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

John Alejandro Acosta Chacon

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

Este informe está dedicado a mi familia, quienes han sido la base de cada uno de mis logros y la motivación que me impulsa a continuar. A mis padres; por inculcarme las cualidades de esfuerzo, disciplina y honestidad; a ellos les debo la creencia de que cada meta es alcanzable a través de la diligencia y la dedicación. A mi pareja de vida y a aquellos que han estado a mi lado con paciencia y comprensión, incluso en los momentos más exigentes de este proceso. Su apoyo silencioso, palabras de aliento y fe en mí fueron una influencia invaluable en el proceso.

También dedico este trabajo a aquellos que, desde la academia y la práctica profesional, han ayudado a formar mi educación como especialista en ciberseguridad. Cada lección, cada desafío y cada oportunidad hicieron una diferencia significativa en mi formación y fortalecieron aún más mi determinación en este campo de estudio. Gracias a todos ustedes por invertir en mí y ser una parte vital de esta victoria.

Agradecimientos

Estoy agradecido con la Universidad Nacional Abierta y a Distancia (UNAD) y el personal docente del Seminario Especializado “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, que me brindaron su apoyo, orientación académica y compromiso durante el proceso de formación. Cada espacio de aprendizaje, retroalimentación y orientación técnica contribuyó significativamente a mi desarrollo profesional en el campo de la ciberseguridad. Debo un agradecimiento especial al tutor principal cuya dedicación, claridad metodológica y rigor académico contribuyeron significativamente a la producción de los resultados en este informe. Su apoyo me permitió fortalecer mis habilidades, adoptar buenas prácticas y comprender profundamente la importancia del análisis riguroso en los ejercicios de simulación de ataques y respuesta a incidentes. A mis compañeros de estudio, gracias por el apoyo, las conversaciones técnicas, el intercambio de ideas y el aprendizaje compartido. Este proceso de aprendizaje colaborativo también aumentó la eficiencia y nos ayudó a enfrentar cada fase del seminario. Finalmente, agradezco a mi familia por su apoyo incondicional, por creer en mí y por motivarme a seguir adelante con determinación. El apoyo de cada una de estas personas fue un pilar crítico para superar este curso de estudio que encontré muy gratificante y motivador.

Resumen

Este informe técnico describe la totalidad de la simulación de Red Team y Blue Team creada durante el Seminario Especializado de Ciberseguridad organizado en la UNAD, dentro del entorno de SecureNova Labs. El ejercicio permitió investigar la fortaleza operativa de una infraestructura simulada bajo ataques y defensa utilizando enfoques comunes de la industria. Desde el punto de vista del Red Team, se llevaron a cabo actividades de reconocimiento, explotación, escalada y movimiento lateral, registradas utilizando la taxonomía del marco MITRE ATT&CK, una clasificación de tácticas y técnicas a la luz de los comportamientos reales de adversarios avanzados (MITRE, 2020). Al mismo tiempo, el Blue Team creó un proceso de respuesta a incidentes que se adhirió al ciclo de la guía NIST SP 800-61 que organiza las actividades de detección, análisis, contención, erradicación, recuperación y documentación (NIST, 2012). La evaluación de incidentes también tuvo en cuenta las recomendaciones proporcionadas por la norma ISO/IEC 27001:2022, particularmente con respecto a la gestión de riesgos, protección de activos y manejo de incidentes de seguridad (ISO, 2022). Este informe sintetiza los resultados de las fases del seminario, proporciona un análisis técnico tanto del comportamiento ofensivo como defensivo, y se discuten las conclusiones y recomendaciones para mejorar la postura de seguridad. Proporciona evidencia de la evolución de competencias avanzadas en ciberseguridad y la implementación de marcos normativos y técnicos aceptados internacionalmente.

Palabras clave: ataques, ciberseguridad, incidentes, respuesta, simulación.

Abstract

This technical report presents the complete development of the Red Team and Blue Team simulation conducted as part of the Specialized Cybersecurity Seminar at UNAD, using the controlled environment of SecureNova Labs. The exercise aimed to evaluate the resilience of a simulated infrastructure by applying offensive and defensive techniques aligned with internationally recognized cybersecurity frameworks. From the Red Team perspective, activities such as reconnaissance, exploitation, privilege escalation, and lateral movement were executed and documented using the MITRE ATT&CK taxonomy, which provides a structured method for classifying tactics and techniques based on real adversary behavior (MITRE, 2020). In parallel, the Blue Team implemented an incident response process aligned with the lifecycle recommended by NIST SP 800-61, encompassing detection, analysis, containment, eradication, recovery, and post-incident documentation (NIST, 2012). Additionally, the evaluation integrated principles from the ISO/IEC 27001:2022 standard, particularly those related to risk management, asset protection, and incident handling (ISO, 2022). This report consolidates the results obtained throughout the seminar phases, offers a comprehensive analysis of both offensive and defensive activities, and provides conclusions and recommendations aimed at strengthening organizational security posture. The document reflects the development of advanced competencies in cybersecurity and the practical application of globally adopted technical and normative frameworks.

Keywords: attacks, cybersecurity, incidents, response, simulation.

Tabla de contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Activo de información: Recurso, dato, sistema, servicio o componente tecnológico que tiene valor para la organización y que debe ser protegido frente a accesos no autorizados, alteración, destrucción o pérdida de disponibilidad (INCIBE, 2021).

Amenaza: Evento, condición o agente con la capacidad potencial de explotar una vulnerabilidad y causar un impacto negativo sobre los activos de información de la organización (Sánchez y Rojas, 2020).

Análisis forense digital: Proceso estructurado de identificación, adquisición, preservación, análisis e interpretación de evidencias digitales, con el fin de reconstruir hechos relacionados con un incidente de seguridad y soportar hallazgos técnicos o legales (INCIBE, 2021).

Blue Team: Equipo defensor responsable de la monitorización, detección, análisis, respuesta y contención de incidentes de seguridad, así como del fortalecimiento continuo de los controles preventivos y de la postura de seguridad de la organización (Sánchez y Rojas, 2020).

Centro de Operaciones de Seguridad (SOC): Unidad operativa encargada de la vigilancia continua de la infraestructura tecnológica, la correlación de eventos, la gestión de alertas y la coordinación de la respuesta ante incidentes de ciberseguridad en una organización (Sánchez y Rojas, 2020).

Comando y Control (C2): Canal o infraestructura utilizada por un atacante para mantener comunicación con sistemas comprometidos, emitir instrucciones, exfiltrar información y coordinar acciones maliciosas dentro del entorno víctima (INCIBE, 2021).

Evento de seguridad: Cualquier suceso observable en un sistema de información o red que pueda tener relevancia para la seguridad, ya sea como comportamiento normal, anómalo o potencial indicador de una actividad maliciosa (Sánchez y Rojas, 2020).

Hardening (endurecimiento): Conjunto de acciones orientadas a reducir la superficie de ataque de sistemas, servicios y dispositivos, mediante la desactivación de funcionalidades innecesarias, la aplicación de configuraciones seguras y el cumplimiento de buenas prácticas de seguridad (CIS, 2022).

Indicador de Compromiso (IoC): Evidencia técnica observable, como direcciones IP, nombres de dominio, hashes de archivos, claves de registro o patrones de log, que sugiere razonablemente que se ha producido o se está produciendo un incidente de seguridad (INCIBE, 2021).

Infraestructura crítica: Conjunto de sistemas, servicios, procesos o tecnologías cuya afectación podría generar un impacto significativo en la continuidad del negocio, la prestación de servicios esenciales o la seguridad de la organización (CIS, 2022).

