# Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

Laura Marcela Bastidas Lame

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

## Dedicatoria

Dedico este trabajo principalmente a Dios, por brindarme la fortaleza, la salud y la sabiduría necesarias para continuar este proceso académico y superar cada uno de los retos presentados durante mi formación profesional.

A toda mi familia, por su apoyo incondicional, comprensión, paciencia y motivación constante en cada etapa de este camino, siendo un pilar fundamental para alcanzar mis metas personales y académicas.

También dedico este trabajo a todas las personas que, de una u otra manera, contribuyeron con sus conocimientos, consejos y acompañamiento durante el desarrollo de este seminario, permitiéndome fortalecer mis habilidades y ampliar mis conocimientos en el área de la ciberseguridad, especialmente a mis compañeros de trabajo, los cuales siempre me ayudaron y me aconsejaron para no rendirme y seguir cumplimiento cada meta.

Finalmente, dedico este esfuerzo a mi crecimiento profesional, con el propósito de seguir aprendiendo y aplicando de manera ética y responsable los conocimientos adquiridos durante este proceso formativo.

**Agradecimientos**

Expreso mis más sinceros agradecimientos a la Universidad Nacional Abierta y a Distancia – UNAD, por brindar espacios de aprendizaje que fortalecen las competencias académicas y profesionales desde el inicio de mi formación de pregrado al postgrado.

De igual forma, agradezco al ingeniero Eduvin Trigos Sánchez por su orientación, acompañamiento y disposición durante el desarrollo de las diferentes actividades, así como por compartir conocimientos que contribuyeron al fortalecimiento de habilidades técnicas y analíticas relacionadas con la seguridad informática.

Asimismo, agradezco a mi familia por el apoyo, la paciencia y la motivación brindada durante este proceso académico, especialmente en los momentos que requirieron mayor dedicación y esfuerzo.

**Resumen**

La presente actividad tiene como finalidad el desarrollo de las actividades relacionadas con los equipos estratégicos Red Team y Blue Team dentro de un entorno controlado de ciberseguridad. A través de diferentes escenarios prácticos se analizaron aspectos éticos, legales, ofensivos y defensivos asociados a la protección de infraestructuras tecnológicas. Durante el desarrollo del laboratorio se utilizaron máquinas virtuales Windows 7 y Kali Linux configuradas en VirtualBox, permitiendo ejecutar procesos de reconocimiento, escaneo de puertos, identificación de vulnerabilidades y simulación de explotación mediante herramientas especializadas como Nmap y Metasploit Framework. Posteriormente, desde el enfoque Blue Team, se plantearon estrategias orientadas al monitoreo, contención y fortalecimiento de la seguridad, incluyendo medidas de hardenización, implementación de controles de acceso, uso de sistemas SIEM y herramientas de prevención de intrusiones. Asimismo, se abordaron temas relacionados con ética profesional y marco normativo en ciberseguridad, resaltando la importancia del uso responsable de herramientas ofensivas y el cumplimiento de la legislación colombiana frente a delitos informáticos. Los resultados obtenidos permitieron comprender cómo las vulnerabilidades presentes en sistemas desactualizados pueden ser aprovechadas por atacantes, así como la relevancia de aplicar mecanismos preventivos y correctivos para reducir riesgos de seguridad dentro de las organizaciones. Finalmente, la actividad fortaleció los conocimientos técnicos y analíticos relacionados con pruebas de penetración, gestión de incidentes y estrategias defensivas aplicadas en entornos reales de ciberseguridad.

***Palabras clave*:** ciberseguridad, defensa, incidentes, pentesting, vulnerabilidades.

**Abstract**

The purpose of this activity is to develop skills related to the Red Team and Blue Team strategic teams within a controlled cybersecurity environment. Through various practical scenarios, ethical, legal, offensive, and defensive aspects associated with the protection of technological infrastructures were analyzed. During the lab, Windows 7 and Kali Linux virtual machines configured in VirtualBox were used, allowing for reconnaissance, port scanning, vulnerability identification, and exploitation simulation using specialized tools such as Nmap and Metasploit Framework. Subsequently, from the Blue Team perspective, strategies were developed for monitoring, containing, and strengthening security, including hardening measures, implementation of access controls, use of SIEM systems, and intrusion prevention tools. Topics related to professional ethics and the regulatory framework in cybersecurity were also addressed, highlighting the importance of the responsible use of offensive tools and compliance with Colombian legislation regarding cybercrime. The results obtained allowed us to understand how vulnerabilities in outdated systems can be exploited by attackers, as well as the importance of implementing preventative and corrective measures to reduce security risks within organizations. Finally, the activity strengthened technical and analytical knowledge related to penetration testing, incident management, and defensive strategies applied in real-world cybersecurity environments.

***Keywords*****:** cybersecurity, defense, incidents, penetration testing, vulnerabilities.

# Tabla de Contenido

Glosario ..... 12

Introducción ..... 15

Justificación ..... 16

Objetivos ..... 17

Objetivo General ..... 17

Objetivos Específicos ..... 17

Fundamentos de Operaciones Red Team y Blue Team ..... 18

Análisis de la legislación relacionada con delitos informáticos. ..... 18

Análisis sobre el ejercicio de Pentesting. ..... 19

Explicación de las herramientas y servicios utilizados en ciberseguridad ..... 21

Herramientas ..... 21

Metasploit. ..... 21

Nmap. ..... 22

OpenVas. ..... 23

Servicios en línea ..... 23

ExploitDB. ..... 23

CVE (Common Vulnerabilities and Exposures). ..... 24

Configuración y análisis del banco de trabajo ..... 24

Ética Profesional y Marco Normativo en Ciberseguridad ..... 29

Identificación de procesos ilegales o no éticos. ..... 29

Vulneración de la Ley 1273 de 2009. ..... 31

Oferta laboral en SecureNova Labs. ..... 33

Argumentación con base en el código de ética del COPNIA. ..... 35

Acceso a información sensible en auditorías. ..... 36
Mecanismos de supervisión y control. ..... 37
Respuesta ante ciberespionaje. ..... 39
Estrategia de Red Team ..... 42
Herramientas y procedimientos utilizados. ..... 42
Fase 1. Reconocimiento ..... 42
Fase 2. Enumeración ..... 45
Fase 3. Identificación de Vulnerabilidad ..... 47
Fase 4. Explotación ..... 49
Fase 5. Escalamiento de Privilegios ..... 51
Fase 6. Post-Explotación y Persistencia ..... 52
Fase 7. Pivoting ..... 53
Datos e Información para Identificar el Fallo de Seguridad ..... 54
Herramienta Utilizada Para Identificar Fallos ..... 55
Análisis del Ataque Presentado ..... 58
Respuesta y Contención ante Incidentes de Ciberseguridad ..... 61
Acciones Ante un Ataque en Tiempo Real ..... 61
Medidas de Hardenización ..... 62
Diferencia entre Blue Team y Respuesta a Incidentes (IR) ..... 64
Uso de CIS (Center for Internet Security) ..... 67
Funciones y características de un SIEM ..... 68
Herramientas de Contención ..... 71
1. Firewall ..... 72
2. Endpoint Detection and Response (EDR) ..... 72

3. Network Access Control (NAC)..... 73

4. Sistemas de Prevención de Intrusiones (IPS) ..... 74

Evidencias de Sustentación.....76

Conclusiones.....77

Recomendaciones .....79

Referencias Bibliográficas.....81

Apéndices.....84

## Lista de Figuras

**Figura 1** *Apertura de la Maquina VirtualBox Instalada en el Equipo* ..... 25

**Figura 2** *Importación de máquinas virtuales* ..... 26

**Figura 3** *Configuración de red y conectividad* ..... 26

**Figura 4** *Instalación de las máquinas virtuales en VirtualBox* ..... 42

**Figura 5** *Identificación de la Dirección IP en Kali Linux* ..... 43

**Figura 6** *Identificación de la Dirección IP en Windows (Host A y Host B)* ..... 43

**Figura 7** *Escaneo de redes* ..... 44

**Figura 8** *Verificación de conexión entre las redes* ..... 45

**Figura 9** *Escaneo de puertos – Host A* ..... 46

**Figura 10** *Identificación de vulnerabilidad – Rejjeto* ..... 47

**Figura 11** *Buscar el exploit para Rejjeto / HFS* ..... 48

**Figura 12** *Inicio de Metasploit en Kali Linux* ..... 49

**Figura 13** *Conexión remota* ..... 50

**Figura 14** *Control del sistema atacante* ..... 51

**Figura 15** *Flujo del ataque en el escenario Red Team* ..... 59

## Lista de Tablas

**Tabla 1** *Características técnicas de las máquinas virtuales utilizadas en el entorno de laboratorio* ..... 27

**Tabla 2** *Clasificación de Herramientas para Identificación de Fallos de Seguridad* ..... 57

**Tabla 3** *Comparación entre Blue Team y Respuesta a Incidentes* ..... 66

**Tabla 4** *Principales Características de un SIEM* ..... 70

**Tabla 5** *Diferencia entre Herramientas de Detección y Contención* ..... 75

## Lista de Apéndices

**Apéndice A** *Resultado de revisión en Turnitin* ..... 84

# Glosario

**Análisis forense:**

Proceso técnico utilizado para recopilar, preservar y analizar evidencias digitales relacionadas con incidentes de ciberseguridad.

**Ataque:**

Acción realizada con el propósito de vulnerar, afectar o comprometer un sistema informático, red o dispositivo.

**Blue Team:**

Equipo encargado de las actividades defensivas de ciberseguridad, incluyendo monitoreo, detección y respuesta ante incidentes.

**Ciberseguridad:**

Conjunto de medidas, procesos y herramientas orientadas a proteger sistemas, redes e información digital frente a amenazas informáticas.

**Contención:**

Acción orientada a limitar el impacto o propagación de un incidente de seguridad.

**EDR:**

Herramienta de seguridad enfocada en la detección, análisis y respuesta ante amenazas en equipos finales o endpoints.

**Escaneo:**

Proceso utilizado para identificar dispositivos, puertos, servicios o vulnerabilidades dentro de una red.

**Exploit:**

Código o técnica utilizada para aprovechar una vulnerabilidad presente en un sistema.

**Firewall:**

Herramienta de seguridad encargada de controlar y filtrar el tráfico de red entrante y saliente.

**Hardening:**

Proceso de fortalecimiento de sistemas mediante configuraciones seguras y reducción de vulnerabilidades.

**IDS:**

Sistema de detección de intrusiones encargado de identificar actividades sospechosas o maliciosas.

**Incidente:**

Evento que compromete la seguridad, integridad o disponibilidad de la información o los sistemas.

**Ingeniería social:**

Técnica utilizada para manipular personas y obtener información sensible o accesos no autorizados.

**IPS:**

Sistema de prevención de intrusiones diseñado para detectar y bloquear actividades maliciosas en tiempo real.

**Kali Linux:**

Distribución de Linux especializada en pruebas de penetración y auditorías de seguridad informática.

**Malware:**

Software malicioso diseñado para afectar, dañar o comprometer sistemas informáticos.

**Metasploit:**

Framework utilizado para pruebas de penetración y explotación de vulnerabilidades.

**Monitoreo:**

Supervisión continua de sistemas y redes con el fin de detectar amenazas o actividades sospechosas.

**Nmap:**

Herramienta utilizada para reconocimiento de red y escaneo de puertos.

**Pentesting:**

Evaluación controlada de seguridad orientada a identificar vulnerabilidades explotables.

**Pivoting:**

Técnica utilizada para desplazarse desde un sistema comprometido hacia otros equipos dentro de una red.

**Puertos:**

Canales de comunicación utilizados por servicios y aplicaciones dentro de una red.

**Red Team:**

Equipo encargado de ejecutar pruebas ofensivas controladas para identificar vulnerabilidades.

**Riesgo:**

Probabilidad de que una amenaza aproveche una vulnerabilidad y genere un impacto negativo.

**SIEM:**

Plataforma orientada a recopilar, correlacionar y analizar eventos de seguridad generados por diferentes sistemas.

**Vulnerabilidad:**

Debilidad o falla de seguridad que puede ser aprovechada por un atacante.

## Introducción

En la actualidad, la tecnología hace parte fundamental del funcionamiento de las organizaciones, ya que permite gestionar información, automatizar procesos y facilitar múltiples actividades diarias. Sin embargo, el crecimiento de los entornos digitales también ha incrementado las amenazas informáticas y los riesgos asociados a vulnerabilidades que pueden afectar la seguridad de los sistemas y la información.

En este caso, la ciberseguridad cumple un papel esencial para proteger los activos tecnológicos de las organizaciones. Por esta razón, los equipos Red Team y Blue Team desarrollan funciones importantes dentro de las estrategias de seguridad informática, la cooperación entre ambos equipos permite fortalecer las capacidades de defensa mediante la identificación y corrección de vulnerabilidades (Chindrus & Caruntu, 2023). Mientras el Red Team realiza pruebas ofensivas controladas para identificar vulnerabilidades, el Blue Team se encarga del monitoreo, protección y respuesta frente a incidentes de seguridad.

El desarrollo de esta actividad permitió aplicar conocimientos técnicos y estratégicos mediante un entorno virtualizado con Windows 7 y Kali Linux en VirtualBox, donde se realizaron procesos de reconocimiento, escaneo de puertos, identificación de vulnerabilidades y simulación de explotación utilizando herramientas como Nmap y Metasploit Framework. Asimismo, desde el enfoque defensivo, se analizaron mecanismos de hardenización, monitoreo y contención de ataques mediante el uso de firewalls, sistemas SIEM y controles de seguridad.

Finalmente, esta actividad permitió fortalecer conocimientos relacionados con pruebas de penetración, análisis de riesgos y estrategias de defensa informática, comprendiendo la importancia de implementar medidas preventivas que contribuyan a proteger la infraestructura tecnológica de una organización.

## Justificación

El desarrollo de esta actividad resulta importante debido a la necesidad actual de fortalecer las competencias relacionadas con análisis ofensivo y defensivo en ciberseguridad. Las organizaciones enfrentan constantemente amenazas que pueden comprometer sus sistemas y afectar la continuidad operativa.

A través del desarrollo de escenarios prácticos de Red Team y Blue Team fue posible comprender cómo un atacante puede aprovechar vulnerabilidades presentes en sistemas desactualizados y, al mismo tiempo, identificar estrategias de defensa orientadas a prevenir, detectar y contener incidentes de seguridad.

Asimismo, esta actividad permitió fortalecer conocimientos relacionados con el uso ético de herramientas de ciberseguridad, la aplicación de estándares de seguridad y la importancia de implementar mecanismos de protección que reduzcan riesgos tecnológicos dentro de una organización.

# Objetivos

## Objetivo General

Analizar las estrategias ofensivas y defensivas aplicadas por los equipos Red Team y Blue Team en escenarios controlados de ciberseguridad, con el fin de identificar vulnerabilidades, fortalecer mecanismos de protección y proponer estrategias de contención dentro de una infraestructura tecnológica.

## Objetivos Específicos

Identificar vulnerabilidades presentes en sistemas Windows mediante técnicas de reconocimiento y escaneo.

Analizar herramientas utilizadas durante procesos de pentesting y monitoreo de seguridad.

Evaluar medidas de hardenización orientadas a fortalecer la seguridad de los sistemas.

Comprender las funciones del Blue Team en procesos de monitoreo y respuesta ante incidentes.

Aplicar criterios éticos y legales relacionados con la ciberseguridad.

Proponer recomendaciones de seguridad orientadas a reducir riesgos tecnológicos.

## Fundamentos de Operaciones Red Team y Blue Team

La ciberseguridad se ha convertido en un pilar fundamental para la protección de la información en entornos digitales, especialmente ante el incremento de amenazas informáticas que afectan tanto a organizaciones como a usuarios individuales. En este contexto, los equipos Red Team y Blue Team desempeñan un papel clave al simular ataques y fortalecer las defensas de los sistemas, respectivamente, siempre bajo principios éticos y legales.

### Análisis de la legislación relacionada con delitos informáticos.

En Colombia, el marco legal relacionado con los delitos informáticos y la protección de datos personales ha evolucionado con el fin de responder a los riesgos asociados al uso de las tecnologías de la información. Estas normativas buscan garantizar la seguridad digital, proteger los derechos de los ciudadanos y establecer sanciones frente a conductas ilícitas en el entorno digital.

En primer lugar, se destaca la Ley 1273 de 2009, conocida como la ley de delitos informáticos. Esta norma introdujo en el Código Penal colombiano un nuevo bien jurídico denominado “la protección de la información y de los datos”. A partir de esta ley, se tipifican conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos, el daño informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios web. Su característica principal es que establece sanciones penales (multas y privación de la libertad) para quienes atenten contra la confidencialidad, integridad y disponibilidad de la información (Congreso de la República de Colombia, 2009).

Por otra parte, en materia de protección de datos personales, una de las normas más relevantes es la Ley 1581 de 2012, la cual establece el régimen general de protección de datos personales en Colombia. Esta ley reconoce el derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos.

Asimismo, define principios como la legalidad, finalidad, libertad, veracidad, transparencia, acceso y seguridad, los cuales deben ser cumplidos por las organizaciones que traten datos personales (Congreso de la República de Colombia, 2012).

