del 'responsable del tratamiento', quien debe garantizar el cumplimiento de estas disposiciones y de responder a las solicitudes de los titulares de datos. Debido a la continua evolución de la tecnología y el crecimiento de la economía digital es importante como organización y como profesionales tener en cuenta su adecuado cumplimiento para evitar sanciones.

5.4 QUÉ ES PENTESTING

Es un ataque simulado autorizado realizado en un sistema informático para evaluar su seguridad. Durante el proceso de Pentesting los profesionales de seguridad utilizan las mismas herramientas, técnicas y procesos que los atacantes para identificar y demostrar los impactos de las debilidades en un sistema. Estas pruebas de penetración suelen simular diversos tipos de ataques que podrían representar una amenaza para una empresa.

Se puede evaluar si un sistema es lo suficientemente robusto como para resistir ataques desde posiciones autenticadas y no autenticadas, así como desde una variedad de roles en el sistema. Con el alcance adecuado, una prueba de penetración puede explorar cualquier aspecto de un sistema de información[18].

[18] SYNOPSYS EDA TOOLS. What is penetration testing and how does it work? Synopsys [página web]. (2023). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.synopsys.com/glossary/what-is-penetration-testing.html>.

5.5 ETAPAS DEL PENTESTING Y EL PROCESO DE RECONOCIMIENTO (FOOTPRINTING)

5.5.1 Reconocimiento (Footprinting)

Se recopila información sobre el objetivo, como direcciones IP, nombres de dominio, subdominios y detalles de la red. El propósito principal es obtener una visión general del entorno que se va a atacar antes de avanzar en el proceso.

5.5.2 Enumeración

Se identifican activos específicos dentro de la red, tales como sistemas, servicios y usuarios. Se emplean herramientas y técnicas para obtener información adicional sobre los activos identificados durante la etapa de reconocimiento.

5.5.3 Detección

Se llevan a cabo escaneos y análisis de seguridad para identificar vulnerabilidades en los sistemas y servicios. Se utilizan tanto herramientas automatizadas como técnicas manuales para evaluar las posibles debilidades.

5.5.4 Explotación

Una vez identificadas las vulnerabilidades, se intenta explotarlas con el fin de obtener acceso no autorizado o elevar los privilegios. Esto implica la utilización de exploits y técnicas de penetración para comprometer los sistemas vulnerables.

5.5.5 Análisis de Resultados

Se evalúan los resultados obtenidos en las fases anteriores para comprender el posible impacto de las vulnerabilidades explotadas y las rutas de ataque utilizadas.

5.5.6 Documentación

Finalmente se registran las vulnerabilidades identificadas y las recomendaciones para mitigar los riesgos. Este informe se presenta a la organización con el fin de que pueda tomar medidas correctivas.

5.6 LA IMPORTANCIA DE LA ETAPA DEL RECONOCIMIENTO (FOOTPRINTING)

El reconocimiento desempeña un papel esencial en la identificación de posibles vulnerabilidades y puntos débiles que se pueden explotar durante las pruebas de penetración, lo que ayuda a las empresas a asegurar sus sistemas de TI y su infraestructura antes de que los actores de amenazas puedan aprovechar una vulnerabilidad. Además, permite a las organizaciones comprender mejor su postura de seguridad actual y construir una base de datos de vulnerabilidades conocidas que puede ser una referencia clave en auditorías de seguridad.

La información obtenida en la fase de reconocimiento proporciona una visión detallada del entorno objetivo, incluyendo su topología, sistemas operativos, servicios en ejecución y posibles puntos de acceso[19]. Esta visión integral es fundamental para planificar y ejecutar de manera efectiva las fases posteriores del pentesting. Al comprender la exposición inicial de la red y los sistemas, los profesionales de ciberseguridad y las organizaciones pueden adaptar sus estrategias y enfoques para maximizar la eficacia del pentesting.

5.7 METASPLOIT COMO PLATAFORMA Y HERRAMIENTA DE SEGURIDAD DE CÓDIGO ABIERTO

5.7.1 ¿Qué es?

Es una plataforma de software de código abierto ampliamente reconocida en la comunidad de profesionales de seguridad informática. Se trata de una herramienta integral que brinda a los expertos en seguridad las capacidades necesarias para identificar, explorar y abordar vulnerabilidades en sistemas y aplicaciones de manera efectiva. Metasploit facilita la realización de pruebas de penetración, el descubrimiento de debilidades en entornos informáticos, y el desarrollo de soluciones de seguridad robustas, desempeñando un papel crucial en la mejora de la seguridad de sistemas y redes[20].

[19] ZOLA, Andrew. What is footprinting in ethical hacking? Techtarget [página web]. (23, noviembre, 2021). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.techtarget.com/searchsecurity/definition/footprinting>.

[20] CHIROU, Álvaro. Metasploit: la herramienta definitiva para pruebas de seguridad. Achirou [página web]. (9, julio, 2023). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://achirou.com/metasploit-la-herramienta-definitiva-para-pruebas-de-seguridad/>.

5.7.2 Utilidad para los profesionales de seguridad de la información

Para los profesionales dedicados a la seguridad de la información Metasploit ofrece una extensa variedad de módulos y exploits que permiten realizar pruebas de penetración, señalar debilidades en sistemas y aplicaciones, y diseñar soluciones de seguridad más efectivas. Sin embargo, su utilidad va más allá de la mera exploración de vulnerabilidades, ya que también desempeña un papel importante en la formación y capacitación en el ámbito de la seguridad informática.
La plataforma permite adquirir experiencia práctica en la identificación y mitigación de amenazas, lo que contribuye al fortalecimiento de la postura de seguridad de las organizaciones.

5.8 CVE - IDENTIFICACIÓN Y MITIGACIÓN DE VULNERABILIDADES

5.8.1 ¿Qué es un CVE?

CVE (Common Vulnerabilities and Exposures) es un sistema de enumeración y catalogación de vulnerabilidades de seguridad informática que desempeña un papel fundamental en el ámbito de la ciberseguridad. Este sistema, de alcance global, proporciona identificadores únicos y estandarizados para cada vulnerabilidad detectada, permitiendo una comunicación clara y eficiente entre profesionales de seguridad, fabricantes de software y organizaciones[21].

5.8.2 Cual es su importancia

Para los profesionales de seguridad de la información, CVE representa una herramienta esencial en su arsenal. Permite mantenerse al tanto de las últimas vulnerabilidades identificadas en software, sistemas operativos y aplicaciones, lo que es crucial para tomar medidas proactivas.

Para las organizaciones, los CVE desempeñan un papel crucial en la protección de sus activos digitales al permitir una gestión proactiva de amenazas y una planificación estratégica de seguridad. Además, contribuye al cumplimiento normativo al proporcionar la información necesaria para aplicar parches de seguridad, lo que evita posibles sanciones. Asimismo, la información de los CVE respalda la identificación de vulnerabilidades y por tanto tomar acciones preventivas para la protección de la reputación de la organización y facilitar una respuesta eficiente a las vulnerabilidades, minimizando el riesgo de brechas de seguridad y pérdida de datos.

[21] RED HAT SOFTWARE. What is a CVE? Red Hat [página web]. (25, noviembre, 2021). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.redhat.com/en/topics/security/what-is-cve>.

5.9 CREACIÓN DEL BANCO DE TRABAJO

Para la ejecución de las pruebas necesarias se crea un banco de trabajo compuesto de dos máquinas virtuales conectadas por NAT, estas máquinas corresponden a una maquina atacante (Kali Linux) y una maquina victima (Windows 10) se aprovecha la conexión entre estos dos dispositivos para realizar las etapas de análisis del caso.

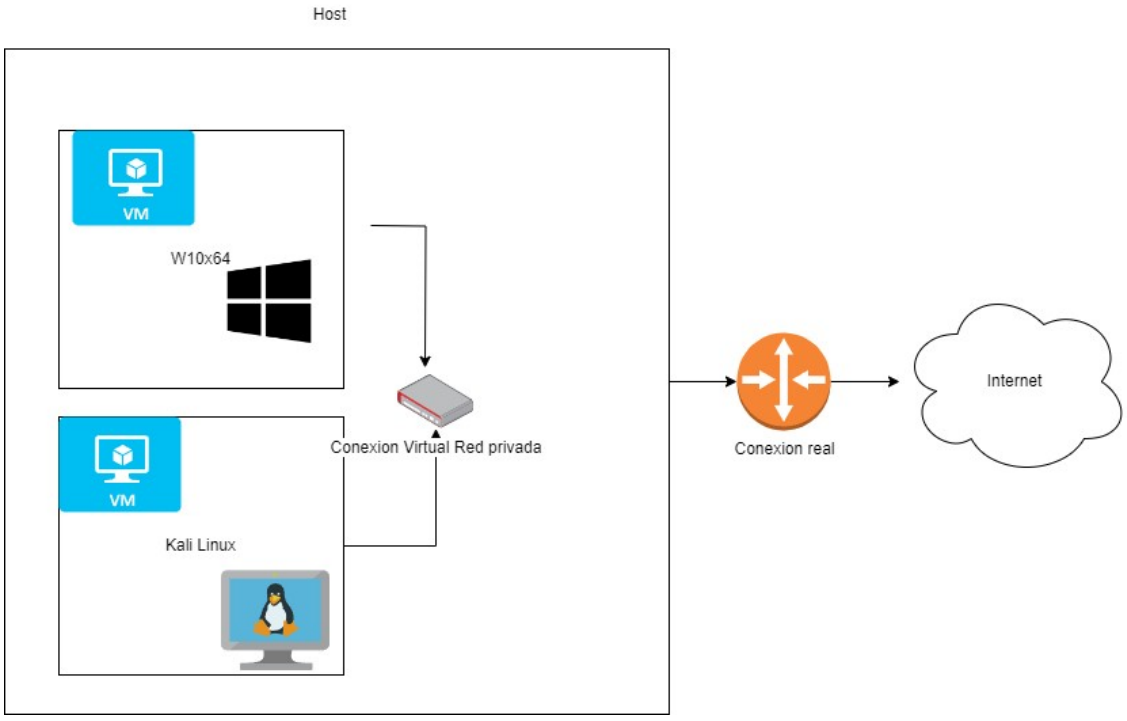

Diagrama 1. Arquitectura del banco de prueba. Fuente: Elaboración propia.

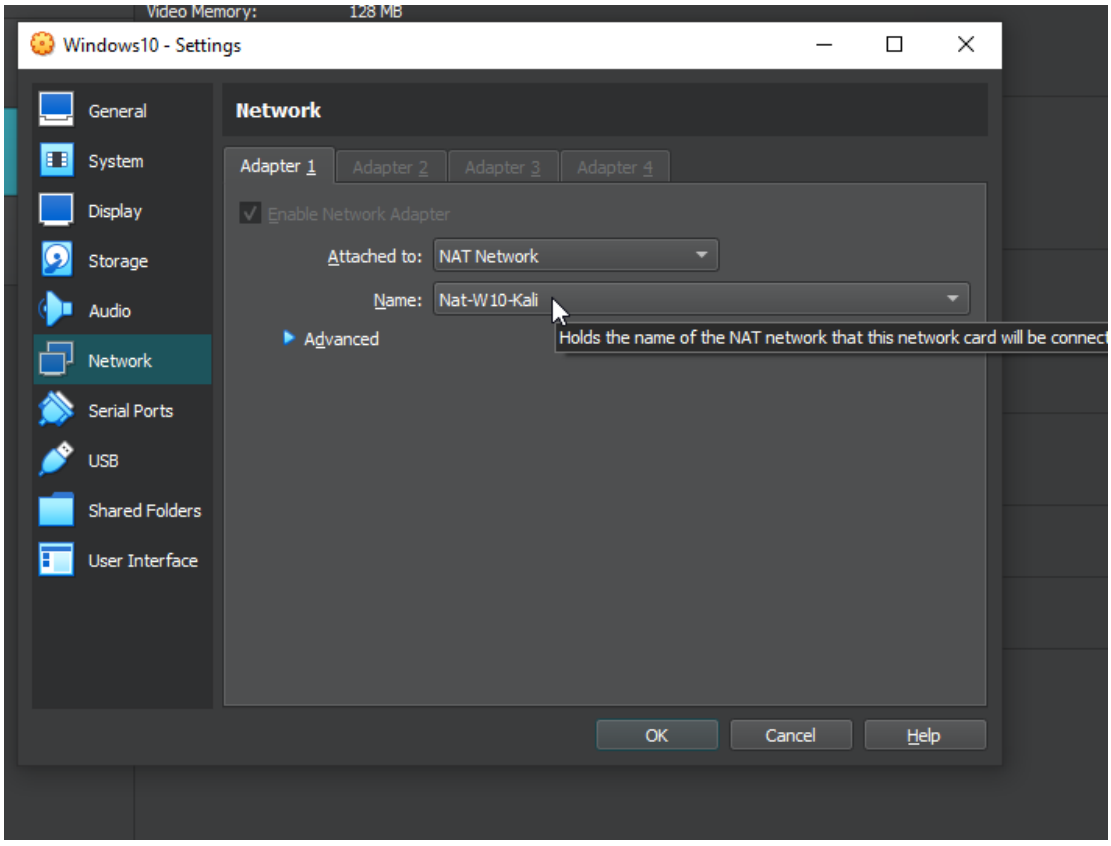

Ilustración 1. Configuración de la red en la VM Windows. Fuente: Elaboración propia.

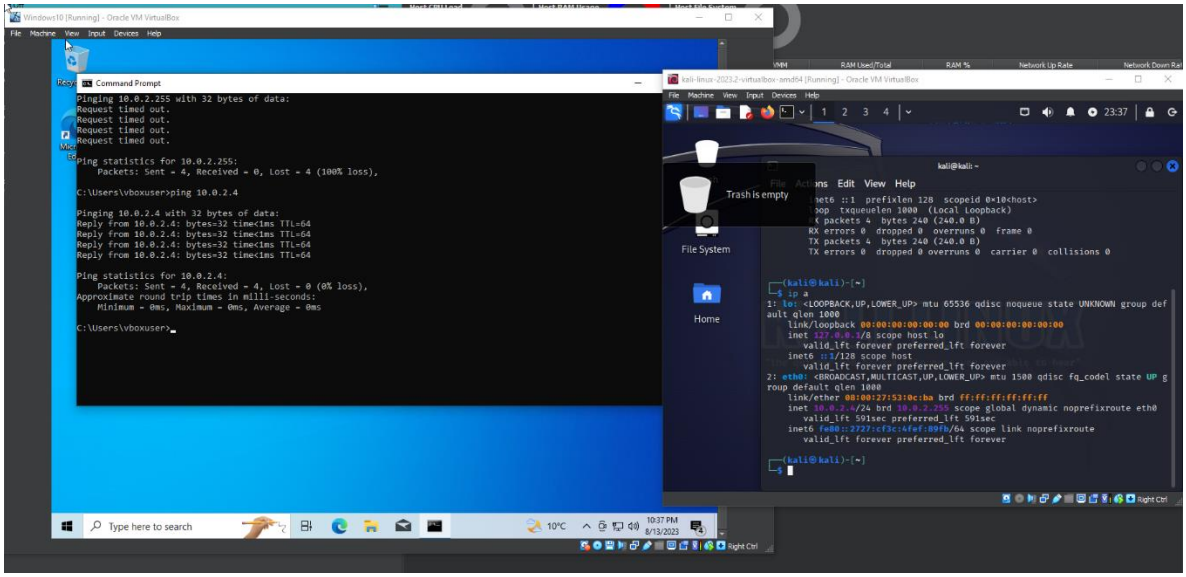

Ilustración 2. Ping para auditar la conexión entre las dos máquinas. Fuente: Elaboración propia.

6 ETAPA 2: ANÁLISIS DE CUMPLIMIENTO ÉTICO Y JURÍDICO

6.1 EVALUACIÓN LEGAL Y ÉTICA DEL ACUERDO DE CONFIDENCIALIDAD

En el documento propuesto como acuerdo de confidencialidad se encuentran detalles altamente sospechosos ya que se presenta una gran cantidad de irregularidades puntuales. A continuación, se presentan las anomalías encontradas por cada clausula citando el documento original.

6.1.1 Clausula 2: Información con origen confidencial y acceso a datos privados sin la autorización debida

Incluye términos como:

> *"datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos"* [22]

En este punto existe la oportunidad de incurrir en actividades ilegales o poco éticas. Esto se convierte en un riesgo legal de aceptar información de origen no legítimo, al aceptarla se abre la oportunidad de ser cómplice en un delito.

