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

Nikolas Valencia Bustamante

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

Dedico este trabajo de grado como Especialista en Seguridad Informática, en primer lugar, a Dios, fuente de fortaleza, sabiduría y perseverancia. Su guía me permitió afrontar cada desafío académico, profesional y personal que se presentó durante este proceso de formación, recordándome en todo momento la importancia de la disciplina, la humildad y la constancia para alcanzar las metas propuestas.

A mi mamá, por ser el pilar fundamental de mi vida y el ejemplo más grande de esfuerzo, sacrificio y amor incondicional. Gracias por creer en mí incluso en los momentos de mayor dificultad, por cada palabra de aliento y por acompañarme silenciosamente durante este proceso. Detrás de cada trabajo entregado, de cada noche de estudio y de cada meta alcanzada, siempre estuvo su apoyo incondicional. Gracias por esos desvelos compartidos, por esos "tinticos" que aparecían en las madrugadas frías mientras avanzaba entre lecturas, investigaciones y entregas, y por demostrarme que el amor más grande muchas veces se expresa en los gestos más sencillos. Este logro también es suyo, porque una parte importante de lo que he alcanzado se construyó gracias a su esfuerzo, sus enseñanzas y su confianza permanente en mí.

A Cash, mi fiel compañero de cuatro patas, quien estuvo presente durante innumerables jornadas de estudio, investigación y desarrollo de este trabajo. Su compañía silenciosa, su lealtad incondicional y su capacidad de permanecer a mi lado durante largas horas frente al computador hicieron mucho más llevadero este camino. Estuvo presente durante madrugadas de estudio, laboratorios de pentesting, despliegues en Kubernetes, análisis forenses, configuraciones de seguridad, revisiones de vulnerabilidades, ejercicios de hardening, construcción de arquitecturas, elaboración de documentos técnicos y largas sesiones de investigación donde cada hallazgo representaba un nuevo reto por resolver. Fue testigo silencioso de incontables horas dedicadas a

comprender amenazas, corregir errores, fortalecer controles, desplegar servicios, analizar riesgos y encontrar soluciones a problemas que parecían imposibles de resolver.

En los momentos de mayor cansancio, estrés o frustración, siempre estuvo ahí, sin emitir juicio alguno y con la misma alegría de cada día, recordándome que incluso los desafíos más complejos pueden afrontarse mejor cuando se cuenta con una compañía sincera y leal. Si de mí dependiera, además de su título como el mejor compañero de vida, también recibiría con honores los diplomas de Ingeniero de Telecomunicaciones y Especialista en Seguridad Informática, pues pocas personas —y aún menos perros— pueden decir que acompañaron tan de cerca horas de investigación, despliegues, análisis de riesgos, búsquedas de vulnerabilidades, construcción de laboratorios, pruebas de seguridad, validaciones de controles, documentación técnica y jornadas completas dedicadas al aprendizaje continuo. Este trabajo también lleva una pequeña huella suya.

Finalmente, dedico este esfuerzo a todas las personas que creen en el poder del conocimiento, la educación y la mejora continua como herramientas para transformar vidas, superar desafíos y construir un futuro mejor. Que este trabajo represente no solo la culminación de una etapa académica, sino también el compromiso permanente con el aprendizaje, la excelencia profesional y el crecimiento personal.

Resumen

El presente documento desarrolla un análisis integral de un escenario de ciberseguridad ofensiva y defensiva sobre una infraestructura controlada basada en el entorno de SecureNova Labs, con el objetivo de evaluar el impacto técnico y organizacional derivado de la explotación de vulnerabilidades críticas, el movimiento lateral y la ausencia de controles adecuados de seguridad. Inicialmente, se ejecutó un ejercicio de pentesting estructurado que permitió identificar servicios vulnerables como Rejetto HTTP File Server (HFS 2.3) y sistemas Windows expuestos a la vulnerabilidad MS17-010, facilitando la obtención de acceso remoto, escalación de privilegios a nivel NT AUTHORITY\SYSTEM y técnicas de pivoting hacia redes internas. Posteriormente, se desarrolló un análisis táctico del incidente mediante actividades de postexplotación, identificación de indicadores de compromiso, análisis de artefactos sospechosos y evaluación del impacto sobre la confidencialidad, integridad y disponibilidad de la infraestructura. A partir de los hallazgos obtenidos, se estructuró una estrategia integral de respuesta a incidentes y fortalecimiento defensivo basada en hardening, segmentación de red, controles CIS, monitoreo centralizado mediante SIEM y mecanismos avanzados de detección y contención. Asimismo, se incorporó un enfoque moderno de seguridad cloud-native sustentado en tecnologías de observabilidad basadas en eBPF, utilizando herramientas como Tetragon y Falco para implementar capacidades de monitoreo y aislamiento en tiempo de ejecución desde el kernel del sistema operativo. Finalmente, el documento integra consideraciones legales, éticas y regulatorias relacionadas con la gestión de incidentes, la responsabilidad profesional y la protección de evidencia digital, demostrando cómo la convergencia entre capacidades Red Team, Blue Team, DFIR y seguridad runtime permite fortalecer la resiliencia organizacional frente a amenazas contemporáneas.

Palabras clave**:** DFIR, eBPF, hardening, pentesting, pivoting.

Abstract

This document presents a comprehensive analysis of an offensive and defensive cybersecurity scenario conducted within a controlled infrastructure based on the SecureNova Labs environment. The main objective was to evaluate the technical and organizational impact resulting from the exploitation of critical vulnerabilities, lateral movement techniques, and the absence of adequate security controls. Initially, a structured penetration testing exercise was performed to identify vulnerable services such as Rejetto HTTP File Server (HFS 2.3) and Windows systems exposed to the MS17-010 vulnerability, enabling remote access, privilege escalation to NT AUTHORITY\SYSTEM level, and pivoting techniques toward internal networks. Subsequently, a tactical incident analysis was developed through post-exploitation activities, identification of indicators of compromise, analysis of suspicious artifacts, and evaluation of the impact on the confidentiality, integrity, and availability of the infrastructure. Based on the findings obtained, a comprehensive incident response and defensive hardening strategy was structured using hardening mechanisms, network segmentation, CIS Controls, centralized monitoring through SIEM platforms, and advanced detection and containment capabilities. In addition, the document incorporates a modern cloud-native security approach supported by eBPF-based observability technologies, using tools such as Tetragon and Falco to implement runtime monitoring and isolation directly from the operating system kernel. Finally, legal, ethical, and regulatory considerations related to incident management, professional responsibility, and digital evidence preservation are integrated, demonstrating how the convergence of Red Team, Blue Team, DFIR, and runtime security capabilities strengthens organizational resilience against contemporary cyber threats.

Keywords**:** DFIR, eBPF, hardening, pentesting, pivoting.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

ACL (Access Control List):

Conjunto de reglas utilizadas para permitir o denegar tráfico de red o acceso a recursos específicos dentro de una infraestructura tecnológica, basado en criterios como direcciones IP, protocolos o puertos.

Blue Team:

Equipo especializado en actividades defensivas de ciberseguridad, encargado de prevenir, detectar, monitorear y responder ante amenazas o incidentes de seguridad mediante controles técnicos y operacionales.

CIS Controls:

Conjunto priorizado de buenas prácticas de seguridad desarrolladas por el Center for Internet Security (CIS), orientadas a fortalecer la postura de seguridad de las organizaciones mediante controles medibles y escalables.

DFIR (Digital Forensics and Incident Response):

Disciplina de ciberseguridad enfocada en la identificación, contención, análisis forense y recuperación frente a incidentes de seguridad informática.

eBPF (Extended Berkeley Packet Filter):

Tecnología integrada en el kernel de Linux que permite ejecutar programas de monitoreo y observabilidad de forma segura y eficiente dentro del núcleo del sistema operativo, sin modificar el código fuente del kernel.

EDR (Endpoint Detection and Response):

Solución de seguridad orientada a la detección, análisis y respuesta ante amenazas en dispositivos endpoint mediante monitoreo continuo y capacidades de contención.

Hardening:

Proceso de fortalecimiento de sistemas mediante la reducción de la superficie de ataque, eliminación de servicios innecesarios y aplicación de configuraciones seguras alineadas con buenas prácticas y estándares de seguridad.

IOC (Indicator of Compromise):

Evidencia técnica que sugiere la posible existencia de una intrusión o actividad maliciosa dentro de un sistema o infraestructura tecnológica.

Kubernetes:

Plataforma de orquestación de contenedores utilizada para automatizar el despliegue, administración y escalabilidad de aplicaciones basadas en contenedores.

Meterpreter:

Payload avanzado del framework Metasploit que proporciona acceso remoto interactivo sobre sistemas comprometidos, permitiendo ejecución de comandos, escalación de privilegios y actividades de postexplotación.

MITRE ATT&CK:

Framework de conocimiento que documenta tácticas, técnicas y procedimientos utilizados por actores maliciosos durante las distintas fases de un ataque cibernético.

MS17-010:

Vulnerabilidad crítica asociada al protocolo SMBv1 de Microsoft Windows, explotada mediante EternalBlue para lograr ejecución remota de código sin autenticación.

Pentesting:

Proceso controlado de pruebas de penetración orientado a identificar, explotar y evaluar vulnerabilidades presentes en sistemas, redes o aplicaciones con el fin de medir su nivel de exposición.

Pivoting:

Técnica utilizada durante un ataque para emplear un sistema previamente comprometido como punto intermedio de acceso hacia otros segmentos internos de red.

Red Team:

Equipo especializado en actividades ofensivas de ciberseguridad encargado de simular ataques reales con el fin de evaluar la capacidad defensiva de una organización.

Reverse Shell:

Conexión remota iniciada desde el sistema comprometido hacia el equipo atacante, utilizada para establecer control interactivo sobre la máquina objetivo.

Runtime Security:

Conjunto de mecanismos orientados a monitorear, detectar y contener amenazas mientras las aplicaciones o contenedores se encuentran en ejecución.

SIEM (Security Information and Event Management):

Plataforma utilizada para la recolección, correlación, monitoreo y análisis centralizado de eventos de seguridad provenientes de múltiples fuentes tecnológicas.

SMB (Server Message Block):

Protocolo de red utilizado principalmente en entornos Windows para compartir archivos, impresoras y recursos de red entre sistemas.

Tetragon:

Herramienta de seguridad basada en eBPF orientada al monitoreo y respuesta en tiempo de ejecución mediante observabilidad de procesos, syscalls y actividad de red desde el kernel de Linux.

Wazuh:

Plataforma open source orientada a funciones SIEM y HIDS, utilizada para monitoreo de seguridad, análisis de logs, detección de amenazas y cumplimiento normativo.

Introducción

Las amenazas informáticas han evolucionado hacia escenarios cada vez más complejos, caracterizados por cadenas de ataque capaces de combinar reconocimiento, explotación remota, escalación de privilegios y movimiento lateral dentro de infraestructuras corporativas. Cichonski et al. (2012) sostienen que la gestión moderna de incidentes requiere capacidades integrales orientadas no solo a la detección de compromisos de seguridad, sino también a la contención, investigación y recuperación de los sistemas afectados. Bajo esta misma línea, Weidman (2014) indica que las pruebas de penetración controladas permiten identificar debilidades reales en la infraestructura antes de que estas sean aprovechadas por actores maliciosos.

La permanencia de sistemas obsoletos y servicios expuestos continúa representando uno de los principales factores de riesgo en entornos organizacionales. Microsoft (2017) advierte que vulnerabilidades como MS17-010, asociadas al protocolo SMBv1, permiten ejecución remota de código y facilitan la propagación lateral de amenazas dentro de redes corporativas. De forma similar, herramientas vulnerables como Rejetto HTTP File Server (HFS 2.3) mantienen un alto nivel de exposición cuando son publicadas hacia internet sin mecanismos adecuados de segmentación, monitoreo o endurecimiento de seguridad (Exploit Database, 2014). Estas condiciones evidencian que los controles perimetrales tradicionales resultan insuficientes cuando no existen procesos sólidos de gestión de vulnerabilidades, control de privilegios y monitoreo continuo.

El presente documento desarrolla un análisis integral sobre un escenario controlado de ciberseguridad basado en la infraestructura simulada de SecureNova Labs, integrando capacidades ofensivas y defensivas dentro de un mismo ciclo técnico y organizacional. Inicialmente, se aborda un ejercicio estructurado de pentesting orientado a la identificación de servicios vulnerables, explotación de debilidades críticas, obtención de acceso remoto,

escalación de privilegios y técnicas de pivoting hacia redes internas. Posteriormente, el análisis evoluciona hacia actividades de respuesta a incidentes, investigación forense digital y fortalecimiento defensivo, permitiendo evaluar el impacto del compromiso sobre la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica. Scarfone y Mell (2007) plantean que los procesos de monitoreo, correlación y detección temprana son fundamentales para reducir el tiempo de exposición y limitar el alcance operativo de un incidente de seguridad.

Además del componente ofensivo y defensivo, el documento incorpora mecanismos modernos de protección orientados a entornos híbridos y cloud-native. Gregg (2020) explica que las tecnologías basadas en eBPF permiten implementar capacidades avanzadas de observabilidad y monitoreo directamente desde el kernel del sistema operativo, mejorando la visibilidad sobre procesos, conexiones y llamadas al sistema. A su vez, la Cloud Native Computing Foundation (CNCF, 2022) resalta que este tipo de tecnologías facilita capacidades de runtime security y contención dinámica en infraestructuras modernas basadas en contenedores y Kubernetes.

De igual forma, el desarrollo del documento integra consideraciones legales, éticas y regulatorias relacionadas con el ejercicio profesional de la ciberseguridad, incluyendo aspectos asociados a responsabilidad profesional, legislación informática colombiana y preservación de evidencia digital. Esto permite comprender el incidente no únicamente desde una perspectiva técnica, sino también desde sus implicaciones organizacionales, operativas y jurídicas dentro de procesos formales de gestión y respuesta ante incidentes.

Finalmente, el análisis propuesto busca demostrar cómo la convergencia entre capacidades Red Team, Blue Team, DFIR, hardening y seguridad cloud-native permite construir modelos de defensa más resilientes frente a amenazas contemporáneas. Más allá de la explotación técnica de vulnerabilidades, el enfoque desarrollado se orienta a transformar los

hallazgos obtenidos durante el incidente en mecanismos permanentes de detección, monitoreo, respuesta y mejora continua de la seguridad organizacional.

Justificación

La realización del presente análisis se justifica ante la necesidad creciente de fortalecer las capacidades técnicas y organizacionales de las infraestructuras modernas frente a amenazas informáticas cada vez más sofisticadas. Según Cichonski et al. (2012), los incidentes de seguridad actuales requieren mecanismos integrales de detección, contención y recuperación debido a la capacidad de las amenazas modernas para propagarse rápidamente dentro de entornos corporativos. Bajo esta misma línea, Scarfone y Mell (2007) señalan que la ausencia de monitoreo continuo y correlación adecuada de eventos incrementa significativamente el tiempo de exposición frente a actividades maliciosas dentro de la infraestructura tecnológica.

La permanencia de sistemas obsoletos y protocolos inseguros continúa representando uno de los principales factores de riesgo para las organizaciones. Microsoft (2017) advierte que la vulnerabilidad MS17-010 permitió la ejecución remota de código y la propagación lateral de amenazas a través del protocolo SMBv1, afectando infraestructuras críticas a nivel mundial. De manera similar, la explotación de servicios vulnerables como Rejetto HTTP File Server (HFS 2.3) evidencia cómo una mala gestión de servicios expuestos hacia internet puede facilitar compromisos completos de seguridad cuando no existen procesos adecuados de hardening, segmentación y control de accesos (Exploit Database, 2014).

Desde una perspectiva técnica, el desarrollo del documento permite integrar capacidades ofensivas y defensivas dentro de un mismo escenario controlado de ciberseguridad. Weidman (2014) sostiene que las pruebas de penetración constituyen un mecanismo fundamental para identificar vulnerabilidades reales antes de que estas sean aprovechadas por actores maliciosos. Asimismo, Sikorski y Honig (2012) indican que las actividades de análisis forense y postexplotación permiten comprender el comportamiento de los artefactos maliciosos,

reconstruir la secuencia de compromiso y determinar el alcance operativo de un incidente de seguridad.

Adicionalmente, el presente trabajo incorpora mecanismos modernos de protección orientados a entornos híbridos y cloud-native mediante tecnologías de observabilidad basadas en eBPF. Gregg (2020) explica que este tipo de tecnologías permite implementar monitoreo avanzado directamente desde el kernel del sistema operativo, proporcionando mayor visibilidad sobre procesos, conexiones y llamadas al sistema. De igual manera, la Cloud Native Computing Foundation (CNCF, 2022) destaca que las capacidades basadas en eBPF facilitan estrategias modernas de runtime security y contención dinámica en infraestructuras basadas en contenedores y Kubernetes.

Desde el componente organizacional y normativo, el análisis también se justifica por la necesidad de comprender las implicaciones éticas, legales y profesionales asociadas al ejercicio de la ciberseguridad ofensiva y defensiva. La Ley 1273 de 2009 establece responsabilidades relacionadas con acceso abusivo a sistemas informáticos, interceptación de datos y protección de la información digital, haciendo indispensable que los ejercicios de análisis y respuesta se desarrollen bajo principios éticos y metodologías controladas. En este sentido, el presente documento busca no solo analizar técnicamente un incidente de seguridad, sino también demostrar cómo la integración entre capacidades Red Team, Blue Team, DFIR, hardening y seguridad cloud-native contribuye al fortalecimiento de la resiliencia organizacional frente a amenazas contemporáneas.

Objetivos

Objetivo General

Analizar un escenario controlado de ciberseguridad mediante actividades ofensivas y defensivas orientadas a la identificación, explotación, contención y mitigación de vulnerabilidades presentes en una infraestructura tecnológica.

Objetivos Específicos

Identificar vulnerabilidades y servicios expuestos en la infraestructura objetivo mediante técnicas de reconocimiento, enumeración y análisis de superficie de ataque.

Explotar de forma controlada las vulnerabilidades identificadas para evaluar escenarios de compromiso, escalación de privilegios y movimiento lateral dentro de la red.

Aplicar procesos de respuesta a incidentes, análisis forense digital y fortalecimiento defensivo mediante estrategias de hardening, monitoreo y contención de amenazas.

Analizar mecanismos modernos de seguridad basados en eBPF y runtime security para fortalecer capacidades de detección y protección en entornos híbridos y cloud-native.

