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

Henry Andres Fraile Gonzalez

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Para mis profesores de la Especialización en Seguridad Informática de la Escuela de Ciencias Básicas, Tecnología e Ingeniería de la UNAD, mi reconocimiento y gratitud por su guía exigente y humana. Su rigor académico, su apertura al debate y su acompañamiento constante me ayudaron a transformar dudas en preguntas de investigación y resultados concretos. Gracias por inspirar excelencia, ética profesional y compromiso con la seguridad digital al servicio de la sociedad.

Agradecimientos

A mi familia, que me sostiene día a día con amor, paciencia y confianza, dedico este esfuerzo. Su apoyo silencioso en las largas jornadas, su comprensión ante mis ausencias y su fe inquebrantable en mis capacidades hicieron posible cada avance de este trabajo. Que estas páginas sean también testimonio de nuestra perseverancia compartida.

Resumen

El informe presenta el desarrollo de un ejercicio integral de ciberseguridad en un entorno de laboratorio, orientado a evaluar la postura de seguridad de la organización ficticia SecureNova Labs mediante la sinergia entre equipos Red Team y Blue Team. En primer lugar, se establece el marco metodológico, legal y ético que regula las pruebas de intrusión en Colombia, incorporando los lineamientos de la Ley 1273 de 2009, la normativa de protección de datos personales y el Código de Ética de COPNIA como límites obligatorios para la actuación profesional. Posteriormente, se describe la ejecución de un escenario Red Team sobre una arquitectura basada en Windows 7 y Parrot OS, donde se demuestra la explotación del servicio vulnerable Rejetto HFS 2.3 (CVE-2014-6287), el uso de técnicas de pivoting desde un host con doble interfaz de red y la explotación de la vulnerabilidad MS17-010 en un servidor interno, alcanzando privilegios de sistema y evidenciando el impacto sobre la confidencialidad, integridad y disponibilidad de los activos. Desde la perspectiva Blue Team, se analizan los indicadores de compromiso a nivel de sistema y red, se proponen estrategias de contención no destructivas y se formulan medidas de hardening soportadas en marcos como los CIS Controls, los CIS Benchmarks y el uso de soluciones SIEM y plataformas de respuesta activa. El documento concluye con un análisis integrador de las cuatro etapas del trabajo, resaltando la importancia de articular las capacidades ofensivas y defensivas con el cumplimiento normativo y la ética profesional, y presentando recomendaciones técnicas y de gobierno para fortalecer la defensa en profundidad de organizaciones con características similares.

***Palabras clave*:** ciberseguridad, defensa, intrusión, pentesting, vulnerabilidades

Abstract

This report presents the development of a comprehensive cybersecurity exercise in a laboratory environment, aimed at assessing the security posture of the fictitious organization SecureNova Labs through the synergy between Red Team and Blue Team activities. First, it establishes the methodological, legal, and ethical framework that governs penetration testing in Colombia, incorporating the guidelines of Law 1273 of 2009, data protection regulations, and the COPNIA Code of Ethics as mandatory boundaries for professional practice. The report then describes the execution of a Red Team scenario on an architecture based on Windows 7 and Parrot OS, where the exploitation of the vulnerable Rejetto HFS 2.3 service (CVE-2014-6287) is demonstrated, together with pivoting techniques from a dual-homed host and the exploitation of the MS17-010 vulnerability on an internal server, achieving system-level privileges and evidencing the impact on the confidentiality, integrity, and availability of information assets. From the Blue Team perspective, the work analyzes host and network indicators of compromise, proposes non-destructive containment strategies, and defines hardening measures supported by frameworks such as the CIS Controls and CIS Benchmarks, as well as SIEM solutions and active response platforms. The document concludes with an integrative analysis of the four stages of the project, highlighting the need to align offensive and defensive capabilities with legal compliance and professional ethics, and providing technical and governance recommendations to strengthen defense-in-depth in organizations with similar characteristics.

Keywords**:** cybersecurity, defense, intrusion, pentesting, vulnerabilities

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

ACL (Access Control List):

Lista de control de acceso que define qué usuarios, equipos o procesos pueden acceder a un recurso de red o de sistema y con qué tipo de permisos (lectura, escritura, ejecución), permitiendo aplicar el principio de mínimo privilegio sobre servicios y dispositivos.

Ataque lateral (Lateral Movement):

Técnica mediante la cual un atacante, después de comprometer un equipo inicial, se desplaza a través de la red interna aprovechando credenciales, vulnerabilidades o malas configuraciones para obtener acceso a otros sistemas y ampliar el impacto del incidente.

Blue Team:

Equipo responsable de la defensa de la infraestructura tecnológica, encargado de la monitorización, detección, análisis, contención y recuperación ante incidentes de seguridad, así como de proponer medidas de mejora continua en la postura de ciberseguridad (Bejtlich, 2013; Rajendran et al., 2011).

Ciberseguridad:

Conjunto de políticas, procesos, tecnologías y prácticas orientadas a proteger los sistemas de información, las redes y los datos frente a accesos no autorizados, alteraciones, destrucción o indisponibilidad, alineando los controles con los objetivos del negocio y el marco legal vigente (Center for Internet Security, 2021; Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, 2022).

CIS Benchmarks:

Guías de configuración segura publicadas por el Center for Internet Security que establecen parámetros técnicos recomendados para endurecer sistemas operativos, bases de datos y aplicaciones, sirviendo como referencia para actividades de hardening (CIS Security, 2020).

CIS Controls (Controles Críticos CIS):

Conjunto priorizado de buenas prácticas de seguridad que orientan la implementación de controles esenciales (inventario de activos, gestión de vulnerabilidades, control de privilegios, monitorización, entre otros) para reducir la superficie de ataque y el riesgo de incidentes (Center for Internet Security, 2021).

Confidencialidad:

Propiedad de la información que garantiza que solo las personas, procesos o sistemas autorizados puedan acceder a los datos, evitando su divulgación no autorizada mediante mecanismos como el control de acceso, la autenticación y el cifrado.

COPNIA:

Consejo Profesional Nacional de Ingeniería, entidad que regula el ejercicio de la ingeniería en Colombia y emite el Código de Ética que establece los deberes, prohibiciones y principios que deben observar los ingenieros en su práctica profesional (COPNIA, 2015).

CSIRT (Computer Security Incident Response Team):

Equipo especializado en la gestión de incidentes de seguridad informática, encargado de recibir reportes, analizar eventos, coordinar la respuesta técnica y comunicar las acciones a los actores relevantes; en el contexto académico se refiere, entre otros, al CSIRT Académico UNAD (CSIRT Académico UNAD, 2024).

CVE (Common Vulnerabilities and Exposures):

Sistema de identificación estandarizado que asigna un código único a vulnerabilidades conocidas en software y hardware, facilitando su referencia, seguimiento y gestión en bases de datos como NVD o Exploit-DB.

Datos personales:

Información vinculada o que pueda asociarse a una persona natural identificada o identificable, como nombres, identificaciones, direcciones, correos o datos de contacto, cuyo tratamiento está regulado en Colombia por la Ley 1581 de 2012 y el Decreto 1377 de 2013 (Congreso de la República de Colombia, 2012; Presidencia de la República de Colombia, 2013).

Defensa en profundidad:

Estrategia de seguridad que consiste en disponer varias capas de controles (perimetrales, de red, de host, de aplicación y de datos) en lugar de confiar en un único mecanismo, de forma que la falla de una barrera no implique la exposición total del sistema frente a un atacante (Bejtlich, 2013; Center for Internet Security, 2021).

DMZ (Zona desmilitarizada):

Segmento de red intermedio entre la red interna y la red externa (por ejemplo, internet), diseñado para alojar servicios expuestos al público (como servidores web), limitando la comunicación directa entre estos y los sistemas internos sensibles mediante reglas estrictas de firewall.

Disponibilidad:

Propiedad de la información y de los servicios que asegura que los recursos estén accesibles y operativos para los usuarios autorizados cuando los necesitan, reduciendo el riesgo de interrupciones o caídas prolongadas.

Explotación (Exploit):

Acción y, en algunos casos, programa o código mediante el cual se aprovecha una vulnerabilidad de un sistema, servicio o aplicación para ejecutar acciones no autorizadas, como la ejecución de código arbitrario, la elevación de privilegios o el acceso indebido a datos.

Firewall: Dispositivo físico o software que controla el tráfico de red entrante y saliente según un conjunto de reglas predefinidas, permitiendo o denegando conexiones con base en direcciones IP, puertos, protocolos u otros criterios, con el fin de reducir la superficie de ataque y separar

zonas con diferentes niveles de confianza (CCN-CERT, 2018; Center for Internet Security, 2021).

Gestión de incidentes de seguridad:

Proceso estructurado para preparar, detectar, analizar, contener, erradicar y recuperar ante eventos que afecten la confidencialidad, integridad o disponibilidad de la información, así como para documentar lecciones aprendidas y fortalecer los controles existentes (Cichonski et al., 2012; Zambrano Hernández et al., 2024).

Gestión de vulnerabilidades:

Conjunto de actividades orientadas a identificar, evaluar, priorizar y mitigar debilidades presentes en sistemas y aplicaciones, apoyándose en escáneres, bases de datos de vulnerabilidades (como CVE/NVD) y procesos de parchado y hardening dentro de un ciclo de mejora continua (CVE Program, s. f.; National Institute of Standards and Technology, s. f.; Incibe, 2019).

Hardening:

Proceso de endurecimiento de sistemas que consiste en deshabilitar servicios innecesarios, aplicar configuraciones seguras, reforzar parámetros por defecto y reducir al mínimo los vectores de ataque, generalmente guiado por estándares como los CIS Benchmarks.

HFS (HTTP File Server):

Aplicación ligera de servidor de archivos que permite compartir contenido mediante HTTP; en el contexto del informe se refiere a HFS 2.3, versión vulnerable a la ejecución remota de comandos (CVE-2014-6287) cuando se configura de forma insegura.

IDS/IPS (Intrusion Detection/Prevention System):

Sistemas de detección y prevención de intrusos que analizan el tráfico de red o los eventos de host para identificar patrones maliciosos; los IDS generan alertas ante actividad sospechosa y los IPS pueden, además, bloquear o interrumpir el tráfico detectado como ataque.

Integridad:

Propiedad de la información que garantiza que los datos no han sido alterados de forma no autorizada, preservando su exactitud y completitud mediante controles como sumas de verificación, firmas digitales, registros de auditoría y restricciones de modificación.

Ley 1273 de 2009:

Norma colombiana que modifica el Código Penal para crear delitos específicos relacionados con la protección de la información y de los datos, como acceso abusivo a sistemas informáticos, interceptación de datos informáticos, daño informático y uso de software malicioso (Congreso de la República de Colombia, 2009).

Ley 1581 de 2012:

Ley general de protección de datos personales en Colombia, que establece principios, derechos y obligaciones para el tratamiento de datos, incluyendo la necesidad de autorización del titular, la finalidad legítima y la implementación de medidas de seguridad adecuadas (Congreso de la República de Colombia, 2012).

MS17-010 (EternalBlue):

Boletín de seguridad de Microsoft que corrige una vulnerabilidad crítica en la implementación del protocolo SMBv1 en varias versiones de Windows; su explotación, popularizada como EternalBlue, permite la ejecución remota de código en el sistema objetivo con altos privilegios si no se aplica el parche correspondiente.

NAC (Network Access Control):

Tecnología que controla el acceso de dispositivos a la red en función de políticas predefinidas, validando aspectos como la identidad del equipo, su estado de seguridad o su pertenencia a un grupo, y pudiendo colocar dispositivos no conformes en VLAN de cuarentena o negarles el acceso.

OSINT (Open Source Intelligence):

Recopilación y análisis de información a partir de fuentes abiertas y públicas (sitios web, redes sociales, registros DNS, fugas de datos, entre otros), utilizada tanto por equipos Red Team para reconocimiento como por equipos defensivos para análisis de exposición.

OSSTMM (Open Source Security Testing Methodology Manual):

Metodología abierta para pruebas de seguridad que proporciona un marco sistemático para evaluar la seguridad de redes, sistemas y procesos, definiendo canales de interacción, métricas orientadas a riesgo y criterios de verificación repetibles (Palomo Luna et al., 2024; Zuluaga Mateus, 2017).

Parrot OS:

Distribución GNU/Linux orientada a seguridad y pruebas de penetración que integra herramientas para análisis de vulnerabilidades, explotación, forense y pruebas de intrusión, utilizada comúnmente como sistema operativo del atacante en laboratorios de Red Team.

Pentesting (Pruebas de penetración):

Proceso controlado mediante el cual se simulan ataques reales contra sistemas y redes con el objetivo de identificar vulnerabilidades, evaluar su impacto y proponer medidas correctivas, siguiendo metodologías estructuradas como OSSTMM, PTES o NIST SP 800-115 (Álvarez Intriago, 2018; Incibe, 2019; Palomo Luna et al., 2024).

Pivoting:

Técnica utilizada por un atacante para aprovechar un equipo ya comprometido como puente o punto de salto hacia otros segmentos de red, redirigiendo tráfico o estableciendo túneles que permiten acceder a sistemas que originalmente no eran alcanzables desde el host atacante.

Red Team:

Equipo especializado en simular ataques reales contra la organización, utilizando tácticas, técnicas y procedimientos similares a los de atacantes reales, con el fin de evaluar la efectividad de los controles de seguridad y descubrir brechas que no se evidencian en auditorías tradicionales (Arroyo, 2025; Kotwani et al., 2023).

Riesgo residual:

Nivel de riesgo que permanece después de aplicar controles y medidas de mitigación, resultante de vulnerabilidades que no pueden eliminarse por completo o de limitaciones técnicas, económicas u operativas en la implementación de medidas de seguridad.

SIEM (Security Information and Event Management):

Plataforma que recolecta, correlaciona y analiza logs y eventos provenientes de múltiples fuentes (sistemas operativos, aplicaciones, dispositivos de red, soluciones de seguridad) para detectar patrones de ataque, generar alertas y apoyar la respuesta a incidentes dentro de una arquitectura de monitoreo centralizado (Moreano Jurado, 2015; Wazuh, Inc., s. f.).

SMB (Server Message Block):

Protocolo de red utilizado principalmente en entornos Windows para compartir archivos, impresoras y otros recursos entre sistemas; versiones inseguras o sin parchar, como SMBv1, pueden ser explotadas por vulnerabilidades como MS17-010.

VLAN (Virtual LAN):

Red lógica configurada sobre una infraestructura física de conmutación que permite segmentar el tráfico en dominios de broadcast separados, mejorando el control, el rendimiento y la seguridad al aislar grupos de equipos según criterios organizativos o de seguridad.

Vulnerabilidad:

Debilidad o fallo de diseño, implementación o configuración en un sistema, aplicación o proceso que puede ser aprovechado por un atacante para afectar la confidencialidad, integridad o disponibilidad de la información o de los servicios asociados.

Wazuh:

Plataforma de seguridad de código abierto que integra funcionalidades de monitorización de archivos, detección de intrusos, correlación de eventos y respuesta activa, y que puede actuar como agente de endpoint integrado con un SIEM central.

Windows 7:

Sistema operativo de Microsoft utilizado ampliamente en entornos corporativos y de usuario final; en el contexto del informe se emplea en máquinas de laboratorio (Host-A y Host-B), las cuales, al permanecer sin soporte y sin parches críticos, resultan especialmente expuestas a vulnerabilidades como MS17-010.

Introducción

La creciente dependencia de las organizaciones respecto de sus sistemas de información, redes de comunicación y servicios digitales ha ampliado significativamente la superficie de ataque disponible para actores maliciosos de distinta naturaleza. En este contexto, las pruebas de intrusión y los ejercicios coordinados entre equipos Red Team y Blue Team se han consolidado como herramientas indispensables para evaluar, bajo condiciones controladas, la resiliencia de la infraestructura frente a amenazas reales y la capacidad institucional para detectarlas y responder oportunamente (Bejtlich, 2013; Kotwani et al., 2023). Este enfoque permite ir más allá de las revisiones documentales o de cumplimiento normativo, trasladando la evaluación de la seguridad a un plano eminentemente práctico, basado en escenarios de ataque y defensa alineados con tácticas, técnicas y procedimientos observados en el mundo real (Chindrus & Caruntu, 2023; Rajendran et al., 2011).

El trabajo que aquí se presenta compila y articula los resultados de cuatro etapas desarrolladas en el marco de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia – UNAD, alrededor del caso de estudio de la organización ficticia SecureNova Labs. En la Etapa 1 se realizó un análisis del marco legal, metodológico y ético aplicable a las pruebas de seguridad informática en Colombia, incluyendo la revisión de metodologías de pentesting como OSSTMM y PTES, así como la identificación de normas clave como la Ley 1273 de 2009 sobre delitos informáticos, la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales, y el Código de Ética de COPNIA (Álvarez Intriago, 2018; Congreso de la República de Colombia, 2009, 2012; COPNIA, 2015; Presidencia de la República de Colombia, 2013; Zuluaga Mateus, 2017).