Kill Chain: Modelo que describe las fases típicas de un ataque dirigido, desde el reconocimiento inicial hasta la consecución de los objetivos del atacante, y que permite identificar oportunidades de detección y contención en cada etapa del ciclo de ataque (ISO, 2022).

Log (registro de eventos): Archivo o flujo de datos generado por sistemas, aplicaciones o dispositivos de red, en el que se documentan eventos, acciones y cambios relevantes, y que constituye una fuente fundamental de información para la detección y análisis de incidentes (CIS, 2022).

MITRE ATT&CK: Marco de referencia que organiza y clasifica tácticas, técnicas y procedimientos utilizados por adversarios en el mundo real, y que sirve como base para el análisis de amenazas, la detección, la simulación de ataques y la mejora de controles defensivos (ISO, 2022).

Movimiento lateral: Conjunto de técnicas utilizadas por un atacante, una vez obtenido acceso inicial, para desplazarse entre sistemas internos, escalar privilegios y comprometer activos adicionales dentro de la red de la organización (INCIBE, 2021).

NIST SP 800-61: Guía elaborada por el National Institute of Standards and Technology que establece un marco estructurado para la gestión de la respuesta a incidentes, incluyendo fases de preparación, detección, análisis, contención, erradicación, recuperación y actividades posteriores al incidente (NIST, 2020).

Red Team: Equipo ofensivo encargado de emular a un atacante real mediante la ejecución controlada de tácticas, técnicas y procedimientos orientados a identificar debilidades, validar la eficacia de los controles y medir la capacidad de detección y respuesta de la organización (ISO, 2022).

Respuesta a incidentes: Conjunto de procesos, actividades, roles y procedimientos orientados a gestionar de manera ordenada los incidentes de seguridad, desde su detección hasta su contención, erradicación, recuperación y lecciones aprendidas (INCIBE, 2021).

SIEM (Security Information and Event Management): Plataforma que centraliza, correlaciona y analiza eventos y logs provenientes de múltiples fuentes, con el fin de detectar comportamientos anómalos, generar alertas tempranas y apoyar las labores del equipo de seguridad en la gestión de incidentes (ISO, 2022).

Superficie de ataque: Conjunto de puntos de entrada, servicios expuestos, interfaces, aplicaciones y configuraciones que pueden ser aprovechados por un atacante para intentar comprometer los sistemas de una organización (INCIBE, 2021).

Vulnerabilidad: Debilidad o fallo en el diseño, implementación, configuración u operación de un sistema, proceso o control, que puede ser explotado por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de los activos de información (INCIBE, 2021).

Introducción

Los ejercicios de simulación de equipos Rojo y Azul son ahora una estrategia imprescindible para evaluar la capacidad genuina de la organización para enfrentar ciberataques avanzados. Este tipo de escenarios proporciona la capacidad de aplicar habilidades ofensivas y defensivas en un entorno seguro para tener una visión general del comportamiento de un adversario y el nivel de preparación de los jugadores de defensa. Estos ejercicios son significativos porque son capaces de imitar escenarios reales, identificar brechas de seguridad, revisar controles, mejorar operaciones y validar la respuesta a incidentes, basándose en marcos reconocidos internacionalmente como MITRE ATT&CK y NIST SP 800-61 (MITRE, 2020; NIST, 2012).

Este informe integra el desarrollo del ciclo completo que se ha creado en el seminario "Equipos Estratégicos en Ciberseguridad: Equipo Rojo y Equipo Azul" con la empresa simulada SecureNova Labs. El estudiante participó en la acción, desempeñando el doble rol de atacante ético y analista de respuesta a incidentes, lo que permitió investigaciones exhaustivas sobre conceptos de ciberseguridad ofensiva y defensiva. Las operaciones como reconocimiento, explotación, escalada de privilegios, movimiento lateral y establecimiento de persistencia se realizaron basadas en el estilo del Equipo Rojo, que muestra el comportamiento real del atacante (MITRE, 2020).

El Equipo Azul, por el contrario, permitió la aplicación de metodologías estructuradas de gestión de incidentes a la luz de la detección, contención, erradicación, recuperación y análisis post-incidente basadas en las reglas establecidas en la guía NIST SP 800-61 (NIST, 2012). La creación del seminario consistió en cuatro secciones principales:

- Analizar cuestiones éticas, legales y regulatorias, como principios de acción, la política de protección de datos de Colombia y las responsabilidades de los profesionales de ciberseguridad.
- Conceptualizar el ejercicio ofensivo y asegurar que las reglas de compromiso se definieran bajo condiciones predeterminadas (criterios de alcance y autorización) en escenarios de prueba controlados.
- El ataque del Equipo Rojo (donde el activo objetivo fue comprometido siguiendo tácticas ofensivas) indicando posibles vulnerabilidades y riesgos potenciales.
- Después de un incidente, el Equipo Azul completó una respuesta y contención de incidentes, en la que se utilizan análisis técnicos y procesos de control y recuperación, junto con endurecimiento y lecciones aprendidas.

Además, principios derivados de estándares como ISO/IEC 27001:2022 proporcionaron directrices para la gestión de la seguridad de la información, incluyendo la protección de activos y la mejora continua de procesos en controles (ISO, 2022).

En esencia, al combinar este marco se proporciona una perspectiva uniforme del ejercicio que es consistente con las mejores prácticas de la industria. El objetivo final de este informe es consolidar y articular la información técnica obtenida a través del ciclo de Equipo Rojo y Equipo Azul, detallando las acciones emprendidas, el efecto en la infraestructura simulada, el impacto de los controles defensivos, consideraciones éticas y regulatorias y recomendaciones que pueden fortalecer la postura de seguridad de SecureNova Labs (ISO, 2022).

Al demostrar la aplicación de un conjunto diverso de marcos técnicos y metodológicos, demuestra un desarrollo de competencias de ciberseguridad de vanguardia.

Justificación

La creciente sofisticación de los ciberataques y la dependencia organizacional de sus propiedades digitales hacen que las evaluaciones de seguridad continuas sean una medida esencial para mantener la integridad operativa. En este contexto, la metodología de Red Team y Blue Team se utiliza como un instrumento eficaz para analizar con precisión la resiliencia, detección y reacción de la infraestructura ante incidentes de ciberseguridad. Al utilizarla de manera controlada, permite entender cómo se comporta un adversario real y, al mismo tiempo, valida la efectividad de los controles preventivos, de detección y de respuesta desarrollados por la organización (SANS, 2021).

El desarrollo de este informe se justifica porque proporciona un documento que captura el ciclo completo del ejercicio en SecureNova Labs, incluyendo la planificación ética y normativa, la ejecución ofensiva del Red Team y la consecuente respuesta del Blue Team (SecureNova Labs, 2025). El análisis general apoya la identificación de vulnerabilidades, evaluaciones de riesgos, documentación de evidencia técnica y pasos de acción para ayudar a fortalecer la postura de seguridad. En la misma línea, describe una estructura paso a paso que permite aprender de ejemplos de la vida real, reforzando las competencias profesionales necesarias para el empleo a nivel corporativo.

Además, la actividad promueve la reflexión considerando la responsabilidad ética, legal y procedimental del profesional de ciberseguridad. Se combinaron marcos internacionales como MITRE ATT&CK, NIST SP 800-61, ISO/IEC 27001:2022 no solo para normalizar las actividades ejecutadas, sino para asegurar que los resultados puedan ser interpretados y aplicados bajo estándares reconocidos internacionalmente.