Desarrollo del informe

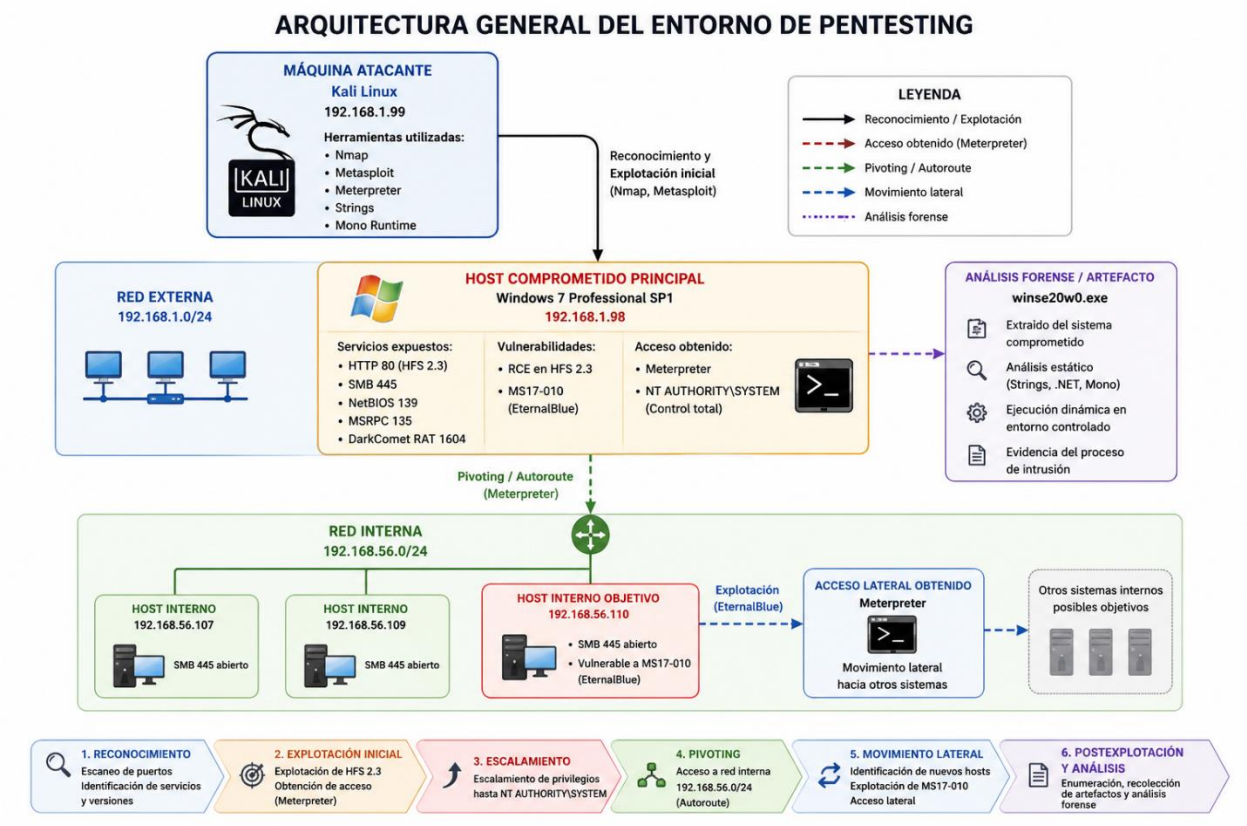
Contextualización del entorno y construcción del laboratorio

El entorno desarrollado para el presente análisis fue construido sobre una infraestructura virtualizada orientada a simular condiciones reales de compromiso dentro de un escenario corporativo controlado. La arquitectura del laboratorio fue desplegada mediante VirtualBox, integrando sistemas Windows y Linux distribuidos en diferentes segmentos de red con el propósito de ejecutar actividades ofensivas, defensivas y de análisis forense de manera controlada. Weidman (2014) indica que los entornos de laboratorio orientados a pruebas de penetración permiten validar vulnerabilidades reales y analizar el impacto operativo de las técnicas utilizadas por actores maliciosos dentro de una infraestructura tecnológica.

La construcción del entorno contempló la implementación de una máquina atacante basada en Kali Linux y múltiples sistemas Windows vulnerables, configurados con servicios expuestos y protocolos inseguros orientados a reproducir escenarios reales de explotación. Entre los servicios identificados se encontraba Rejetto HTTP File Server (HFS 2.3), vulnerable a ejecución remota de comandos, así como sistemas con SMBv1 habilitado y exposición a la vulnerabilidad MS17-010. Microsoft (2017) sostiene que este tipo de vulnerabilidades facilita la ejecución remota de código y la propagación lateral de amenazas dentro de redes corporativas cuando no existen controles adecuados de actualización y segmentación de red.

Figura 1

Arquitectura general del laboratorio.

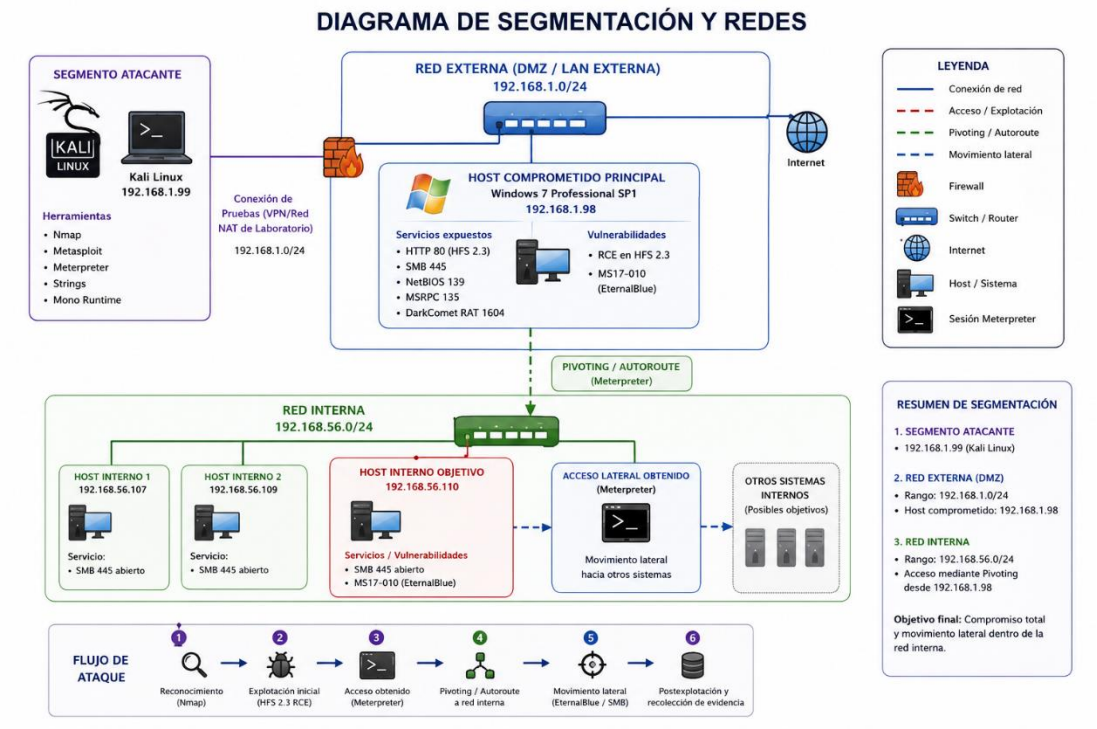


Nota. Elaboración propia.

La segmentación del entorno permitió simular escenarios de pivoting y movimiento lateral entre diferentes redes internas, facilitando el análisis de técnicas ofensivas orientadas a la expansión progresiva del compromiso. La infraestructura incorporó múltiples interfaces de red y segmentos aislados con el propósito de evaluar el impacto derivado de configuraciones inseguras, privilegios excesivos y ausencia de controles de segmentación. Según Microsoft (2017), la falta de controles adecuados sobre protocolos como SMBv1 incrementa significativamente el riesgo de propagación lateral dentro de redes corporativas vulnerables.

Figura 2

Segmentación de red



Nota. Elaboración propia.

Desde la perspectiva metodológica, el laboratorio permitió desarrollar actividades de reconocimiento, enumeración, explotación, escalación de privilegios y análisis defensivo dentro de un entorno controlado. Weidman (2014) afirma que las pruebas de penetración controladas constituyen un mecanismo fundamental para identificar debilidades técnicas antes de que estas sean aprovechadas por actores maliciosos en entornos reales. Bajo esta misma línea, el escenario implementado facilitó la validación práctica de múltiples vectores de ataque asociados a exposición de servicios vulnerables, protocolos inseguros y ausencia de monitoreo interno.

Tabla 1

Direcciones IP y roles de los sistemas dentro del laboratorio.

Máquina	Dirección IP	Rol	Sistema Operativo
Kali Linux	192.168.1.99	Equipo atacante	Kali Linux
Host A	192.168.1.98 192.168.56.109	Sistema Vulnerable/Pivoting interno	Windows 7 SP1
Host B	192.168.56.110	Host interno vulnerable	Windows 7 SP1

Nota. Elaboración propia

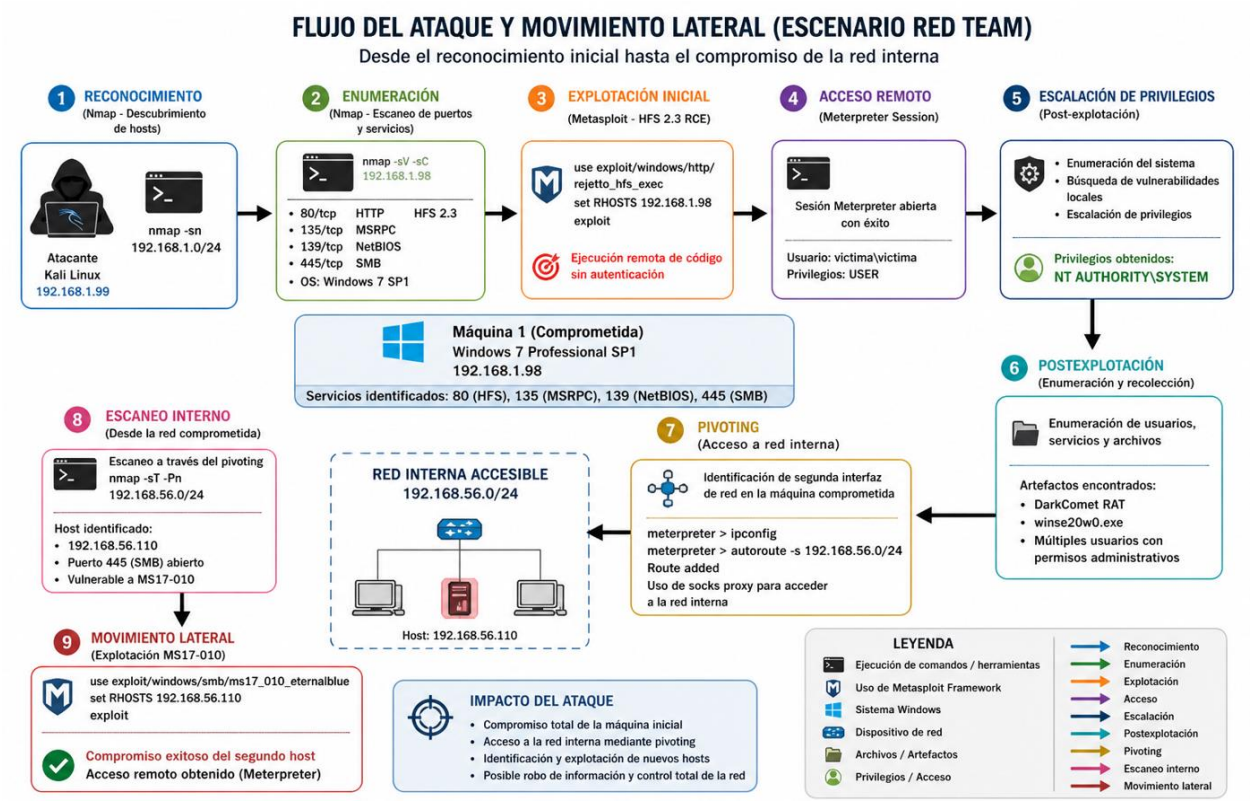
Adicionalmente, el entorno construido permitió analizar problemáticas comunes presentes en múltiples organizaciones, especialmente aquellas que mantienen infraestructura heredada y capacidades limitadas de monitoreo interno. Scarfone y Mell (2007) señalan que la ausencia de monitoreo centralizado y correlación adecuada de eventos incrementa significativamente el tiempo de exposición frente a actividades maliciosas dentro de la infraestructura tecnológica. De igual forma, la ausencia de segmentación efectiva y controles de mínimo privilegio facilita escenarios de movimiento lateral y persistencia una vez que el atacante logra comprometer un activo inicial.

Como parte del desarrollo técnico del laboratorio, también se definió un flujo general de ataque orientado a integrar las diferentes etapas ofensivas y defensivas desarrolladas durante el

análisis. Este flujo permitió estructurar metodológicamente las actividades de reconocimiento, explotación, obtención de acceso remoto, escalación de privilegios, pivoting y movimiento lateral dentro de la infraestructura simulada. Weidman (2014) plantea que la estructuración secuencial de las fases ofensivas permite comprender con mayor precisión el comportamiento del atacante y el impacto derivado del compromiso sobre la infraestructura objetivo.

Figura 3

Flujo general del ataque desarrollado



Nota. Elaboración propia.

Marco legal, ético y responsabilidad profesional

El ejercicio de la ciberseguridad ofensiva y defensiva implica responsabilidades técnicas, legales y éticas que deben ser consideradas durante todas las fases de análisis, explotación y respuesta ante incidentes. Cichonski et al. (2012) señalan que las actividades relacionadas con identificación de vulnerabilidades, análisis de amenazas y gestión de incidentes deben ejecutarse bajo procedimientos controlados que permitan garantizar trazabilidad y protección de los activos tecnológicos involucrados. Bajo esta misma línea, las pruebas de penetración únicamente pueden desarrollarse dentro de entornos autorizados, debido a que la ejecución no controlada de estas actividades puede derivar en afectaciones operativas y responsabilidades legales.

La legislación informática colombiana establece límites claros frente al acceso no autorizado a sistemas, interceptación de información y afectación de activos digitales. El Congreso de Colombia (2009), mediante la Ley 1273, incorporó nuevos tipos penales relacionados con acceso abusivo a sistemas informáticos, interceptación de datos, daño informático y utilización de software malicioso. Según esta normativa, el acceso no autorizado a infraestructuras tecnológicas puede generar responsabilidades penales incluso cuando no exista destrucción directa de información, debido a la afectación potencial sobre la confidencialidad, integridad y disponibilidad de los sistemas comprometidos.

Desde la perspectiva ética, las actividades ofensivas desarrolladas dentro de procesos de pentesting deben ejecutarse bajo principios de proporcionalidad, autorización y control metodológico. Weidman (2014) sostiene que las pruebas de penetración tienen como propósito identificar debilidades técnicas para fortalecer la postura defensiva de las organizaciones y no para generar afectaciones operativas o comprometer información de manera ilegítima. De igual

forma, el uso de capacidades ofensivas fuera del alcance autorizado representa una vulneración a los principios fundamentales asociados al ejercicio responsable de la ciberseguridad.

La responsabilidad profesional en el ámbito tecnológico también exige que los especialistas actúen bajo criterios de confidencialidad, integridad y protección de la información organizacional. El Consejo Profesional Nacional de Ingeniería (COPNIA, 2022) establece que los profesionales del área tecnológica deben desarrollar sus actividades bajo principios éticos orientados a proteger la información sensible, preservar la integridad de los sistemas y prevenir riesgos derivados de malas prácticas operativas. En consecuencia, ocultar incidentes de seguridad, manipular evidencia digital o ejecutar actividades ofensivas no autorizadas constituye una vulneración directa a los principios éticos y profesionales asociados al ejercicio de la ingeniería y la ciberseguridad.

Asimismo, la gestión de incidentes y el análisis forense digital requieren procedimientos orientados a preservar la integridad de la evidencia recolectada durante el proceso investigativo. Cichonski et al. (2012) indican que la respuesta a incidentes debe contemplar actividades estructuradas de identificación, contención, erradicación y recuperación, manteniendo trazabilidad sobre las acciones ejecutadas durante el análisis técnico. Bajo este enfoque, la preservación de logs, artefactos sospechosos, hashes criptográficos y registros de actividad resulta fundamental para garantizar validez técnica y soporte investigativo dentro del proceso forense.

Figura 4

Relación entre responsabilidades legales, éticas y técnicas dentro del ejercicio de la ciberseguridad.

Nota. Elaboración propia.

Adicionalmente, la creciente dependencia organizacional de infraestructuras digitales ha incrementado la necesidad de establecer políticas formales de gobierno de seguridad, segregación de funciones y control de privilegios. Scarfone y Mell (2007) señalan que la ausencia de monitoreo, auditoría y mecanismos adecuados de control incrementa significativamente la probabilidad de compromisos internos y abuso de privilegios dentro de la infraestructura tecnológica. Bajo esta misma línea, la implementación de principios de mínimo

privilegio, monitoreo continuo y trazabilidad operativa constituye un componente esencial dentro de cualquier estrategia moderna de ciberseguridad.

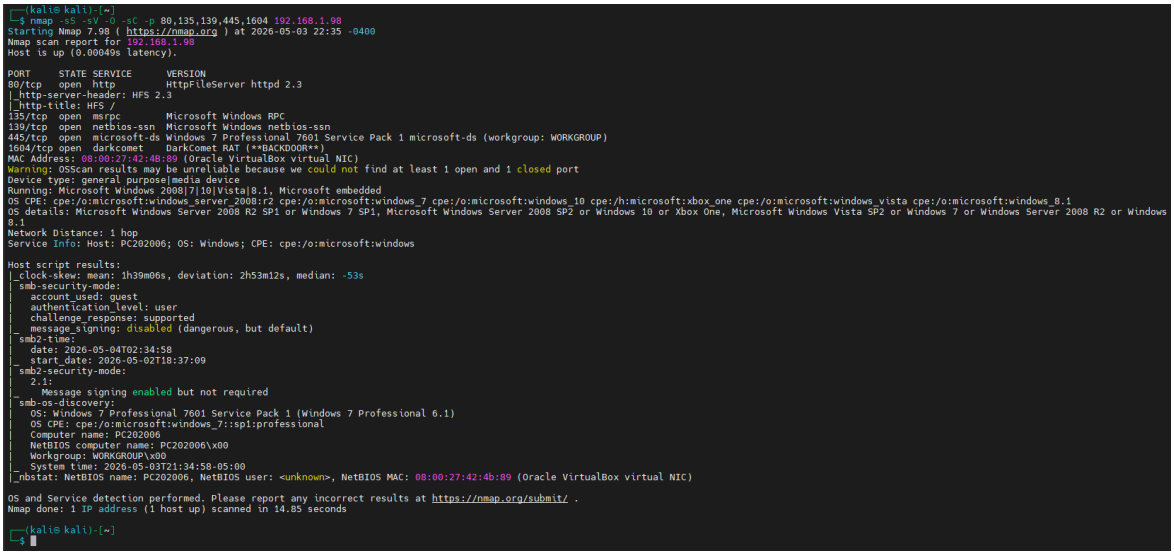
Finalmente, el análisis del presente escenario permite comprender que las capacidades ofensivas y defensivas no pueden separarse de las implicaciones legales y éticas asociadas al tratamiento de información digital. Más allá de la explotación técnica de vulnerabilidades, la gestión adecuada de incidentes exige responsabilidad profesional, control metodológico y cumplimiento normativo orientado a proteger la integridad de los sistemas, la evidencia digital y la información organizacional frente a amenazas contemporáneas.

Las estrategias Red Team desarrolladas dentro del presente escenario estuvieron orientadas a simular tácticas reales utilizadas por actores maliciosos para comprometer infraestructuras corporativas mediante reconocimiento, explotación de vulnerabilidades, escalación de privilegios y movimiento lateral. Según Weidman (2014), los ejercicios ofensivos controlados permiten identificar debilidades técnicas y validar el impacto operativo derivado de configuraciones inseguras y servicios vulnerables presentes en la infraestructura tecnológica. Bajo esta misma línea, Hutchins et al. (2011) sostienen que las cadenas modernas de ataque generalmente siguen fases progresivas de reconocimiento, explotación, persistencia y expansión lateral dentro de la red comprometida.

El proceso ofensivo inició mediante actividades de reconocimiento y enumeración orientadas a identificar hosts activos, servicios expuestos y posibles vectores de ataque dentro de la red objetivo. Durante esta fase se utilizó Nmap para realizar descubrimiento de puertos, identificación de servicios y detección de versiones vulnerables presentes en los sistemas analizados. Lyon (2009) explica que las actividades de escaneo y enumeración permiten construir un mapa detallado de exposición sobre la infraestructura objetivo, facilitando la identificación de superficies de ataque aprovechables por actores maliciosos.

Figura 5

Enumeración de servicios y detección de vulnerabilidades mediante Nmap sobre el host objetivo.