Complementando esta ley, se encuentra el Decreto 1377 de 2013, que reglamenta parcialmente la Ley 1581 de 2012. Este decreto detalla aspectos relacionados con la autorización del titular para el tratamiento de datos, las políticas de privacidad y los procedimientos para el ejercicio de los derechos de los titulares. Su principal característica es que establece lineamientos más específicos para que las organizaciones implementen adecuadamente la protección de datos (Presidencia de la República de Colombia, 2013).

Adicionalmente, la Ley 1266 de 2008, también conocida como la ley de habeas data financiero, regula el manejo de la información financiera, crediticia, comercial y de servicios. Esta ley busca proteger el derecho al buen nombre y la privacidad de las personas en relación con su historial crediticio, estableciendo reglas sobre la recolección, almacenamiento y circulación de este tipo de datos (Congreso de la República de Colombia, 2008).

En conjunto, estas normas constituyen un marco legal sólido que permite regular tanto las acciones ofensivas (como los delitos informáticos) como las responsabilidades defensivas (protección de datos), lo cual es fundamental para el análisis de las actividades de equipos Red Team y Blue Team dentro de una organización. Desde una perspectiva ética y legal, estas leyes obligan a que cualquier actividad de ciberseguridad se realice con autorización, respetando la privacidad y los derechos fundamentales de los usuarios.

**Análisis sobre el ejercicio de Pentesting.**

En el ámbito de la ciberseguridad, las pruebas de penetración o pentesting son procesos estructurados que permiten identificar vulnerabilidades en los sistemas de información antes de que sean explotadas por atacantes. Estas pruebas siguen una metodología organizada en etapas,

donde cada fase tiene un objetivo específico y utiliza herramientas especializadas, lo que garantiza un análisis sistemático, ético y controlado, alineado con los principios de los equipos Red Team (ofensivos) y Blue Team (defensivos), estas estrategias son complementarias, ya que combinan capacidades ofensivas y defensivas para mejorar la postura de seguridad organizacional (Kotwani, 2023).

La primera etapa es la planificación y reconocimiento (reconnaissance). En esta fase se define el alcance, los objetivos, los activos a evaluar y se obtiene la autorización formal de la organización, lo cual es fundamental desde el punto de vista legal. Además, se recopila información pública del objetivo mediante técnicas OSINT. Herramientas como Maltego permiten recolectar y analizar información de diversas fuentes, estableciendo relaciones entre datos como dominios, direcciones IP o usuarios (NFLO Tech, 2023). Esta etapa es fundamental porque permite construir una visión inicial del sistema objetivo sin interactuar directamente con él (Penetration Testing Authority, 2014).

La segunda etapa es el escaneo y enumeración. Aquí se identifican los sistemas activos, puertos abiertos, servicios y versiones de software. Esta fase permite detectar posibles vulnerabilidades técnicas. Una de las herramientas más utilizadas es Nmap, que permite descubrir hosts, servicios y características de seguridad en una red (Pentesting101, 2026). Este proceso facilita mapear la superficie de ataque del sistema evaluado (Penetration Testing Authority, 2014).

La tercera etapa es la explotación. En esta fase se intenta aprovechar las vulnerabilidades encontradas para obtener acceso al sistema, siempre bajo autorización. Una herramienta ampliamente utilizada es Metasploit Framework, que permite desarrollar y ejecutar exploits contra sistemas vulnerables, facilitando la simulación de ataques reales. Esta etapa demuestra el impacto real de las fallas de seguridad identificadas.

La cuarta etapa corresponde a la post-explotación. Una vez se ha logrado el acceso, se evalúa el nivel de control que se puede obtener sobre el sistema comprometido, incluyendo la escalación de privilegios o el movimiento lateral dentro de la red. En esta fase se pueden utilizar herramientas derivadas de Metasploit u otras utilidades para mantener acceso y analizar el alcance del ataque (Scribd, 2025).

Finalmente, la quinta etapa es la elaboración del informe (reporting). En esta fase se documentan todos los hallazgos, evidencias y recomendaciones para mitigar las vulnerabilidades encontradas. Herramientas como Dradis permiten organizar la información y generar reportes profesionales, facilitando la comunicación con el equipo defensivo (Scribd, 2025). Esta etapa es clave para fortalecer la seguridad organizacional.

En conclusión, el pentesting es un proceso metodológico que combina técnicas ofensivas con principios éticos y legales. Cada una de sus etapas permite simular ataques reales de forma controlada, aportando información valiosa para que los equipos Blue Team fortalezcan las defensas de la organización.

## Explicación de las herramientas y servicios utilizados en ciberseguridad

### *Herramientas*

En el campo de la ciberseguridad, las herramientas especializadas y los servicios en línea son fundamentales para identificar, analizar y mitigar vulnerabilidades en sistemas informáticos. Estas herramientas son utilizadas tanto por equipos Red Team, para simular ataques, como por equipos Blue Team, para fortalecer la defensa de los sistemas. A continuación, se describen algunas de las herramientas y servicios más relevantes.

**Metasploit.** Metasploit es un framework de código abierto ampliamente utilizado en pruebas de penetración que permite a los profesionales de ciberseguridad simular ataques reales de manera controlada. Su importancia radica en que no solo facilita la explotación de

vulnerabilidades, sino que también permite validar si estas representan un riesgo real para un sistema. Esto es clave, ya que muchas vulnerabilidades teóricas no siempre son explotables en la práctica.

Además, Metasploit cuenta con una arquitectura modular que incluye exploits, payloads y herramientas de post-explotación, lo que lo convierte en una plataforma integral para el análisis de seguridad. Desde la perspectiva de un Red Team, esta herramienta permite replicar el comportamiento de un atacante; mientras que, desde el enfoque Blue Team, ayuda a comprender cómo se materializan las amenazas y cómo pueden ser mitigadas. Su uso debe estar estrictamente autorizado, ya que su potencial puede ser mal utilizado fuera de entornos controlados (Rapid7, 2012).

**Nmap.** Nmap, conocido como Network Mapper, es una herramienta fundamental en la fase de reconocimiento y escaneo dentro de la ciberseguridad. Su principal función es identificar dispositivos en una red, detectar puertos abiertos, servicios activos y, en algunos casos, inferir el sistema operativo utilizado por los equipos analizados.

La relevancia de Nmap radica en que permite a los analistas comprender la superficie de ataque de una organización. Esto significa que ayuda a identificar posibles puntos de entrada que podrían ser aprovechados por un atacante. Además, su flexibilidad y capacidad de automatización lo convierten en una herramienta indispensable tanto para auditorías de seguridad como para monitoreo continuo.

Desde el punto de vista ético y legal, el uso de Nmap debe realizarse con autorización previa, ya que el escaneo de redes sin consentimiento puede considerarse una actividad intrusiva. Sin embargo, utilizado correctamente, es una herramienta clave para la prevención de incidentes de seguridad (Nmap Project, s.f.).

**OpenVas.** OpenVAS (Open Vulnerability Assessment System) es una herramienta diseñada específicamente para la gestión de vulnerabilidades. A diferencia de herramientas como Nmap, que se enfocan en el descubrimiento de servicios, OpenVAS realiza análisis más profundos orientados a identificar fallas de seguridad conocidas en sistemas, aplicaciones y dispositivos de red.

Esta herramienta se destaca por su capacidad de realizar escaneos automatizados y generar informes detallados que clasifican las vulnerabilidades según su nivel de riesgo. Esto permite a las organizaciones priorizar acciones correctivas, optimizando recursos y mejorando su postura de seguridad.

Desde una perspectiva organizacional, OpenVAS es fundamental para el trabajo del Blue Team, ya que permite una evaluación continua de los activos tecnológicos. Asimismo, su uso contribuye al cumplimiento de normativas de seguridad y protección de datos, al evidenciar una gestión activa de riesgos (Greenbone Networks, 2020).

### *Servicios en línea*

**ExploitDB.** ExploitDB es una base de datos pública que recopila exploits, vulnerabilidades y pruebas de concepto desarrolladas por investigadores en seguridad informática. Su principal valor radica en que proporciona ejemplos reales de cómo pueden ser explotadas ciertas vulnerabilidades, lo que facilita el aprendizaje y la investigación.

Para un profesional en ciberseguridad, ExploitDB es una herramienta clave para comprender la evolución de las amenazas y analizar técnicas utilizadas por atacantes. Desde el enfoque Red Team, permite identificar métodos de explotación; mientras que, para el Blue Team, ayuda a anticipar ataques y fortalecer mecanismos de defensa.

Sin embargo, su uso implica una gran responsabilidad ética, ya que el acceso a este tipo de información puede ser mal utilizado. Por ello, debe emplearse exclusivamente con fines académicos, de investigación o en entornos autorizados (Offensive Security, s.f.).

**CVE (Common Vulnerabilities and Exposures).** CVE es un sistema estandarizado de identificación de vulnerabilidades de seguridad reconocido a nivel mundial. Cada vulnerabilidad registrada recibe un identificador único (por ejemplo, CVE-2023-XXXX), lo que permite su clasificación, seguimiento y análisis en diferentes plataformas y herramientas de seguridad.

La importancia de CVE radica en que facilita la comunicación entre organizaciones, investigadores y fabricantes de software, al proporcionar un lenguaje común para referirse a vulnerabilidades específicas. Esto es fundamental para la gestión de riesgos, ya que permite correlacionar información de múltiples fuentes, como bases de datos de vulnerabilidades, herramientas de escaneo y reportes de seguridad.

Desde una perspectiva estratégica, el uso de CVE permite a las organizaciones mantenerse actualizadas frente a nuevas amenazas y tomar decisiones informadas sobre la aplicación de parches y controles de seguridad. Es una pieza clave dentro de cualquier programa de gestión de vulnerabilidades (MITRE, s.f.).

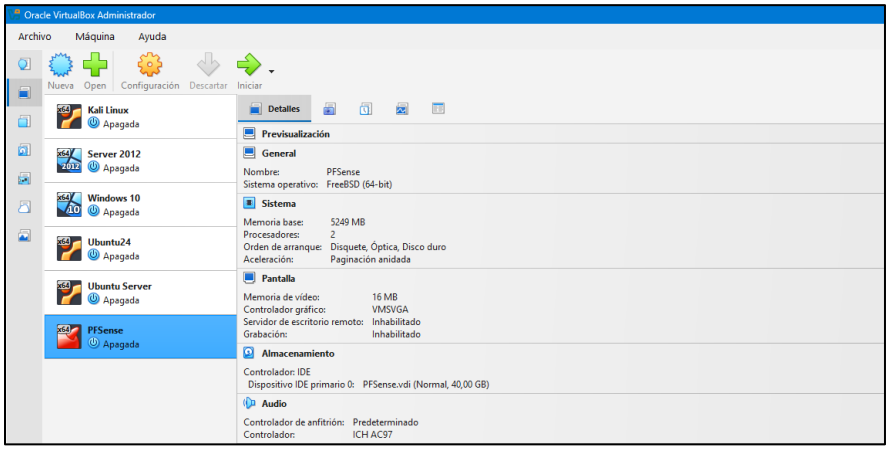
## Configuración y análisis del banco de trabajo

El montaje del banco de trabajo constituye una fase fundamental dentro del proceso de formación en ciberseguridad, ya que permite simular entornos reales donde se ejecutan pruebas controladas. En este caso, el escenario planteado por SecureNova Labs tiene como objetivo evaluar las capacidades técnicas iniciales del estudiante mediante la instalación, configuración y validación de un entorno virtual basado en software de código abierto.

En el Paso A, se realizó la instalación de la herramienta de virtualización VirtualBox en su última versión. Esta herramienta es ampliamente utilizada en entornos académicos y profesionales debido a su capacidad para crear máquinas virtuales que simulan sistemas operativos completos sin afectar el sistema principal (host). Su uso permite aislar entornos de prueba, lo cual es esencial en actividades de ciberseguridad para evitar riesgos.

**Figura 1**

*Apertura de la Maquina VirtualBox Instalada en el Equipo*

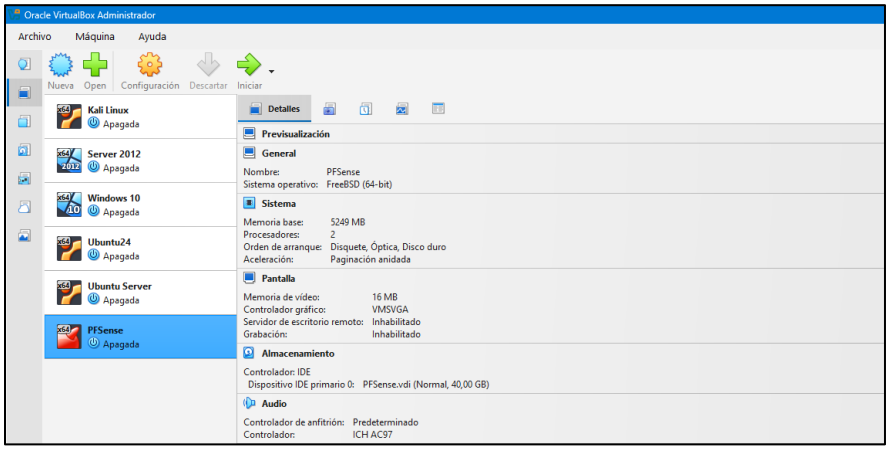



*Nota.* Se busca en el navegador de preferencia el instalador de la última versión de VirtualBox, posterior a la descarga se realiza la instalación en el equipo, con el fin de poder realizar el desarrollo de la actividad.

En el Paso B, se procede a la importación de las máquinas virtuales en formato .OVA proporcionadas en el repositorio del curso. Estas imágenes corresponden a un sistema operativo Windows (Win7-SE2020-X64) y una distribución orientada a seguridad (Parrot Security o Kali Linux). La utilización de este tipo de imágenes preconfiguradas permite ahorrar tiempo en la instalación y garantiza que el entorno esté listo para ejecutar pruebas técnicas. En este caso, se evidencia la disponibilidad de archivos como *Parrot-security-6.3.2_amd64.ova* y *Win7-SE2020-X64.ova*, los cuales serán utilizados para el laboratorio.

**Figura 2**

*Importación de máquinas virtuales*

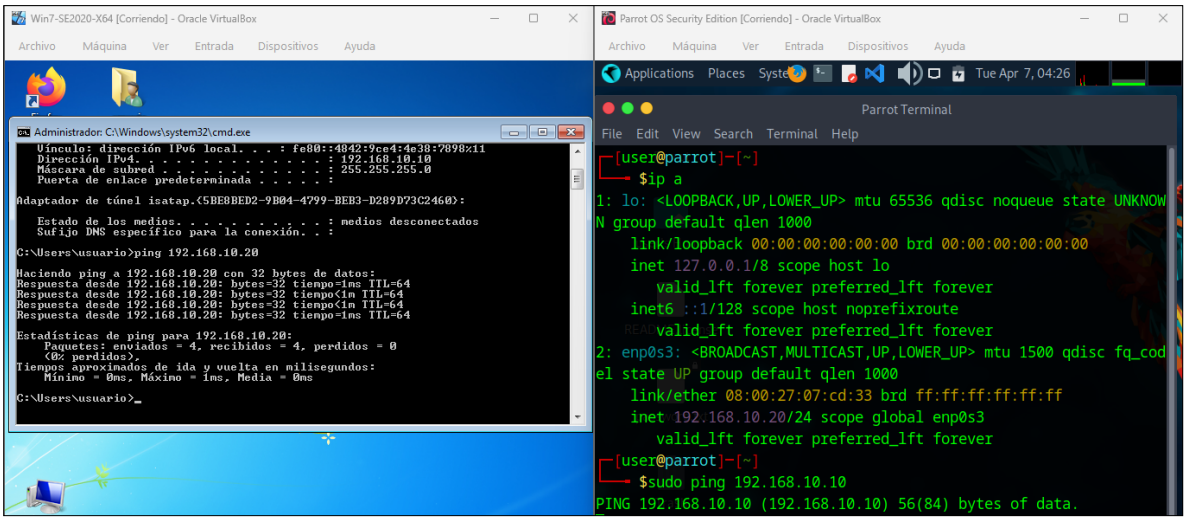



*Nota.* Después de descargar los archivos suministrados se importa la máquina virtual de Windows 7 y Kali Linux, igualmente se identifican las características de cada una de las máquinas.

En el Paso C, se realiza la verificación de conectividad entre las máquinas virtuales. Este paso es crítico, ya que garantiza la comunicación entre el sistema atacante (Kali/Parrot) y el sistema objetivo (Windows). Para lograr esto, se configura la red de las máquinas virtuales en modo "Adaptador Interno" o "Red NAT", dependiendo de los requerimientos del laboratorio. Posteriormente, se valida la conectividad mediante comandos como ping desde la máquina atacante hacia la víctima. Es importante seguir la recomendación de no encender todas las máquinas simultáneamente para evitar sobrecarga en los recursos del equipo host, gestionando adecuadamente la memoria RAM y el procesamiento.

**Figura 3**

*Configuración de red y conectividad*




*Nota.* Después de verificar cada una de las direcciones IP de las máquinas virtuales, se procede a verificar la conexión y comunicación entre las mismas.