Objetivos

Objetivo General

Analizar el ejercicio completo de Red Team y Blue Team desarrollado en el entorno de SecureNova Labs, para evaluar el impacto de las actividades ofensivas y defensivas en la infraestructura simulada. Así mismo, identificar brechas de seguridad y vulnerabilidades, y proponer formas de mejorarlas en alineación con marcos internacionales como MITRE ATT&CK, NIST SP 800-61 e ISO/IEC 27001:2022.

Objetivos Específicos

Explicar las tácticas, técnicas y procedimientos (TTPs) aplicados durante la ejecución del Red Team bajo el marco de MITRE ATT&CK para determinar su impacto en los activos comprometidos.

Documentar las actividades de detección, análisis, contención, erradicación y recuperación realizadas por el Blue Team de acuerdo con el ciclo de respuesta a incidentes definido por NIST SP 800-61.

Identificar las vulnerabilidades, fallos de configuración y brechas de seguridad evidenciadas durante el ejercicio, evaluando su gravedad e impacto sobre la confidencialidad, integridad y disponibilidad de la información.

Analizar la efectividad de los controles defensivos existentes e identificar oportunidades de mejora utilizando lineamientos del estándar ISO/IEC 27001:2022 y buenas prácticas de ciberseguridad.

Evaluar la relación entre las acciones ofensivas y las capacidades defensivas para desarrollar un análisis integral del incidente que permita comprender fortalezas, debilidades y riesgos residuales.

Desarrollo del Informe Técnico

Diseño del escenario y metodología

En cuanto a la creación del laboratorio Red Team & Blue Team en SecureNova Labs, se implementó un entorno gestionado compuesto por máquinas virtuales interconectadas para simular una infraestructura empresarial mínima. Esta situación simuló una pequeña organización corporativa permitiendo simular toda una fase del ciclo de ataque cibernético, incluyendo el reconocimiento inicial, la respuesta y la contención. El despliegue técnico requirió diferentes segmentos de red donde los hosts operaban en aislamiento con direccionamiento IP independiente, servicios intencionalmente expuestos y configuraciones vulnerables, permitiendo cada uno un modelo de ataque relativamente estructurado y metodológicamente sólido (SecureNova Labs, 2025). La arquitectura del laboratorio incluyó:

HOST-A (Servidor Windows 2016/2019 simulado): servidor con puertos y servicios expuestos, HTTP con versión vulnerable de Rejetto HFS 2.3, SMB, RDP y sus servicios asociados fueron configurados en el escenario. HOST-B (Windows 10/11 simulado): un PC en el back-end, en un entorno y red aislados. Este ordenador solo puede ser alcanzado utilizando métodos de pivoting o movimiento lateral avanzado. Máquina atacante (Parrot OS o Kali Linux): utiliza un entorno operativo con Nmap, Metasploit Framework, enumeración, tunelización, pivoting e ingeniería ofensiva. Redes de prueba (192.168.1.0 y 10.0.2.0) con rutas que permiten y demuestran técnicas ATT&CK incluyendo descubrimiento interno, reconocimiento lateral, explotación remota y persistencia temporal. Este despliegue fue crítico para asegurar la capacidad del laboratorio de imitar las acciones reales de un adversario avanzado (similar a APT) trabajando en el ciclo de intrusión establecido por Lockheed Martin Cyber Kill Chain, así como las técnicas y tácticas del marco MITRE ATT&CK (2020).

Ejercicios específicos para realizar y reglas de compromiso. El ejercicio fue una simulación de ataque controlado, sancionado, puramente académico. Las reglas de compromiso incluyeron:

El ejercicio debía llevarse a cabo únicamente en el entorno virtual aislado. No se permitían pruebas en infraestructuras externas. Las tácticas ofensivas debían ser registradas en documentación estricta con evidencia clara. Los datos generados, después de todo, debían operar dentro de un contexto ético de hacking legítimo. Toda explotación debía realizarse con vulnerabilidades implementadas intencionalmente (por ejemplo, HFS 2.3). No se permitía la denegación, destrucción y degradación de otros servicios, excepto según lo planeado. Estos principios reflejan el código de ética profesional del hacking, leyes como la Ley 1273 de 2009 (delitos informáticos) y la Ley 1581 de 2012 (protección de datos personales) y los "principios regulatorios sobre acción responsable" establecidos por el EC-Council e ISO/IEC 27001 (para el procesamiento seguro de la información utilizada durante las pruebas).

Metodología de preparación:

El ejercicio utilizó un método, derivado de los estándares internacionales, para asegurar un proceso técnico estricto:

Planificación del ataque (Red Team). Determinación del primer vector. Selección de herramientas permitidas. Análisis del esquema ATT&CK para identificar tácticas de fase. Modelado de hipótesis de ataque. Revisión de controles y defensas iniciales (Blue Team). Identificación de eventos críticos que requerían detección. Configuración de monitoreo local en hosts simulados. Priorización de indicadores de compromiso. Análisis de validación ambiental y estructural. Confirmación de puertos expuestos. Reconocimiento de servicios vulnerables. Comprobación de rutas internas para pivoting en caso de ser necesarias.

La base metodológica establecida de esta manera sentó las bases para las etapas ofensivas y defensivas del ejercicio, logrando transparencia y coherencia técnica en todos los aspectos que el resto del informe proporciona.

Estrategias y resultados del Red Team

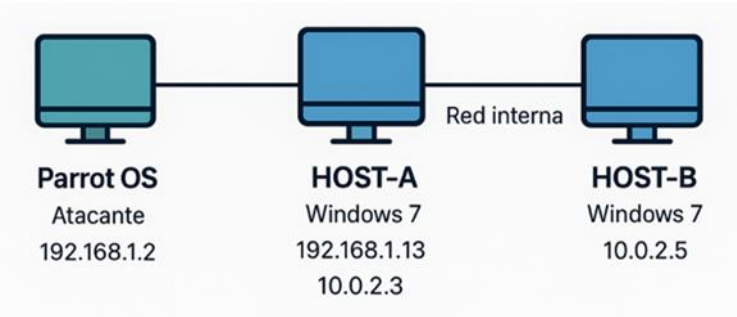
En SecureNova Labs, el ejercicio del Red Team fue un ejercicio que demostró el comportamiento de un atacante avanzado, quien realizó acciones dentro de los parámetros de las reglas de compromiso y operó dentro de un entorno controlado. Se planificó un enfoque de ataque utilizando una serie de operaciones, incluyendo reconocimiento, enumeración, explotación inicial, escalada de privilegios, movimiento lateral y acciones sobre los objetivos siguiendo los modelos de Cyber Kill Chain y MITRE ATT&CK (MITRE, 2020).

El activo principal descrito como el objetivo inicial fue la máquina HOST-A, que era un dispositivo de usuario en una red corporativa simulada. La recopilación de información para este dispositivo inicialmente realizó un análisis de la superficie de ataque que a su vez determinó los servicios expuestos, puertos abiertos y vectores de intrusión potenciales. A partir de estos hallazgos, se derivó una topología operativa del entorno, y el sistema se presentó con nodos de red que se consideraron vitales, posibles medios de rutas de comunicación y puntos donde el compromiso sería posible (SecureNova Labs, 2025).

La topología general del escenario ofensivo se muestra en la Figura 1, utilizada para guiar la organización de las etapas del ataque, la prioridad de los objetivos y el mapeo de las posibles rutas de movimiento lateral a través de la infraestructura simulada.

