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

Walter Gonzalez Rincon

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

A mi familia, por su paciencia y apoyo incondicional en cada etapa de este proceso. Su confianza fue el motor que impulsó cada hora de estudio y cada línea de este trabajo.

Agradecimientos

Al programa de Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia (UNAD), por ofrecer un espacio de formación riguroso y accesible que permite a profesionales en ejercicio alcanzar niveles de especialización de alto impacto.

Al docente Eduvin Trigos Sánchez, cuya orientación académica, disposición permanente y retroalimentación oportuna fueron determinantes para el desarrollo de este informe y del proceso formativo en su conjunto.

A los compañeros del curso Seminario Especializado: Equipos Estratégicos en Ciberseguridad Red Team & Blue Team, por los intercambios técnicos, las discusiones en los foros y el aprendizaje colaborativo que enriqueció cada etapa del seminario.

Finalmente, a mi familia, por la comprensión y el respaldo brindados durante el tiempo dedicado a este proceso de especialización. Su apoyo silencioso fue, en muchas ocasiones, el argumento más sólido para continuar.

Resumen

El presente informe técnico integra y analiza los resultados obtenidos en cuatro etapas tomando como base el caso articulador de SecureNova Labs, empresa de ciberseguridad cuyo entorno informático fue sometido a un ciclo completo de evaluación ofensiva y defensiva.

En la Etapa 1 se establecieron los fundamentos del marco legal colombiano aplicable a operaciones de seguridad informática, incluyendo la Ley 1273 de 2009, la Ley Estatutaria 1581 de 2012 y la Ley 2502 de 2025, además de las seis fases del pentesting con sus herramientas representativas. La Etapa 2 abordó el análisis ético y normativo de un acuerdo de confidencialidad con cláusulas ilegales que pretendían proteger actividades como chuzadas y accesos abusivos, identificando vulneraciones directas a los artículos 269A, 269B y 269F de la Ley 1273 y al Código de Ética del COPNIA. La Etapa 3 constituyó el núcleo técnico del ejercicio: sobre un entorno virtualizado aislado (Kali Linux, Host-A con HFS 2.3 vulnerable, Host-B con Windows 7 sin parches), el equipo Red Team ejecutó reconocimiento con Nmap, explotación de CVE-2014-6287 vía Metasploit, escalamiento de privilegios a NT AUTHORITY\SYSTEM, pivoting hacia Host-B y explotación de MS17-010 (EternalBlue), culminando con la creación controlada de una cuenta administrativa como prueba de concepto forense. Finalmente, la Etapa 4 formuló la respuesta Blue Team: protocolos de detección en tiempo real, hardenización, diferencias entre Blue Team y equipos de respuesta a incidentes, uso de frameworks CIS, funciones del SIEM y herramientas de contención GPL como IPTables, Wazuh y CrowdSec. Los hallazgos revelan que los vectores de ataque más críticos del escenario eran completamente prevenibles mediante gestión de parches, segmentación de red y monitoreo continuo. El informe concluye con recomendaciones estratégicas orientadas a elevar la madurez de seguridad de SecureNova Labs dentro de un marco legal, ético y técnicamente fundamentado.

***Palabras clave*:** forense, hardening, pentesting, virtualización, vulnerabilidades

Abstract

This technical report integrates and analyzes the results obtained in four stages, using SecureNova Labs, a cybersecurity company, as the case study. SecureNova Labs' IT environment underwent a complete offensive and defensive evaluation cycle. Stage 1 established the foundations of the Colombian legal framework applicable to cybersecurity operations, including Law 1273 of 2009, Statutory Law 1581 of 2012, and Law 2502 of 2025, as well as the six phases of penetration testing and their representative tools. Stage 2 addressed the ethical and regulatory analysis of a confidentiality agreement with illegal clauses intended to protect activities such as wiretapping and unauthorized access, identifying direct violations of Articles 269A, 269B, and 269F of Law 1273 and the COPNIA Code of Ethics. Stage 3 constituted the technical core of the exercise: in an isolated virtualized environment (Kali Linux, Host-A with a vulnerable HFS 2.3, Host-B with unpatched Windows 7), the Red Team performed reconnaissance with Nmap, exploited CVE-2014-6287 via Metasploit, escalated privileges to NT AUTHORITY\SYSTEM, pivoted to Host-B, and exploited MS17-010 (EternalBlue), culminating in the controlled creation of an administrative account as a forensic proof of concept. Finally, Stage 4 formulated the Blue Team's response: real-time detection protocols, hardening, differences between the Blue Team and incident response teams, use of CIS frameworks, SIEM functions, and GPL containment tools such as IPTables, Wazuh, and CrowdSec. The findings reveal that the most critical attack vectors in the scenario were entirely preventable through patch management, network segmentation, and continuous monitoring. The report concludes with strategic recommendations aimed at raising the security maturity of SecureNova Labs within a legal, ethical and technically sound framework.

***Keywords*:** forensics, hardening, pentesting, virtualization, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Equipo de seguridad defensiva responsable de la protección continua, detección de amenazas, respuesta a incidentes y fortalecimiento de controles.

CIS Controls:

Controles de seguridad del Centro de Seguridad de Internet (Center for Internet Security, CIS), reconocidos internacionalmente como guía de mejores prácticas defensivas.

COPNIA:

Consejo Profesional Nacional de Ingeniería: organismo colombiano que regula el ejercicio ético de la ingeniería y sus disciplinas afines.

CVE-2014-6287:

Vulnerabilidad de ejecución remota de código en Rejetto HTTP File Server versión 2.x, causada por validación inadecuada de entradas en la funcionalidad de búsqueda.

Escalamiento de privilegios:

Proceso de obtención de permisos superiores a los inicialmente asignados dentro de un sistema comprometido, típicamente hasta nivel SYSTEM o root.

EternalBlue (MS17-010):

Vulnerabilidad crítica en el protocolo SMBv1 de Windows, originalmente desarrollada por la NSA y filtrada en 2017, que permite ejecución remota de código sin autenticación.

Exploit:

Código o técnica que aprovecha una vulnerabilidad específica para obtener acceso no autorizado o ejecutar acciones maliciosas en un sistema.

Habeas Data:

Derecho fundamental que garantiza a las personas conocer, actualizar y rectificar la información personal almacenada en bases de datos.

Hardenización:

Proceso de fortalecimiento de sistemas mediante la reducción de la superficie de ataque: deshabilitación de servicios innecesarios, aplicación de parches y configuración segura.

IOC:

Indicators of Compromise: artefactos observables (IPs, hashes, dominios) que indican la posible ocurrencia de una intrusión o compromiso de seguridad.

Meterpreter:

Shell avanzada de Metasploit Framework que permite controlar un sistema comprometido en memoria, sin escribir artefactos en disco.

Pentesting:

Proceso controlado y autorizado de pruebas de penetración en el que se simulan ataques reales para identificar y validar vulnerabilidades en sistemas, redes o aplicaciones.

Pivoting:

Técnica mediante la cual un atacante utiliza un sistema comprometido como punto intermedio para alcanzar otros sistemas en redes internas no accesibles directamente.

PTES:

Penetration Testing Execution Standard: estándar metodológico que estructura las pruebas de penetración en siete fases sistemáticas y repetibles.

Purple Team:

Equipo que integra las perspectivas ofensivas y defensivas, facilitando la colaboración entre Red Team y Blue Team para mejorar la postura de seguridad de manera iterativa.

Red Team:

Equipo de seguridad ofensiva que simula ataques reales contra una organización para identificar vulnerabilidades antes de que actores maliciosos las exploten.

SIEM:

Security Information and Event Management: plataforma que centraliza, correlaciona y analiza eventos de seguridad en tiempo real para detectar amenazas y facilitar la respuesta a incidentes.

Timeline forense:

Registro cronológico detallado de eventos ocurridos durante un incidente o ejercicio, con marcas de tiempo precisas, utilizado en análisis forense digital.

Introducción

El avance exponencial de las amenazas cibernéticas en entornos organizacionales ha impulsado el desarrollo de modelos de seguridad basados en la simulación controlada de ataques reales. En este contexto, los equipos Red Team y Blue Team se consolidan como pilares fundamentales de cualquier estrategia de ciberseguridad madura, dado que permiten identificar, reproducir y mitigar vulnerabilidades desde perspectivas complementarias: ofensiva y defensiva.

SecureNova Labs representa un escenario empresarial verosímil en el que convergen múltiples desafíos de la ciberseguridad contemporánea: infraestructura con software desactualizado, ausencia de segmentación de red, marcos éticos comprometidos en contratos de confidencialidad y la necesidad imperiosa de responder eficientemente a incidentes sin incurrir en elevados costos de licenciamiento. Estas características hacen del caso un vehículo pedagógico de alto valor para el análisis técnico y estratégico.

El informe articula cuatro dimensiones complementarias: (1) el marco legal y regulatorio colombiano aplicable a operaciones de seguridad; (2) el análisis ético y normativo de las relaciones contractuales en ciberseguridad; (3) la ejecución técnica documentada de un ciclo completo de ataque Red Team con evidencia forense; y (4) la formulación de la respuesta defensiva Blue Team con herramientas, protocolos y marcos de referencia internacionales. La integración de estas dimensiones busca reflejar la complejidad real del ejercicio profesional en seguridad informática, donde las competencias técnicas deben estar necesariamente acompañadas de sólido criterio ético y conocimiento normativo.

Justificación

La justificación de este informe se sustenta en tres ejes fundamentales que reflejan la complejidad del panorama actual de la ciberseguridad.

Eje técnico. El entorno evaluado en SecureNova Labs reproduce condiciones comunes en organizaciones latinoamericanas: sistemas operativos sin actualizaciones críticas, aplicaciones legacy en producción y redes sin segmentación adecuada. Estas características no son excepcionales; representan la norma en sectores con infraestructura tecnológica envejecida y baja inversión en mantenimiento preventivo. Ante este escenario, la metodología PTES establece que las pruebas de penetración controladas son el mecanismo más preciso para cuantificar el riesgo real al que está expuesta una organización (The Penetration Testing Execution Standard, s.f.). Documentar el ciclo completo de ataque, desde el reconocimiento hasta la creación de persistencia, genera evidencia técnica de primera línea que fundamenta planes de remediación concretos y priorizados.

Eje legal y ético. El caso SecureNova Labs expone una problemática recurrente en el sector de la seguridad privada: el uso de instrumentos contractuales para encubrir actividades ilícitas o trasladar responsabilidades penales a terceros. Este riesgo no es hipotético. El análisis del acuerdo de confidencialidad presentado por la empresa evidencia violaciones directas a la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009) y contradicciones explícitas con el Código de Ética del COPNIA (Ley 842 de 2003). Ambas referencias recuerdan un principio que no admite excepciones: el ejercicio de la ciberseguridad no es éticamente neutro, y el profesional conserva responsabilidades legales inalienables que ningún contrato puede suprimir.

Eje estratégico. La restricción presupuestal de SecureNova Labs es una condición frecuente en organizaciones de tamaño mediano. Lejos de ser un obstáculo, esta limitación abre

la oportunidad de demostrar que herramientas de código abierto como Wazuh (Wazuh, 2024), CrowdSec (CrowdSec, 2024) e IPTables (Purdy, 2004) ofrecen capacidades de detección y contención comparables a las de soluciones comerciales de alto costo. Este argumento tiene un valor estratégico significativo para la toma de decisiones gerenciales: desmitifica la creencia de que la seguridad de alto nivel depende del presupuesto de licenciamiento, y reorienta el foco hacia la competencia del equipo humano y la rigurosidad de la implementación.

Objetivos

Objetivo General

Elaborar un informe integrando el análisis legal y ético del marco normativo colombiano, la ejecución documentada de un ciclo completo de prueba de penetración sobre el caso SecureNova Labs y la formulación de estrategias defensivas orientadas a la toma de decisiones gerenciales y técnicas.

Objetivos Específicos

Analizar el marco normativo colombiano vigente en materia de delitos informáticos y protección de datos personales, identificando su aplicabilidad concreta en el contexto de las operaciones de Red Team y Blue Team.

Documentar técnicamente el ciclo completo de ataque ejecutado en la Etapa 3, detallando el reconocimiento, la explotación de CVE-2014-6287, el escalamiento de privilegios, el pivoting y la explotación de MS17-010, con su respectiva evidencia forense y timeline.

Formular estrategias de respuesta Blue Team ante el escenario analizado, incluyendo protocolos de detección en tiempo real, medidas de hardenización, uso del framework CIS, funciones del SIEM y selección justificada de herramientas de contención con licencia GPL.

Integrar los hallazgos técnicos, éticos y normativos en un conjunto de conclusiones estratégicas y recomendaciones accionables que eleven la postura de seguridad de SecureNova Labs.

Desarrollo del informe

Estrategias de Red Team

Las operaciones Red Team dentro del caso SecureNova Labs siguieron una metodología estructurada basada en el Penetration Testing Execution Standard (PTES), que establece siete fases sistemáticas para garantizar la reproducibilidad, la trazabilidad y la validez técnica de los hallazgos. A diferencia de un escaneo automatizado puntual, la metodología Red Team replica las tácticas, técnicas y procedimientos (TTPs) de adversarios reales, lo que permite evaluar no solo la presencia de vulnerabilidades técnicas, sino la efectividad de los controles defensivos ante un atacante persistente y orientado a objetivos específicos (Penetration Testing Execution Standard Working Group, 2014).

Reconocimiento y Recolección de Inteligencia (Etapa 1 y Etapa 3)

La fase de reconocimiento constituye una de las etapas fundamentales dentro del proceso de evaluación de seguridad y pruebas de penetración, ya que permite obtener información relevante acerca de los sistemas objetivo antes de ejecutar actividades de análisis o explotación. Esta etapa combina técnicas de reconocimiento activo con el propósito de identificar la infraestructura de red, los servicios disponibles, los sistemas operativos en ejecución y otros elementos que puedan representar vectores potenciales de ataque.

El reconocimiento activo implica la interacción directa con los sistemas objetivo con el fin de identificar hosts disponibles, puertos abiertos, servicios en ejecución y características específicas de los dispositivos conectados a la red. Para esta tarea se utilizó la herramienta Nmap, ampliamente reconocida en el ámbito de la seguridad informática por sus capacidades de descubrimiento de hosts, escaneo de puertos, detección de servicios y reconocimiento de sistemas operativos. La información obtenida mediante estas técnicas permite determinar

posibles superficies de ataque y establecer las bases para las etapas posteriores del análisis de seguridad.