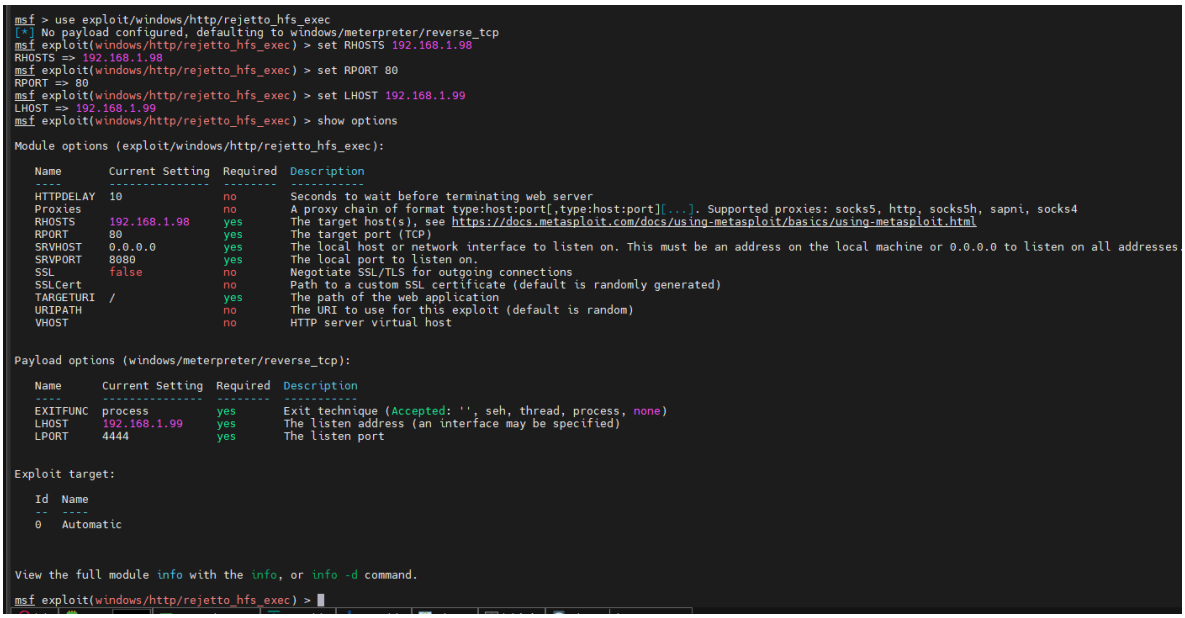


Nota. Elaboración propia.

Los resultados obtenidos permitieron identificar la exposición del servicio Rejetto HTTP File Server (HFS 2.3), vulnerable a ejecución remota de comandos mediante exploits documentados públicamente. Offensive Security (2014) documenta que este servicio presenta debilidades críticas que permiten a un atacante ejecutar comandos arbitrarios sobre el sistema afectado cuando el servicio se encuentra expuesto sin controles adecuados de protección. A partir de este hallazgo, se procedió a utilizar Metasploit Framework para ejecutar el exploit asociado y obtener acceso remoto inicial sobre el sistema objetivo.

Figura 6

Explotación de Rejetto HFS 2.3 mediante Metasploit Framework.

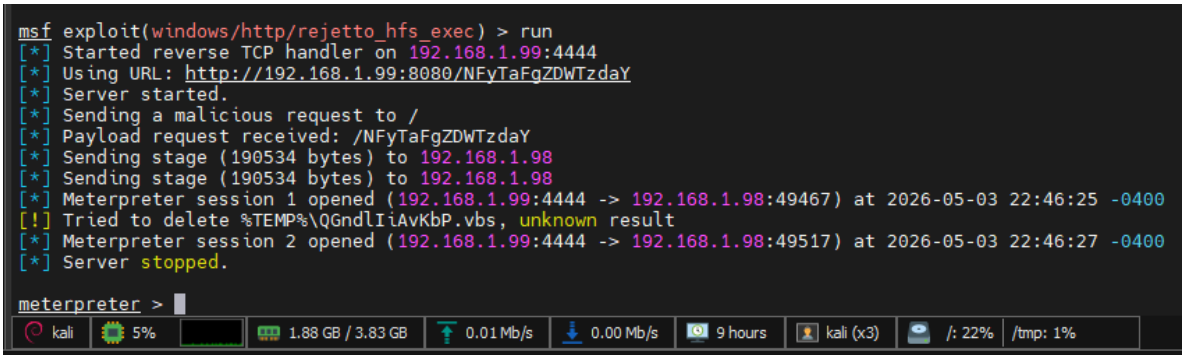


Nota. Elaboración propia.

La explotación exitosa permitió establecer una reverse shell y posteriormente una sesión Meterpreter sobre el sistema comprometido. Rapid7 (2023) indica que Meterpreter proporciona capacidades avanzadas de postexplotación orientadas a ejecución remota de comandos, escalación de privilegios, evasión y movimiento lateral dentro de redes comprometidas. Bajo este escenario, la sesión obtenida permitió ejecutar actividades de reconocimiento interno y validación de privilegios sobre el sistema comprometido.

Figura 7

Obtención de sesión Meterpreter sobre el sistema comprometido.

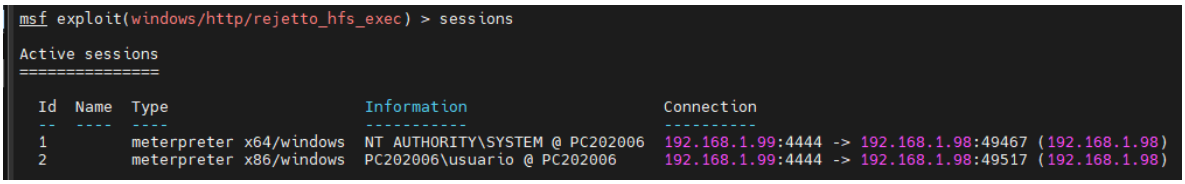


Nota. Elaboración propia.

Posteriormente, se desarrollaron actividades de escalación de privilegios orientadas a obtener control total sobre el sistema afectado. Durante esta fase se logró acceso con privilegios NT AUTHORITY\SYSTEM, permitiendo ejecutar acciones administrativas y ampliar el alcance operativo del compromiso. Según MITRE ATT&CK (2024), las técnicas de privilege escalation permiten incrementar capacidades de persistencia, evasión y control sobre los activos comprometidos, representando una de las fases más críticas dentro de un ataque avanzado.

Figura 8

Escalación de privilegios hacia NT AUTHORITY\SYSTEM



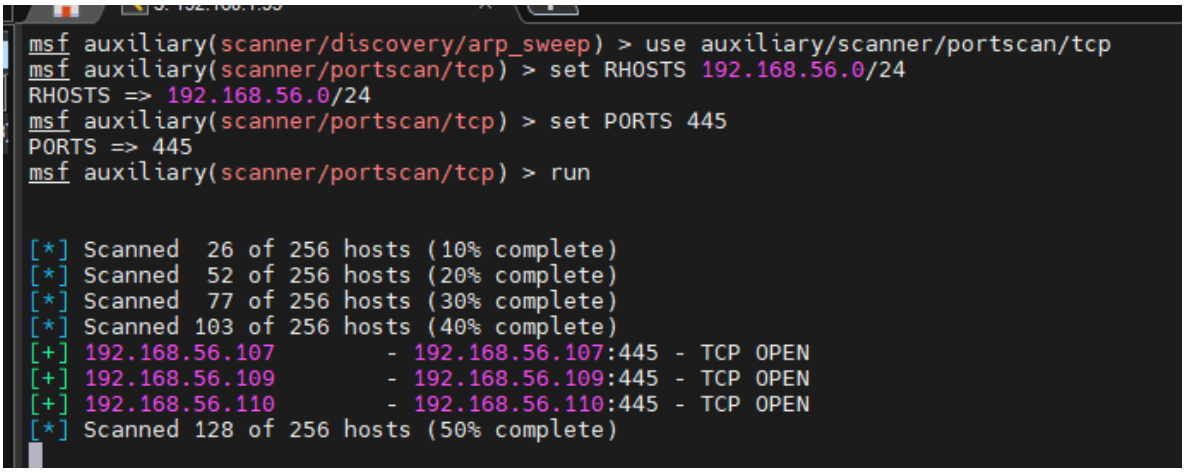
Nota. Elaboración propia.

Una vez comprometido el sistema inicial, se ejecutaron técnicas de pivoting y movimiento lateral orientadas a acceder a segmentos internos previamente no accesibles desde el

equipo atacante. Hutchins et al. (2011) explican que el movimiento lateral constituye una de las principales capacidades utilizadas por actores avanzados para expandir progresivamente el compromiso dentro de redes corporativas. En el presente escenario, el sistema inicialmente comprometido fue utilizado como puente de acceso hacia redes internas adicionales, facilitando la expansión operativa del ataque.

Figura 9

Pivoting y acceso hacia segmentos internos de red

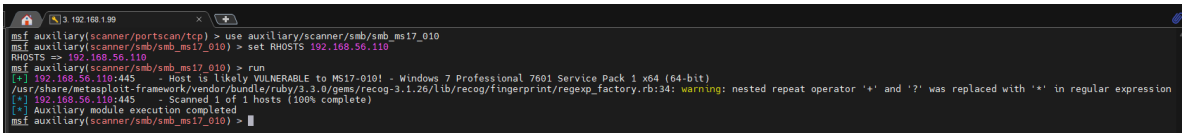


Nota. Elaboración propia.

Como parte del movimiento lateral, se ejecutó la explotación de MS17-010 sobre sistemas Windows vulnerables dentro de la red interna. CISA (2020) advierte que las vulnerabilidades asociadas a SMBv1 continúan siendo utilizadas para comprometer infraestructuras que mantienen sistemas obsoletos o configuraciones inseguras dentro de redes corporativas. Bajo este escenario, la explotación permitió ampliar el alcance del compromiso sobre nuevos activos internos mediante ejecución remota de código.

Figura 10

Explotación de MS17-010 sobre sistemas internos vulnerables

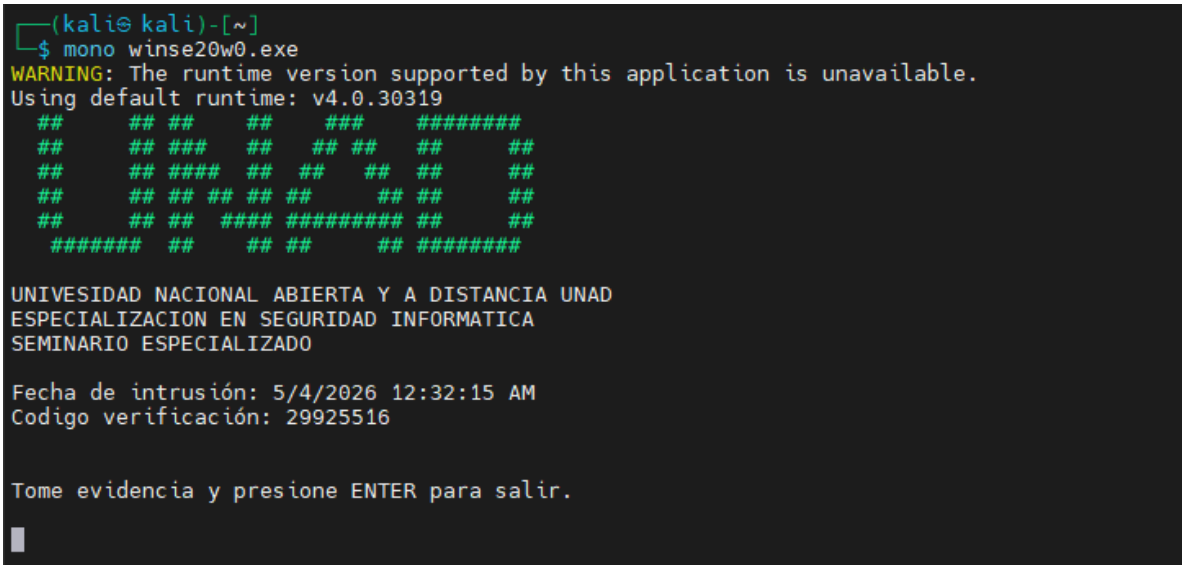


Nota. Elaboración propia.

Finalmente, durante las actividades de postexplotación se realizó análisis de artefactos sospechosos encontrados dentro del sistema comprometido, incluyendo el archivo winse20w0.exe. Sikorski y Honig (2012) sostienen que el análisis preliminar de artefactos maliciosos permite identificar indicadores de compromiso, patrones de comportamiento y posibles mecanismos de persistencia utilizados durante un incidente de seguridad. Para el análisis inicial se utilizaron herramientas básicas de inspección como Strings y generación de hashes criptográficos orientados a validar posibles indicadores asociados al artefacto identificado.

Figura 11

Análisis preliminar del artefacto winse20w0.exe



Nota. Elaboración propia.

Estrategias defensivas y capacidades Blue Team

La capacidad de detectar oportunamente actividades maliciosas constituye uno de los pilares fundamentales de cualquier estrategia moderna de ciberseguridad. Aunque la prevención continúa siendo un componente esencial dentro de los programas de seguridad, diversos estudios han demostrado que ninguna organización puede asumir que sus controles preventivos serán completamente efectivos frente a amenazas avanzadas. En consecuencia, las capacidades de detección temprana, análisis y respuesta adquieren un papel crítico para reducir el impacto derivado de un compromiso de seguridad. Según Cichonski et al. (2012), la respuesta a incidentes debe concebirse como un proceso continuo orientado a limitar la propagación de las amenazas, preservar la evidencia digital y restaurar las operaciones afectadas en el menor tiempo posible.

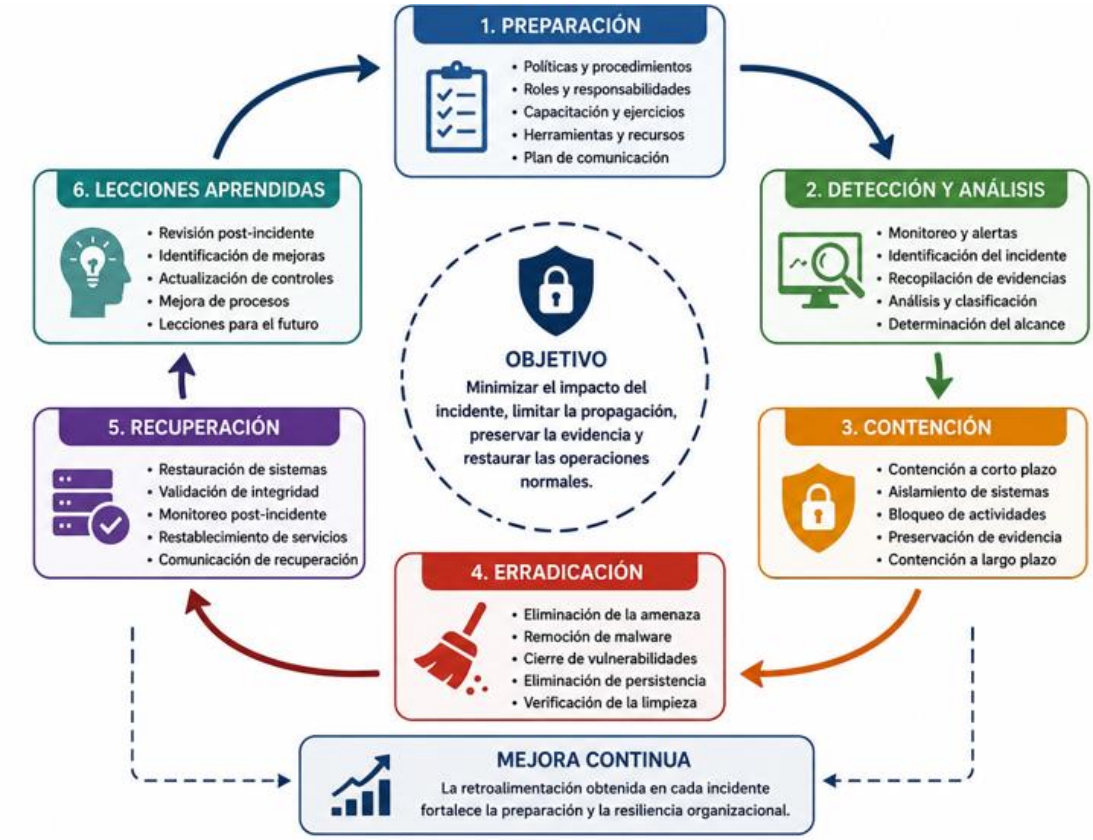
Durante el escenario desarrollado en SecureNova Labs, la fase ofensiva permitió evidenciar cómo una vulnerabilidad inicialmente explotada puede evolucionar rápidamente hacia escenarios de escalación de privilegios, pivoting y movimiento lateral dentro de la infraestructura. Este comportamiento coincide con lo descrito por Hutchins, Cloppert y Amin (2011), quienes plantean que los ataques modernos siguen una secuencia progresiva de actividades que incrementan gradualmente el nivel de compromiso sobre los activos organizacionales. Bajo esta perspectiva, la detección temprana de anomalías durante las primeras etapas del ataque representa uno de los mecanismos más efectivos para reducir el alcance operativo del incidente.

La respuesta a incidentes debe ejecutarse mediante procedimientos estructurados que permitan mantener control sobre las acciones realizadas durante el proceso de investigación. El marco propuesto por el National Institute of Standards and Technology (NIST) establece cuatro

grandes fases para la gestión de incidentes: preparación, detección y análisis, contención, erradicación y recuperación (Cichonski et al., 2012). Estas fases buscan garantizar que la organización pueda responder de manera coordinada, minimizando tanto el impacto técnico como las consecuencias operativas derivadas del incidente.

Figura 12

Ciclo de vida de respuesta a incidentes basado en NIST SP 800-61



Nota. Adaptado de Cichonski et al, (2012).

Dentro del escenario analizado, las actividades de detección estuvieron orientadas a identificar indicadores de compromiso asociados a la explotación de HFS 2.3, establecimiento de sesiones remotas, elevación de privilegios y ejecución de herramientas de postexplotación.

Según MITRE ATT&CK (2024), las técnicas relacionadas con ejecución remota de comandos, escalación de privilegios y movimiento lateral generan múltiples evidencias que pueden ser detectadas mediante correlación de eventos, análisis de comportamiento y monitoreo continuo de procesos. La capacidad de identificar estos indicadores de forma temprana permite reducir significativamente la permanencia del atacante dentro de la infraestructura.

Desde la perspectiva operativa, la detección efectiva requiere visibilidad sobre diferentes capas de la infraestructura tecnológica. Bejtlich (2013) sostiene que la combinación de registros de eventos, tráfico de red, telemetría de endpoints y análisis de comportamiento proporciona una capacidad superior de detección frente a enfoques que dependen exclusivamente de firmas o indicadores conocidos. Esta visión resulta especialmente relevante en escenarios donde el atacante utiliza herramientas legítimas del sistema operativo para evadir mecanismos tradicionales de seguridad.

Una vez identificado el incidente, la contención constituye la siguiente prioridad operativa. Según CISA (2023), el objetivo principal de esta fase consiste en limitar la capacidad de propagación de la amenaza mientras se preserva la evidencia necesaria para el análisis posterior. Dependiendo del nivel de compromiso identificado, las medidas de contención pueden incluir aislamiento de sistemas, segmentación temporal de redes, revocación de credenciales comprometidas o bloqueo de comunicaciones maliciosas detectadas durante la investigación.

Posteriormente, las actividades de erradicación buscan eliminar los elementos que permitieron el compromiso inicial, incluyendo vulnerabilidades explotadas, mecanismos de persistencia y configuraciones inseguras presentes dentro de la infraestructura. Cichonski et al. (2012) indican que la erradicación debe ejecutarse únicamente después de comprender completamente el alcance del incidente, evitando generar pérdida de evidencia o comprometer el proceso de investigación. Finalmente, la recuperación tiene como objetivo restablecer la

operación normal de los sistemas afectados, verificando que no persistan indicadores de compromiso ni vectores de acceso asociados al incidente previamente identificado.