6.1.2 Clausula 3: Origen ilegal de la información

Si bien la mayor parte de la cláusula incluye decisiones legitimas tales como la protección intelectual de datos es altamente sospechosa la mención de:

> *"transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos"*[2]

En esta cláusula se requiere de un mejor detalle del origen de la información ya que podría incluir un amplio grupo de formas de comunicación, incluyendo posiblemente medios ilícitos o ilegales. Por tanto, el origen de la los datos a manipular debe ser explícitamente indicado en las cláusulas del acuerdo de confidencialidad.

6.1.3 Clausula 4: Inclusión de obligaciones ilegales como responsabilidad laboral

Esta cláusula contiene las repercusiones legales más delicadas de todo el documento, aunque la organización tiene el derecho a la confidencialidad tanto en sus datos como en sus procedimientos los demás detalles abren la puerta a acciones ilegales y pueden comprometer al profesional de seguridad a aceptar acciones ilícitas.

---

[22] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN. Guía de actividades y rúbrica de evaluación – Etapa 2 Actuación ética y legal - Anexo 3: ACUERDO DE CONFIDENCIALIDAD. Bogotá: UNAD, 2023. 12 p. Guia de trabajo.

6.1.3.1 1.3.1 Numeral dos

> *´´Proteger la información confidencial, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba´´*[23]

Nuevamente como en la segunda clausula se está mencionando información de dudosa procedencia que no se encuentra claramente descrito su origen.

6.1.3.2 1.3.2 Numeral tres

´´No denunciar ante las autoridades actividades sospechosas´´[24]

Esta cláusula es supremamente grave, se está comprometiendo confidencialidad de información ilegal por lo que de aceptarla como profesional directamente se estaría aceptando complicidad en la participación de delitos al actuar como colaborador de la organización encubriendo la existencia de información altamente ilegal.

6.1.3.3 1.3.3 Numeral cuatro

> *´´Responder por el mal uso que le den sus representantes a la información confidencial´´*[25]

En esta cláusula se está comprometiendo al profesional a responder legalmente por la información y por los delitos asociados a la misma, por lo tanto, aceptar esta cláusula es equivalente a tomar el compromiso de la entidad HackerHouse haciendo responsable de las consecuencias legales.

6.1.3.4 1.3.4 Numeral cinco

> *´´La parte receptora se obliga a no transmitir… la información confidencial o* ***ilegal*** *sin el previo consentimiento´´*[26]

En esta cláusula nuevamente se está aceptando complicidad en las acciones ilegales de la organización y aceptando también la responsabilidad de proteger información ilegal al aceptar la necesidad de un consentimiento de la entidad sobre las instituciones legales.

6.1.4 Clausula 7: inexistente

Las cláusulas saltan directamente de la sexta a la octava lo que puede indicar alguna irregular en el contrato, al no estar incluida la cláusula número siete es posible que se

[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ibid

esté aceptando una condición adicional potencialmente ilegal que no está incluida en el documento presentado.

6.1.5 Clausula 8: Adiciones a la ilegalidad de la información y a su manejo

> *´´En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado´´*[27]

Se indica que el profesional debe acudir a un abogado privado y proteger de responsabilidad legal a HackerHouse esto sería equivalente a comprometerse a evitar la responsabilidad de la empresa en caso de actividades ilegales.

6.2 ANÁLISIS DE LAS CLÁUSULAS DEL DOCUMENTO EN COMPARACIÓN CON LA LEY EN COLOMBIA.

Tomando en cuenta los resultados que obtuvimos de la evaluación del documento de confidencialidad se procede a evaluar los puntos sospechosos encontrados comparándolos contra la legislación colombiana vigente a de septiembre de 2023 para poder indicar puntualmente en que se estaría trasgrediendo la ley de aceptarlo.

6.2.1 Clausula 2: Información ilegalmente obtenida de origen confidencial

Esta cláusula sería ilegal ante la **ley 1273 de 2009** ya que afecta la protección de datos al incluir la existencia de información de datos con orígenes ilegales. En el artículo 269A, del capítulo dos de esta ley se menciona penas de prisión o económicas por este tipo de obtención ilegal de la información.

Ya que esta información de terceros es obtenida de forma ilegal también se aplicaría el articulo 269C ya que siendo una entidad privada sin demostrar una orden judicial no podría hacer la captación de este tipo de información.

6.2.2 Clausula 3: Origen ilegal de la información

Esta cláusula sería ilegal ante la **ley 1581 de 2012**

> *TÍTULO II PRINCIPIOS RECTORES*
> *h) Principio de confidencialidad*

En este título, en el numeral h se menciona explícitamente la obligación de responder por la confidencialidad de la información, debido a que no existe una autorización para poseer la data, se estaría incurriendo en un delito[28].

---

[27] Ibid

[28] COLOMBIA. CONGRESO DE COLOMBIA. Ley 1581 [en línea]. (17, octubre, 2012) [consultado el 25, septiembre, 2023]. Disposiciones generales para la protección de datos personales. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

6.2.3 Clausula 4: Asumir obligaciones ilegales de responsabilidad

Esta es la cláusula más crítica de todo el contrato y es ilegal ante la **ley 1273 de 2009** ya que afecta la protección de datos, la **ley 1581 de 2012,** también por la protección de datos y la **ley 1480 de 2011** que si bien se enfoca en el consumidor aplica también el manejo de cláusulas abusivas en contratos.

De la **ley 1273 de 2009** se aplicarían:

- Artículo 269A: Acceso abusivo a un sistema informático.
- *Artículo 269C: Interceptación de datos informáticos.*
- *Artículo 269F: Violación de datos personales.*

Nuevamente se menciona la existencia de información ilegal y su responsabilidad en el manejo de estos datos personales adquiridos de forma ilícita.

De la **ley 1581 de 2012** se aplicarían:

- *TÍTULO II PRINCIPIOS RECTORES*
  - *f) Principio de acceso y circulación restringida*
  - *h) Principio de confidencialidad*
- *TÍTULO III*
- *CATEGORÍAS ESPECIALES DE DATOS*
  - *Artículo 5°. Datos sensibles.12*
  - *Artículo 6°. Tratamiento de datos sensibles.13*

Si se tiene conocimiento de actividades ilegales, se está en la obligación de informar a las autoridades, al restringir esta acción se estaría interfiriendo con la obligación legal de informar actividades ilícitas. Al prohibir la divulgación de información ilegal sin importar las circunstancias se utilizaría el contrato para encubrir actividades ilegales.

De la **ley 1480 de 2011** se aplicaría

- *TÍTULO II*
- *PRINCIPIOS RECTORES*
- *Artículo 4°. Principios para el Tratamiento de datos personales.*

Dentro de este título se define el tratamiento de los datos sensibles, al solicitarse la aceptación de proteger información adquirida con un origen ilegal esta clausura haría invalido el documento porque está solicitando una acción que no puede ser aceptada de forma legal.

6.3 ANÁLISIS DEL DOCUMENTO DE CONFIDENCIALIDAD ANTE EL CÓDIGO DE ÉTICA PROFESIONAL DEL COPNIA

6.3.1 Revisión del documento ante el código de ética

No aceptaría el contrato independientemente de la suma de dinero ofrecida en el mismo, ya que este contrato llevaría potencialmente no solo a las consecuencias legales mencionadas anteriormente, sino que ante el código de ética profesional de COPNIA entraría directamente en conflicto con el ejercicio de mi profesión.

Si bien las acciones potenciales de aceptar este contrato entrar en conflicto con la mayor parte del código, puntualmente mencionaría dos de los artículos de mayor impacto para el caso.

6.3.1.1 Artículo 31. deberes generales de los profesionales

En este artículo se describe la importancia de la protección de los bienes por parte del profesional, para este caso específico hablaríamos de la apropiación de información y el manejo que se le da a esta. Ya que el contrato menciona la protección de datos indebidos se estaría actuando en contra del código[29].

6.3.1.2 Artículo 32. prohibiciones generales a los profesionales

Aquí se mencionan los límites legales de las acciones como profesional vigilado por el COPNIA puntualmente:

> *b) Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley[30]*

Al estar tolerando el ejercicio profesional conociendo que la información manejada es potencialmente ilegal se estaría también actuando en contra y por lo tanto podría haber una suspensión.

---

[29] COPNIA. Código de ética |. Copnia [página web]. (2023). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.
[30] Ibid.

6.3.2 Opinión del comportamiento ético como profesional

Si bien no es posible establecer el impacto de las consecuencias legales de aceptar este contrato de confidencialidad, si es posible conocer el riesgo al cual se estaría exponiendo. Considero que no solamente es un riesgo legal al exponerse tanto a sanciones económicas como potencialmente cárcel. O ético, que podría llevar incluso hasta a la suspensión de la licencia.

También a estas preocupaciones sería importante añadirles que el objetivo del estudio de una profesión como la ingeniería y especialmente al desempeñarse en un área donde el acceso a la información sensible es parte de nuestra labor el actuar de forma poco ética no solamente nos impactaría como personas profesionales, sino que afectaría em general al resto de la comunidad de la ingeniera al dar un pobre ejemplo de responsabilidad y de cumplimiento ético.

7 ETAPA 3: EQUIPO ROJO - EJECUCIÓN DEL LABORATORIO DE PRUEBAS DE PENETRACIÓN (PENTESTING) PARA LA SEGURIDAD OFENSIVA

Para analizar el escenario del caso de la vulnerabilidad encontrada en HackerHouse, se plantea la elaboración de un escenario de laboratorio que replica la situación presentada en un ambiente controlado de forma que sea posible establecer como el atacante llegó a la explotación de la vulnerabilidad documentando las herramientas y procesos necesarios. A continuación, se describe la metodología propuesta para el desarrollo del laboratorio basado en la metodología publicada por Triaxom Security[31].

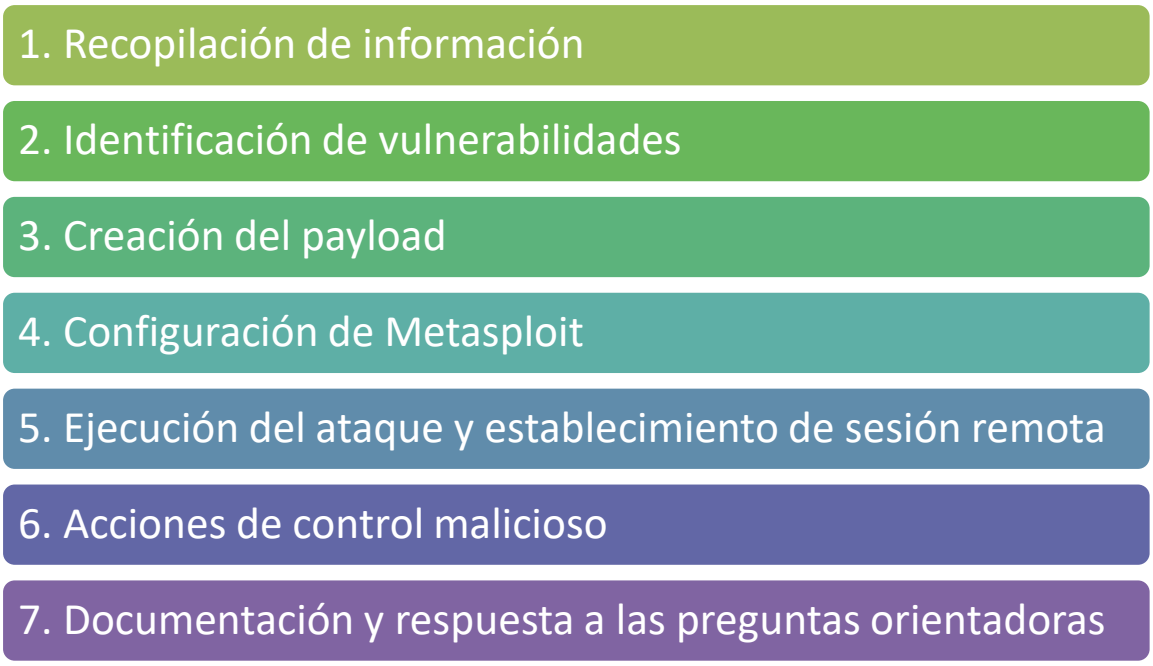

Diagrama 2. Metodología propuesta para el análisis del caso HackerHouse. Fuente: Elaboración propia

[31] MILLER, Matt. Penetration testing methodology. Triaxiom Security [página web]. (14, junio, 2018). [Consultado el 28, septiembre, 2023]. Disponible en Internet: <https://www.triaxiomsecurity.com/our-internal-penetration-testing-methodology/>.

7.1 EJECUCIÓN DE LA PRUEBA DE PENETRACIÓN Y DOCUMENTACIÓN

7.1.1 Recopilación de información

Se obtiene información sobre la máquina como lo puede hacer el atacante, incluyendo sistema operativo, configuración, IP, usuarios, servicios y datos relevantes.

Para obtener información detallada sobre el sistema operativo en una red, se usa **Nmap**, herramienta de código abierto que identifica el sistema operativo mediante un escaneo avanzado. Para atacar, es necesario evaluar la configuración de la máquina objetivo. Se usa Nmap debido a que es eficaz para extraer información sin generar ruido adicional.

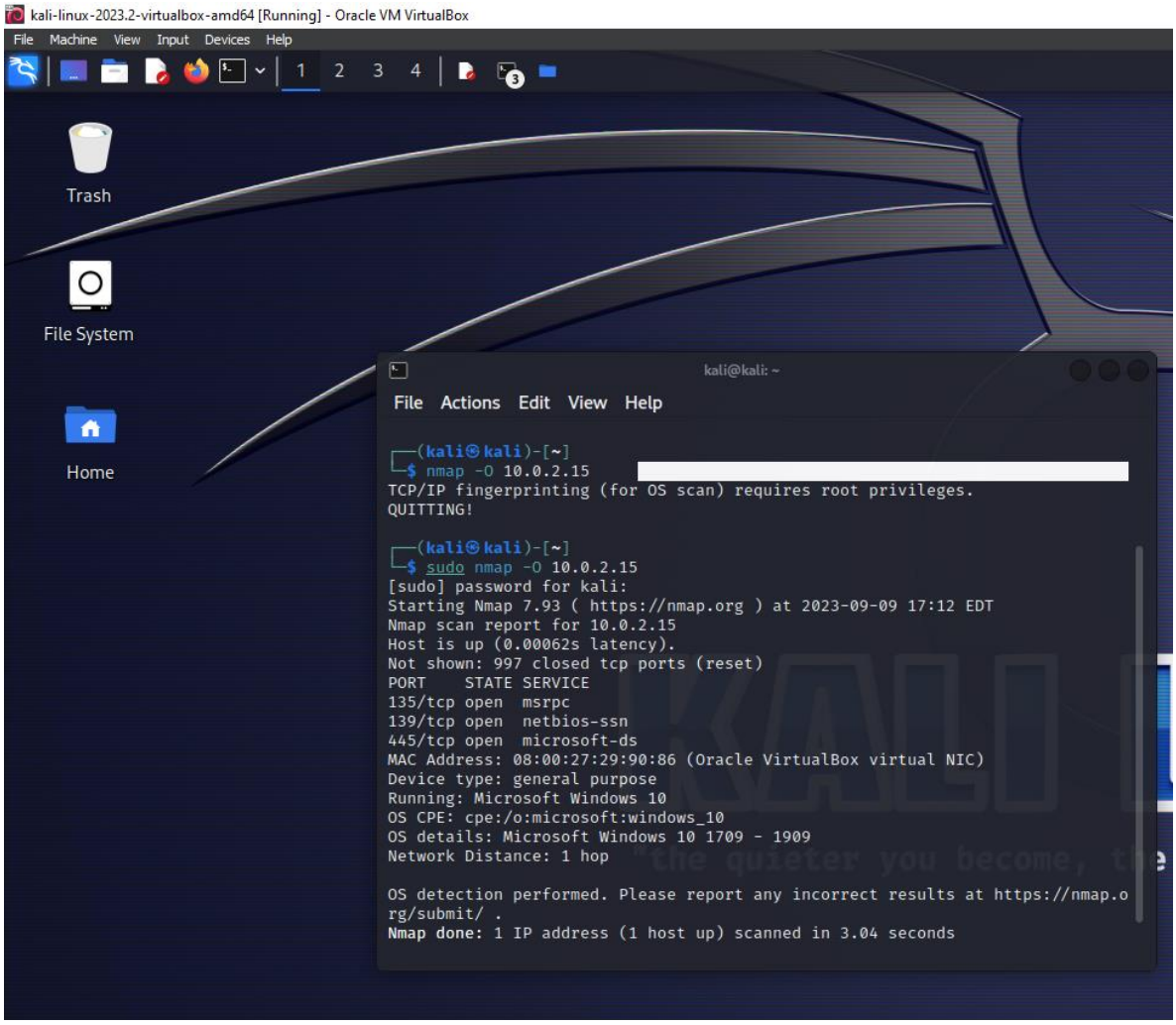

Ilustración 3. Resultados del comando nmap -O a la Ip objetivo. Fuente: Elaboración propia

De este comando se recopila la siguiente información.