En el contexto del banco de trabajo correspondiente a la Etapa 1, tal como se muestra en la Figura 1, se implementó un entorno virtualizado utilizando el software Oracle VirtualBox, con el objetivo de simular un escenario controlado para la ejecución de las pruebas de reconocimiento y análisis de vulnerabilidades. La virtualización permitió aislar el entorno experimental, garantizando la integridad de los sistemas físicos y facilitando la reproducción de los resultados obtenidos.

El laboratorio estuvo conformado por tres máquinas virtuales interconectadas dentro de una misma red local. La primera corresponde a la máquina atacante, configurada con el sistema operativo Kali Linux, una distribución especializada en pruebas de penetración y auditorías de seguridad que incorpora un amplio conjunto de herramientas destinadas al análisis de redes, evaluación de vulnerabilidades y explotación controlada.

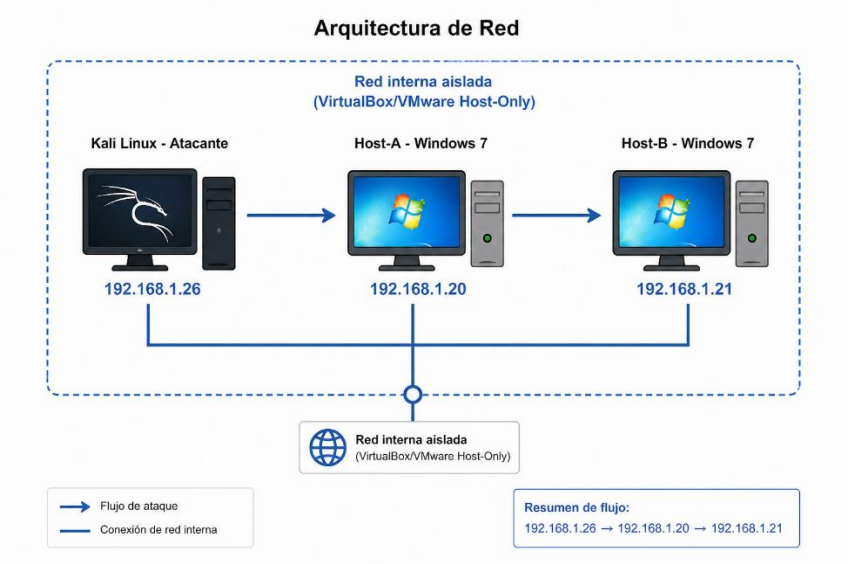
Adicionalmente, se configuraron dos máquinas objetivo: la máquina Host A, equipada con el sistema operativo Windows 7 y asignada a la dirección IP 192.168.1.20, y la máquina Host B, igualmente instalada con Windows 7 y configurada con la dirección IP 192.168.1.21. Ambas máquinas fueron implementadas en modo de adaptador puente, permitiendo su integración dentro de la misma red y facilitando la comunicación entre los diferentes dispositivos del entorno virtual.

Previo a la ejecución de las pruebas de reconocimiento, se realizaron verificaciones de conectividad entre los hosts mediante herramientas de diagnóstico de red, con el fin de confirmar la correcta configuración del entorno virtual. Esta validación constituyó un requisito indispensable para garantizar la disponibilidad de los equipos y la confiabilidad de los resultados obtenidos durante las fases posteriores del proceso de evaluación de seguridad.

La correcta implementación del entorno experimental permitió desarrollar las actividades de reconocimiento de manera controlada, obteniendo información relevante sobre la infraestructura de red y sentando las bases para las siguientes etapas del análisis, tales como la identificación de vulnerabilidades, la evaluación de riesgos y la ejecución de pruebas de penetración sobre los sistemas objetivo.

Figura 1

Arquitectura de red



Nota. Arquitectura de red de las máquinas virtuales para efectos de las pruebas.

En la Etapa 3 del proceso de reconocimiento y análisis de la infraestructura, tal como se ilustra en la Figura 2, se llevó a cabo un escaneo activo sobre la máquina objetivo Host-A mediante la herramienta Nmap, empleando el comando nmap -sV -sC -O 192.168.1.20.

La ejecución de este comando permitió realizar una enumeración exhaustiva de los servicios disponibles en el sistema objetivo. Los parámetros utilizados posibilitaron la detección de versiones de servicios (-sV), la ejecución de scripts predeterminados del motor NSE de Nmap (-sC) y la identificación del sistema operativo mediante técnicas de huella digital (-O). La

combinación de estas opciones proporcionó información detallada acerca de la configuración del host analizado y de los servicios expuestos a la red.

Los resultados obtenidos revelaron la presencia de varios servicios considerados críticos desde la perspectiva de la seguridad informática. En primer lugar, se identificó el puerto 8080/TCP abierto, asociado al servicio HTTP File Server (HFS) versión 2.3. La detección de esta aplicación resultó particularmente relevante debido a que determinadas versiones de HFS presentan vulnerabilidades conocidas que pueden permitir la ejecución remota de código o el acceso no autorizado al sistema, convirtiéndose en un objetivo prioritario durante las fases posteriores del análisis.

Asimismo, se detectó el puerto 445/TCP correspondiente al protocolo Server Message Block (SMB), ampliamente utilizado en entornos Windows para el intercambio de archivos, impresoras y recursos compartidos dentro de la red. La exposición de este servicio representa un elemento de interés durante las pruebas de seguridad, debido a que históricamente ha sido objeto de múltiples vulnerabilidades y ataques dirigidos a sistemas operativos Microsoft.

De igual manera, se identificó el puerto 135/TCP asociado al servicio Microsoft Remote Procedure Call (MSRPC), mecanismo utilizado por diversos componentes del sistema operativo Windows para la comunicación entre procesos y servicios remotos. La presencia de este servicio proporciona información adicional acerca de la arquitectura del sistema y puede facilitar procesos de enumeración o identificación de otros servicios dependientes.

El descubrimiento de estos servicios permitió establecer el vector de ataque principal dentro del entorno de pruebas, orientando las actividades de análisis y explotación hacia aquellos componentes que presentaban una mayor superficie de exposición. La información obtenida durante esta fase constituyó la base para la toma de decisiones respecto a las técnicas,

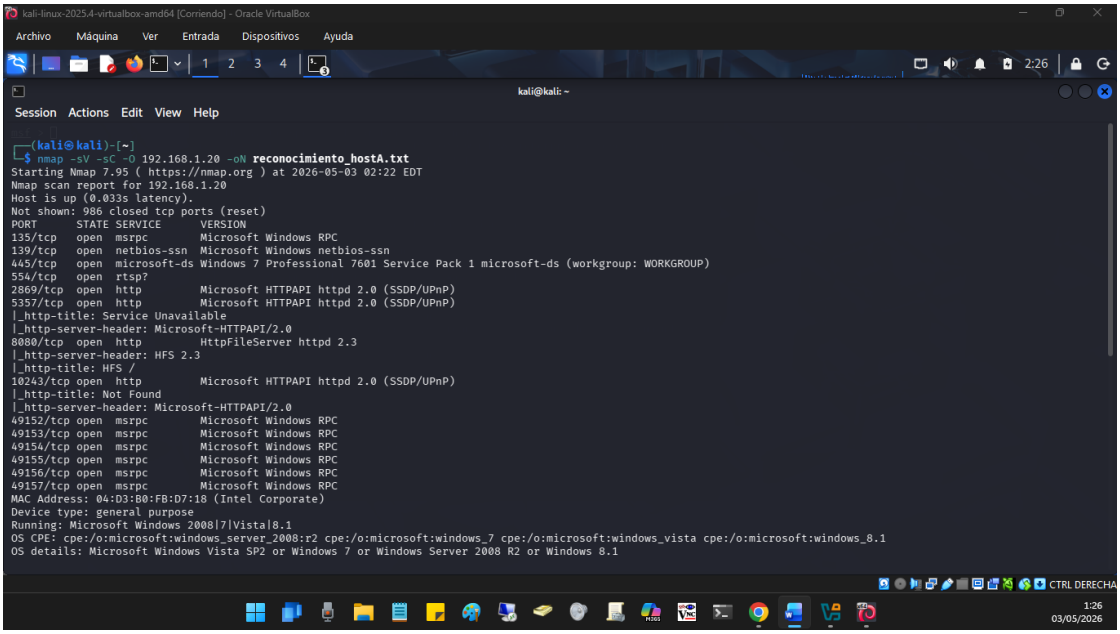
herramientas y procedimientos que serían aplicados en las etapas posteriores del proceso de evaluación de seguridad.

Este resultado evidencia la importancia estratégica de la fase de reconocimiento dentro del ciclo de pruebas de penetración. Una identificación precisa de los servicios, versiones y configuraciones presentes en el sistema objetivo incrementa significativamente la efectividad de las etapas subsiguientes, tales como la identificación de vulnerabilidades, la explotación controlada y la evaluación del impacto. Por el contrario, una fase de reconocimiento incompleta o incorrecta puede conducir a conclusiones erróneas, pérdida de tiempo y omisión de posibles vectores de ataque.

En consecuencia, el reconocimiento constituye uno de los pilares fundamentales de cualquier metodología de pruebas de penetración, ya que la calidad y precisión de la información recopilada durante esta etapa condiciona directamente el éxito de las fases posteriores del proceso de auditoría y evaluación de la seguridad informática.

Figura 2

Reconocimiento del host-A



Nota. Resultado del escaneo realizado con la herramienta nmap

Análisis y Validación de Vulnerabilidades

Con el propósito de validar los hallazgos obtenidos durante la fase de reconocimiento y enumeración, se empleó Metasploit Framework v6.4 como plataforma de verificación controlada de vulnerabilidades. La utilización de esta herramienta permitió confirmar la presencia de la vulnerabilidad CVE-2014-6287 en el servicio Rejetto HTTP File Server (HFS) versión 2.3, instalado en el Host-A (ver Figura 3).

Esta vulnerabilidad posee una puntuación de 9.8 sobre 10 en la escala CVSS v3, siendo catalogada como Crítica debido a su elevado impacto sobre la confidencialidad, integridad y disponibilidad del sistema afectado. La falla se origina en un mecanismo de validación insuficiente dentro de la funcionalidad de búsqueda del servidor web, permitiendo a un atacante remoto enviar solicitudes especialmente manipuladas que derivan en la ejecución arbitraria de comandos del sistema operativo con los privilegios del proceso del servidor. Una característica particularmente relevante de esta vulnerabilidad es que no requiere autenticación previa, lo que reduce significativamente la complejidad del ataque y amplía la superficie de exposición del servicio (NVD, s. f. a).

La fase de validación se desarrolló siguiendo principios de ética profesional y metodologías de pruebas de penetración controladas. Antes de ejecutar cualquier intento de explotación, se verificó la presencia del servicio vulnerable mediante técnicas de enumeración y análisis de versiones. Este enfoque resulta fundamental dentro de los procesos de seguridad ofensiva, ya que evita la ejecución innecesaria de código potencialmente disruptivo y minimiza el riesgo de afectar la estabilidad de los sistemas evaluados. Asimismo, la validación previa garantiza que los hallazgos incluidos en el informe final correspondan a vulnerabilidades efectivamente comprobadas y no a simples indicios o falsos positivos.

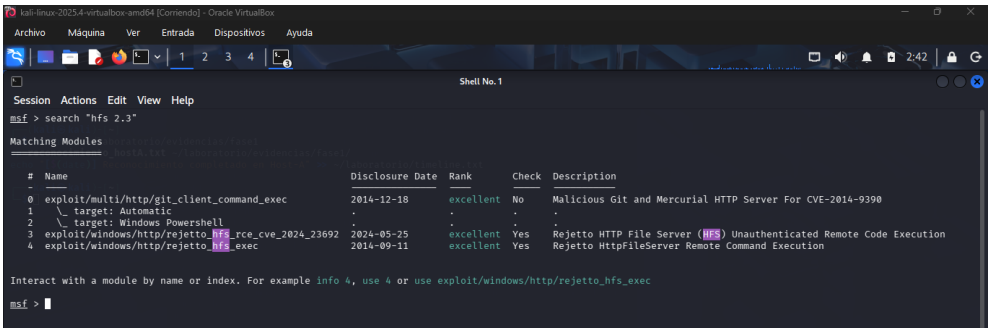
Adicionalmente, durante la etapa de exploración de puertos y servicios se identificó el puerto TCP 445 abierto tanto en el Host-A como en el Host-B. Este puerto se encuentra asociado al protocolo Server Message Block (SMB), ampliamente utilizado en sistemas Microsoft Windows para compartir archivos, impresoras y otros recursos de red. La presencia de este servicio, junto con las características del sistema operativo identificado, sugirió la posible existencia de la vulnerabilidad MS17-010, relacionada con la implementación del protocolo SMBv1.

La vulnerabilidad MS17-010, posteriormente registrada como una de las más críticas en entornos Windows, fue explotada por el malware WannaCry y otros códigos maliciosos de alcance global. Esta debilidad permite la ejecución remota de código mediante el envío de paquetes SMB especialmente diseñados, afectando principalmente sistemas Windows que no cuentan con los parches de seguridad correspondientes (NVD, s. f. b). La validación realizada mediante módulos específicos de Metasploit confirmó la presencia de esta vulnerabilidad en los sistemas analizados, constituyendo un hallazgo de alto impacto debido a las posibilidades de compromiso total del equipo afectado.

La confirmación de ambas vulnerabilidades evidenció la existencia de servicios expuestos y configuraciones inseguras dentro del entorno evaluado. Asimismo, los resultados obtenidos permitieron establecer una base técnica sólida para la fase posterior de explotación controlada, orientada a demostrar el impacto real de las vulnerabilidades identificadas y a formular recomendaciones de mitigación acordes con el nivel de riesgo detectado.

Figura 3

Escaneo de vulnerabilidades del Host-A



Nota. Vulnerabilidad encontrada luego de la ejecución de búsqueda

Explotación, Escalamiento de Privilegios y Movimiento Lateral

Una vez confirmada la vulnerabilidad CVE-2014-6287 en el servicio Rejetto HTTP File Server (HFS) 2.3, se procedió a la fase de explotación controlada utilizando el módulo exploit/windows/http/rejetto_hfs_exec de Metasploit Framework. La ejecución del módulo permitió establecer exitosamente una sesión Meterpreter sobre el Host-A, tal como se observa en la Figura 4. Esta sesión proporcionó un canal de comunicación interactivo entre el sistema comprometido y el equipo atacante, permitiendo la ejecución remota de comandos, la obtención de información del sistema y la administración del host afectado.

Meterpreter constituye una de las cargas útiles más avanzadas de Metasploit debido a que opera principalmente en memoria, lo que reduce la huella en disco y dificulta su detección por soluciones de seguridad tradicionales (Kennedy et al., 2011). A través de esta sesión es posible recopilar información del sistema, ejecutar comandos y realizar actividades de post-explotación, incluyendo enumeración de privilegios y persistencia.