La experiencia obtenida durante el desarrollo del laboratorio evidencia que las capacidades de respuesta no dependen exclusivamente de herramientas tecnológicas, sino también de procesos claramente definidos, procedimientos documentados y personal capacitado para actuar frente a situaciones de compromiso. Bajo esta perspectiva, la integración entre monitoreo continuo, análisis técnico y respuesta estructurada constituye uno de los elementos más importantes para fortalecer la resiliencia organizacional frente a amenazas contemporáneas.

Tabla 2

Relación entre fases de respuesta a incidentes y actividades desarrolladas en el escenario

Fase NIST	Actividad realizada	Objetivo
Preparación	Construcción del laboratorio y definición de alcance	Simular el entorno controlado
Detección y análisis	Identificación de explotación HFS y sesiones remotas	Detectar compromiso
Contención	Aislamiento lógico de sistemas afectados	Limitar propagación.

Erradicación	Eliminación de vulnerabilidades y vectores de acceso	Remover amenaza
Recuperación	Validación operativa de sistemas afectados	Restablecer operación.
Lecciones aprendidas.	Definición de controles ofensivos.	Mejorar postura de seguridad.

Nota. Elaboración propia

Análisis forense digital (DFIR)

Una vez identificado el compromiso de la infraestructura, resulta fundamental desarrollar actividades orientadas a la preservación, recolección, análisis y correlación de evidencia digital. Según Casey (2011), el análisis forense digital tiene como objetivo reconstruir los eventos asociados a un incidente de seguridad mediante el examen sistemático de artefactos digitales, permitiendo comprender cómo ocurrió el compromiso, qué activos fueron afectados y cuál fue el alcance real de las acciones ejecutadas por el atacante. Bajo esta perspectiva, el análisis forense constituye un componente esencial dentro de cualquier proceso formal de respuesta a incidentes.

Dentro del escenario desarrollado en SecureNova Labs, las actividades forenses estuvieron orientadas a identificar indicadores de compromiso (IOC), analizar artefactos sospechosos y preservar evidencia asociada a las fases de explotación y postexplotación ejecutadas durante el ejercicio Red Team. NIST (Kent et al., 2006) establece que la evidencia

digital debe ser recolectada y preservada siguiendo procedimientos que garanticen integridad, trazabilidad y reproducibilidad de los hallazgos obtenidos durante la investigación. En consecuencia, cualquier actividad realizada sobre los sistemas comprometidos debe documentarse adecuadamente para evitar alteraciones que comprometan la validez del análisis.

La fase inicial del proceso forense consistió en la identificación y preservación de evidencias potencialmente relevantes para la investigación. Entre los principales elementos analizados se incluyeron registros de eventos del sistema operativo, sesiones remotas establecidas mediante Meterpreter, artefactos ejecutables identificados durante la postexplotación y configuraciones del sistema susceptibles de haber sido modificadas por el atacante. Casey (2011) señala que la correlación entre diferentes fuentes de evidencia permite reconstruir de manera más precisa la secuencia cronológica de un incidente de seguridad.

Figura 13

Proceso general de análisis forense digital aplicado al incidente

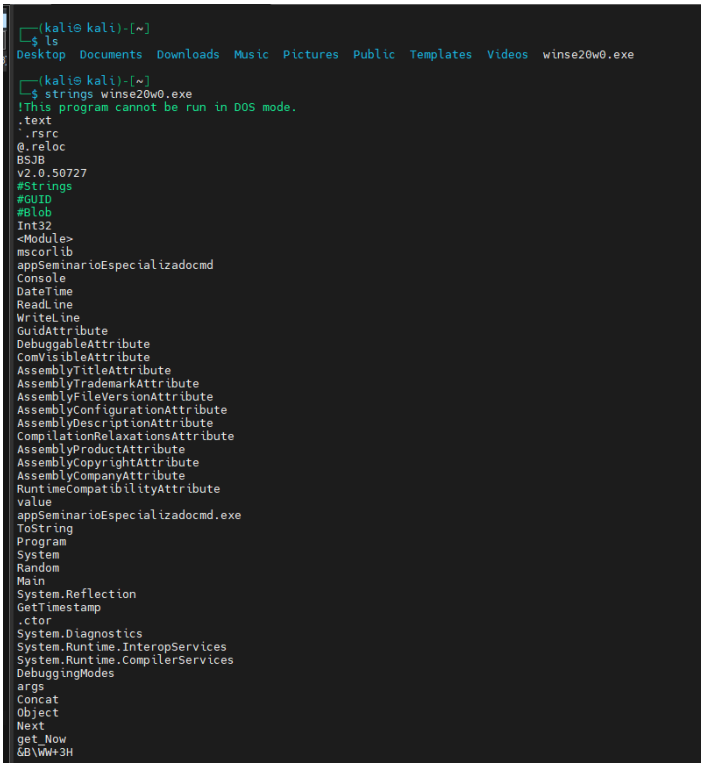
Nota. Adaptado de Kent et al. (2006) y Casey (2011).

Como parte del análisis técnico, se realizó la identificación de indicadores de compromiso asociados a ejecución remota de comandos, conexiones sospechosas, creación de procesos anómalos y actividades relacionadas con movimiento lateral. MITRE ATT&CK (2024) indica que múltiples técnicas ofensivas generan rastros observables en registros de eventos, memoria, procesos y actividad de red, los cuales pueden ser utilizados para determinar la presencia y comportamiento de un atacante dentro de la infraestructura comprometida.

Adicionalmente, se efectuó el análisis preliminar del archivo sospechoso identificado durante la fase ofensiva, denominado winse20w0.exe. Para ello se emplearon técnicas básicas de análisis estático orientadas a identificar cadenas de texto, posibles indicadores de comportamiento y elementos asociados a funcionalidades internas del artefacto. Sikorski y Honig (2012) explican que el análisis estático constituye una de las primeras aproximaciones utilizadas para comprender el propósito y comportamiento potencial de un archivo ejecutable antes de su ejecución controlada en entornos aislados.

Figura 14

Análisis preliminar del artefacto winse20w0.exe mediante Strings.



Nota. Elaboración propia.

Con el propósito de garantizar la integridad de la evidencia recolectada, también se aplicaron mecanismos de verificación mediante funciones hash criptográficas. Según Carrier (2005), la generación de hashes permite demostrar que la evidencia digital no ha sido modificada desde el momento de su adquisición, constituyendo una práctica fundamental dentro de los procedimientos forenses modernos. En este sentido, los valores hash obtenidos durante el análisis permitieron validar la integridad de los artefactos evaluados y asegurar la trazabilidad de la investigación.

Tabla 3

Ejemplo de evidencias digitales recolectadas durante el análisis.

Evidencia	Tipo	Propósito
Logs del Sistema	Registro de eventos	Reconstrucción cronológica
Sesiones Meterpreter	Evidencia de compromiso	Identificación de actividades ofensivas
Archivo winse20w0.exe	Artefacto sospechoso	Análisis técnico
Hash SHA-256	Integridad	Validación de evidencia
Configuración del Sistema	Evidencia de persistencia	Verificación de modificaciones.

Nota. Elaboración propia

Posteriormente, las evidencias obtenidas fueron correlacionadas para reconstruir la secuencia de eventos asociada al incidente. Bejtlich (2013) sostiene que la correlación de múltiples fuentes de información permite identificar relaciones entre actividades aparentemente

aisladas y comprender con mayor precisión el comportamiento del atacante dentro de la infraestructura. Este proceso facilitó la identificación de la cadena de compromiso desde la explotación inicial hasta las actividades de postexplotación y movimiento lateral observadas durante el ejercicio.

Finalmente, el análisis forense permitió establecer una visión integral del incidente, identificando los vectores de ataque utilizados, los sistemas afectados y los riesgos derivados de las vulnerabilidades explotadas. Más allá de la simple identificación de artefactos o registros de actividad, el proceso DFIR proporcionó información crítica para fortalecer las estrategias defensivas posteriores, permitiendo transformar los hallazgos obtenidos en mecanismos concretos de detección, monitoreo y respuesta frente a amenazas similares en escenarios futuros.

Hardening y reducción de superficie de ataque

Los resultados obtenidos durante las actividades ofensivas evidenciaron que el éxito del compromiso no estuvo asociado a una única vulnerabilidad, sino a la acumulación de múltiples debilidades de seguridad presentes dentro de la infraestructura. La exposición de servicios vulnerables, la utilización de protocolos obsoletos, la ausencia de segmentación efectiva y la existencia de privilegios elevados permitieron que un acceso inicial evolucionara progresivamente hacia escenarios de escalación de privilegios y movimiento lateral. Esta situación coincide con lo planteado por el Center for Internet Security (CIS, 2024), que identifica la reducción de la superficie de ataque como uno de los mecanismos más efectivos para disminuir las probabilidades de explotación exitosa dentro de entornos corporativos.

Durante la fase Red Team se logró comprometer un servicio HFS 2.3 expuesto a la red y posteriormente expandir el alcance del incidente hacia otros sistemas vulnerables. Este

comportamiento demuestra que la presencia de servicios innecesarios o desactualizados incrementa significativamente las oportunidades disponibles para un atacante. Según CISA (2023), la exposición de aplicaciones vulnerables continúa siendo uno de los vectores de acceso inicial más utilizados durante incidentes reales, razón por la cual la eliminación de servicios innecesarios y la reducción de componentes expuestos deben considerarse medidas prioritarias dentro de cualquier programa de endurecimiento de seguridad.

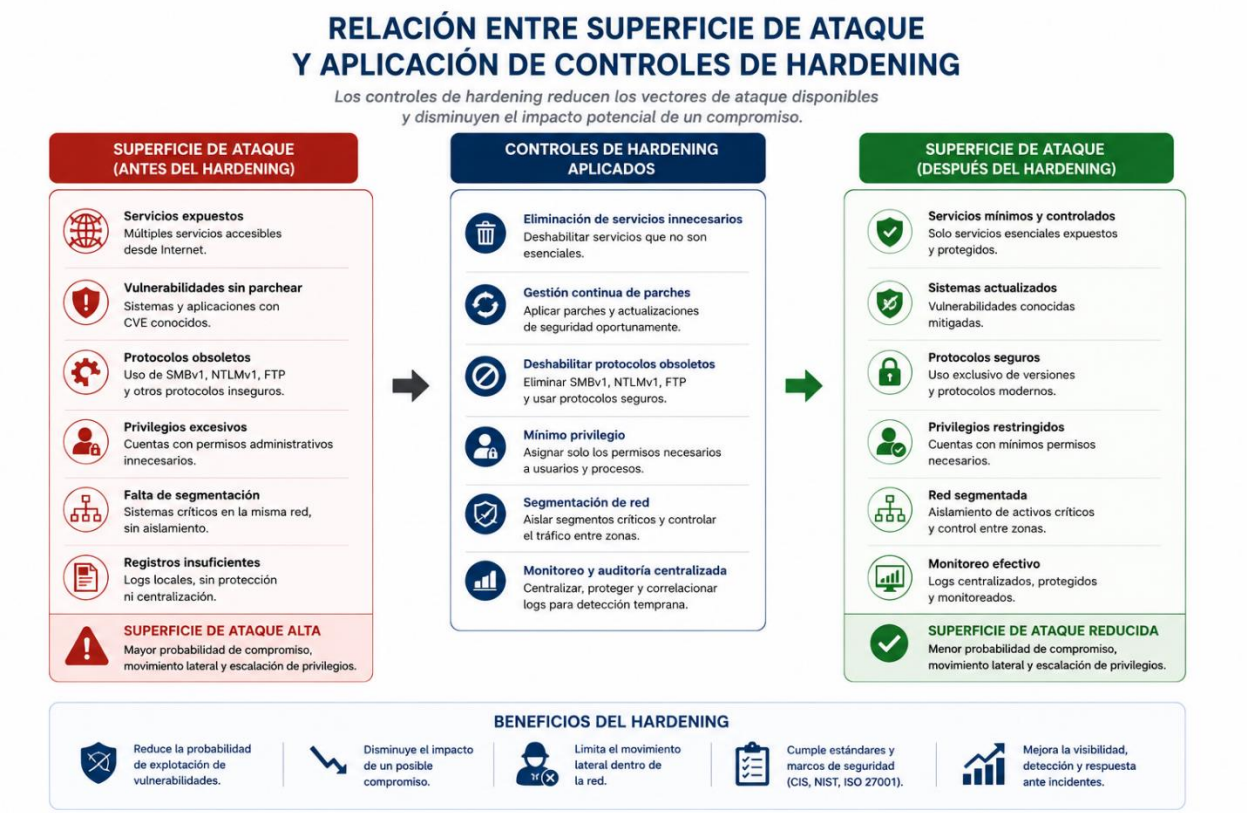
Uno de los hallazgos más relevantes identificados durante el ejercicio fue la explotación de sistemas que mantenían habilitado SMBv1. Aunque este protocolo ha sido catalogado como inseguro desde hace varios años, aún continúa presente en múltiples infraestructuras debido a dependencias heredadas y procesos de modernización incompletos. Microsoft (2023) advierte que SMBv1 carece de múltiples mecanismos de seguridad incorporados en versiones posteriores del protocolo, lo que ha permitido históricamente su utilización como vector de ejecución remota de código y propagación lateral de amenazas. Esta problemática quedó ampliamente evidenciada durante los incidentes globales de WannaCry y NotPetya, donde EternalBlue fue utilizado para comprometer miles de sistemas vulnerables alrededor del mundo (CISA, 2023). En consecuencia, la eliminación de SMBv1 debe considerarse una acción prioritaria de mitigación y no simplemente una recomendación opcional de configuración.

La obtención de privilegios elevados observada durante las actividades de postexplotación también evidenció debilidades relacionadas con la gestión de identidades y permisos administrativos. Una vez que el atacante obtiene acceso inicial, la existencia de privilegios excesivos amplifica considerablemente el impacto potencial del incidente, facilitando actividades de persistencia, evasión de controles y acceso a información sensible. El principio de mínimo privilegio ha sido reconocido por NIST como uno de los mecanismos más efectivos para limitar las capacidades operativas de un atacante dentro de un entorno comprometido (Joint Task

Force, 2020). De forma complementaria, MITRE ATT&CK (2024) documenta que numerosas técnicas de escalación de privilegios dependen directamente de configuraciones inseguras, cuentas sobreprivilegiadas o mecanismos inadecuados de control de acceso.

Figura 15

Relación entre superficie de ataque y aplicación de controles de hardening.



Nota. Elaboración propia.

Además de la gestión de vulnerabilidades y privilegios, el endurecimiento de la infraestructura debe contemplar configuraciones seguras a nivel de sistema operativo, servicios y aplicaciones. CIS (2024) sostiene que la implementación consistente de configuraciones seguras permite reducir significativamente los vectores de ataque disponibles para actores maliciosos. En

este contexto, controles relacionados con deshabilitación de servicios innecesarios, protección de registros de auditoría, fortalecimiento de políticas de autenticación y control de acceso a recursos críticos constituyen elementos esenciales dentro de una estrategia integral de hardening.

Particularmente relevante resulta el control de ejecución de aplicaciones. Durante un incidente real, muchas de las actividades posteriores al acceso inicial dependen de la capacidad del atacante para ejecutar herramientas adicionales dentro del sistema comprometido. NIST (Joint Task Force, 2020) destaca que los mecanismos de application control permiten restringir la ejecución de software no autorizado, reduciendo considerablemente el riesgo asociado a malware, herramientas de postexplotación y ejecución arbitraria de código. Soluciones como AppLocker y Windows Defender Application Control (WDAC) representan ejemplos concretos de controles que habrían dificultado varias de las actividades desarrolladas durante el ejercicio ofensivo.

Tabla 4

Controles de hardening recomendados para la infraestructura analizada

Control	Descripción	Beneficio esperado
Deshabilitar SMBv1	Eliminación de protocolo heredado	Mitigar explotación de MS17-010.
Gestión continua de parches.	Corrección oportuna de vulnerabilidades.	Reducir exposición a CVE Desconocido.

Mínimo privilegio.	Restricción de permisos administrativos.	Limitar escalación de privilegios.
Segmentación de red.	Separación lógica de activos críticos	Reducir movimiento lateral.
Control de aplicaciones.	Protección y monitoreo de registros.	Mejorar capacidades de detección.

Nota. Adaptado del CIS controls v8 (CIS, 2024).

Otro aspecto crítico identificado durante el análisis corresponde a la necesidad de fortalecer los mecanismos de monitoreo y auditoría. La detección efectiva de amenazas depende directamente de la capacidad de observar comportamientos anómalos dentro de la infraestructura. Scarfone y Mell (2007) señalan que la disponibilidad de registros confiables constituye un requisito indispensable para detectar, investigar y responder adecuadamente a incidentes de seguridad. Desde esta perspectiva, la protección de logs, la centralización de eventos y la correlación continua de actividades deben considerarse extensiones naturales de cualquier programa de hardening moderno.

Finalmente, los resultados obtenidos permiten concluir que el hardening no debe entenderse como una actividad puntual ejecutada durante el despliegue inicial de los sistemas. Por el contrario, constituye un proceso continuo de mejora orientado a reducir progresivamente la superficie de ataque de la organización. La combinación entre gestión de vulnerabilidades, control de privilegios, segmentación, monitoreo y configuraciones seguras genera capas

adicionales de protección que dificultan el éxito de futuras actividades ofensivas y fortalecen la resiliencia de la infraestructura frente a amenazas contemporáneas.

Monitoreo y correlación mediante SIEM

La capacidad de recopilar, centralizar y correlacionar eventos de seguridad constituye uno de los componentes más importantes dentro de una estrategia moderna de defensa. Los resultados obtenidos durante el ejercicio Red Team demostraron que actividades como reconocimiento interno, explotación de vulnerabilidades, creación de sesiones remotas, escalación de privilegios y movimiento lateral generan múltiples evidencias distribuidas en diferentes capas de la infraestructura. Sin embargo, cuando estos eventos permanecen aislados en cada sistema, resulta considerablemente más difícil identificar patrones de ataque y responder oportunamente a un incidente. Según Bejtlich (2013), uno de los principales desafíos de los equipos defensivos consiste en transformar grandes volúmenes de registros dispersos en información accionable que permita detectar comportamientos maliciosos.

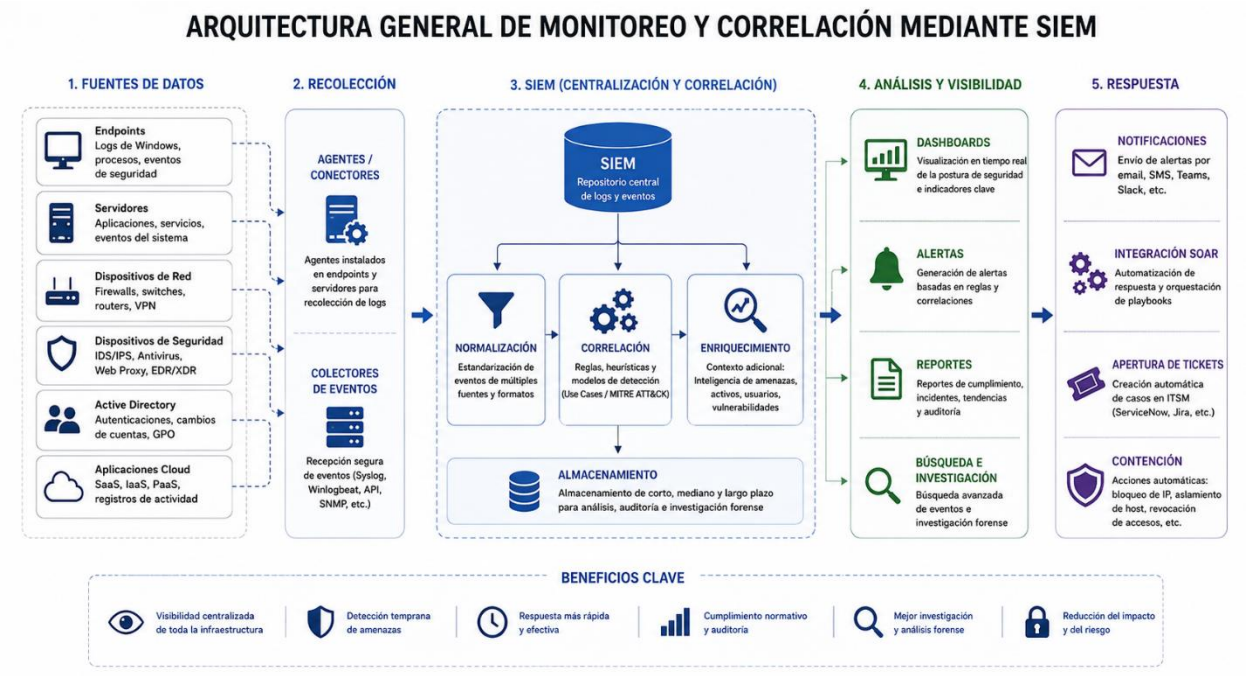
Los sistemas Security Information and Event Management (SIEM) fueron diseñados precisamente para abordar esta problemática. NIST define la correlación de eventos como el proceso mediante el cual múltiples registros provenientes de distintas fuentes son analizados conjuntamente para identificar actividades sospechosas que podrían pasar desapercibidas de forma individual (Kent & Souppaya, 2006). Bajo esta perspectiva, el valor de un SIEM no radica únicamente en almacenar logs, sino en su capacidad para relacionar eventos aparentemente independientes y convertirlos en alertas de seguridad contextualizadas.