Host is up (0.00062s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 08:00:27:29:90:86 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop

7.1.2 Identificación de vulnerabilidades

Con la información obtenida de posibles debilidades se evalúa el sistema objetivo utilizando la información recopilada, incluyendo la búsqueda de exploits conocidos.

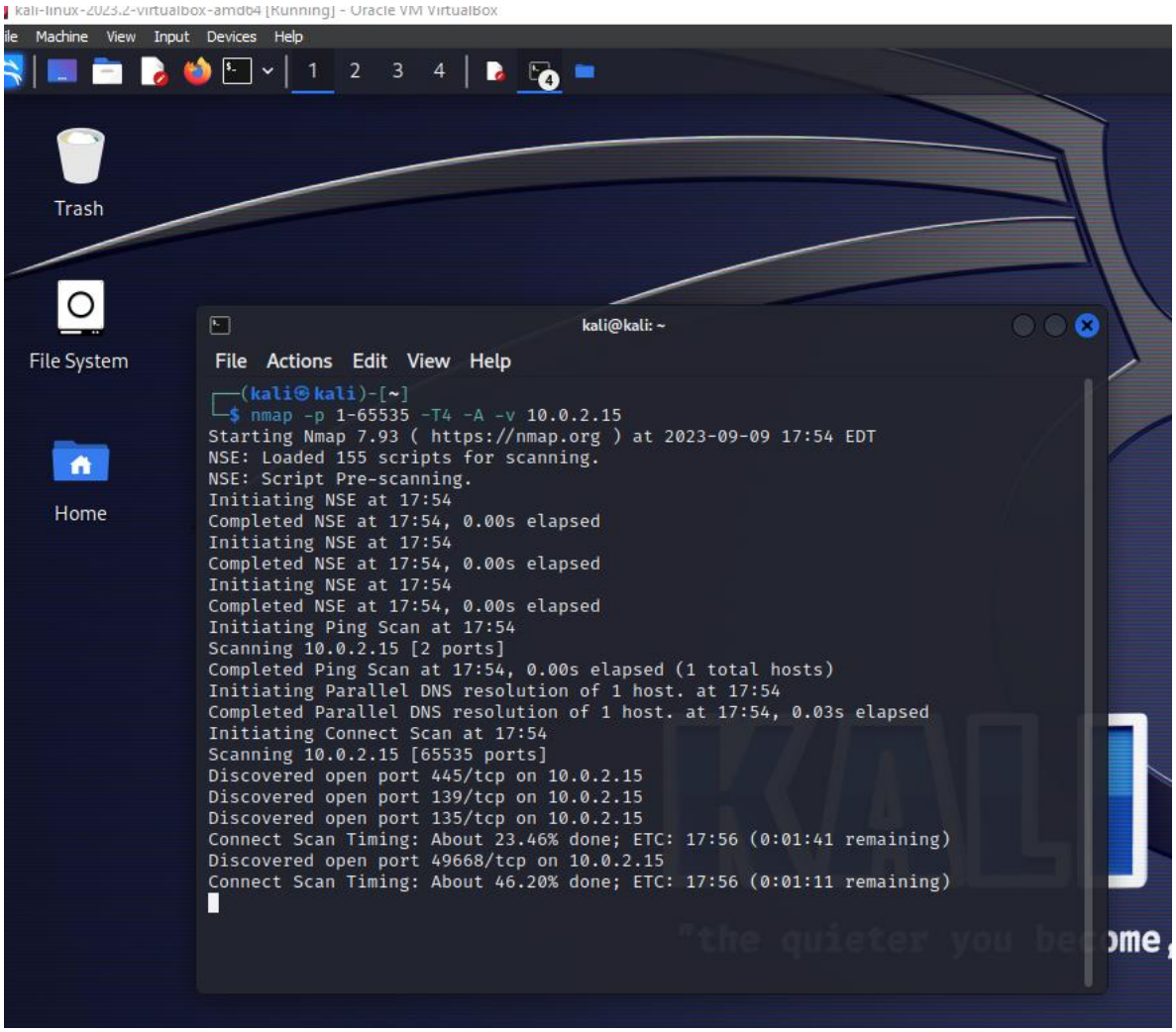

Ilustración 4. Escaneo del estado de cada uno de los puertos para encontrar vulnerabilidades. Fuente: Elaboración propia

7.1.3 Creación del payload

Msfvenom es una herramienta de Metasploit que permite diseñar estas cargas útiles de manera personalizada, eligiendo el tipo de exploit, el sistema operativo de destino, el formato del archivo y otros parámetros para simular la elaboración del agente malicioso usado.

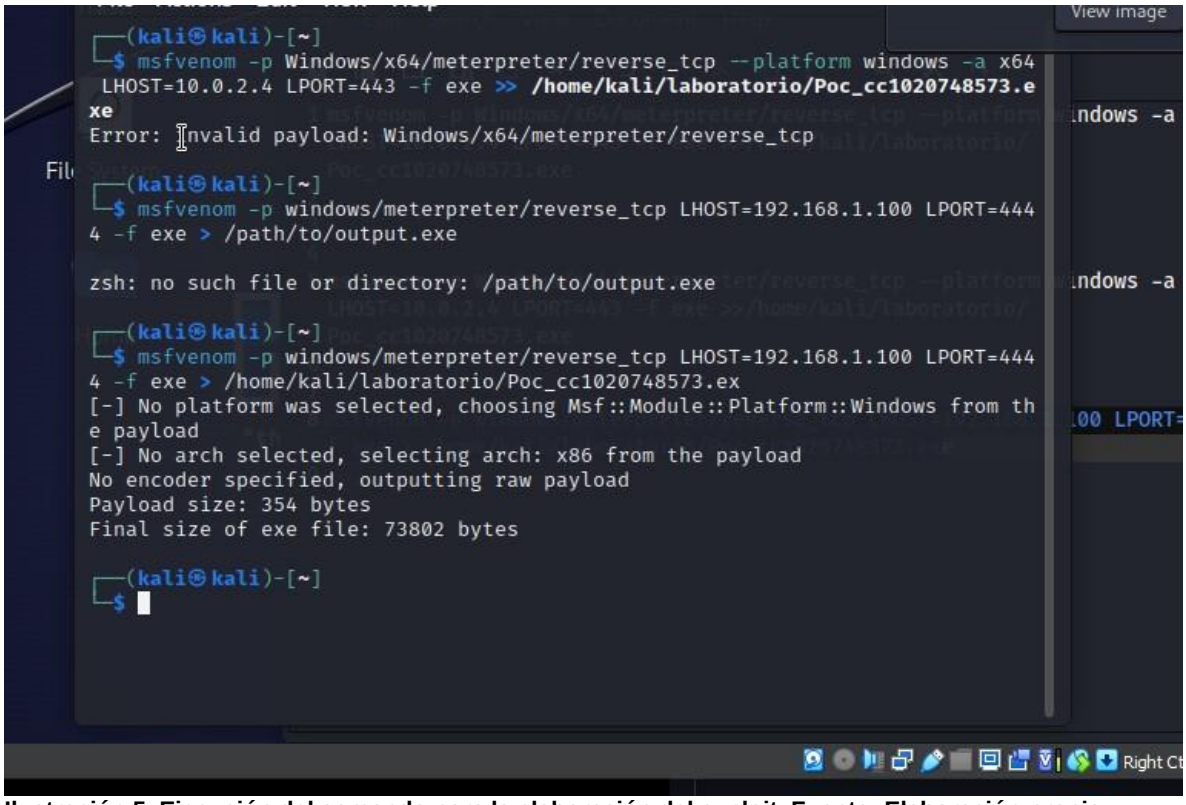

Ilustración 5. Ejecución del comando para la elaboración del exploit. Fuente: Elaboración propia

7.1.4 Configuración de Metasploit para escucha

Ahora se prepara el shell inverso seleccionando el módulo adecuado, configurando las opciones necesarias y eligiendo el puerto para la sesión de control remoto, listo para aprovechar la vulnerabilidad.

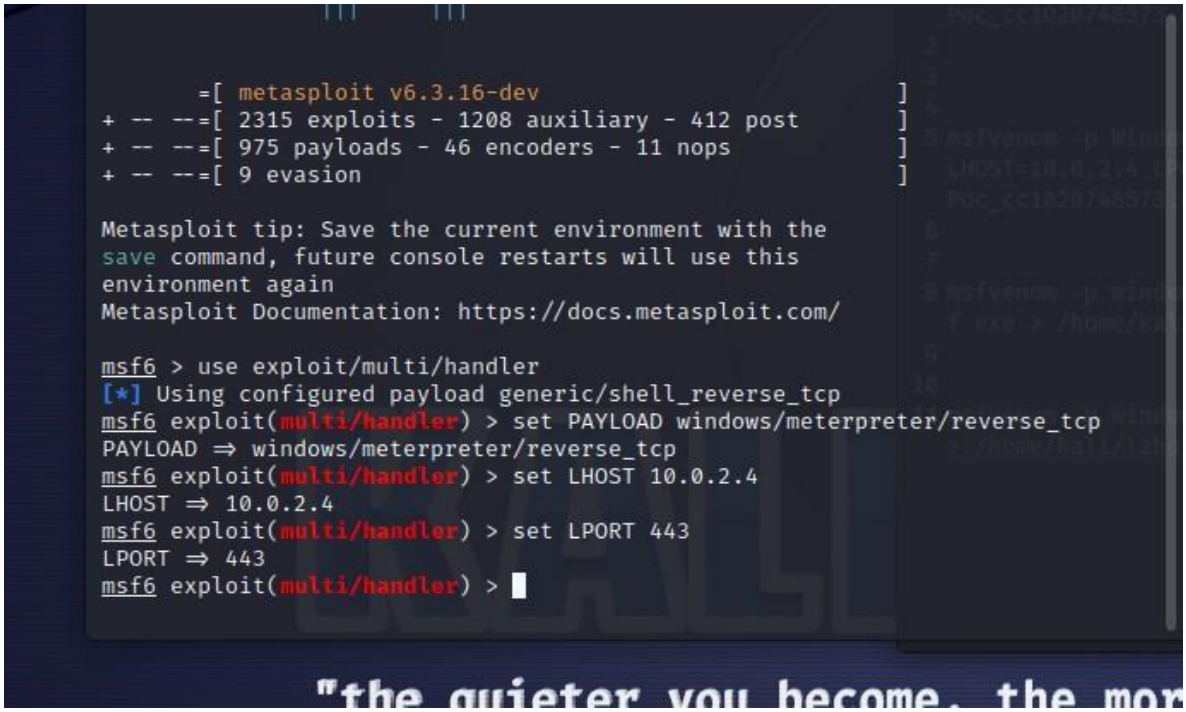

Ilustración 6. Consola de Metasploit, configuración para escucha Fuente: Elaboración propia

7.1.5 Ejecución del ataque y establecimiento de la sesión remota

Se envía el archivo malicioso al administrador de Windows 10 X64, utilizando en este caso la plataforma de transferencia de archivos WeTransfer. Cuando el usuario lo ejecuta, Metasploit establece una sesión remota en la máquina objetivo, permitiendo el acceso al sistema comprometido.

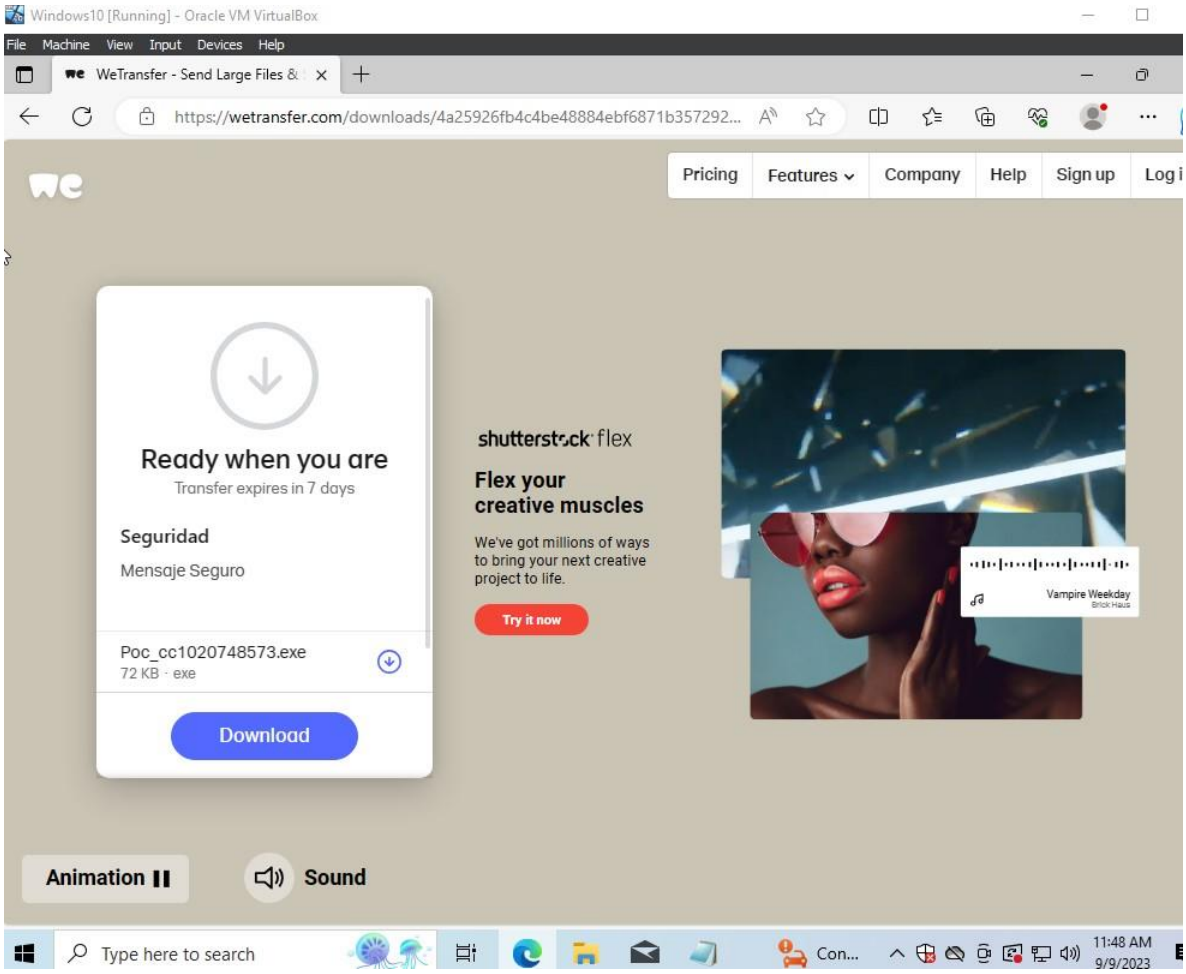

Ilustración 7. Link de Wetransfer desde Windows 10 Maquina de la víctima. Fuente: Elaboración propia

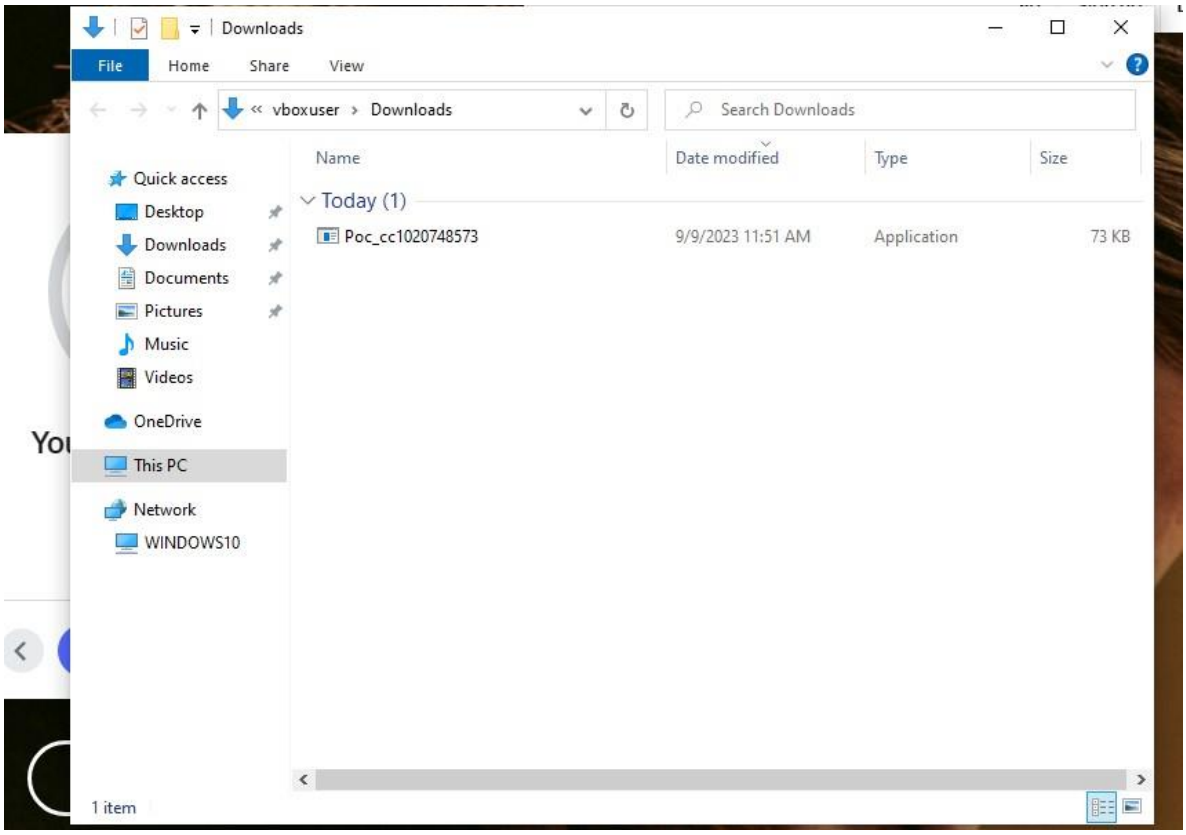

Ilustración 8. Archivo malicioso en la maquina víctima. Fuente: Elaboración propia

7.1.6 Acciones de control malicioso

Para realizar el ataque basta con mantenerse a la escucha activa de la conexión y la espera de que el usuario ejecute la aplicación desde su equipo. Cuando el usuario realice la ejecución de la aplicación obtendremos la conexión a la máquina.