La Etapa 2 profundizó en la dimensión contractual y de riesgo legal, mediante el estudio de un acuerdo propuesto por SecureNova Labs para la realización de pruebas de intrusión. Este

análisis permitió identificar cláusulas abiertamente incompatibles con el ordenamiento jurídico colombiano y con los deberes deontológicos del ingeniero, tales como la prohibición de denunciar posibles delitos informáticos, la exigencia de confidencialidad sobre actividades ilícitas y la pretensión de exonerar a la empresa de responsabilidad penal mediante acuerdos privados. Este contraste evidenció la importancia de revisar los instrumentos contractuales como parte integral de la gestión de riesgos de ciberseguridad (Guarnizo Portela, 2024).

En la Etapa 3 se implementó un escenario práctico de Red Team en un entorno de laboratorio construido con máquinas virtuales, compuesto por un equipo atacante con Parrot OS, un Host-A con Windows 7 Professional que expone el servicio vulnerable Rejetto HTTP File Server (HFS) 2.3 hacia una red "externa", y un Host-B con Windows 7 Professional ubicado en una red interna accesible únicamente a través de Host-A. Sobre esta topología se ejecutó una cadena completa de ataque: identificación y explotación de la vulnerabilidad CVE-2014-6287 en HFS 2.3, establecimiento de una sesión Meterpreter en Host-A, configuración de rutas y redirecciones para pivotar hacia la red 192.168.56.0/24 y, finalmente, explotación de la vulnerabilidad MS17-010 (EternalBlue) sobre el servicio SMB en Host-B, alcanzando privilegios de sistema y demostrando la posibilidad de crear y eliminar cuentas administrativas de forma controlada (CVE Program, s. f.; National Institute of Standards and Technology, s. f.; Offensive Security, s. f.).

La Etapa 4 retomó el mismo escenario desde la óptica de un equipo Blue Team, orientado a la detección, análisis y respuesta frente a la intrusión ejecutada previamente. Se definieron acciones de contención no destructivas, se revisaron indicadores de compromiso a nivel de sistema y red, y se propusieron medidas de hardening y monitoreo alineadas con marcos como los CIS Critical Security Controls y los CIS Benchmarks, así como con buenas prácticas de gestión de incidentes y valoración de riesgos de ciberseguridad (Center for Internet Security,

2021; CIS Security, 2020; Cichonski et al., 2012; CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024; Wazuh, Inc., s. f.).

Este informe técnico final tiene como propósito integrar dichas etapas en un único documento, articulando: i) un marco normativo y ético que delimite la actuación del profesional en pruebas de intrusión; ii) la descripción técnica detallada del escenario y de las estrategias Red Team implementadas; iii) el análisis defensivo desde la perspectiva Blue Team, incorporando monitoreo, respuesta y mejora continua; y iv) la relación entre las evidencias técnicas recogidas, los riesgos de negocio y las recomendaciones de gobierno y de infraestructura que podrían adoptar organizaciones con características similares a SecureNova Labs. En conjunto, se busca mostrar cómo la conjunción de fallos de configuración, ausencia de gestión de vulnerabilidades y debilidad en los controles de monitoreo puede derivar en compromisos de alto impacto, y cómo un enfoque estructurado de defensa en profundidad contribuye a contener y mitigar dichos riesgos de manera coherente con el marco jurídico colombiano y las buenas prácticas internacionales en ciberseguridad.

Justificación

La ejecución de ejercicios integrados de Red Team y Blue Team se ha convertido en una necesidad para organizaciones que dependen de forma crítica de sus sistemas de información y servicios digitales. La experiencia muestra que la simple existencia de políticas, controles y herramientas de seguridad no garantiza, por sí sola, una protección efectiva frente a amenazas avanzadas o incluso frente a ataques relativamente sencillos, si estos controles no se someten a pruebas periódicas en escenarios realistas (Bejtlich, 2013; PandaSecurity, 2018). Los ejercicios de intrusión controlada y de defensa coordinada permiten evaluar, en condiciones cercanas a la operación real, la efectividad de la arquitectura de seguridad, la robustez de los procesos y la capacidad de respuesta de los equipos técnicos (Chindrus & Caruntu, 2023; Kotwani et al., 2023).

En Colombia, esta necesidad operativa se ve acompañada por un marco jurídico robusto en materia de delitos informáticos y protección de datos personales. La Ley 1273 de 2009 introdujo tipos penales específicos para conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos, la violación de datos personales y la utilización de software malicioso, elevando el estándar de responsabilidad penal para quienes administran o acceden a sistemas de información (Congreso de la República de Colombia, 2009). A su vez, la Ley 1581 de 2012 y el Decreto 1377 de 2013 establecen principios y obligaciones en el tratamiento de datos personales, exigiendo que las organizaciones implementen medidas de seguridad proporcionales a los riesgos asociados al tratamiento de la información (Congreso de la República de Colombia, 2012; Presidencia de la República de Colombia, 2013).

En este contexto, cualquier prueba de seguridad mal planificada, carente de autorización expresa o que involucre el tratamiento inadecuado de datos personales, puede traducirse en responsabilidad penal, administrativa o disciplinaria para la organización y para los profesionales

involucrados. De ahí que el análisis conjunto de los componentes técnico, normativo, contractual y ético resulte indispensable para garantizar que los ejercicios de Red Team y Blue Team se ejecutan bajo parámetros de licitud y responsabilidad profesional (COPNIA, 2015; Guarnizo Portela, 2024).

El caso de estudio de SecureNova Labs proporciona un escenario propicio para explorar este equilibrio. Por una parte, la empresa requiere la realización de pruebas avanzadas de intrusión sobre su infraestructura; por otra, el acuerdo contractual propuesto incorpora cláusulas que, de ser aceptadas, podrían conducir a situaciones de encubrimiento de delitos o de renuncia indebida al deber de denuncia. Analizar estas tensiones permite al profesional de seguridad identificar cuándo un contrato pone en riesgo su ética y su responsabilidad jurídica, y formular condiciones mínimas para la celebración de acuerdos de pruebas de seguridad alineados con el interés público (CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024).

Desde el punto de vista técnico, el escenario diseñado —basado en sistemas operativos Windows 7 sin soporte, servicios vulnerables expuestos en máquinas con doble interfaz de red, ausencia de gestión de parches para vulnerabilidades críticas como MS17-010 y carencias en la segmentación y el monitoreo— refleja problemas frecuentes en entornos productivos (CVE Program, s. f.; Moreano Jurado, 2015). Demostrar, fase por fase, cómo un atacante puede encadenar estas debilidades para comprometer tanto la máquina expuesta (Host-A) como el servidor interno (Host-B) permite cuantificar de manera tangible el riesgo asociado a decisiones de diseño, operación y mantenimiento que, a primera vista, podrían considerarse menores.

Académicamente, el trabajo se justifica porque integra la reflexión sobre metodologías de pruebas de penetración, el estudio del marco jurídico y ético colombiano, la ejecución práctica de un ejercicio Red Team y el diseño de estrategias Blue Team apoyadas en estándares como los CIS Controls, los CIS Benchmarks y las guías de gestión de incidentes (Álvarez Intriago, 2018;

Center for Internet Security, 2021; CIS Security, 2020; Cichonski et al., 2012; Palomo Luna et al., 2024). Esta integración permite generar un producto que trasciende el ámbito de la asignatura y puede servir como referencia para profesionales que se enfrenten a retos similares en organizaciones reales.

Objetivos

Objetivo General

Analizar de manera integral el escenario de SecureNova Labs desde las perspectivas Red Team y Blue Team, articulando los marcos normativos y éticos aplicables con la demostración práctica de vulnerabilidades y la propuesta de medidas de mejora que fortalezcan la postura de ciberseguridad de la organización.

Objetivos Específicos

Caracterizar el marco legal y deontológico que regula las pruebas de seguridad informática en Colombia, con énfasis en la Ley 1273 de 2009, la normativa de protección de datos personales y el Código de Ética de COPNIA, y determinar sus implicaciones sobre los ejercicios de Red Team y Blue Team.

Diseñar y ejecutar un ejercicio Red Team en un entorno de laboratorio controlado que permita demostrar la explotación de Rejetto HFS 2.3 (CVE-2014-6287) en un Host-A, el uso de técnicas de pivoting y la explotación de MS17-010 en un Host-B, documentando la cadena de ataque y el impacto sobre la confidencialidad, integridad y disponibilidad de los sistemas comprometidos.

Analizar el mismo escenario desde la óptica del Blue Team, identificando indicadores de compromiso en el sistema operativo y en la red, proponiendo acciones de contención inmediata y definiendo medidas de hardening soportadas en estándares y buenas prácticas internacionales.

Integrar los resultados de las Etapas 1 a 4 en un análisis técnico que relacione las evidencias obtenidas con los riesgos de negocio, los requisitos legales y las obligaciones éticas del ingeniero, generando conclusiones y recomendaciones aplicables a entornos organizacionales reales.

Desarrollo Del Informe

Marco Teórico, Normativo y Ético

El punto de partida de este informe es el reconocimiento de que las pruebas de penetración constituyen una actividad intrusiva que, aunque orientada a la mejora de la seguridad, implica acceder a sistemas, servicios y, potencialmente, a datos sensibles bajo el control de terceros. Por tanto, su diseño y ejecución deben apoyarse simultáneamente en metodologías técnicas reconocidas y en el cumplimiento estricto del marco jurídico y de los códigos de ética profesional que regulan el ejercicio de la ingeniería y la protección de la información (Álvarez Intriago, 2018; COPNIA, 2015; Guarnizo Portela, 2024).

Desde la perspectiva metodológica, diversas propuestas han sistematizado la forma de abordar un ejercicio de pentesting. OSSTMM, PTES y las guías orientadas a riesgos coinciden en la necesidad de estructurar las pruebas en fases claramente definidas: planificación y alcance, recopilación de información (incluyendo OSINT), escaneo y enumeración, análisis y explotación controlada de vulnerabilidades, post-explotación, documentación y remediación (Álvarez Intriago, 2018; Incibe, 2019; Palomo Luna et al., 2024; Zuluaga Mateus, 2017). Este enfoque permite que las actividades ofensivas, lejos de ser acciones improvisadas, se desarrollen conforme a un plan previamente acordado, con objetivos claros, criterios de éxito, límites de actuación y procedimientos de retroalimentación hacia la organización.

En paralelo, la normativa colombiana configura el marco de licitud sobre el cual deben operar tanto los ejercicios Red Team como las actividades de defensa. La Ley 1273 de 2009 modificó el Código Penal para introducir tipos penales específicos relacionados con la protección de datos y sistemas de información, tales como el acceso abusivo a sistemas informáticos, la interceptación ilícita de comunicaciones, el daño informático y el uso de software malicioso,

entre otros (Congreso de la República de Colombia, 2009; Guarnizo Portela, 2024). Cualquier actuación que exceda el marco de autorización otorgado por la organización y que afecte sistemas o datos de terceros puede encajar en estas figuras.

Por su parte, la Ley 1581 de 2012 y el Decreto 1377 de 2013 desarrollan el régimen de protección de datos personales, introduciendo principios como legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, que también deben observarse al diseñar y ejecutar pruebas de seguridad que involucren bases de datos o sistemas con información de personas naturales (Congreso de la República de Colombia, 2012; Presidencia de la República de Colombia, 2013). En la práctica, esto implica, por ejemplo, el uso preferente de datos anonimizados en entornos de laboratorio, la minimización del uso de información real de clientes o empleados, y la implementación de medidas técnicas y organizativas que reduzcan la probabilidad de filtraciones durante un ejercicio de intrusión.

El Código de Ética de COPNIA refuerza estas obligaciones desde la dimensión deontológica. Entre otros aspectos, exige a los ingenieros actuar con probidad, proteger la información a la que tienen acceso en razón de su trabajo, rechazar órdenes contrarias a la ley y denunciar los hechos posiblemente delictivos de los que tengan conocimiento en el ejercicio profesional (COPNIA, 2015). De ello se desprende que un profesional de la seguridad no puede ampararse en acuerdos de confidencialidad para encubrir delitos, ni aceptar cláusulas contractuales que le impidan informar a las autoridades sobre actividades ilícitas detectadas durante una auditoría de seguridad (Guarnizo Portela, 2024).

Sobre este marco teórico, normativo y ético se construyó el resto del ejercicio. La intrusión demostrada en el entorno de laboratorio, basada en la explotación de HFS 2.3 y MS17-010, se diseñó específicamente para ejecutarse en máquinas virtuales aisladas, con datos de prueba, sin impacto sobre sistemas productivos y bajo un alcance claramente delimitado en el

contexto académico del seminario de especialización (CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024). Esta aproximación permite que las capacidades técnicas desarrolladas en el ejercicio Red Team y las estrategias Blue Team propuestas posteriormente se mantengan en coherencia con los principios de legalidad, proporcionalidad y responsabilidad profesional.

Estrategias Red Team

El diseño de las estrategias Red Team partió de la topología de laboratorio definida: un host atacante Parrot OS, un Host-A con Windows 7 Professional SP1 x64 con doble interfaz de red (192.168.40.12/24 y 192.168.56.101/24) y un Host-B con Windows 7 Professional SP1 x64 ubicado en la red 192.168.56.0/24, con el servicio SMB expuesto en el puerto 445/TCP. Host-A publicaba el servicio Rejetto HTTP File Server (HFS) 2.3 en el puerto 80/TCP hacia la red 192.168.40.0/24, constituyéndose en el punto de entrada al entorno interno.

Sobre esta base se siguió una metodología alineada con PTES/NIST SP 800-115:

- **Reconocimiento y mapeo del entorno:** identificación de los hosts accesibles desde Parrot y descubrimiento de puertos expuestos, corroborando la presencia del servicio HTTP no estándar en Host-A.
- **Identificación de la vulnerabilidad inicial:** al acceder a la URL http://192.168.40.12/ se confirmó que el servicio correspondía a Rejetto HFS 2.3. La revisión de fuentes públicas permitió asociar esta versión a la vulnerabilidad CVE-2014-6287, que habilita ejecución remota de comandos a través del parámetro search y el uso de macros {.exec|… .} en peticiones HTTP especialmente formadas.
- **Validación controlada de la vulnerabilidad:** se construyó una petición HTTP que inyectaba un comando ping desde Host-A hacia Parrot, mientras en Parrot se capturaba el

tráfico ICMP con tcpdump. La observación de los paquetes ICMP provenientes de 192.168.40.12 confirmó la ejecución remota del comando y, por tanto, la explotabilidad de HFS en Host-A.

- **Explotación automatizada con Metasploit:** se empleó el módulo exploit/windows/http/rejetto_hfs_exec con el payload windows/meterpreter/reverse_tcp, configurando a Host-A como objetivo y a Parrot como equipo de escucha. El exploit permitió establecer una sesión Meterpreter sobre Host-A, proporcionando control interactivo del sistema.
- **Pivoting hacia la red interna:** con la sesión Meterpreter en Host-A, se utilizó el módulo post/multi/manage/autoroute para registrar en Metasploit las rutas hacia las redes 192.168.40.0/24 y 192.168.56.0/24. Posteriormente, el módulo post/windows/manage/portproxy configuró una regla v4tov4 que redirigía el puerto 5000/TCP de Host-A hacia 192.168.56.102:445 (SMB de Host-B), abriendo además el puerto en el firewall de Windows. Con esto, el servicio SMB de Host-B quedó expuesto de forma controlada a través de Host-A.
- **Explotación de MS17-010 (EternalBlue) en Host-B:** desde Parrot se ejecutó el módulo exploit/windows/smb/ms17_010_eternalblue, apuntando a 192.168.40.12:5000. El módulo verificó que el destino era vulnerable, identificó la versión de Windows 7 SP1 y completó la explotación, cargando un payload Meterpreter x64 y abriendo una nueva sesión asociada a Host-B con privilegios NT AUTHORITY\SYSTEM.
- **Acciones de post-explotación:** en la sesión de Host-B se verificó el contexto de privilegios, se enumeraron interfaces y configuración, y en la imagen clonada del sistema se creó la cuenta local efímera HenryFraile con una contraseña fuerte, agregándola al grupo de Administradores y verificando su existencia mediante los comandos net user y net localgroup. Finalmente, la cuenta se eliminó de forma controlada, comprobando en el registro de seguridad de Windows los eventos correspondientes a creación, modificación de grupos y eliminación de cuentas (IDs 4720, 4732, 4733 y 4726).

Esta estrategia Red Team evidenció que un único servicio vulnerable expuesto en un host con doble interfaz de red puede ser suficiente para comprometer, mediante pivoting y explotación encadenada, tanto la máquina intermedia como el servidor interno, con impacto directo sobre la confidencialidad, integridad y disponibilidad de los activos de las organizaciones.