Durante el escenario analizado, un atacante exitoso habría generado múltiples evidencias observables desde diferentes componentes de la infraestructura. Por ejemplo, la explotación

inicial de HFS 2.3 habría producido eventos asociados a conexiones remotas, ejecución de procesos y generación de tráfico inusual. Posteriormente, la obtención de una sesión Meterpreter habría generado nuevas actividades relacionadas con ejecución remota de comandos, reconocimiento interno y movimientos entre sistemas comprometidos. MITRE ATT&CK (2024) documenta que las técnicas de Command and Scripting Interpreter, Remote Services y Lateral Tool Transfer generan patrones observables que pueden ser detectados mediante mecanismos adecuados de correlación.

Figura 16

Arquitectura general de monitoreo y correlación mediante SIEM.



Nota. Elaboración propia.

La efectividad de un SIEM depende directamente de la calidad y diversidad de las fuentes de información integradas. Según Chuvakin y Schmidt (2013), las plataformas de monitoreo deben recopilar eventos provenientes de sistemas operativos, dispositivos de red, aplicaciones, mecanismos de autenticación, herramientas de seguridad y plataformas cloud para obtener una visión completa del entorno. Limitar la recolección únicamente a registros tradicionales reduce significativamente la capacidad de detectar ataques complejos que involucran múltiples vectores y sistemas.

Dentro del contexto del laboratorio, las principales fuentes de información habrían estado asociadas a registros del sistema operativo Windows, eventos de autenticación, conexiones de red, actividad de procesos y registros generados por herramientas defensivas desplegadas en la infraestructura. La correlación de estos elementos permitiría reconstruir la secuencia completa del incidente, desde la explotación inicial hasta las actividades de postexplotación y movimiento lateral observadas durante el ejercicio.

Tabla 5

Fuentes de información recomendadas para proceso de correlación

Fuentes de datos	Información obtenida	Utilidad defensiva
Logs de Windows.	Procesos, autenticaciones, eventos de seguridad.	Detección de actividad sospechosa.
Firewalls.	Conexiones entrantes y salientes.	Identificación de comunicaciones anómalas.

IDS/IPS.	Alertas de amenazas conocidas.	Correlación de ataques.
Active Directory.	Cambios de cuentas y privilegios.	Detección de abuso de identidades.
EDR/XDR	Telemetría de endpoints.	Investigación y respuesta.
Aplicaciones.	Eventos específicos del negocio.	Contextualización del incidente.

Nota. Adaptado de Chuvakin y Schmidtt (2013).

Otro aspecto fundamental corresponde a la generación de casos de uso orientados a la detección de amenazas. Un SIEM correctamente implementado no debe limitarse a almacenar registros, sino que debe incorporar reglas capaces de identificar comportamientos asociados a tácticas y técnicas documentadas por marcos como MITRE ATT&CK. Según Strom et al. (2018), el mapeo entre eventos de seguridad y técnicas ATT&CK permite incrementar significativamente la capacidad de detección y priorización de amenazas dentro de los centros de operaciones de seguridad (SOC).

Por ejemplo, durante el escenario desarrollado podrían definirse reglas orientadas a detectar múltiples intentos de conexión sobre servicios vulnerables, creación anómala de procesos, cambios inesperados de privilegios o conexiones entre segmentos de red que

normalmente no deberían comunicarse. La correlación de estos eventos permitiría identificar indicadores tempranos de compromiso antes de que el atacante alcance fases avanzadas del ataque.

Finalmente, los resultados obtenidos evidencian que el monitoreo continuo constituye un componente esencial dentro de cualquier estrategia Blue Team. La combinación entre recolección centralizada de eventos, correlación avanzada, inteligencia de amenazas y monitoreo basado en comportamiento proporciona capacidades significativamente superiores frente a enfoques reactivos centrados únicamente en la revisión manual de registros. En consecuencia, la implementación de un SIEM debe considerarse un mecanismo estratégico para incrementar la visibilidad, acelerar la detección de incidentes y fortalecer la capacidad de respuesta de la organización frente a amenazas actuales.

Segmentación de red y contención de amenazas.

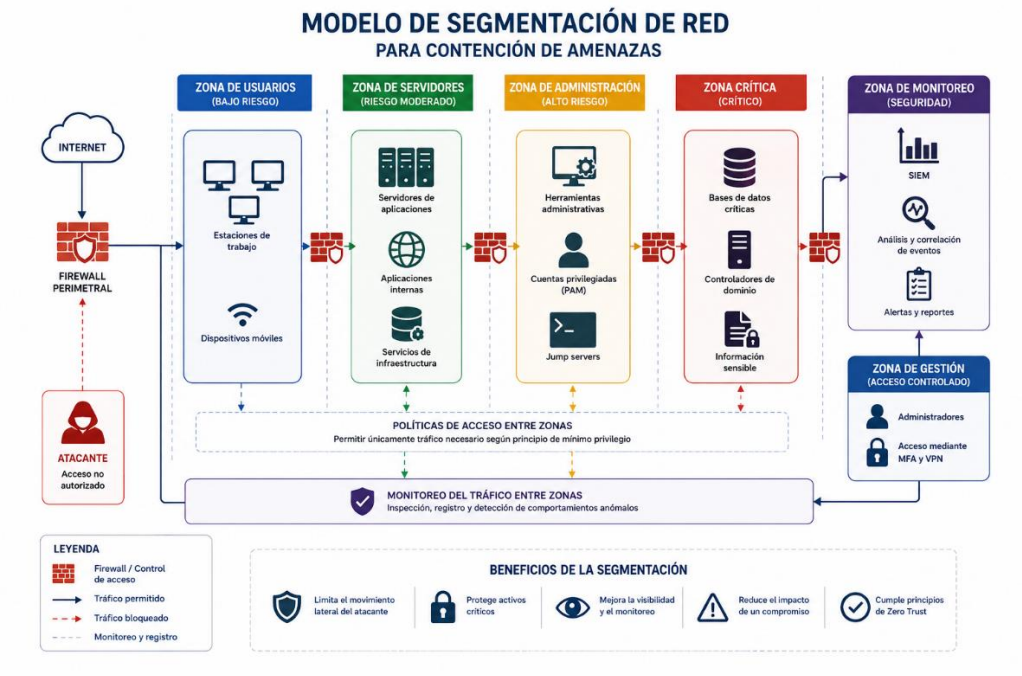
La segmentación de red constituye uno de los mecanismos defensivos más efectivos para limitar la propagación de amenazas dentro de una infraestructura comprometida. Aunque los controles preventivos buscan evitar el acceso inicial de un atacante, la experiencia demuestra que ninguna organización puede asumir que sus mecanismos de protección serán infalibles. Por esta razón, los modelos modernos de seguridad consideran indispensable implementar controles capaces de contener el impacto de un compromiso una vez que este ocurre. Según Rose et al. (2020), los principios asociados a Zero Trust establecen que ningún sistema, usuario o segmento de red debe considerarse confiable por defecto, incluso cuando se encuentra dentro del perímetro corporativo.

Durante el ejercicio desarrollado en SecureNova Labs, la fase de postexplotación permitió demostrar cómo un sistema comprometido puede transformarse en una plataforma para ejecutar actividades de reconocimiento interno, pivoting y movimiento lateral. Una vez obtenida una sesión privilegiada sobre el host vulnerable, fue posible identificar otros activos presentes dentro de la infraestructura y utilizar el sistema inicialmente comprometido como punto de acceso hacia segmentos adicionales de red. Este comportamiento coincide con lo documentado por MITRE ATT&CK (2024), donde las técnicas de Lateral Movement representan una de las principales capacidades utilizadas por actores avanzados para expandir progresivamente el alcance de un ataque.

La ausencia de segmentación efectiva constituye uno de los factores que más favorecen este tipo de escenarios. Cuando todos los activos comparten el mismo dominio de confianza y poseen conectividad irrestricta entre sí, el atacante puede desplazarse lateralmente con relativa facilidad una vez obtiene acceso inicial. Según NIST SP 800-125A, la segmentación permite establecer límites de seguridad entre diferentes zonas de la infraestructura, reduciendo significativamente la superficie disponible para movimientos laterales y compromisos en cascada (Souppaya et al., 2017).

Figura 17

Modelo de segmentación de red para contención de amenazas.



Nota. Elaboración propia.

Desde una perspectiva defensiva, la segmentación debe diseñarse considerando el nivel de criticidad de los activos y los flujos legítimos de comunicación requeridos por la operación. No todos los sistemas necesitan comunicarse entre sí, y asumir conectividad total dentro de la infraestructura incrementa innecesariamente la superficie de ataque. Rose et al. (2020) argumentan que la aplicación de controles de acceso basados en identidad, contexto y necesidad operativa permite reducir significativamente las oportunidades disponibles para un atacante que ya se encuentra dentro de la red.

Un aspecto particularmente relevante identificado durante el laboratorio corresponde a la necesidad de aislar sistemas críticos de los segmentos de usuario. Durante numerosos incidentes reales, el compromiso inicial suele ocurrir sobre estaciones de trabajo o servidores con

exposición externa, mientras que los activos de mayor valor permanecen ubicados en segmentos internos. Sin embargo, cuando no existen mecanismos adecuados de segmentación, un atacante puede utilizar el sistema comprometido como punto de tránsito hacia bases de datos, controladores de dominio o aplicaciones críticas. CISA (2023) destaca que la segmentación continúa siendo una de las medidas más efectivas para limitar el impacto operativo de ataques de ransomware y amenazas persistentes avanzadas.

Además de la separación lógica entre zonas, la segmentación moderna debe complementarse con mecanismos de microsegmentación. Según Shackleford (2022), la microsegmentación permite definir políticas específicas entre cargas de trabajo individuales, restringiendo las comunicaciones exclusivamente a los flujos estrictamente necesarios para la operación. Este enfoque resulta especialmente relevante en infraestructuras virtualizadas, centros de datos modernos y entornos cloud-native, donde los límites tradicionales de red han perdido gran parte de su efectividad.

Tabla 6

Ejemplo de segmentación recomendada para la infraestructura analizada.

Segmento.	Activos incluidos.	Nivel de acceso.
Zona de usuarios.	Estaciones de trabajo.	Acceso restringido.
Zona de servidores.	Apllicaciones corporativas.	Acceso controlado.

Zona de administración.	Herramientas administrativas.	Acceso privilegiado.
Zona crítica.	Bases de datos y activos sensbles.	Acceso altamente restringido.
Zona de monitoreo.	SIEM, logs y herramientas defensivas.	Acceso controlado.

Nota. Elaboración propia.

La efectividad de la segmentación depende también de la capacidad de monitorear las comunicaciones entre zonas. Un segmento aislado, pero no monitoreado puede convertirse en un punto ciego dentro de la infraestructura. Por esta razón, NIST (Rose et al., 2020) recomienda complementar la segmentación con capacidades de inspección, registro y análisis continuo del tráfico que atraviesa los diferentes límites de seguridad definidos por la organización. Este enfoque permite identificar comportamientos anómalos y detectar intentos de movimiento lateral antes de que alcancen activos críticos.

Finalmente, los resultados obtenidos durante el ejercicio demuestran que la segmentación no debe entenderse únicamente como una práctica de diseño de red, sino como un mecanismo estratégico de contención. La combinación entre segmentación tradicional, microsegmentación, monitoreo continuo y principios Zero Trust permite reducir significativamente la capacidad de propagación de una amenaza dentro de la infraestructura. En consecuencia, incluso cuando un atacante logra comprometer un sistema inicial, la organización conserva mayores probabilidades

de limitar el alcance del incidente y proteger los activos más críticos para la operación del negocio.

Seguridad cloud-native y observabilidad basada en eBPF.

La evolución de las infraestructuras tecnológicas hacia arquitecturas basadas en contenedores, microservicios y plataformas cloud-native ha generado nuevos desafíos para las estrategias tradicionales de monitoreo y seguridad. Los mecanismos convencionales de supervisión, diseñados originalmente para entornos monolíticos y servidores estáticos, presentan limitaciones para proporcionar visibilidad adecuada sobre cargas de trabajo altamente dinámicas que pueden crearse, modificarse o eliminarse en cuestión de segundos. Según Burns et al. (2016), la adopción masiva de plataformas de orquestación como Kubernetes ha transformado la manera en que las organizaciones despliegan aplicaciones, exigiendo nuevos enfoques para la observabilidad, detección de amenazas y protección de cargas de trabajo.

La observabilidad se ha convertido en un componente fundamental de la seguridad moderna. Mientras que el monitoreo tradicional se centra en la supervisión de eventos previamente definidos, la observabilidad busca proporcionar visibilidad suficiente para comprender comportamientos inesperados dentro de sistemas complejos. Gregg (2020) señala que la observabilidad permite responder preguntas sobre el comportamiento interno de una plataforma incluso cuando no se habían previsto escenarios específicos durante su diseño, proporcionando capacidades superiores para detección de anomalías y análisis de incidentes.

Una de las tecnologías que ha impulsado significativamente este enfoque es Extended Berkeley Packet Filter (eBPF). Originalmente concebido para el procesamiento eficiente de paquetes de red dentro del kernel de Linux, eBPF evolucionó hasta convertirse en una plataforma

capaz de ejecutar programas seguros directamente en el espacio del kernel sin necesidad de modificar el sistema operativo. Según Gregg (2020), esta capacidad permite observar procesos, llamadas al sistema, conexiones de red y actividades del sistema con niveles de visibilidad que anteriormente requerían modificaciones complejas o agentes altamente invasivos.

eBPF ofrece una ventaja particularmente relevante: la posibilidad de observar comportamientos en tiempo real directamente desde el núcleo del sistema operativo. Esto permite identificar actividades asociadas a ejecución de procesos sospechosos, conexiones no autorizadas, modificaciones de archivos críticos y comportamientos compatibles con técnicas documentadas por MITRE ATT&CK (2024). A diferencia de los enfoques tradicionales basados exclusivamente en logs, la observación directa de eventos a nivel kernel proporciona una fuente de telemetría significativamente más rica para actividades de detección e investigación.

Figura 18

Arquitectura de observabilidad basada en eBPF para detección de amenazas.

Nota. Elaboración propia con base en Gregg (2020) y CNCF (2023).

La adopción de eBPF ha resultado especialmente relevante dentro de entornos Kubernetes y arquitecturas cloud-native. Según la Cloud Native Computing Foundation (CNCF, 2023), las plataformas modernas requieren mecanismos de observabilidad capaces de adaptarse dinámicamente a entornos distribuidos donde los límites tradicionales de red, host y aplicación ya no son suficientes para comprender el comportamiento de las cargas de trabajo. Bajo esta perspectiva, eBPF permite capturar telemetría directamente desde nodos, contenedores y procesos sin depender exclusivamente de agentes desplegados dentro de cada carga de trabajo.

Durante el análisis realizado en SecureNova Labs se evidenció cómo múltiples actividades ofensivas generaban comportamientos observables a nivel de sistema operativo. La ejecución de exploits, la creación de procesos remotos, las conexiones de red asociadas al movimiento lateral y las actividades de postexplotación representan eventos que podrían ser detectados mediante plataformas de observabilidad basadas en eBPF. Esta capacidad incrementa significativamente la visibilidad disponible para los equipos Blue Team, permitiendo identificar actividades anómalas antes de que alcancen fases avanzadas del ataque.

Otro aspecto relevante corresponde al impacto operativo de los mecanismos de observabilidad. Tradicionalmente, las organizaciones debían elegir entre obtener altos niveles de visibilidad o minimizar el consumo de recursos generado por agentes de monitoreo. Gregg (2020) argumenta que eBPF reduce significativamente esta problemática debido a que gran parte del procesamiento ocurre directamente dentro del kernel, disminuyendo la necesidad de capturar y transferir grandes volúmenes de información hacia componentes externos. Esto permite implementar capacidades avanzadas de observabilidad con un impacto considerablemente menor sobre el rendimiento de los sistemas monitoreados.

Tabla 7

Comparación entre monitoreo tradicional y observabilidad basada en eBPF.

Característica.	Monitoreo tradicional.	Observabilidad con eBPF.
Nivel de visibilidad.	Aplicación y logs.	Kernel, procesos, red y aplicaciones.

Dependencia de agente.	Alta.	Reducida.
Telemetría en tiempo real.	Limitada	Alta
Detección de comportamiento.	Parcial.	Avanzada.
Adaptación a Kubernetes.	Moderada.	Alta.
Impacto operativo.	Medio-Alto.	Bajo-medio.

Nota. Adaptado de Gregg (2020) y CNCF (2023).

la incorporación de capacidades de observabilidad basadas en eBPF representa una evolución natural de las estrategias modernas de defensa. La combinación entre monitoreo tradicional, correlación mediante SIEM, análisis de comportamiento y observabilidad a nivel kernel proporciona una capacidad significativamente superior para detectar amenazas avanzadas, investigar incidentes y fortalecer la resiliencia de infraestructuras cloud-native frente a escenarios de compromiso similares a los observados durante el presente ejercicio.

Tetragon y Falco como mecanismos de Runtime Security

La creciente adopción de arquitecturas basadas en contenedores y Kubernetes ha impulsado la necesidad de implementar mecanismos de seguridad capaces de detectar amenazas durante la ejecución de las cargas de trabajo. Aunque controles como el hardening, el escaneo de vulnerabilidades y la gestión de configuraciones seguras reducen significativamente la superficie de ataque, estos mecanismos no son suficientes para identificar comportamientos maliciosos que ocurren una vez una aplicación ya se encuentra en ejecución. Según la Cloud Native Computing Foundation (CNCF, 2023), las capacidades de runtime security se han convertido en un componente esencial para proteger entornos cloud-native frente a amenazas que logran evadir los controles preventivos tradicionales.

Herramientas como Falco y Tetragon han ganado relevancia debido a su capacidad para observar actividades ejecutadas en tiempo real dentro de sistemas Linux, contenedores y clústeres Kubernetes. Ambas soluciones permiten detectar comportamientos sospechosos asociados a procesos, conexiones de red, acceso a archivos sensibles y modificaciones sobre componentes críticos del sistema operativo. Sin embargo, aunque comparten objetivos similares, sus enfoques técnicos presentan diferencias importantes que impactan directamente las capacidades de observabilidad y detecciones disponibles para los equipos Blue Team.