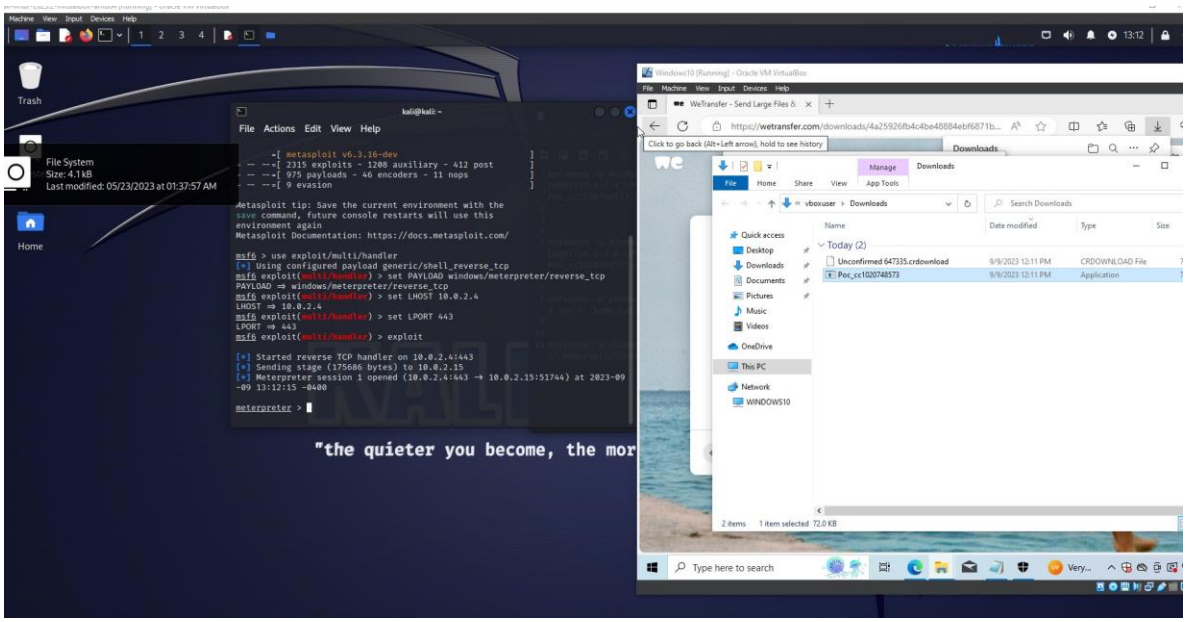

Ilustración 9. Ejecución del software y conexión desde la consola en Kali

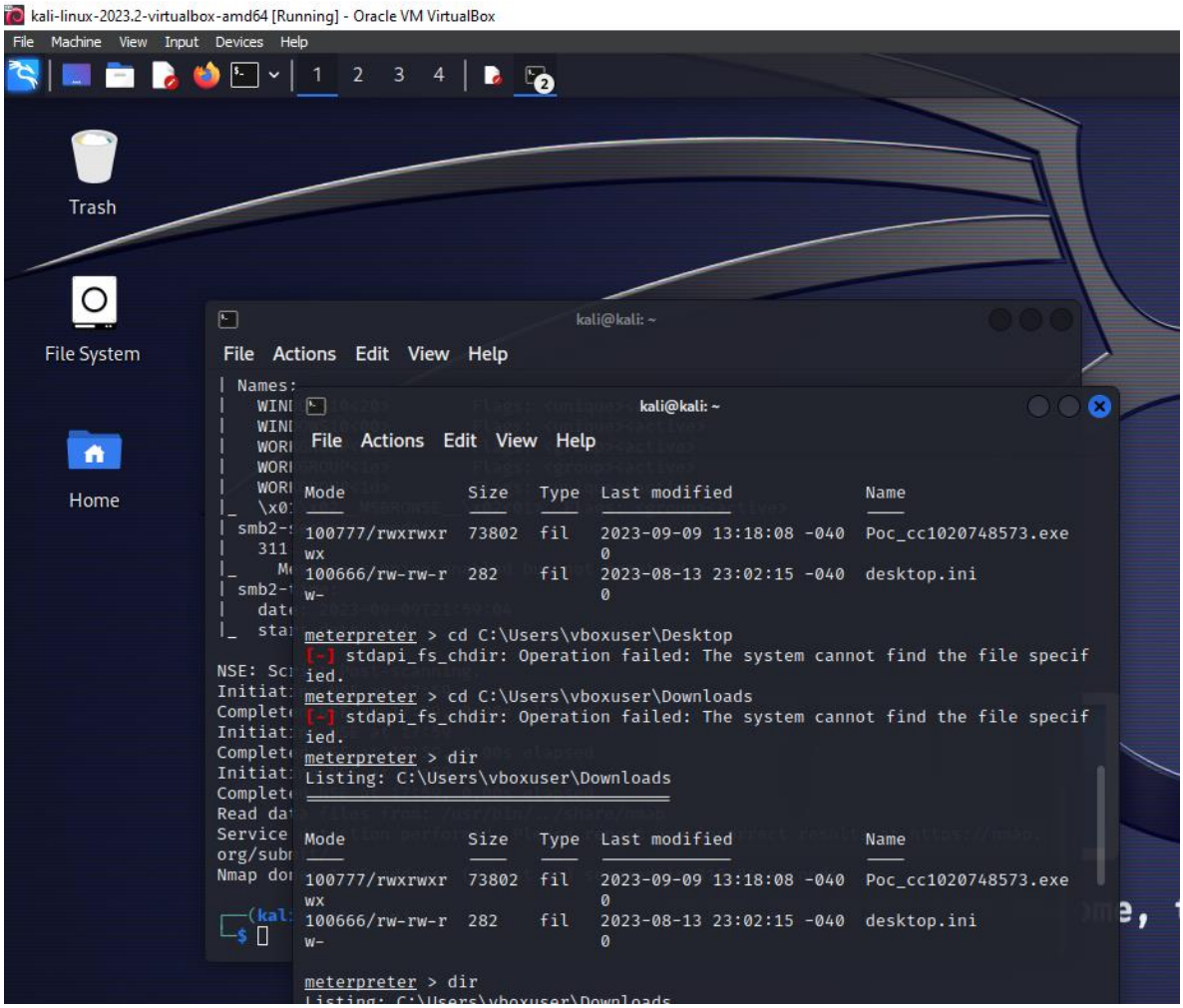

Ilustración 10. Uso de los comandos dir y cd para la búsqueda y navegación. Fuente: Elaboración propia

7.1.7 Documentación

Del análisis presentado por el anexo se extrajeron los siguientes datos. Estos datos Se extrajeron por una cara desde la maquina atacante y desde la otra de la metadata de la maquina afectada.

NOMBRE DEL ARCHIVO	**SERGIO_RODRIGUEZ_1020748573_09-09-2023**
TIPO	File (Archivo)
EXTENSIÓN	txt
TAMAÑO	400 bytes
FECHA DE LA ÚLTIMA MODIFICACIÓN	2023-09-09 13:16:30

Tabla 1. Metada del archivo objetivo. Fuente: Elaboración propia

NOMBRE	**DETALLES**
SISTEMA OPERATIVO	Windows 10 de 64 bits
ESTADO DE SEGURIDAD DEL SISTEMA	• Firewall desactivado • Windows Defender desactivado • Antivirus desactivado
ARCHIVO OBJETIVO	• Sergio_Rodriguez_1020748573_09-09-2023.txt • Hallado en el escritorio del usuario
ARCHIVO DESCARGADO Y EJECUTADO	Poc_cc1020748573.exe
POSIBLE HERRAMIENTA DE ATAQUE	MSFVENOM

Tabla 2. Data extraída del análisis de la maquina víctima. Fuente: Elaboración propia.

7.2 PROCESO DE AFECTACIÓN DE LA MAQUINA VICTIMA

A continuación, se presenta el diagrama que representa el flujo del proceso usado para simular el ataque en la infraestructura del diagrama 1

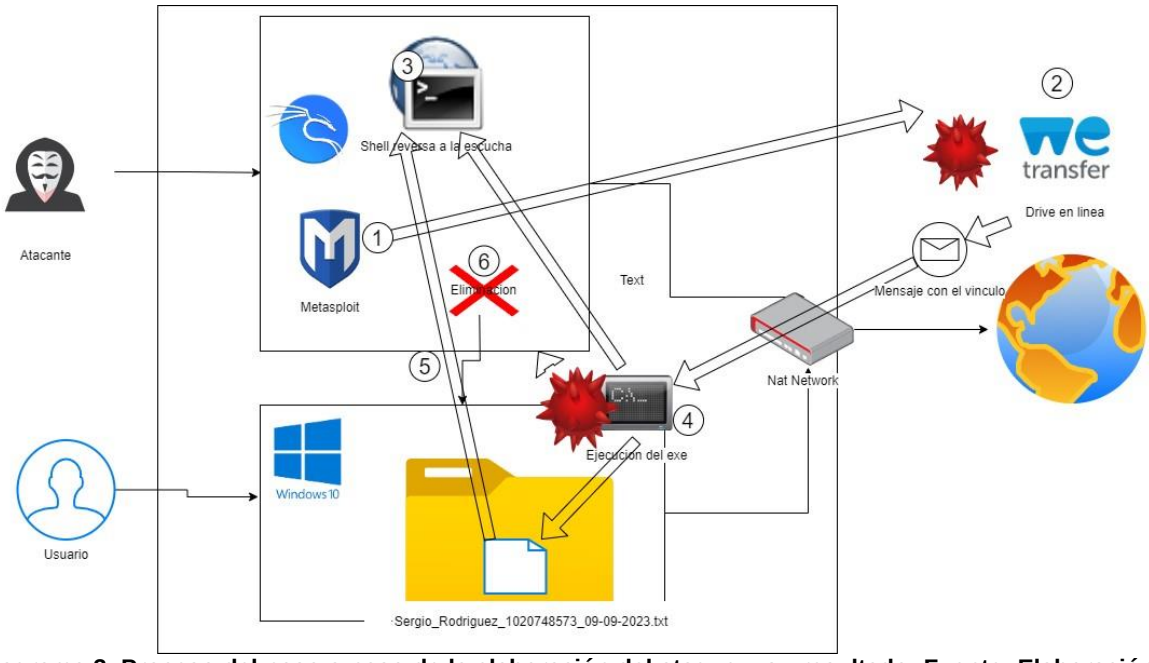

Diagrama 3. Proceso del paso a paso de la elaboración del ataque y su resultado. Fuente: Elaboración propia

1. Generación de Payload: El atacante utiliza la herramienta `msfvenom` para crear un archivo ejecutable (Payload) llamado "Poc_cc1020748573.exe". Este archivo contiene código malicioso que se ejecutará en la máquina objetivo.

2. Envío del Payload: El atacante de alguna manera logra que el usuario de la máquina objetivo descargue y ejecute el archivo "Poc_cc1020748573.exe" en su sistema por medio de Wetransfer.

3. Establecimiento de la Conexión: Una vez que el usuario ejecuta el archivo, el Payload se inicia y trata de conectarse de vuelta al atacante a través de una conexión de red. En este caso, la dirección IP del atacante es "10.0.2.4" y el puerto es "443".

4. Ejecución del Payload: Una vez que se ejecuta el Payload en la máquina objetivo, comienza a realizar acciones maliciosas en el sistema. Esto puede

incluir la explotación de vulnerabilidades en el sistema operativo o en aplicaciones, dependiendo de cómo esté configurado el Payload.

5. Control Remoto: Una vez que se establece la conexión de vuelta al atacante, este obtiene un control remoto sobre la máquina objetivo.

6. Con la conexión establecida se puede realizar una serie de acciones maliciosas, en este caso la eliminación del archivo.

7.3 HERRAMIENTAS USADAS POR EL EQUIPO ROJO PARA LA PRUEBA DE PENETRACIÓN

7.3.1 Virtual Box (Virtualización de la red)

Aplicación para la creación de las máquinas virtuales de diferentes sistemas operativos incluyendo Windows y Linux, ofrece la posibilidad de configurar múltiples características tales como los recursos de disco y memoria y la virtualización de la red.

7.3.2 Kali Linux (SO atacante)

Distribución de Linux especializada en seguridad informática y pruebas de penetración. Incluye una amplia variedad de herramientas y utilidades de seguridad preinstaladas, lo que la hace popular entre los profesionales de la ciberseguridad.

7.3.3 Nmap (Network Mapper)

Herramienta de escaneo de redes que se utiliza para descubrir dispositivos y servicios en una red. Permitió identificar hosts activos y puertos abiertos, lo que es fundamental para evaluar la seguridad de una red.

7.3.4 Metasploit (Suite de herramientas de pentesting)

Es un marco de desarrollo y explotación de código abierto utilizado para probar, desarrollar y ejecutar exploits en sistemas informáticos. Ampliamente utilizado en pruebas de penetración y por equipos Red Team para evaluar la seguridad de sistemas y aplicaciones.

7.3.5 Meterpreter (Creación del payload)

Se utiliza junto con Metasploit para lograr acceso y control remoto en sistemas comprometidos. Proporciona una interfaz en tiempo real con capacidades avanzadas, lo que facilita su uso.

7.3.6 MSFVenom (Creación del payload)

MSFVenom es una herramienta integrada en Metasploit que se utiliza para generar payloads maliciosos. Puede crear archivos ejecutables, scripts y otros tipos de payloads personalizables que se utilizan en los ataques.

7.3.7 WeTransfer (Transferencia de archivos):

Plataforma de transferencia de archivos en línea que permite a los usuarios cargar y compartir archivos grandes con otras personas a través de enlaces de descarga temporales.

7.3.8 CMD (Como Consola inversa):

La consola CMD (Command Prompt) se puede utilizar en el contexto de un ataque como una "consola inversa" o una "shell inversa". Esto ocurre cuando un atacante logra ejecutar comandos en una máquina comprometida y obtiene acceso a una interfaz de línea de comandos remota para controlar la máquina.

8 ETAPA 4: EQUIPO AZUL – TOMA DE ACCIONES DEFENSIVAS ANTE EVENTOS DE SEGURIDAD INFORMÁTICA

En esta etapa por medio de las acciones del Blue Team se dio resolución al problema que afectó la máquina.

- Se obtuvo la guía de endurecimiento para Windows 10, se selecciono endurecer las configuraciones de antivirus y firewall
- Se aseguro la maquina creando una copia de seguridad de la misma y realizando un análisis de los sucesos del ataque tanto por medio del uso del software Autopsy como por análisis de logs de Windows.
- Se documentaron los resultados del proceso

8.1 IDENTIFICACIÓN DEL ATAQUE

En el papel del equipo Blue Team, se adoptó un enfoque proactivo para identificar ataques informáticos en tiempo real. Esto implica una vigilancia constante de la red y sistemas, utilizando herramientas de monitorización y detección para detectar actividades inusuales. La estrategia seleccionada para la identificación de acciones del ataque es la siguiente.