Estrategias Blue Team

La perspectiva Blue Team partió del supuesto de que el ataque se encontraba en curso o había ocurrido recientemente sobre la máquina Windows involucrada en la Etapa 3. El objetivo fue definir qué acciones debía ejecutar un equipo de defensa para confirmar el incidente, contenerlo sin destruir evidencia y fortalecer el entorno frente a futuros ataques.

Las estrategias se estructuraron en varios ejes:

- **Confirmación del incidente y aislamiento lógico**: antes de adoptar medidas radicales como el apagado de la máquina, se planteó la necesidad de corroborar la existencia de indicadores de compromiso (procesos o servicios anómalos, conexiones no habituales, creación de cuentas inesperadas). Una vez confirmado el incidente, la recomendación fue aislar lógicamente el equipo mediante dispositivos de red (VLAN de cuarentena, reglas de firewall, listas de control de acceso) para frenar el movimiento lateral sin perder la información contenida en la memoria y en los procesos activos.
- **Análisis de estado del sistema operativo y de las conexiones**: se propuso el uso de herramientas nativas y de software libre, como netstat -ano, tasklist /svc, wmic process list, ipconfig /all y el Administrador de tareas, para identificar procesos sospechosos, servicios iniciados recientemente y conexiones hacia puertos como 5000/TCP o 445/TCP que pudieran estar siendo usados como canal de pivoting. En el plano de red, la captura de tráfico mediante

Wireshark o tcpdump permitiría registrar sesiones HTTP, SMB y posibles túneles entre Parrot, Host-A y Host-B.

- **Revisión intensiva de logs y eventos de seguridad**: la consulta detallada del Visor de eventos, especialmente del registro de Seguridad, se planteó como una fuente clave para detectar eventos de inicio de sesión, escalamiento de privilegios, creación y eliminación de cuentas, y modificaciones en grupos de alto privilegio. En el escenario del laboratorio, esto permitiría identificar la cuenta efímera creada durante la intrusión y reconstruir la secuencia temporal de acciones.

- **Hardenización posterior al incidente**: aprovechando el conocimiento obtenido en la Etapa 3, se definieron acciones de hardening como la desinstalación o sustitución de HFS 2.3, la aplicación del parche MS17-010 en todos los sistemas afectados, la deshabilitación de SMBv1, la segmentación estricta de redes y el reforzamiento del firewall de Windows para limitar puertos expuestos. Estas medidas se alinean con los CIS Benchmarks y con los Controles Críticos de CIS, que priorizan la gestión de vulnerabilidades y la configuración segura de sistemas.

- **Uso de SIEM y herramientas de contención**: se resaltó el papel de un SIEM en la recolección, normalización y correlación de logs, así como en la generación de alertas ante patrones anómalos (por ejemplo, combinación de actividad inusual en HFS, cambios en cuentas administrativas y conexiones entre puertos 5000 y 445). Se recomendaron herramientas de contención como firewalls perimetrales y host-based (por ejemplo, pfSense), IPS libres (Snort, Suricata), soluciones NAC (PacketFence) y plataformas de seguridad como Wazuh con capacidades de respuesta activa, capaces de aislar automáticamente equipos comprometidos o bloquear IPs maliciosas.

Estas estrategias defensivas muestran cómo el aprendizaje obtenido en un ejercicio Red Team se traduce en controles concretos de detección y respuesta, reforzando el concepto de sinergia entre equipos ofensivos y defensivos.

Análisis técnico del incidente desde la perspectiva Blue Team

Desde la óptica defensiva, el incidente observado en el laboratorio puede describirse como una cadena de eventos que, en un entorno real, debería generar múltiples indicadores de compromiso tanto a nivel de host como de red. Reconstruir esta secuencia cronológica permite al Blue Team identificar qué señales debieron haberse detectado, qué herramientas podrían haberlas registrado y qué decisiones de contención habrían sido más adecuadas en cada momento (Bejtlich, 2013; Cichonski et al., 2012).

La intrusión se inicia con la explotación de Rejetto HFS 2.3 en Host-A. Desde el punto de vista de monitoreo, este primer paso se traduce en peticiones HTTP anómalas, con parámetros poco habituales en la cadena de consulta (search con contenido de macros) y posiblemente con patrones repetitivos propios de procesos automatizados. Un Blue Team con un proxy, un WAF o un IDS adecuadamente configurado podría generar alertas ante este tipo de solicitudes, basadas en firmas específicas o en reglas de comportamiento anómalo. Adicionalmente, en los registros de HFS y en los logs del sistema operativo de Host-A deberían aparecer entradas de acceso repetidas desde la IP del atacante, así como errores o advertencias derivados de la ejecución de comandos a nivel del sistema (Moreano Jurado, 2015).

Una vez que Metasploit obtiene una sesión Meterpreter en Host-A, se abren nuevas oportunidades de detección. En el plano del sistema operativo, el Blue Team podría identificar procesos inusuales asociados al payload, conexiones salientes desde Host-A hacia la máquina atacante en puertos no habituales (como el puerto 2222/TCP utilizado para la conexión reversa) y, eventualmente, modificaciones en la tabla de rutas o en la configuración de cortafuegos local.

Herramientas nativas como netstat -ano, tasklist /svc y el Visor de eventos de Windows permiten evidenciar estas anomalías, que, correlacionadas en un SIEM, deberían elevar el nivel de criticidad del incidente (Cichonski et al., 2012; Moreano Jurado, 2015).

El siguiente hito técnico es la configuración del pivoting y del portproxy en Host-A. En este punto, desde la perspectiva Blue Team, resulta clave identificar la apertura inesperada del puerto 5000/TCP en el firewall de Windows y la presencia de reglas de redirección de tráfico configuradas a través de netsh interface portproxy. La aparición de un servicio escuchando en un puerto no contemplado en la línea base del servidor, junto con tráfico entrante desde la red externa y saliente hacia la red interna, constituye un indicador claro de movimiento lateral. Estos eventos pueden recogerse mediante registros del firewall local, auditorías de cambios de configuración y sondas de red que monitoricen conexiones entre segmentos (Bejtlich, 2013; CCN-CERT, 2018).

La explotación de MS17-010 en Host-B a través del canal establecido completa la fase de compromiso profundo. En un escenario real, el Blue Team debería monitorizar de forma prioritaria los servidores Windows con servicios SMB expuestos, correlacionando intentos de conexión desde orígenes no habituales, errores de autenticación, mensajes de fallo en el servicio y posibles reinicios inesperados. Los registros de seguridad de Windows pueden contener eventos relacionados con errores en el servicio de servidor (srv) o con accesos anómalos a recursos compartidos. Un IDS/IPS de red, desplegado en el segmento donde reside Host-B, podría detectar firmas asociadas al exploit EternalBlue y generar alertas de alta criticidad (National Institute of Standards and Technology, s. f.; Offensive Security, s. f.).

Finalmente, en la fase de post-explotación sobre Host-B, la creación y eliminación de la cuenta efímera HenryFraile deja una huella muy clara en el registro de seguridad de Windows. Eventos como 4720 (creación de cuenta), 4732 y 4733 (adición y eliminación de miembros en

grupos de privilegio, como Administradores) y 4726 (eliminación de cuenta) constituyen indicadores directos de manipulación de identidades privilegiadas. Un caso de uso bien definido en el SIEM debería generar alertas inmediatas cuando se crean cuentas administrativas fuera de los procedimientos estándar, o cuando se modifica la composición del grupo de administradores locales en servidores críticos (Cichonski et al., 2012; Moreano Jurado, 2015).

En conjunto, este análisis técnico del incidente demuestra que, aunque el atacante se apoyó en vulnerabilidades conocidas y herramientas ampliamente documentadas, existieron múltiples puntos de observación en los que un Blue Team con capacidades maduras pudo haber detectado actividad anómala. La lección principal es que la eficacia defensiva no depende únicamente de instalar herramientas, sino de definir casos de uso concretos, mantener líneas base de comportamiento normal y correlacionar de manera inteligente los indicadores de compromiso generados a lo largo de toda la cadena de ataque (Bejtlich, 2013; Zambrano Hernández et al., 2024).

Análisis técnico integrador de las Etapas 1 a 4

El valor central de este informe final no reside únicamente en la ejecución aislada de actividades Red Team o Blue Team, ni en la mera revisión del marco legal aplicable, sino en la integración coherente de las cuatro etapas desarrolladas en torno a un mismo caso de estudio: la organización ficticia SecureNova Labs y su infraestructura vulnerable. Este apartado profundiza en esa integración, mostrando cómo cada etapa aporta insumos específicos al ciclo completo de gestión de la seguridad, desde la planificación y la definición de límites legales hasta la explotación técnica, la respuesta defensiva y la formulación de recomendaciones de mejora continua.

En términos generales, las Etapas 1 y 2 aportan la “arquitectura conceptual” del ejercicio (marco normativo, metodológico y ético), mientras que las Etapas 3 y 4 materializan esa

arquitectura en un entorno técnico realista, primero desde la óptica ofensiva y luego desde la defensiva. El resultado es un ciclo cerrado en el que cada decisión técnica puede ser trazada hacia una justificación regulatoria o metodológica, y cada hallazgo práctico se traduce en lecciones de gobierno y cumplimiento para la organización.

Visión global del ciclo de pruebas realizadas a SecureNova Labs:

Desde una perspectiva de ciclo de vida, las cuatro etapas pueden organizarse de la siguiente forma:

Etapa 1: Fase de planificación y marco de referencia, en la que se identifican las normas penales y de protección de datos aplicables, se revisan metodologías de pruebas de penetración y se establecen los principios éticos que limitarán las actividades técnicas posteriores.

Etapa 2: Fase de evaluación del contexto contractual y de riesgos legales, donde se analiza el acuerdo propuesto por SecureNova Labs, se identifican cláusulas contrarias al ordenamiento jurídico y se determinan las condiciones mínimas que debería cumplir un contrato lícito de pruebas de seguridad.

Etapa 3: Fase de ejecución técnica ofensiva en un entorno controlado de laboratorio, en la que se demuestra la explotación de vulnerabilidades críticas, el movimiento lateral y el impacto real sobre sistemas Windows desactualizados, bajo las premisas metodológicas definidas en la Etapa 1.

Etapa 4: Fase de respuesta defensiva y propuesta de mejora, que recoge los hallazgos de la intrusión, los analiza desde la óptica de un Blue Team y los traduce en acciones de contención, hardening, monitoreo y gestión de riesgos alineadas con estándares reconocidos.

Esta secuencia reproduce, en la escala del seminario de especialización, el ciclo que deberían seguir las organizaciones maduras en ciberseguridad: planear, atacar de forma controlada, defender, aprender y ajustar sus controles. El análisis técnico integrador consiste

precisamente en demostrar cómo el trabajo realizado en cada etapa alimenta las siguientes, y cómo las conclusiones finales solo son comprensibles si se consideran en conjunto las dimensiones legal, contractual, técnica y organizacional.

Aporte de la Etapa 1: marco legal, metodológico y ético

La Etapa 1 constituye la base sobre la cual se apoyan todas las decisiones posteriores. Desde el punto de vista técnico, la revisión de metodologías como OSSTMM, PTES y las guías orientadas a riesgo permite estructurar el ejercicio de Red Team y Blue Team en fases claramente diferenciadas: reconocimiento, escaneo, enumeración, explotación, post-explotación, reporte y remediación.

En lugar de ejecutar ataques de forma aislada, la intrusión demostrada en la Etapa 3 se alinea con una lógica metodológica:

- El reconocimiento inicial del servicio HFS 2.3 se justifica como parte de la fase de recopilación de información.
- La validación de la vulnerabilidad CVE-2014-6287 mediante pruebas controladas de ejecución remota se integra en la fase de análisis de debilidades.
- La explotación con Metasploit, el uso de autoroute y portproxy, y la posterior explotación de MS17-010 en Host-B se inscriben en la fase de explotación y post-explotación documentada en las metodologías estudiadas.

En paralelo, la Etapa 1 delimita claramente qué sería admisible y qué no en un entorno real. La identificación de la Ley 1273 de 2009 y de la normativa de protección de datos personales evidencia que actividades como el acceso no autorizado a sistemas productivos, la exfiltración de información sensible o la instalación de malware en infraestructuras reales solo podrían efectuarse bajo autorizaciones expresas, contratos válidos y un tratamiento responsable

de la información. El laboratorio diseñado para la Etapa 3 respeta estas restricciones al trabajar con máquinas virtuales dedicadas, datos de prueba y un alcance previamente acotado.

Finalmente, la reflexión ética introducida en esta etapa trasciende lo normativo. No se trata únicamente de "cumplir la ley", sino de entender que el conocimiento técnico en materia de intrusión conlleva una responsabilidad profesional: las habilidades de explotación y pivoting demostradas posteriormente solo adquieren legitimidad cuando se aplican al servicio de la protección de la información y no para la comisión de delitos.

Aporte de la Etapa 2: análisis del acuerdo y gestión del riesgo legal

La Etapa 2 complementa el marco general incorporando la dimensión contractual. El análisis minucioso del acuerdo propuesto por SecureNova Labs permite evidenciar un riesgo que frecuentemente se subestima en la práctica: la posibilidad de que organizaciones intenten instrumentalizar a los profesionales de la seguridad para actividades de espionaje, interceptación ilegal o encubrimiento de delitos, amparándose en cláusulas de confidencialidad redactadas de forma abusiva.

Desde el punto de vista técnico, esta etapa introduce una lección crucial: un ejercicio de pruebas de penetración no comienza cuando se lanza el primer escaneo de puertos, sino cuando se revisan y negocian las condiciones contractuales. Un pentest técnicamente impecable puede ser jurídicamente inviable si el contrato:

- Prohíbe denunciar delitos informáticos detectados durante las pruebas.
- Exige guardar silencio frente a prácticas ilegales previas de la organización.
- Pretende exonerar de responsabilidad penal a la empresa frente a actividades ilícitas descubiertas por el equipo técnico.

El análisis de estas cláusulas y su contraste con el Código de Ética de COPNIA refuerzan la capacidad crítica del ingeniero para decidir cuándo aceptar o rechazar una oferta de trabajo. Integrado con las Etapas 3 y 4, este ejercicio muestra que la misma explotación de HFS 2.3 y MS17-010 que en el laboratorio se usa para fines académicos y de mejora, podría convertirse en herramienta de delito si se ejecutara en un contexto contractual viciado.

En este sentido, la Etapa 2 funciona como un "filtro ético y jurídico" previo a la ejecución técnica, y su integración con el resto del informe permite presentar a SecureNova Labs no solo como un entorno vulnerable desde el punto de vista tecnológico, sino también como un caso de riesgo reputacional y penal si persiste en utilizar acuerdos contractuales contrarios a la ley.

Aporte de la Etapa 3: ejecución Red Team y demostración de impacto

Figura 1

Banco de trabajo de máquinas virtuales creado en virtual box

Nota. Captura del banco de máquinas virtuales usado en el laboratorio (máquina atacante y objetivos). Elaboración propia.

Topologia de Red del Ejercicio Red Team. La topología del banco de trabajo se resume así:

Parrot (atacante)

- Sistema operativo: Parrot OS Security

- Dirección IP: 192.168.40.11
- Red accesible: 192.168.40.0/24
- Rol: equipo Red Team, ejecución de Metasploit, nmap y tareas de pivoting.

Host-A – Máquina Intermedia Vulnerable

- Sistema operativo: Windows 7 Professional SP1 x64
- IP NIC 1 (externa): 192.168.40.12 /24
- IP NIC 2 (interna): 192.168.56.101 /24
- Servicio vulnerable: Rejetto HTTP File Server 2.3 en 80/TCP
- Rol: máquina con vulnerabilidad inicial y puente entre redes externa e interna.

Host-B – Servidor Interno

- Sistema operativo: Windows 7 Professional SP1 x64
- IP (interna): 192.168.56.102 /24
- Servicios: SMB (puerto 445/TCP), otros servicios de servidor de laboratorio.
- Rol: servidor interno que solo ve el segmento 192.168.56.0/24, objetivo final del movimiento lateral.
- La comunicación directa entre Parrot y Host-B está bloqueada por diseño: Parrot solo alcanza 192.168.40.0/24; la única ruta hacia 192.168.56.0/24 pasa por Host-A.

Figura 2

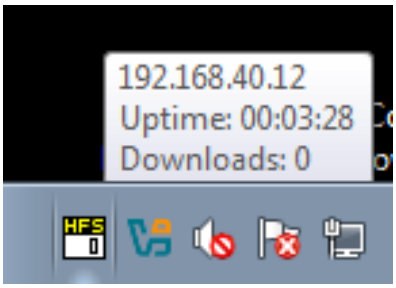
Direccionamiento de máquinas virtuales entorno banco de trabajo virtual box

Nota. Direccionamiento IP y segmentación del escenario (red externa e interna) usados para demostrar aislamiento y necesidad de pivoteo. Elaboración propia.