Figura 4

Conexión establecida con el Host-A

Nota. Ejecución comando de explotación y sesión generada

Posteriormente, se ejecutó el comando getsystem, mecanismo diseñado para obtener privilegios elevados mediante diversas técnicas integradas en Meterpreter. Como resultado, se alcanzó el contexto de seguridad NT AUTHORITY\SYSTEM, tal como se muestra en la Figura 5. Este nivel de privilegio representa la máxima autoridad disponible en sistemas operativos Windows y supera incluso los privilegios de un usuario administrador convencional (Microsoft, s. f.).

Este nivel de privilegio otorga control total sobre el sistema operativo, permitiendo realizar acciones como:

- Acceder, modificar o eliminar cualquier archivo del sistema.
- Instalar o eliminar servicios del sistema operativo.
- Alterar configuraciones de seguridad y políticas locales.
- Manipular cuentas de usuario y privilegios.
- Desactivar mecanismos de protección o monitoreo.
- Extraer credenciales almacenadas en memoria o el sistema.
- Ejecutar aplicaciones con privilegios absolutos.

Desde la perspectiva de la ciberseguridad ofensiva, el escalamiento de privilegios constituye una etapa crítica dentro del modelo de ataque, ya que permite transformar un acceso inicial limitado en un compromiso total del sistema (MITRE, 2024). Este proceso es una fase común dentro del marco ATT&CK, específicamente asociado a técnicas de Privilege Escalation (T1068 y otras relacionadas).

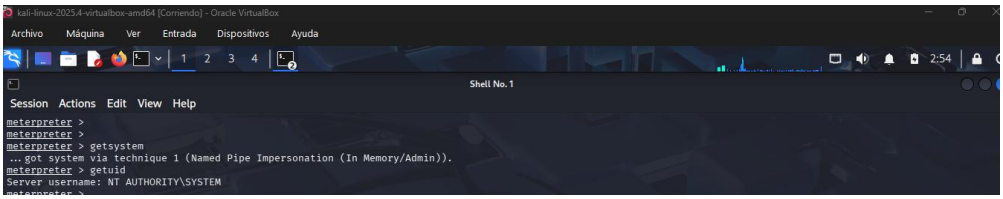
Una vez obtenido el control total del Host-A, se inició la fase de movimiento lateral, cuyo objetivo consiste en utilizar un sistema comprometido como punto de apoyo para acceder a otros equipos dentro de la misma red. Durante las etapas previas de reconocimiento se identificó que tanto Host-A como Host-B tenían habilitado el puerto TCP 445 asociado al protocolo SMB, el cual es frecuentemente utilizado en ataques de propagación lateral (Microsoft Security Response Center, 2017).

El acceso privilegiado sobre Host-A permitió recopilar información de la red interna, identificar servicios accesibles y verificar la presencia de vulnerabilidades adicionales en otros sistemas. La existencia de la vulnerabilidad MS17-010 en Host-B permitió la propagación del compromiso hacia este segundo equipo, una técnica ampliamente documentada en ataques reales como WannaCry y otras campañas basadas en EternalBlue (CVE, 2017).

Este comportamiento refleja uno de los principales riesgos de las redes corporativas modernas: la capacidad de un atacante para desplazarse lateralmente entre equipos comprometidos hasta alcanzar activos de mayor valor. Informes de seguridad han demostrado que muchas intrusiones avanzadas utilizan movimiento lateral para expandir el impacto del ataque una vez obtenido el acceso inicial (MITRE, 2024).

Figura 5

Obtención de privilegios



Nota. Escalamiento de privilegios comando getsystem

Desde Host-A comprometido, mediante la explotación de la vulnerabilidad CVE-2014-6287 y alcanzados privilegios elevados sobre el sistema, se procedió a implementar una técnica de pivoting con el propósito de acceder a segmentos de red que inicialmente no eran alcanzables desde la máquina atacante. Como se observa en la Figura 6, desde la sesión Meterpreter establecida en Host-A se configuró una ruta mediante el módulo autoroute, permitiendo que el sistema comprometido actuara como un intermediario entre el atacante y la red interna donde se encontraba Host-B (192.168.1.21).

El pivoting constituye una de las técnicas de post-explotación más relevantes dentro de las operaciones de ciberseguridad ofensiva y pruebas de penetración avanzadas. Su objetivo consiste en utilizar un sistema previamente comprometido como punto de tránsito hacia otros equipos o segmentos de red que se encuentran protegidos por mecanismos de aislamiento, segmentación o restricciones de acceso. De esta manera, el atacante puede ampliar el alcance de la intrusión más allá del sistema inicialmente comprometido (Kennedy et al., 2011).

La ejecución del comando route add 192.168.1.0/24 2, permitió asociar la red 192.168.1.0/24 a la sesión número 2 de Meterpreter, correspondiente al acceso obtenido sobre Host-A. Posteriormente, la verificación mediante el comando route print confirmó la correcta incorporación de la ruta dentro de la tabla de enrutamiento de Metasploit.

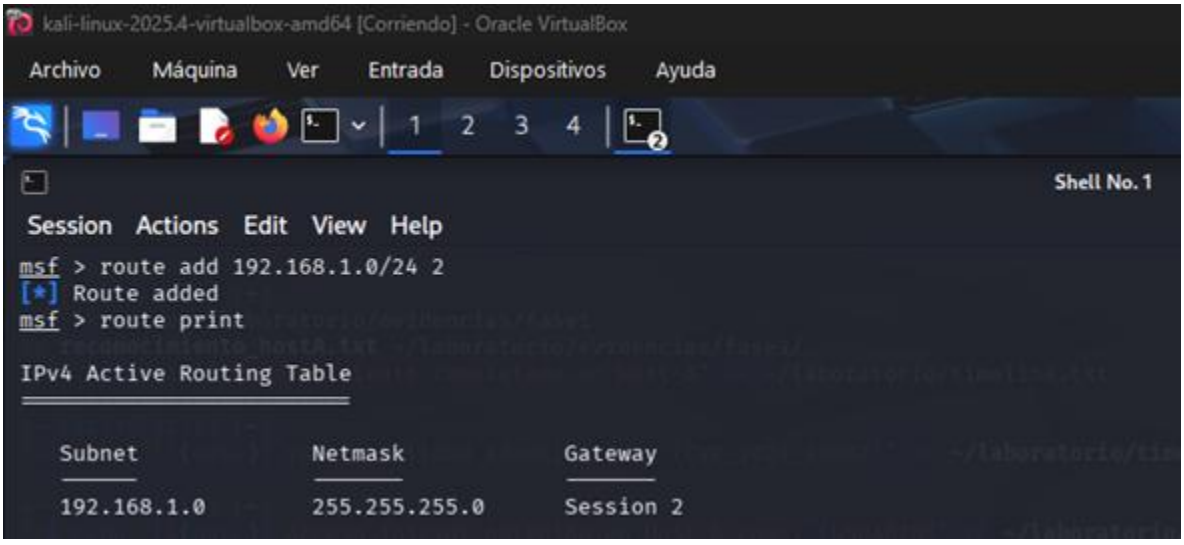
Como resultado, cualquier módulo de explotación, escaneo o enumeración ejecutado desde Metasploit pudo enviar tráfico hacia la red interna utilizando Host-A como punto de salto. Este comportamiento es equivalente al funcionamiento de un proxy o gateway comprometido, permitiendo extender la superficie de ataque hacia sistemas que originalmente no eran visibles para el atacante.

La Figura 6 muestra la configuración de la ruta de pivoting y la tabla de enrutamiento generada dentro de Metasploit.

Desde la perspectiva de la seguridad ofensiva, el pivoting representa una fase crítica del movimiento lateral, ya que permite a un atacante atravesar los límites de segmentación de red y comprometer sistemas adicionales. Según el marco ATT&CK de MITRE, estas actividades se encuentran relacionadas con las técnicas de Proxy (T1090) y Lateral Tool Transfer (T1570), utilizadas frecuentemente por grupos de amenazas avanzadas para expandir su presencia dentro de una organización (MITRE, 2025).

Figura 6

Ruta pivoting



Nota. Configuración ruta pivoting hacia la ruta del Host-B

Tras establecer exitosamente la ruta de pivoting a través de Host-A, se procedió a realizar actividades de reconocimiento sobre Host-B con el propósito de identificar los servicios accesibles y evaluar posibles vectores de ataque. El reconocimiento interno constituye una fase fundamental dentro del movimiento lateral, ya que permite al atacante determinar qué sistemas son alcanzables desde el equipo comprometido y cuáles presentan condiciones susceptibles de explotación (MITRE ATT&CK, 2025).

Como se observa en la Figura 7, se utilizó el módulo auxiliary/scanner/portscan/tcp de Metasploit para efectuar un escaneo de puertos sobre la dirección IP 192.168.1.21 correspondiente a Host-B. La ejecución del escaneo a través del canal de pivoting permitió enviar tráfico desde la sesión comprometida en Host-A hacia el segundo sistema, simulando el comportamiento de un atacante que opera desde una posición interna dentro de la red. Este tipo de técnicas son ampliamente utilizadas durante las pruebas de penetración y las operaciones de postexplotación, ya que permiten extender el alcance del atacante hacia segmentos de red inicialmente inaccesibles (Kennedy et al., 2011).

Los resultados del reconocimiento evidenciaron la presencia de varios puertos abiertos, entre ellos los puertos TCP 135, 139 y 445. El puerto 135 corresponde al servicio RPC (Remote Procedure Call), mientras que los puertos 139 y 445 se encuentran asociados al protocolo Server Message Block (SMB), ampliamente utilizado en sistemas Windows para compartir archivos, impresoras y recursos de red. Históricamente, estos servicios han constituido un objetivo frecuente de ataques debido a las numerosas vulnerabilidades descubiertas en distintas implementaciones del protocolo SMB (Stallings y Brown, 2018).

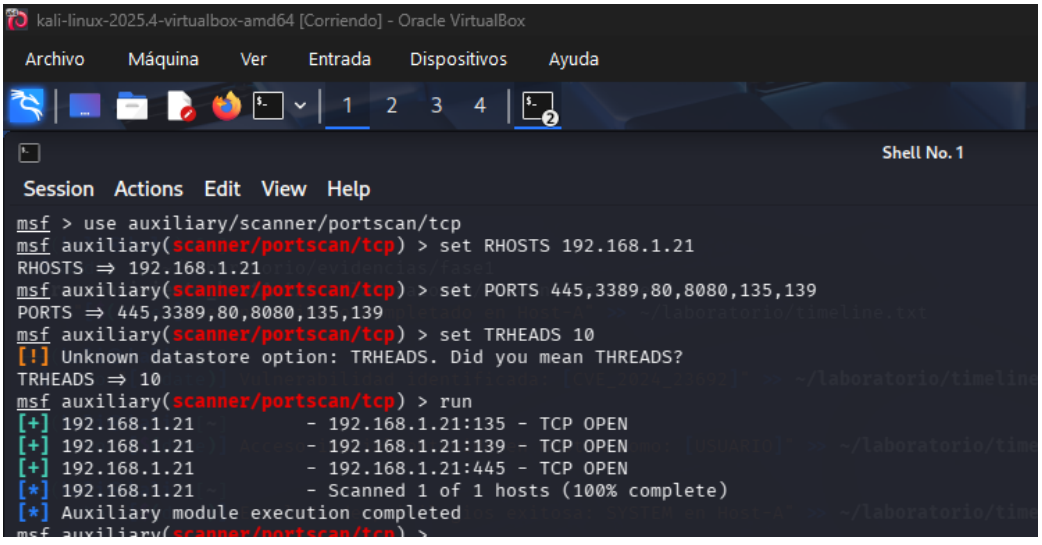
La exposición del puerto TCP 445 resultó particularmente relevante, dado que este servicio constituye el principal vector de explotación de la vulnerabilidad MS17-010. Esta vulnerabilidad, corregida por Microsoft en marzo de 2017, afecta al protocolo SMBv1 y permite

la ejecución remota de código sin autenticación mediante el envío de paquetes especialmente diseñados al servicio vulnerable. La gravedad de esta vulnerabilidad radica en que un atacante puede comprometer completamente un sistema remoto sin necesidad de credenciales válidas, obteniendo ejecución arbitraria de código con privilegios elevados (Microsoft Security Response Center, 2017). Asimismo, el National Vulnerability Database clasifica esta vulnerabilidad como crítica debido a su alto impacto sobre la confidencialidad, integridad y disponibilidad de los sistemas afectados (NIST, 2017).

Una vez confirmada la disponibilidad del servicio SMB, se procedió a utilizar el módulo exploit/windows/smb/ms17_010_eternalblue, el cual implementa la técnica de explotación conocida como EternalBlue. Esta vulnerabilidad fue originalmente desarrollada como una capacidad ofensiva atribuida a la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y posteriormente divulgada públicamente por el grupo Shadow Brokers en 2017, convirtiéndose en uno de los vectores de ataque más relevantes de la última década (Chen y Abu-Nimeh, 2018).

Figura 7

Escaneo de puertos desde pivote

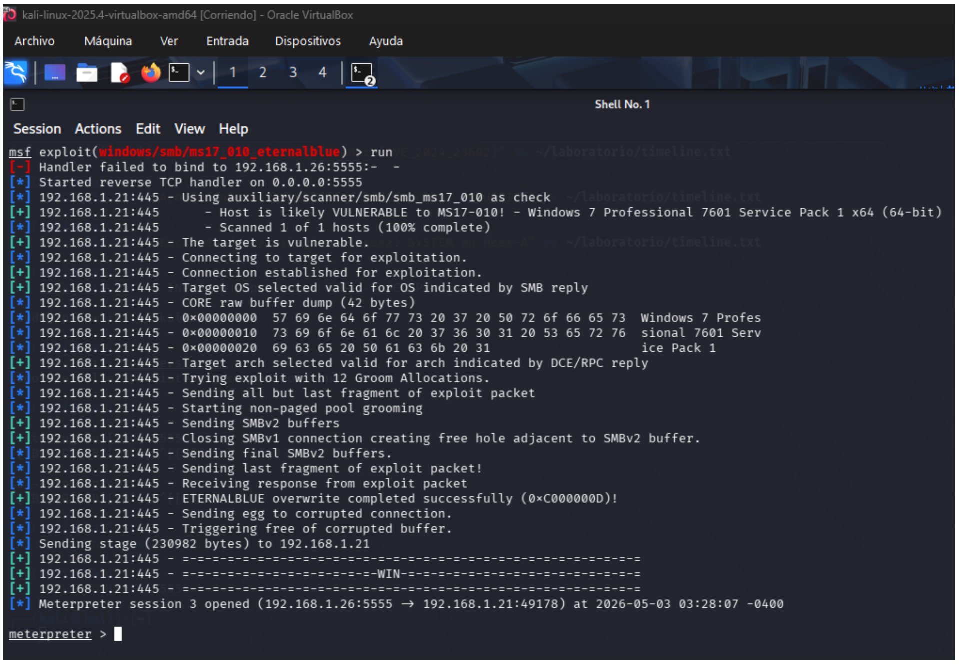


Nota. Escaneo de puertos disponibles en Host-B mediante pivote

La explotación exitosa del servicio vulnerable permitió obtener una sesión Meterpreter sobre Host-B, tal como se evidencia en la Figura 8.