Diagrama 4. Pasos para la identificación del ataque. Fuente: Elaboración propia

Se optó por una estrategia de investigación forense. En primer lugar, se creó una copia de la máquina virtual para preservar la integridad de la imagen original. Luego, se aseguró la copia y se procedió a utilizar la herramienta forense Autopsy para llevar a cabo una inspección exhaustiva.

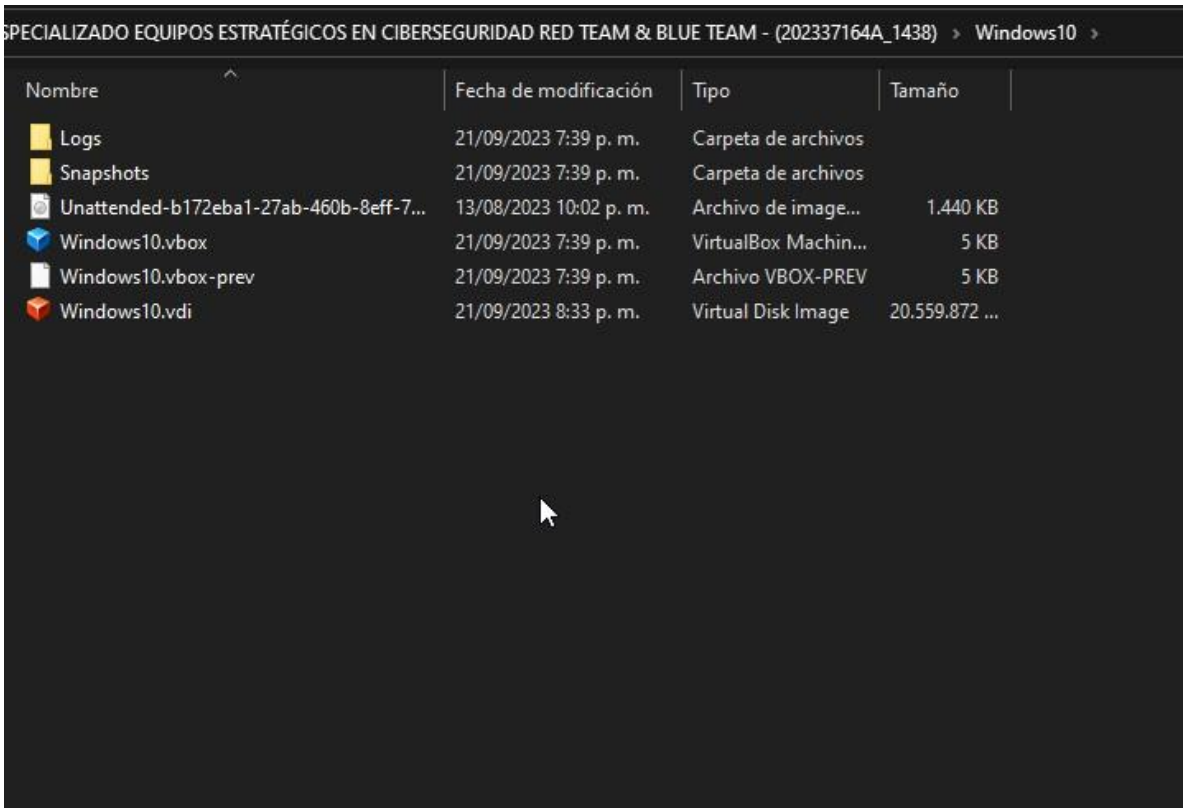

Ilustración 11. Imagen de la MV afectada en el equipo host. Fuente: Elaboración propia

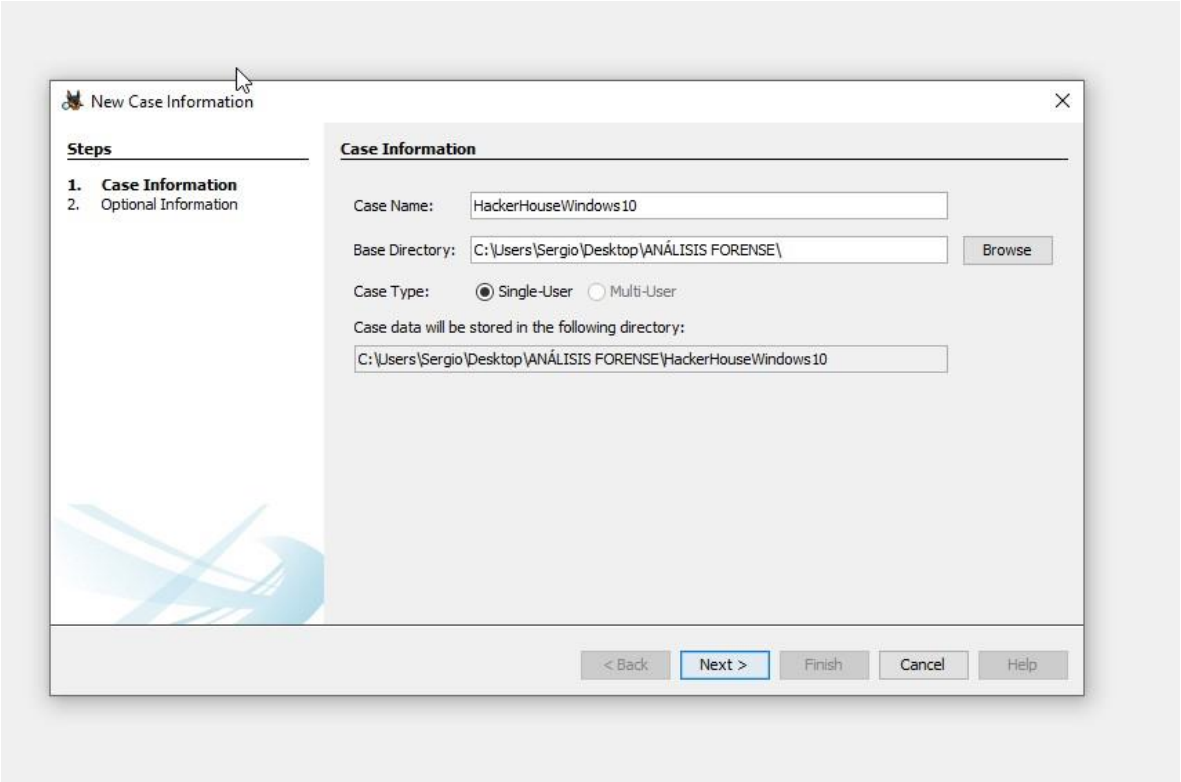

Ilustración 12. Creación del caso dentro de la herramienta. Fuente: Elaboración propia

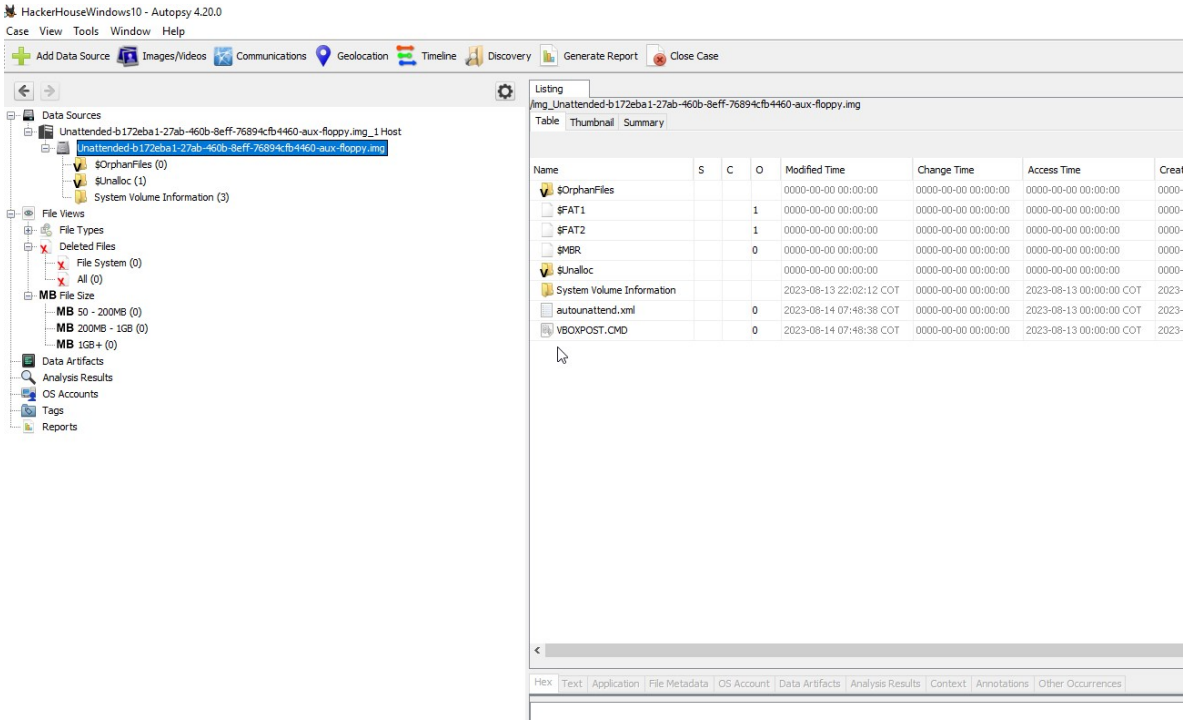

Ilustración 13. Vista de la imagen desde la ventana principal. Fuente: Elaboración propia

Con Autopsy, se exploró la copia de la máquina virtual en busca de pistas y evidencias del ataque. Esta herramienta permitió analizar detalles relacionados con archivos modificados o eliminados, así como acceder a registros relevantes.

Además, se usó del visor de eventos de Windows para buscar eventos de logins (**ID 4624**) y detectar conexiones sospechosas.

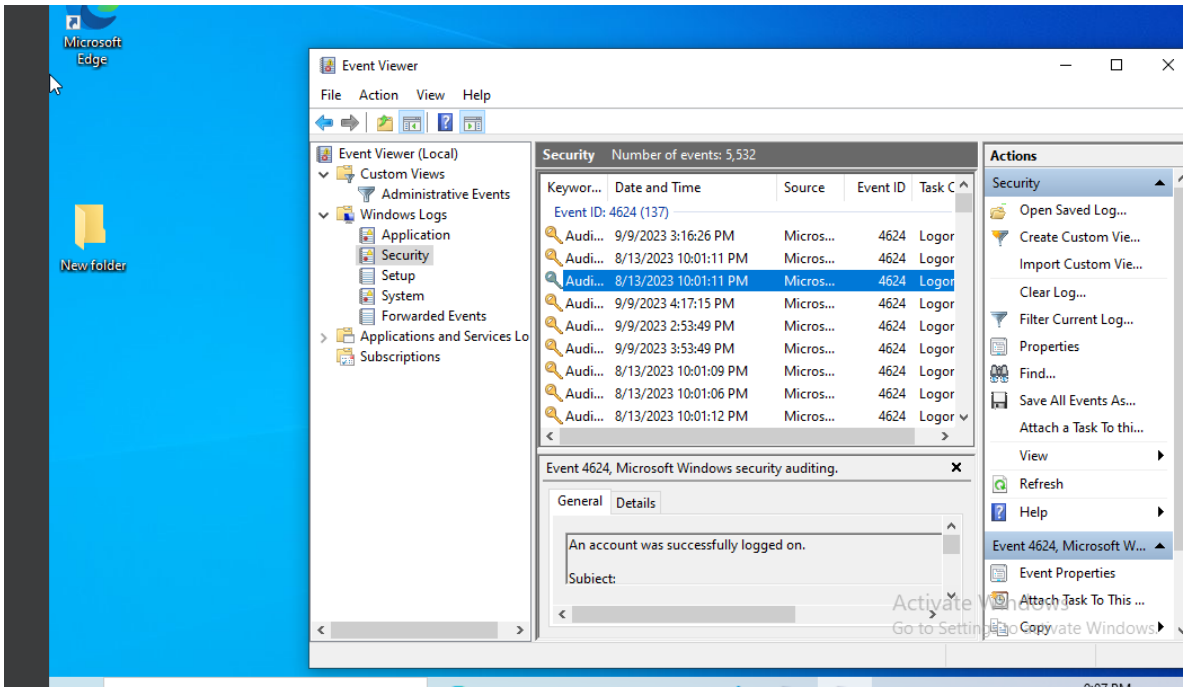

Ilustración 14. Clasificación de eventos por ID. Fuente: Elaboración propia

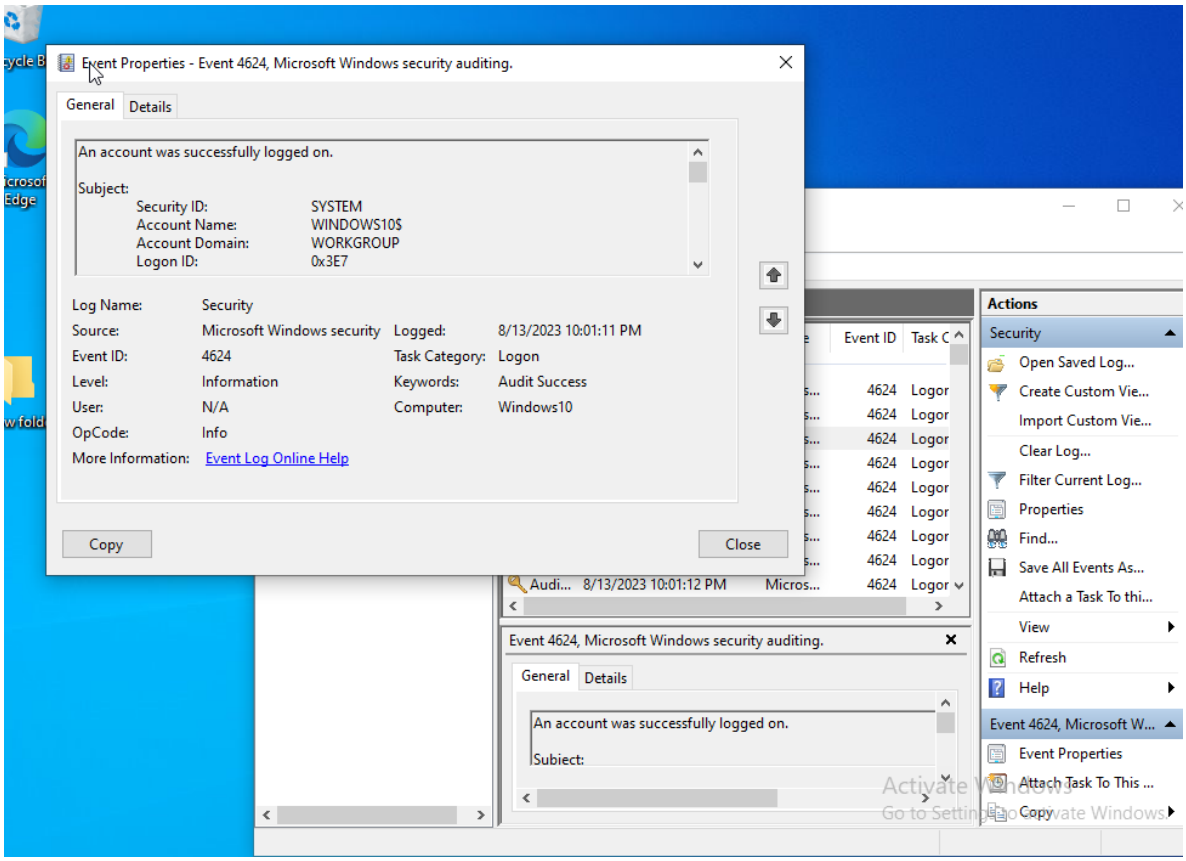

Ilustración 15. Detalles del evento en el log de la MV. Fuente: Elaboración propia

8.2 LA IMPORTANCIA DEL ENDURECIMIENTO DEL FIREWALL

El firewall juega un papel fundamental en la defensa de una red contra intrusiones no autorizadas y ataques cibernéticos. Actúa como una barrera de seguridad que controla el tráfico de entrada y salida, permitiendo o bloqueando ciertas conexiones según las reglas predefinidas. Sin embargo, la efectividad del firewall depende en gran medida de su configuración. Un firewall mal configurado o con reglas laxas puede dejar la red vulnerable a ataques.

Aquí es donde entra en juego la guía de endurecimiento del firewall del CIS. Esta guía proporciona un conjunto de pautas y mejores prácticas respaldadas por expertos en seguridad cibernética para optimizar la configuración del firewall. Al seguir estas recomendaciones, se fortalece la postura de seguridad de la red, se reducen las posibilidades de explotación y se mejora la capacidad de detectar y responder a posibles amenazas.