En el Host A se habilita la aplicación entregada; la cual es Rejjeto HFS (HTTP File Server) en su versión 2.3. Al habilitarlo se observa la aplicación corriendo en el servidor y lo puedo ver desde la maquina llamada Host A de la siguiente forma:

Figura 3

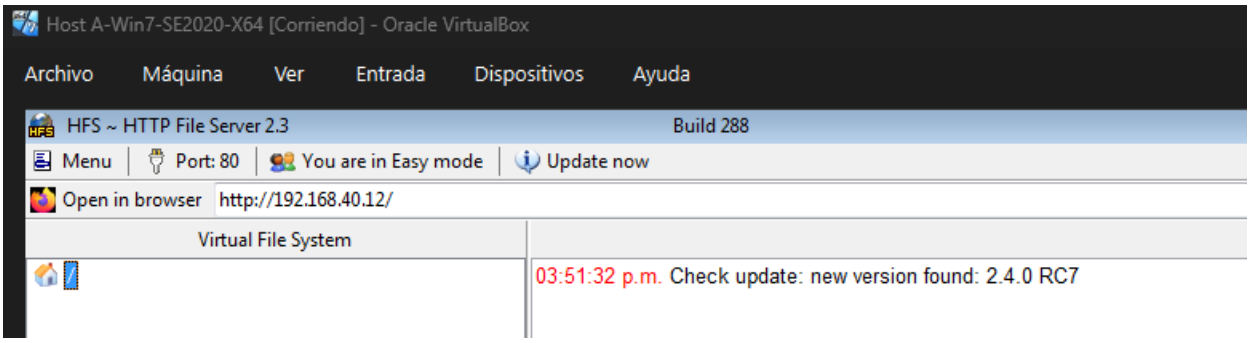
Servidor HFS 2.3 corriendo en Windows 7 Host A



Nota. Evidencia de que el servicio HFS 2.3 está en ejecución en el host vulnerable del laboratorio. Elaboración propia.

Figura 4

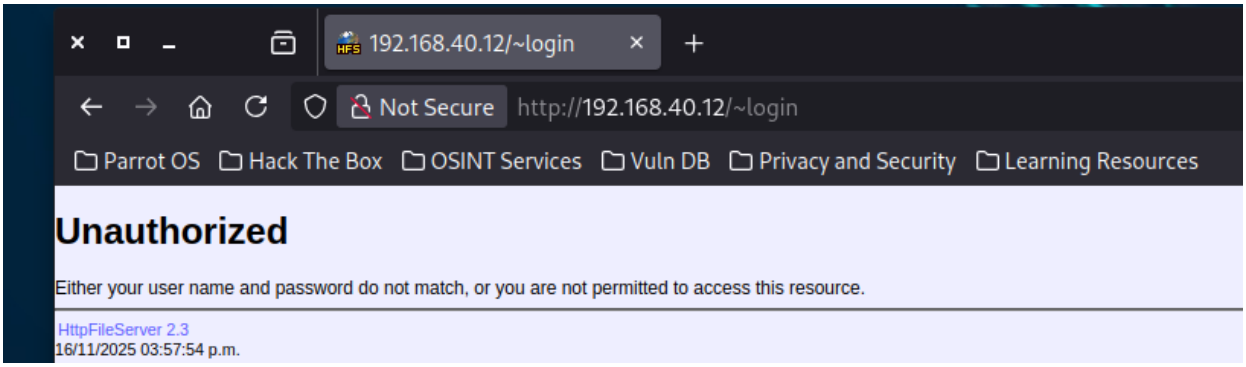
Entorno grafico servidor HFS desde Host A



Nota. Interfaz del servicio HFS 2.3 en el host vulnerable, utilizada para verificar estado y parámetros generales del servicio. Elaboración propia.

Figura 5

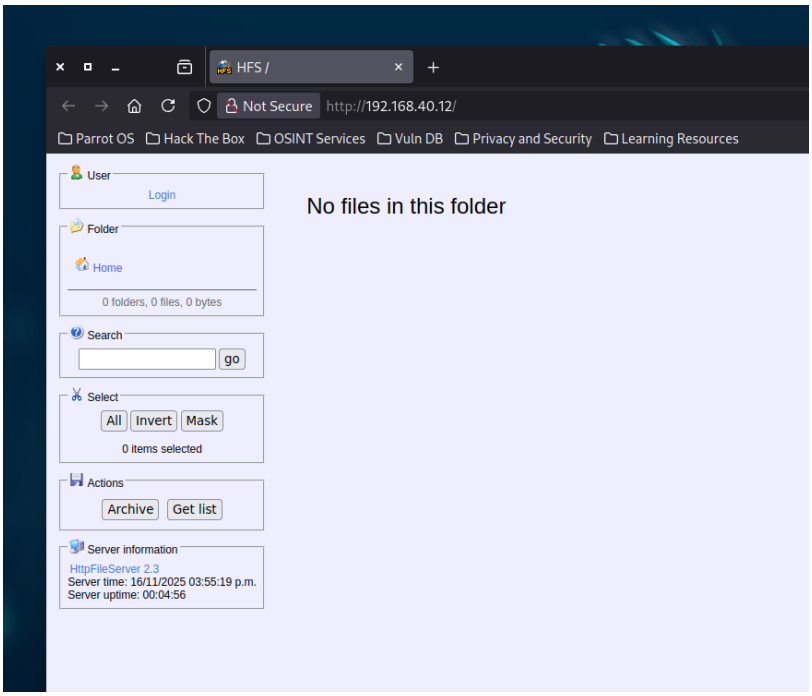
Versión de servidor HFS consultado desde máquina atacante



Nota. Validación remota (desde la máquina atacante) de la versión del servicio expuesto, empleada para el análisis de vulnerabilidad. Elaboración propia.

Figura 6

Versión cliente de servidor HFS vista desde máquina atacante



Nota. Vista cliente del servicio desde la máquina atacante, usada para confirmar versión/huella del servidor antes de la validación de la vulnerabilidad. Elaboración propia.

Plan de Ejecución del Ejercicio Red Team. Desde la maquina atacante (Parrot) comprometo al Host-A (Windows 7 64 Bits) explotando Rejetto/HFS 2.3, desde esa sesión se escalan privilegios y se configura Host-A como pivote hacia la red interna 192.168.56.0/24 donde solo se encuentra el Host B; a través de ese pivoting con la maquina Parrot ataco y comprometo el Host-B (servidor interno), obteniendo privilegios administrativos en Host-B y como PoC controlado (según solicitud de la guía de actividades), creo y elimino la cuenta administrativa efímera con formato primerNombre+primerApellido.

Metodología de Pentesting Empleada. Se empleo una estructura alineada con metodologías estándar de pruebas de penetración (PTES / NIST SP 800-115), adaptada al contexto académico:

Reconocimiento y Mapeo del Entorno

- Identificación de hosts accesible desde Parrot.
- Descubrimiento de servicios y versiones.

Escaneo y Enumeración

- Enumeración de puertos y servicios en Host-A.
- Identificación de tecnologías y posibles vulnerabilidades.

Explotación

- Explotación de Rejetto HFS 2.3 en Host-A (RCE).
- Obtención de sesión Meterpreter en Host-A.
- Explotación de MS17-010 en Host-B aprovechando el pivot SMB.

Post-explotación y Pivoting

- Enumeración de red desde Host-A (doble NIC).
- Configuración de rutas internas (autoroute) y portproxy (v4tov4) para exponer el SMB de Host-B.
- Establecimiento de sesión con privilegios elevados en Host-B.

Acciones Controladas en Host-B

- Creación de cuenta administrativa efímera en la imagen clonada.
- Eliminación posterior de la cuenta.
- Recopilación de evidencias en el registro de seguridad.
    - Consideraciones éticas y de buenas prácticas.

Identificación y Validación de la Vulnerabilidad en Rejetto HFS 2.3 (CVE-2014-6287).

Durante la fase de reconocimiento externo se identificó que la máquina intermedia Host-A (192.168.40.12) exponía el puerto 80/TCP ejecutando un servicio HTTP que no correspondía a un servidor web tradicional. El acceso desde la máquina atacante Parrot (192.168.40.11) a la

URL http://192.168.40.12/ permitió confirmar que se trataba de Rejetto HTTP File Server (HFS) en su versión 2.3, herramienta ligera para compartir archivos a través de HTTP ampliamente documentada en comunidades técnicas y bases de datos de vulnerabilidades (CVE Program, s. f.; Offensive Security, s. f.).

Con base en esta identificación se procedió a revisar las vulnerabilidades públicas asociadas a dicha versión, encontrando la CVE-2014-6287, clasificada como una vulnerabilidad de ejecución remota de código (RCE). Diversas fuentes señalan que el problema reside en el manejo del parámetro search por parte del motor de macros de HFS: bajo determinadas condiciones, es posible inyectar expresiones de macro que terminan interpretándose como comandos del sistema operativo, lo que abre la puerta a que un atacante ejecute instrucciones arbitrarias en el servidor (CVE Program, s. f.; National Institute of Standards and Technology, s. f.; Offensive Security, s. f.).

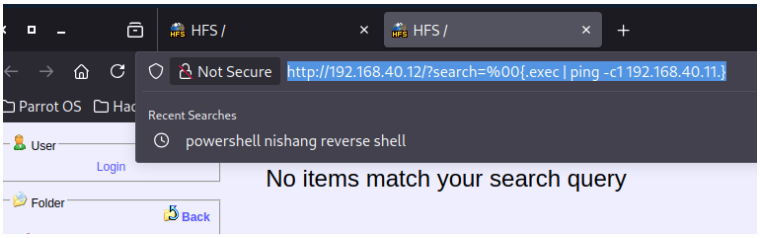
Para comprobar que la instancia concreta desplegada en Host-A era vulnerable, se diseñó una prueba controlada con impacto mínimo sobre el sistema. Específicamente, se construyó una petición HTTP en la que el parámetro search contenía una macro del tipo {.exec|… .} orientada a lanzar un comando ping desde Host-A hacia la dirección IP de Parrot (192.168.40.11). De forma paralela, en Parrot se inició una captura de tráfico en la interfaz conectada a la red 192.168.40.0/24 utilizando tcpdump, con el fin de detectar cualquier tráfico ICMP saliente desde Host-A.

Tras enviar la petición manipulada al servicio HFS, en la consola de captura de Parrot se observaron paquetes ICMP Echo Request originados en 192.168.40.12 con destino 192.168.40.11, seguidos de las correspondientes respuestas Echo Reply. Esta evidencia demuestra que el sistema operativo de Host-A ejecutó efectivamente el comando ping como

consecuencia directa de la petición HTTP enviada al servicio, confirmando así la explotación práctica de la vulnerabilidad CVE-2014-6287 en el entorno de laboratorio.

Figura 7

Petición HTTP al servidor HFS en Host A (Rejjeto)

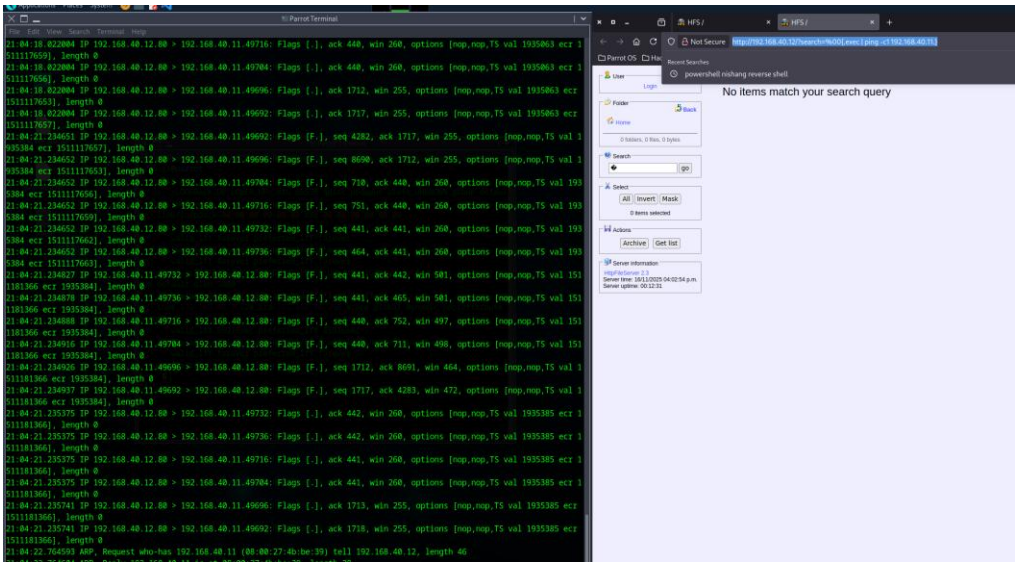


Nota. Solicitud HTTP especialmente construida usada como prueba de concepto para validar ejecución remota de comandos en HFS 2.3 (CVE-2014-6287) dentro del entorno controlado de laboratorio. Elaboración propia.

http://192.168.40.12/?search=%00{.exec%20|%20ping%20-c1%20192.168.40.11.}

Figura 8

Captura de paquetes ICMP realizado desde la explotación de macros en Host A rejjeto



Nota. Correlación de evidencia: a partir de la solicitud enviada al servicio, se observa tráfico generado por el host vulnerable en la captura de red, confirmando la ejecución como consecuencia directa de la explotación en el laboratorio. Elaboración propia.

Esta imagen evidencia simultáneamente:

- A la derecha, la interfaz web de HFS 2.3 en Host-A con la URL utilizada en la prueba, donde el parámetro search contiene la carga maliciosa.
- A la izquierda, la salida de tcpdump en Parrot registrando el tráfico ICMP generado por Host-A inmediatamente después de la explotación.

Con esta prueba confirmo que:

- El servicio HFS 2.3 desplegado en Host-A es vulnerable a CVE-2014-6287.
- Un atacante remoto ubicado en la red 192.168.40.0/24 (Parrot) puede ejecutar comandos arbitrarios en Host-A simplemente enviando una petición HTTP especialmente formada al puerto 80/TCP.

A partir de este hallazgo se estableció el vector inicial de compromiso del escenario: un atacante ubicado en la red 192.168.40.0/24, sin credenciales previas y con acceso al puerto 80/TCP de Host-A, puede obtener capacidad de ejecución de comandos en dicho host utilizando exclusivamente peticiones HTTP especialmente construidas, lo cual sienta las bases para la posterior obtención de una sesión interactiva y la preparación del pivoting hacia la red interna 192.168.56.0/24 (Host-B).

Establecimiento de una sesión Meterpreter en Host-A mediante explotación remota de HFS 2.3 (Rejjeto). Tras comprobar que la vulnerabilidad asociada a Rejetto HFS 2.3 permitía la ejecución de código remoto, se avanzó desde una prueba básica (envío de ping desde Host-A hacia Parrot) hacia el objetivo operativo como atacante: obtener una sesión interactiva persistente en Host-A.

Para ello se utiliza el framework Metasploit, concretamente el módulo **exploit/windows/http/rejetto_hfs_exec**, el cual explota la vulnerabilidad de HFS y carga de forma automática un payload en la máquina víctima. En la máquina atacante Parrot

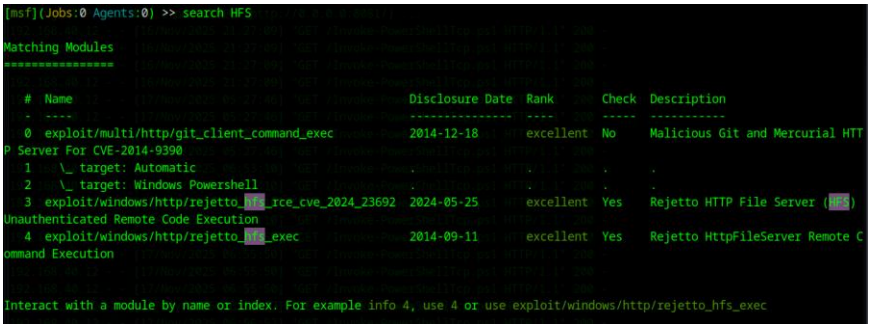
(192.168.40.11) se configuro dicho módulo estableciendo como objetivo a Host-A (192.168.40.12) sobre el puerto 80/TCP, seleccionando como payload windows/meterpreter/reverse_tcp, definiendo a Parrot como equipo de escucha (LHOST=192.168.40.11, LPORT=2222).