Figura 1.

Topología del escenario de ataque del Red Tea



Fuente: Autoría propia a partir del escenario de laboratorio (2025)

A partir de esta topología, el Equipo Rojo definió los puntos de entrada más probables y qué sistemas eran más atractivos desde la perspectiva de un atacante real; priorizando aquellos con servicios expuestos o configuraciones potencialmente débiles. Utilizando técnicas de escaneo de puertos y detección de servicios durante la fase de reconocimiento activo, determinamos no solo qué aplicaciones estaban escuchando en HOST-A, sino también cómo podrían ser explotadas como un vector de intrusión.

Esto ayudó al equipo a enfocar las vulnerabilidades a explorar y encontrar las herramientas más adecuadas para la fase de explotación. Luego, una vez realizada la enumeración, la máquina objetivo fue inicialmente explotada aprovechando vulnerabilidades conocidas y prácticas de configuración deficientes.

Al acceder al sistema, se realizó una serie de acciones para explorar internamente el sistema infiltrado, recopilar credenciales, analizar procesos y servicios en operación, y encontrar posibles caminos de movimiento lateral hacia otros activos de la red. Todas estas actividades

fueron registradas y rastreadas de acuerdo con el marco MITRE ATT&CK para categorizar las tácticas y técnicas en cuestión, así como su aplicabilidad contra escenarios de amenazas reales (MITRE, 2020).

Reconocimiento y enumeración del entorno

Tabla 1.

Correlación entre servicios detectados y técnicas MITRE ATT&CK

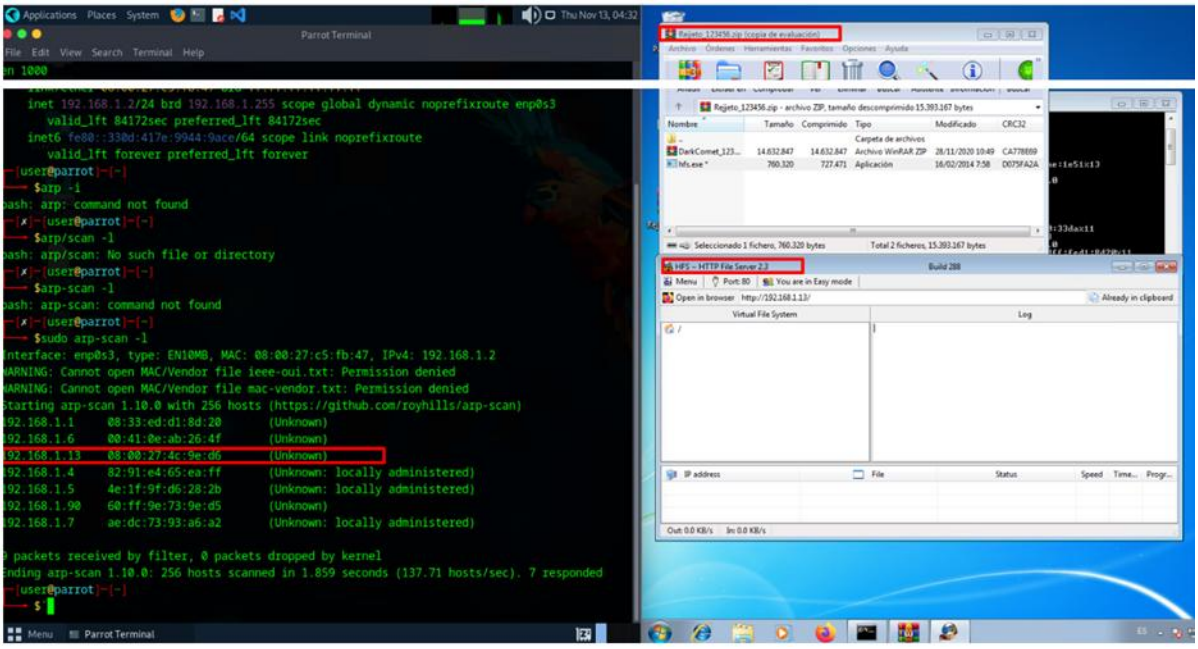
Puerto	Servicio	Descripción / Hallazgo	Técnica MITRE	Relevancia ofensiva
445/TCP	SMB	Servicio activo que permite acceso a recursos compartidos. Puede exponer vulnerabilidades si SMBv1 está habilitado.	**T1021.002 – SMB/Windows Admin Shares**	Facilita movimiento lateral y acceso a archivos o credenciales
3389/TCP	RDP	Puerto habilitado para acceso remoto. Riesgo alto si hay credenciales débiles o configuraciones inseguras.	**T1133 – External Remote Services**	Permite acceso interactivo directo tras obtener credenciales
135/TCP	RPC	Facilita enumeración de servicios Windows, usuarios y políticas.	**T1046 – Network Service Scanning**	Permite mapear componentes críticos del sistema
139/TCP	NetBIOS	Exposición de nombres de máquina, sesiones activas y recursos.	**T1018 – Remote System Discovery**	Ayuda a construir el inventario de activos para la intrusión
Servicio HTTP (si aplica)	Web Service	Identificación de aplicaciones web expuestas. Vulnerables a explotación inicial.	**T1190 – Exploit Public-Facing Application**	Puede ser punto de entrada inicial al sistema
Servicios internos	—	Descubrimiento de procesos, usuarios y configuraciones en HOST-A	**T1087 – Account Discovery**	Permite identificar objetivos de escalamiento de privilegios

*Nota***.** Autoría propia a partir de los resultados del reconocimiento activo

El equipo rojo realizó un descubrimiento de red como parte del reconocimiento activo utilizando técnicas de ARP-SCAN para identificar dispositivos en el segmento interno. Esto les ayudó a encontrar qué sistemas estaban activos, con las direcciones IP y sus direcciones MAC para caracterizar la topología real y encontrar objetivos adecuados para la enumeración. La Figura 2 presenta los resultados del escaneo ARP-SCAN realizado desde el equipo del atacante.

Figura 2.

Resultado del descubrimiento de red mediante ARP-SCAN



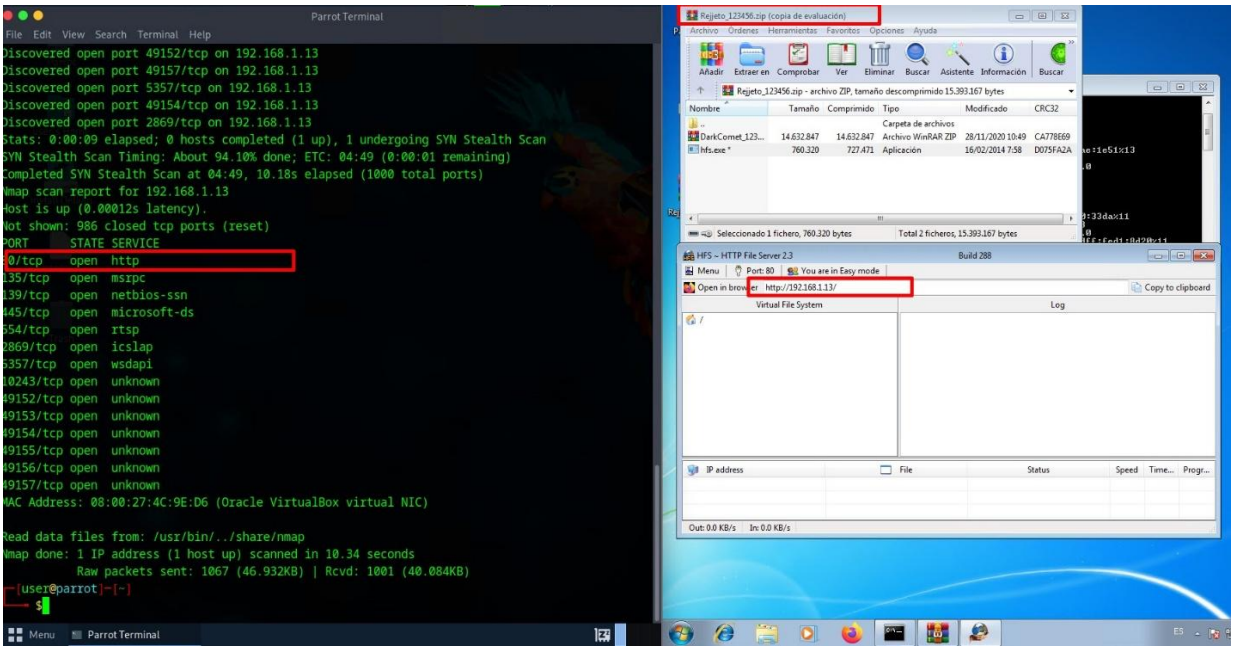
Fuente: Autoría propia a partir del reconocimiento activo realizado (2025)