8.3 IMPLEMENTACIÓN DE LAS RECOMENDACIONES DE LA GUÍA DE ENDURECIMIENTO DEL FIREWALL

Tras haber descargado la guía de endurecimiento del firewall desde el Center for Internet Security (CIS), el siguiente paso es implementar las recomendaciones proporcionadas. Se describen ahora los procesos y pasos necesarios para aplicar eficazmente las medidas de seguridad sugeridas en la guía. La correcta implementación de estas recomendaciones es esencial para fortalecer la postura de seguridad de la red y garantizar una protección sólida contra amenazas cibernéticas.

8.3.1 Evaluación y Preparación Inicial

Antes de comenzar con la implementación, es importante llevar a cabo una evaluación exhaustiva de la infraestructura de red y los sistemas que serán afectados por los cambios en la configuración del firewall. Esto implica identificar todos los componentes críticos de la red, las dependencias de servicios y las aplicaciones que pueden verse afectadas por las nuevas reglas del firewall. Además, es crucial realizar una copia de seguridad completa de la configuración actual del firewall y de todos los sistemas involucrados para evitar pérdida de datos o interrupciones no deseadas.

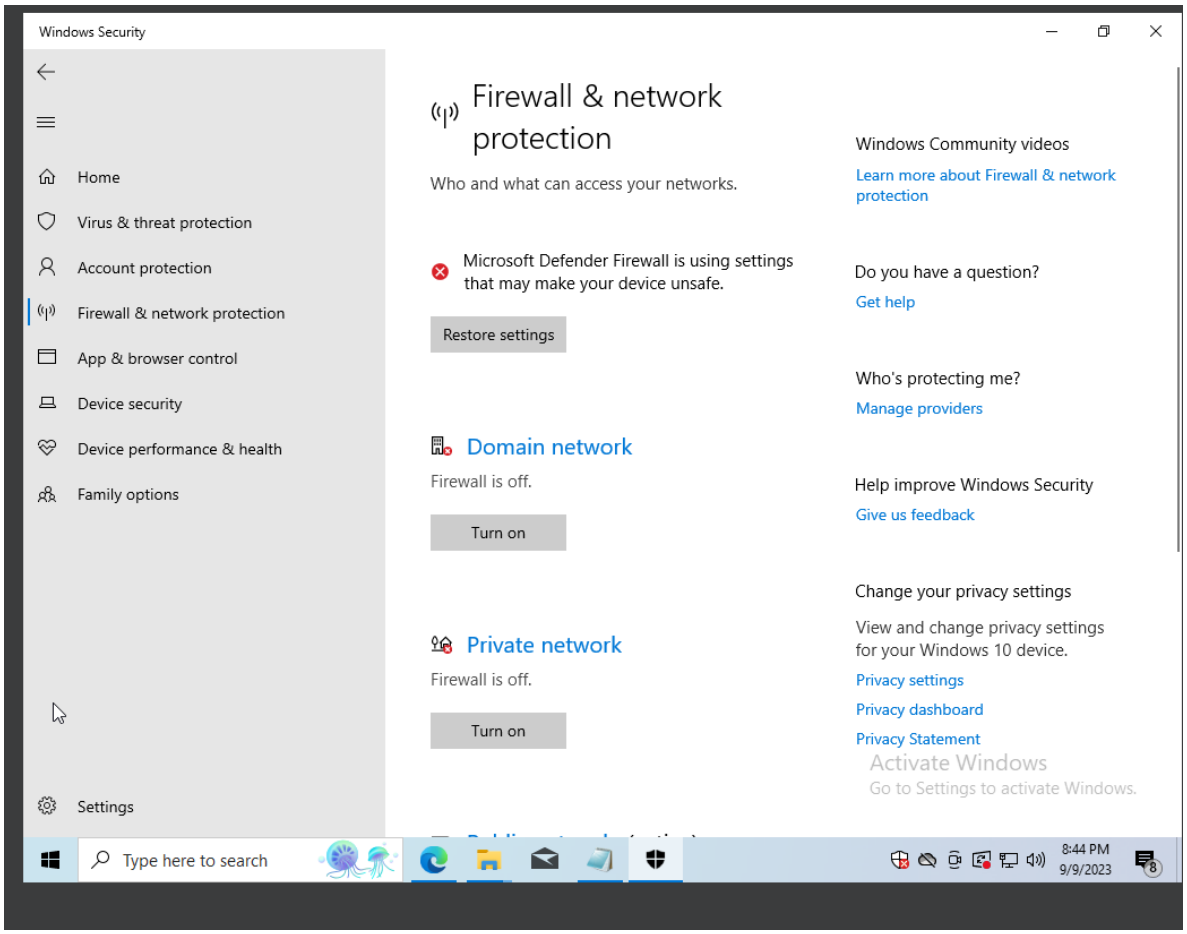

Ilustración 16. Configuración inicial del firewall. Fuente: Elaboración propia

8.3.2 Implementación de las Recomendaciones

La guía del CIS proporcionará una serie de recomendaciones específicas que deben seguirse para endurecer el firewall. Estas recomendaciones incluyen la configuración de reglas de filtrado y la actualización de firmas de seguridad entre otras. Cada recomendación se evalúa en función de la infraestructura y las necesidades de seguridad.

Ilustración 17. Path de las políticas con las configuraciones del firewall para Windows 10. Fuente: Elaboración propia.

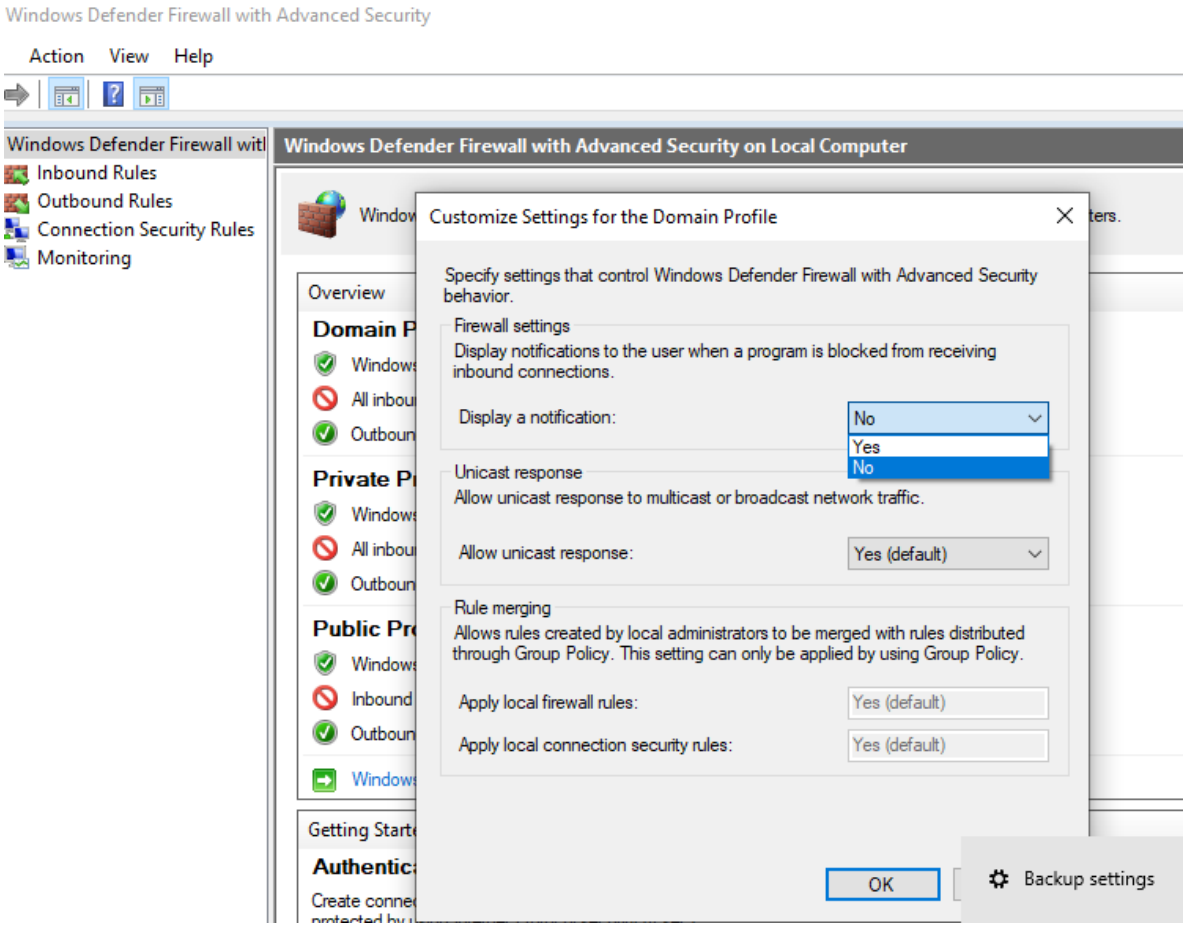

Ilustración 18. Configuración desde el firewall avanzado. Fuente: Elaboración propia

8.3.3 Pruebas y Validación

Una vez que se han implementado todas las recomendaciones de la guía, es esencial llevar a cabo pruebas exhaustivas. Esto implica verificar que las reglas del firewall estén funcionando según lo previsto y que no haya conflictos.

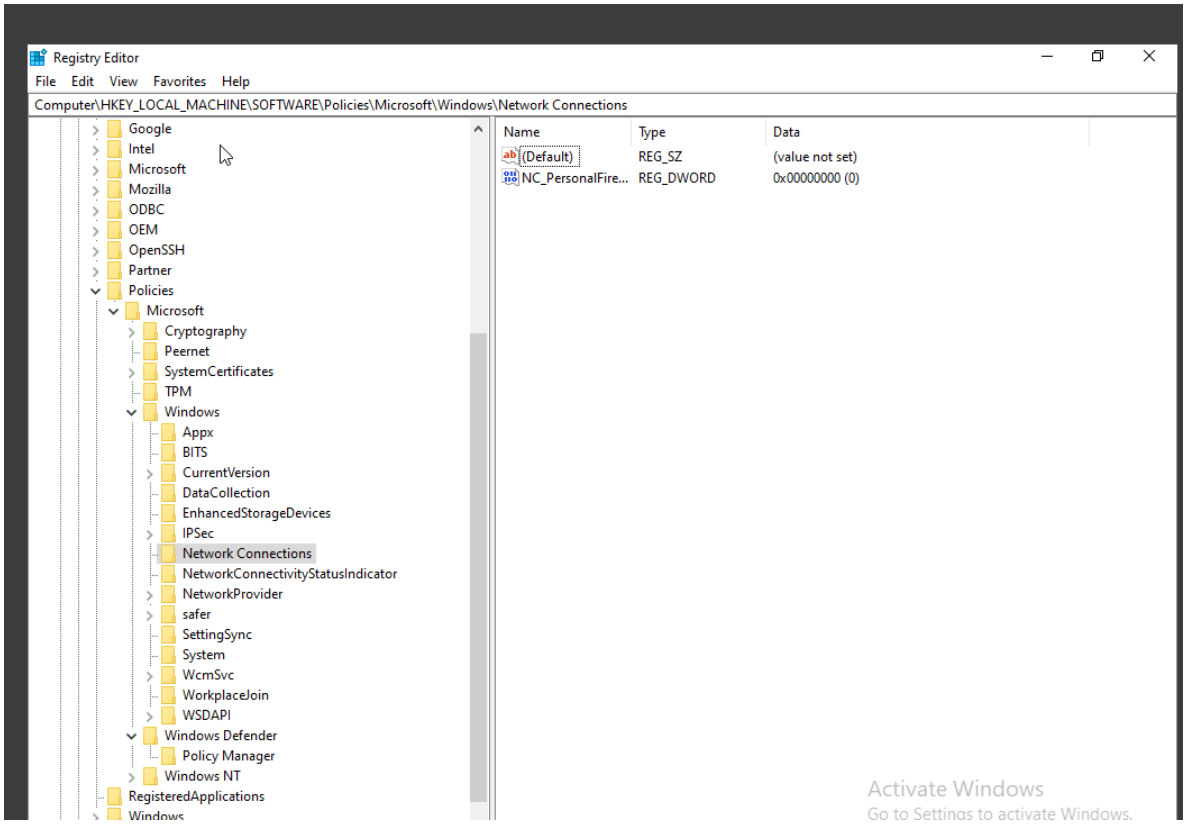

Ilustración 19. Auditoria desde el registro del status del firewall. Fuente: Elaboración propia.

8.3.4 La importancia del mantenimiento Continuo

La implementación de las recomendaciones de endurecimiento del firewall no es un evento único, sino un proceso continuo. La seguridad cibernética es un campo en constante evolución, y las amenazas cambian con el tiempo. Por lo tanto, es esencial mantenerse actualizado con las mejores prácticas de seguridad y revisar periódicamente la configuración del firewall para realizar ajustes según sea necesario. El monitoreo constante y las actualizaciones de seguridad son parte integral de mantener una red segura.

8.4 SIEM Y XDR: COMO HERRAMIENTAS CLAVE PARA LA SEGURIDAD CIBERNÉTICA

En el campo de la seguridad de la información, contar con herramientas efectivas de monitoreo y detección es fundamental para proteger una infraestructura de TI contra amenazas cada vez más sofisticadas. Se analizan dos tecnologías esenciales en este contexto para la estrategia defensiva por parte Blue Team: **SIEM** (Security Information and Event Management) y **XDR** (Extended Detection and Response). Se analiza sus roles, importancia y cómo complementan los esfuerzos de seguridad de una organización.

8.4.1 SIEM: Gestión de Información y Eventos de Seguridad

Es una tecnología diseñada para brindar visibilidad y contexto sobre la seguridad de una red o sistema. Esta solución integra diversas fuentes de datos, como registros de seguridad, registros de eventos, alertas de intrusiones y otros datos relevantes, en una única plataforma centralizada. El objetivo principal de SIEM es permitir a los equipos de seguridad cibernética monitorear y responder a eventos de seguridad en tiempo real.

Beneficios de SIEM:

- Detección de Amenazas en Tiempo Real: Permite la detección y notificación inmediata de actividades sospechosas o incidentes de seguridad.
- **Análisis y Correlación de Datos:** La capacidad de correlacionar eventos y datos de múltiples fuentes proporciona una visión más completa de la seguridad de la red.
- **Generación de Informes y Cumplimiento Normativo:** Ayuda en la generación de informes de cumplimiento y puede ser valioso para auditorías y cumplimiento de regulaciones.
- **Automatización de Respuestas:** Puede automatizar respuestas a eventos de seguridad predefinidos.

8.4.2 XDR: Detección y Respuesta Extendida

En esencia es una evolución de SIEM que aborda los desafíos emergentes en la seguridad cibernética. A diferencia de SIEM, que se enfoca principalmente en la recopilación y análisis de datos, XDR agrega capacidades adicionales para la detección y respuesta más allá del alcance de una sola plataforma. XDR integra datos de múltiples fuentes, incluidas las de endpoints, redes y aplicaciones, y utiliza técnicas avanzadas de análisis de amenazas.

Beneficios de XDR:

- **Mayor Cobertura de Amenazas:** Amplía la capacidad de detección y respuesta a amenazas en una variedad de entornos, incluidos endpoints, servidores y nubes.
- **Análisis de Comportamiento y Machine Learning:** Utiliza técnicas de análisis de comportamiento y aprendizaje automático para identificar amenazas desconocidas.
- **Reducción de Ruido y Falsos Positivos:** XDR mejora la precisión en la identificación de amenazas al reducir el ruido y minimizar los falsos positivos.
- **Automatización de Respuestas Avanzada:** Permite respuestas automatizadas más sofisticadas, como la cuarentena de endpoints comprometidos.

8.4.3 Comparativa de las capacidades de SIEM y XDR

Si bien SIEM se centra en la gestión de eventos y la visibilidad, y XDR amplía la detección y respuesta a través de múltiples capas de seguridad para abordar amenazas más sofisticadas[32]. A continuación, se contrasta las características de cada uno.

[32] BLACKBERRY. XDR vs SIEM: what's the difference? BlackBerry [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.blackberry.com/us/en/solutions/endpoint-security/extended-detection-and-response/xdr-vs-siem>.