En el Paso D se documentó la configuración del entorno de laboratorio mediante capturas de pantalla y la descripción de las características técnicas de las máquinas virtuales utilizadas, las cuales se resumen a continuación:

**Tabla 1**

*Características técnicas de las máquinas virtuales utilizadas en el entorno de laboratorio*

| Característica | Windows | Kali Linux / Parrot |
|---|---|---|
| Memoria RAM | 4 GB | 4 GB |
| Procesadores (CPU) | 1 núcleo | 2 núcleos |
| Disco duro virtual | Incluido en archivo .OVA | Incluido en archivo .OVA |
| Configuración de red | Red interna | Red interna |

*Nota*. La tabla presenta la configuración de hardware y red asignada a las máquinas virtuales Windows 7 y Kali Linux utilizadas durante el desarrollo del laboratorio. Estos recursos permitieron establecer un entorno controlado para la ejecución de pruebas de reconocimiento, análisis de vulnerabilidades y simulación de ataques de ciberseguridad.

Estas evidencias permiten demostrar que el entorno está correctamente configurado y listo para ejecutar pruebas de ciberseguridad.

El banco de trabajo fue desplegado mediante la virtualización de dos sistemas operativos: una máquina Windows como objetivo y una máquina Parrot Security (Kali Linux) como entorno de pruebas de seguridad. Ambas máquinas fueron configuradas en una red interna que permite la comunicación directa entre ellas. La verificación de conectividad se realizó exitosamente mediante pruebas de red, dejando el entorno listo para el desarrollo de actividades de ciberseguridad.

## Ética Profesional y Marco Normativo en Ciberseguridad

Durante el desarrollo del seminario se analizaron aspectos éticos y legales relacionados con el ejercicio profesional de la ciberseguridad. El caso de SecureNova Labs permitió identificar riesgos asociados al uso indebido de herramientas ofensivas y acceso no autorizado a información sensible.

Se evidenció que las actividades ofensivas dentro de un entorno organizacional deben ejecutarse bajo autorización expresa, políticas claras y límites establecidos previamente. De lo contrario, podrían vulnerarse principios éticos y normas legales relacionadas con delitos informáticos. La protección de datos y el manejo responsable de la información deben realizarse conforme a las políticas de privacidad y buenas prácticas establecidas por las entidades competentes (MinTIC, 2022)

En Colombia, la Ley 1273 de 2009 establece sanciones relacionadas con acceso abusivo a sistemas informáticos, interceptación de datos y uso malicioso de software. Asimismo, el código de ética del COPNIA resalta la responsabilidad profesional de actuar con integridad y respeto por la información y los sistemas tecnológicos.

**Identificación de procesos ilegales o no éticos.**

Tras el análisis del escenario planteado, es posible evidenciar la existencia de prácticas que pueden considerarse tanto ilegales como contrarias a la ética profesional en ciberseguridad. Estas irregularidades se relacionan principalmente con el uso indebido de herramientas de análisis, el acceso desproporcionado a información sensible y la falta de delimitación clara en el alcance de las actividades autorizadas.

En primer lugar, uno de los aspectos más críticos identificados es la posibilidad de que el acuerdo permita el acceso amplio e indiscriminado a sistemas de información de los clientes, sin establecer límites específicos sobre qué tipo de datos pueden ser consultados o manipulados. Este

tipo de cláusula, comúnmente expresada en términos como “acceso total a la infraestructura tecnológica” o “recolección de información sin restricción para fines de análisis”, constituye una práctica riesgosa, ya que puede derivar en un uso abusivo de privilegios. Desde el punto de vista legal, esto podría configurarse como una conducta sancionable si se excede el consentimiento otorgado, en concordancia con lo establecido en la Ley 1273 de 2009, particularmente en lo relacionado con el acceso abusivo a sistemas informáticos (Congreso de la República de Colombia, 2009).

Se evidencian posibles irregularidades en fragmentos del acuerdo que sugieren la recolección, almacenamiento o análisis de información sensible sin mecanismos claros de protección o anonimización. Si el acuerdo no especifica medidas de seguridad como cifrado, control de acceso o confidencialidad, se estaría vulnerando el derecho fundamental a la protección de datos personales. Esta situación puede encuadrarse dentro de conductas como la violación de datos personales, lo cual también está tipificado como delito en la legislación colombiana (Guarnizo Portela, 2024).

Otro aspecto crítico es la posible inclusión de actividades que pueden interpretarse como ciberespionaje, especialmente si el acuerdo permite el uso de herramientas ofensivas más allá de los objetivos de una auditoría de seguridad. Por ejemplo, fragmentos que autoricen “monitoreo continuo de comunicaciones”, “extracción de información estratégica” o “evaluación encubierta de sistemas sin notificación explícita” representan una clara desviación de las buenas prácticas del hacking ético. Estas acciones no solo vulneran la legalidad, sino que contradicen los principios fundamentales de metodologías reconocidas como OSSTMM, las cuales establecen que toda prueba de seguridad debe realizarse con consentimiento informado, alcance definido y trazabilidad (Zuluaga Mateus, 2017).

Teniendo en cuenta un enfoque ético, estas prácticas también entran en conflicto con los lineamientos establecidos por el COPNIA, que exigen que los profesionales actúen con integridad, responsabilidad y respeto por la ley. En este sentido, aceptar o ejecutar actividades que impliquen acceso indebido a información o uso desproporcionado de herramientas tecnológicas constituye una falta grave al ejercicio profesional, ya que se priorizan intereses particulares sobre el bienestar general y la legalidad (COPNIA, 2015).

Adicionalmente, la ausencia de cláusulas claras relacionadas con la responsabilidad del manejo de la información, la trazabilidad de las acciones y los límites operativos del equipo de ciberseguridad evidencia una debilidad estructural en el acuerdo. Esto no solo abre la puerta a posibles abusos, sino que también dificulta la auditoría y el control de las actividades realizadas, lo cual es fundamental en entornos donde se manejan datos críticos.

**Vulneración de la Ley 1273 de 2009.**

A partir del análisis anterior, es posible afirmar que las condiciones allí establecidas no solo presentan vacíos éticos, sino que además podrían configurar conductas tipificadas como delitos informáticos en la Ley 1273 de 2009. Esta ley tiene como finalidad proteger la información y los sistemas informáticos frente a accesos indebidos, manipulación no autorizada y uso malicioso de herramientas tecnológicas. En este contexto, las cláusulas identificadas no solo son ambiguas, sino que abren la posibilidad de incurrir en vulneraciones concretas de varios artículos.

En primer lugar, el Artículo 269A Acceso abusivo a un sistema informático resulta directamente comprometido. Aunque el acuerdo establece una autorización general para acceder a los sistemas del cliente, dicha autorización carece de delimitación específica en términos de alcance, profundidad y finalidad. Esto es problemático, ya que en el ámbito jurídico no basta con un consentimiento amplio; este debe ser expreso, informado y limitado. En consecuencia, cuando

el acuerdo permite “acceso total sin restricción”, se habilita la posibilidad de que el profesional exceda los límites razonables de una auditoría, lo cual puede ser interpretado como acceso abusivo. En otras palabras, el problema no es únicamente el acceso en sí, sino la falta de control sobre ese acceso, lo que lo convierte en potencialmente ilegal (Congreso de la República de Colombia, 2009).

En segundo lugar, el Artículo 269F Violación de datos personales también podría verse vulnerado de manera significativa. El acuerdo permite la recopilación y análisis de “toda la información encontrada” sin establecer criterios de clasificación, protección o tratamiento de los datos. Desde una perspectiva jurídica y ética, esto representa una falla grave, ya que no diferencia entre información técnica y datos personales sensibles. La ausencia de medidas como anonimización, cifrado o control de acceso implica que los datos podrían ser utilizados de manera indebida o incluso filtrados. Así, el acuerdo no solo facilita el acceso a la información, sino que desprotege activamente los datos, lo cual encaja dentro de las conductas sancionadas por este artículo (Guarnizo Portela, 2024).

En tercer lugar, el Artículo 269C Interceptación de datos informáticos se relaciona con las cláusulas que permiten el monitoreo de comunicaciones sin notificación al cliente. Este tipo de prácticas trasciende el ámbito del pentesting legítimo y se acerca peligrosamente al ciberespionaje. En una auditoría ética, el monitoreo debe ser transparente, justificado y previamente autorizado de forma específica. Sin embargo, el acuerdo sugiere la posibilidad de realizar vigilancia encubierta, lo cual vulnera el derecho a la privacidad y puede constituir una interceptación ilegal de datos. Aquí se evidencia un problema estructural: el acuerdo no solo permite acciones intrusivas, sino que además normaliza la falta de transparencia, lo cual agrava su ilegalidad.

El Artículo 269G Uso de software malicioso también podría ser vulnerado debido a la autorización abierta para utilizar “cualquier herramienta de explotación”. Si bien es cierto que en el contexto del hacking ético se emplean herramientas ofensivas, estas deben utilizarse bajo un marco estricto de control, con objetivos definidos y sin generar afectaciones reales a los sistemas. La falta de restricciones en el acuerdo implica que se podrían emplear herramientas que alteren el funcionamiento de los sistemas o comprometan su integridad, lo que podría ser interpretado como uso indebido de software malicioso. En este sentido, el problema no es la herramienta en sí, sino el uso desproporcionado y sin control, lo cual desborda el ámbito legal del pentesting (Zuluaga Mateus, 2017).

Finalmente, el Artículo 269D Daño informático puede verse comprometido como consecuencia de las prácticas anteriormente descritas. El uso no controlado de herramientas de explotación, sumado al acceso irrestricto a los sistemas, incrementa significativamente el riesgo de generar daños, ya sea de forma intencional o accidental. En este escenario, el acuerdo no contempla mecanismos de prevención ni responsabilidades claras frente a posibles afectaciones, lo que agrava la situación. Esto evidencia una falta de diligencia que puede derivar en consecuencias legales, ya que cualquier alteración, pérdida o deterioro de la información podría ser sancionada bajo este artículo.

**Oferta laboral en SecureNova Labs.**

Considerando que la oferta económica y un contrato vitalicio, la cual resulta muy atractiva y teniendo en cuenta la situación económica actual del país, no aplicaría al trabajo en SecureNova Labs, debido a las implicaciones éticas y legales evidenciadas, teniendo en cuenta lo anterior:

Aceptar una vinculación laboral bajo condiciones que habilitan prácticas ambiguas o potencialmente ilegales implica asumir riesgos jurídicos personales. En ciberseguridad, la responsabilidad no recae únicamente en la organización, sino también en el profesional que ejecuta

las acciones técnicas. Si el acuerdo permite accesos sin delimitación, recolección indiscriminada de datos o monitoreo encubierto, el profesional podría incurrir en conductas sancionables por la Ley 1273 de 2009, incluso si dichas acciones fueron “autorizadas” contractualmente. Es decir, un contrato no legitima prácticas que vulneren la ley; por el contrario, puede convertirse en un factor de riesgo al intentar normalizar conductas ilícitas (Congreso de la República de Colombia, 2009).

Igualmente teniendo en cuenta la perspectiva ética, aceptar este tipo de condiciones contraviene los principios fundamentales del ejercicio profesional. El COPNIA establece que los ingenieros deben actuar con integridad, responsabilidad social y respeto por la normatividad vigente. Esto implica que el profesional no solo debe abstenerse de realizar actos ilegales, sino también evitar participar en organizaciones que promuevan prácticas cuestionables. En este sentido, aceptar el cargo implicaría priorizar el beneficio económico sobre la ética profesional, lo cual deteriora la confianza en el ejercicio de la ciberseguridad (COPNIA, 2015).

Adicionalmente, desde el punto de vista reputacional, trabajar en una organización asociada a prácticas como el acceso indebido a información o el posible ciberespionaje puede tener consecuencias negativas a largo plazo. La carrera en ciberseguridad se construye sobre la confianza, la transparencia y el cumplimiento normativo, por lo que vincularse a una empresa con antecedentes o políticas dudosas puede afectar la credibilidad profesional y limitar oportunidades futuras.

Es importante considerar que el ejercicio del hacking ético se basa en metodologías que exigen consentimiento informado, alcance definido y trazabilidad de las acciones. Cuando un acuerdo carece de estos elementos, se desdibuja la línea entre una auditoría legítima y una actividad intrusiva no autorizada. En consecuencia, el profesional no tendría garantías de que su trabajo se mantenga dentro de los límites legales y éticos, lo que incrementa la exposición a sanciones disciplinarias y penales (Zuluaga Mateus, 2017).

De acuerdo con lo anteriormente expresado y aunque la estabilidad laboral y la remuneración son factores relevantes, no pueden prevalecer sobre la legalidad y la ética.

**Argumentación con base en el código de ética del COPNIA.**

La decisión de no aplicar al trabajo en SecureNova Labs se fundamenta de manera directa en los principios establecidos por el COPNIA en su Código de Ética para el ejercicio de la ingeniería. Dicho código no solo orienta el comportamiento profesional, sino que establece límites claros frente a situaciones donde puedan existir conflictos entre beneficios personales y el cumplimiento de la ley y la ética.

El COPNIA establece que el ingeniero debe actuar con integridad, honestidad y responsabilidad social, priorizando el bienestar general sobre intereses particulares. En este caso, aunque la oferta laboral presenta beneficios económicos significativos, aceptar un cargo dentro de una organización que promueve prácticas ambiguas o potencialmente ilegales implicaría actuar en contravía de estos principios. La ética profesional exige que el ingeniero no participe en actividades que puedan afectar la privacidad, la seguridad de la información o los derechos de terceros.

Es importante tener en cuenta que el código enfatiza el deber de cumplir y hacer cumplir la normativa vigente. Esto implica que el profesional no puede justificar acciones ilegales bajo el argumento de obedecer órdenes o cumplir con un contrato laboral. En el contexto del acuerdo analizado, donde se evidencian posibles vulneraciones a la Ley 1273 de 2009, aceptar el empleo significaría exponerse a responsabilidades legales directas. Por tanto, el ingeniero tiene la obligación ética de abstenerse de participar en entornos donde se puedan cometer delitos informáticos, incluso si estos están implícitamente permitidos por la organización.

Otro aspecto relevante es el principio de competencia profesional y diligencia, el cual implica que el ingeniero debe desempeñar sus funciones dentro de estándares técnicos y éticos

reconocidos. En ciberseguridad, esto se traduce en aplicar metodologías que garanticen consentimiento informado, delimitación del alcance y protección de la información. Sin embargo, el acuerdo de SecureNova Labs presenta vacíos en estos aspectos, lo que impide al profesional ejercer su labor bajo condiciones adecuadas. En consecuencia, aceptar el cargo implicaría trabajar en un entorno que no respeta las buenas prácticas del sector.

Asimismo, el COPNIA resalta la importancia de la transparencia y la confianza en el ejercicio profesional. Participar en actividades que puedan interpretarse como ciberespionaje o acceso indebido a información compromete no solo la reputación del ingeniero, sino también la credibilidad de la profesión en general. La confianza es un activo fundamental en ciberseguridad, y su pérdida puede tener consecuencias irreparables tanto a nivel individual como organizacional

**Acceso a información sensible en auditorías.**

El acceso a información sensible por parte de empresas de ciberseguridad debe estar estrictamente limitado al principio de necesidad y proporcionalidad. Es decir, solo se debe acceder a la información estrictamente necesaria para cumplir con los objetivos definidos en la auditoría. Cualquier acceso adicional, aunque técnicamente posible, resulta injustificado y potencialmente ilegal, es importante tener en cuenta que la gestión responsable de la información debe estar alineada con políticas de privacidad que garanticen la protección de los datos personales y la transparencia en su tratamiento (MinTIC, 2022).

En este sentido, el límite no lo define la capacidad técnica del equipo, sino el alcance contractual y ético previamente establecido. Una auditoría de seguridad no otorga un permiso general sobre la información del usuario, sino una autorización controlada, delimitada y supervisada. Superar ese límite implica pasar de una práctica legítima a una conducta cuestionable o incluso ilícita.

Para garantizar que este nivel de acceso no sea utilizado de forma indebida y que las actividades de auditoría se desarrollen dentro de parámetros éticos y legales, es indispensable establecer mecanismos de control y supervisión adecuados. En primer lugar, se debe definir claramente el alcance de la auditoría, especificando los sistemas, datos y técnicas autorizadas para la evaluación. Asimismo, resulta fundamental suscribir acuerdos de confidencialidad que regulen el tratamiento y la protección de la información a la que se tenga acceso durante el proceso. De igual manera, debe aplicarse el principio de mínimo privilegio, otorgando únicamente los permisos estrictamente necesarios para el cumplimiento de las funciones asignadas. Complementariamente, todas las actividades realizadas deben quedar registradas mediante mecanismos de trazabilidad y generación de logs, con el fin de facilitar su seguimiento y verificación. Finalmente, es recomendable implementar procesos de supervisión y auditoría interna, así como mecanismos de segmentación y anonimización de datos que permitan reducir el riesgo de exposición de información sensible y fortalecer la seguridad de los activos de la organización.

Estas medidas no solo reducen el riesgo de abuso, sino que también garantizan la transparencia y la rendición de cuentas, elementos fundamentales en el ejercicio ético de la ciberseguridad. Tal como lo plantea la metodología OSSTMM, las pruebas de seguridad deben ejecutarse bajo condiciones controladas, con consentimiento informado y con plena trazabilidad de las acciones realizadas (Zuluaga Mateus, 2017).