Al ejecutar el exploit, Metasploit se levanta un servidor HTTP temporal en Parrot y envió a HFS en Host-A una petición HTTP especialmente construida hacia la ruta raíz /. Esta petición provocó que el servicio HFS solicitara al servidor HTTP de Metasploit un recurso ubicado en una URL aleatoria y ejecutara el contenido recibido en el contexto del sistema operativo de Host-A. Ese contenido correspondía al payload de Meterpreter, que al iniciarse estableció una conexión reversa desde Host-A hacia el handler en Parrot.

Como resultado, Metasploit abrió correctamente una sesión Meterpreter desde la dirección 192.168.40.12, lo que me permitió disponer de una consola interactiva sobre Host-A, con capacidad para ejecutar comandos, recopilar información del sistema y preparar las fases de post-explotación y pivoting hacia el Host B 192.168.56.0/24.

Figura 9

Buscando exploits de HFS

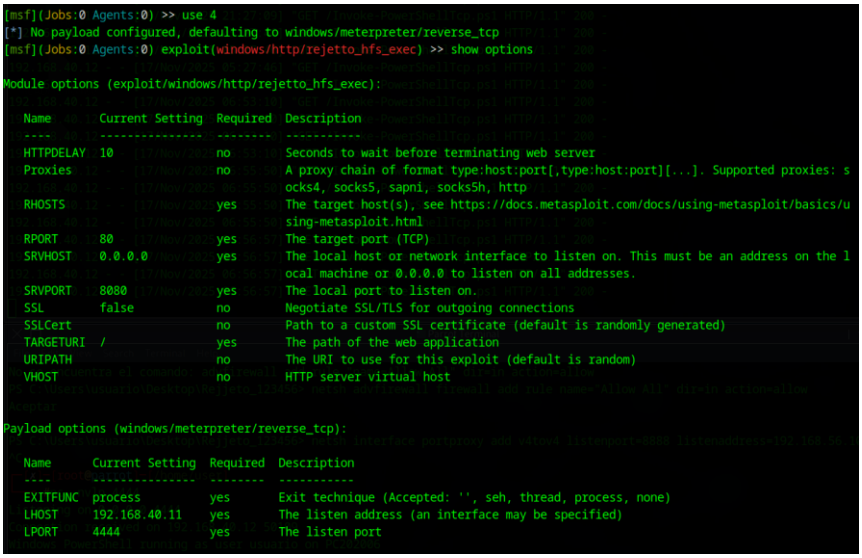


Nota. Búsqueda de módulos/vectores de explotación asociados al servicio HFS para seleccionar el método de prueba en el laboratorio. Elaboración propia.

Explicado comando por comando de la siguiente forma: primero se inicia metasploit para buscar los exploits relacionados con HFS, use el numero 4

Figura 10

Seleccionando exploit indicado para explotar HFS.

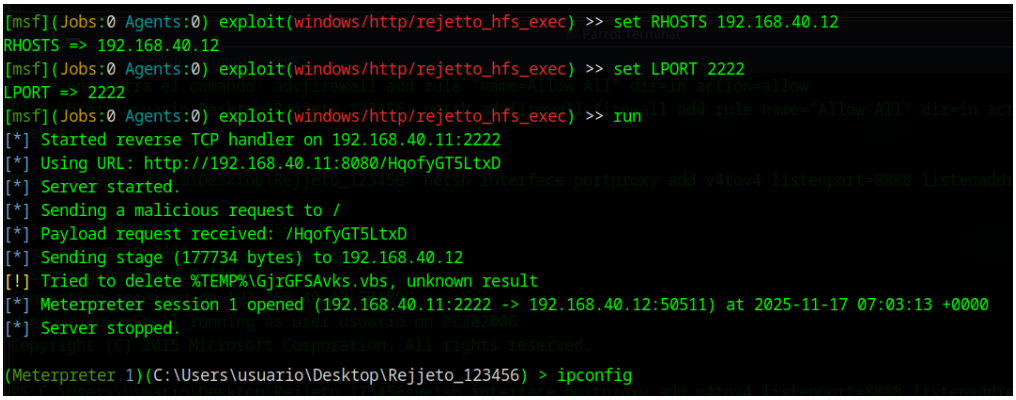


Nota. Selección del módulo de explotación para ejecutar la prueba de compromiso controlada del servicio HFS en el host objetivo. Elaboración propia.

Luego se configuran las opciones y se ejecuta de la siguiente manera:

Figura 11

Configuración de opciones exploit rejetto_hfs_exec

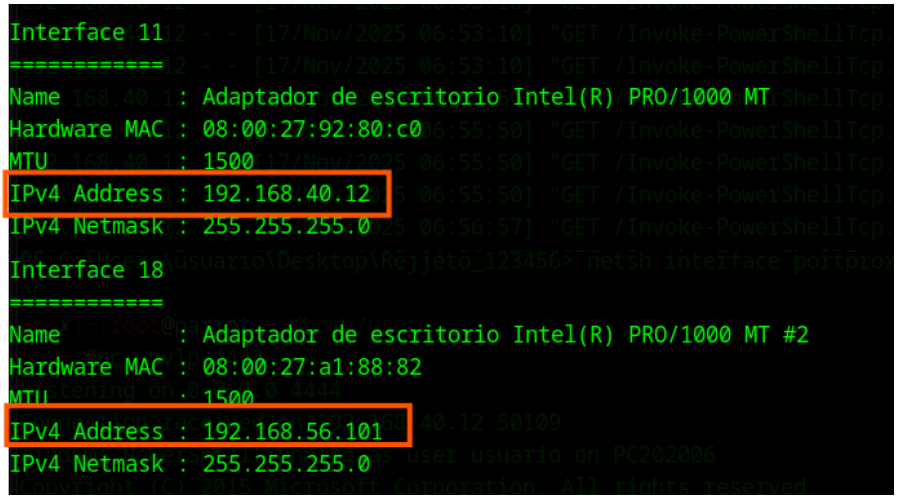


Nota. Parámetros de configuración del módulo (objetivo, puertos y “listener”) ajustados a las direcciones del laboratorio para obtener una sesión remota controlada. Elaboración propia.

Con esto logramos ganar acceso de administrador al Host A revisando de primera medida sus interfaces de red:

Figura 12

Interfaz de red Host A externa



Nota. Enumeración de interfaces en el host comprometido que evidencia doble conectividad (segmento externo e interno), condición necesaria para realizar el pivoting hacia la red interna. Elaboración propia.

Pivoting Host-A → Host-B y Explotación de MS17-010 (EternalBlue) a través de SMB.

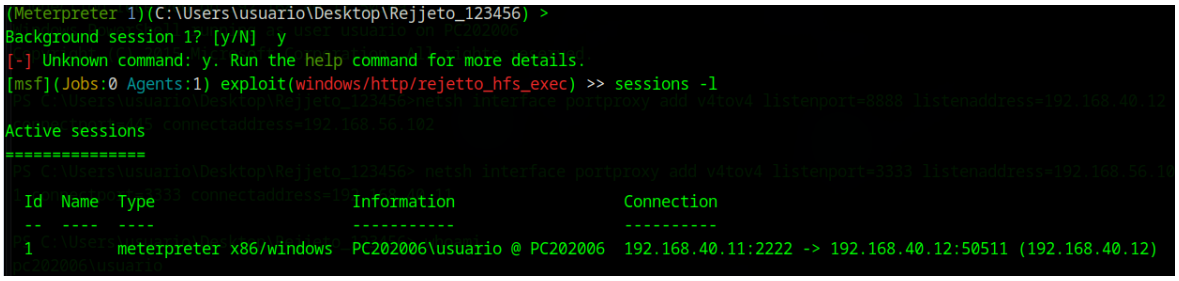
Una vez obtenida una sesión Meterpreter estable en Host-A mediante la explotación de Rejetto HFS 2.3, el siguiente objetivo consistió en aprovechar la posición alcanzada para extender el alcance del ataque hacia la red interna 192.168.56.0/24, donde se encontraba el servidor Host-B. Esta transición se realizó aplicando técnicas de pivoting soportadas por los módulos de post-explotación de Metasploit, de manera coherente con las fases de movimiento lateral descritas en la literatura de Red Teaming (Bejtlich, 2013; Kotwani et al., 2023).

En primer lugar, se suspendió temporalmente la interacción directa con la sesión de Meterpreter en Host-A para lanzar el módulo **post/multi/manage/autoroute**. Este módulo analiza la tabla de rutas del sistema comprometido y registra, en el contexto de Metasploit, las

redes a las que Host-A tiene conectividad. En el escenario de laboratorio, se añadieron automáticamente dos rutas: una hacia 192.168.40.0/24 (segmento “externo”, donde reside Parrot) y otra hacia 192.168.56.0/24 (segmento “interno”, donde se encuentra Host-B). Con ello se indicó al framework que todo tráfico dirigido a la red interna debía ser canalizado a través de la sesión de Host-A.

Figura 13

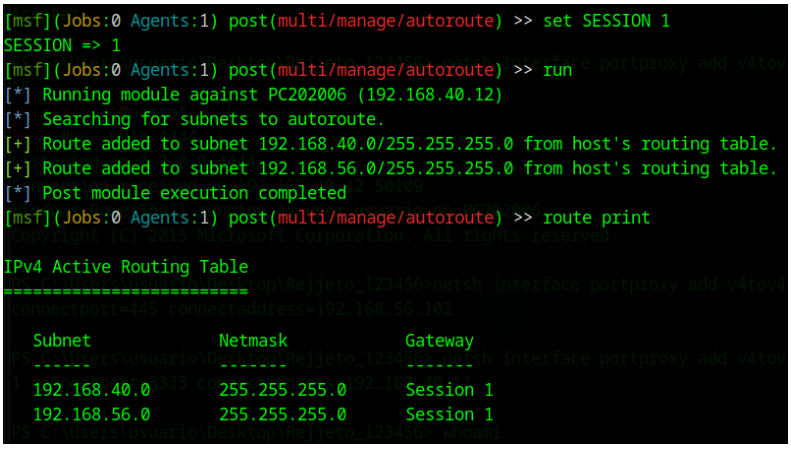
Enviando la sesión de meterpreter a segundo plano



Nota. Cambio de estado de la sesión remota para ejecutar módulos de post-explotación sin perder acceso al host intermedio. Elaboración propia.

Figura 14

Corriendo exploit autoroute

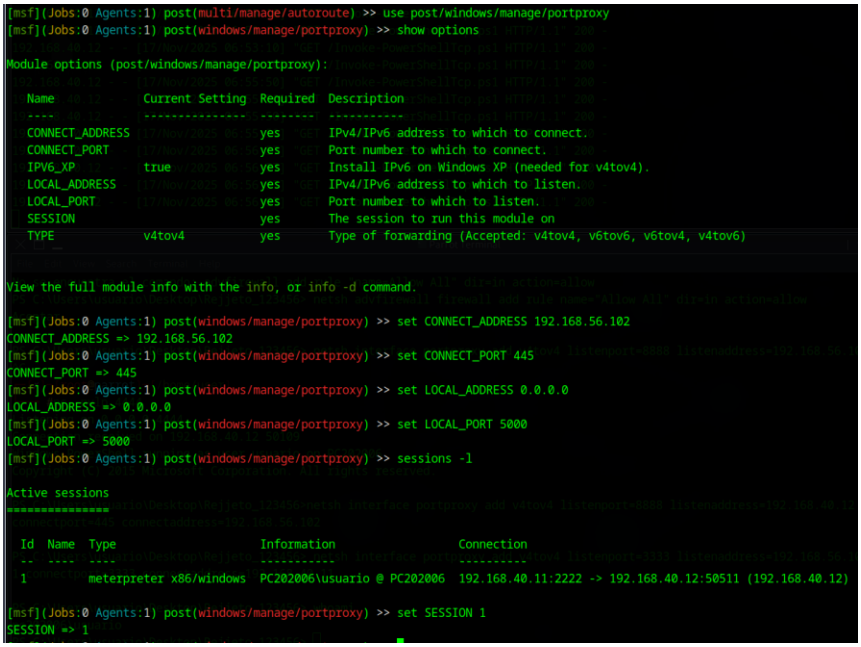


Nota. Registro de rutas hacia redes alcanzables desde el host intermedio, habilitando el enrutamiento del tráfico a la red interna a través de la sesión comprometida. Elaboración propia.

Posteriormente, se configuró un mecanismo de redirección de puertos a nivel del propio sistema Windows comprometido, utilizando el módulo **post/windows/manage/portproxy**. Se creó una regla de tipo v4tov4 que redirigía el tráfico recibido en Host-A en el puerto 5000/TCP hacia el servicio SMB de Host-B en el puerto 445/TCP, abriendo a su vez la regla correspondiente en el firewall local. En términos prácticos, cualquier conexión que la máquina atacante realizara a 192.168.40.12:5000 sería reenviada de forma transparente hacia 192.168.56.102:445, exponiendo de manera controlada el servicio SMB interno a través del pivote.

Figura 15

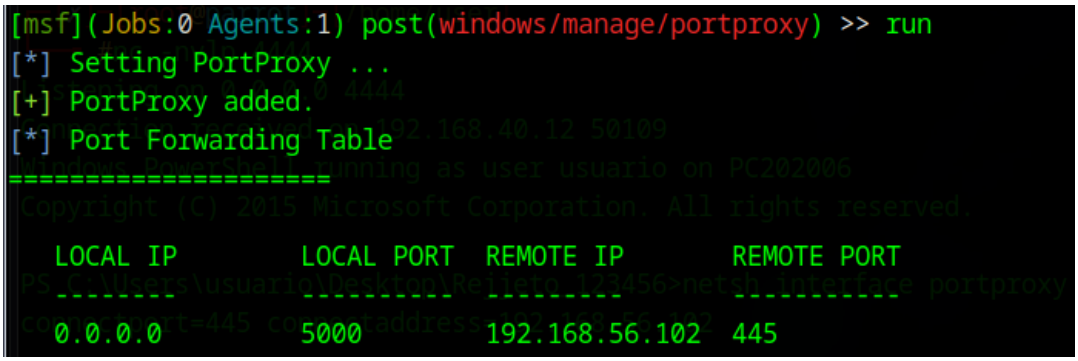
Configurando opciones de exploit de portproxy



Nota. Configuración de redirección de puertos en el host intermedio para exponer de forma controlada el servicio SMB del host interno a través del pivote, según el escenario del laboratorio. Elaboración propia.

Figura 16

Ejecutando exploit portproxy

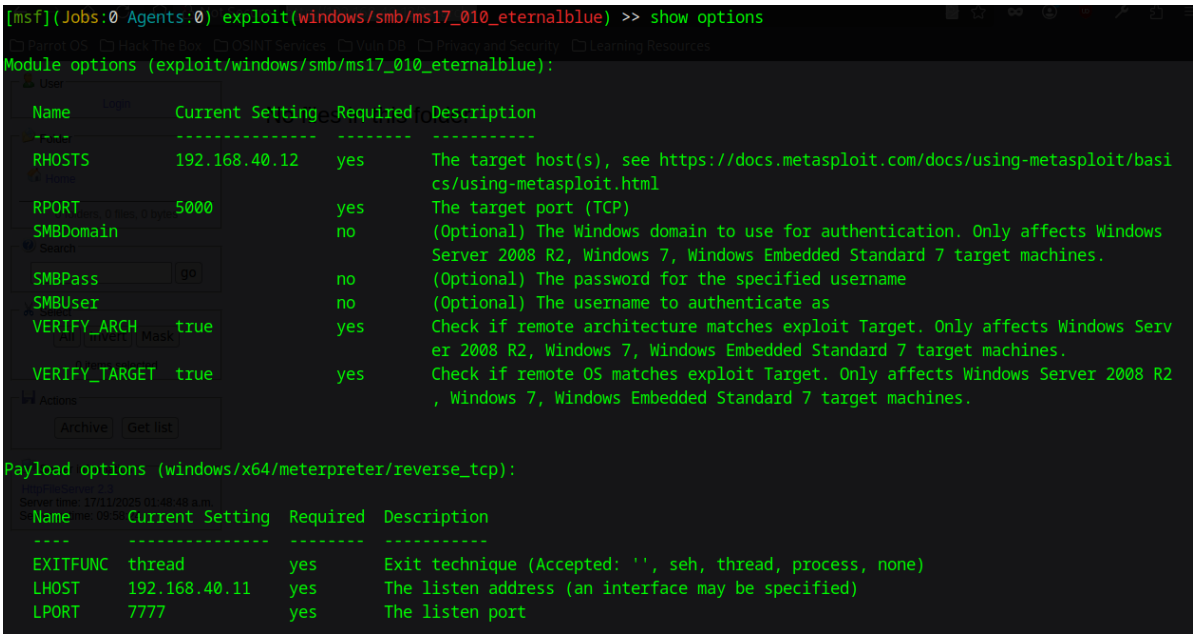


Nota. Evidencia de ejecución/activación de la redirección de puertos y ajustes asociados para permitir el tránsito hacia el servicio interno a través del host pivote. Elaboración propia.