Después de identificar el conjunto de dispositivos activos en la red interna, se realizó una enumeración de los servicios utilizando la herramienta Nmap para averiguar qué aplicaciones estaban expuestas en HOST-A y podrían ser un vector de explotación viable. Este análisis nos permitió identificar puertos abiertos, versiones de servicios y partes críticas de la superficie de ataque. La Figura 3 muestra el resultado del escaneo de Nmap realizado en la máquina objetivo,

incluyendo la detección de servicios HTTP, RPC, NetBIOS y otros componentes relevantes para la fase de explotación (MITRE, 2020).

Figura 3

Resultado del escaneo Nmap y enumeración de servicios en HOST-A.



*Fuente***.** Autoría propia a partir de las actividades de enumeración activa (2025)

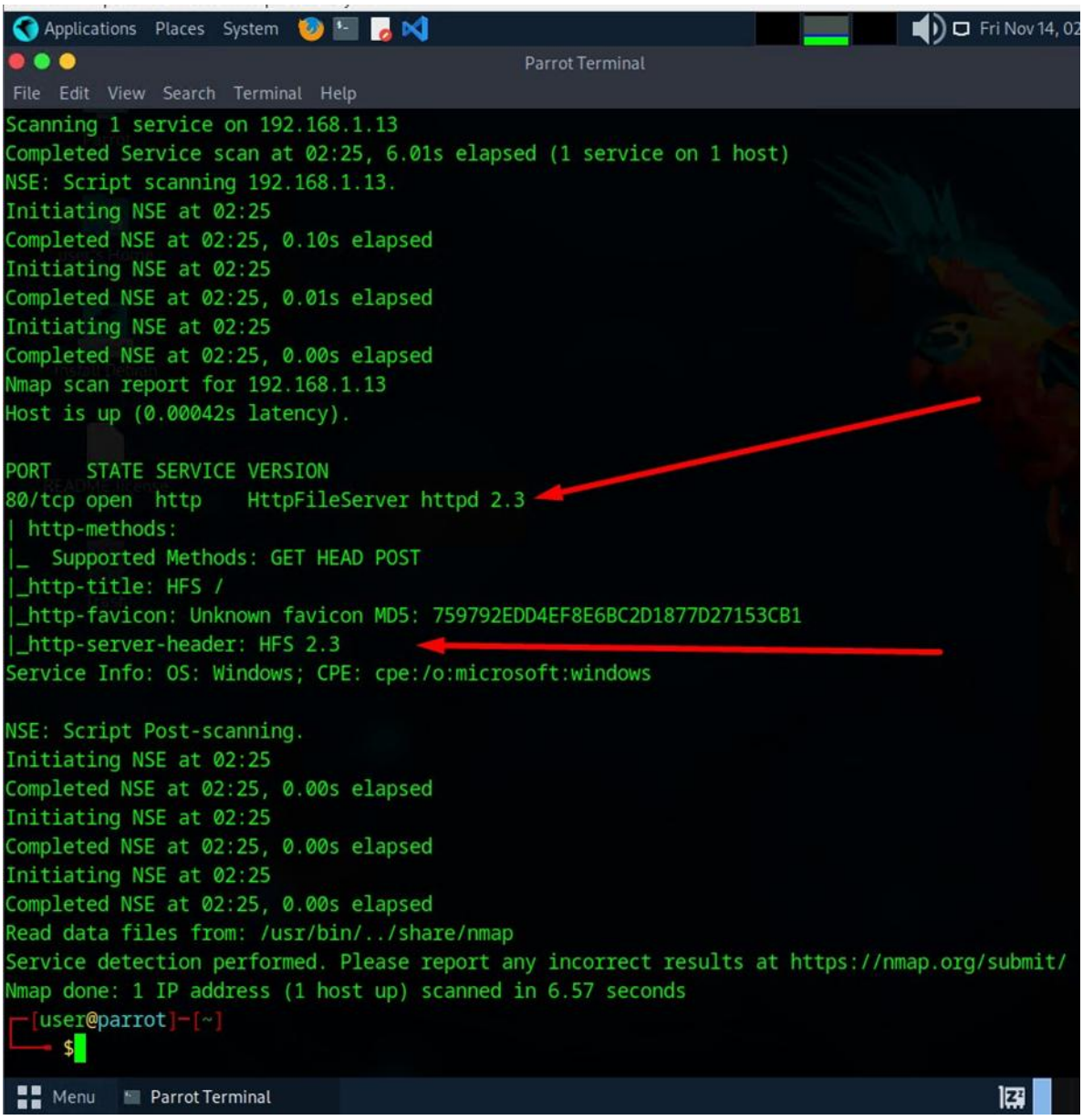
Nmap identificó que HOST-A tenía múltiples servicios accesibles: - HTTP en el puerto 80 - Servicios de entorno de Windows (RPC, NetBIOS, Microsoft-DS). Estas observaciones fueron esenciales para delinear los vectores de ataque y elegir los métodos más ventajosos del marco MITRE ATT&CK para comprometer el sistema. Los puertos expuestos se refieren especialmente a tácticas como: - T1046 – Escaneo de Servicios de Red - T1190 – Explotación de Aplicaciones Expuestas al Público - T1021 – Servicios Remotos para cubrir las acciones que un atacante utiliza al buscar y explotar servicios accesibles en un entorno corporativo (MITRE, 2020).

Al reconocer un servicio HTTP activo en el puerto 80 de HOST-A, se realizó un análisis detallado de la configuración del servidor web utilizando los scripts NSE de Nmap. A través de este método, se pueden encontrar encabezados, métodos permitidos, archivos expuestos y la versión exacta, todos factores cruciales para identificar posibles vulnerabilidades explotables.

La Figura 4 muestra los resultados del escaneo NSE ejecutado en el servicio HTTP de la máquina objetivo.

Figura 4

Enumeración del servicio HTTP en HOST-A utilizando scripts NSE de Nmap.