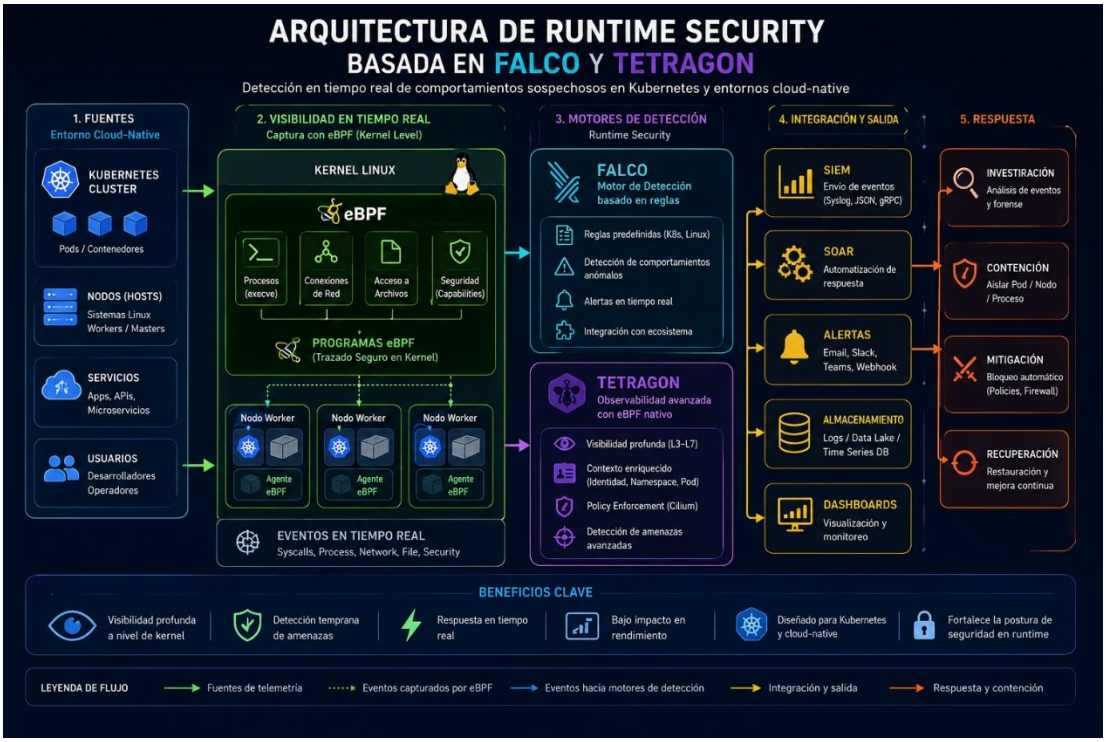
Falco fue desarrollado originalmente por Sysdig y posteriormente incorporado como proyecto incubado dentro de la CNCF. Según Falco Project (2024), su principal objetivo consiste en detectar comportamientos anómalos mediante reglas que analizan eventos generados por el sistema operativo, permitiendo identificar actividades asociadas a ejecución de shells interactivas, escalación de privilegios, modificaciones sospechosas de archivos y accesos no autorizados dentro de contenedores. Esta capacidad convierte a Falco en una herramienta

especialmente útil para implementar detección basada en comportamiento dentro de plataformas Kubernetes.

Por otra parte, Tetragon adopta un enfoque diferente basado completamente en eBPF. Según Isovalent (2024), Tetragon permite observar eventos directamente desde el kernel de Linux, proporcionando visibilidad detallada sobre procesos, syscalls, conexiones de red y actividades ejecutadas dentro de los contenedores. A diferencia de enfoques basados principalmente en reglas estáticas, Tetragon aprovecha la capacidad de eBPF para capturar información contextual de alto valor directamente desde la fuente donde ocurre el evento, incrementando significativamente la calidad de la telemetría disponible para procesos de detección e investigación.

Figura 19

Arquitectura de Runtime Security basada en Falco y Tetragon.



Nota. Elaboración propia con base en Falco Project (2024) e Isovalent (2024).

La utilidad práctica de estas herramientas puede relacionarse directamente con múltiples actividades observadas durante el ejercicio desarrollado en SecureNova Labs. Por ejemplo, la ejecución de procesos asociados a herramientas de postexplotación, la apertura de conexiones de red inesperadas, la modificación de archivos sensibles o la ejecución de comandos privilegiados representan comportamientos que podrían ser detectados mediante reglas Falco o políticas de observación implementadas en Tetragon. MITRE ATT&CK (2024) documenta que gran parte de las actividades asociadas a ejecución, persistencia y movimiento lateral generan eventos observables a nivel de sistema operativo, lo que convierte a estas plataformas en componentes valiosos para la detección temprana de amenazas.

Desde una perspectiva operacional, Falco destaca por su simplicidad de adopción y su amplio ecosistema de reglas predefinidas orientadas a Kubernetes. Sin embargo, Tetragon proporciona capacidades de observabilidad considerablemente más profundas debido a su integración nativa con eBPF y su capacidad para capturar contexto adicional sobre cada evento generado. Según Gregg (2020), la observación directa desde el kernel reduce significativamente los puntos ciegos presentes en soluciones tradicionales de monitoreo y proporciona información más precisa para actividades de investigación y respuesta.

Tabla 8

Comparación entre Falco y Tetragon para entornos Kubernetes.

Característica.	Falco.	Tetragon.
Proyecto.	CNCF.	Isovalent/Cilium.
Tecnología principal.	Syscalls y reglas.	eBPF Nativo.
Observabilidad de procesos.	Alta.	Muy alta.
Observabilidad de red.	Limitada.	Avanzada.
Contexto de ejecución.	Medio.	Alto.
Integración con Kubernetes.	Alto.	Alto.
Curva de aprendizaje.	Baja.	Media.

Capacidades de investigacion.	Buenas.	Avanzadas.

Nota. Adaptado de Falco Project (2024) e Isovalent (2024).

Un aspecto particularmente relevante para los equipos Blue Team corresponde a la capacidad de transformar eventos técnicos en acciones de respuesta. Tanto Falco como Tetragon pueden integrarse con plataformas SIEM, sistemas SOAR y mecanismos automatizados de respuesta ante incidentes. Esto permite que una actividad sospechosa identificada dentro de un contenedor genere alertas, active procesos de investigación o incluso desencadene acciones automáticas de contención. Según CNCF (2023), la integración entre observabilidad, runtime security y automatización representa una de las tendencias más importantes dentro de las estrategias modernas de protección cloud-native.

Finalmente, la incorporación de herramientas como Falco y Tetragon fortalece significativamente la capacidad de detectar actividades maliciosas que ocurren después del acceso inicial del atacante. Mientras los controles preventivos buscan reducir la probabilidad de compromiso, las plataformas de runtime security permiten observar el comportamiento real de las cargas de trabajo durante su ejecución, proporcionando una capa adicional de protección frente a amenazas avanzadas. En consecuencia, la combinación entre observabilidad basada en eBPF, monitoreo continuo y capacidades de respuesta automatizada constituye un componente fundamental dentro de cualquier arquitectura moderna de ciberseguridad orientada a entornos Kubernetes y cloud-native.

Fortalecimiento de la resiliencia organizacional.

La resiliencia organizacional en ciberseguridad puede definirse como la capacidad de una organización para anticipar, resistir, responder y recuperarse de incidentes que afecten la confidencialidad, integridad o disponibilidad de sus activos digitales. A diferencia de los enfoques tradicionales centrados exclusivamente en la prevención, los modelos modernos de seguridad reconocen que los incidentes son inevitables y que, por tanto, la capacidad de recuperación resulta tan importante como la capacidad de protección. Según Linkov y Kott (2019), las organizaciones resilientes no son aquellas que nunca sufren incidentes, sino aquellas capaces de mantener sus funciones críticas incluso bajo condiciones de compromiso.

Los resultados obtenidos durante el desarrollo de SecureNova Labs permitieron evidenciar cómo una vulnerabilidad aparentemente aislada puede evolucionar progresivamente hacia escenarios de mayor impacto cuando no existen mecanismos adecuados de detección, contención y respuesta. La explotación inicial del servicio vulnerable, seguida por actividades de escalación de privilegios y movimiento lateral, demostró que la seguridad no puede depender exclusivamente de controles preventivos. En consecuencia, la resiliencia debe construirse mediante la integración coordinada de capacidades ofensivas, defensivas y forenses que permitan identificar debilidades antes de que sean aprovechadas por actores maliciosos.

Desde esta perspectiva, las actividades Red Team desempeñan un papel fundamental dentro del fortalecimiento de la postura de seguridad organizacional. Según NIST SP 800-115 (Scarfone et al., 2008), los ejercicios de pruebas de penetración permiten identificar vulnerabilidades técnicas, errores de configuración y debilidades operativas que frecuentemente permanecen ocultas durante las evaluaciones tradicionales de cumplimiento. La explotación

controlada de estas debilidades proporciona información valiosa para priorizar inversiones de seguridad y mejorar los mecanismos de protección existentes.

Sin embargo, la resiliencia no puede construirse únicamente a partir de capacidades ofensivas. La capacidad de detección temprana, monitoreo continuo y respuesta estructurada representa un componente igualmente importante dentro de la estrategia defensiva. Como se evidenció durante las secciones anteriores, mecanismos como SIEM, análisis forense digital, segmentación de red, hardening y observabilidad basada en eBPF permiten reducir significativamente el tiempo requerido para identificar y contener un incidente. Según Cichonski et al. (2012), la reducción del tiempo de detección y respuesta constituye uno de los factores que más influyen en la disminución del impacto operativo de un compromiso de seguridad.

Figura 20

Modelo integrado de resiliencia organizacional en ciberseguridad.

Nota. Elaboración propia con base en NIST SP 800-61 (Cichonski et al., 2012), NIST SP 800-115 (Scarfone et al., 2008) y Linkov y Kott (2019).

Un elemento particularmente relevante dentro de la resiliencia organizacional corresponde a la capacidad de transformar incidentes en oportunidades de mejora continua. Cada vulnerabilidad identificada, cada técnica ofensiva observada y cada indicador de compromiso detectado proporciona información que puede utilizarse para fortalecer controles existentes y desarrollar nuevas capacidades defensivas. Este enfoque coincide con el concepto de aprendizaje organizacional propuesto por Linkov y Kott (2019), quienes sostienen que la adaptación continua constituye uno de los principales diferenciadores entre organizaciones resilientes y organizaciones vulnerables.

Asimismo, la resiliencia requiere la integración efectiva entre personas, procesos y tecnología. La implementación de herramientas avanzadas carece de valor cuando no existen procedimientos claramente definidos para responder a incidentes o cuando el personal responsable no posee las competencias necesarias para interpretar adecuadamente la información disponible. Según NIST (Joint Task Force, 2020), la efectividad de un programa de seguridad depende de la capacidad de coordinar controles técnicos, procesos operativos y capacidades humanas dentro de una estrategia unificada de gestión del riesgo.

Tabla 9

Contribución de los componentes analizados al fortalecimiento de la resiliencia organizacional.

Componente.	Función principal.	Contribución a la resiliencia.
Red team.	Identificación de vulnerabilidades.	Descubrimiento de debilidades.
DFIR	Investigación de incidentes.	Comprensión del compromiso.
Hardening.	Reducción de superficie de ataque.	Disminución de riesgos de explotación.
SIEM.	Monitoreo y correlación.	Detección temprana.
Segmentación.	Contención de amenazas.	Limitación del movimiento lateral.

eBPF.	Observabilidad avanzada.	Visibilidad profunda.
Falto y Tetragon.	Runtime Security.	Detección en tiempo real.
Respuesta a incidentes.	Gestión operativa.	Recuperación y continuidad.

Nota. Elaboración propia.

Los resultados obtenidos permiten concluir que la resiliencia organizacional no debe entenderse como un estado final alcanzable, sino como un proceso continuo de adaptación frente a amenazas en constante evolución. La combinación entre pruebas ofensivas, monitoreo continuo, análisis forense, segmentación, observabilidad avanzada y capacidades de respuesta constituye una estrategia integral capaz de incrementar significativamente la capacidad de las organizaciones para resistir, contener y recuperarse de incidentes de ciberseguridad. Bajo este enfoque, la resiliencia se convierte en el resultado natural de una postura de seguridad madura, dinámica y orientada a la mejora continua.

Análisis integral del incidente.

Reconstrucción de la cadena de ataque y mapeo a MITRE ATT&CK.

Uno de los principales objetivos de un proceso de análisis de incidentes consiste en comprender cómo se desarrolló el compromiso desde el acceso inicial hasta las acciones finales ejecutadas por el atacante. Más allá de identificar vulnerabilidades individuales, resulta fundamental reconstruir la secuencia completa de eventos para comprender los mecanismos

utilizados, las debilidades explotadas y las oportunidades de detección que existieron durante cada etapa del ataque. Según Strom et al. (2018), el marco MITRE ATT&CK proporciona una metodología estructurada para clasificar tácticas, técnicas y procedimientos utilizados por actores maliciosos, facilitando el análisis sistemático de incidentes y el fortalecimiento de capacidades defensivas.

El escenario desarrollado en SecureNova Labs evidenció una cadena de ataque compuesta por múltiples fases consecutivas que permitieron al atacante incrementar progresivamente su nivel de acceso dentro de la infraestructura. El proceso inició mediante actividades de reconocimiento orientadas a identificar servicios expuestos, versiones vulnerables y posibles vectores de compromiso. Durante esta fase se emplearon técnicas de descubrimiento de servicios y enumeración de puertos que permitieron identificar la presencia de HFS 2.3 dentro del entorno analizado. MITRE ATT&CK clasifica estas actividades dentro de la táctica Reconnaissance, particularmente mediante técnicas asociadas a Active Scanning (T1595) y Gather Victim Network Information (T1590) (MITRE ATT&CK, 2024).

Posteriormente, el atacante aprovechó una vulnerabilidad conocida presente en HFS 2.3 para obtener acceso inicial al sistema comprometido. Esta acción permitió la ejecución remota de comandos y el establecimiento de una sesión interactiva sobre el host vulnerable. Según MITRE ATT&CK (2024), este comportamiento se encuentra alineado con las tácticas Initial Access y Execution, particularmente mediante Exploit Public-Facing Application (T1190) y Command and Scripting Interpreter (T1059). La explotación exitosa evidenció la ausencia de controles adecuados de actualización y gestión de vulnerabilidades dentro del entorno objetivo.

Una vez obtenido acceso inicial, las actividades ofensivas evolucionaron hacia escenarios de postexplotación orientados a incrementar privilegios y ampliar el control sobre el sistema afectado. Durante esta fase se estableció una sesión Meterpreter y posteriormente se obtuvo

acceso con privilegios elevados. MITRE ATT&CK (2024) documenta este comportamiento dentro de las tácticas Privilege Escalation y Persistence, las cuales permiten a un atacante aumentar sus capacidades operativas y mantener acceso prolongado dentro de la infraestructura comprometida.

Figura 21

Cadena completa de ataque mapeada contra MITRE ATT&CK

Nota. Elaboración propia con base en NIST SP 800-61 (Cichonski et al., 2012), NIST SP 800-115 (Scarfone et al., 2008) y Linkov y Kott (2019).

La fase más crítica del incidente correspondió al movimiento lateral hacia otros sistemas presentes dentro de la infraestructura. Aprovechando la conectividad existente entre segmentos de red y la presencia de sistemas vulnerables a MS17-010, fue posible expandir el compromiso más allá del host inicialmente afectado. Este comportamiento coincide con las tácticas Lateral Movement y Discovery descritas por MITRE ATT&CK (2024), donde técnicas como Remote

Services (T1021), Network Service Discovery (T1046) y Exploitation of Remote Services (T1210) son utilizadas para incrementar progresivamente el alcance operativo del ataque.

Desde una perspectiva defensiva, resulta particularmente relevante observar que cada una de estas fases generó indicadores de compromiso susceptibles de ser detectados mediante mecanismos adecuados de monitoreo. La ejecución de procesos anómalos, las conexiones remotas, la creación de nuevas sesiones privilegiadas y los intentos de acceso a sistemas internos representan evidencias que podrían haber sido identificadas mediante correlación de eventos, observabilidad basada en eBPF o plataformas de runtime security como Falco y Tetragon. Según CISA (2023), la detección temprana durante las fases iniciales del ataque constituye uno de los factores que más influye en la reducción del impacto operativo de un incidente.

Tabla 10

Mapeo de actividades observadas contra MITRE ATT&CK

Fase del incidente	Actividad observada	Táctica ATT&CK	Técnica ATT&CK
Reconocimiento	Escaneo de puertos con Nmap	Reconnaissance	T1595
Enumeración	Identificación de servicios vulnerables	Reconnaissance	T1590
Acceso inicial	Explotación de HFS 2.3	Initial Access	T1190
Ejecución	Obtención de reverse shell	Execution	T1059
Escalación	Obtención de privilegios SYSTEM	Privilege Escalation	T1068
Descubrimiento	Reconocimiento interno	Discovery	T1046

Fase del incidente	Actividad observada	Táctica ATT&CK	Técnica ATT&CK
Movimiento lateral	Explotación de MS17-010	Lateral Movement	T1210
Postexplotación	Control remoto del sistema	Command and Control	T1105

Nota. Adaptado de MITRE ATT&CK Enterprise Matrix (2024).

El análisis integral de la cadena de ataque permite concluir que el compromiso observado no fue consecuencia de una única vulnerabilidad aislada, sino del encadenamiento de múltiples debilidades presentes en diferentes capas de la infraestructura. La combinación entre servicios vulnerables, protocolos inseguros, privilegios excesivos y ausencia de segmentación efectiva facilitó la progresión del ataque desde una fase inicial de reconocimiento hasta escenarios avanzados de movimiento lateral. Esta situación demuestra la importancia de implementar estrategias de defensa en profundidad capaces de interrumpir la cadena de ataque en múltiples puntos antes de que el incidente alcance activos críticos para la organización.

Análisis del impacto técnico sobre la confidencialidad, integridad y disponibilidad.

La evaluación del impacto constituye una de las actividades más importantes dentro del análisis de incidentes, debido a que permite determinar las consecuencias reales derivadas del compromiso de una infraestructura tecnológica. Más allá de identificar vulnerabilidades o reconstruir la secuencia de ataque, resulta necesario comprender cómo las acciones ejecutadas

por el atacante afectan los principios fundamentales de seguridad de la información. Según Stallings (2018), la confidencialidad, la integridad y la disponibilidad conforman los tres pilares esenciales sobre los cuales se construyen los programas modernos de protección de información, siendo comúnmente conocidos como la tríada CIA (Confidentiality, Integrity and Availability).

En el escenario desarrollado durante SecureNova Labs, la explotación inicial del servicio HFS 2.3 permitió al atacante obtener acceso remoto sobre el sistema vulnerable, generando una afectación directa sobre el principio de confidencialidad. Una vez comprometido el host, fue posible ejecutar comandos arbitrarios, visualizar información del sistema y acceder a recursos internos previamente restringidos. Según NIST (Joint Task Force, 2020), la pérdida de confidencialidad ocurre cuando individuos, procesos o sistemas no autorizados obtienen acceso a información que debería permanecer protegida. Aunque el laboratorio fue ejecutado en un entorno controlado, las técnicas utilizadas reproducen escenarios observados frecuentemente en incidentes reales donde el objetivo principal consiste en acceder a información sensible de carácter corporativo.

La integridad también se vio potencialmente comprometida durante diversas fases del ejercicio ofensivo. La capacidad de ejecutar comandos remotos con privilegios elevados implica que un atacante podría modificar configuraciones del sistema operativo, alterar registros de auditoría, manipular archivos críticos o instalar mecanismos de persistencia. Según Whitman y Mattord (2022), la pérdida de integridad ocurre cuando la información es modificada de manera no autorizada, afectando su exactitud, consistencia o confiabilidad. Esta situación resulta particularmente crítica en entornos empresariales donde decisiones operativas dependen directamente de la precisión de los datos almacenados.