Figura 8

Ejecución exploit MS17-010



Nota. Explotación vulnerabilidad MS17-010 EternalBlue

Posteriormente, la sesión establecida se ejecutó con privilegios NT AUTHORITY\SYSTEM, como se observa en la Figura 9, otorgando control absoluto sobre el segundo sistema comprometido. El contexto SYSTEM representa el nivel máximo de privilegios en sistemas Windows, permitiendo acceder a todos los recursos del equipo, modificar configuraciones críticas, instalar servicios y ejecutar cualquier operación administrativa (Stallings y Brown, 2018).

Desde la perspectiva del modelo de cadena de ataque, este escenario evidencia un encadenamiento completo de técnicas ofensivas que comprende el acceso inicial mediante la explotación de CVE-2014-6287 en Host-A, el escalamiento de privilegios hasta el contexto SYSTEM, la implementación de técnicas de pivoting y movimiento lateral, y finalmente la

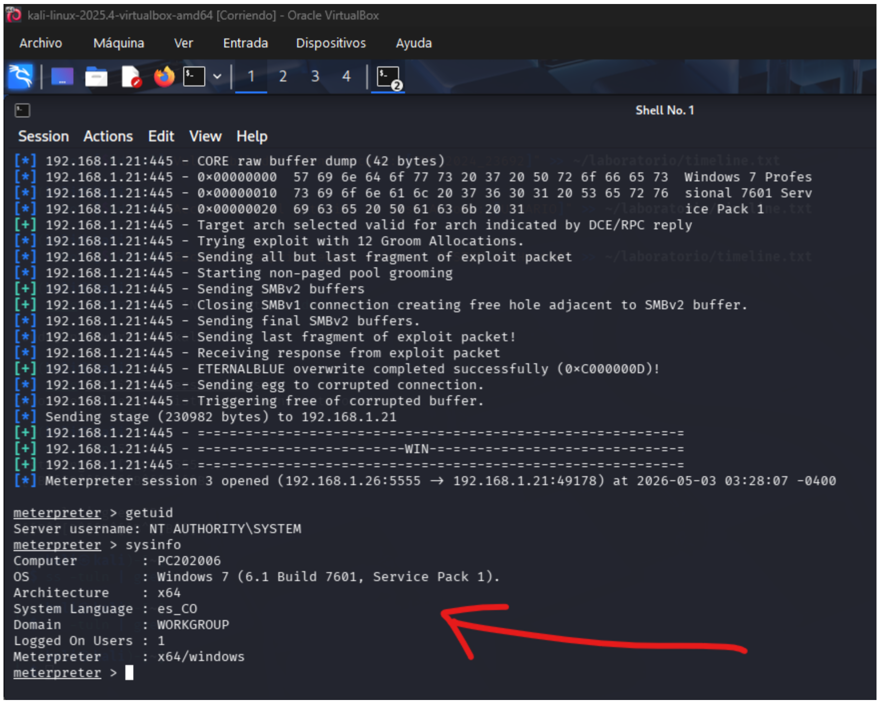
explotación de una segunda vulnerabilidad crítica en Host-B. Este tipo de progresión se encuentra alineado con múltiples tácticas del marco MITRE ATT&CK, incluyendo Initial Access, Privilege Escalation, Discovery, Lateral Movement y Execution (MITRE ATT&CK, 2025).

La secuencia de eventos desarrollada durante el laboratorio demuestra que la seguridad de una infraestructura no depende únicamente de la protección individual de cada equipo, sino de la interacción entre todos los componentes de la red. Un único sistema vulnerable puede convertirse en el punto de entrada para comprometer múltiples activos cuando existen servicios expuestos, sistemas desactualizados y mecanismos de segmentación insuficientes. Este fenómeno ha sido ampliamente documentado en la literatura de seguridad informática, donde se destaca que la ausencia de controles de defensa en profundidad incrementa significativamente la superficie de ataque de las organizaciones (Stallings y Brown, 2018).

Este comportamiento ha sido observado en incidentes reales de gran impacto, como los ataques de ransomware WannaCry y NotPetya, los cuales utilizaron la vulnerabilidad MS17-010 para propagarse automáticamente entre sistemas conectados a la misma red. En ambos casos, la combinación de equipos sin actualizar, protocolos inseguros y ausencia de controles de segmentación permitió una rápida expansión de la intrusión, ocasionando importantes afectaciones operativas y económicas a nivel mundial (Chen y Abu-Nimeh, 2018).

Figura 9

Escalamiento de privilegios en el Host-B



Nota. Escalamiento de privilegios en Host-B mediante sesión Meterpreter.

Prueba de Concepto y Documentación Forense

La Una vez comprometido Host-B mediante la explotación exitosa de la vulnerabilidad MS17-010 y obtenidos privilegios NT AUTHORITY\SYSTEM, se procedió a desarrollar una prueba de concepto (Proof of Concept, PoC) orientada a demostrar el impacto real que tendría un atacante con control total sobre el sistema objetivo. Para ello, se creó la cuenta local WalterGonzalez, la cual posteriormente fue incorporada al grupo de administradores del sistema, tal como se evidencia en la Figura 10.

La creación de cuentas privilegiadas constituye una de las técnicas más utilizadas para establecer mecanismos de persistencia dentro de sistemas comprometidos. El objetivo de esta práctica consiste en garantizar que el atacante pueda recuperar el acceso al equipo incluso después de reinicios, cierres de sesión o eliminación de las sesiones inicialmente comprometidas.

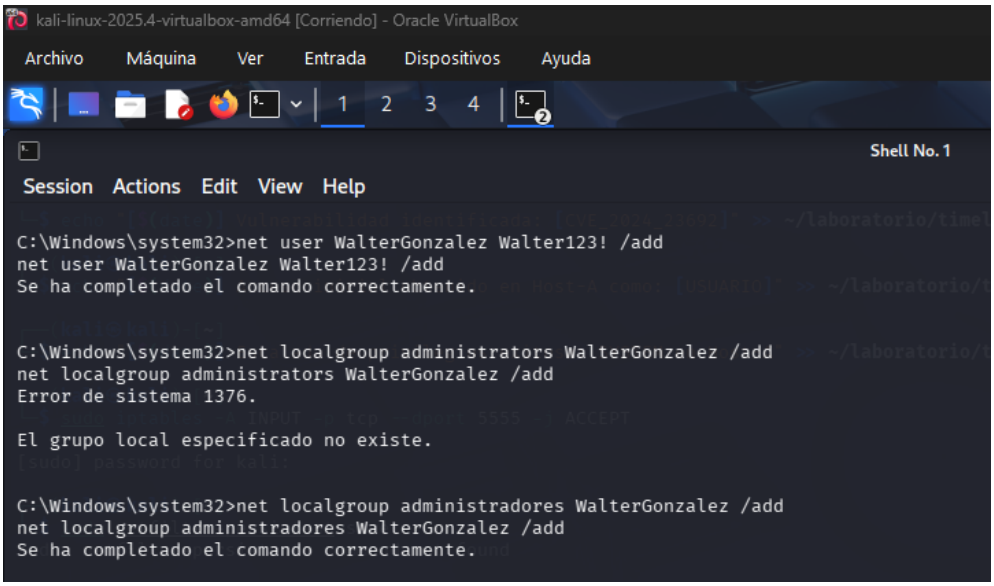
De acuerdo con el marco MITRE ATT&CK, la creación de cuentas locales se encuentra asociada a la técnica Create Account (T1136), mientras que la asignación de privilegios administrativos puede relacionarse con mecanismos de persistencia y escalamiento de privilegios (MITRE, 2025). La ejecución de los comandos: net user WalterGonzalez Walter123! /add y net localgroup administradores WalterGonzalez /add permitió crear un nuevo usuario local y asignarle privilegios administrativos sobre Host-B. Durante el procedimiento se evidenció una diferencia de nomenclatura entre las versiones del sistema operativo en español e inglés, ya que el grupo local "Administrators" no existía bajo dicha denominación. La utilización del grupo "Administradores" permitió completar exitosamente la operación, lo que pone de manifiesto la importancia de considerar la configuración regional del sistema durante las actividades de administración o respuesta a incidentes.

Desde la perspectiva ofensiva, la creación de cuentas administrativas representa una técnica de persistencia altamente efectiva debido a que genera mecanismos legítimos de acceso al sistema. Un atacante que dispone de credenciales válidas puede acceder posteriormente utilizando servicios remotos como SMB, RDP o herramientas administrativas, dificultando en algunos casos la diferenciación entre actividad legítima y actividad maliciosa.

No obstante, dentro del contexto del presente laboratorio, la creación de la cuenta WalterGonzalez tuvo un propósito estrictamente demostrativo y controlado. Su objetivo consistió en evidenciar el nivel de compromiso alcanzado y demostrar que un atacante con privilegios SYSTEM podría establecer mecanismos permanentes de acceso sobre el sistema comprometido.

Figura 10

Creación cuenta WalterGonzalez



Nota. Creación cuenta con privilegios de administrador

Además de la demostración técnica, esta actividad cumplió una segunda función fundamental: la generación de evidencia digital verificable. Todas las acciones ejecutadas fueron documentadas mediante capturas de pantalla, registros de consola, evidencia del Visor de Eventos de Windows y la construcción de una línea temporal forense.

La documentación cronológica de los eventos permite reconstruir la secuencia completa del incidente, identificar las etapas del ataque y establecer relaciones entre las diferentes evidencias recolectadas. La Norma ISO/IEC 27037 destaca la importancia de preservar, identificar y documentar adecuadamente la evidencia digital con el fin de garantizar su integridad y trazabilidad durante los procesos de análisis forense.

La Tabla 1 presenta la línea temporal forense construida durante el laboratorio.

Tabla 1

Timeline Forense

Fecha/Hora	Acción
Sun May 3 02:27:24 AM EDT 2026	Reconocimiento completado en Host-A
Sun May 3 02:43:46 AM EDT 2026	Vulnerabilidad identificada: [CVE_2014_6287]
Sun May 3 02:53:02 AM EDT 2026	Acceso inicial obtenido en Host-A como: [USUARIO]
Sun May 3 02:56:22 AM EDT 2026	Escalada de privilegios exitosa: SYSTEM en Host-A
Sun May 3 03:42:02 AM EDT 2026	PIVOTING: Acceso obtenido en Host-B (192.168.1.21) desde Host-A
Sun May 3 03:42:02 AM EDT 2026	POC: Cuenta WalterGonzalez creada en grupo Administradores de Host-B

Nota. Timeline detallada del proceso de ataque

La elaboración del timeline constituye una práctica esencial dentro del análisis forense digital, ya que permite reconstruir la secuencia temporal de un incidente, correlacionar eventos y establecer la relación entre las acciones del atacante y los artefactos generados en los sistemas comprometidos. La información temporal obtenida puede ser posteriormente utilizada en procesos de respuesta a incidentes, auditorías de seguridad o investigaciones forenses.

Los resultados obtenidos demuestran que un atacante con acceso privilegiado puede establecer mecanismos de persistencia relativamente simples, pero altamente efectivos. Asimismo, evidencian la importancia de implementar controles de monitoreo, auditoría de cuentas privilegiadas y revisión periódica de grupos administrativos como medidas de detección y mitigación frente a este tipo de amenazas.

Finalmente, la combinación de evidencia técnica, registros del sistema, cronología forense y documentación visual proporciona un conjunto de evidencias robustas que permiten sustentar objetivamente los hallazgos del laboratorio y justificar la necesidad de implementar medidas de remediación sobre los sistemas evaluados.

Estrategias de Blue Team

La respuesta defensiva formulada en la Etapa 4 establece un enfoque estructurado en tres niveles: detección en tiempo real, contención inmediata y hardenización preventiva. Este enfoque refleja la naturaleza operacional continua del Blue Team, que no actúa únicamente en respuesta a incidentes confirmados, sino que opera permanentemente para elevar la postura de seguridad de la organización (Nelson et al., 2025).

Los equipos Blue Team desempeñan un papel fundamental dentro de las estrategias actuales de ciberdefensa, ya que son responsables de proteger la infraestructura tecnológica, detectar actividades maliciosas, responder a incidentes y fortalecer los controles de seguridad con el fin de reducir la superficie de ataque. A diferencia de los ejercicios ofensivos desarrollados por los equipos Red Team, cuyo objetivo consiste en identificar vulnerabilidades mediante la simulación de ataques, el Blue Team se enfoca en la prevención, detección, análisis y mitigación de amenazas reales o simuladas (NIST, 2018). Esta función defensiva resulta esencial para garantizar la continuidad operativa y la resiliencia de las organizaciones frente a un panorama de amenazas cada vez más complejo.

La evolución de las amenazas cibernéticas ha llevado a las organizaciones a adoptar modelos de defensa basados en la vigilancia continua y la capacidad de respuesta temprana. En este contexto, la efectividad de un programa de seguridad no depende únicamente de la implementación de controles preventivos, sino también de la capacidad para detectar comportamientos anómalos, contener rápidamente un incidente y recuperar las operaciones afectadas. El NIST Cybersecurity Framework establece cinco funciones fundamentales, identificar, proteger, detectar, responder y recuperar, que permiten desarrollar capacidades integradas de ciberseguridad orientadas a la gestión del riesgo (NIST, 2018). De manera complementaria, los controles del Center for Internet Security (CIS) promueven la

implementación de medidas técnicas y organizacionales destinadas a fortalecer la postura de seguridad institucional (CIS, 2021).

La detección en tiempo real constituye el primer nivel de la estrategia defensiva. Su objetivo consiste en identificar actividades sospechosas antes de que el atacante alcance sus objetivos o amplíe el alcance de la intrusión. Para ello, se emplean mecanismos de monitoreo continuo, análisis de registros, correlación de eventos, sistemas de detección de intrusiones (IDS) y plataformas de gestión de eventos e información de seguridad (SIEM). La identificación temprana de indicadores de compromiso permite reducir significativamente el tiempo de permanencia del atacante dentro de la infraestructura y minimizar el impacto del incidente. Asimismo, el análisis de eventos y registros constituye una fuente fundamental de evidencia para los procesos de respuesta a incidentes y análisis forense.