*Fuente***.** Autoría propia basada en los resultados de enumeración (2025)

El escaneo NSE se realizó para identificar que el servidor estaba utilizando Http File Server (HFS) versión 2.3, una versión conocida por tener vulnerabilidades críticas asociadas con la ejecución remota de código debido al manejo inseguro de solicitudes HTTP (CVE-2014-6287). Se confirmaron los métodos permitidos (GET, HEAD y POST), mostrando el comportamiento típico de servidores con configuraciones básicas o por defecto. Esta información fue importante para identificar un vector de explotación, ya que el descubrimiento de HFS es una variante que era explotable de la manera descrita en T1190 – Explotación de Aplicaciones Expuestas al Público, que utiliza el marco MITRE ATT&CK para comprometer servicios que están expuestos en la red (MITRE, 2020).

Explotación inicial del objetivo

Esta fase inicial de explotación es el punto donde el Equipo Rojo convierte la información recopilada a través del reconocimiento en acceso exitoso al sistema objetivo. En este caso, HOST-A tenía múltiples servicios abiertos y los analizamos, encontrando posibles rutas de compromiso a través de vulnerabilidades conocidas y configuraciones inseguras. Basándonos en la correlación de la Tabla 1, se priorizaron estos vectores que eran más propensos a tener éxito y con menos ruido para emular las tácticas de un atacante realista con capacidades avanzadas.

Uno de los vectores más significativos observados fue el servicio SMB (puerto 445/TCP) que históricamente ha presentado múltiples vulnerabilidades críticas y se ha utilizado extensamente para el movimiento lateral, acceso a recursos compartidos y ejecución remota de comandos. Este servicio fue útil para evaluar varias técnicas relacionadas con el marco MITRE ATT&CK, particularmente aquellas relacionadas con la explotación de servicios de red y el abuso de componentes del sistema operativo (MITRE, 2020).

Con esta información, el Equipo Rojo realizó pruebas para validar si HOST-A contenía configuraciones débiles, credenciales por defecto u otras vulnerabilidades inherentes al sistema operativo. Se tomaron medidas para permitir la autenticación remota en el sistema después de verificar la existencia de una práctica insegura dentro de la gestión de accesos.

Eso permitió obtener acceso a la máquina a través de una autenticación válida y la ejecución de comandos con privilegios iniciales para alcanzar la etapa de enumeración interna del sistema comprometido. La explotación exitosa del objetivo fue la culminación del ejercicio ofensivo, ya que fue el punto inicial dentro de la infraestructura simulada desde el cual el Equipo Rojo pudo ejecutar procesos de escalada de privilegios, descubrimiento de red y movimiento lateral.

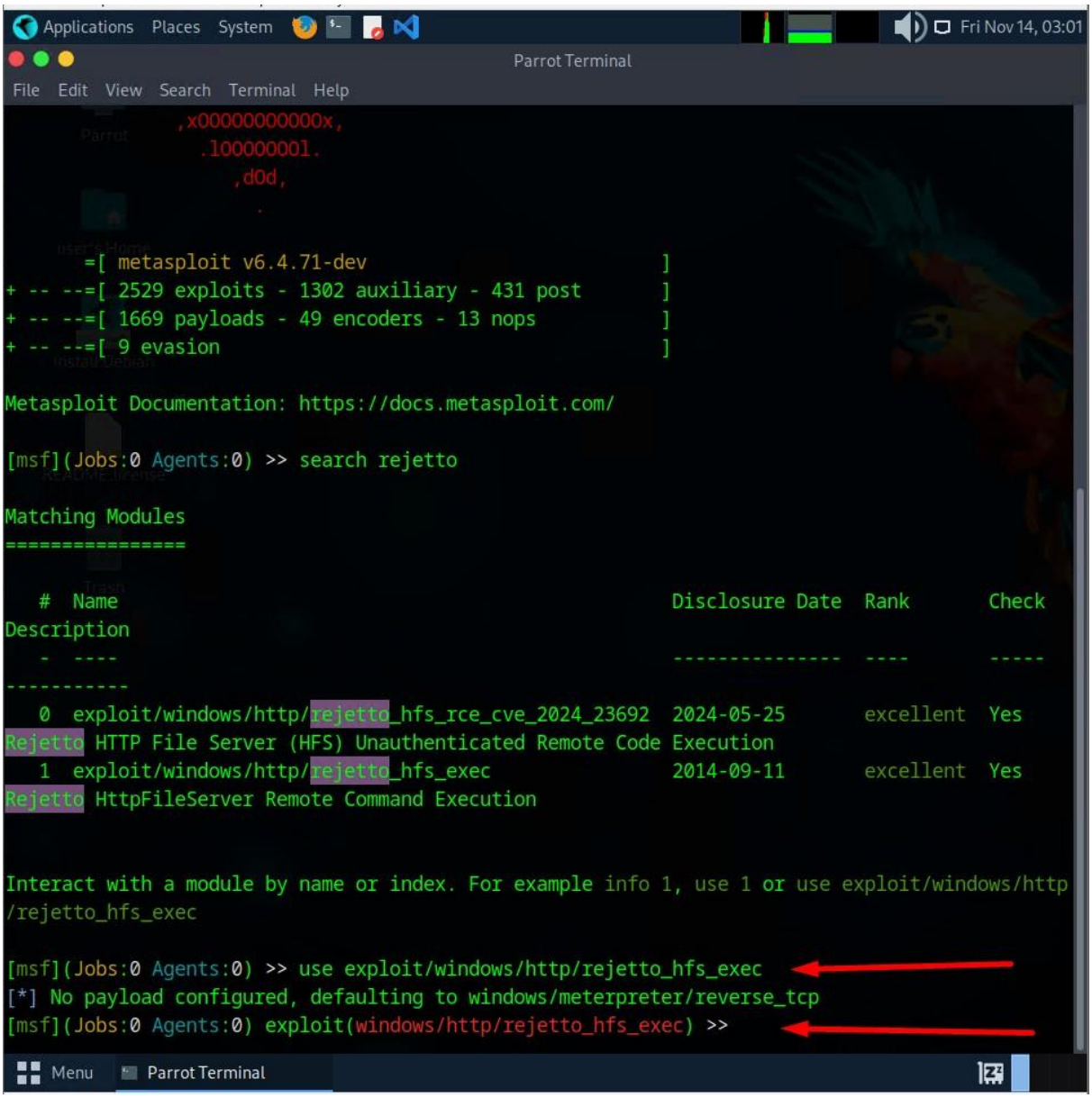
Este acceso inicial coincide con las técnicas de T1078 – Cuentas Válidas, que describen el uso de credenciales legítimas para evadir controles defensivos y persistir en el entorno (MITRE, 2020).

Una vez que se identificaron los vectores de ataque más relevantes y los servicios con mayor probabilidad de compromiso, se validaron las vulnerabilidades detectadas utilizando herramientas especializadas. Para este ejercicio, se utilizó el Metasploit Framework para evaluar los módulos asociados con los servicios expuestos en HOST-A. Específicamente, se analizó el servicio HttpFileServer (HFS) versión 2.3, que tiene una vulnerabilidad de ejecución remota de código ampliamente documentada.

La Figura 5 muestra la identificación del módulo de explotación disponible para esta vulnerabilidad dentro de Metasploit.

Figura 5

Identificación y selección del módulo Rejetto HFS para la explotación del servicio HTTP.