La obtención de privilegios NT AUTHORITY\SYSTEM durante las actividades de postexplotación representa uno de los eventos con mayor impacto potencial sobre la integridad

del entorno. MITRE ATT&CK (2024) documenta que los atacantes frecuentemente utilizan privilegios elevados para modificar configuraciones de seguridad, evadir mecanismos de detección y alterar registros utilizados posteriormente durante investigaciones forenses. Bajo estas circunstancias, el impacto ya no se limita al sistema inicialmente comprometido, sino que puede extenderse progresivamente a otros activos de la infraestructura.

Figura 22

Impacto del incidente sobre la tríada CIA (Confidencialidad, Integridad y Disponibilidad).

Nota. Elaboración propia con base en Stallings (2018) y NIST SP 800-53 Rev. 5 (Joint Task Force, 2020).

El tercer componente afectado corresponde a la disponibilidad. Aunque durante el ejercicio no se ejecutaron acciones orientadas a provocar interrupciones deliberadas del servicio, la explotación exitosa de vulnerabilidades críticas y la posibilidad de ejecutar código arbitrario

habrían permitido a un atacante generar indisponibilidad parcial o total de los sistemas comprometidos. Según CISA (2023), muchas campañas modernas de ransomware utilizan inicialmente técnicas similares a las observadas en este laboratorio para posteriormente ejecutar acciones orientadas a cifrar sistemas, destruir información o interrumpir operaciones críticas.

Particularmente relevante resulta el análisis del movimiento lateral observado durante la explotación de MS17-010. La capacidad de comprometer múltiples sistemas dentro de una misma infraestructura incrementa exponencialmente el impacto potencial sobre la disponibilidad organizacional. Como demostraron incidentes históricos como WannaCry y NotPetya, una vulnerabilidad explotada de forma masiva puede generar interrupciones operativas de gran escala cuando no existen mecanismos adecuados de segmentación y contención (Greenberg, 2018). Esta situación evidencia que la disponibilidad no depende únicamente de la robustez individual de un sistema, sino también de la capacidad de la organización para limitar la propagación de amenazas dentro de su infraestructura.

Tabla 11

Evaluación del impacto observado sobre la tríada CIA.

Principio	Evidencia observada	Impacto potencial
Confidencialidad	Acceso remoto al sistema y reconocimiento interno	Exposición de información sensible
Integridad	Ejecución de comandos y escalación de privilegios	Modificación no autorizada de datos y configuraciones
Disponibilidad	Explotación de vulnerabilidades críticas y movimiento lateral	Interrupción parcial o total de servicios

Principio	Evidencia observada	Impacto potencial
Autenticidad	Uso de sesiones privilegiadas comprometidas	Suplantación de usuarios o servicios
Trazabilidad	Posible alteración de registros y evidencias	Dificultad para investigaciones posteriores

Nota. Elaboración propia.

El análisis de impacto demuestra que las consecuencias de un incidente no dependen exclusivamente de la vulnerabilidad explotada, sino de la combinación entre capacidades ofensivas, arquitectura de red, controles defensivos y capacidad de respuesta. La presencia simultánea de servicios vulnerables, privilegios excesivos y ausencia de segmentación efectiva permitió incrementar progresivamente el alcance potencial del compromiso. Esta situación coincide con lo señalado por NIST (Joint Task Force, 2020), donde se establece que el impacto de un incidente debe evaluarse considerando tanto los activos directamente afectados como los efectos secundarios que pueden extenderse a otros componentes de la organización.

En consecuencia, los resultados obtenidos evidencian que la protección efectiva de la confidencialidad, integridad y disponibilidad requiere un enfoque integral que combine prevención, detección, contención y recuperación. La implementación aislada de controles individuales resulta insuficiente cuando los atacantes son capaces de encadenar múltiples técnicas para avanzar dentro de la infraestructura. Por esta razón, el fortalecimiento de la resiliencia organizacional debe orientarse a proteger simultáneamente los tres pilares fundamentales de la seguridad de la información y no únicamente aquellos asociados al acceso inicial o la explotación de vulnerabilidades.

Impacto organizacional, operativo y estratégico del incidente.

Si bien las vulnerabilidades explotadas durante el laboratorio fueron analizadas desde una perspectiva eminentemente técnica, las consecuencias reales de un incidente de seguridad trascienden ampliamente los sistemas comprometidos. Actualmente, los activos digitales soportan procesos críticos de negocio, operaciones financieras, gestión documental, comunicaciones corporativas y toma de decisiones estratégicas. Por esta razón, una afectación tecnológica puede transformarse rápidamente en un problema operativo, financiero, regulatorio e incluso reputacional. Según Von Solms y Van Niekerk (2013), la ciberseguridad dejó de ser un problema exclusivamente técnico para convertirse en un componente fundamental de la gestión organizacional y del gobierno corporativo.

El escenario desarrollado evidenció cómo una vulnerabilidad expuesta a Internet permitió obtener acceso inicial a la infraestructura y posteriormente avanzar hacia sistemas internos mediante técnicas de movimiento lateral. Aunque el ejercicio fue realizado dentro de un entorno controlado, un incidente similar en una organización real podría generar interrupciones operativas significativas, especialmente cuando los sistemas afectados soportan procesos esenciales para el negocio. NIST señala que el impacto de un incidente debe evaluarse considerando no solamente los activos tecnológicos comprometidos, sino también los procesos organizacionales que dependen de dichos activos para su funcionamiento normal (Joint Task Force, 2020).

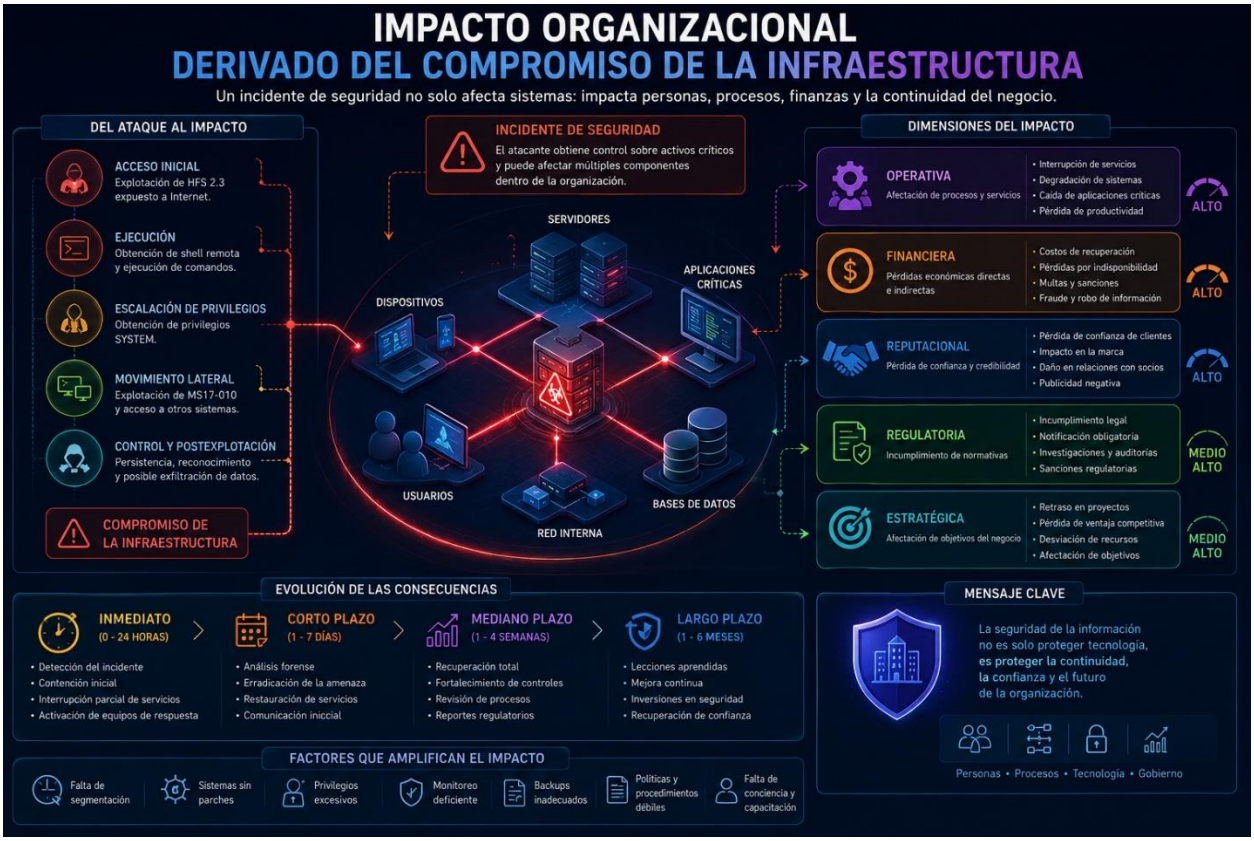
Desde una perspectiva operativa, la explotación de sistemas vulnerables puede provocar degradación de servicios, indisponibilidad temporal de aplicaciones críticas o interrupción de procesos de negocio. Esta situación resulta particularmente relevante en organizaciones que

dependen de la disponibilidad continua de plataformas tecnológicas para atender clientes, procesar transacciones o ejecutar actividades productivas. Según ENISA (2023), la interrupción de servicios continúa siendo una de las principales consecuencias observadas durante incidentes de seguridad de alto impacto, especialmente cuando los atacantes logran expandirse hacia múltiples sistemas dentro de la infraestructura.

El impacto financiero también representa una consecuencia relevante derivada de este tipo de incidentes. La recuperación de sistemas comprometidos, la ejecución de investigaciones forenses, la implementación de medidas de remediación y las pérdidas asociadas a la interrupción operativa generan costos directos e indirectos que pueden afectar significativamente a una organización. El estudio anual de IBM Security (2024) indica que los costos asociados a incidentes de seguridad continúan incrementándose a nivel global, impulsados principalmente por actividades de recuperación, indisponibilidad operativa y afectaciones derivadas de la pérdida de información.

Figura 23

Impacto organizacional derivado del compromiso de la infraestructura.



Nota. Elaboración propia con base en NIST SP 800-53 Rev. 5 (Joint Task Force, 2020), ENISA (2023) e IBM Security (2024).

Otro componente particularmente crítico corresponde al impacto reputacional. La pérdida de confianza por parte de clientes, socios estratégicos o entidades reguladoras puede generar consecuencias que persisten incluso después de que el incidente ha sido técnicamente resuelto. Von Solms y Van Niekerk (2013) sostienen que la confianza constituye uno de los activos más valiosos dentro de los ecosistemas digitales modernos, razón por la cual los incidentes de seguridad suelen tener efectos que trascienden ampliamente las pérdidas económicas inmediatas.

Desde el punto de vista regulatorio, la exposición de información sensible puede generar incumplimientos asociados a normativas de protección de datos, obligaciones contractuales o

requisitos sectoriales de seguridad. Aunque el laboratorio desarrollado no involucró información real, las técnicas observadas durante el ejercicio demuestran que un atacante con acceso privilegiado podría potencialmente acceder a datos sensibles, alterar información corporativa o comprometer sistemas críticos. Bajo estas circunstancias, las organizaciones podrían enfrentar sanciones regulatorias, obligaciones de notificación y procesos de auditoría derivados del incidente.

Tabla 12

Ejemplo de evidencias digitales recolectadas durante el análisis.

Dimensión	Consecuencia potencial	Nivel de impacto
Operativa	Interrupción de procesos de negocio	Alto
Financiera	Costos de recuperación y remediación	Alto
Reputacional	Pérdida de confianza de clientes y socios	Alto
Regulatoria	Incumplimiento normativo y sanciones	Medio-Alto
Estratégica	Afectación de objetivos corporativos	Medio-Alto
Tecnológica	Compromiso de activos críticos	Alto

Nota. Elaboración propia.

Los hallazgos obtenidos durante el análisis demuestran que la materialización de una amenaza no afecta únicamente la infraestructura tecnológica, sino que impacta directamente la capacidad de la organización para cumplir sus objetivos estratégicos. La combinación entre vulnerabilidades técnicas, deficiencias de monitoreo y ausencia de controles de contención puede

transformar rápidamente un incidente localizado en una situación con consecuencias organizacionales significativas.

La gestión moderna de la ciberseguridad debe abordarse como una disciplina estratégica orientada a proteger la continuidad del negocio y no únicamente como una actividad técnica enfocada en la administración de infraestructura. Los resultados observados durante el presente ejercicio refuerzan la necesidad de integrar capacidades ofensivas, defensivas, forenses y de gestión del riesgo dentro de una estrategia unificada que permita fortalecer la resiliencia organizacional frente a amenazas cada vez más sofisticadas.

Implicaciones legales, éticas y profesionales del incidente.

Uno de los aspectos más relevantes dentro de cualquier incidente de ciberseguridad corresponde a las implicaciones legales, éticas y profesionales derivadas de las acciones ejecutadas por los actores involucrados. Aunque las actividades desarrolladas durante SecureNova Labs fueron realizadas dentro de un entorno controlado, académico y expresamente autorizado, las mismas técnicas observadas durante el ejercicio son utilizadas frecuentemente por actores maliciosos para comprometer sistemas, acceder a información sensible y afectar la continuidad operacional de organizaciones públicas y privadas. Por esta razón, el análisis de un incidente no puede limitarse exclusivamente a la dimensión técnica, sino que debe incorporar el estudio de los marcos normativos, regulatorios y éticos que gobiernan el uso legítimo de las capacidades ofensivas y defensivas en ciberseguridad.

La legislación colombiana establece mecanismos específicos para la protección de la información y de los sistemas informáticos. Mediante la Ley 1273 de 2009, el Estado colombiano incorporó al Código Penal un conjunto de delitos informáticos orientados a proteger la confidencialidad, integridad y disponibilidad de la información digital (Congreso de

Colombia, 2009). Entre las conductas tipificadas se encuentran el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, el daño informático, la obstaculización ilegítima de sistemas y la utilización de software malicioso. Estas disposiciones constituyen actualmente el principal marco jurídico colombiano para la persecución de actividades relacionadas con ciberdelincuencia.

Las actividades de reconocimiento, enumeración y movimiento lateral desarrolladas durante el ejercicio evidencian cómo un atacante puede obtener acceso progresivo a múltiples activos dentro de una infraestructura comprometida. Aunque estas acciones fueron ejecutadas con fines académicos y controlados, su utilización en escenarios reales podría derivar en afectaciones directas a la confidencialidad, integridad y disponibilidad de la información. La Organización de los Estados Americanos señala que el crecimiento de las amenazas digitales ha incrementado la necesidad de fortalecer simultáneamente los mecanismos tecnológicos y los marcos regulatorios destinados a la protección de infraestructuras críticas y activos de información (OEA, 2020).

Figura 24

Relación entre actividades técnicas observadas y posibles implicaciones legales y éticas.

Nota. Elaboración propia con base en NIST SP 800-53 Rev. 5 (Joint Task Force, 2020), ENISA (2023) e IBM Security (2024).

La relevancia de la Ley 1273 de 2009 dentro del contexto del presente análisis radica en que muchas de las técnicas utilizadas durante el ejercicio representan exactamente las conductas que el legislador buscó sancionar cuando incorporó los delitos informáticos al ordenamiento jurídico colombiano. El reconocimiento de servicios expuestos, la explotación de vulnerabilidades, la obtención de acceso remoto y el movimiento lateral observado durante las fases ofensivas constituyen actividades que, fuera de un contexto autorizado, podrían configurar el delito de acceso abusivo a un sistema informático contemplado en el artículo 269A del Código Penal Colombiano (Congreso de Colombia, 2009).

La posibilidad de acceder a información almacenada dentro de los sistemas comprometidos introduce implicaciones jurídicas directamente relacionadas con la protección de datos y la confidencialidad de la información. Aunque durante el ejercicio no se manipuló información real, el escenario técnico demostró que un atacante que alcance privilegios elevados podría consultar, copiar, modificar o extraer información sensible perteneciente a una organización. Gómez y Martínez (2021) sostienen que el principal riesgo jurídico derivado de los incidentes modernos no se limita al acceso inicial, sino a las consecuencias posteriores asociadas con la exposición, alteración o destrucción de la información comprometida.

La explotación de vulnerabilidades conocidas merece un análisis específico debido a las responsabilidades jurídicas que puede generar cuando se realiza sobre sistemas que no cuentan con autorización expresa. Desde una perspectiva técnica, la explotación de HFS 2.3 y MS17-010 permitió demostrar debilidades presentes en la infraestructura evaluada. Desde una perspectiva jurídica, la utilización de herramientas ofensivas sobre sistemas de terceros sin consentimiento puede derivar en responsabilidades penales, civiles e incluso administrativas. El Council of Europe (2001), mediante la Convención de Budapest sobre Ciberdelincuencia, estableció principios internacionales orientados a sancionar el acceso ilícito, la interceptación ilegal y la interferencia sobre sistemas informáticos, lineamientos que posteriormente fueron incorporados por múltiples legislaciones nacionales.

Las responsabilidades derivadas de un incidente de seguridad no recaen exclusivamente sobre los atacantes. Los marcos modernos de gestión del riesgo reconocen que las organizaciones tienen la obligación de implementar medidas razonables para proteger los activos de información bajo su custodia. El NIST establece que la gestión adecuada de vulnerabilidades, los controles de acceso, el monitoreo continuo y la respuesta estructurada ante incidentes constituyen elementos fundamentales de una estrategia efectiva de protección de activos digitales (Joint Task Force,

2020). La ausencia de controles adecuados no solamente incrementa la probabilidad de materialización de amenazas, sino que también puede aumentar la exposición jurídica y regulatoria de la organización frente a clientes, socios comerciales y entidades de supervisión.

La preservación de evidencia digital constituye uno de los elementos más sensibles dentro de cualquier investigación asociada a incidentes de ciberseguridad. Durante las actividades de análisis forense desarrolladas en este trabajo se aplicaron mecanismos orientados a garantizar la integridad de los artefactos analizados mediante generación de hashes criptográficos, documentación de procedimientos y conservación de registros asociados al incidente. La norma ISO/IEC 27037 establece que la identificación, recolección, adquisición y preservación de evidencia digital deben ejecutarse siguiendo procedimientos que garanticen autenticidad, integridad, confiabilidad y trazabilidad (ISO, 2012). El incumplimiento de estas prácticas podría comprometer la validez técnica y jurídica de los hallazgos obtenidos durante una investigación.

El análisis del incidente no puede limitarse al cumplimiento normativo. Las actividades observadas durante el laboratorio también plantean cuestionamientos relacionados con la ética profesional y el uso responsable de las capacidades ofensivas en ciberseguridad. El desarrollo de competencias asociadas al pentesting, análisis forense, ingeniería inversa o investigación de vulnerabilidades constituye una necesidad legítima para fortalecer la seguridad de las organizaciones; sin embargo, dichas capacidades deben encontrarse permanentemente subordinadas a principios de responsabilidad, transparencia y respeto por los derechos de terceros.

El Código de Ética Profesional del Consejo Profesional Nacional de Ingeniería establece que los ingenieros deben actuar con honestidad, responsabilidad social, integridad profesional y protección del interés público (COPNIA, 2022). Bajo este marco, el conocimiento técnico

asociado a pruebas de penetración, explotación de vulnerabilidades o análisis de amenazas no puede considerarse éticamente neutro. Las mismas herramientas empleadas para fortalecer la seguridad de una organización pueden utilizarse para afectar la confidencialidad, integridad o disponibilidad de sistemas ajenos cuando son empleadas fuera de contextos autorizados.

Casey (2011) explica que la principal diferencia entre una actividad legítima de seguridad ofensiva y una conducta ilícita no radica en la técnica utilizada, sino en la existencia de autorización expresa, alcance definido y objetivos claramente orientados a la protección de los activos de información. La práctica profesional del pentesting y de la seguridad ofensiva requiere que toda actividad se encuentre respaldada por autorizaciones formales, alcances previamente definidos y mecanismos adecuados de documentación y reporte.