CARACTERÍSTICA	SIEM	XDR
DEFINICIÓN	Enfocado en la recopilación de registros de incidentes.	Detención de incidentes con correlación y respuesta automatizada
ALCANCE	Gestión de eventos y registros	Proporcionar una visión más amplia de la detección y acción
FUENTES DE DATOS	• Logs de eventos • Firewalls • IDS/IPS	• Logs de eventos • Firewalls • Trafico de red • End points • IDS/IPS
CORRELACIÓN	De patrones que puedan identificar amenazas	De comportamientos en tiempo real y automatizado
DETECCIÓN	Amenazas conocidas	Adaptabilidad para la detección de amenazas en evolución y desconocidas
AUTOMATIZACIÓN DE RESPUESTA	Generación de alertas	Detección y respuesta de amenazas
INTEGRACIÓN DE SEGURIDAD	Puede integrarse con herramientas de seguridad, como firewalls y antivirus	Mayor integración para una visión holística de la seguridad.
ESCALABILIDAD	Grandes volúmenes de datos de seguridad en tiempo real.	Grandes volúmenes de datos de seguridad en tiempo real.
EXPERIENCIA DEL USUARIO	UIs minimas o línea de comando	UIs amigables con el usuario

Tabla 3. Comparación SIEM vs XDR

8.5 HERRAMIENTAS DE DETECCIÓN DE ATAQUES CON LICENCIAS GPL PARA EL ROBUSTECIMIENTO POR EL EQUIPO AZUL

8.5.1 Autopsy (Software forense)

Está diseñada para ser una plataforma completa de análisis forense, Autopsy permite a los investigadores examinar sistemas de archivos, discos duros y dispositivos de almacenamiento en busca de evidencia digital, como archivos borrados, registros de actividad y artefactos de sistema. Ofrece una interfaz gráfica de usuario (GUI) intuitiva que facilita la navegación a través de grandes cantidades de datos[33].

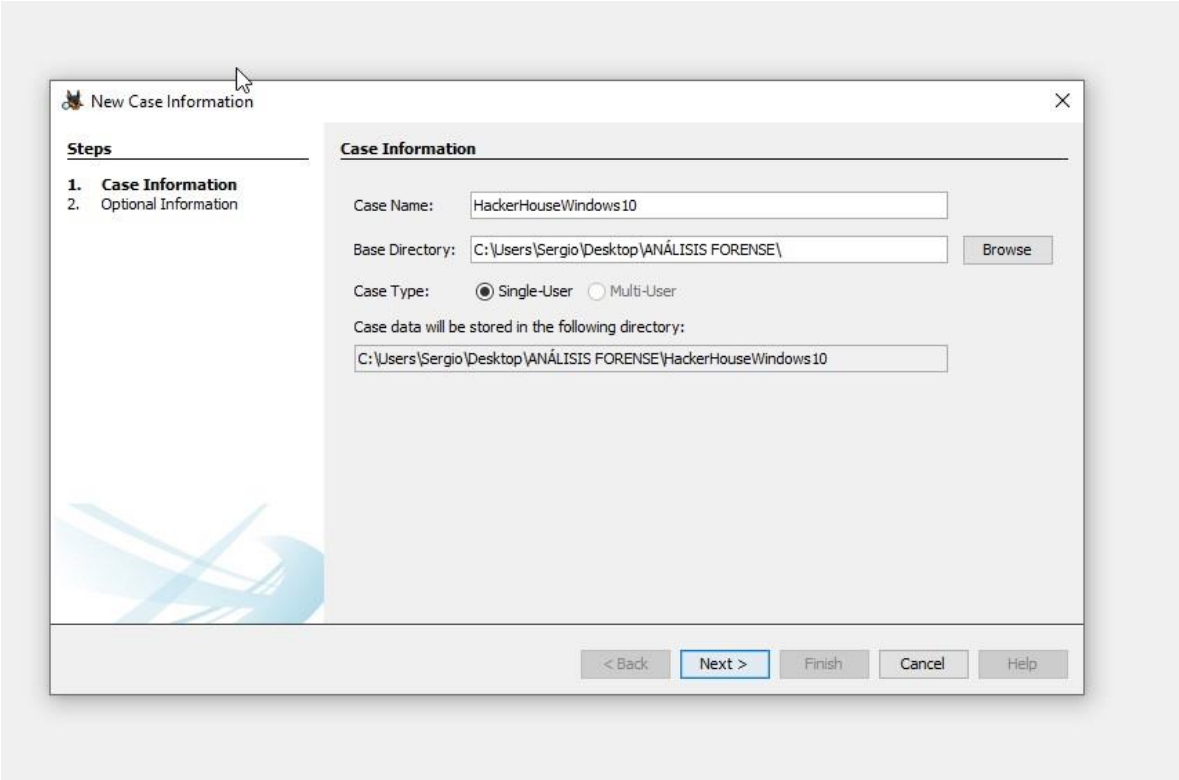

Ilustración 20. Caso de uso de Autopsy. Fuente: Elaboración propia

De las características de autopsy más destables son:

- Tiene una interfaz gráfica intuitiva que facilita la navegación y el uso
- Incluye la adquisición de evidencia, la recuperación de datos y el análisis de artefactos.

[33] BASISTECH. Autopsy - about. Autopsy [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.autopsy.com/about/>.

- Ofrece soporte para múltiples sistemas de archivos lo que lo hace versátil para diversas investigaciones.

8.5.2 Snort (IDS)

Es un potente IDS de código abierto diseñado para monitorear y analizar el tráfico de red en tiempo real. Conocido por su capacidad para identificar y alertar sobre actividades maliciosas o inusuales en una red[34].

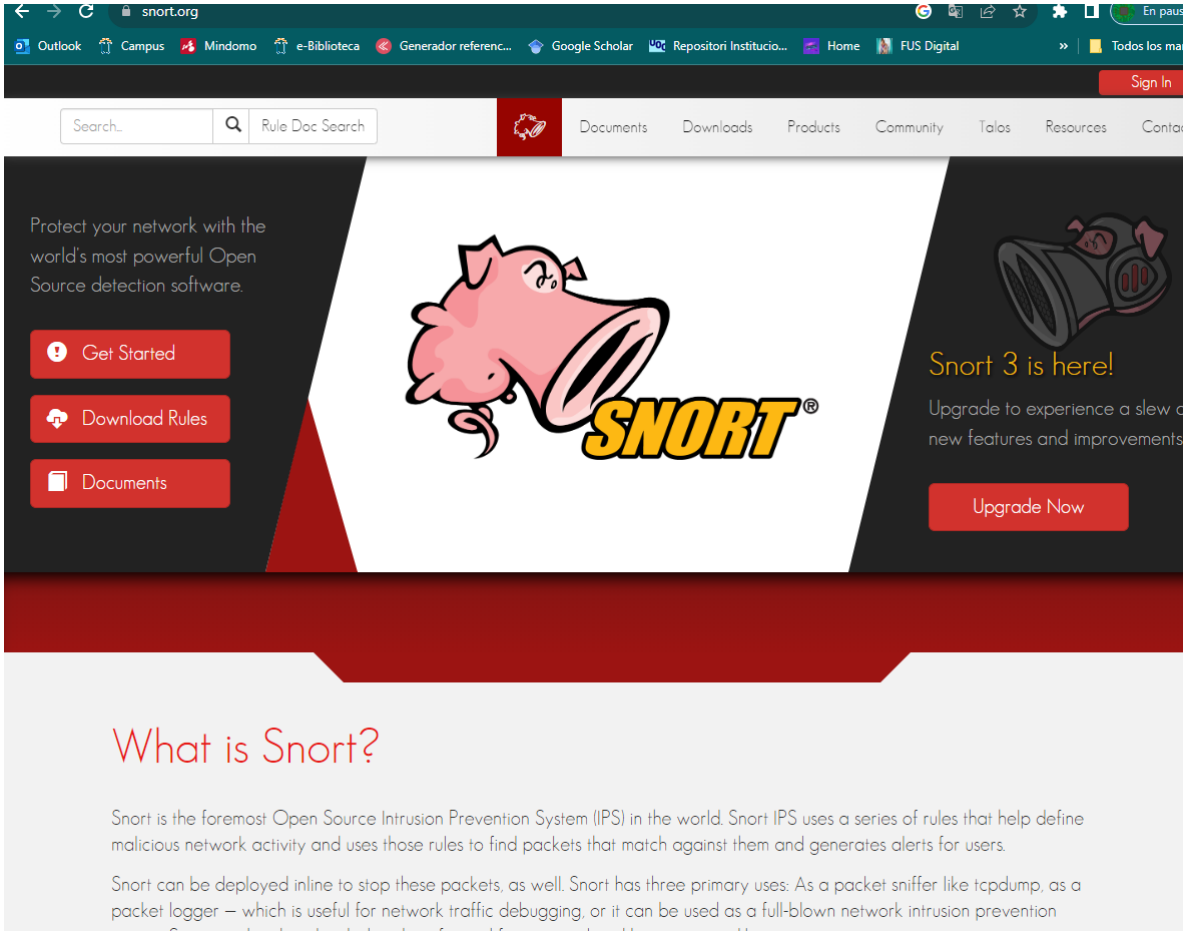

Ilustración 21. Homepage de Snort. Fuente: Elaboración propia

Las características más destacables para la detección son:

[34] CISCO. Snort documents. Snort [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: <https://www.snort.org/documents#OfficialDocumentation>.

- Snort es una herramienta de detección de intrusiones de red (IDS) de código abierto que ofrece numerosos puntos fuertes que lo han convertido en una opción popular en el ámbito de la ciberseguridad. Aquí tienes 10 de sus puntos fuertes:

- Es altamente configurable en sus reportes y compatible con otras herramientas

- Fácil manejo de ataques conocidos por configuración de reglas por IPs, URLs, etc.

- Puede identificar comportamientos inusuales en el tráfico de red

- Sus reglas son fácilmente actualizables para mantenerlo al día.

- Ofrece capacidades de análisis forense al registrar eventos y tráfico (muy útil para un evento como el del laboratorio).

8.5.3 Suricata (IDS)

Es un IDS diseñado para monitorear el tráfico de red en tiempo real, ofrece una amplia gama de características que van más allá de la detección de amenazas tal como el análisis de comportamiento[35].

Ilustración 22. Diagrama de la oferta de servicios de Suricata. Fuente: Stamus Networks

[35] OSIF. Home - suricata. Suricata [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://suricata.io/>.

De manera similar las características destacables de Snort son:

- Es compatible con múltiples sistemas operativos,
- Admite reglas de detección personalizadas
- Genera registros detallados de eventos, lo que facilita la investigación de eventos
- Se mantiene actualizado con regularidad con nuevas firmas y reglas para abordar las amenazas emergentes.
- Es ligero y consume pocos recursos

8.5.4 Fail2ban (Prevención activa de intrusiones)

Está diseñada para proteger servidores y sistemas contra ataques de fuerza bruta y otros tipos de ataques automatizados. Su enfoque principal es la prevención de intrusiones al bloquear el acceso de direcciones IP que muestran comportamientos sospechosos o maliciosos.

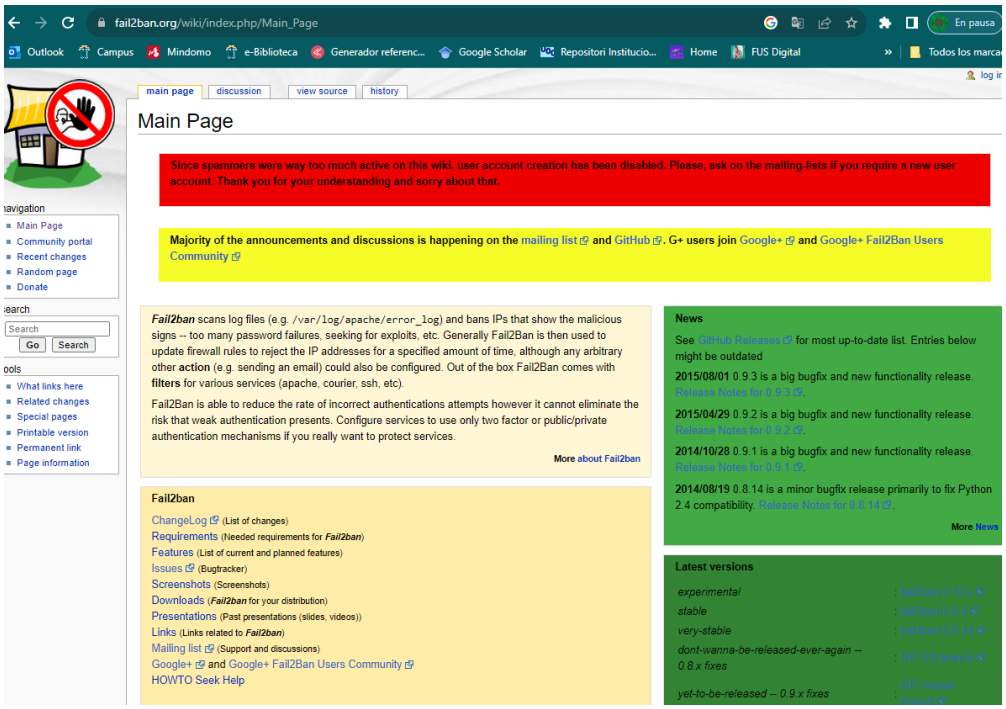

Ilustración 23. Wiki de fail2Ban. Fuente: Elaboración propia

Por su enfoque contra los ataques de fuerza bruta destaca especialmente en:

- Es altamente efectivo para prevenir intrusiones bloqueando automáticamente direcciones IP que realizan intentos de acceso fallidos o comportamientos sospechosos.

- Se puede utilizar para proteger una variedad de servicios y aplicaciones, incluyendo SSH, FTP, HTTP, correos electrónicos y más.

- Genera registros detallados de actividad, lo que facilita la identificación y el análisis de posibles amenazas.

- No bloquea permanentemente las direcciones IP, sino que aplica bloqueos temporales, lo que minimiza el riesgo de bloquear direcciones legítimas de manera permanente.

9 ETAPA 5.1: ANÁLISIS DEL EJERCICIO E IMPORTANCIA DE LA INTEGRACIÓN DE EQUIPOS AZULES, ROJOS Y PURPURAS PARA LA SEGURIDAD DIGITAL DE LA INFORMACIÓN.

El resultado del ejercicio de implementar ambos equipos en el caso de estudio demuestra que, en un panorama digital cada vez más amenazante, la seguridad de la información digital se ha convertido en una prioridad ineludible para organizaciones y que esta debe ser tenida en cuenta no solo por el departamento TI sino también por la gerencia general y el gobierno digital.

De la protección de activos digitales y la continuidad de operaciones dependen en gran medida de la capacidad de una organización para anticipar, detectar y mitigar amenazas cibernéticas. Para alcanzar estos objetivos el adoptar la estrategia de integración de equipos especializados en seguridad cibernética, entre ellos los equipos Azules, rojos y purpuras.

Son múltiples los beneficios que ofrece a la organización la implementación y coordinación de estos equipos. Se presenta a continuación los puntos mas destacables basado en el ejercicio realizado, y las ventajas que pudo haber ofrecido coordinar la estrategia de los equipos rojo y azul con un equipo purpura como articulador.

9.1 CONCIENCIA DE LAS AMENAZAS

La integración y organización de los equipos de seguridad permite obtener una comprensión más completa de las amenazas. Los equipos rojo y azul se complementan de manera fundamental. El equipo rojo, al actuar como atacante simulado, pone a prueba la infraestructura de seguridad desde una perspectiva realista, identificando debilidades y explotando vulnerabilidades potenciales. Esta información es invaluable para el equipo azul, ya que les brinda una visión de primera mano de cómo operan los adversarios en el mundo real, lo que a su vez les ayuda a afinar sus estrategias de defensa.

Por otro lado, el equipo púrpura, desempeña un papel crucial como mediador y facilitador de la colaboración entre el equipo rojo y el equipo azul. Actúa como un puente que conecta la simulación de ataque con las operaciones de defensa en tiempo real. El equipo púrpura planifica y coordina pruebas de penetración controladas junto con el equipo rojo y luego comparte los resultados, hallazgos y recomendaciones con el equipo azul. Esto garantiza que los conocimientos adquiridos durante las pruebas de penetración se traduzcan en mejoras prácticas en las estrategias de seguridad y en la infraestructura de la organización.

En conjunto, esta integración de equipos crea una sinergia que no solo mejora la postura de seguridad de la organización, sino que también promueve un ciclo de mejora continua en el que los equipos aprenden y se adaptan constantemente en respuesta a las amenazas emergentes.

9.2 MEJORA DE LA PREPARACIÓN Y DE LA CAPACIDAD DE RESPUESTA

La colaboración entre el equipo azul y el equipo rojo en el marco del equipo purpura mejora significativamente la preparación de la organización para futuros ataques. El equipo rojo ofrece información crítica sobre debilidades que el azul puede abordar proactivamente. Esta colaboración no solo se limita a la identificación de vulnerabilidades, sino que también incluye la simulación de incidentes y ataques reales que permiten al Blue Team perfeccionar sus respuestas y técnicas de mitigación. Asimismo, el equipo facilita la comunicación efectiva y asegurando que los hallazgos y las lecciones aprendidas se implementen eficazmente para fortalecer las defensas de la organización.