Sobre esta infraestructura de pivoting se procedió a explotar la vulnerabilidad MS17-010, utilizando el módulo **exploit/windows/smb/ms17_010_eternalblue de Metasploit**. El módulo se configuró apuntando a RHOSTS=192.168.40.12 y RPORT=5000, es decir, hacia el host intermedio y el puerto redirigido. Durante la etapa de verificación, la herramienta identificó que el destino final correspondía a un sistema Windows 7 Professional Service Pack 1 x64 vulnerable a MS17-010, lo que permitió continuar con la explotación hasta completar la ejecución remota de código en el contexto del kernel (National Institute Standards and Technology, s. f.; Offensive Security, s. f.).

Figura 17

Configurando opciones de ms17_010_eternalblue



Nota. Parámetros del módulo de verificación/explotación ajustados para alcanzar el host interno a través del puerto redirigido en el pivote (laboratorio). Elaboración propia.

Una vez satisfecha la condición de explotación, el módulo cargó el payload **windows/x64/meterpreter/reverse_tcp**, configurado para establecer una conexión reversa desde Host-B hacia la máquina atacante Parrot. La apertura de una nueva sesión Meterpreter, distinta de la inicial, permitió verificar, mediante los comandos sysinfo, ipconfig y getuid, que se trataba efectivamente de Host-B (IP 192.168.56.102) y que la sesión se ejecutaba con privilegios de NT AUTHORITY\SYSTEM. De esta manera, se demostró en la práctica que la combinación de un servicio vulnerable expuesto en Host-A, una configuración de red con doble interfaz y la ausencia de parches críticos en Host-B permite a un atacante externo romper la segmentación lógica y comprometer un servidor interno que, en principio, no es accesible directamente desde el exterior.

Figura 18

Ejecutando exploit ms17_010_eternalblue

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run
[*] Started reverse TCP handler on 192.168.40.11:7777
[*] 192.168.40.12:5000 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.40.12:5000    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.40.12:5000    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.40.12:5000 - The target is vulnerable.
[*] 192.168.40.12:5000 - Connecting to target for exploitation.
[+] 192.168.40.12:5000 - Connection established for exploitation.
[+] 192.168.40.12:5000 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.40.12:5000 - CORE raw buffer dump (42 bytes)
[*] 192.168.40.12:5000 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.40.12:5000 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.40.12:5000 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.40.12:5000 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.40.12:5000 - Trying exploit with 12 Groom Allocations.
[*] 192.168.40.12:5000 - Sending all but last fragment of exploit packet
[*] 192.168.40.12:5000 - Starting non-paged pool grooming
[+] 192.168.40.12:5000 - Sending SMBv2 buffers
[+] 192.168.40.12:5000 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.40.12:5000 - Sending final SMBv2 buffers.
[*] 192.168.40.12:5000 - Sending last fragment of exploit packet!
[*] 192.168.40.12:5000 - Receiving response from exploit packet
[+] 192.168.40.12:5000 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.40.12:5000 - Sending egg to corrupted connection.
[*] 192.168.40.12:5000 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.40.10
[*] Meterpreter session 1 opened (192.168.40.11:7777 -> 192.168.40.10:60365) at 2025-11-17 08:49:38 +0000
[+] 192.168.40.12:5000 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.40.12:5000 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.40.12:5000 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

(Meterpreter 1)(C:\Windows\system32) >
```

Nota. Evidencia de obtención de una nueva sesión remota en el host interno tras la explotación a través del pivote, confirmando compromiso del objetivo final. Elaboración propia.

Figura 19

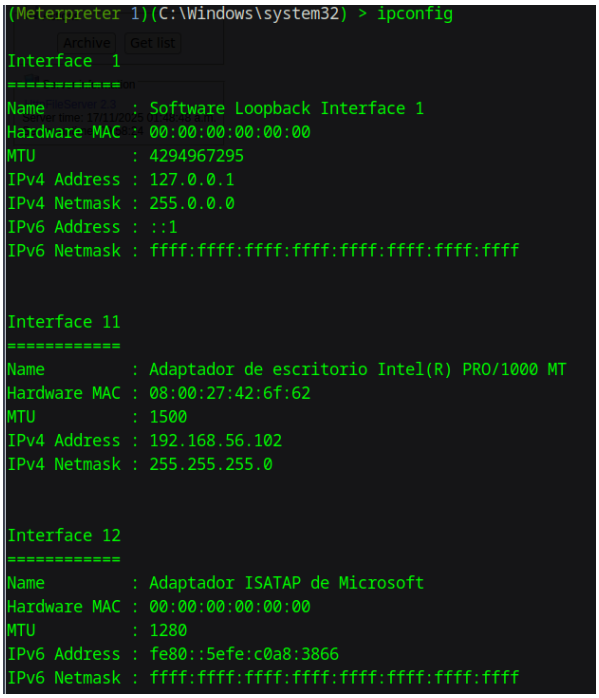
Ejecutando comando desde Host B

```
(Meterpreter 1)(C:\Windows\system32) > sysinfo
Computer        : PC202006
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_CO
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

Nota. Comandos de verificación ejecutados desde la sesión en el host interno para confirmar identidad del sistema comprometido y contexto de privilegios. Elaboración propia.

Figura 20

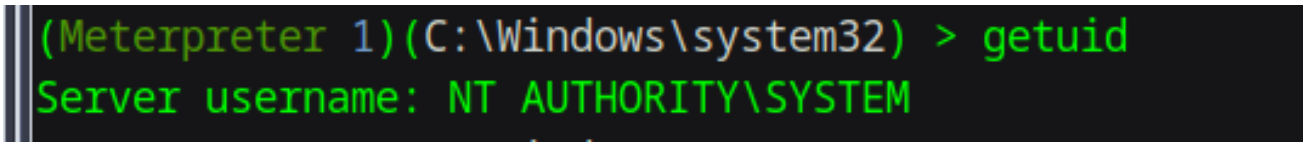
Ejecutando comandos desde Host B



Nota. Evidencias complementarias de validación (enumeración/confirmación operativa) ejecutadas en el host interno durante la post-explotación controlada. Elaboración propia.

Figura 21

Ejecutando comando desde Host B



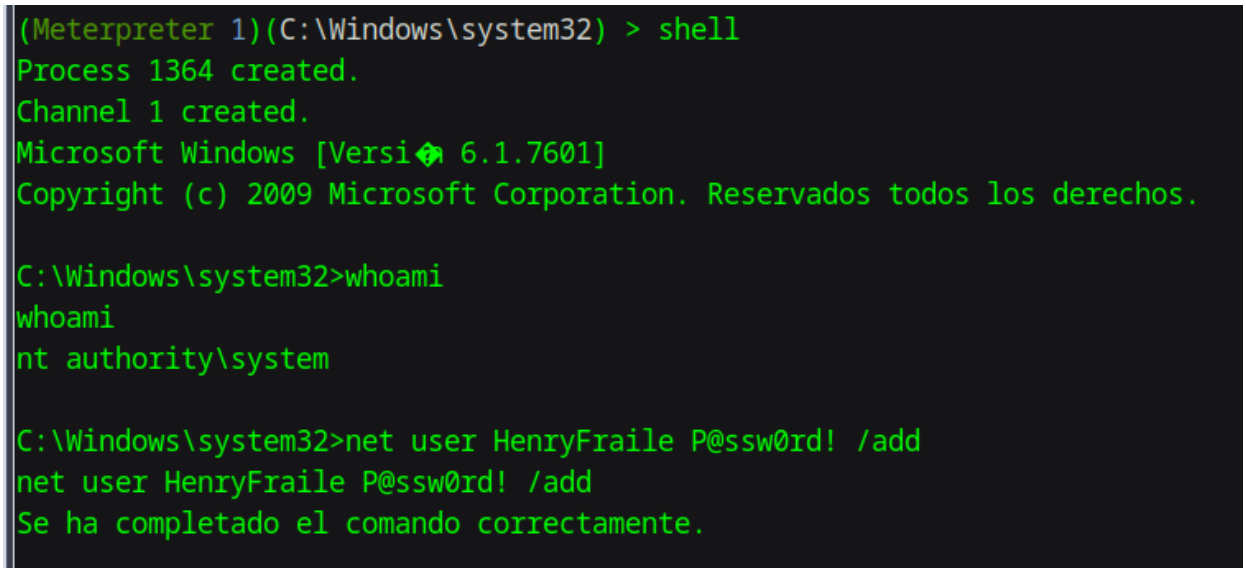
Nota. Verificación adicional desde el host interno para sustentar el acceso logrado y la continuidad de la sesión en el laboratorio. Elaboración propia.

Creación y eliminación de cuentas en Host B. En la fase final de post-explotación sobre la imagen clonada de Host-B, ya contando con una sesión con privilegios de **NT AUTHORITY\SYSTEM**, se realiza la creación y posterior eliminación de la cuenta administrativa efímera requerida por el escenario.

Primero, desde una consola cmd.exe elevada se verifica que el contexto de ejecución mediante whoami, confirmando que las acciones se ejecutarían con privilegios de sistema. A continuación, se crea la cuenta local con el formato solicitado *primerNombre+primerApellido*, Seguidamente, se le otorgue privilegios agregándolo al grupo local de administradores.

Figura 22

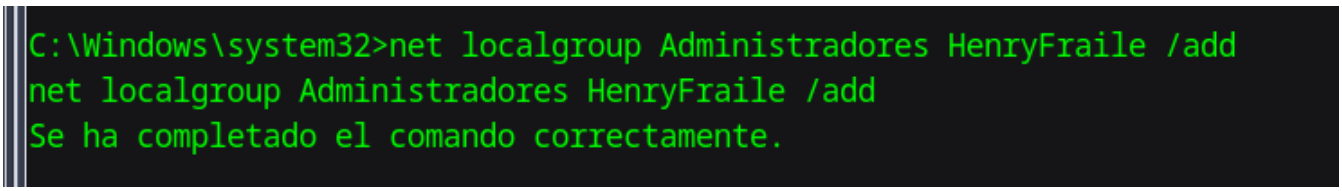
Ejecutando comandos desde shell con privilegios en Host B



Nota. Verificación del contexto elevado previo a la manipulación de cuentas locales en el host interno, como parte de la prueba de concepto solicitada por el laboratorio. Elaboración propia.

Figura 23

Ejecutando comandos desde shell con privilegios en Host B

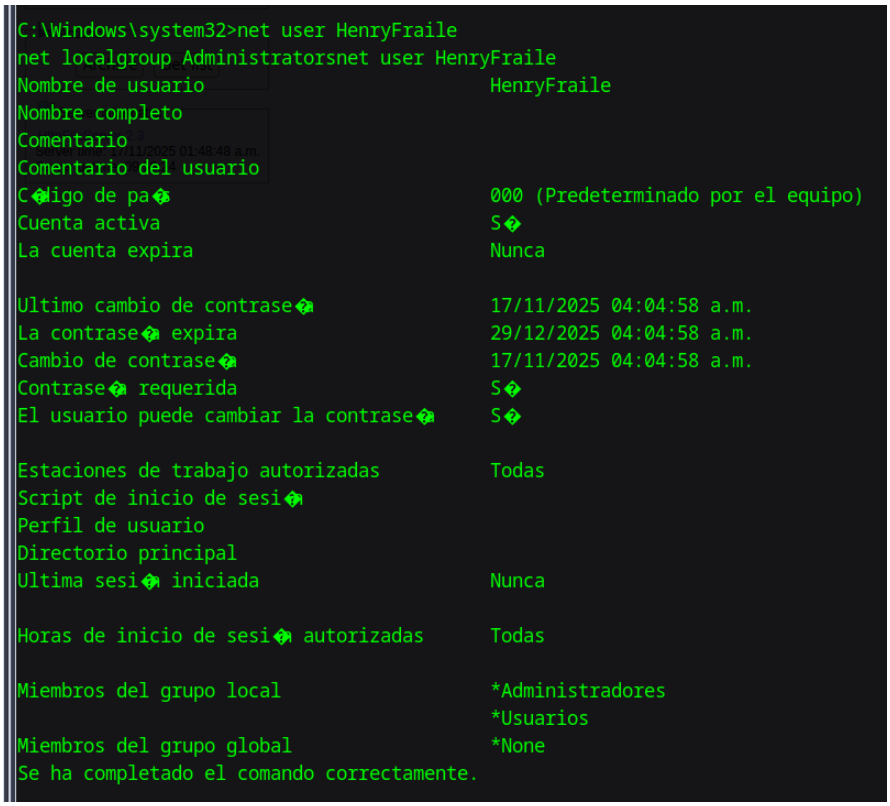


Nota. Creación de cuenta local temporal y asignación a grupo privilegiado en el host interno para demostrar impacto sobre gestión de identidades (entorno controlado). Elaboración propia.

Para validar la operación, ejecute:

Figura 24

Ejecutando comandos desde shell con privilegios en Host B



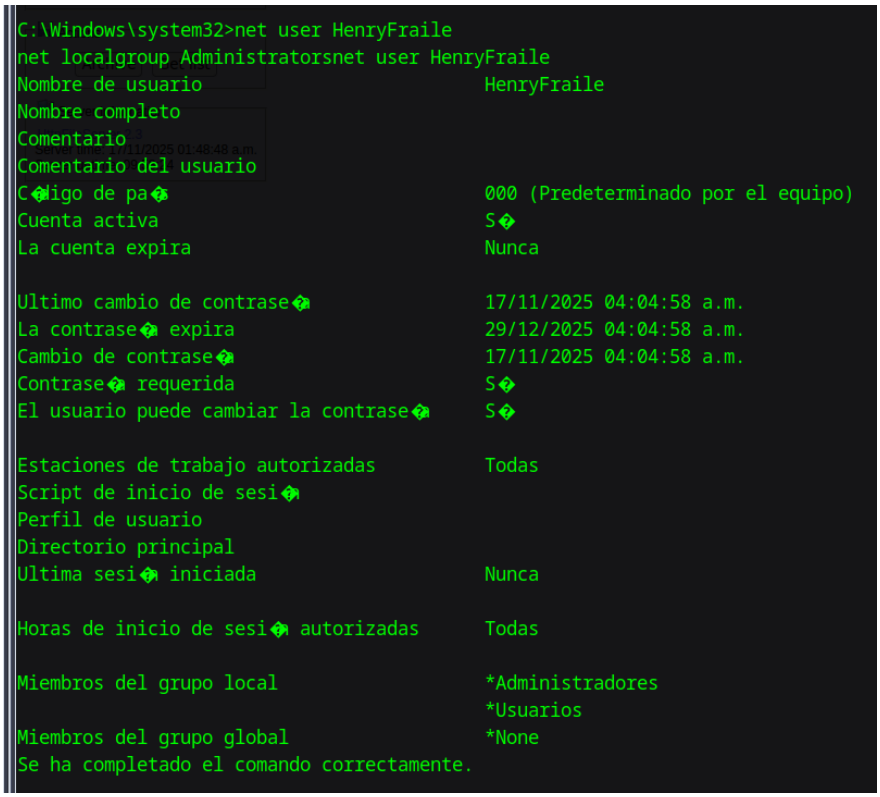
Nota. Validación de la existencia de la cuenta y su pertenencia a grupos locales, evidenciando privilegios asignados durante la prueba de concepto. Elaboración propia.

La salida de este comando nos indica que la cuenta HenryFraile se encuentra activa, con contraseña requerida y, en el apartado *Miembros del grupo local*, figuran los grupos Administradores y Usuarios, evidenciando que el nuevo usuario disponía de permisos de administrador en Host-B.

Una vez documentada la prueba de concepto, se procede a eliminar de forma controlada la cuenta efímera para no dejar persistencia en el sistema.

Figura 25

Ejecutando comandos desde shell con privilegios en Host B



Nota. Eliminación controlada de la cuenta temporal y verificación posterior para asegurar que no queda persistencia tras documentar la evidencia. Elaboración propia.

Comprobando que únicamente permanecían las cuentas locales originales (Administrador, Invitado y usuario) y que HenryFraile ya no figuraba en el sistema. Esta secuencia demuestra que, una vez comprometido Host-B con privilegios elevados, es posible crear una cuenta administrativa efímera siguiendo el formato indicado y eliminarla posteriormente.

Resultados del Ejercicio Red Team en la Etapa 3. La Etapa 3 constituye el corazón técnico ofensivo del trabajo. Allí se materializan en un entorno de laboratorio los riesgos identificados conceptualmente en las etapas previas. El análisis integrador permite mostrar cómo:

- La decisión de utilizar Windows 7 sin soporte y sin el parche MS17-010, junto con la publicación de HFS 2.3 en un host con doble interfaz de red, representa la combinación de varios errores de diseño y operación que se habían advertido en las discusiones teóricas de la Etapa 1.
- La cadena de ataque —explotación de HFS, establecimiento de Meterpreter, configuración de rutas y portproxy, explotación de SMB en Host-B— ilustra de forma concreta lo que, en la Etapa 1, se describía como "exposición de activos críticos sin gestión adecuada de vulnerabilidades".
- La posibilidad de crear y eliminar cuentas administrativas en Host-B demuestra que el impacto no se limita a obtener acceso temporal, sino que permite alterar la gestión de identidades y privilegios, con consecuencias directas sobre las dimensiones de integridad y trazabilidad.