El segundo nivel corresponde a la contención inmediata, cuya finalidad es impedir la propagación del ataque y limitar el daño sobre los activos comprometidos. Las acciones de contención pueden incluir el aislamiento de equipos afectados, el bloqueo de direcciones IP maliciosas, la deshabilitación de cuentas comprometidas, la revocación de credenciales y la aplicación de controles temporales de acceso. La rapidez con la que se implementan estas medidas influye directamente en la capacidad de la organización para minimizar las consecuencias operativas del incidente y evitar movimientos laterales dentro de la red. Según las recomendaciones del NIST, la contención constituye una de las fases críticas del manejo de incidentes, ya que permite preservar la disponibilidad de los servicios y reducir el alcance del compromiso.

La hardenización preventiva o fortalecimiento de la infraestructura representa el componente estratégico de largo plazo. Esta fase busca eliminar las causas que permitieron la intrusión mediante la aplicación de parches de seguridad, la desactivación de servicios

innecesarios, la implementación del principio de mínimo privilegio, la segmentación de redes, el endurecimiento de configuraciones y la adopción de políticas de seguridad más robustas. El objetivo no consiste únicamente en corregir la vulnerabilidad explotada, sino también en reducir la probabilidad de futuros compromisos y aumentar la resiliencia de la infraestructura tecnológica (CIS, 2021). La aplicación de medidas de hardening permite disminuir la superficie de ataque y fortalecer los mecanismos de protección frente a amenazas conocidas y emergentes.

Los resultados obtenidos durante las etapas ofensivas del laboratorio evidenciaron cómo la combinación de servicios vulnerables, sistemas desactualizados y ausencia de segmentación permitió el compromiso progresivo de múltiples equipos. En consecuencia, las estrategias Blue Team propuestas buscan interrumpir la cadena de ataque en diferentes fases, incrementando la capacidad de detección y reduciendo las posibilidades de escalamiento de privilegios, movimiento lateral y persistencia. Este enfoque se encuentra alineado con los principios de defensa en profundidad, los cuales establecen la necesidad de implementar múltiples capas de seguridad para dificultar el avance de un atacante dentro de la infraestructura (NIST, 2018).

Detección en Tiempo Real y Respuesta Inicial

Ante un ataque activo como el identificado durante la Etapa 3, la respuesta del Blue Team debe orientarse a reducir el tiempo de permanencia del atacante dentro de la infraestructura y limitar el impacto operativo del incidente. La fase inicial de respuesta se centra en la detección temprana de indicadores de compromiso, la identificación del alcance del ataque y la recolección de evidencia que permita comprender la secuencia de eventos ocurridos. Según las recomendaciones del NIST, las primeras acciones de respuesta deben priorizar la identificación, análisis y contención del incidente con el fin de preservar la disponibilidad de los sistemas y evitar la propagación del compromiso.

En el escenario desarrollado durante la Etapa 3, el atacante logró obtener acceso inicial a Host-A, escalar privilegios hasta el contexto NT AUTHORITY\SYSTEM, realizar técnicas de pivoting y comprometer posteriormente Host-B mediante la explotación de la vulnerabilidad MS17-010. Ante una situación de estas características, el protocolo Blue Team comienza con la ejecución de procedimientos de diagnóstico orientados a determinar la presencia de actividad maliciosa y establecer el alcance del incidente.

Entre las primeras acciones de respuesta se encuentran los comandos nativos del sistema operativo Windows, los cuales proporcionan información valiosa sobre conexiones de red, procesos activos, cuentas de usuario y privilegios locales. El comando netstat -anob permite identificar las conexiones de red activas, los puertos abiertos y los procesos responsables de cada conexión. Esta información resulta particularmente útil para detectar sesiones remotas no autorizadas, conexiones persistentes establecidas por herramientas de post-explotación o comunicaciones con sistemas externos controlados por el atacante.

De forma complementaria, el comando tasklist /v proporciona información detallada acerca de los procesos en ejecución, el consumo de recursos y las sesiones asociadas. El análisis de procesos anómalos, procesos ejecutados bajo cuentas privilegiadas o aplicaciones no autorizadas puede revelar la presencia de malware, herramientas de administración remota o cargas útiles utilizadas durante la fase de post-explotación. En escenarios donde se emplean herramientas como Meterpreter, la inspección de procesos constituye una actividad fundamental para identificar comportamientos sospechosos en memoria.

Asimismo, los comandos net user y net localgroup administrators, permiten identificar cuentas locales existentes y verificar la pertenencia a grupos privilegiados. En el contexto del laboratorio, estos comandos habrían permitido detectar la creación de la cuenta WalterGonzalez y su incorporación al grupo de administradores locales de Host-B. La aparición de cuentas no

autorizadas representa un indicador claro de compromiso y puede evidenciar la implementación de mecanismos de persistencia por parte del atacante.

La recopilación de esta información constituye una fuente importante de indicadores de compromiso (Indicators of Compromise, IoC), entendidos como evidencias observables que permiten identificar actividades maliciosas dentro de una infraestructura. Direcciones IP sospechosas, cuentas desconocidas, procesos anómalos y conexiones de red inusuales son ejemplos de artefactos que facilitan la detección y el análisis de incidentes.

Sin embargo, el análisis manual de los sistemas comprometidos debe complementarse con la revisión de los registros de auditoría generados por el sistema operativo. El Visor de Eventos de Windows constituye una de las principales fuentes de evidencia durante un proceso de respuesta a incidentes, ya que almacena información relacionada con autenticaciones, privilegios, modificaciones del sistema y actividades administrativas.

El análisis de los registros debe enfocarse en aquellos eventos que presentan mayor relevancia para el escenario identificado. La Tabla 2 resume los principales Event ID asociados con las actividades observadas durante la fase ofensiva.

Tabla 2

Eventos críticos visor de eventos

Event ID	Significado	Relevancia en el escenario
4624	Inicio de sesión exitoso	Detectar sesiones no autorizadas vía Meterpreter
4625	Intento de inicio de sesión fallido	Identificar ataques de fuerza bruta
4720	Cuenta de usuario creada	Detectar creación de WalterGonzalez en Host-B
4732	Usuario agregado a grupo de administradores	Detectar escalamiento de privilegios post-compromiso
7045	Nuevo servicio instalado	Detectar instalación de backdoors o servicios maliciosos

Nota. Detalle de registros relevantes del visor de eventos

El Event ID 4624 resulta especialmente relevante debido a que registra los inicios de sesión exitosos. La correlación de horarios, tipos de autenticación y cuentas utilizadas puede revelar accesos anómalos o sesiones establecidas por herramientas de administración remota. Por su parte, el Event ID 4720 documenta la creación de nuevas cuentas locales, mientras que el Event ID 4732 evidencia la incorporación de usuarios a grupos privilegiados, actividades que pueden indicar la existencia de mecanismos de persistencia.

El Event ID 7045 también posee un alto valor forense, ya que registra la instalación de nuevos servicios en el sistema. Diversas familias de malware y herramientas de acceso remoto utilizan servicios de Windows para mantener persistencia, ejecutar código automáticamente y evadir ciertos mecanismos de detección.

La verdadera capacidad defensiva surge cuando estos eventos son centralizados y correlacionados mediante plataformas de gestión de eventos e información de seguridad (SIEM). Los sistemas SIEM permiten consolidar registros provenientes de múltiples equipos, identificar patrones de comportamiento y generar alertas automáticas ante eventos sospechosos. Según Chuvakin et al. (2013), la correlación de eventos constituye uno de los mecanismos más efectivos para transformar grandes volúmenes de registros en información útil para la detección de incidentes.

La integración de eventos de autenticación, creación de cuentas, modificaciones de privilegios y actividad de red permite reconstruir el timeline del ataque con un alto grado de precisión. Este proceso facilita la identificación de la secuencia de compromiso, la determinación del alcance del incidente y la preservación de evidencia para posteriores actividades forenses.

Desde la perspectiva del análisis forense digital, la construcción de una línea temporal constituye una actividad fundamental, ya que permite correlacionar eventos del sistema, acciones del atacante y evidencias obtenidas durante la investigación. La norma ISO/IEC 27037 destaca la

importancia de preservar la integridad y trazabilidad de la evidencia digital para garantizar la confiabilidad de los hallazgos.

La detección temprana y la respuesta inicial representan uno de los factores más importantes para limitar el impacto de un incidente. Investigaciones recientes indican que la reducción del tiempo de detección y respuesta disminuye significativamente la capacidad del atacante para realizar movimiento lateral, establecer persistencia o comprometer activos adicionales. En consecuencia, la combinación de monitoreo continuo, análisis de registros, correlación de eventos y procedimientos de respuesta estructurados constituye un componente esencial de las estrategias modernas de Blue Team.

Contención y Preservación de Evidencia

Una vez confirmado el compromiso de un sistema, la respuesta inicial del Blue Team debe orientarse simultáneamente a dos objetivos fundamentales: limitar la propagación del incidente y preservar la evidencia digital necesaria para comprender el alcance del ataque. Estas dos actividades, aunque complementarias, requieren una ejecución cuidadosamente planificada, ya que una acción de contención inapropiada puede destruir información crítica para el análisis forense posterior.

En el escenario desarrollado durante la Etapa 3, la presencia de sesiones Meterpreter operando con privilegios elevados, la creación de cuentas administrativas no autorizadas y la ejecución de técnicas de movimiento lateral evidencian la existencia de un compromiso activo. Ante este tipo de incidentes, el procedimiento de respuesta establece el aislamiento controlado del host comprometido sin realizar un apagado inmediato del sistema.

Esta decisión metodológica resulta especialmente importante debido a la naturaleza de las amenazas modernas. Diversas herramientas de post-explotación, incluyendo Meterpreter, ejecutan gran parte de sus funciones directamente en memoria, minimizando la generación de

archivos en disco y dificultando su detección mediante mecanismos tradicionales de seguridad (Kennedy et al., 2011). Como consecuencia, el apagado del sistema puede provocar la pérdida irreversible de información crítica para la investigación.

La memoria RAM constituye una de las fuentes de evidencia más valiosas durante un incidente de seguridad. En ella pueden encontrarse procesos activos, conexiones de red establecidas, credenciales temporales, sesiones remotas, módulos cargados, inyecciones de código y artefactos asociados a herramientas de post-explotación. Casey (2011) señala que la evidencia volátil puede proporcionar información que no se encuentra disponible en los medios de almacenamiento permanentes, razón por la cual su adquisición debe considerarse una prioridad durante las primeras fases de respuesta.

En el caso específico de Meterpreter, muchas de sus capacidades operan exclusivamente en memoria. Las sesiones activas, los canales de comunicación, las cargas útiles inyectadas y determinadas técnicas de evasión pueden desaparecer completamente una vez que el sistema es reiniciado o apagado. Por este motivo, la preservación de la evidencia volátil resulta esencial para reconstruir la actividad del atacante y determinar el alcance real del compromiso.

Conforme a las recomendaciones del NIST SP 800-61 (Cichonski et al., 2012) y del NIST SP 800-86 (Kent et al., 2006), la secuencia de actuación recomendada frente a un incidente de esta naturaleza comprende las siguientes etapas:

- Captura forense de la memoria RAM.
- Aislamiento del sistema comprometido.
- Preservación del estado del sistema.
- Inicio de la cadena de custodia digital.

La adquisición de la memoria RAM puede realizarse mediante herramientas especializadas como WinPmem o mediante soluciones compatibles con Volatility. Estas herramientas permiten generar imágenes de memoria que posteriormente pueden ser analizadas para identificar procesos ocultos, conexiones de red, módulos cargados, credenciales almacenadas y otros artefactos relevantes. El análisis de memoria se ha convertido en una disciplina fundamental dentro de la informática forense moderna debido a la creciente utilización de malware y herramientas de ataque que operan principalmente en memoria.

Volatility, por ejemplo, permite extraer listas de procesos, identificar conexiones de red activas, recuperar módulos cargados y detectar posibles técnicas de ocultamiento empleadas por el atacante. De igual forma, WinPmem facilita la adquisición forense de la memoria física del sistema preservando la integridad de la evidencia para posteriores análisis.

Una vez obtenida la evidencia volátil, el siguiente paso consiste en el aislamiento del host comprometido. El objetivo de esta fase no es apagar el sistema, sino impedir que continúe interactuando con otros equipos de la red o con la infraestructura del atacante. Las medidas de contención pueden incluir:

- Deshabilitación temporal de interfaces de red.
- Aplicación de reglas de firewall para bloquear comunicaciones.
- Segmentación temporal del sistema afectado.
- Aislamiento mediante soluciones EDR o plataformas de seguridad.
- Revocación de credenciales comprometidas.

El aislamiento de red resulta particularmente importante en escenarios donde el atacante ha realizado técnicas de pivoting o movimiento lateral. En el laboratorio desarrollado, la capacidad de utilizar Host-A como punto de acceso hacia Host-B demuestra cómo un sistema comprometido puede convertirse rápidamente en una plataforma para la propagación del ataque.

La contención temprana reduce la posibilidad de que el adversario continúe desplazándose lateralmente dentro de la infraestructura.

Posteriormente, debe preservarse el estado del sistema comprometido. Esto implica mantener la integridad de los registros, archivos temporales, configuraciones, servicios activos y demás artefactos digitales que puedan resultar relevantes para la investigación. La documentación detallada de las acciones realizadas por el equipo de respuesta constituye un requisito esencial para garantizar la trazabilidad del proceso.

Finalmente, se inicia la cadena de custodia digital, entendida como el conjunto de procedimientos destinados a garantizar la integridad, autenticidad y trazabilidad de la evidencia digital desde su adquisición hasta su análisis y presentación. La norma ISO/IEC 27037 establece que toda evidencia debe ser identificada, recolectada, preservada y documentada mediante procedimientos que aseguren su validez técnica y legal (ISO/IEC, 2012).

La documentación de la cadena de custodia debe incluir información como:

- Fecha y hora de adquisición.
- Identificación del sistema afectado.
- Herramientas utilizadas.
- Personal responsable de la adquisición.
- Valores hash de las evidencias recolectadas.
- Transferencias o accesos posteriores a la evidencia.

Desde la perspectiva del análisis forense, la preservación adecuada de la evidencia permite reconstruir la secuencia del ataque, identificar las técnicas utilizadas por el adversario y determinar el impacto real del incidente. Asimismo, facilita la generación de lecciones aprendidas y el fortalecimiento de los controles de seguridad organizacionales.