Tabla 13

Relación entre actividades observadas y posibles implicaciones legales.

Actividad observada	Implicación potencial	Referencia normativa
Escaneo no autorizado de sistemas	Acceso indebido a infraestructura	Ley 1273 de 2009
Explotación de vulnerabilidades	Acceso abusivo a sistemas informáticos	Ley 1273 de 2009
Obtención de información sensible	Violación de confidencialidad	Ley 1273 de 2009
Alteración de configuraciones	Daño o modificación no autorizada	Ley 1273 de 2009
Manipulación de evidencia digital	Afectación de investigaciones	ISO/IEC 27037

Actividad observada	Implicación potencial	Referencia normativa
Ocultamiento de incidentes	Incumplimiento ético profesional	COPNIA (2022)

Nota. Elaboración propia.

La protección de la información exige mucho más que la implementación de controles tecnológicos. Los profesionales de ciberseguridad tienen la responsabilidad de proteger la información obtenida durante sus evaluaciones, evitar conflictos de interés, preservar la confidencialidad de los hallazgos y actuar conforme a los principios éticos establecidos por los organismos reguladores y las buenas prácticas internacionales. Von Solms y Van Niekerk (2013) sostienen que la gobernanza de la ciberseguridad requiere integrar aspectos técnicos, legales, organizacionales y humanos dentro de una estrategia unificada de gestión del riesgo.

Lecciones aprendidas y análisis crítico del incidente.

El análisis desarrollado a lo largo de las diferentes fases del presente trabajo permitió demostrar que los incidentes de ciberseguridad rara vez son consecuencia de una única vulnerabilidad aislada. Por el contrario, suelen originarse a partir de la combinación de múltiples debilidades técnicas, operativas y organizacionales que, al interactuar entre sí, crean condiciones favorables para el compromiso progresivo de la infraestructura. La mayoría de los compromisos significativos observados en organizaciones modernas son el resultado de fallos acumulativos en diferentes capas de protección y no de una única falla tecnológica (Joint Task Force, 2020; ENISA, 2023). La explotación exitosa observada durante el escenario analizado no fue producto exclusivamente de la vulnerabilidad presente en HFS 2.3 ni de la exposición de sistemas

vulnerables a MS17-010, sino del encadenamiento de deficiencias relacionadas con gestión de vulnerabilidades, segmentación de red, monitoreo y control de privilegios. Este comportamiento coincide con numerosos incidentes documentados por organismos internacionales, donde los atacantes aprovechan combinaciones de errores de configuración, vulnerabilidades sin remediar y deficiencias de monitoreo para ampliar progresivamente el alcance del compromiso (CISA, 2023; ENISA, 2023).

Una de las principales lecciones obtenidas durante el ejercicio corresponde a la importancia de la gestión continua de vulnerabilidades. La explotación de servicios vulnerables evidenció que la existencia de software desactualizado continúa siendo uno de los vectores de compromiso más frecuentes dentro de las organizaciones. CISA (2023) advierte que una proporción significativa de los incidentes observados a nivel mundial aprovecha vulnerabilidades para las cuales existen medidas de mitigación o actualizaciones disponibles desde hace meses o incluso años. ENISA (2023) llega a conclusiones similares al identificar la gestión deficiente de vulnerabilidades como uno de los factores de riesgo más recurrentes dentro del panorama actual de amenazas. Bajo esta perspectiva, la gestión de vulnerabilidades no debe limitarse a actividades periódicas de escaneo, sino convertirse en un proceso continuo de identificación, evaluación, priorización y remediación de riesgos tecnológicos.

Los resultados también demostraron que la ausencia de segmentación efectiva amplifica significativamente el impacto potencial de un incidente. Una vez obtenido acceso inicial al sistema vulnerable fue posible identificar otros activos presentes dentro de la infraestructura y avanzar hacia nuevos objetivos mediante técnicas de movimiento lateral. Rose et al. (2020) sostienen que los modelos modernos de seguridad deben asumir que el compromiso de algún componente de la infraestructura es una posibilidad permanente, razón por la cual los mecanismos de contención y segmentación adquieren una importancia estratégica dentro de la

defensa organizacional. Esta visión también es respaldada por CISA (2023), que identifica la segmentación como una de las medidas más efectivas para limitar la propagación de amenazas y reducir el alcance operativo de un incidente.

Otra lección relevante se relaciona con la necesidad de fortalecer las capacidades de visibilidad y monitoreo. Durante el análisis fue posible identificar múltiples eventos que habrían generado indicadores de compromiso observables para un equipo Blue Team adecuadamente equipado. Conexiones remotas inusuales, ejecución de procesos sospechosos, creación de sesiones privilegiadas y actividades asociadas al movimiento lateral representan comportamientos que pueden ser detectados mediante SIEM, plataformas EDR, observabilidad basada en eBPF o mecanismos de runtime security. Bejtlich (2013) argumenta que la diferencia entre una intrusión contenida y un incidente de gran impacto suele estar directamente relacionada con la capacidad de la organización para identificar actividades anómalas durante las etapas iniciales del ataque. Esta necesidad continúa vigente en entornos modernos, donde NIST (2024) destaca que la observabilidad, la correlación de eventos y el monitoreo continuo constituyen elementos fundamentales para reducir los tiempos de detección y respuesta frente a amenazas avanzadas.

La evaluación realizada también evidenció la importancia de adoptar una estrategia de defensa en profundidad. Ningún control individual habría sido suficiente para impedir completamente el desarrollo del escenario ofensivo observado. La aplicación de parches podría haber mitigado la explotación inicial; la segmentación habría limitado el movimiento lateral; los mecanismos de mínimo privilegio habrían reducido el impacto de la escalación; y las capacidades de monitoreo habrían incrementado las probabilidades de detección temprana. CIS (2024) señala que la seguridad efectiva surge de la implementación coordinada de múltiples capas de protección que compensan las limitaciones inherentes de cada control individual. Este

principio también se encuentra alineado con el enfoque de defensa en profundidad promovido por NIST, donde la protección de los activos depende de la integración de controles preventivos, detectivos y correctivos distribuidos a través de diferentes capas de la infraestructura (Joint Task Force, 2020).

El ejercicio permitió validar igualmente la relevancia de los enfoques Zero Trust dentro de las arquitecturas modernas. El movimiento lateral observado durante el incidente demuestra que asumir confianza implícita entre sistemas internos representa un riesgo significativo para la organización. El modelo propuesto por NIST establece que ninguna entidad debe ser considerada confiable por defecto, independientemente de su ubicación dentro o fuera de la red corporativa (Rose et al., 2020). CISA (2023) identifica la adopción de arquitecturas Zero Trust como uno de los mecanismos más efectivos para limitar la expansión lateral de amenazas dentro de infraestructuras modernas. Bajo esta filosofía, cada solicitud de acceso debe ser validada continuamente mediante criterios de identidad, contexto y nivel de riesgo, reduciendo considerablemente las oportunidades disponibles para un atacante que ya ha comprometido parte de la infraestructura.

La dimensión legal y ética del incidente también aporta enseñanzas relevantes para el ejercicio profesional de la ciberseguridad. El laboratorio permitió evidenciar que muchas de las técnicas utilizadas por equipos de pentesting son técnicamente idénticas a aquellas empleadas por actores maliciosos durante ataques reales. Casey (2011) sostiene que la legitimidad de una actividad de seguridad ofensiva depende tanto del cumplimiento técnico como del respeto a los marcos legales y éticos que regulan su ejecución. Este principio resulta coherente con los lineamientos establecidos por el Consejo Profesional Nacional de Ingeniería, que exige que las actividades profesionales sean desarrolladas bajo criterios de responsabilidad, integridad y protección del interés público (COPNIA, 2022).

Los hallazgos obtenidos demuestran que la resiliencia organizacional no puede construirse exclusivamente mediante la adquisición de herramientas tecnológicas. La efectividad de una estrategia de seguridad depende de la integración entre procesos, personas y tecnología. Linkov y Kott (2019) sostienen que las organizaciones resilientes se caracterizan por su capacidad para aprender continuamente de los incidentes y transformar dichos aprendizajes en mecanismos permanentes de fortalecimiento institucional. Esta visión también se encuentra reflejada en el NIST Cybersecurity Framework 2.0, el cual establece que la mejora continua y la capacidad de adaptación frente a nuevos escenarios de amenaza constituyen elementos esenciales para mantener una postura de seguridad sostenible en el tiempo (NIST, 2024).

Figura *25*

Lecciones aprendidas derivadas del análisis integral del incidente.

Nota. Elaboración propia con base en NIST SP 800-53 Rev. 5 (Joint Task Force, 2020), NIST Cybersecurity Framework 2.0 (2024), CIS Controls v8 (2024), ENISA Threat Landscape (2023) y Zero Trust Architecture (Rose et al., 2020).

El caso analizado demuestra que la seguridad efectiva no depende de la ausencia de vulnerabilidades, sino de la capacidad de la organización para identificarlas, contenerlas y responder adecuadamente cuando estas son explotadas. La combinación entre gestión de vulnerabilidades, segmentación, monitoreo, análisis forense, cumplimiento normativo y mejora continua constituye la base sobre la cual se construyen programas maduros de ciberseguridad

capaces de enfrentar amenazas cada vez más sofisticadas y persistentes (ENISA, 2023; NIST, 2024; CIS, 2024). El principal aprendizaje derivado del ejercicio consiste en reconocer que la resiliencia organizacional surge de la integración coordinada de controles técnicos, capacidades humanas, procesos de gestión y mecanismos de mejora continua, y no de la implementación aislada de herramientas o tecnologías específicas.

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/cmpMG8bLsws

Conclusiones

El desarrollo integral del presente trabajo permitió evidenciar que los incidentes de ciberseguridad rara vez son consecuencia de una única vulnerabilidad aislada. El escenario analizado demostró que la explotación exitosa de una infraestructura generalmente se produce mediante el encadenamiento de múltiples debilidades relacionadas con gestión de vulnerabilidades, segmentación de red, monitoreo insuficiente y control inadecuado de privilegios. Esta situación confirma la necesidad de adoptar enfoques de defensa en profundidad que permitan reducir las oportunidades disponibles para un atacante a lo largo de las diferentes etapas de la cadena de ataque.

Las actividades desarrolladas durante la fase de seguridad ofensiva permitieron comprobar la efectividad de metodologías estructuradas de pentesting para identificar debilidades presentes en los sistemas evaluados. La explotación de HFS 2.3, la obtención de acceso remoto y las actividades de movimiento lateral evidenciaron cómo vulnerabilidades conocidas pueden convertirse en puntos de entrada críticos cuando no existen procesos adecuados de actualización, endurecimiento y gestión continua de riesgos tecnológicos.

El análisis realizado desde la perspectiva Blue Team demostró que la detección temprana continúa siendo uno de los factores más importantes para reducir el impacto de un incidente. La implementación de capacidades de monitoreo continuo, correlación de eventos, análisis forense digital, observabilidad basada en eBPF y mecanismos de runtime security permite incrementar significativamente la capacidad de identificar actividades anómalas antes de que estas evolucionen hacia compromisos de mayor alcance.

Los resultados obtenidos permitieron validar la importancia de arquitecturas modernas basadas en principios de Zero Trust y segmentación de red. El movimiento lateral observado durante el ejercicio evidenció que asumir confianza implícita entre sistemas internos incrementa

considerablemente el riesgo organizacional. La aplicación de controles de segmentación, mínimo privilegio y verificación continua constituye una medida efectiva para limitar la propagación de amenazas dentro de infraestructuras corporativas.

El componente jurídico y ético desarrollado durante la investigación permitió establecer que las capacidades técnicas asociadas al pentesting, análisis forense e investigación de vulnerabilidades deben ejercerse siempre dentro de marcos de autorización claramente definidos. La Ley 1273 de 2009, la Convención de Budapest, las buenas prácticas internacionales de manejo de evidencia digital y los principios establecidos por el COPNIA proporcionan una base fundamental para garantizar que las actividades de ciberseguridad se desarrollen bajo criterios de legalidad, responsabilidad profesional y protección del interés público.

La aplicación de procedimientos de Digital Forensics and Incident Response (DFIR) permitió comprender la importancia de preservar adecuadamente la evidencia digital durante investigaciones asociadas a incidentes de seguridad. La generación de hashes, la conservación de registros, la documentación de procedimientos y la trazabilidad de las evidencias constituyen elementos indispensables para garantizar la validez técnica y jurídica de los hallazgos obtenidos durante una investigación forense.

Finalmente, el principal aprendizaje derivado del presente trabajo consiste en reconocer que la resiliencia organizacional no depende exclusivamente de la implementación de herramientas tecnológicas, sino de la integración coordinada entre personas, procesos y tecnología. La combinación de capacidades ofensivas, controles defensivos, monitoreo continuo, análisis forense, cumplimiento normativo y mejora continua permite construir organizaciones más preparadas para anticipar, resistir, contener y recuperarse de incidentes de ciberseguridad cada vez más sofisticados.

Recomendaciones

Las recomendaciones propuestas se fundamentan en los hallazgos identificados durante las actividades de análisis jurídico, pentesting, respuesta a incidentes y fortalecimiento defensivo desarrolladas a lo largo del seminario. Su objetivo consiste en reducir la probabilidad de materialización de amenazas similares, fortalecer la resiliencia organizacional y mejorar la capacidad de detección, contención y recuperación frente a incidentes de ciberseguridad.

La primera recomendación consiste en fortalecer el programa de gestión de vulnerabilidades mediante la implementación de procesos continuos de descubrimiento, evaluación, priorización y remediación. Los resultados obtenidos durante las actividades ofensivas demostraron que la presencia de software vulnerable continúa representando uno de los principales vectores de acceso inicial para los atacantes. La organización debe establecer mecanismos formales que permitan identificar oportunamente vulnerabilidades críticas, validar la disponibilidad de actualizaciones de seguridad y verificar la aplicación efectiva de los controles correctivos (CISA, 2023; ENISA, 2023).

Se recomienda implementar una estrategia de segmentación de red basada en principios de mínimo privilegio y Zero Trust. El movimiento lateral observado durante el laboratorio evidenció que la comunicación excesiva entre sistemas facilita la expansión de las amenazas una vez se produce un compromiso inicial. La segmentación debe orientarse a restringir el acceso entre activos críticos, limitar la propagación de amenazas y reducir el impacto potencial de incidentes futuros (Rose et al., 2020).

Resulta necesario fortalecer las capacidades de monitoreo continuo mediante la integración de plataformas SIEM, mecanismos avanzados de correlación de eventos y fuentes de telemetría capaces de proporcionar visibilidad sobre actividades sospechosas dentro de la infraestructura. La detección temprana de comportamientos anómalos permite reducir

significativamente los tiempos de respuesta y minimizar el impacto asociado a incidentes de seguridad. La incorporación de capacidades de observabilidad basadas en eBPF y herramientas de runtime security como Falco o Tetragon puede complementar significativamente los mecanismos tradicionales de monitoreo (NIST, 2024; CNCF, 2023).

Se recomienda formalizar procedimientos de Digital Forensics and Incident Response (DFIR) alineados con estándares internacionales para garantizar una respuesta estructurada ante incidentes de seguridad. La organización debe establecer lineamientos para la identificación, recolección, preservación y análisis de evidencia digital, asegurando que las investigaciones futuras puedan desarrollarse de manera técnica, trazable y jurídicamente válida (ISO, 2012; Casey, 2011).

Otro aspecto prioritario corresponde al fortalecimiento de los controles de identidad y acceso. La aplicación consistente de autenticación multifactor, segregación de funciones, gestión de privilegios y revisión periódica de permisos reduce significativamente las oportunidades de abuso de cuentas comprometidas o privilegios excesivos. Este enfoque debe complementarse con revisiones periódicas de acceso y mecanismos de validación continua acordes con los principios de Zero Trust (Rose et al., 2020; Joint Task Force, 2020).

Se recomienda fortalecer los procesos de capacitación y concientización dirigidos a personal técnico, administrativo y directivo. La seguridad organizacional no depende exclusivamente de controles tecnológicos; también requiere que los usuarios comprendan los riesgos asociados al manejo de la información, el uso de credenciales y la identificación de actividades potencialmente maliciosas. Las iniciativas de formación deben integrarse dentro de un programa permanente de cultura de ciberseguridad (NIST, 2024).

Desde una perspectiva de cumplimiento, la organización debe asegurar que sus actividades de ciberseguridad se encuentren alineadas con los requisitos legales y regulatorios

aplicables. La implementación de procesos de auditoría, conservación de evidencia digital y documentación de actividades contribuye a fortalecer la capacidad de respuesta frente a investigaciones internas, auditorías regulatorias o procesos judiciales asociados a incidentes de seguridad. Este enfoque debe apoyarse en los lineamientos establecidos por la Ley 1273 de 2009, ISO/IEC 27037 y los principios éticos definidos por el COPNIA (Congreso de Colombia, 2009; ISO, 2012; COPNIA, 2022).

Finalmente, se recomienda adoptar un modelo de mejora continua de la postura de seguridad basado en ejercicios periódicos de validación ofensiva y defensiva. Las pruebas de penetración, los ejercicios Red Team, las simulaciones de respuesta a incidentes y las evaluaciones de madurez permiten identificar nuevas debilidades, validar la efectividad de los controles implementados y fortalecer progresivamente la resiliencia organizacional frente a amenazas en constante evolución (Scarfone et al., 2008; Linkov & Kott, 2019).

Referencias Bibliográficas

Bejtlich, R. (2013). The practice of network security monitoring: Understanding incident detection and response. No Starch Press.

Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, Omega, and Kubernetes. *Communications of the ACM, 59*(5), 50–57. https://doi.org/10.1145/2890784

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Center for Internet Security. (2024). *CIS Controls Version 8*. https://www.cisecurity.org

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

Cloud Native Computing Foundation. (2023). *Cloud native security whitepaper*. https://www.cncf.io

Congreso 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" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. Diario Oficial No. 47.223.

Consejo Profesional Nacional de Ingeniería (COPNIA). (2022). *Código de ética profesional de la ingeniería en Colombia*.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. https://www.coe.int

Cybersecurity and Infrastructure Security Agency. (2023). *Cross-sector cybersecurity performance goals*. https://www.cisa.gov

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu

Falco Project. (2024). *Falco documentation*. https://falco.org

Gómez, J., & Martínez, C. (2021). Delitos informáticos y protección jurídica de la información en Colombia. *Revista Iberoamericana de Derecho Informático, 14*(2), 45–63.

Greenberg, A. (2018). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Gregg, B. (2020). *BPF performance tools: Linux system and application observability*. Addison-Wesley Professional.

IBM Security. (2024). *Cost of a data breach report 2024*. https://www.ibm.com/security

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

International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection—Information security management systems—Requirements*.

Isovalent. (2024). *Tetragon documentation*. https://tetragon.io

Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kent, K., & Souppaya, M. (2006). *Guide to computer security log management* (NIST Special Publication 800-92). National Institute of Standards and Technology.

Linkov, I., & Kott, A. (2019). *Cyber resilience of systems and networks*. Springer. https://doi.org/10.1007/978-3-319-77492-3

MITRE Corporation. (2024). *MITRE ATT&CK Enterprise Matrix*. https://attack.mitre.org

National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. https://www.nist.gov/cyberframework

Organization of American States. (2020). *Estado de la ciberseguridad en América Latina y el Caribe*. https://www.oas.org

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Scarfone, K., Grance, T., & Masone, K. (2008). *Technical guide to information security testing and assessment* (NIST Special Publication 800-115). National Institute of Standards and Technology.

Sikorski, M., & Honig, A. (2012). *Practical malware analysis: The hands-on guide to dissecting malicious software*. No Starch Press.

Stallings, W. (2018). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley Professional.

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2018). *MITRE ATT&CK: Design and philosophy*. MITRE Corporation.

Von Solms, B., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Apéndices

Apéndice A

Resultado de revisión en Turnitin