**Mecanismos de supervisión y control.**

El uso de herramientas avanzadas de análisis forense en ciberseguridad implica un alto nivel de poder técnico, ya que permiten acceder, reconstruir y analizar información sensible de sistemas y usuarios. Por esta razón, su utilización debe estar sujeta a controles estrictos, dado que, en ausencia de supervisión, pueden convertirse en instrumentos para prácticas indebidas, incluyendo accesos no autorizados o incluso conductas cercanas al ciberespionaje.

Desde la parte legal, el uso no autorizado de estas herramientas podría derivar en la vulneración de la Ley 1273 de 2009, especialmente en lo relacionado con el acceso abusivo a sistemas informáticos, la interceptación de datos y la violación de datos personales. Por tanto, las organizaciones deben implementar mecanismos que no solo prevengan abusos, sino que también garanticen la trazabilidad, responsabilidad y control de todas las acciones realizadas por sus analistas (Congreso de la República de Colombia, 2009).

Uno de los mecanismos fundamentales es la definición clara de políticas internas de seguridad y uso aceptable, donde se establezcan de manera clara los límites en la utilización de herramientas forenses. Estas políticas deben incluir lineamientos sobre el alcance de las actividades, el tratamiento de la información y las sanciones en caso de incumplimiento. Sin una normativa interna sólida, el ejercicio técnico queda sujeto a interpretaciones individuales, aumentando el riesgo de comportamientos no éticos.

Otro mecanismo clave es la implementación del principio de mínimo privilegio y control de accesos. Esto implica que cada analista solo debe tener acceso a las herramientas, sistemas y datos estrictamente necesarios para el desarrollo de sus funciones. La asignación de privilegios elevados debe ser temporal, justificada y monitoreada, evitando así el uso no adecuado de capacidades técnicas avanzadas.

Asimismo, es indispensable contar con sistemas de registro y monitoreo continuo (logs). Todas las acciones realizadas por los analistas deben quedar registradas, incluyendo accesos, consultas, modificaciones y uso de herramientas. Esta trazabilidad permite auditar posteriormente las actividades y detectar comportamientos anómalos o no autorizados. La existencia de registros no solo facilita la supervisión, sino que también actúa como un mecanismo disuasivo frente a posibles abusos.

Se deben realizar auditorías internas y externas periódicas, orientadas a evaluar el cumplimiento de las políticas de seguridad y la correcta utilización de herramientas forenses. Estas auditorías permiten identificar debilidades en los controles y corregirlas oportunamente, fortaleciendo la gobernanza de la seguridad dentro de la organización.

Otro aspecto relevante es la segregación de funciones, la cual busca evitar que una sola persona tenga control total sobre un proceso crítico. Por ejemplo, quien ejecuta un análisis forense no debería ser la misma persona que aprueba el alcance o valida los resultados. Esta separación reduce el riesgo de manipulación indebida de la información y promueve la transparencia en los procesos.

Es fundamental promover una cultura organizacional basada en la integridad y la responsabilidad profesional, alineada con los principios del COPNIA. Esto implica capacitar constantemente a los empleados en temas de ética, normativa legal y buenas prácticas en ciberseguridad, de manera que comprendan no solo el "cómo" utilizar las herramientas, sino también el "hasta dónde" y el "por qué" de su uso responsable (COPNIA, 2015).

**Respuesta ante ciberespionaje.**

Cuando un gobierno u organización descubre que una empresa de ciberseguridad contratada ha incurrido en actos de ciberespionaje, no se trata únicamente de un incidente técnico, sino de una ruptura estructural de la confianza, la legalidad y la ética profesional. Por ello, la respuesta no puede limitarse a acciones correctivas aisladas; debe concebirse como un proceso integral orientado a restablecer el orden jurídico, proteger a los afectados y reconstruir la legitimidad institucional.

Las medidas adecuadas para restaurar la confianza serian:

Primero, desde la parte jurídica, la reacción debe ser inmediata y contundente. El ciberespionaje implica conductas que pueden encuadrarse en delitos como acceso abusivo a

sistemas informáticos, interceptación de datos o violación de información personal, todos contemplados en la Ley 1273 de 2009. En este sentido, la organización afectada tiene no solo el derecho, sino la obligación de denunciar los hechos ante las autoridades competentes, activar los mecanismos contractuales de incumplimiento y exigir responsabilidades civiles y penales. Este paso es fundamental, ya que tolerar o minimizar este tipo de conductas enviaría un mensaje de impunidad que debilita el marco normativo y favorece la repetición de prácticas indebidas (Congreso de la República de Colombia, 2009).

Sin embargo, limitar la respuesta al ámbito legal sería insuficiente. Es necesario comprender que el daño generado por el ciberespionaje trasciende lo jurídico y afecta directamente la confianza organizacional y social. Por esta razón, la organización debe adoptar una postura de transparencia activa, informando a las partes interesadas sobre lo ocurrido, el alcance del incidente y las medidas adoptadas. Aunque esta exposición puede implicar costos reputacionales a corto plazo, en el mediano y largo plazo constituye un elemento clave para la reconstrucción de la credibilidad. Ocultar o minimizar la situación, por el contrario, profundiza la crisis y deteriora aún más la confianza.

Desde la parte técnica, la respuesta debe incluir una investigación forense rigurosa e independiente. Este análisis permite identificar fallas en los controles, debilidades en la supervisión y posibles responsabilidades individuales o estructurales. Además, proporciona evidencia clave para procesos legales y para la toma de decisiones correctivas. En este contexto, la trazabilidad de las acciones (logs) y la adecuada preservación de la evidencia resultan fundamentales para garantizar la validez del proceso.

No obstante, el elemento más crítico radica en la prevención de recurrencias. Un incidente de ciberespionaje revela, en esencia, una falla en los mecanismos de gobernanza de la seguridad. Por ello, la organización debe replantear su modelo de relación con proveedores de ciberseguridad,

transitando de un esquema basado en la confianza implícita a uno sustentado en el control verificable y la rendición de cuentas. Esto implica redefinir los contratos con alcances estrictamente delimitados, implementar el principio de mínimo privilegio, establecer controles de acceso temporales y asegurar la supervisión continua de las actividades realizadas por terceros.

Adicionalmente, resulta imprescindible fortalecer los mecanismos de auditoría y control interno, incluyendo revisiones periódicas, segregación de funciones y sistemas de monitoreo que permitan detectar comportamientos anómalos en tiempo real. Estas medidas no solo reducen el riesgo de abuso, sino que también generan un entorno donde las acciones indebidas son más difíciles de ejecutar y más fáciles de identificar.

Ya teniendo en cuenta la ética, se debe analizar los principios establecidos por el COPNIA, los cuales exigen que el ejercicio profesional se base en la integridad, la responsabilidad y el respeto por la ley. En este sentido, las organizaciones no solo deben sancionar a los responsables, sino también promover una cultura ética sólida, donde el uso del conocimiento técnico esté orientado al bienestar y no a la explotación de vulnerabilidades. Esto implica invertir en formación ética, establecer códigos de conducta exigibles y fomentar mecanismos de denuncia que permitan identificar irregularidades antes de que se conviertan en incidentes mayores (COPNIA, 2015).

De acuerdo con lo anterior, restaurar la confianza no es un proceso inmediato, sino progresivo. Requiere demostrar, mediante acciones concretas, que se han aprendido las lecciones del incidente y que se han implementado cambios estructurales para evitar su repetición. En este sentido, la confianza no se recupera con declaraciones, sino con evidencia de control, transparencia y compromiso ético sostenido en el tiempo.

## Estrategia de Red Team

### Herramientas y procedimientos utilizados.

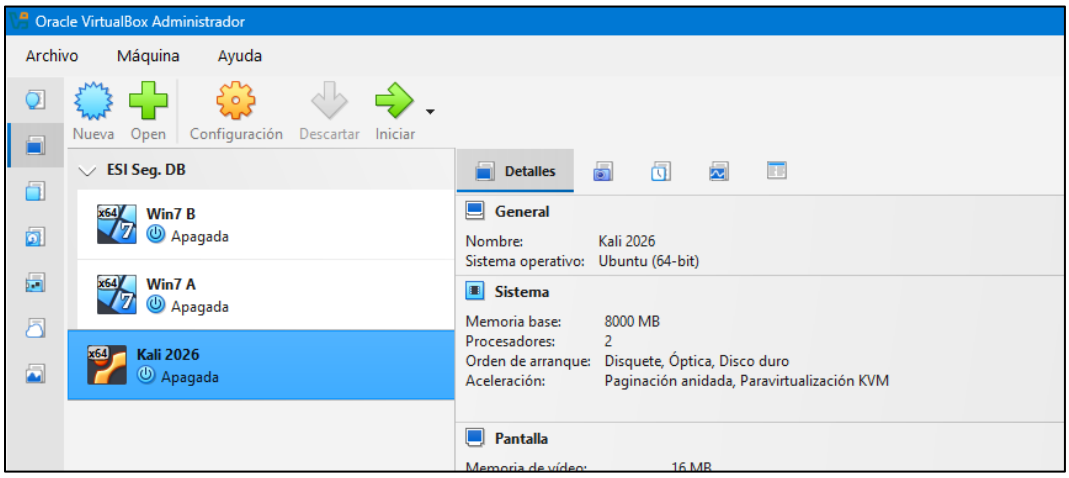
El desarrollo del escenario propuesta para la práctica de Red Team se realizó siguiendo una metodología estructurada de pentesting, aplicada sobre un entorno controlado con las siguientes máquinas virtuales instaladas en VirtualBox:

- Host A: Windows 7 (máquina vulnerable)
- Host B: Windows 7 (objetivo de pivoting)
- Atacante: Kali Linux

Se continua con el paso a paso de acuerdo con las fases de pentesting.

**Figura 4**

*Instalación de las máquinas virtuales en VirtualBox*




*Nota.* Se descarga las imágenes ISO de Window 7 y Kali Linux en su última versión, con el fin de importarlas en VirtualBox, para el desarrollo de la actividad, igualmente de acuerdo al Escenario se define quien actúa como el Host A, Host B y el atacante.

### *Fase 1. Reconocimiento*

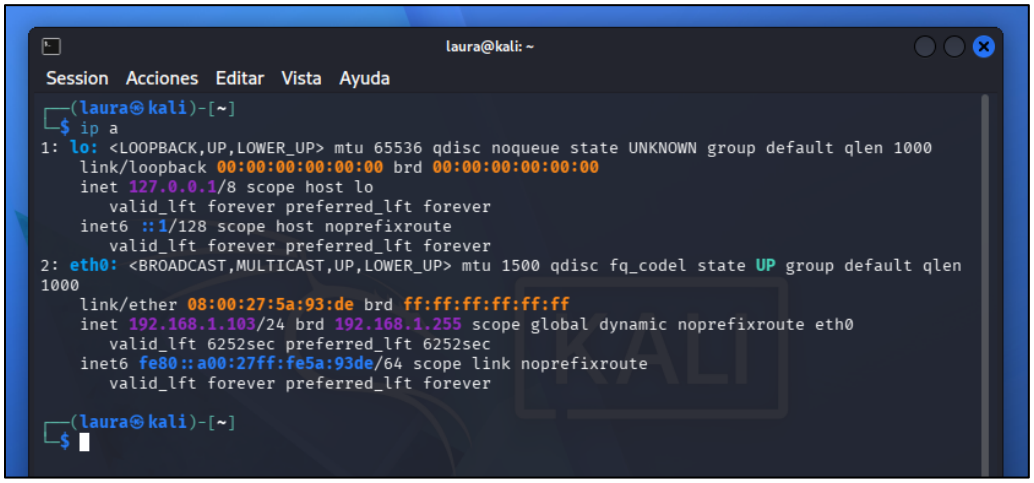
La fase de reconocimiento constituye el punto de partida del pentesting y tiene como finalidad recolectar información sobre la red y los sistemas. En el desarrollo de la actividad, esta

etapa se ejecutó desde Kali Linux instalada en VirtualBox mediante el uso de herramientas como Nmap, permitiendo identificar los hosts activos dentro del rango de red.

Esta fase permite al atacante construir un mapa inicial del entorno, identificando direcciones IP, disponibilidad de equipos y posibles objetivos. El escaneo permitió detectar la presencia de Host A y Host B, lo cual es coherente con lo planteado en el Anexo 4 – Escenario 3.

**Figura 5**

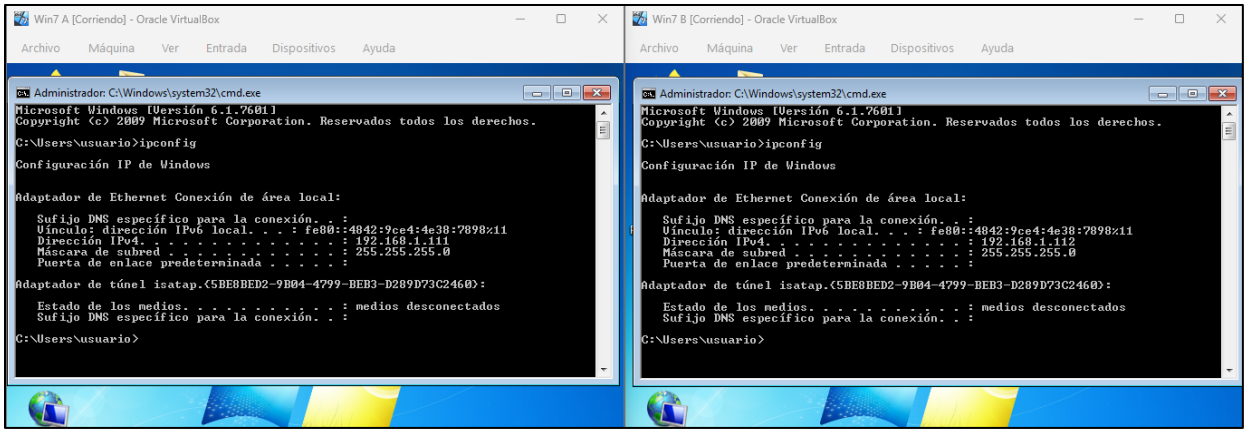
*Identificación de la Dirección IP en Kali Linux*




*Nota.* Se inicia la máquina virtual de Kali Linux en el cual lo primero que se hace es la identificación y reconocimiento de la dirección IP, la cual corresponde 192.168.1.103, es importante tener en cuenta esta máquina es la atacante y antes de realizar reconocimiento de la IP se realizó la actualización del sistema.

**Figura 6**

*Identificación de la Dirección IP en Windows (Host A y Host B)*

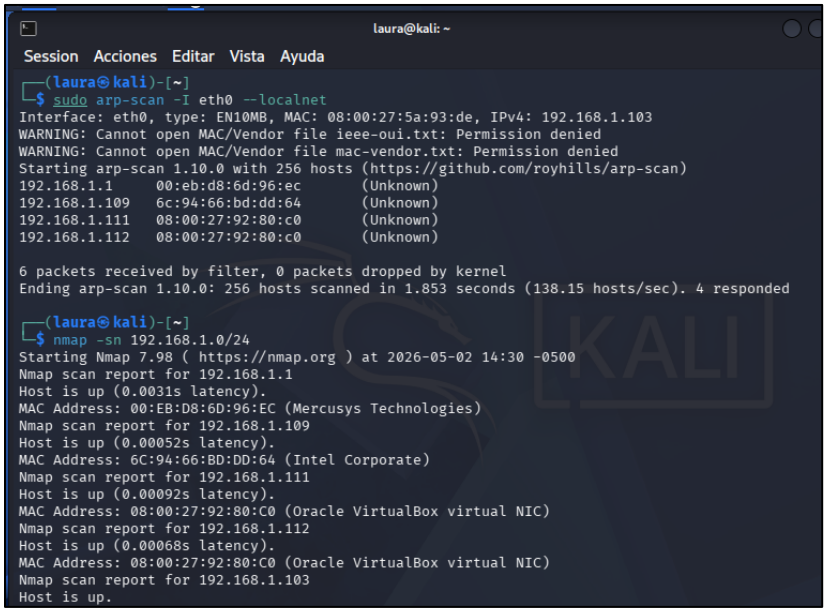



*Nota.* Igualmente se realiza el reconocimiento de las direcciones IP de las dos máquinas virtuales identificadas como Win7 A (Host A) el cual corresponde a 192.168.1.111 y Win7 B (Host B) el cual corresponde a 192.168.1.112

Posteriormente se realiza el proceso de escaneo de las redes encontradas desde la máquina de Kali Linux, con este escaneo se termina la fase de reconocimiento de pentesting.