Los resultados del laboratorio demuestran que la contención no debe entenderse únicamente como la desconexión de un sistema comprometido. Por el contrario, constituye un proceso estructurado que busca equilibrar la reducción del riesgo operativo con la preservación de la evidencia digital. La captura de memoria, el aislamiento controlado, la preservación del estado del sistema y la adecuada gestión de la cadena de custodia permiten maximizar el valor forense de la evidencia y mejorar la capacidad de respuesta frente a incidentes de seguridad.

En consecuencia, las actividades de contención y preservación de evidencia representan una de las fases más críticas del proceso de respuesta a incidentes, ya que las decisiones tomadas durante las primeras horas del compromiso pueden determinar tanto la eficacia de la investigación forense como la capacidad de la organización para comprender, contener y erradicar la amenaza.

Herramientas de Contención GPL

Las restricciones presupuestales identificadas en el contexto de SecureNova Labs obligan a diseñar una estrategia de ciberdefensa que maximice las capacidades de detección, contención y respuesta sin recurrir a soluciones comerciales de alto costo. Esta situación refleja una realidad común en pequeñas y medianas organizaciones, las cuales frecuentemente enfrentan limitaciones económicas que dificultan la adquisición de plataformas propietarias de seguridad, como soluciones EDR, XDR o SIEM de carácter empresarial. En este escenario, el software libre y de código abierto constituye una alternativa técnicamente viable para implementar capacidades avanzadas de protección y respuesta ante incidentes.

Diversos estudios han demostrado que las herramientas open source pueden ofrecer niveles de funcionalidad comparables a soluciones comerciales cuando son adecuadamente implementadas y administradas (NIST, 2018). Además de reducir costos de licenciamiento, estas

tecnologías proporcionan transparencia, flexibilidad, capacidad de personalización e integración con otros componentes del ecosistema de seguridad.

Considerando las técnicas observadas durante la Etapa 3, explotación remota, escalamiento de privilegios, movimiento lateral y establecimiento de persistencia, la estrategia Blue Team propuesta se fundamenta en la implementación de tres herramientas GPL de alta capacidad: IPTables, Wazuh y CrowdSec. Estas soluciones permiten cubrir diferentes niveles de la defensa en profundidad, proporcionando controles preventivos, mecanismos de detección y capacidades de respuesta automatizada.

IPTables constituye uno de los mecanismos de filtrado de paquetes más robustos disponibles en sistemas Linux. Su funcionamiento a nivel del kernel le permite inspeccionar, aceptar, rechazar o modificar el tráfico de red antes de que este alcance las aplicaciones del sistema. Debido a su integración directa con el subsistema Netfilter del kernel Linux, las reglas implementadas pueden aplicarse con un impacto mínimo sobre el rendimiento del sistema (Purdy, 2004).

Dentro de una estrategia de respuesta a incidentes, IPTables desempeña un papel fundamental en la fase de contención. Una vez identificada una dirección IP maliciosa o una conexión sospechosa, las reglas del firewall pueden bloquear inmediatamente el tráfico entrante o saliente, limitando la capacidad del atacante para mantener el acceso o continuar el movimiento lateral.

En el contexto del laboratorio, un mecanismo de filtrado de este tipo habría permitido bloquear las comunicaciones asociadas a las sesiones Meterpreter o impedir el acceso al servicio SMB vulnerable, reduciendo significativamente las posibilidades de explotación y propagación.

Asimismo, los principios de defensa en profundidad establecen que los controles de red constituyen una de las primeras barreras frente a las amenazas, ya que permiten limitar la exposición de servicios y reducir la superficie de ataque (NIST, 2018).

Wazuh representa el componente central de la estrategia defensiva propuesta. Se trata de una plataforma XDR (Extended Detection and Response) de código abierto diseñada para proporcionar capacidades integradas de monitoreo, análisis de registros, detección de intrusiones, cumplimiento normativo y respuesta automatizada.

La arquitectura de Wazuh se basa en agentes instalados en los sistemas protegidos, los cuales recopilan información relacionada con eventos del sistema operativo, archivos, procesos, autenticaciones y configuraciones de seguridad. Esta información es posteriormente analizada mediante reglas de correlación que permiten identificar comportamientos anómalos o indicadores de compromiso.

La funcionalidad Active Response permite ejecutar acciones automáticas una vez confirmada una amenaza. Estas acciones pueden incluir el bloqueo de direcciones IP, la finalización de procesos, la deshabilitación de cuentas o la ejecución de scripts personalizados. De esta manera, Wazuh reduce considerablemente el tiempo de respuesta ante incidentes y limita la intervención manual del equipo de seguridad (Wazuh, 2024).

La capacidad de correlar múltiples eventos convierte a Wazuh en una herramienta especialmente útil para reconstruir la secuencia de ataque y detectar actividades de movimiento lateral.

CrowdSec incorpora un enfoque innovador basado en la inteligencia colectiva y el análisis del comportamiento. A diferencia de los mecanismos tradicionales basados exclusivamente en firmas, esta plataforma analiza patrones de actividad para identificar comportamientos compatibles con ataques.

Cuando se identifica una amenaza, CrowdSec genera decisiones de bloqueo que son aplicadas por componentes denominados bouncers, los cuales pueden integrarse con firewalls, servidores web, proxies o aplicaciones. Esta capacidad permite responder automáticamente ante actividades maliciosas sin intervención humana.

Uno de los aspectos más relevantes de CrowdSec es su modelo de inteligencia compartida. Las direcciones IP identificadas como maliciosas pueden ser compartidas con otros miembros de la comunidad, generando una base de conocimiento colectiva que incrementa la capacidad de detección global (CrowdSec, 2024).

Este enfoque se alinea con los principios modernos de ciberinteligencia y defensa colaborativa, donde la información obtenida por una organización puede beneficiar a otras entidades que enfrentan amenazas similares.

La selección conjunta de IPTables, Wazuh y CrowdSec permite implementar una arquitectura defensiva multinivel que cubre las principales fases del ciclo de respuesta a incidentes.

- IPTables proporciona capacidades inmediatas de contención a nivel de red.
- Wazuh ofrece monitoreo, correlación de eventos y respuesta automatizada.
- CrowdSec aporta inteligencia colectiva y detección basada en comportamiento.

Esta combinación permite establecer controles preventivos, capacidades de detección temprana y mecanismos de respuesta automatizada sin requerir inversiones significativas en licenciamiento. Asimismo, las tres soluciones poseen una amplia comunidad de desarrollo, documentación técnica y mecanismos de integración que facilitan su adopción en organizaciones con recursos limitados.

Desde la perspectiva de SecureNova Labs, la implementación de estas herramientas representa una estrategia costo-efectiva que fortalece la capacidad de detección, reduce los tiempos de respuesta y mejora la resiliencia organizacional frente a amenazas similares a las observadas durante la Etapa 3. En consecuencia, la adopción de soluciones GPL demuestra que las restricciones presupuestales no necesariamente constituyen una barrera para el desarrollo de capacidades avanzadas de ciberdefensa.

Medidas de Hardenización

La fase de hardenización constituye el componente preventivo de la estrategia Blue Team y tiene como objetivo reducir la superficie de ataque, eliminar configuraciones inseguras y fortalecer los controles de seguridad de la infraestructura tecnológica. A diferencia de las acciones de contención, que buscan detener un incidente en curso, las medidas de hardening se orientan a corregir las debilidades que hicieron posible el compromiso inicial, disminuyendo la probabilidad de futuros ataques.

Diversos marcos de referencia, entre ellos el NIST Cybersecurity Framework, los controles del Center for Internet Security (CIS) y las guías de endurecimiento de sistemas de la industria, coinciden en que la reducción de la superficie de ataque constituye uno de los mecanismos más efectivos para mejorar la resiliencia organizacional (NIST, 2018; CIS, 2021). En este sentido, el análisis de las vulnerabilidades explotadas durante la Etapa 3 permitió identificar un conjunto de acciones prioritarias orientadas a mitigar los riesgos detectados y fortalecer la postura de seguridad de SecureNova Labs.

La Tabla 3 resume las principales acciones de hardenización derivadas del ejercicio de Red Team.

Tabla 3

Acciones prioritarias

Vulnerabilidad	Remediación	Riesgo	Prioridad
HFS 2.3 (CVE-2014-6287)	Actualizar o reemplazar HFS; aplicar WAF; deshabilitar si no es esencial	Crítico	Alta
MS17-010 EternalBlue	Instalar parche KB4012212; deshabilitar SMBv1 en todos los sistemas	Crítico	Alta
Ausencia de segmentación	Implementar VLANs y reglas de firewall inter-segmento	Alto	Alta
Sin monitoreo de cuentas	Desplegar SIEM con alertas sobre cambios en grupos administrativos	Alto	Media
Privilegios excesivos	Aplicar principio de mínimo privilegio en servicios y usuarios	Medio	Media
Sin cifrado de datos	Implementar DLP y cifrado en reposo y tránsito (TLS 1.3)	Medio	Media

Nota: Esta tabla contiene las acciones prioritarias para el plan de hardenización. Elaborada por el autor a partir del análisis del caso SecureNova Labs.

Remediación de CVE-2014-6287 en Rejetto HFS

La explotación inicial del laboratorio fue posible debido a la presencia de la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3. Esta vulnerabilidad permite la ejecución remota de comandos mediante la manipulación de solicitudes HTTP especialmente diseñadas, comprometiendo completamente el servidor expuesto.

La medida correctiva prioritaria consiste en la actualización del software hacia versiones no vulnerables o, preferiblemente, en la sustitución del servicio por soluciones que continúen recibiendo soporte y actualizaciones de seguridad. Cuando el servicio no resulta esencial para la operación, su desinstalación o deshabilitación constituye la alternativa más segura.

Adicionalmente, la implementación de un Web Application Firewall (WAF) puede proporcionar una capa adicional de protección mediante la inspección del tráfico HTTP y el

bloqueo de solicitudes maliciosas. Según OWASP, los mecanismos de filtrado de aplicaciones web permiten reducir significativamente la exposición frente a ataques de ejecución remota de código y explotación de aplicaciones vulnerables.

Mitigación de MS17-010 y deshabilitación de SMBv1

La vulnerabilidad MS17-010 representa uno de los ejemplos más significativos de las consecuencias derivadas de la falta de actualización de sistemas operativos. La explotación mediante EternalBlue permitió el compromiso completo de Host-B y demostró la capacidad del atacante para realizar movimiento lateral dentro de la red.

La principal medida correctiva consiste en la instalación del parche de seguridad KB4012212 publicado por Microsoft. Asimismo, Microsoft recomienda la deshabilitación definitiva del protocolo SMBv1 debido a sus múltiples deficiencias de seguridad y su utilización en diversos incidentes de alcance mundial, incluyendo WannaCry y NotPetya (Microsoft, 2017).

La eliminación de protocolos obsoletos constituye una práctica fundamental del hardening, ya que reduce significativamente la exposición frente a vulnerabilidades conocidas.

Segmentación de red y limitación del movimiento lateral

El laboratorio evidenció que la ausencia de segmentación permitió utilizar Host-A como plataforma para comprometer Host-B mediante técnicas de pivoting. Este comportamiento demuestra que una arquitectura de red plana facilita el desplazamiento del atacante entre diferentes sistemas.

La implementación de VLAN, listas de control de acceso y reglas de firewall entre segmentos permite limitar las comunicaciones innecesarias y restringir el movimiento lateral. El principio de segmentación de red establece que los sistemas deben comunicarse únicamente con aquellos recursos estrictamente necesarios para su funcionamiento.

Los modelos modernos de seguridad, incluyendo Zero Trust, recomiendan verificar continuamente las comunicaciones internas y asumir que ningún segmento de la red debe considerarse completamente confiable (Rose et al., 2020).

Monitoreo de cuentas privilegiadas

La creación de la cuenta WalterGonzalez y su incorporación al grupo de administradores evidenció la ausencia de controles sobre las cuentas privilegiadas. Este tipo de actividades suele ser utilizado por los atacantes para establecer persistencia y mantener el acceso al sistema comprometido.

La implementación de plataformas SIEM y sistemas de monitoreo continuo permite generar alertas ante eventos críticos como:

- Creación de usuarios.
- Modificación de grupos administrativos.
- Elevación de privilegios.
- Cambios en políticas de seguridad.
- Inicios de sesión sospechosos.

La supervisión de eventos como los Event ID 4720 y 4732 permite detectar tempranamente actividades asociadas a persistencia o escalamiento de privilegios.

Aplicación del principio de mínimo privilegio

El principio de mínimo privilegio establece que usuarios, aplicaciones y servicios deben disponer únicamente de los permisos estrictamente necesarios para realizar sus funciones. La existencia de cuentas con privilegios excesivos incrementa significativamente el impacto potencial de una intrusión.

La implementación de este principio puede incluir:

- Restricción de privilegios administrativos.
- Separación de cuentas administrativas y operativas.
- Eliminación de cuentas innecesarias.
- Uso de privilegios temporales.
- Auditoría periódica de permisos.

NIST y CIS consideran el mínimo privilegio como uno de los controles fundamentales para limitar el escalamiento de privilegios y reducir la capacidad de movimiento lateral del atacante (CIS, 2021).

Protección de la información mediante cifrado

El análisis realizado también identificó la ausencia de mecanismos robustos de protección de la información. El cifrado de datos constituye un control fundamental para preservar la confidencialidad de la información incluso en escenarios de compromiso parcial de la infraestructura.

Las medidas recomendadas incluyen:

- Cifrado de datos en reposo.
- Cifrado de discos y sistemas de archivos.
- Protección de bases de datos.
- Implementación de TLS 1.3 para comunicaciones.
- Soluciones de Data Loss Prevention (DLP).

TLS 1.3 proporciona mejoras significativas en seguridad y rendimiento respecto a versiones anteriores del protocolo, reduciendo la exposición a diversos ataques criptográficos y fortaleciendo la protección de las comunicaciones (Rescorla, 2018).

Priorización basada en el riesgo

La priorización de las medidas propuestas se fundamenta en el impacto potencial y la probabilidad de explotación de cada vulnerabilidad. Las vulnerabilidades que permitieron el acceso inicial y el movimiento lateral fueron clasificadas como críticas debido a su capacidad para comprometer completamente la infraestructura.

Este enfoque basado en riesgos permite asignar eficientemente los recursos de seguridad, priorizando aquellas acciones que generan una mayor reducción del riesgo organizacional. Según NIST, la gestión del riesgo constituye el fundamento de las estrategias modernas de ciberseguridad, ya que permite orientar los esfuerzos de protección hacia los activos y amenazas de mayor relevancia.