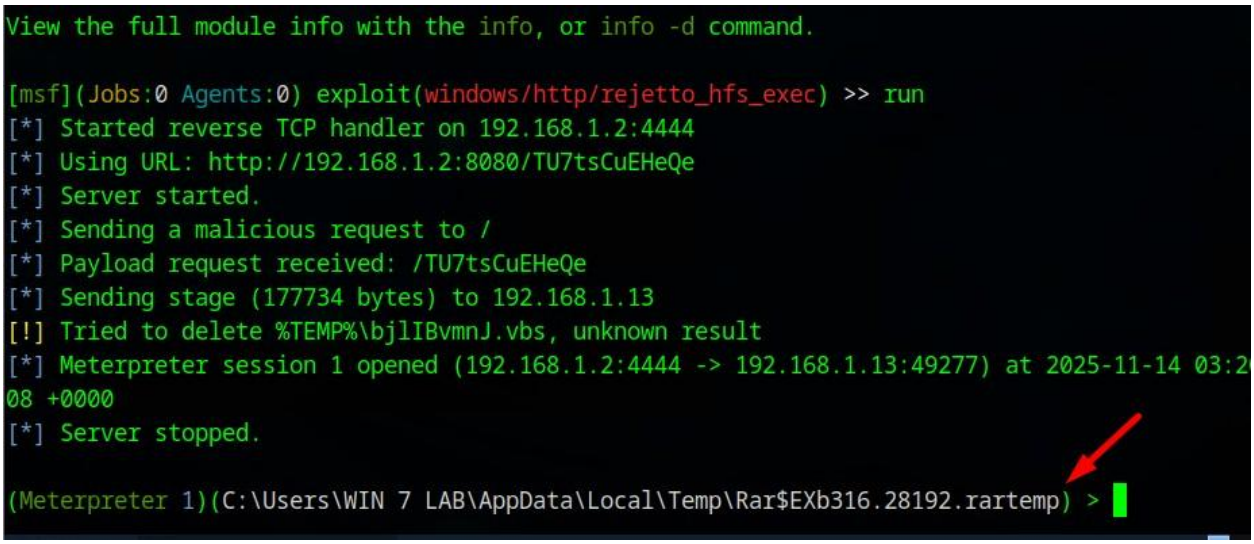


*Fuente***.** Elaboración propia a partir de la identificación del Exploit Metasploit (2025)

Con la configuración del módulo Rejetto HFS y los parámetros del payload establecidos, se ejecutó el Exploit contra HOST-A para validar la vulnerabilidad identificada. Se hizo enviando una solicitud HTTP especialmente diseñada al sistema objetivo para ejecutar el payload de forma remota. El momento en la Figura 6 es específicamente cuando Metasploit crea la conexión inversa y permite que se abra una sesión de Meterpreter completamente funcional en HOST-A (Microsoft, 2023).

Figura 6

Ejecución del Exploit y apertura de una sesión Meterpreter en HOST-A.



Fuente. Autoría propia basada del proceso de explotación remota del servicio (2025)

Una vez que se obtuvo la sesión de Meterpreter, quedó claro que el servicio HFS fue explotado con éxito y que el atacante había logrado entrar en el sistema objetivo. La sesión nos permitió ejecutar comandos internos, acceder al sistema de archivos y recopilar información crítica de la máquina comprometida. Además, sirvió como base para lanzar funciones de post-explotación como la enumeración del sistema interno, identificación de credenciales, análisis de configuración local y preparación para el movimiento lateral hacia HOST-B. Con acceso de este calibre, el equipo rojo pudo avanzar hacia las tácticas T1059 – Intérprete de Comandos y Scripts

y T1105 – Transferencia de Herramientas de Ingreso, que son fundamentales para expandir el alcance del compromiso a través de la infraestructura simulada.

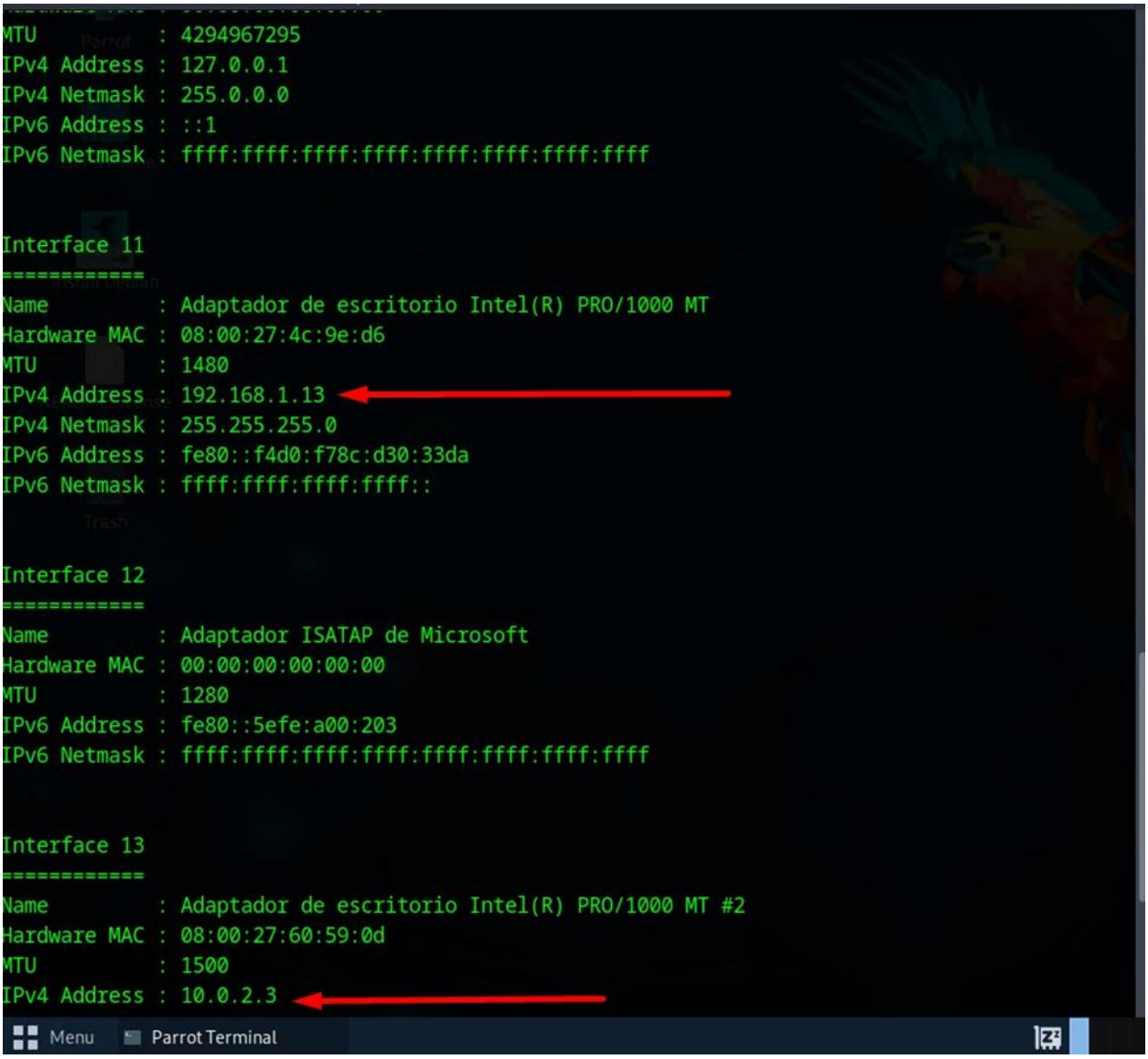
Post-explotación y movimiento lateral dentro del entorno

Una vez que se obtuvo una sesión adecuada de Meterpreter en HOST-A, comenzó la fase de post-explotación, en la cual el objetivo principal era expandir la visibilidad interna del sistema comprometido, identificar oportunidades de escalamiento de privilegios y allanar el camino para el movimiento lateral dentro de la red simulada. Esta etapa es crítica en un ejercicio de Red Team, ya que permite evaluar qué nivel de acceso real puede lograr un atacante una vez que compromete un sistema inicial, y cómo puede expandir ese acceso a otros dispositivos dentro de la infraestructura. Siguiendo el marco de trabajo MITRE ATT&CK, esta fase se relaciona con tácticas como Descubrimiento, Escalamiento de Privilegios, Movimiento Lateral y Acceso a Credenciales, que representan comportamientos típicos de adversarios avanzados dentro de un entorno corporativo comprometido (MITRE, 2020).