**Figura 7**

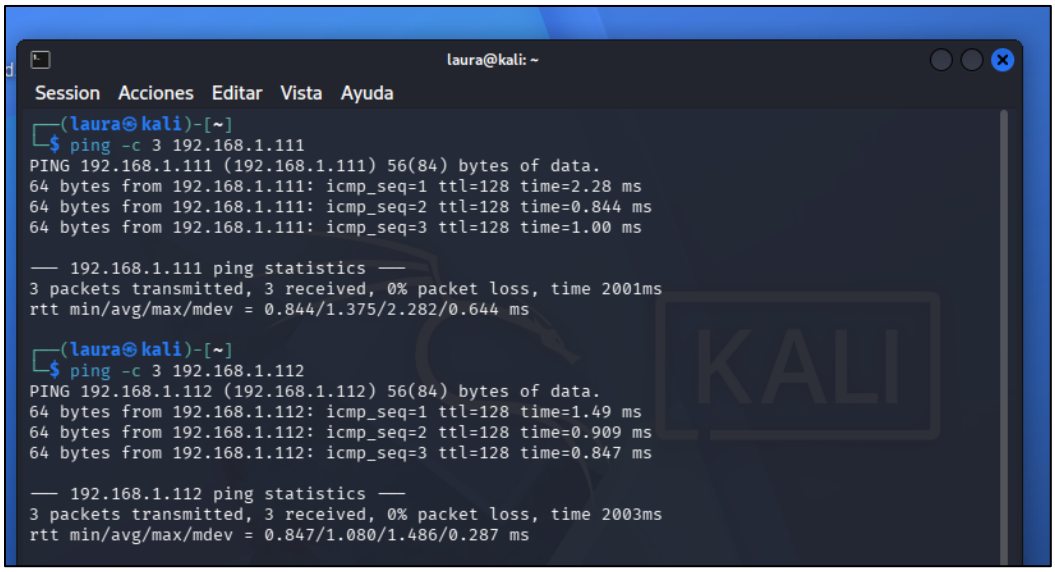
*Escaneo de redes*



*Nota.* Se hace el escaneo de las direcciones IP que están dentro de la misma red de la máquina de Kali Linux, dentro de esta identificación se reconocen las dos direcciones del Host A y B, con las cuales se van a trabajar en el desarrollo de la actividad.

**Figura 8**

*Verificación de conexión entre las redes*




*Nota.* Desde la máquina de Kali Linux se realiza la verificación de conexión entre las redes utilizando ping, en este caso se verifico que se tiene conexión con el Host a y Host B.

***Fase 2. Enumeración***

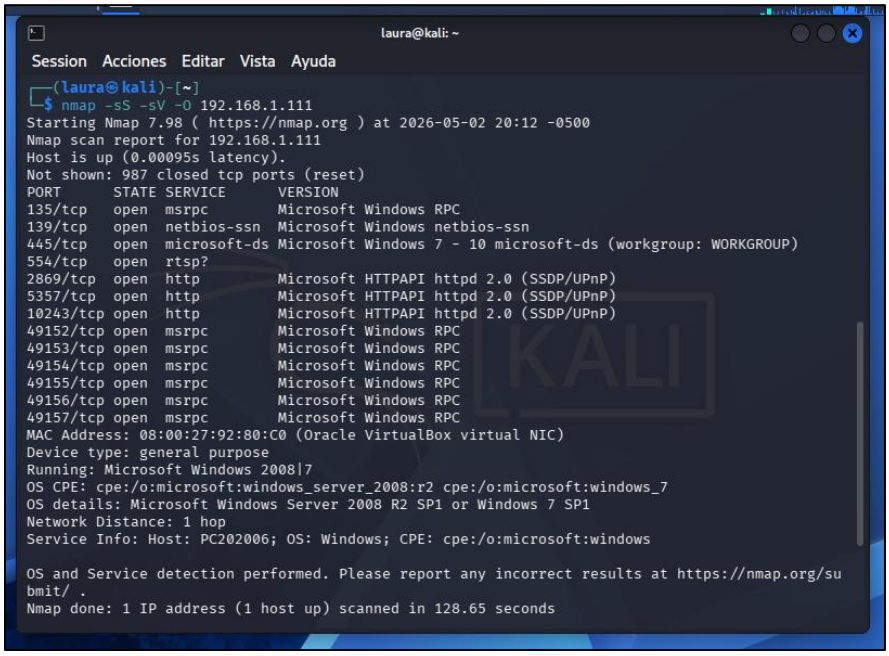
La fase de enumeración profundiza en el análisis de los sistemas detectados, identificando servicios, versiones y configuraciones específicas. En este caso, se utilizó nuevamente Nmap con parámetros avanzados para determinar puertos abiertos.

Esta fase permite identificar posibles vectores de ataque. Según Zuluaga Mateus (2017), la enumeración transforma datos generales en información específica que puede ser utilizada para identificar vulnerabilidades concretas.

En el escenario desarrollado, la detección de servicios en el Host-A permite inferir la posible existencia de vulnerabilidades asociadas al protocolo.

**Figura 9**

*Escaneo de puertos – Host A*




*Nota.* Dentro del escaneo del estado del Host A, se verifican los puertos abiertos, servicios activos, versiones del software y sistema operativo.

El escaneo realizado con Nmap sobre la dirección IP 192.168.1.111 permitió identificar que el equipo se encuentra activo dentro de la red y accesible desde la máquina atacante. Igualmente se evidencia la baja latencia observada indica que se trata de un entorno local, lo cual facilita la ejecución de pruebas de seguridad sin mayores restricciones.

Uno de los hallazgos que más se evidencia es la presencia de varios puertos abiertos asociados a servicios propios de sistemas Windows, especialmente los puertos 135 (RPC), 139 (NetBIOS) y 445 (SMB). Estos servicios son fundamentales para la comunicación interna y el intercambio de recursos en red; sin embargo, también representan un riesgo significativo cuando están expuestos, ya que pueden ser utilizados por posibles atacantes para obtener información del sistema o ejecutar accesos no autorizados.

El puerto 445 (SMB) se destaca como un punto crítico, ya que es un vector de ataque ampliamente conocido en sistemas Windows desactualizados. Esto se refuerza con la identificación del sistema operativo como Windows 7, una versión que actualmente no cuenta con soporte de seguridad, lo que incrementa considerablemente la probabilidad de explotación.

Tambien, se evidencian otros servicios activos como HTTP internos y puertos dinámicos de RPC, lo que indica que el sistema tiene múltiples procesos expuestos en red, ampliando la superficie de ataque.

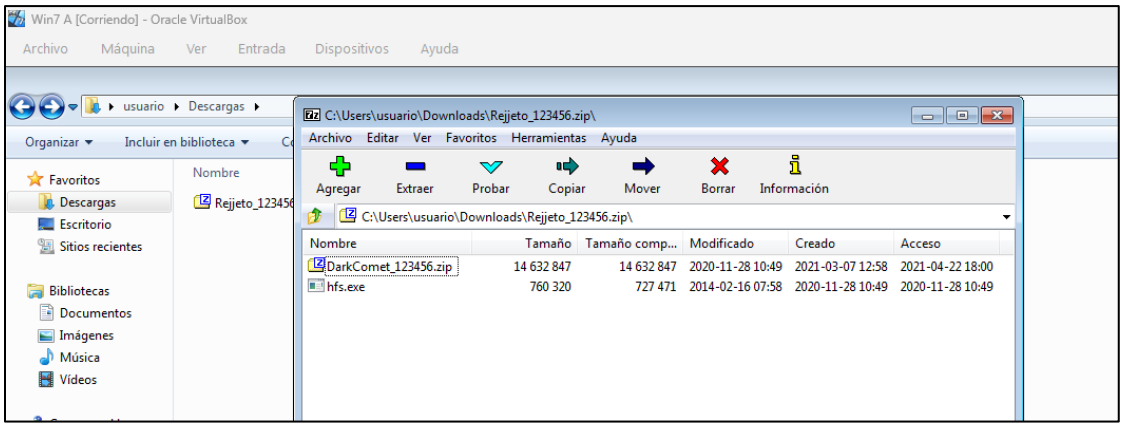
***Fase 3. Identificación de Vulnerabilidad***

En esta etapa se van a analizar los servicios identificados para determinar debilidades explotables. En esta fase se relaciona directamente con la presencia del archivo Rejjeto suministrado en la actividad, el cual actúa como un vector de ataque que simula una aplicación vulnerable.

De acuerdo con la fase anterior, la ejecución del archivo en Host A permitió validar la existencia de una vulnerabilidad que habilita acceso remoto, lo que se alinea con la descripción del anexo donde se menciona la obtención de una shell.

**Figura 10**

*Identificación de vulnerabilidad – Rejjeto*




*Nota.* Se descarga el archivo denominado Rejjeto para continuar con el desarrollo de la actividad.

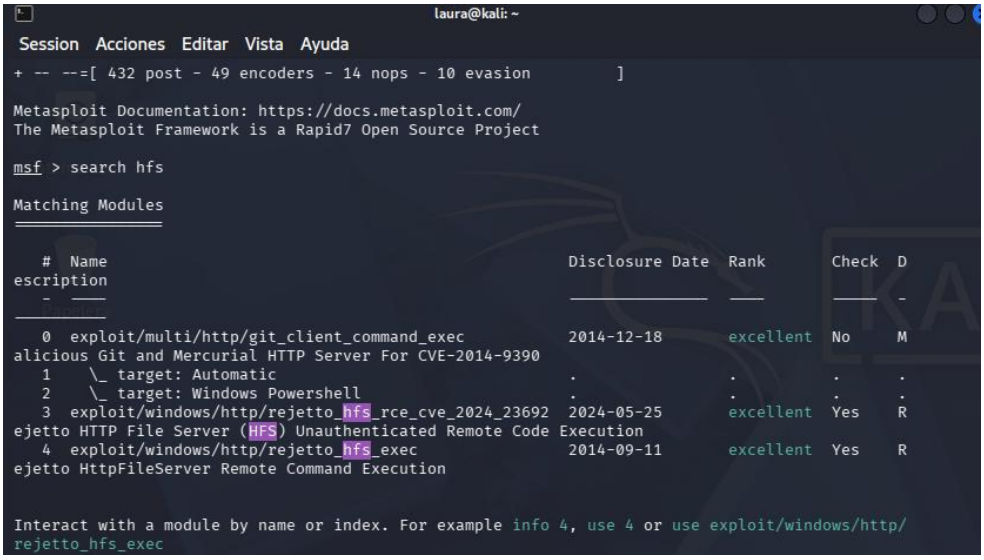
En esta fase se identificó que la máquina Host-A contenía un archivo comprimido denominado *Rejjeto_123456.zip*, el cual incluye herramientas asociadas a un troyano de acceso remoto conocido como DarkComet RAT. Este tipo de software es comúnmente utilizado para establecer conexiones remotas no autorizadas hacia un sistema comprometido.

El análisis del contenido del archivo permitió evidenciar la presencia de ejecutables como *DarkComet.exe*, así como archivos de configuración y librerías que permiten la ejecución del malware. Este tipo de herramienta funciona bajo un modelo cliente-servidor, donde la víctima ejecuta el archivo malicioso y establece una conexión hacia el atacante, permitiendo el control total del sistema.

La vulnerabilidad no corresponde únicamente a un fallo del sistema operativo, sino a una debilidad en la seguridad del usuario, quien ejecuta un archivo potencialmente malicioso sin validación previa. Esto facilita la obtención de acceso remoto (shell), escalamiento de privilegios y persistencia, tal como se describe en el escenario planteado.

**Figura 11**

*Buscar el exploit para Rejjeto / HFS*



*Nota.* Una vez identificado el servicio HFS (Rejjeto), procedemos a buscar un exploit compatible en la base de datos de Metasploit.

***Fase 4. Explotación***

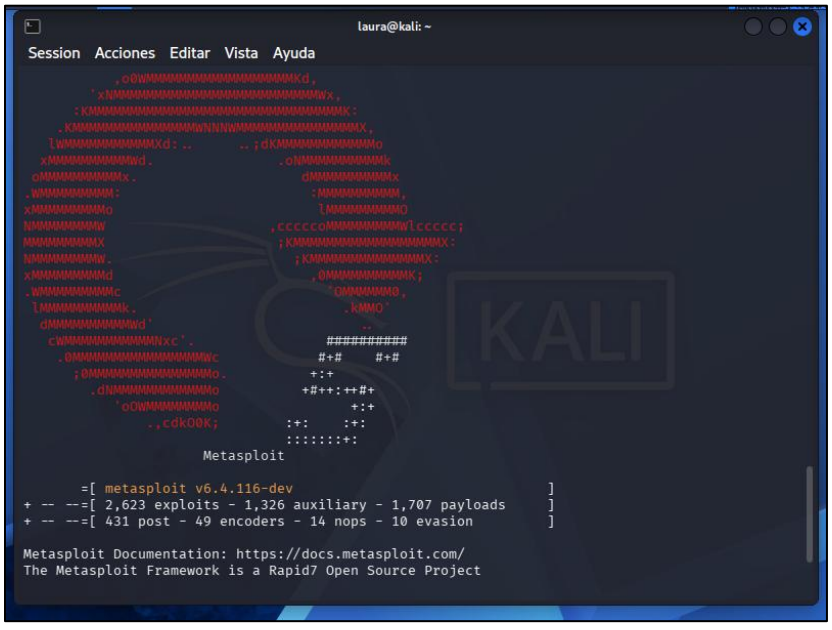
La explotación consiste en aprovechar la vulnerabilidad identificada para obtener acceso al sistema. En este caso, se utilizó Metasploit para establecer una conexión remota tipo reverse shell hacia la máquina atacante.

Esta fase representa el momento en el que el pentester valida de forma práctica el riesgo identificado. Según Scarfone y Mell (2007), la explotación permite demostrar el impacto real de una vulnerabilidad, transformando un riesgo teórico en una evidencia concreta.

La ejecución del archivo Rejjeto permitió establecer una sesión Meterpreter, confirmando el acceso no autorizado a Host A.

**Figura 12**

*Inicio de Metasploit en Kali Linux*

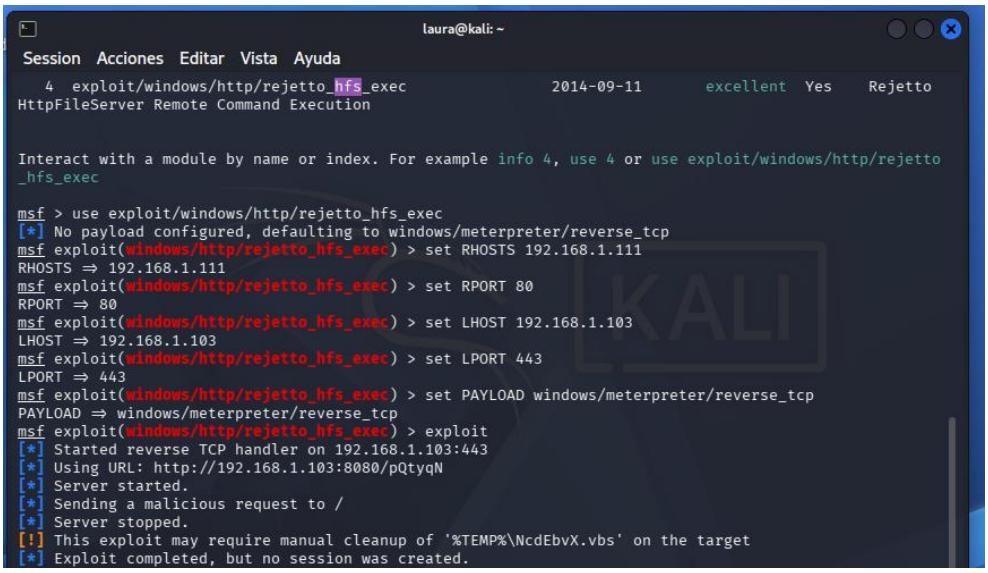



*Nota.* Se realiza el código msfconsole con el fin de iniciar el Metasploy, igualmente se continua con la explotación de la vulnerabilidad detectada.

Es importante tener en cuenta que Metasploit es una de las plataformas más utilizadas para la validación de vulnerabilidades y simulación de ataques controlados (Offensive Security, s.f.)

**Figura 13**

*Conexión remota*




*Nota.* Se utiliza el módulo exploit/windows/http/reanjohn_hfs_exec para obtener una sesión de Meterpreter. Se definió un payload tipo *windows/meterpreter/reverse_tcp*, el cual permite establecer una sesión interactiva entre la máquina víctima en este caso el Host A y el atacante Kali Linux.

Es importante tener en cuenta que inicialmente se presentó un error al intentar asociar el listener a la dirección IP en el puerto, lo cual indica que la dirección configurada no correspondía a la interfaz de red del atacante o que el puerto se encontraba en uso.

Una vez corregida la configuración de la dirección IP correspondiente al atacante, el sistema arrojó el mensaje *"Started reverse TCP handler on 192.168.1.103:4444"*, lo cual indica que la herramienta ha iniciado correctamente un servicio de escucha en la dirección IP de la

máquina Kali. Este estado confirma que el entorno de ataque se encuentra preparado para recibir una conexión entrante desde la máquina comprometida (Host A).

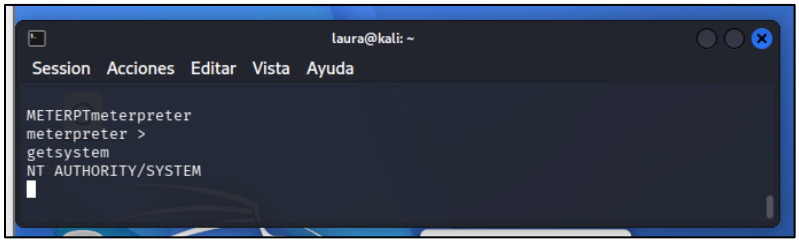
***Fase 5. Escalamiento de Privilegios***

Una vez obtenido el acceso inicial, el siguiente paso a seguir corresponde a elevar los privilegios para obtener control total del sistema.