En consecuencia, el plan de hardenización propuesto no debe entenderse únicamente como un conjunto de medidas técnicas aisladas, sino como una estrategia integral de fortalecimiento orientada a reducir la superficie de ataque, limitar las capacidades del adversario y aumentar la resiliencia de la infraestructura frente a futuras amenazas. La implementación progresiva de estas medidas permitirá a SecureNova Labs mejorar significativamente su postura de seguridad y disminuir la probabilidad de incidentes similares a los observados durante el ejercicio de Red Team.

Análisis Técnico de las Etapas 1 a 4

Etapa 1 Fundamentos y Marco Regulatorio

La Etapa 1 establece los cimientos sobre los cuales se sustenta la legalidad de cualquier operación de ciberseguridad en Colombia. Desde una perspectiva crítica, el marco normativo colombiano presenta fortalezas significativas: la Ley 1273 de 2009 tipifica con precisión conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos y la violación de datos personales, proporcionando una base penal sólida para perseguir ciberdelitos

(Congreso de la República de Colombia, 2009). La Ley Estatutaria 1581 de 2012 incorpora principios de protección de datos alineados con estándares internacionales como el GDPR europeo (Congreso de la República de Colombia, 2012), y la reciente Ley 2502 de 2025 refleja la adaptación del ordenamiento jurídico a amenazas emergentes como la suplantación mediante inteligencia artificial (Congreso de la República de Colombia, 2025).

Sin embargo, persisten brechas relevantes: Colombia carece aún de una ley específica de ciberseguridad nacional que establezca obligaciones de notificación de incidentes para entidades críticas, similar al Cybersecurity Information Sharing Act (CISA) estadounidense o la Directiva NIS2 europea. Esta ausencia genera zonas grises en la responsabilidad de las organizaciones frente a incidentes que afecten a terceros. Adicionalmente, la Ley 1273 data de 2009 y no contempla explícitamente fenómenos como ataques de ransomware, cryptojacking o amenazas persistentes avanzadas (APTs), lo que obliga a los fiscales a realizar interpretaciones extensivas de tipos penales existentes.

Desde la perspectiva del pentesting, la definición precisa de las etapas reconocimiento, escaneo, análisis de vulnerabilidades, explotación, post-explotación e informe y la comprensión de las herramientas asociadas a cada una (Maltego, Nmap, Nessus, Metasploit, Wireshark, Burp Suite) no es meramente técnica: es también legal. Ejecutar cualquiera de estas fases sin autorización documentada por escrito constituye un delito tipificado en el Artículo 269A de la Ley 1273 (Congreso de la República de Colombia, 2009).

Etapa 2 Ética Profesional y Marco Normativo

El análisis del acuerdo de confidencialidad de SecureNova Labs constituye un caso de estudio de extraordinaria relevancia pedagógica y práctica. El documento presenta una arquitectura jurídica orientada a proteger actividades ilegales bajo la apariencia de un acuerdo de

confidencialidad legítimo. Identificar esta arquitectura requiere competencia técnica, jurídica y ética simultáneamente.

Las violaciones detectadas revelan un patrón de tres estrategias: equiparación entre actividades ilegales e información confidencial (Cláusula 1 y 2), supresión del deber cívico de denuncia de delitos (Cláusula 4, numerales 3 y 4) y traslado contractual de responsabilidad penal (Cláusula 8). Ninguna de estas estrategias tiene validez jurídica en Colombia: el Artículo 25 del Código Penal establece que la responsabilidad penal es personal e intransferible; el Artículo 441 tipifica la omisión de denuncia como delito; y el Artículo 23 de la Constitución Política reconoce el derecho de petición y denuncia como derecho fundamental.

La decisión de rechazar el contrato, a pesar de la oferta de $15.000.000 COP mensuales y contrato vitalicio, refleja la primacía del criterio ético sobre el incentivo económico. El COPNIA, en su Código de Ética Profesional, establece con claridad que el ingeniero debe actuar conforme a la ley y proteger el bienestar de la sociedad (Ley 842 de 2003). Aceptar el acuerdo habría implicado no solo la complicidad en la ocultación de delitos, sino el riesgo real de responsabilidad penal por hechos ajenos transferidos contractualmente, con consecuencias irreversibles sobre la trayectoria profesional del especialista.

Desde un ángulo crítico, este escenario ilustra una práctica real en el sector privado de seguridad: el uso de cláusulas contractuales para comprometer éticamente a los profesionales antes de que descubran la naturaleza de las operaciones para las que son contratados. La conciencia de este riesgo y la capacidad de identificarlo tempranamente constituyen competencias profesionales tan valiosas como cualquier habilidad técnica.

Etapa 3 Capacidades Técnicas Red Team

La Etapa 3 representa el ejercicio técnico más exigente del seminario y su análisis merece una reflexión que trascienda la descripción de comandos ejecutados. El encadenamiento de

vulnerabilidades que condujo desde el reconocimiento hasta la creación de persistencia en Host-B ilustra tres principios fundamentales de la seguridad ofensiva contemporánea.

Primero, la interdependencia de controles: ninguna vulnerabilidad explotada en este escenario era técnicamente sofisticada o novedosa. CVE-2014-6287 fue publicada en 2014 y MS17-010 en 2017. Ambas tienen parches disponibles desde sus respectivas fechas de publicación. El éxito del ataque no dependió de exploits de día cero ni de técnicas avanzadas de evasión, sino de la simple ausencia de actualizaciones de seguridad. Esto confirma que la mayor superficie de ataque en entornos reales no la constituyen las amenazas emergentes, sino las vulnerabilidades conocidas sin remediar.

Segundo, el efecto amplificador de la ausencia de segmentación: el pivoting desde Host-A hacia Host-B no habría sido posible si existiera segmentación de red con reglas de firewall entre segmentos. Un único punto de compromiso se convirtió en la puerta de entrada hacia un segundo sistema crítico, demostrando que la seguridad perimetral sin defensa en profundidad es fundamentalmente insuficiente.

Tercero, el valor de la documentación forense: la construcción del timeline forense con marcas de tiempo precisas, capturas de pantalla y evidencias de eventos del sistema no es un requisito burocrático adicional. Es la diferencia entre una prueba de penetración que genera valor real y un ejercicio sin impacto. En un entorno profesional, el informe forense es el único producto tangible del trabajo del Red Team y su calidad determina directamente la calidad de las decisiones que tomará la organización auditada.

Etapa 4 Respuesta y Contención Blue Team

La Etapa 4 establece una distinción conceptual frecuentemente ignorada en la práctica: la diferencia entre el equipo Blue Team y el equipo de respuesta a incidentes. El Blue Team opera de manera continua y proactiva, monitoreando, detectando y fortaleciendo controles. El equipo

de respuesta a incidentes (CSIRT/CERT) se activa reactivamente cuando una amenaza se ha materializado, con foco en contención, erradicación, recuperación y comunicación. Ambos son complementarios, pero no intercambiables, y confundirlos genera vacíos operacionales críticos.

La incorporación del framework CIS Controls v8 como referencia de hardenización proporciona al Blue Team una guía estructurada y priorizada. Los controles básicos inventario de activos autorizados, configuración segura de hardware y software, gestión continua de vulnerabilidades habrían prevenido directamente las vulnerabilidades explotadas en la Etapa 3. Esto subraya que la defensa efectiva no requiere herramientas exóticas: requiere disciplina operacional en la implementación consistente de controles fundamentales.

La elección del SIEM como eje central de la estrategia de monitoreo responde a una necesidad real del entorno SecureNova Labs: correlacionar eventos de múltiples fuentes para identificar patrones de ataque que serían invisibles analizando fuentes de forma aislada. La creación de una cuenta administrativa (Event ID 4720) seguida inmediatamente de su adición a un grupo de administradores (Event ID 4732) es un patrón de alta fidelidad para la detección de persistencia; sin un SIEM que correlacione ambos eventos, este comportamiento podría pasar desapercibido.

Relación con Aspectos Legales y Éticos

La intersección entre el ejercicio técnico de la ciberseguridad y el marco legal-ético no es periférica ni complementaria: es constitutiva. Ninguna operación de Red Team o Blue Team puede ser considerada profesional si no opera dentro de límites legales claros y principios éticos sólidos.

Legalidad de las Operaciones de Pentesting

La autorización escrita y previa es el requisito sine qua non de cualquier prueba de penetración. Sin ella, todas las acciones técnicas descritas en la Etapa 3 reconocimiento activo,

escaneo de puertos, explotación de vulnerabilidades constituirían delitos tipificados en los Artículos 269A (acceso abusivo) y 269C (interceptación de datos) de la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009). La frontera entre el experto en ciberseguridad y el criminal informático es, en última instancia, un documento de autorización y el respeto escrupuloso de su alcance.

El entorno virtualizado aislado en el que se realizaron los ejercicios de las Etapas 1 y 3 es una práctica indispensable: asegura que las pruebas no afecten sistemas productivos, terceros no autorizados o redes fuera del alcance definido. La segmentación del laboratorio es tanto una medida técnica como una salvaguarda ética y legal.

Ética en la Divulgación de Vulnerabilidades

El manejo responsable de vulnerabilidades descubiertas conocido como Responsible Disclosure o Coordinated Vulnerability Disclosure (CVD) es un principio ético central en la comunidad de ciberseguridad. Implica notificar al fabricante o propietario del sistema afectado antes de la divulgación pública, otorgando un tiempo razonable para la remediación. Las organizaciones como MITRE, con su sistema CVE, y el NIST, con el NVD, formalizan este proceso proporcionando identificadores estandarizados que facilitan la comunicación y el seguimiento de vulnerabilidades entre fabricantes, investigadores y organizaciones.

Protección de Datos en Operaciones de Seguridad

Las operaciones de Blue Team que implican análisis de logs, captura de tráfico de red y análisis forense de sistemas generan inevitablemente el procesamiento de datos personales de los usuarios de los sistemas evaluados. La Ley Estatutaria 1581 de 2012 exige que este procesamiento sea proporcional, limitado a la finalidad de seguridad establecida y protegido mediante controles técnicos adecuados (Congreso de la República de Colombia, 2012). El principio de mínimo privilegio aplica aquí con igual fuerza que en el contexto técnico: los

analistas de seguridad solo deben acceder a la información estrictamente necesaria para el cumplimiento de sus funciones defensivas.

Responsabilidad Profesional y COPNIA

El Código de Ética Profesional del COPNIA, establecido mediante la Ley 842 de 2003, impone al ingeniero la obligación de velar por la seguridad pública, actuar con honestidad e integridad y rechazar cualquier asignación que implique violación de la ley o de sus principios éticos (Congreso de la República de Colombia [CRC], 2003). En el contexto de la ciberseguridad, esta obligación adquiere dimensiones adicionales: el conocimiento de técnicas de intrusión que posee el profesional lo convierte en un actor con capacidad real de causación de daño, lo que eleva proporcionalmente su responsabilidad ética de utilizarlas exclusivamente dentro de marcos legales y autorizados. La tentación del acuerdo de SecureNova Labs remuneración elevada a cambio de silencio sobre actividades ilegales ilustra exactamente el tipo de situación frente a la cual el Código de Ética busca proteger tanto al profesional como a la sociedad.

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/42Mrw4EFPa8

Conclusiones

El presente trabajo permitió integrar de manera articulada el análisis normativo, la ejecución técnica de un ciclo completo de ataque y la formulación de estrategias defensivas, logrando una visión integral del modelo Red Team/Blue Team aplicado al caso de estudio SecureNova Labs. A continuación, se presentan las conclusiones estructuradas en relación con los objetivos específicos planteados y sustentadas en los marcos normativos y técnicos analizados durante el desarrollo del informe.

El análisis del marco normativo colombiano en materia de ciberseguridad y protección de datos permitió identificar una base jurídica consolidada en la Ley 1273 de 2009, orientada a la tipificación de los delitos informáticos, y en la Ley 1581 de 2012, enfocada en la protección de datos personales. Estas disposiciones constituyen el principal soporte legal para la persecución de conductas relacionadas con el acceso abusivo a sistemas informáticos, la interceptación de datos y la afectación de la información, así como para la regulación del tratamiento de datos personales en las organizaciones (Congreso de Colombia, 2009; Congreso de Colombia, 2012).

No obstante, el estudio evidenció que el marco normativo nacional se encuentra principalmente orientado a la dimensión penal y a la protección de datos, mientras que aspectos relacionados con la gestión integral de incidentes, la notificación obligatoria de eventos de seguridad y la protección de infraestructuras críticas presentan un menor desarrollo normativo. Esta situación contrasta con marcos internacionales como el NIST Cybersecurity Framework, que promueve funciones de identificación, protección, detección, respuesta y recuperación (NIST, 2024), así como con la Directiva NIS2 de la Unión Europea, que establece obligaciones específicas de gestión del riesgo y reporte de incidentes (Unión Europea, 2022).

En este contexto, la Ley 2502 de 2025 representa un avance en la evolución de la política pública de ciberseguridad en Colombia; sin embargo, su implementación y alcance frente a

amenazas emergentes, como el ransomware, las amenazas persistentes avanzadas (APT) y el uso de inteligencia artificial en actividades ofensivas, requerirán procesos de reglamentación y fortalecimiento institucional, tal como lo recomiendan organismos internacionales especializados en ciberseguridad (ENISA, 2023; NIST, 2024).

De otro lado el análisis del acuerdo de confidencialidad de SecureNova Labs permitió concluir que la dimensión ética y jurídica en ciberseguridad no constituye un elemento accesorio, sino un componente esencial de la práctica profesional. El estudio del caso evidenció cómo determinadas cláusulas contractuales pueden generar conflictos cuando se enfrentan a situaciones que comprometen la legalidad, la integridad profesional o los principios éticos de la seguridad informática.

En este contexto, se concluye que la competencia técnica debe estar acompañada de criterios éticos sólidos y del conocimiento del marco legal vigente, ya que las decisiones adoptadas por los profesionales de ciberseguridad pueden generar consecuencias jurídicas, disciplinarias y profesionales. Asimismo, los principios de responsabilidad, diligencia y actuación ética promovidos por organismos internacionales y códigos de conducta profesionales refuerzan la necesidad de rechazar cualquier acuerdo que implique la realización, ocultamiento o facilitación de actividades ilícitas.

De igual manera la documentación del ciclo completo de ataque desarrollado en la Etapa 3 permitió demostrar que vulnerabilidades ampliamente conocidas y corregidas, como CVE-2014-6287 (Rejetto HFS) y MS17-010 (EternalBlue), continúan representando un riesgo significativo en entornos donde no existe una adecuada gestión de parches ni mecanismos efectivos de segmentación de red.