Integrar la Etapa 3 con las Etapas 1 y 2 permite, además, traducir la narrativa técnica en un lenguaje de riesgo comprensible para la alta dirección de una organización:

- Un único servicio vulnerable expuesto en un host que conecta dos redes puede romper la segmentación lógica y permitir acceso no autorizado a servidores internos.
- La ausencia de parchado y de controles básicos de hardening convierte vulnerabilidades conocidas desde hace años en puertas de entrada para atacantes con capacidades relativamente estándar.
- La falta de monitoreo centralizado y de alertas basadas en eventos (creación de cuentas, conexiones anómalas, cambios en la configuración de red) favorece que este tipo de intrusiones pasen desapercibidas durante largos periodos.

Este análisis técnico, lejos de ser una simple “historia de explotación”, se convierte en evidencia concreta para sustentar las recomendaciones de gobierno, cumplimiento y mejora que se presentan más adelante en el informe.

Aporte de la Etapa 4: perspectiva Blue Team y cierre del ciclo

La Etapa 4 toma como insumo directo la intrusión demostrada en la Etapa 3 y la reinterpreta desde la óptica defensiva. El análisis integrador evidencia cómo los mismos eventos que, desde el punto de vista del atacante, se leen como “éxitos” (explotación, pivoting, escalamiento de privilegios), desde la perspectiva Blue Team se traducen en:

- Indicadores de compromiso a nivel de sistema operativo: procesos sospechosos, puertos abiertos inesperados, servicios modificados, creación de cuentas de usuario fuera de los procedimientos normales.
- Indicadores de compromiso a nivel de red: conexiones entre segmentos que deberían estar aislados, uso de puertos no habituales (por ejemplo, redirecciones sobre el puerto 5000/TCP hacia servicios SMB), patrones de tráfico que combinan HTTP, SMB y posibles túneles o backdoors.
- Oportunidades de mejora en la recolección y correlación de logs: eventos del registro de seguridad de Windows (creación y eliminación de cuentas, cambios en grupos de administradores), eventos de firewall, registros de IDS/IPS y de otros dispositivos de seguridad.

De este modo, la Etapa 4 cierra el ciclo definido metodológicamente en la Etapa 1: a partir de una intrusión controlada se identifican brechas de monitoreo, se proponen reglas de detección y casos de uso en el SIEM, y se plantean controles de hardening y segmentación que, de haber estado implementados, habrían dificultado o bloqueado la cadena de ataque Red Team.

En términos de madurez, la integración entre la Etapa 3 y la Etapa 4 permite mostrar dos fotografías contrapuestas de SecureNova Labs:

- Una "situación inicial" caracterizada por sistemas desactualizados, exposición innecesaria de servicios, falta de monitoreo y ausencia de procedimientos de respuesta a incidentes.
- Una "situación objetivo" en la que, a partir de las recomendaciones Blue Team, la organización cuenta con controles en capas (defensa en profundidad), capacidades de detección temprana y un marco de actuación ante incidentes apoyado en estándares reconocidos.

Trazabilidad entre amenazas, vulnerabilidades, controles y evidencias

Uno de los elementos más importantes del análisis integrador es la construcción de trazabilidad entre:

- Amenazas identificadas (intrusos externos, insiders maliciosos, malware, abuso de privilegios).
- Vulnerabilidades concretas (uso de Windows 7 sin soporte, ausencia de parchado MS17-010, despliegue de HFS 2.3 vulnerable, configuraciones de firewall permisivas, falta de segmentación efectiva).
- Controles propuestos (parchado sistemático, hardening según CIS Benchmarks, refuerzo de firewalls, deshabilitación de SMBv1, implementación de SIEM, uso de NAC, etc.).
- Evidencias técnicas obtenidas en el laboratorio (capturas de pantalla, salidas de comandos, registros de eventos, diagramas de topología, flujos de ataque y flujos de respuesta).

A partir del escenario de SecureNova Labs, esta trazabilidad puede ejemplificarse de manera sintética en una matriz que relacione vulnerabilidades concretas, evidencias observadas durante el laboratorio y controles de hardening propuestos para reducir el riesgo:

Tabla 1

Vulnerabilidades, Evidencias y Controles de Hardening Propuestos

VULNERABILIDAD / DEBILIDAD DETECTADA	EVIDENCIA OBSERVADA EN EL LABORATORIO	CONTROL DE HARDENING PROPUESTO	REFERENCIA DE SOPORTE
USO DE WINDOWS 7 SIN SOPORTE NI PARCHE MS17-010 EN HOST-A Y HOST-B	Explotación exitosa de EternalBlue y obtención de sesión Meterpreter con privilegios de sistema en Host-B	Proceso formal de gestión de parches, priorización de vulnerabilidades críticas y plan de migración de sistemas operativos sin soporte	CVE Program, s. f.; Incibe, 2019
EXPOSICIÓN DE HFS 2.3 VULNERABLE EN HOST-A CON DOBLE INTERFAZ DE RED	Ejecución remota de comandos vía CVE-2014-6287 y uso de Host-A como pivote hacia la red interna	Retiro o sustitución de HFS 2.3, ubicación de servicios expuestos en DMZ, refuerzo de reglas de firewall y deshabilitación de servicios innecesarios	CIS Security, 2020; Center for Internet Security, 2021
HOST CON DOBLE NIC ACTUANDO COMO PUENTE ENTRE RED EXTERNA E INTERNA	Configuración de autoroute y portproxy que permite redirigir tráfico desde 192.168.40.12:5000 hacia 192.168.56.102:445	Prohibir equipos puente no controlados, obligar a que todo tráfico entre segmentos pase por firewalls y routers con ACL bajo	Bejtlich, 2013; CCN-CERT, 2018

		principio de mínimo privilegio	
USO DE SMBV1 Y EXPOSICIÓN DE SMB SIN CONTROLES ADICIONALES EN HOST-B	Explotación de MS17-010 sobre SMBv1 y compromiso total del servidor interno	Deshabilitación de SMBv1, aplicación de configuraciones seguras recomendadas en CIS Benchmarks y segmentación reforzada del tráfico SMB	CIS Security, 2020; Center for Internet Security, 2021
GESTIÓN DÉBIL DE CUENTAS LOCALES PRIVILEGIADAS EN SERVIDORES	Creación y eliminación de cuenta administrativa efímera en Host-B, evidenciada por eventos 4720, 4732, 4733 y 4726	Implementación de soluciones tipo LAPS/PAM, políticas estrictas de cuentas privilegiadas y casos de uso en el SIEM para monitorizar estos eventos	Moreano Jurado, 2015; Zambrano Hernández et al., 2024

Nota. Esta matriz ejemplifica cómo cada vulnerabilidad identificada en el ejercicio Red Team se traduce en un conjunto de controles concretos que el Blue Team y la organización pueden implementar para reducir el riesgo residual, apoyándose en marcos de referencia como los CIS Controls y las guías del CSIRT Académico UNAD (Center for Internet Security, 2021; CSIRT Académico UNAD, 2024).

Esta trazabilidad convierte este informe final en un instrumento útil no solo para demostrar competencias técnicas, sino también para planear proyectos de mejora dentro de una organización real. El responsable de seguridad puede, por ejemplo, partir de la matriz de vulnerabilidades y controles derivados del ejercicio para definir un plan de trabajo priorizado, alineado con los riesgos más críticos evidenciados en la intrusión.

Visión de madurez de SecureNova Labs

A partir de la integración de las cuatro etapas, es posible esbozar una lectura de la "madurez" de SecureNova Labs en materia de ciberseguridad:

En el nivel más básico, la organización presenta deficiencias claras de cumplimiento normativo y ético (Etapas 1 y 2), reflejadas en la intención de apoyarse en acuerdos contractuales cuestionables y en la falta de alineación con la legislación vigente en delitos informáticos y protección de datos.

En el plano técnico, la configuración del entorno (Etapa 3) muestra la ausencia de prácticas elementales de seguridad: sistemas desactualizados, servicios vulnerables expuestos, falta de políticas de contraseñas y de gestión de cuentas privilegiadas.

Desde la perspectiva defensiva (Etapa 4), se evidencia la necesidad de fortalecer capacidades de monitoreo, correlación de eventos, respuesta a incidentes y gestión de riesgos, así como de integrar estas capacidades en un sistema de gestión de seguridad de la información de alcance organizacional.

El análisis integrador permite posicionar a SecureNova Labs en un nivel de madurez relativamente bajo, pero, al mismo tiempo, ofrece un conjunto concreto de acciones —tanto de gobierno como técnicas— que la organización podría adoptar para avanzar hacia niveles superiores, reduciendo el riesgo global y cumpliendo con sus obligaciones legales.

Relación con aspectos legales y éticos

Cada una de las actividades desarrolladas en el laboratorio fue concebida como una simulación de lo que, en un entorno productivo, solo podría llevarse a cabo bajo contratos, políticas y autorizaciones estrictamente ajustadas a la ley. Acciones como la explotación de vulnerabilidades en servicios expuestos (HFS 2.3), la obtención de shells remotas con privilegios elevados, el movimiento lateral entre segmentos de red y la creación de cuentas administrativas constituyen, fuera de un marco de pruebas debidamente autorizado, conductas que pueden subsumirse en tipos penales como el acceso abusivo a un sistema informático, la violación de datos personales, la interceptación de datos o el daño informático (Congreso de la República de Colombia, 2009; Guarnizo Portela, 2024).

El análisis del acuerdo propuesto por SecureNova Labs puso de manifiesto un segundo nivel de riesgo: el contractual y reputacional. Cláusulas que pretenden impedir la denuncia de posibles delitos informáticos, exigir confidencialidad sobre actividades ilícitas previas o exonerar de responsabilidad penal a la organización ante hallazgos de información ilegal son incompatibles tanto con el orden público penal como con los deberes deontológicos establecidos en el Código de Ética de COPNIA (COPNIA, 2015). Aceptar este tipo de disposiciones implicaría que el profesional de la seguridad informática renuncie, de facto, a su obligación de colaborar con la justicia y de proteger el interés público, convirtiéndose en partícipe de conductas reprochables.

El trabajo desarrollado busca precisamente resaltar que la excelencia técnica en Red Team y Blue Team no puede desligarse del cumplimiento normativo ni de la ética profesional. Un pentester o analista de seguridad no solo debe dominar herramientas como Nmap, Metasploit, SIEM o plataformas de respuesta activa, sino también ser capaz de identificar cuándo un encargo, un contrato o una orden interna traspasan la frontera entre una auditoría legítima y un

delito informático (Bejtlich, 2013; CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024). Esta capacidad crítica forma parte de las competencias esenciales del ingeniero en seguridad informática en el contexto colombiano.

En última instancia, la relación entre técnica, derecho y ética que se evidencia a lo largo del informe refuerza una idea fundamental: la ciberseguridad no se limita a explotar vulnerabilidades ni a aplicar parches, sino que exige tomar decisiones responsables sobre el impacto de las acciones técnicas en las personas, las organizaciones y la sociedad. Un ejercicio como el desarrollado con SecureNova Labs solo alcanza su sentido pleno cuando las conclusiones técnicas se convierten en recomendaciones de mejora organizacional que respetan la dignidad de los titulares de la información y el marco jurídico que protege sus derechos.

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:

https://youtu.be/4RsHg76qzUo

Conclusiones

La articulación de las cuatro etapas desarrolladas permitió comprobar que un ejercicio de Red Team y Blue Team solo adquiere pleno sentido cuando se concibe como un ciclo integral que abarca la planificación, la ejecución controlada, el análisis defensivo y la formulación de mejoras. La demostración práctica de la explotación de Rejetto HFS 2.3 y de la vulnerabilidad MS17-010 en el entorno de laboratorio permitió llevar a la práctica los principios de las metodologías de pruebas de penetración estudiadas, confirmando la utilidad de enfoques estructurados como OSSTMM, PTES y las guías orientadas a riesgos para organizar estas actividades en fases coherentes y trazables (Álvarez Intriago, 2018; Incibe, 2019; Sanne, 2024; Zuluaga Mateus, 2017).

El escenario de SecureNova Labs evidenció que una máquina intermedia con doble interfaz de red, configurada sin criterios de seguridad, puede convertirse en un vector de compromiso especialmente crítico. La experiencia de Host-A mostró que la combinación de un servicio vulnerable expuesto a internet y la ausencia de segmentación efectiva facilita el pivoting hacia redes internas, la exposición de servicios sensibles y, en última instancia, el compromiso de servidores que, en principio, no deberían ser accesibles desde el exterior. Estos hallazgos coinciden con recomendaciones técnicas que resaltan la importancia de una segmentación adecuada, del principio de mínimo privilegio y de la eliminación de puntos de tránsito innecesarios (Bejtlich, 2013; CCN-CERT, 2018; Chindrus & Caruntu, 2023).

Desde la óptica del Blue Team, el trabajo permitió corroborar que una respuesta eficaz a incidentes depende de forma directa de la calidad de la telemetría disponible y del grado de formalización de los procedimientos internos. La reconstrucción del ataque a partir de registros de eventos de Windows, logs de firewall, capturas de tráfico y otros artefactos evidenció que, sin una estrategia de registro y correlación adecuada, incluso ataques basados en vulnerabilidades

conocidas pueden pasar desapercibidos o ser gestionados de manera incompleta. Este resultado refuerza la necesidad de adoptar marcos de gestión de incidentes que contemplen fases de preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas (Cichonski et al., 2012; Moreano Jurado, 2015; Zambrano Hernández et al., 2024).

En el plano normativo y ético, el análisis detallado del acuerdo propuesto por SecureNova Labs permitió concluir que no toda solicitud de "auditoría de seguridad" puede considerarse legítima. La presencia de cláusulas orientadas a impedir la denuncia de delitos informáticos, encubrir actividades ilícitas o exonerar anticipadamente de responsabilidad penal a la organización contraviene lo dispuesto por la Ley 1273 de 2009, por el régimen general de protección de datos personales y por el Código de Ética de COPNIA, que exige al ingeniero actuar con probidad y denunciar los hechos posiblemente delictivos de los que tenga conocimiento (Congreso de la República de Colombia, 2009, 2012; COPNIA, 2015; Guarnizo Portela, 2024; Presidencia de la República de Colombia, 2013). Este ejercicio subraya la obligación del profesional de evaluar críticamente los instrumentos contractuales y rechazar aquellos que lo sitúen en conflicto con el ordenamiento jurídico o con sus deberes deontológicos.

El estudio confirmó, igualmente, la importancia de adoptar marcos de buenas prácticas como los CIS Critical Security Controls y los CIS Benchmarks para estructurar la estrategia de seguridad de una organización. La experiencia del escenario de laboratorio mostró que la aplicación sistemática de controles relativos a inventario de activos, gestión de vulnerabilidades, configuración segura, control de privilegios y monitoreo continuo, complementados con soluciones de SIEM, sistemas de detección y prevención de intrusos, tecnologías NAC y capacidades de respuesta activa, constituye la base de una arquitectura de defensa en profundidad capaz de reducir la superficie de exposición de forma tangible (Center for Internet Security, 2021; CIS Security, 2020; Cichonski et al., 2012; Wazuh, Inc., s. f.).

La comparación entre la situación inicial de SecureNova Labs y el escenario objetivo planteado en las recomendaciones permite ubicar a la organización en un nivel de madurez de ciberseguridad bajo, caracterizado por el uso de sistemas operativos sin soporte, la ausencia de un proceso formal de parchado, la exposición de servicios vulnerables en equipos puente, la debilidad de la segmentación y la carencia de capacidades robustas de monitoreo y respuesta. No obstante, el ejercicio ofrece una hoja de ruta clara para avanzar hacia niveles superiores de madurez, integrando políticas, procesos y controles técnicos dentro de un sistema de gestión de seguridad de la información y de gestión de riesgos más estructurado (CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024).

A nivel formativo y profesional, el desarrollo de las cuatro etapas contribuyó de manera significativa al fortalecimiento de competencias claves para el ejercicio de la seguridad informática: el análisis crítico del marco jurídico y ético aplicable, el diseño y la ejecución de pruebas de intrusión en entornos controlados, la lectura e interpretación de evidencias desde la perspectiva del Blue Team y la elaboración de informes técnicos claros, trazables y alineados con estándares académicos. Estas competencias responden a las exigencias actuales del mercado laboral y al rol del ingeniero como garante de la seguridad de la información y del cumplimiento normativo dentro de las organizaciones (Arroyo, 2025; Kotwani et al., 2023; Rajendran et al., 2011).