9.3 USO EFICIENTE DE LOS RECURSOS DE TI

La integración de los equipos garantiza que en lugar de duplicar esfuerzos o trabajar de manera independiente, los equipos colaboran estrechamente para abordar las áreas de mayor riesgo y prioridad en términos de seguridad. Esto se traduce en una asignación más inteligente de recursos humanos y tecnológicos, evitando gastos innecesarios y redundancias.

El ejercicio realizado es un ejemplo práctico de este uso eficiente de recursos es la planificación de ejercicios de simulación de ataques. En lugar de realizar ejercicios separados, Red Team y Blue Team pueden colaborar en la creación de escenarios realistas guiados por el equipo purpura y que estos desafiantes y que involucren a ambos equipos. Esto ahorra tiempo y recursos, al tiempo que mejora la calidad y la efectividad de los ejercicios.

10 ETAPA 5.2 POLÍTICAS Y RECOMENDACIONES PROPUESTAS PARA EL ROBUSTECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Como resultado de este ejercicio se puede observar que, para fortalecer la seguridad de la información, es esencial establecer políticas de seguridad claras y efectivas. Pero las políticas no son suficientes, estas deben ser aplicables y ser adaptadas según evolucionen las necesidades de la infraestructura y la capacidad de la organización.

Se hace énfasis en la **Política de capacitación en seguridad de la información**, ya que no solo el resultado del incidente fue logrado debido al desconocimiento del usuario afectado, sino también porque esta política puede ser implementada de forma inmediata sin necesidad de ninguna modificación infraestructural. A cambio, ofrece la capacidad de cambiar la cultura organizacional hacia una mayor conciencia y responsabilidad en cuanto a la seguridad cibernética. Al educar a los empleados sobre las amenazas y prácticas de seguridad, la organización está mejor preparada para prevenir incidentes y responder de manera efectiva en caso de que ocurran.

10.1 POLÍTICA DE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Esta política establece las siguientes pautas para todo el personal de la organización:

10.1.1 Objetivos de Capacitación

1. Proporcionar a todos los empleados una comprensión sólida de los principios básicos de la seguridad cibernética, incluyendo las amenazas comunes y las mejores prácticas de seguridad.
2. Educar a los empleados sobre los procedimientos y políticas específicos de seguridad cibernética de la organización.
3. Capacitar a los empleados para identificar posibles amenazas cibernéticas, como correos electrónicos de phishing y malware.
4. Asegurar que los empleados sepan cómo reportar incidentes de seguridad y a quién deben informar.
5. Fomentar una cultura de seguridad cibernética en toda la organización.

10.1.2 Contenido de la Capacitación

Este contenido debe ser dado a todos los empleados nuevos y antiguos, debe establecerse con el área de recursos humanos la articulación para la creación de los espacios necesarios. También es importante tener en cuenta que esta capacitación ha de ser continua y debe ser renovada al menos una vez por año.

1. Introducción a la seguridad cibernética.
2. Identificación de amenazas comunes, como phishing, ransomware y ataques de ingeniería social.
3. Uso seguro de contraseñas y autenticación de dos factores.
4. Políticas y procedimientos de seguridad cibernética de la organización*.
5. Uso seguro de dispositivos y redes corporativas.
6. Cómo reconocer y reportar incidentes de seguridad.
7. Cumplimiento con regulaciones y estándares de seguridad aplicables.

*Estas serán las políticas aquí descritas, se debe manejar la ultima actualización de las mismas.

10.1.3 Programa de capacitación continua

1. Se establecerá un programa de capacitación que incluya módulos en línea y sesiones presenciales, según sea necesario.
2. Todos los empleados nuevos recibirán capacitación en seguridad cibernética como parte de su proceso de incorporación.
3. Los empleados existentes recibirán capacitación de seguridad cibernética al menos una vez al año, con actualizaciones periódicas para mantenerse al tanto de las últimas amenazas y mejores prácticas.
4. Se mantendrán registros de la asistencia y el progreso de la capacitación para cada empleado.

10.1.4 Cumplimiento y sanciones

1. Los empleados están obligados a completar la capacitación en seguridad cibernética según lo especificado en esta política.
2. El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la suspensión o terminación del empleo, dependiendo de la gravedad del incumplimiento y las circunstancias.

10.1.5 Evaluación de la efectividad

1. Se llevará a cabo una evaluación periódica de la efectividad del programa de capacitación en seguridad cibernética.

2. Se recopilarán comentarios de los empleados para mejorar continuamente el contenido y la entrega de la capacitación.

10.2 POLÍTICAS DE SEGURIDAD PROPUESTAS PARA ROBUSTECER LA INFRAESTRUCTURA

Se presenta adicionalmente las políticas de seguridad básicas para mejorar y robustecer la infraestructura de la organización. Estas políticas son generales y deben ser refinadas durante su implementación y según evolucione el riesgo organizacional.

10.2.1 Política de evaluación de riesgos

Realizar una evaluación exhaustiva de los riesgos de seguridad cibernética para identificar las amenazas y vulnerabilidades específicas de la organización. Esta revisión debe ser realizada de manera periódica por el área de TI para su implementación debe crearse un formato que incluye características como

- Tipo de riesgo
- Nivel de riesgo
- Impacto potencial
- Probabilidad de ocurrencia
- Áreas o sistemas afectados
- Responsable de la mitigación
- Fecha límite de mitigación

Una vez que se haya realizado la evaluación de riesgos, es importante establecer un plan de acción claro para abordar las vulnerabilidades identificadas. Esto puede incluir la implementación de medidas de seguridad adicionales, la actualización de políticas y procedimientos existentes, y la asignación de responsabilidades específicas para la mitigación de riesgos.

10.2.2 Política de gestión de contraseñas

Se establece una política de contraseñas sólidas para garantizar la seguridad de los sistemas y datos. Esta política requiere que los empleados sigan prácticas seguras de contraseña, que incluyen:

- Contraseñas complejas que combinan letras mayúsculas y minúsculas, números y caracteres especiales.
- Rotación de contraseñas cada 90 días.

- No compartir contraseñas y evitar el almacenamiento no seguro de contraseñas.

10.2.3 Política de actualización de software y parches

- Mantener la seguridad de los sistemas mediante la aplicación oportuna de actualizaciones de software y parches.
- Actualización de todo el software y sistemas con los últimos parches de seguridad en un plazo de 30 días después del último reléase importante.
- Revisión regular de actualizaciones pendientes y aplicación inmediata de parches críticos.
- Establecimiento de un proceso para probar parches en un entorno de desarrollo antes de aplicarlos en producción para el software organizacional.

10.2.4 Política de control de acceso

Esta política establece las siguientes directrices para limitar el alcance de potenciales atacantes

- Limitar el acceso a sistemas y datos solo a empleados autorizados con base en la necesidad de su trabajo. Para su implementación se requiere.
    - Separar por áreas seguras los recursos, especialmente los críticos tales como los servidores
    - Separa los accesos a los recursos por roles
    - Monitorear el acceso a los recursos
- Emplear autenticación de dos factores (2FA) siempre que sea posible para verificar la identidad de los usuarios.
    - Para esto es importante aprovechar las alternativas que ofrece de 2FA Microsoft, Google o el proveedor alternativo que se maneje
- Revisar y ajustar regularmente los niveles de acceso para asegurarse de que reflejen los roles y responsabilidades actuales del personal.

10.2.5 Política de gestión de incidentes

Se establece la siguiente política para dar capacidad de reacción a la organización en caso de un evento de seguridad

- Se debe establecer un procedimiento claro para la notificación de incidentes de seguridad.
    - Notificar por correo, teams, etc y documentar
    - Se debe establecer un responsable para esto
- Se debe documentar cada incidente, incluyendo detalles sobre la naturaleza del incidente, el impacto potencial y las medidas tomadas para contenerlo y mitigarlo.
- Después de cada incidente, se debe llevar a cabo una revisión post-incidente para evaluar lo sucedido y determinar mejoras en la preparación y respuesta futura.

CONCLUSIONES

La comprensión de los conceptos relevantes a la seguridad de la información es una necesidad crítica tanto del profesional de seguridad como de la organización. En el contexto colombiano, el estudio de la legislación relacionada con la seguridad de la información, como la Ley 1273 de 2009 y la Ley 1581 de 2012, es esencial para garantizar el cumplimiento de las normativas de protección de datos y la prevención de delitos informáticos. Además, se ha destacado la importancia de contar con una metodología sólida en las pruebas de penetración (pentesting) para obtener resultados efectivos. Se ha otorgado especial relevancia a la etapa de reconocimiento (footprinting), ya que esta fase permite identificar vulnerabilidades y evaluar proactivamente la seguridad de los sistemas, brindando así a la organización la capacidad de implementar medidas preventivas con el fin de salvaguardar sus activos digitales.

Para el ejercicio como profesional tanto ingeniero de sistemas o áreas afines, así como para el caso específico del especialista en seguridad es necesario el adecuado cumplimiento de la legislación colombiana, tanto en protección de datos (Ley 1581 de 2012) como para delitos informáticos (1273 de 2009), para evitar situaciones legales posibles que pueden llegar desde multas hasta penas de prisión no excarcelables. Esto se suma al cumplimiento del código de ética del Copnia y evitar sanciones que van desde notificaciones a la suspensión temporal o permanente de la licencia del profesional. Por tanto, el estudio detenido de cualquier contrato debe estar debidamente estipulado, resaltando los peligros y riesgos de aceptar compromisos ilegales en dicho contrato, lo que puede resultar en consecuencias legales y éticas adversas tanto para el profesional como para la entidad contratante y la reputación de ambos.

Como lo demuestra el laboratorio realizado la labor del equipo rojo es de vital importancia para la organización y su capacidad de detección de problemas en la seguridad de la información. Su capacidad para identificar vulnerabilidades específicas en la red de y en el equipo vulnerado ha proporcionado una visión clara de los puntos débiles en la infraestructura de seguridad evaluada, lo que fue también fundamental para guiar las tareas de respuesta por parte del equipo azul. Además, el diseño y desarrollo del laboratorio de simulación permitió una reproducción altamente realista del suceso, brindando una experiencia práctica invaluable para comprender cómo se llevan a cabo los ataques y qué medidas preventivas deben implementarse.

En contraste el rol del equipo azul en la protección de la organización es actuar contra los riesgos emergentes de seguridad hallados. Su labor no solo radica en la detección y mitigación de amenazas, sino también en establecer una línea de defensa efectiva que fortalezca la postura de seguridad de la organización. El uso

de guías reconocidas como las proporcionadas por CIS se ha demostrado como un enfoque acertado, ya que brinda directrices estandarizadas respaldadas por el conocimiento y la experiencia de una entidad con reconocimiento global por su experticia, permitiendo una toma de decisiones informada y eficiente. En este contexto, las soluciones SIEM y, especialmente, las tecnologías XDR se presentan como una solución para abordar las amenazas de manera proactiva. Entre estas, XDR se erige como la opción más recomendable, ofreciendo un enfoque integral y avanzado. El optar por herramientas de seguridad de software libre no solo implica un ahorro de costos, sino que también proporciona la ventaja de contar con código visible y herramientas respaldadas por comunidades activas, otorgando flexibilidad y confiabilidad en la protección.

Finalmente, la integración entre los equipos azul, rojo y púrpura se destaca como una excelente estrategia para fortalecer la postura de seguridad de la organización. La colaboración y el intercambio de conocimientos entre estos equipos permiten una detección temprana, una respuesta ágil y una corrección eficiente de las amenazas. Esto debe estar acompañado de la creación de una **cultura de seguridad de la información** en toda la organización el cual debe ser un objetivo de la alta gerencia, la concienciación y la formación constante son herramientas clave para involucrar a todos los empleados en la protección de los activos digitales. Se resalta por último la importancia de la implementación y evolución de las políticas de seguridad aquí presentadas, adaptándolas a las cambiantes necesidades y amenazas. Estas políticas proporcionan un marco inicial sólido para guiar las prácticas de seguridad y garantizar el cumplimiento de estándares y regulaciones.

BIBLIOGRAFÍA

BASIS TECH. About Autopsy. Autopsy [página web]. [Consultado el 28, septiembre, 2023]. Disponible en Internet: <https://www.autopsy.com/about/>.

BLACKBERRY. XDR vs SIEM: what's the difference? BlackBerry [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.blackberry.com/us/en/solutions/endpoint-security/extended-detection-and-response/xdr-vs-siem>.

CISCO. Snort documents. Snort [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: <https://www.snort.org/documents#OfficialDocumentation>.

CHIROU, Álvaro. Metasploit: la herramienta definitiva para pruebas de seguridad. Achirou [página web]. (9, julio, 2023). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://achirou.com/metasploit-la-herramienta-definitiva-para-pruebas-de-seguridad/>.

COLOMBIA. CONGRESO DE COLOMBIA. Ley 1273 [en línea]. (5, enero, 2009). De la Protección de la información y de los datos. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>.

----------. Ley 1581 [en línea]. (17, octubre, 2012) [consultado el 25, septiembre, 2023]. Disposiciones generales para la protección de datos personales. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

COPNIA. Código de ética |. Copnia [página web]. (2023). [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

DIOGENES, Yuri y OZKAYA, Erdal. Cybersecurity – attack and defense strategies: infrastructure security with red team and blue team tactics. [s.l.]: Packt Publishing, 2018. 384 p. ISBN 9781788475297.

GRANGER, Sarah. Social engineering fundamentals. Symantec Enterprise [página web]. (18, diciembre, 2001). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=891b1f29-e2e7-4484-89c0-a2137ee82f8b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.

IBM. What is threat intelligence? IBM [página web]. [Consultado el 23, septiembre, 2023]. Disponible en Internet: <https://www.ibm.com/topics/threat-intelligence>.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Seguridad de la información. ISO/IEC 27001. [s.l.]: ISO, 2013.

ISO27K. ISO/IEC 27001 certification standard. ISO27k infosec [página web]. (2022). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.iso27001security.com/html/27001.html>.

KEEPCODING. ¿Qué es blue team en ciberseguridad? KeepCoding Bootcamps [página web]. (2023). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/>.

LOPEZ DELGADO, Miguel. Análisis forense digital [en línea]. 2a ed. Bogotá: MinTIC, 2007 [consultado el 23, septiembre, 2023]. 40 p. Disponible en Internet: <https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf>.

NORMAS ISO. ISO 27001 - seguridad de la información: norma ISO IEC 27001/27002. Normas ISO [página web]. [Consultado el 25, septiembre, 2023]. Disponible en Internet: <https://www.normas-iso.com/iso-27001/>.

OSIF. Home - suricata. Suricata [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://suricata.io/>.

OSTEC. ¿Qué es security awareness? OSTEC [página web]. (1, agosto, 2022). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://ostec.blog/es/aprendizaje-descubrimiento/que-es-security-awareness/>.

OWASP. Authentication. OWASP Cheat Sheet Series [página web]. (2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html>.

--------. Authorization. Introduction - OWASP Cheat Sheet Series [página web]. (2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html>.

RED HAT SOFTWARE. What is a CVE? Red Hat [página web]. (25, noviembre, 2021). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.redhat.com/en/topics/security/what-is-cve>.

ROUSE, Margaret. Equipo rojo-Equipo azul. KW Foundation [página web]. (10, diciembre, 2020). [Consultado el 25, septiembre, 2023]. Disponible en Internet:

<https://kwfoundation.org/blog/2020/12/10/equipo-rojo-equipo-azul/#htoc-red-team-the-network>.

SYNOPSYS EDA TOOLS. What is penetration testing and how does it work? Synopsys [página web]. (2023). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.synopsys.com/glossary/what-is-penetration-testing.html>.

TECHTARGET. What is red teaming? WhatIs.com [página web]. (21, abril, 2021). [Consultado el 24, septiembre, 2023]. Disponible en Internet: <https://www.techtarget.com/whatis/definition/red-teaming>.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN. Guía de actividades y rúbrica de evaluación – Etapa 2 Actuación ética y legal - Anexo 3: ACUERDO DE CONFIDENCIALIDAD. Bogotá: UNAD, 2023. 12 p. Guia de trabajo.

ZOLA, Andrew. What is footprinting in ethical hacking? Techtarget [página web]. (23, noviembre, 2021). [Consultado el 26, septiembre, 2023]. Disponible en Internet: <https://www.techtarget.com/searchsecurity/definition/footprinting>.

ANEXOS

10.3 VIDEO DE SUSTENTACIÓN, VINCULO 1

Youtube:

https://youtu.be/ShDepY7_Wpo

10.4 VIDEO DE SUSTENTACIÓN, VINCULO 2

OneDrive:

SERGIO_ANDRES_RODRÍGUEZ_RODRÍGUEZ_-_SEMINARIO_ESPECIALIZADO_EQUIPOS_ESTRATÉGICOS_EN_CIBERSEGURIDAD_RED_TEAM_&_BLUE_TEAM_(202337164A_1438)_–_SUSTENTACION_FINAL.mp4