El ejercicio evidenció la ejecución completa de la cadena de ataque, incluyendo reconocimiento, explotación de vulnerabilidades, escalamiento de privilegios, pivoting y compromiso de sistemas internos. Estos resultados coinciden con los hallazgos de MITRE ATT&CK, que identifica el movimiento lateral y la explotación de servicios vulnerables como técnicas recurrentes utilizadas por actores maliciosos (MITRE, 2024). De igual manera, la Agencia de Ciberseguridad e Infraestructura de Estados Unidos (CISA) ha señalado que las vulnerabilidades conocidas y sin corregir continúan siendo una de las principales causas de compromiso de sistemas (CISA, 2023).

Asimismo, la construcción del timeline forense y la documentación de evidencia técnica permitieron validar la trazabilidad del ataque, fortaleciendo la validez metodológica del ejercicio y demostrando la importancia de la documentación técnica y la preservación de evidencias en procesos de análisis forense e investigación de incidentes.

La formulación de estrategias Blue Team permitió establecer un modelo defensivo basado en la detección, la contención y la hardenización de la infraestructura. Este enfoque se encuentra alineado con el NIST Cybersecurity Framework y con los CIS Controls, los cuales promueven una gestión integral de la seguridad mediante controles preventivos, detectivos y correctivos (NIST, 2024; CIS, 2021).

Asimismo, la evaluación de herramientas de código abierto como IPTables, Wazuh y CrowdSec evidenció que las organizaciones pueden implementar capacidades defensivas robustas mediante soluciones GPL, siempre que estas sean adecuadamente configuradas y administradas. Diversos estudios han señalado que la efectividad de las herramientas de seguridad depende en gran medida de la capacitación del personal y de la madurez de los procesos organizacionales (SANS Institute, 2023).

Adicionalmente, se identificó que la ausencia de segmentación de red y de monitoreo centralizado incrementa significativamente la probabilidad de movimiento lateral y escalamiento de ataques. En consecuencia, la implementación de mecanismos SIEM, políticas de mínimo privilegio, segmentación lógica de redes y monitoreo continuo constituye una medida prioritaria para reducir la superficie de ataque y mejorar la capacidad de detección y respuesta (CIS, 2021; NIST, 2024).

La integración de los hallazgos técnicos, normativos y defensivos permite concluir que la postura de seguridad de una organización no depende únicamente de la existencia de controles tecnológicos, sino de la coherencia entre políticas institucionales, arquitectura de red, gestión de vulnerabilidades, capacitación del personal y capacidades de respuesta ante incidentes.

El caso analizado demuestra que la explotación de sistemas desactualizados puede escalar rápidamente hacia compromisos críticos cuando existen debilidades estructurales como la falta de segmentación, la ausencia de monitoreo centralizado y la aplicación insuficiente del principio de mínimo privilegio. Estas conclusiones coinciden con las recomendaciones de organismos internacionales que promueven la gestión continua del riesgo y la mejora permanente de los controles de seguridad (NIST, 2024; ENISA, 2023).

Finalmente, se concluye que la separación funcional entre Blue Team e Incident Response Team constituye un factor organizacional relevante para evitar la sobrecarga operativa y garantizar la efectividad en la gestión de incidentes. La definición clara de roles, responsabilidades y procedimientos contribuye significativamente a mejorar la capacidad de respuesta y recuperación ante eventos de seguridad.

Como conclusión general cabe indicar que el desarrollo del presente informe permitió cumplir satisfactoriamente los objetivos propuestos, integrando el análisis normativo colombiano, la ejecución técnica de un escenario Red Team completo y la formulación de

estrategias defensivas basadas en herramientas de código abierto. Los resultados obtenidos evidencian la importancia de una visión integral de la ciberseguridad, en la cual los aspectos legales, técnicos, éticos y organizacionales deben abordarse de manera conjunta para fortalecer la resiliencia de las infraestructuras tecnológicas frente a las amenazas actuales.

Asimismo, el estudio confirma que la gestión efectiva de la ciberseguridad requiere no solo la implementación de controles tecnológicos, sino también la consolidación de marcos normativos adecuados, la formación ética de los profesionales y la adopción de buenas prácticas internacionales orientadas a la prevención, detección y respuesta ante incidentes. Estas conclusiones constituyen una base para la formulación de recomendaciones estratégicas que contribuyan al fortalecimiento de la postura de seguridad de organizaciones similares a SecureNova Labs.

Recomendaciones

Las recomendaciones formuladas a continuación se derivan de los hallazgos técnicos, normativos y organizacionales obtenidos durante el desarrollo del caso SecureNova Labs. Su propósito consiste en fortalecer la postura de seguridad de la organización mediante la implementación progresiva de controles técnicos, administrativos y operacionales orientados a reducir la probabilidad de incidentes similares a los documentados durante el ejercicio.

Gestión de vulnerabilidades y actualización de sistemas

Los resultados obtenidos durante la fase Red Team demostraron que la explotación exitosa de Host-A y Host-B fue posible debido a la permanencia de vulnerabilidades conocidas y corregidas desde hace varios años. En consecuencia, la implementación de un programa formal de gestión de vulnerabilidades constituye la medida de mayor prioridad para la organización.

Se recomienda aplicar inmediatamente el parche de seguridad KB4012212 en todos los sistemas Windows afectados por MS17-010 y deshabilitar el protocolo SMBv1 mediante políticas de grupo corporativas. Asimismo, el servicio Rejetto HFS 2.3 debe ser actualizado, reemplazado por una solución moderna o deshabilitado si no resulta esencial para la operación.

Adicionalmente, se recomienda establecer un proceso periódico de identificación y remediación de vulnerabilidades mediante herramientas como OpenVAS o Nessus, definiendo acuerdos de nivel de servicio (SLA) según la criticidad de los hallazgos.

- La efectividad de estas medidas podrá verificarse mediante:
- Reducción del número de vulnerabilidades críticas detectadas.
- Ausencia de sistemas vulnerables a MS17-010.
- Eliminación del uso de SMBv1.
- Informes periódicos de escaneo de vulnerabilidades.

Segmentación de red y reducción del movimiento lateral

El ejercicio evidenció que la ausencia de segmentación permitió el movimiento lateral desde Host-A hacia Host-B mediante técnicas de pivoting. Por esta razón, la segmentación de la infraestructura debe considerarse una medida prioritaria de reducción del riesgo.

Se recomienda implementar VLAN independientes para estaciones de trabajo, servidores, sistemas administrativos y activos críticos, acompañadas por reglas de firewall que permitan únicamente las comunicaciones estrictamente necesarias para la operación.

Igualmente, los servicios web internos que deban permanecer disponibles deberían protegerse mediante un firewall de aplicaciones web (WAF), reduciendo la exposición frente a ataques de explotación remota.

La validación de estas medidas puede realizarse mediante:

- Pruebas de conectividad entre segmentos.
- Ejercicios controlados de movimiento lateral.
- Revisión de reglas de firewall.
- Verificación de accesos autorizados entre VLAN.

Monitoreo continuo y capacidades de detección

La ausencia de monitoreo centralizado dificultó la detección temprana de las actividades ofensivas desarrolladas durante el laboratorio. En consecuencia, se recomienda implementar una plataforma SIEM basada en Wazuh como componente central de la estrategia defensiva.

Los agentes deberán desplegarse en servidores y estaciones de trabajo, configurando reglas de correlación para eventos asociados a:

- Creación de cuentas de usuario (Event ID 4720).
- Modificación de grupos privilegiados (Event ID 4732).
- Múltiples intentos de autenticación fallidos (Event ID 4625).

- Actividad anómala sobre servicios SMB.
- Instalación de servicios no autorizados.

Complementariamente, la integración de CrowdSec permitirá incorporar capacidades de inteligencia colaborativa y bloqueo automático de direcciones IP maliciosas.

La eficacia del sistema de monitoreo podrá evaluarse mediante indicadores como:

- Tiempo medio de detección (MTTD).
- Número de eventos correlacionados correctamente.
- Tiempo medio de respuesta (MTTR).
- Cantidad de incidentes detectados automáticamente.

La responsabilidad operativa de estas actividades deberá recaer en el equipo de seguridad o en el personal encargado de la administración de la infraestructura.

Gestión de privilegios y control de accesos

La creación de la cuenta administrativa WalterGonzalez evidenció la necesidad de fortalecer la administración de privilegios dentro de la organización.

Se recomienda realizar una auditoría completa de las cuentas de usuario y de servicio, eliminando privilegios administrativos innecesarios y aplicando el principio de mínimo privilegio. Asimismo, las cuentas con acceso a sistemas críticos deben incorporar mecanismos de autenticación multifactor.

Adicionalmente, debe verificarse que las aplicaciones y servicios no operen bajo cuentas con privilegios elevados cuando ello no resulte estrictamente necesario.

La efectividad de estas medidas podrá comprobarse mediante:

- Disminución del número de cuentas administrativas.
- Auditorías periódicas de privilegios.

- Cobertura de MFA en cuentas críticas.
- Revisiones de permisos en servicios y aplicaciones.

Fortalecimiento del marco legal y ético

El análisis del acuerdo de confidencialidad permitió identificar la necesidad de fortalecer los mecanismos internos de revisión jurídica y cumplimiento normativo.

Se recomienda revisar los acuerdos contractuales vigentes con asesoría especializada en derecho informático, eliminando cláusulas que puedan generar conflictos con la legislación nacional o con los principios éticos de la profesión.

Igualmente, la organización debería establecer procedimientos internos de revisión contractual que involucren áreas jurídicas, de cumplimiento y de seguridad de la información antes de la suscripción de nuevos acuerdos.

La capacitación del personal técnico en la Ley 1273 de 2009, la Ley 1581 de 2012 y los códigos de ética profesionales permitirá fortalecer la toma de decisiones frente a situaciones de riesgo legal o ético.

La verificación de estas medidas puede realizarse mediante:

- Auditorías de cumplimiento.
- Registros de capacitación.
- Evaluaciones de conocimiento.
- Revisión periódica de contratos y políticas.

Cultura de seguridad y mejora continua

Finalmente, se recomienda implementar programas permanentes de concientización en ciberseguridad dirigidos a todo el personal, abordando aspectos como ingeniería social, phishing, manejo de información y buenas prácticas de seguridad.

Asimismo, la realización periódica de ejercicios de Red Team y Blue Team permitirá evaluar la efectividad de los controles implementados y fortalecer la capacidad de respuesta organizacional. En etapas posteriores, la adopción de un enfoque Purple Team podría facilitar la transferencia de conocimiento entre equipos ofensivos y defensivos.

La efectividad de estas iniciativas podrá medirse mediante indicadores tales como:

- Participación del personal en actividades de capacitación.
- Resultados de simulaciones de phishing.
- Número de hallazgos corregidos después de ejercicios internos.
- Reducción del tiempo de respuesta ante incidentes.

En conjunto, estas recomendaciones buscan transformar los hallazgos obtenidos durante el caso SecureNova Labs en acciones concretas de mejora, contribuyendo al fortalecimiento de la resiliencia organizacional y a la consolidación de una postura de seguridad más madura y sostenible. seguridad.

Referencias Bibliográficas

Casey, E. (2011). Digital Evidence and Computer Crime (3.ª ed.). Academic Press.

Center for Internet Security. (2021). CIS Controls v8. Center for Internet Security. https://www.cisecurity.org/controls

Chen, T. M., & Abu-Nimeh, S. (2018). Lessons from Stuxnet and WannaCry attacks. IEEE Computer.

Chuvakin, A., Schmidt, K., & Phillips, C. (2013). Logging and log management: The authoritative guide to understanding the concepts surrounding logging and log management. Syngress.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Congreso de la República de Colombia. (2003). Ley 842 de 2003: Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y auxiliares y se adopta el Código de Ética Profesional. Diario Oficial No. 45.340.

Congreso de la República de Colombia. (2009). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado «de la protección de la información y de los datos». Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012). Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2025). Ley 2502 de 2025: Por medio de la cual se modifica el artículo 296 de la Ley 599 de 2000 referente al delito de falsedad personal

para la modalidad de suplantación utilizando Inteligencia Artificial. Diario Oficial. https://www.suin-juriscol.gov.co/viewDocument.asp?id=30055329

CrowdSec. (2024). CrowdSec open source documentation. https://docs.crowdsec.net

Cybersecurity and Infrastructure Security Agency. (2023). Known exploited vulnerabilities catalog. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023. ENISA. https://www.enisa.europa.eu

ISO/IEC. (2012). ISO/IEC 27037:2012 Information technology Security techniques Guidelines for identification, collection, acquisition and preservation of digital evidence.

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). National Institute of Standards and Technology.

Microsoft Security Response Center. (2017). Microsoft Security Bulletin MS17-010. https://msrc.microsoft.com

Microsoft. (s. f.). LocalSystem Account. Microsoft Learn. https://learn.microsoft.com/en-us/windows/win32/services/localsystem-account

MITRE. (2024). MITRE ATT&CK Framework: Privilege Escalation & Lateral Movement. https://attack.mitre.org

MITRE ATT&CK. (2025). T1090: Proxy. https://attack.mitre.org/techniques/T1090/

MITRE ATT&CK. (2025). T1570: Lateral Tool Transfer. https://attack.mitre.org/techniques/T1570/

MITRE ATT&CK. (2025). Enterprise ATT&CK Matrix. https://attack.mitre.org

National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.

National Institute of Standards and Technology (NIST). (2017). CVE-2017-0144. National Vulnerability Database. https://nvd.nist.gov

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. NIST. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2026). CVE-2014-6287: Rejetto HTTP File Server remote code execution vulnerability. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2014-6287

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Penetration Testing Execution Standard Working Group. (2014). The penetration testing execution standard. http://www.pentest-standard.org/index.php/Main_Page

Purdy, G. N. (2004). Linux iptables pocket reference. O'Reilly Media.

SANS Institute. (2023). Security operations center survey. SANS Institute.

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4.ª ed.). Pearson.

The Penetration Testing Execution Standard. (s. f.). Main page. http://www.pentest-standard.org/index.php/Main_Page

Unión Europea. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union.

Wazuh. (2024). Wazuh open source security platform documentation.

https://documentation.wazuh.com

Apéndices

Apéndice A

Resultado de revisión en Turnitin

	Título del Envío	Identificador del trabajo de Turnitin	Enviado	Similitud	Calificación	Calificación General	
Ver Recibo Digital	InformeFinalSeminario	2989555153	25/06/2026 18:01	11%	N/A	--	Entregar Trabajo

Nota. Resumen revisión de Turnitin, índice de similitud 11%