Finalmente, el trabajo permitió concluir que la sinergia entre equipos Red Team y Blue Team constituye un enfoque idóneo para organizaciones que desean mejorar su resiliencia frente a amenazas persistentes, siempre que dicha sinergia se articule con un gobierno corporativo que entienda la seguridad como un proceso continuo y transversal. La combinación de ejercicios ofensivos controlados, capacidades defensivas maduras y un marco de gobierno que incorpore explícitamente la gestión del riesgo de ciberseguridad en la toma de decisiones estratégicas se

configura como un elemento esencial para la protección de infraestructuras, servicios y datos personales en el contexto colombiano (Center for Internet Security, 2021; CSIRT Académico UNAD, 2024; Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, 2022, 2024).

Recomendaciones

A partir del análisis realizado en cada una de las fases del ejercicio (marco normativo y ético, valoración contractual, ejecución Red Team y respuesta Blue Team) se formulan las siguientes recomendaciones dirigidas a una organización con características similares a SecureNova Labs. Estas recomendaciones se agrupan en cuatro ámbitos: gobierno y cumplimiento, infraestructura técnica, monitoreo y respuesta, y formación y mejora continua:

Recomendaciones de gobierno y cumplimiento

Estructurar y aprobar formalmente una política integral de ciberseguridad que incluya lineamientos explícitos para la contratación y ejecución de pruebas de intrusión. Dicha política debe definir requisitos mínimos de autorización, alcance, responsables, tratamiento de datos, manejo de evidencias y trazabilidad, en coherencia con la Ley 1273 de 2009, la Ley 1581 de 2012, el Decreto 1377 de 2013 y la normativa sectorial aplicable (Congreso de la República de Colombia, 2009, 2012; Presidencia de la República de Colombia, 2013; Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, 2022, 2024).

Implementar un procedimiento estándar para la revisión jurídica y técnica de contratos relacionados con servicios de seguridad, que contemple listas de chequeo para identificar cláusulas contrarias al orden público penal o a la ética profesional. Cualquier disposición que busque prohibir la denuncia de delitos, encubrir actividades ilícitas o exonerar anticipadamente a la organización de responsabilidad penal debe ser modificada o rechazada, en consonancia con el Código de Ética de COPNIA (COPNIA, 2015; Guarnizo Portela, 2024).

Integrar la gestión de ciberseguridad al sistema de gestión de la seguridad de la información de la organización (por ejemplo, siguiendo principios de ISO/IEC 27001), incorporando expresamente marcos de referencia como los CIS Critical Security Controls y los CIS Benchmarks, así como guías de organismos como INCIBE, NIST y el CSIRT Académico

UNAD. Esto permite que las actividades técnicas de Red Team y Blue Team se apoyen en estándares reconocidos internacionalmente y se articulen con la gestión de riesgos institucional (Center for Internet Security, 2021; CIS Security, 2020; Cichonski et al., 2012; CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024).

Establecer un marco formal de gestión de riesgos de ciberseguridad que identifique activos críticos, amenazas, vulnerabilidades y controles existentes, asignando niveles de riesgo residuales y planes de tratamiento documentados. Este marco debe tomar como insumo tanto los resultados de ejercicios Red Team/Blue Team como las valoraciones internas y externas de riesgo (CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024).

Definir roles y responsabilidades claros en materia de ciberseguridad, incluyendo la designación de un responsable de seguridad de la información y la articulación con el CSIRT o equipo interno de respuesta a incidentes, de forma que exista un punto de contacto definido para coordinar pruebas, gestionar hallazgos y reportar incidentes a las autoridades competentes cuando corresponda (Cichonski et al., 2012; Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, 2022).

Recomendaciones técnicas sobre infraestructura

Eliminar o sustituir servicios vulnerables como HFS 2.3 en máquinas con doble interfaz de red o en equipos que actúan como puente entre segmentos internos y externos. En caso de requerir servicios de compartición de archivos hacia el exterior, estos deben ubicarse en una DMZ o segmento controlado, con reglas de firewall estrictas, monitoreo permanente y sin acceso directo a redes internas sensibles (Bejtlich, 2013; CCN-CERT, 2018; Center for Internet Security, 2021).

Implementar un proceso formal de gestión de vulnerabilidades y parches que contemple inventario de activos, evaluación de criticidad, priorización, programación de ventanas de mantenimiento y verificación posterior. En particular, se debe garantizar la aplicación oportuna de parches para vulnerabilidades de alto impacto, como MS17-010, y el reemplazo o actualización de sistemas operativos sin soporte como Windows 7 (CVE Program, s. f.; Incibe, 2019; National Institute of Standards and Technology, s. f.).

Reforzar la segmentación de red evitando que estaciones de trabajo o servidores no diseñados para tal fin actúen como puentes entre redes internas y externas. El tráfico entre segmentos debe canalizarse a través de dispositivos de seguridad dedicados (firewalls, routers con ACL), con reglas basadas en el principio de mínimo privilegio y revisiones periódicas de las configuraciones para evitar aperturas no justificadas (Bejtlich, 2013; CCN-CERT, 2018; Center for Internet Security, 2021).

Aplicar políticas de hardening sistemático en sistemas Windows y otros sistemas operativos, deshabilitando servicios innecesarios (por ejemplo, SMBv1), configurando adecuadamente el firewall local, restringiendo los puertos expuestos y aplicando las recomendaciones de seguridad contenidas en los CIS Benchmarks para cada plataforma (CIS Security, 2020; Center for Internet Security, 2021).

Implementar una gestión robusta de cuentas privilegiadas, evitando la reutilización de contraseñas de administrador local, segregando funciones, minimizando el número de cuentas con permisos de administración y adoptando soluciones específicas (por ejemplo, LAPS o plataformas de Privileged Access Management – PAM) para la rotación y custodia de credenciales de alto privilegio (Center for Internet Security, 2021; Zambrano Hernández et al., 2024).

Planificar la migración progresiva de sistemas legados que ya no reciben actualizaciones de seguridad, priorizando aquellos que cumplen funciones críticas o que se encuentran expuestos a redes externas. La permanencia prolongada de sistemas fuera de soporte incrementa de forma significativa la superficie de ataque y el riesgo de explotación de vulnerabilidades conocidas (CVE Program, s. f.; Incibe, 2019; Sanne, 2024).

Recomendaciones sobre monitoreo, respuesta e inteligencia de amenazas

Establecer un procedimiento formal de respuesta a incidentes basado en guías como NIST SP 800-61 que contemple fases de preparación, detección y análisis, contención, erradicación, recuperación y lecciones aprendidas, asegurando la coordinación entre el Blue Team operativo y el CSIRT o • Implementar una solución SIEM que recolecte, normalice y correlacione logs provenientes de sistemas operativos, firewalls, IDS/IPS, servidores, aplicaciones y plataformas de seguridad. El SIEM debe contar con casos de uso específicos orientados a detectar patrones similares a los observados en el ejercicio de laboratorio: explotación de servicios vulnerables, creación y eliminación inusual de cuentas, conexiones entre puertos no habituales (como 5000 y 445), cambios de configuración en equipos puente, entre otros (Bejtlich, 2013; Cichonski et al., 2012; Moreano Jurado, 2015).

Complementar el SIEM con herramientas de contención y control como firewalls perimetrales y host-based, sistemas de detección y prevención de intrusos (IDS/IPS) en línea, soluciones de Network Access Control (NAC) y agentes con capacidad de respuesta activa (por ejemplo, Wazuh), de manera que ante la detección de patrones maliciosos se puedan bloquear IPs, mover equipos a VLAN de cuarentena o detener procesos sospechosos de forma automatizada o semiautomatizada (CCN-CERT, 2018; Moreano Jurado, 2015; Wazuh, Inc., s. f.).

Establecer un procedimiento formal de respuesta a incidentes basado en guías como NIST SP 800-61, que contemple las fases de preparación, detección y análisis, contención, erradicación, recuperación y lecciones aprendidas, asignando responsables y tiempos objetivos para cada actividad. Este procedimiento debe estar alineado con el CSIRT interno o el equipo de respuesta a incidentes de la organización (Cichonski et al., 2012; CSIRT Académico UNAD, 2024).

Definir canales y formatos estándar para el registro, clasificación y escalamiento de incidentes de ciberseguridad, de forma que el personal de primera línea (mesa de servicio, operación de infraestructura) pueda notificar eventos de manera oportuna y consistente, reduciendo el tiempo de detección y aumentando la calidad de la información disponible para el análisis (Zambrano Hernández et al., 2024).

Integrar fuentes de inteligencia de amenazas (threat intelligence) que aporten información actualizada sobre vulnerabilidades, campañas activas y TTPs de atacantes relevantes para el sector de la organización. Esta información puede utilizarse para ajustar reglas de detección, priorizar parches y diseñar escenarios de ataque más realistas para futuros ejercicios Red Team/Blue Team (Bejtlich, 2013; Sanne, 2024).equipo de respuesta a incidentes de la organización.

Recomendaciones de formación y mejora continua

Programar ejercicios periódicos de Red Team y Blue Team, que incluyan tanto simulaciones técnicas en entornos de laboratorio como escenarios de tipo table-top con participación de áreas técnicas y de gestión. Estos ejercicios permiten validar la eficacia de los controles implementados, mejorar la capacidad de detección y respuesta, y fortalecer la coordinación entre equipos (Arroyo, 2025; Kotwani et al., 2023; Rajendran et al., 2011).

Desarrollar programas de capacitación continua para el personal técnico y directivo en aspectos legales, éticos y técnicos de la seguridad informática. La formación debe abarcar desde conceptos normativos básicos (delitos informáticos, protección de datos personales, deber de denuncia) hasta temas avanzados de gestión de incidentes, análisis forense y operación de herramientas de seguridad (Congreso de la República de Colombia, 2009, 2012; COPNIA, 2015; PandaSecurity, 2018).

Fomentar una cultura organizacional de reporte responsable de incidentes y de eventos de seguridad "cercanos al incidente" (near-misses), mediante canales de comunicación internos y externos que faciliten la notificación temprana de anomalías sin temor a represalias. Esta cultura contribuye a detectar patrones incipientes de ataque y a activar con mayor rapidez los procesos de respuesta y contención (Cichonski et al., 2012; CSIRT Académico UNAD, 2024; Zambrano Hernández et al., 2024).

Promover la participación del personal de seguridad en comunidades profesionales, foros académicos, conferencias y actividades de actualización relacionadas con ciberseguridad, Red Team, Blue Team y threat hunting, con el fin de mantener una visión actualizada de las técnicas de ataque y defensa, así como de las buenas prácticas emergentes (Arroyo, 2025; Sanne, 2024).

Realizar revisiones posts-incidentes y posts-ejercicios (lecciones aprendidas) de manera sistemática, documentando qué funcionó, qué falló y qué ajustes son necesarios en políticas, procedimientos, herramientas o capacidades humanas. Estas revisiones deben traducirse en acciones concretas de mejora que se integren al sistema de gestión de la seguridad de la información (Cichonski et al., 2012; CSIRT Académico UNAD, 2024).

Referencias Bibliográficas

Álvarez Intriago, V. K. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos [Manuscrito]. Semantic Scholar.

Arroyo, E. L. (2025). Sinergia de equipos Red Team y Blue Team en la protección de entornos corporativos [Objeto virtual de información]. Repositorio Institucional UNAD.

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

CCN-CERT. (2018). Guía de seguridad de las TIC. CCN-STIC-495: Seguridad en IPv6. Centro Criptológico Nacional.

Center for Internet Security. (2021). CIS Critical Security Controls version 8. Center for Internet Security.

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

CIS Security. (2020). CIS Benchmarks. Center for Internet Security.

Chindrus, C., & Caruntu, C.-F. (2023). Securing the network: A Red and Blue cybersecurity competition case study. Information, 14(11), 587.

Congreso de la República de Colombia. (2009). Ley 1273 de 2009 (5 de enero de 2009). Por la cual se modifica el Código Penal y se crean nuevos tipos penales relacionados con la protección de la información y de los datos.

Congreso de la República de Colombia. (2012). Ley 1581 de 2012 (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales.

COPNIA. (2015). Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares (pp. 3–26). Consejo Profesional Nacional de Ingeniería.

CSIRT Académico UNAD. (2024). Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS (Versión 1.0). Universidad Nacional Abierta y a Distancia – UNAD.

CVE Program. (s. f.). Overview / about the CVE Program. CVE.

Guarnizo Portela, M. P. (2024). La naturaleza jurídica de los delitos informáticos en Colombia [Monografía de pregrado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD.

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. Instituto Nacional de Ciberseguridad.

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

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2022). Políticas de privacidad y condiciones de uso.

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2024). Políticas de privacidad y condiciones de uso.

Moreano Jurado, P. J. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management) [Tesis de pregrado, Universidad San Francisco de Quito]. Repositorio USFQ.

National Institute of Standards and Technology. (s. f.). CVEs and the NVD process. National Vulnerability Database.

Offensive Security. (s. f.). About the Exploit Database. Exploit-DB.

Palomo Luna, D. F., Zambrano Hernández, L. F., Moreno Molano, S. X., & Peña Hidalgo, H. J. (2024, octubre). Una mirada a metodologías para pruebas de penetración en ciberseguridad. Boletín Informativo CSIRT Académico UNAD, 28.

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter.

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013 (27 de junio de 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. In 2011 IEEE 29th International Conference on Computer Design (ICCD) (pp. 285–288). IEEE. https://doi.org/10.1109/ICCD.2011.6081410

Sanne, S. H. V. (2024). Investigations into security testing techniques, tools and methodologies for identifying and mitigating security vulnerabilities. URF Journals.

Wazuh, Inc. (s. f.). Wazuh: The open source security platform. Wazuh Documentation.

Zambrano Hernández, J., Peña Hidalgo, H. J., & Cárdenas Corral, M. (2024). Guía para la gestión y clasificación de incidentes de ciberseguridad. Sello Editorial UNAD.

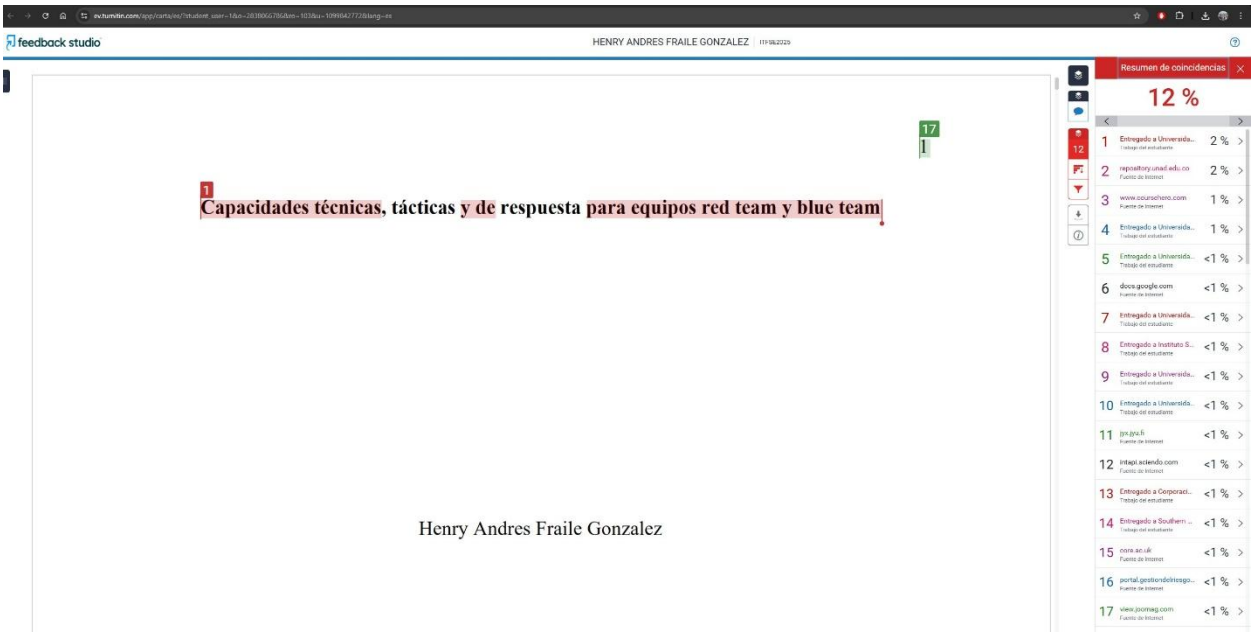
Zuluaga Mateus, A. D. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD.

Apéndices

Apéndice A

Figura 26

Resultado de revisión en Turnitin



Nota. En este apéndice se presenta el resultado de la revisión de similitud realizada en Turnitin sobre el documento final. La tabla resume el porcentaje de coincidencia detectado, las principales fuentes asociadas.