Esta fase es clave, ya que muchas vulnerabilidades iniciales otorgan acceso limitado. Según Zuluaga Mateus (2017), el escalamiento de privilegios permite ampliar el alcance del ataque, facilitando la manipulación completa del sistema comprometido.

**Figura 14**

*Control del sistema atacante*




*Nota.* Una vez establecida la sesión remota mediante la herramienta Metasploit, se procede a la fase de escalamiento de privilegios, la cual se ejecuta dentro de la misma sesión activa sin necesidad de iniciar un nuevo proceso. El atacante (Kali Linux) ya cuenta con un acceso inicial al sistema, generalmente con permisos limitados, por lo que el objetivo es obtener control total sobre la máquina comprometida.

En este caso con el fin de lograrlo, se emplean funcionalidades propias de la sesión Meterpreter, como el comando getsystem, el cual intenta elevar los privilegios del usuario actual mediante diferentes técnicas automatizadas. Al ejecutarse correctamente, el sistema otorga permisos de nivel administrador, comúnmente representados como *NT AUTHORITY\SYSTEM*, lo que representa el máximo nivel de acceso en sistemas operativos Windows.

Esta fase es fundamental dentro del proceso de pentesting, ya que amplía significativamente el alcance del ataque. Este resultado indica que el atacante ha logrado el control total del sistema comprometido, permitiéndole ejecutar cualquier tipo de acción, como la modificación de configuraciones, creación de usuarios, acceso a archivos sensibles y manipulación de servicios del sistema.

***Fase 6. Post-Explotación y Persistencia***

La persistencia tiene como objetivo mantener el acceso al sistema comprometido incluso después de reinicios o cambios en la sesión. En la actividad, se evidenció mediante la creación de un usuario con privilegios administrativos.

Se representa un riesgo crítico, ya que permite al atacante conservar el control del sistema sin ser detectado. Behl y Behl (2017) destacan que la persistencia es una técnica común en ataques avanzados para garantizar acceso continuo.

La fase de post-explotación corresponde al conjunto de acciones que se realizan después de haber obtenido acceso al sistema objetivo. En esta etapa, el atacante (o el analista en un contexto de pentesting) busca aprovechar el acceso logrado para recolectar información, mantener el control del sistema y preparar posibles acciones posteriores.

Dentro de esta fase de acuerdo con lo investigado las herramientas como Metasploit permiten ejecutar comandos avanzados mediante sesiones como *Meterpreter*, facilitando actividades como:

- Obtención de información del sistema (usuarios, procesos, red)
- Escalamiento de privilegios (acceso a nivel administrador)
- Implementación de persistencia (creación de usuarios o backdoors)
- Extracción de credenciales o archivos sensibles

En el desarrollo de la actividad, se logró configurar correctamente el entorno de ataque y preparar el listener para la recepción de conexiones. Sin embargo, debido a limitaciones en la ejecución del archivo malicioso contenido en el recurso “Rejjeto”, no fue posible establecer una sesión remota real que permitiera ejecutar completamente esta fase. A pesar de ello, se comprendió el funcionamiento del proceso y se documentaron los comandos y procedimientos necesarios para su ejecución.

***Fase 7. Pivoting***

El pivoting es una técnica avanzada que se utiliza cuando un atacante, tras comprometer una máquina dentro de una red, la emplea como punto de acceso para atacar otros sistemas internos que inicialmente no eran accesibles.

Es este caso el atacante utiliza la máquina comprometida (Host A) como un “puente” para llegar a otra máquina (Host B), ampliando así el alcance del ataque dentro de la red.

El objetivo del pivoting es demostrar cómo una sola vulnerabilidad puede comprometer toda una red, evidenciando fallas en la segmentación y control de accesos.

En la actividad el pivoting estaba orientado a utilizar la máquina Host A (Windows 7) como punto de acceso para alcanzar la máquina Host B. No obstante, debido a que no se logró establecer una sesión activa con la primera máquina (Host A), no fue posible ejecutar esta fase de manera práctica.

Durante el desarrollo de la actividad se intentó en múltiples ocasiones establecer la conexión entre la máquina atacante (Kali Linux) y la máquina víctima (Host-A), configurando correctamente los parámetros de red, el listener y los puertos de comunicación. Sin embargo, el archivo proporcionado comprimido en formato .zip denominado Rejjeto presentó problemas en la ejecución, incluyendo solicitudes de autenticación y configuraciones previas desconocidas, lo que impidió generar la conexión necesaria para abrir una sesión Meterpreter.

A pesar de aplicar diferentes alternativas y configuraciones, no fue posible completar la explotación de manera real, lo que limitó la ejecución práctica de todas las fases de post-explotación y pivoting

**Datos e Información para Identificar el Fallo de Seguridad**

Durante el desarrollo del escenario de la actividad, fue posible identificar varios elementos importantes que permitieron reconocer el fallo de seguridad presente en la máquina Host A. Más allá de ejecutar las herramientas, el análisis consistió en interpretar la información disponible y entender cómo diferentes factores pueden facilitar un ataque.

Primero que todo, uno de los aspectos más relevantes fue el sistema operativo utilizado, ya que se trata de Windows 7. Este sistema, aunque fue ampliamente usado durante muchos años, actualmente se considera vulnerable debido a que ya no recibe actualizaciones de seguridad. Esto significa que existen múltiples fallos conocidos que pueden ser aprovechados por un atacante, lo que incrementa significativamente el riesgo de compromiso del sistema (Guarnizo Portela, 2024).

Por otra parte, mediante el uso de herramientas de reconocimiento como Nmap, se logró observar que la máquina tenía varios puertos abiertos, entre ellos el 135, 139 y 445. Estos puertos están asociados a servicios propios de Windows, como RPC, NetBIOS y SMB, los cuales permiten la comunicación y compartición de recursos dentro de la red. Sin embargo, cuando estos servicios están expuestos, también pueden convertirse en una puerta de entrada para ataques, especialmente en sistemas desactualizados (Scarfone & Mell, 2007).

Uno de los hallazgos más importantes fue la presencia del archivo comprimido denominado Rejjeto, el cual contenía herramientas como DarkComet.exe. Se tiene entendido que este tipo de software es conocido por permitir el acceso remoto a un equipo sin autorización, lo que indica que el ataque no solo depende de vulnerabilidades técnicas, sino también de la

interacción del usuario. En este caso, si el usuario ejecuta el archivo sin verificar su origen, facilita directamente el acceso al sistema, lo que evidencia una debilidad en la seguridad a nivel humano.

Se puede decir que el fallo de seguridad identificado no es único, sino que responde a la combinación de varios factores. Por un lado, existe una vulnerabilidad técnica asociada al sistema operativo y a los servicios expuestos en la red. Por otro lado, se evidencia una vulnerabilidad relacionada con el usuario, quien podría ejecutar software malicioso sin tomar las precauciones necesarias.

Adicionalmente, la conectividad entre las máquinas dentro del entorno virtual permitió comprobar que existe comunicación directa entre el atacante (Kali Linux) y la víctima (Host-A). Esto es importante, ya que demuestra que no hay restricciones significativas en la red, como reglas de firewall o segmentación, lo que facilita aún más la ejecución de ataques.

Aunque se configuró correctamente el entorno de explotación utilizando Metasploit, no fue posible establecer una conexión real con la máquina víctima en este caso el Host A debido a limitaciones del archivo proporcionado. Sin embargo, este proceso permitió comprender cómo se prepararía un ataque real y cómo se aprovecharían las vulnerabilidades identificadas

**Herramienta Utilizada Para Identificar Fallos**

Durante el desarrollo de la actividad, la identificación de fallos de seguridad en la máquina Host A (Windows 7) se realizó principalmente mediante el uso de herramientas de reconocimiento y análisis de red. Entre ellas, una de las más importantes fue Nmap, la cual permitió obtener información detallada sobre los servicios activos y los puertos abiertos en el sistema objetivo.

El uso de esta herramienta consistió en ejecutar un escaneo de puertos sobre la dirección IP de la máquina víctima, lo que permitió determinar qué servicios estaban expuestos en la red.

Este tipo de análisis es fundamental en una prueba de penetración, ya que permite identificar posibles puntos de entrada que podrían ser aprovechados por un atacante (Scarfone & Mell, 2007).

Como resultado del escaneo realizado, se evidenció la presencia de varios puertos abiertos, entre los cuales destacan el puerto 135 (RPC), 139 (NetBIOS) y especialmente el puerto 445 (SMB). Este último es particularmente importante, ya que está asociado al protocolo Server Message Block (SMB), utilizado para la compartición de archivos e impresoras en sistemas Windows. Aunque este servicio es útil en entornos de red, también es conocido por haber presentado múltiples vulnerabilidades a lo largo del tiempo, especialmente en versiones antiguas del sistema operativo.

La identificación del puerto 445 como abierto representa un hallazgo crítico, ya que este puerto ha sido históricamente utilizado como vector de ataque en sistemas Windows desactualizados. En versiones como Windows 7, la exposición de este servicio puede permitir la ejecución remota de código si no se cuenta con las actualizaciones de seguridad correspondientes. Esto lo convierte en un punto clave para el desarrollo de ataques y para la posterior explotación del sistema.

Igualmente, el análisis del escenario permitió identificar la presencia de un archivo malicioso dentro de la máquina víctima, lo que sugiere que el ataque no depende únicamente de una vulnerabilidad de red, sino también de la ejecución de software no confiable por parte del usuario. Este tipo de situaciones es común en entornos reales, donde los atacantes combinan técnicas de ingeniería social con vulnerabilidades técnicas para aumentar las probabilidades de éxito.

Para la fase de explotación se utilizó la herramienta Metasploit, la cual permite gestionar exploits y establecer conexiones remotas con sistemas vulnerables. En este caso, se configuró un

listener mediante el módulo multi/handler, con el objetivo de recibir una conexión desde la máquina víctima a través de un payload de tipo reverse_tcp.

Sin embargo, durante la ejecución de la actividad no fue posible establecer una conexión real entre la máquina atacante y la víctima, debido a limitaciones en el archivo proporcionado (Rejjeto), el cual requería configuraciones adicionales no disponibles. A pesar de esto, el proceso permitió comprender cómo se prepararía un ataque real y cómo se aprovecharía el puerto identificado para obtener acceso al sistema.

**Tabla 2**

*Clasificación de Herramientas para Identificación de Fallos de Seguridad*

| Fase | Herramienta | Propósito |
|---|---|---|
| Reconocimiento / Escaneo de red | Nmap (nmap -sV) | Se ejecutó un escaneo de puertos y detección de servicios para identificar la superficie de ataque, confirmando que el Host A (192.168.1.111) Identificación de puertos abiertos: 135, 139, 445 |
| Análisis de Vulnerabilidades | Searchsploit / MSF (search hfs) | Localizar el exploit para la aplicación vulnerable. |
| Explotación | Metasploit (exploit) | Se utilizó el módulo rejetto_hfs_exec para romper el perímetro de seguridad del Host-A, logrando establecer una conexión reversa y obteniendo una sesión de Meterpreter. |
| Post-Explotación | Meterpreter (getsystem) | Eleva privilegios mediante el comando getsystem para alcanzar el nivel de SYSTEM y se crea una cuenta administrativa personalizada, |

| Fase | Herramienta | Propósito |
|---|---|---|
| | | cumpliendo con la validación de la intrusión solicitada |
| Pivoting | Autoroute | Configura una ruta de red interna a través de la máquina comprometida para permitir que el equipo atacante pueda alcanzar el Host-B (192.168.1.112), simulando un movimiento lateral en la red. |

*Nota*. Resume de manera estructurada el proceso seguido para la identificación de fallos de seguridad en la máquina Host-A. Se evidencia cómo el uso de herramientas de reconocimiento como Nmap permitió detectar servicios vulnerables, mientras que Metasploit se utilizó para preparar la fase de explotación

**Análisis del Ataque Presentado**

Una vez se pudieron identificar las vulnerabilidades presentes en la máquina Host A, es importante tener en cuenta cómo estas pueden ser aprovechadas por un atacante y cuál sería el impacto real sobre los sistemas involucrados. En este caso, el análisis que realice se enfocó en cómo un ataque podría afectar a las máquinas Windows dentro de la red, considerando tanto el acceso inicial como las posibles acciones posteriores.

El ataque inicia cuando el atacante, desde su equipo (Kali Linux), identifica servicios vulnerables en la máquina objetivo mediante herramientas de reconocimiento como Nmap. Este proceso permite detectar puertos abiertos y servicios activos, como el protocolo SMB en el puerto 445, que representa un punto crítico en sistemas Windows desactualizados.

El siguiente paso consiste en preparar el entorno de explotación. Esto se logra mediante herramientas especializadas como Metasploit, que permiten configurar un listener para recibir

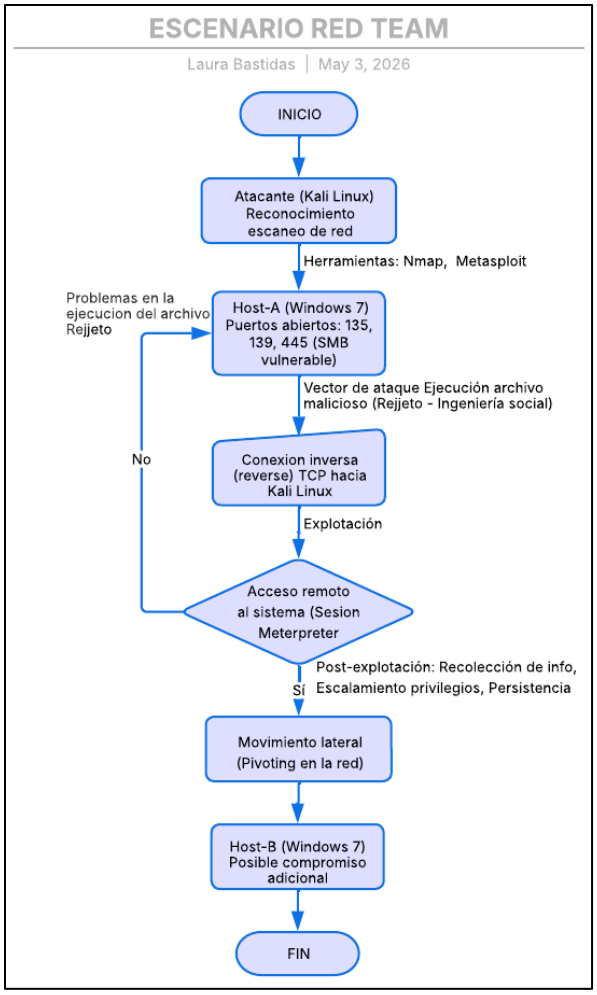
conexiones desde la máquina víctima. Esta conexión puede generarse mediante la ejecución de un archivo malicioso por parte del usuario, como el identificado "*Rejjeto"*, lo cual evidencia el uso de técnicas de ingeniería social.

Una vez que la máquina víctima ejecuta este archivo malicioso, se establece de forma inmediata una conexión inversa hacia el atacante, permitiendo el acceso remoto al sistema. En este punto, el atacante puede obtener control del equipo, ejecutar comandos, acceder a archivos, capturar información sensible e incluso modificar configuraciones del sistema. Además, el impacto del ataque no se limita únicamente a la máquina comprometida. Si el atacante logra mantener el acceso y escalar privilegios, puede utilizar la máquina afectada como punto de entrada para atacar otros dispositivos dentro de la red. Este proceso, conocido como movimiento lateral o pivoting, puede comprometer múltiples equipos, ampliando el alcance del incidente y generando un riesgo significativo para toda la infraestructura (Scarfone & Mell, 2007).

Es importante tener en cuenta que de tantos intentos y revisión de la configuración de las máquinas virtuales, no fue posible establecer una conexión real debido a limitaciones del archivo proporcionado, en este caso se logró comprender y practicar cómo se desarrollaría el ataque en un entorno real, con los diferentes errores y obstáculos presentados, poniéndose en los zapatos de un atacante. Esto permitió analizar el impacto potencial y evidenciar la importancia de implementar medidas de seguridad adecuadas, como la actualización de sistemas, la restricción de servicios innecesarios y la capacitación de los usuarios.

**Figura 15**

*Flujo del ataque en el escenario Red Team*




*Nota.* La figura muestra las fases del ataque desde el reconocimiento hasta el movimiento lateral dentro de la red. https://lucid.app/lucidchart/20ab946e-2b4f-4210-8c9d-8eb03cd10de7/view

El flujo del ataque inicia con la fase de reconocimiento, donde el atacante identifica los servicios activos en la máquina objetivo. Posteriormente, se aprovecha un vector de ataque basado en la ejecución de un archivo malicioso por parte del usuario, lo que permite establecer una conexión inversa hacia el equipo atacante.

Una vez obtenida la conexión, el atacante puede acceder al sistema de manera remota, ejecutar comandos y realizar acciones propias de la fase de post-explotación. Finalmente, el ataque puede extenderse a otros equipos dentro de la red mediante técnicas de movimiento lateral, comprometiendo así múltiples sistemas.

## Respuesta y Contención ante Incidentes de Ciberseguridad

### Acciones Ante un Ataque en Tiempo Real

En el desarrollo de la actividad donde se detectó un ataque informático en tiempo real, lo primero que se debe realizar como integrante de un equipo Blue Team es identificar el alcance del incidente y recopilar la mayor cantidad de información posible sin alterar las evidencias del sistema. Esto es fundamental, ya que una reacción apresurada puede ocasionar la pérdida de información importante para el análisis del ataque y dificultar posteriormente las labores de contención y respuesta.

Se debe verificar qué equipos están siendo afectados, qué servicios presentan comportamientos anormales y si existen conexiones sospechosas activas dentro de la red. Para ello, es importante revisar aspectos técnicos del sistema operativo como procesos en ejecución, consumo inusual de recursos, usuarios conectados, servicios activos y eventos registrados en el sistema. Igualmente, analizar el tráfico de red para identificar direcciones IP desconocidas, conexiones remotas no autorizadas o transferencia anormal de datos.

En el caso planteado por SecureNova Labs, donde previamente se trabajó sobre una máquina Windows 7 vulnerable, uno de los primeros pasos que se realiza es validar si existen conexiones activas relacionadas con el puerto 445 (SMB) o procesos asociados a herramientas maliciosas utilizadas en el ejercicio de Red Team. Esto permite determinar si el ataque sigue activo y qué nivel de compromiso tiene el sistema.

Posteriormente, se aplican medidas de contención inmediatas con el fin de evitar que el ataque continúe propagándose dentro de la red. Entre estas acciones esta aislar temporalmente la máquina afectada, desconectándola de la red o limitando sus comunicaciones mediante reglas de firewall. Esta práctica es ampliamente utilizada en gestión de incidentes porque permite reducir el impacto mientras se realiza el análisis forense correspondiente (Zambrano Hernández, 2024).

Se utiliza herramientas de monitoreo y análisis con licencia libre o GPL, teniendo en cuenta las condiciones del escenario. Entre las herramientas a emplearse se encuentran:

Wireshark para analizar el tráfico de red y detectar conexiones sospechosas, TCPView para revisar conexiones activas y procesos asociados, Sysmon para generar registros avanzados de actividad del sistema y Snort como herramienta de detección de intrusos.

También es importante conservar evidencias del incidente. Por ello, se deben guardar registros del sistema, capturas de tráfico y logs de eventos antes de reiniciar o modificar el equipo comprometido. Esto permite comprender posteriormente cómo ocurrió el ataque, qué vulnerabilidades fueron aprovechadas y determinar el tipo de ataque que se está presentando.

Por último, después de contener el incidente, se procede a realizar un análisis más profundo para identificar la causa raíz del ataque, corregir la vulnerabilidad explotada y fortalecer las medidas de seguridad del sistema con el fin de evitar que la situación vuelva a repetirse.

**Medidas de Hardenización**

Después de realizar el ejercicio práctico de Red Team, fue posible identificar varias debilidades de seguridad presentes en la máquina Windows utilizada en el laboratorio. Entre las principales vulnerabilidades se encontraron servicios expuestos en la red, puertos abiertos, un sistema operativo desactualizado y la posibilidad de ejecutar archivos sospechosos sin mayores restricciones. Estas condiciones demostraron cómo un atacante puede aprovechar configuraciones inseguras para comprometer un equipo y posiblemente afectar otros sistemas dentro de la misma red.

De acuerdo con lo anterior, una de las primeras medidas que se proponen es fortalecer el sistema mediante procesos de hardenización. La hardenización consiste en aplicar

configuraciones de seguridad que permitan reducir riesgos y limitar las oportunidades de ataque sobre los sistemas informáticos (CIS Security, 2020).

Es importante en este caso mantener actualizado el sistema operativo y todas las aplicaciones instaladas. En la actividad se trabajó con Windows 7, el cual actualmente ya no cuenta con soporte oficial ni actualizaciones de seguridad constantes. Esto representa un riesgo considerable, ya que muchas vulnerabilidades conocidas continúan siendo explotadas precisamente en sistemas antiguos. Por esta razón, utilizar versiones actualizadas y aplicar parches de seguridad periódicamente ayuda a disminuir las posibilidades de compromiso.

Otra medida fundamental es revisar y deshabilitar servicios innecesarios. Durante el escaneo realizado en el ejercicio de Red Team se identificaron puertos abiertos relacionados con servicios de red como SMB, especialmente el puerto 445, el cual suele ser utilizado en ataques dirigidos a sistemas Windows vulnerables. Si estos servicios no son necesarios dentro de la organización, lo más recomendable sería deshabilitarlos o restringir su acceso únicamente a usuarios autorizados.

Es necesario implementar políticas de control sobre la ejecución de software. El escenario demostró cómo la ejecución de archivos sospechosos puede convertirse en un vector de ataque crítico. Por ello, sería recomendable restringir permisos de instalación, bloquear la ejecución de aplicaciones desconocidas y utilizar herramientas de control de aplicaciones para validar qué programas pueden ejecutarse en los equipos.

También sería importante implementar herramientas de supervisión continua, tales como: Snort para detectar actividades sospechosas en la red, Wazuh para monitoreo de eventos y correlación de alertas, y Sysmon para registrar actividad avanzada en sistemas Windows.

Estas herramientas permiten identificar comportamientos anormales y responder de manera temprana ante posibles incidentes.

Otra medida importante es aplicar el principio de mínimo privilegio. Esto significa que los usuarios únicamente deben tener los permisos necesarios para realizar sus funciones, evitando cuentas con privilegios administrativos innecesarios. Esta práctica reduce considerablemente el impacto que podría tener un malware o un atacante dentro del sistema.

Asimismo, se propone segmentar la red para evitar movimientos laterales entre equipos. En el escenario analizado se planteó la posibilidad de pivoting hacia otras máquinas Windows, por lo que dividir la red en segmentos controlados permitiría limitar la propagación de un ataque.

También es fundamental fortalecer la concientización de los usuarios. Muchos ataques informáticos exitosos dependen de errores humanos, como abrir archivos maliciosos o descargar software no confiable. Por ello, la capacitación constante en temas de seguridad informática resulta esencial para reducir riesgos.

**Diferencia entre Blue Team y Respuesta a Incidentes (IR)**

Siempre se tiene pensado desde un principio que el equipo de Blue Team y el equipo de respuesta a incidentes realizan exactamente las mismas funciones, en realidad cada uno cumple un papel diferente dentro de la ciberseguridad de una organización. Ambos trabajan para proteger la información y los sistemas, pero su enfoque y momento de actuación son distintos.

El equipo de Blue Team se enfoca principalmente en la prevención y defensa continua de la infraestructura tecnológica. Su trabajo consiste en monitorear la red, identificar vulnerabilidades, fortalecer configuraciones de seguridad y detectar comportamientos sospechosos antes de que se conviertan en un problema mayor. Esto quiere decir que el equipo de Blue Team busca anticiparse a los ataques y mantener protegidos los sistemas de la organización.

Como ejemplo tenemos la actividad desarrollada, en este caso el equipo de Blue Team sería el encargado de revisar constantemente el tráfico de red, analizar los puertos abiertos encontrados en la máquina Windows y verificar si existen conexiones o actividades que puedan representar una amenaza. Además, se tiene la responsabilidad de implementar medidas de hardenización para evitar que vulnerabilidades como las identificadas en el ejercicio de Red Team vuelvan a ser explotadas.

Para cumplir estas funciones, el Blue Team suele apoyarse en herramientas de monitoreo y análisis como Wazuh, Snort o sistemas SIEM que permiten supervisar eventos de seguridad en tiempo real.

El equipo de respuesta a incidentes informáticos entra en acción cuando el ataque ya ocurrió o existe evidencia de un compromiso de seguridad. Su función principal es controlar la situación, reducir el impacto del incidente y recuperar los sistemas afectados lo más rápido posible.

Este equipo debe analizar qué ocurrió, cómo se produjo el ataque, qué equipos resultaron comprometidos y qué acciones deben ejecutarse para contener la amenaza. También se encarga de preservar evidencias digitales, realizar análisis forense y documentar el incidente para evitar que vuelva a repetirse en el futuro (Zambrano Hernández, 2024).

En el caso desarrollado en la actividad, si la máquina Windows llegara a ser comprometida por completo, el equipo de respuesta a incidentes sería quien aislaría el equipo afectado, revisaría los registros del sistema, identificaría el origen del ataque y coordinaría las acciones necesarias para restaurar la operación normal.

La principal diferencia entre ambos equipos es que el equipo de Blue Team trabaja de forma preventiva y constante, mientras que el equipo de respuesta a incidentes actúa cuando ya existe una afectación real. Sin embargo, ambos deben trabajar de manera coordinada, ya que la

información obtenida durante un incidente ayuda posteriormente al Blue Team a fortalecer las medidas de protección y mejorar la seguridad de la organización.

También existe una diferencia en el enfoque de trabajo de cada uno ya que el equipo de Blue Team suele concentrarse más en monitoreo, prevención y fortalecimiento de controles de seguridad, mientras que el equipo de respuesta a incidentes tiene un enfoque más operativo y forense, debido a que debe actuar rápidamente frente a situaciones críticas.

Es importante tener en cuenta que, con respecto al nivel organizacional, ambos equipos son igual de importantes. El equipo de Blue Team ayuda a disminuir la probabilidad de que ocurra un ataque, mientras que el equipo de respuesta a incidentes permite controlar el daño cuando las medidas preventivas no fueron suficientes.

**Tabla 3**

*Comparación entre Blue Team y Respuesta a Incidentes*

| Blue Team | Equipo de Respuesta a Incidentes |
|---|---|
| Trabaja de manera preventiva. | Actúa cuando el incidente ya ocurrió. |
| Monitorea continuamente la infraestructura. | Gestiona y contiene incidentes de seguridad. |
| Implementa controles y hardenización. | Analiza evidencias y recupera sistemas. |
| Detecta actividades sospechosas. | Realiza análisis forense del incidente. |
| Busca reducir vulnerabilidades y riesgos. | Busca minimizar el impacto del ataque. |
| Utiliza herramientas de monitoreo y detección. | Utiliza herramientas forenses y de contención. |

*Nota*. La comparación anterior permite evidenciar que, aunque el Blue Team y el equipo de respuesta a incidentes tienen funciones diferentes dentro de la ciberseguridad, ambos trabajan de manera complementaria para fortalecer la protección de la organización. Mientras uno se enfoca en la prevención y monitoreo continuo, el otro actúa directamente frente a incidentes ya materializados, buscando contener y minimizar el impacto de las amenazas.

**Uso de CIS (Center for Internet Security)**

Si dentro de un equipo Blue Team se solicita trabajar con CIS (Center for Internet Security), lo utilizaría principalmente como una guía de buenas prácticas para fortalecer la seguridad de los sistemas y reducir vulnerabilidades dentro de la infraestructura tecnológica de la organización. CIS es reconocido a nivel mundial por desarrollar estándares, controles y configuraciones seguras que ayudan a proteger sistemas operativos, redes, aplicaciones y dispositivos frente a diferentes amenazas informáticas. Los CIS Benchmarks constituyen un conjunto de buenas prácticas reconocidas internacionalmente para fortalecer la configuración segura de sistemas operativos, servidores y dispositivos de red (CIS Security, 2020).

Uno de los recursos más importantes de CIS son los llamados CIS Benchmarks, los cuales contienen recomendaciones técnicas detalladas para realizar procesos de hardenización en diferentes plataformas tecnológicas. Estas guías permiten configurar de manera más segura sistemas Windows, Linux, servidores, dispositivos de red y aplicaciones, disminuyendo la superficie de ataque y evitando configuraciones inseguras (CIS Security, 2020).

De acuerdo con la actividad desarrollada en el escenario de Blue Team, se requiere utilizar CIS principalmente para corregir las debilidades identificadas durante el ejercicio de Red Team. En este caso, después de detectar puertos vulnerables, servicios innecesarios y configuraciones inseguras en Windows 7, se deben aplicar las recomendaciones de CIS para fortalecer el sistema operativo y mejorar la protección de la red.

Entre las principales acciones que se podrían implementar utilizando CIS se encuentran: deshabilitar servicios innecesarios, configurar políticas seguras de contraseñas, restringir privilegios administrativos, fortalecer reglas de firewall, desactivar protocolos inseguros, aplicar configuraciones seguras sobre SMB y otros servicios de red y también, mejorar los registros y auditorías del sistema.

Todas estas acciones ayudan a disminuir la superficie de ataque y hacen más difícil que un atacante logre comprometer los sistemas.

Además de servir para fortalecer equipos y servidores, CIS también puede utilizarse para realizar auditorías de seguridad. Muchas organizaciones comparan sus configuraciones actuales frente a los estándares CIS para identificar qué aspectos necesitan mejorar y qué riesgos podrían existir dentro de la infraestructura tecnológica.

Otro tema importante es que CIS permite establecer una línea base de seguridad. Esto significa que todos los equipos y sistemas pueden configurarse siguiendo los mismos criterios de protección, reduciendo errores de configuración y fortaleciendo la gestión de seguridad dentro de la organización.

Desde un equipo de Blue Team, trabajar con CIS también facilita las tareas de monitoreo y prevención, ya que los sistemas correctamente endurecidos presentan menos vulnerabilidades explotables y generan una postura defensiva más sólida frente a ataques externos.

Adicionalmente, una ventaja importante es que CIS ofrece documentación ampliamente reconocida en el ámbito profesional y académico, lo que permite implementar controles basados en estándares internacionales y buenas prácticas de ciberseguridad.

**Funciones y características de un SIEM**

Un SIEM (Security Information and Event Management) es una plataforma de seguridad diseñada para recopilar, centralizar y supervisar los registros generados por diferentes dispositivos, aplicaciones y sistemas dentro de una organización. Su principal propósito es analizar y correlacionar eventos de seguridad provenientes de múltiples fuentes, permitiendo identificar comportamientos inusuales, actividades sospechosas y posibles incidentes de manera oportuna. Además, estas herramientas facilitan la generación de alertas, el monitoreo continuo de la infraestructura tecnológica y el apoyo a los procesos de investigación y respuesta ante

incidentes, fortaleciendo así las capacidades de detección temprana de amenazas (Moreno, 2015).

Actualmente, las organizaciones generan una gran cantidad de información relacionada con seguridad, proveniente de servidores, firewalls, antivirus, aplicaciones, dispositivos de red y sistemas operativos. Analizar manualmente toda esta información sería una tarea compleja y poco eficiente. Por esta razón, los SIEM permiten centralizar los registros o logs de múltiples fuentes para facilitar su monitoreo y análisis (Moreno, 2015).

Dentro de un equipo Blue Team, un SIEM es una herramienta fundamental porque permite tener visibilidad continua sobre lo que ocurre en la infraestructura tecnológica. Gracias a esto, es posible identificar comportamientos anormales, accesos no autorizados, intentos de ataque o actividades que puedan representar un riesgo para la organización.

En el escenario trabajado anteriormente durante el desarrollo de la actividad, un SIEM sería útil para detectar conexiones sospechosas relacionadas con el ataque realizado desde el ejercicio de Red Team. Por ejemplo, permitiría identificar intentos de conexión al puerto 445, tráfico inusual en la red o la ejecución de procesos maliciosos dentro de la máquina Windows analizada.

Las principales funciones identificadas de un SIEM son:

**Recolección de eventos y logs:** El SIEM recopila información proveniente de múltiples dispositivos y sistemas, como servidores, routers, firewalls, estaciones de trabajo y aplicaciones. Esta información incluye eventos de acceso, errores, conexiones de red y actividades de usuarios.

**Correlación de eventos**: Una de las características más importantes de un SIEM es su capacidad para relacionar eventos provenientes de diferentes fuentes. Esto permite detectar patrones sospechosos que individualmente podrían parecer normales, pero que en conjunto representan un posible ataque. Un posible caso puede ser varios intentos fallidos de autenticación

seguidos de un acceso exitoso desde una dirección IP desconocida podrían indicar un intento de intrusión.

**Monitoreo en tiempo real:** Los SIEM permiten supervisar continuamente la infraestructura tecnológica y generar alertas automáticas cuando se detectan actividades anormales o indicadores de compromiso.

Esta capacidad es fundamental para los equipos Blue Team, ya que facilita una respuesta rápida frente a incidentes de seguridad.

**Generación de alertas:** Cuando el sistema identifica un comportamiento sospechoso, el SIEM genera notificaciones o alertas para que los analistas de seguridad puedan investigar el incidente.

**Análisis forense y auditoría:** Los registros almacenados por un SIEM también son útiles para investigaciones posteriores. Permiten reconstruir eventos, analizar cómo ocurrió un ataque y determinar qué sistemas fueron afectados.

**Cumplimiento normativo:** Muchas organizaciones utilizan SIEM para cumplir requisitos legales y normativos relacionados con seguridad y protección de datos, ya que facilitan la conservación y auditoría de registros.

**Tabla 4**

*Principales Características de un SIEM*

| Característica | Descripción |
|---|---|
| Centralización de logs | Reúne registros de múltiples dispositivos y sistemas. |
| Correlación de eventos | Relaciona eventos para detectar amenazas complejas. |
| Monitoreo continuo | Supervisa la infraestructura en tiempo real. |
| Generación de alertas | Notifica actividades sospechosas automáticamente. |
| Análisis forense | Permite investigar incidentes y reconstruir eventos. |
| Escalabilidad | Puede adaptarse al crecimiento de la organización. |

| | |
|---|---|
| Automatización | Facilita respuestas rápidas ante incidentes. |

*Nota*. Los sistemas SIEM se han convertido en herramientas fundamentales para los equipos Blue Team, ya que permiten supervisar continuamente la infraestructura tecnológica y detectar amenazas de manera más eficiente. Gracias a la centralización y correlación de eventos, las organizaciones pueden responder rápidamente frente a incidentes de seguridad y reducir el impacto de posibles ataques.

Existen diferentes herramientas SIEM utilizadas en ciberseguridad, tanto comerciales como de código abierto. Algunas de las más conocidas son: Wazuh, Splunk, OSSIM y Elastic Stack

En escenarios académicos y laboratorios, herramientas como Wazuh y OSSIM suelen ser utilizadas debido a que ofrecen funcionalidades avanzadas y pueden implementarse con tecnologías de código abierto.

**Herramientas de Contención**

Dentro de la ciberseguridad, las herramientas de contención cumplen un papel fundamental cuando ocurre un incidente informático, ya que su principal objetivo es limitar el impacto del ataque y evitar que continúe propagándose dentro de la infraestructura tecnológica. A diferencia de las herramientas de detección, que se enfocan en identificar amenazas o actividades sospechosas, las herramientas de contención buscan bloquear, aislar o restringir las acciones del atacante una vez el incidente ha sido identificado.

En un escenario de Blue Team, como el desarrollado del caso de SecureNova Labs, las herramientas de contención serían esenciales para impedir que un ataque comprometa más equipos dentro de la red o genere mayores afectaciones sobre la información de la organización.

Sin embargo, saber que el Host-A fue sido comprometido por un agente remoto no detiene el avance del adversario. Es allí donde interviene la contención, que representa la acción de desplegar "puertas cortafuegos" lógicas o físicas para limitar el radio de explosión del ataque, impidiendo la exfiltración de activos y cerrando el paso a movimientos laterales hacia servidores críticos como el Host-B.

A continuación, se describen tres herramientas de contención ampliamente utilizadas en ciberseguridad:

***1. Firewall***

Un firewall es una herramienta de seguridad que puede implementarse tanto en hardware como en software y cuya función principal es controlar el tráfico de red entrante y saliente mediante reglas de seguridad previamente definidas.

Durante un incidente de seguridad, el firewall permite bloquear conexiones sospechosas, restringir puertos vulnerables y aislar equipos comprometidos para evitar la propagación del ataque hacia otros sistemas de la red. Por ejemplo, en el escenario trabajado durante el ejercicio de Red Team, una medida de contención importante habría sido bloquear el puerto 445 asociado al protocolo SMB, reduciendo así la posibilidad de explotación remota.

Además, los firewalls ayudan a segmentar redes y limitar las comunicaciones únicamente a servicios autorizados, fortaleciendo la seguridad general de la infraestructura.

Entre las herramientas de firewall más conocidas se encuentran: pfSense, iptables y Windows Defender Firewall

***2. Endpoint Detection and Response (EDR)***

Las soluciones EDR son herramientas enfocadas en proteger los dispositivos finales o endpoints, como computadores y servidores. Aunque muchas plataformas EDR incluyen

funciones de detección, también poseen capacidades avanzadas de contención automática frente a incidentes de seguridad.

Estas herramientas permiten aislar un equipo comprometido de la red, finalizar procesos maliciosos, bloquear archivos sospechosos y evitar la ejecución de malware en tiempo real. Su uso es especialmente importante cuando un atacante ya logró acceder al sistema y se requiere reducir rápidamente el impacto del incidente.

En el caso de la actividad, una herramienta EDR podría haber bloqueado la ejecución del archivo malicioso identificado en el ejercicio de Red Team, evitando el establecimiento de conexiones remotas no autorizadas. Si el analista del SOC identifica que un atacante ha ganado privilegios de SYSTEM y está ejecutando comandos de reconocimiento de red local, se activa la función de Aislamiento de Host. Esta orden modifica instantáneamente las reglas de red del Host-A, cortando de raíz cualquier comunicación hacia la red interna o internet. La herramienta congela el dispositivo en su estado actual, impidiendo físicamente el puente técnico (pivoting) hacia el Host-B, pero manteniendo abierto de forma exclusiva un canal cifrado de gestión para que el equipo forense pueda extraer el volcado de memoria RAM antes de que se pierda la evidencia volátil.

Algunas herramientas conocidas en esta categoría son: Wazuh, CrowdStrike Falcon y Microsoft Defender for Endpoint

***3. Network Access Control (NAC)***

Las herramientas NAC (Control de Acceso a la Red) permiten gestionar qué dispositivos pueden conectarse a una red y en qué condiciones pueden hacerlo. Estas soluciones son utilizadas para aislar equipos sospechosos o restringir automáticamente dispositivos que representen un riesgo para la organización.

En caso de detectarse un incidente, el NAC puede bloquear el acceso del equipo comprometido o moverlo automáticamente a una red aislada para evitar que el ataque continúe expandiéndose.

Esta herramienta resulta especialmente útil en ataques donde existe movimiento lateral o pivoting entre diferentes máquinas dentro de la misma red, tal como se planteó en el escenario práctico del laboratorio.

Entre las soluciones NAC más utilizadas se encuentran: PacketFence, Cisco Identity Services Engine y FortiNAC

***4. Sistemas de Prevención de Intrusiones (IPS)***

Los Sistemas de Prevención de Intrusiones o IPS (Intrusion Prevention Systems) son herramientas de seguridad diseñadas para identificar actividades maliciosas dentro de la red y actuar automáticamente para detenerlas antes de que afecten los sistemas de la organización.

A diferencia de un IDS, que únicamente detecta amenazas y genera alertas, un IPS tiene la capacidad de bloquear conexiones sospechosas, detener tráfico malicioso o impedir intentos de explotación en tiempo real. Por esta razón, los IPS son considerados herramientas de contención, ya que ayudan a limitar el impacto de un ataque y evitar su propagación.

Dentro de un entorno Blue Team, un IPS resulta muy útil para proteger la red frente a ataques conocidos, escaneos de puertos, intentos de explotación o tráfico malicioso proveniente de atacantes externos.

En el escenario trabajado durante el laboratorio, un IPS habría permitido detectar y bloquear automáticamente conexiones sospechosas dirigidas al puerto 445 de la máquina Windows vulnerable, evitando que el ataque continuara avanzando dentro de la red, igualmente, al detectar el patrón exacto de una inyección de macros o comandos dirigida al puerto 80 del servicio Rejjeto, el IPS interrumpe inmediatamente el flujo de datos. Ejecuta acciones como el

descarte de paquetes maliciosos (drop) o el envío de paquetes de reinicio TCP (TCP reset) hacia la IP del atacante ($192.168.1.103$), neutralizando la sesión de Meterpreter en el instante exacto de su gestación, evitando que el software malicioso termine de alojarse en la memoria del host.

Entre las herramientas IPS más conocidas se encuentran: Snort, Suricata y Cisco Firepower

Es importante aclarar que las herramientas de contención no cumplen la misma función que las herramientas de detección.

**Tabla 5**

*Diferencia entre Herramientas de Detección y Contención*

| Herramientas de detección | Herramientas de contención |
|---|---|
| Identifican amenazas o actividades sospechosas. | Buscan detener o limitar el ataque. |
| Generan alertas y monitorean eventos. | Bloquean conexiones o aíslan sistemas. |
| Ejemplo: IDS, SIEM, antivirus. | Ejemplo: Firewall, EDR, NAC. |

*Nota*. La principal diferencia entre las herramientas de detección y las herramientas de contención radica en su función dentro de la ciberseguridad. Las herramientas de detección se encargan de identificar amenazas, actividades sospechosas o posibles incidentes mediante el monitoreo y análisis de eventos de seguridad; mientras que las herramientas de contención actúan directamente para limitar o detener el ataque, bloqueando conexiones, aislando equipos comprometidos o restringiendo accesos no autorizados. Ambas son complementarias y fundamentales para fortalecer la capacidad defensiva de un equipo Blue Team.

## Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/0tuBvjyxPY8

## Conclusiones

El desarrollo del seminario permitió comprender de manera práctica la importancia que tienen los equipos Red Team y Blue Team dentro de la ciberseguridad organizacional. A través de las diferentes actividades fue posible analizar cómo un atacante puede identificar y aprovechar vulnerabilidades presentes en un sistema, así como las estrategias defensivas necesarias para prevenir, detectar y contener este tipo de amenazas dentro de una infraestructura tecnológica.

Durante las prácticas realizadas en el laboratorio virtualizado se evidenció que muchas vulnerabilidades surgen debido a configuraciones inseguras, servicios expuestos, sistemas desactualizados o falta de controles adecuados de seguridad. Esto permitió reconocer que la protección de la información no depende únicamente de herramientas tecnológicas, sino también de procesos de monitoreo continuo, actualización permanente y aplicación de buenas prácticas dentro de las organizaciones.

Asimismo, el ejercicio desarrollado desde la perspectiva Red Team fortaleció los conocimientos relacionados con reconocimiento de red, escaneo de puertos, análisis de vulnerabilidades y simulación de explotación mediante herramientas como Nmap y Metasploit Framework. Aunque algunas fases no pudieron completarse totalmente debido a limitaciones propias del entorno virtualizado y del archivo utilizado durante el laboratorio, el proceso permitió comprender la lógica y funcionamiento de un ejercicio de pentesting en un escenario controlado.

Por otra parte, desde el enfoque Blue Team se logró identificar la importancia de implementar mecanismos de hardenización, segmentación de red, monitoreo de eventos y herramientas de contención como firewalls, IPS, EDR y sistemas SIEM, los cuales permiten fortalecer la seguridad y reducir el impacto de posibles incidentes informáticos. También se

comprendió que la respuesta ante ataques no debe enfocarse únicamente en reaccionar cuando ocurre un incidente, sino en mantener una postura preventiva basada en análisis de riesgos y controles de seguridad.

Otro aspecto importante desarrollado durante el seminario estuvo relacionado con la ética profesional y el marco normativo en ciberseguridad. El análisis del caso SecureNova Labs permitió reflexionar sobre la responsabilidad que tienen los profesionales del área frente al uso adecuado de herramientas ofensivas y el manejo de información sensible. Además, se identificó la importancia del cumplimiento de la Ley 1273 de 2009 y de los principios éticos establecidos por el COPNIA para garantizar un ejercicio profesional responsable y alineado con la legislación colombiana.

Finalmente, esta experiencia académica permitió fortalecer habilidades técnicas, analíticas y críticas relacionadas con pruebas de penetración, gestión de incidentes y defensa informática. Del mismo modo, dejó en evidencia que la ciberseguridad requiere un proceso constante de actualización y aprendizaje, debido a la evolución permanente de las amenazas digitales y a la necesidad de proteger adecuadamente los activos tecnológicos y la información dentro de las organizaciones.

## Recomendaciones

Se recomienda a las organizaciones mantener actualizados sus sistemas operativos, aplicaciones y servicios de red, ya que muchas vulnerabilidades explotadas por atacantes están relacionadas con software obsoleto o configuraciones inseguras. La actualización permanente permite corregir fallos de seguridad y reducir significativamente los riesgos de explotación.

Es importante implementar procesos de hardenización sobre servidores, estaciones de trabajo y dispositivos de red, deshabilitando servicios innecesarios, restringiendo puertos vulnerables y aplicando políticas de seguridad orientadas a minimizar la superficie de ataque dentro de la infraestructura tecnológica.

Asimismo, se recomienda fortalecer los mecanismos de monitoreo y supervisión mediante herramientas SIEM, firewalls, IPS y soluciones EDR, con el fin de detectar comportamientos anómalos y responder de manera oportuna frente a posibles incidentes de ciberseguridad.

Las organizaciones también deberían establecer procesos periódicos de auditoría y pruebas de penetración controladas, ya que este tipo de ejercicios permite identificar vulnerabilidades antes de que puedan ser aprovechadas por atacantes reales. Del mismo modo, resulta fundamental realizar análisis de riesgos constantes para evaluar el nivel de exposición de los activos tecnológicos.

Se recomienda fortalecer los procesos de capacitación y concientización en ciberseguridad dirigidos a usuarios, administradores y personal técnico, debido a que muchos incidentes ocurren por errores humanos, malas prácticas o desconocimiento frente a amenazas digitales.

Finalmente, se recomienda a las organizaciones adoptar una estrategia integral de seguridad basada en prevención, monitoreo y mejora continua, entendiendo que la

ciberseguridad no debe verse como un proceso temporal, sino como una práctica permanente orientada a proteger la información y garantizar la continuidad operativa frente a amenazas cada vez más sofisticadas.

## Referencias Bibliográficas


Alvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos* (pp. 1–26). Semantic Scholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Arroyo, E. (2025). *Sinergcertia de equipos Red Team y Blue Team en la protección de entornos corporativos* [Objeto Virtual de Información – OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/74595

Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://global.oup.com

Chindrus, C., & Caruntu, C.-F. (2023). *Securing the network: A Red and Blue cybersecurity competition case study. Information, 14(11),* 587. https://doi.org/10.2478/bipie-2023-0008

CIS Security. (2020). *CIS Benchmarks*. https://www.cisecurity.org/cis-benchmarks/

Congreso de la República de Colombia. (2008). *Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea el bien jurídico de protección de la información y de los datos*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Consejo Profesional Nacional de Ingeniería (COPNIA). (2015). *Código de ética para el ejercicio de la ingeniería*. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Greenbone Networks. (2020). *OpenVAS – Open Vulnerability Assessment System*. https://www.greenbone.net/en/openvas/

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia*. Universidad Nacional Abierta y a Distancia – UNAD. https://repository.unad.edu.co/handle/10596/41392

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). *Red Teaming vs. Blue Teaming: A* comparative analysis of cybersecurity strategies in the digital battlefield. *International Journal of Scientific Research in Engineering and Management, 7*(12), 1–11. https://doi.org/10.55041/IJSREM27675

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Políticas de privacidad y condiciones de uso*. https://www.mintic.gov.co/portal/inicio/Secciones-Uso

MITRE. (s.f.). *CVE – Common Vulnerabilities and Exposures*. https://cve.mitre.org/

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management)* (pp. 31–63). Universidad San Francisco de Quito. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

NFLO Tech. (2023). *Penetration testing tools overview*. https://nflo.tech/knowledge-base/penetration-testing-tools-overview/

Nmap Project. (s.f.). *Nmap Reference Guide*. https://nmap.org/book/man.html

Offensive Security. (s.f.). *Exploit Database (ExploitDB)*. https://www.exploit-db.com/

Offensive Security. (s.f.). *Metasploit Unleashed*. https://www.offensive-security.com/metasploit-unleashed/

Penetration Testing Authority. (2014). *Penetration testing tools*. https://penetrationtestingauthority.com/penetration-testing-tools

Pentesting101. (2026). *Pentesting tools*. https://pentesting101.net/tools/

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Rapid7. (2012). *Metasploitable 2*. https://metasploit.help.rapid7.com/docs/metasploitable-2

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Scribd. (2025). *PenTest phases*. https://www.scribd.com/document/968728733/PenTest-Phases

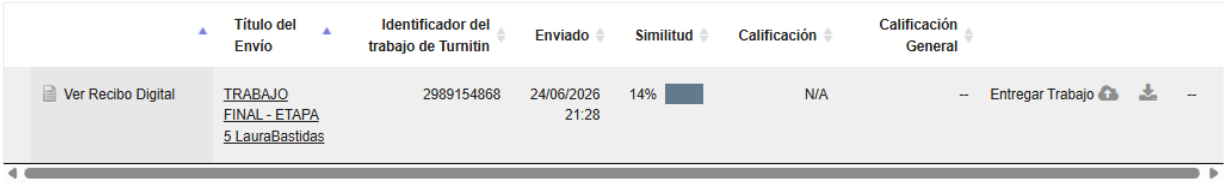
Zambrano Hernández, L. F., Peña Hidalgo, H. J., & Cárdenas Corral, M. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad*. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus, J. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, Seccional Armenia*. Universidad Nacional Abierta y a Distancia – UNAD. https://repository.unad.edu.co/handle/10596/17410

# Apéndices

## Apéndice A

*Resultado de revisión en Turnitin*



| | Título del Envío | Identificador del trabajo de Turnitin | Enviado | Similitud | Calificación | Calificación General | |
|---|---|---|---|---|---|---|---|
| Ver Recibo Digital | TRABAJO FINAL - ETAPA 5 LauraBastidas | 2989154868 | 24/06/2026 21:28 | 14% | N/A | -- | Entregar Trabajo -- |

*Nota.* La imagen presenta el reporte de similitud generado por la herramienta Turnitin para el documento evaluado, evidenciando un índice de coincidencia del 14 %, resultado obtenido a partir de la comparación del contenido con fuentes disponibles en bases de datos académicas, publicaciones y documentos previamente indexados.