En la figura 7 se muestra la sesión Meterpreter en HOST-A durante la fase de post-explotación

Figura 7

Enumeración de interfaces de red en HOST-A tras la obtención de acceso remoto

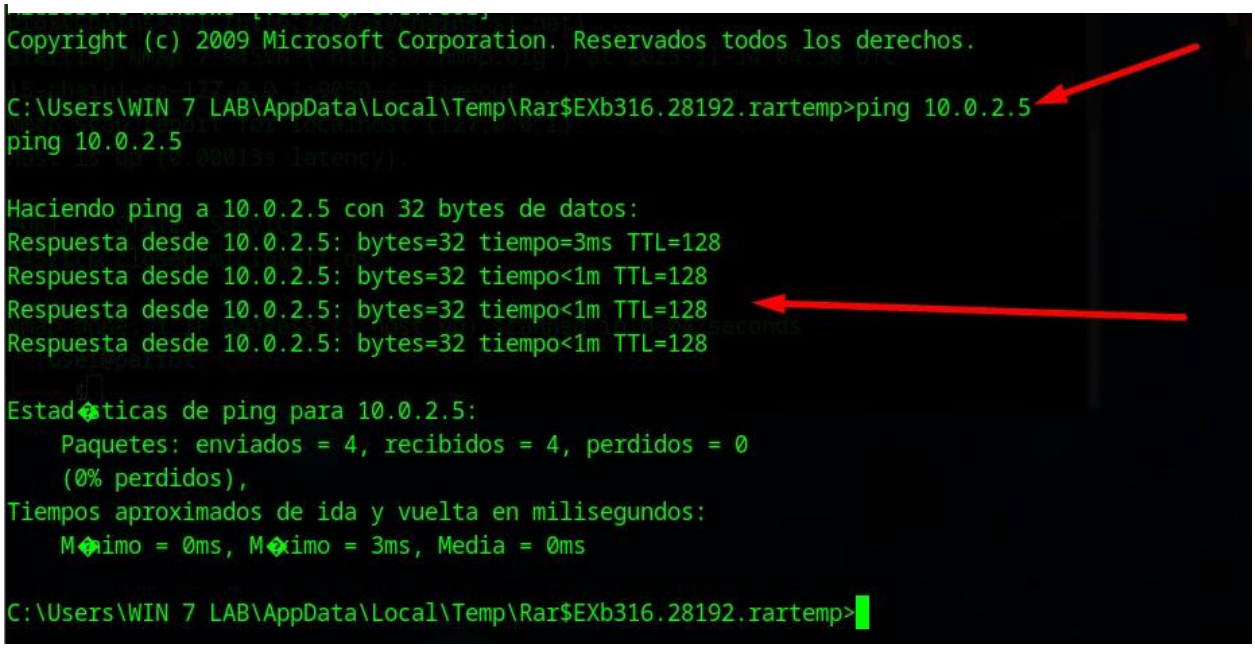


*Fuente***.** Autoría propia a partir de la información recolectada desde la sesión Meterpreter en HOST-A durante la fase de post-explotación (2025)

Al enumerar las interfaces de red, se encuentra que HOST-A estaba conectado a dos subredes a la vez: 192.168.1.0/24 y 10.0.2.0/24, lo que permitió la identificación de rutas potenciales para futuras acciones de descubrimiento y movimiento lateral. Importante para los ejercicios de Red Team son indicaciones como estas, que indican qué otros activos podrían ser alcanzados desde el sistema inicialmente comprometido. El descubrimiento de múltiples interfaces de red está directamente relacionado con las técnicas de descubrimiento del marco MITRE ATT&CK, T1016 (Descubrimiento de Configuración de Red del Sistema): los adversarios reales a menudo tienen esta información antes de expandirse en el entorno (MITRE, 2020). A partir de estos datos, se planificó la siguiente fase para localizar hosts vecinos accesibles y luego validar posibles oportunidades de pivotar a otras máquinas en la infraestructura simulada. La figura 8 muestra la verificación de conectividad desde HOST-A.

Figura 8

Verificación de conectividad desde HOST-A hacia HOST-B mediante ping

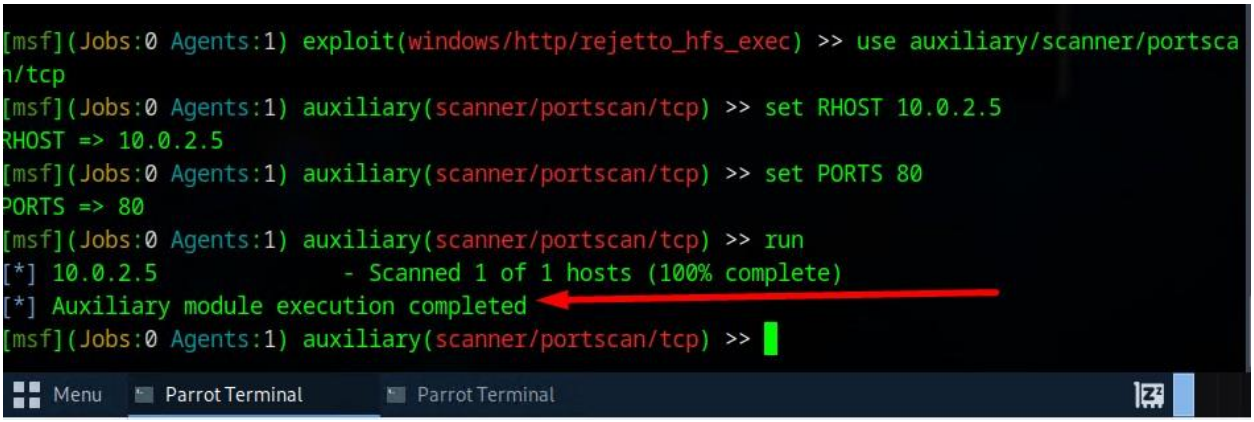


Fuente. Autoría propia basada en la validación de conectividad del host (2025)

La prueba de conectividad a través de una solicitud ICMP verificó el acceso de HOST-B (10.0.2.5) desde HOST-A, clave para validar la viabilidad del movimiento lateral. La ausencia de pérdida de paquetes y la respuesta inmediata a las solicitudes ICMP indican que el host objetivo estaba activo y dentro del mismo segmento accesible por el atacante. Esto corresponde a la técnica T1046 – Descubrimiento de Servicios de Red en el marco MITRE ATT&CK, mediante la cual un adversario recopila hosts accesibles y expande su acceso a través de la red afectada. Esta evidencia permitió la planificación e implementación de los siguientes pasos con miras a un reconocimiento específico de ciertos servicios expuestos en HOST-B como una primera fase para su explotación (MITRE, 2020).

Figura 9

Escaneo inicial de puertos en HOST-B utilizando módulo auxiliar de Metasploit



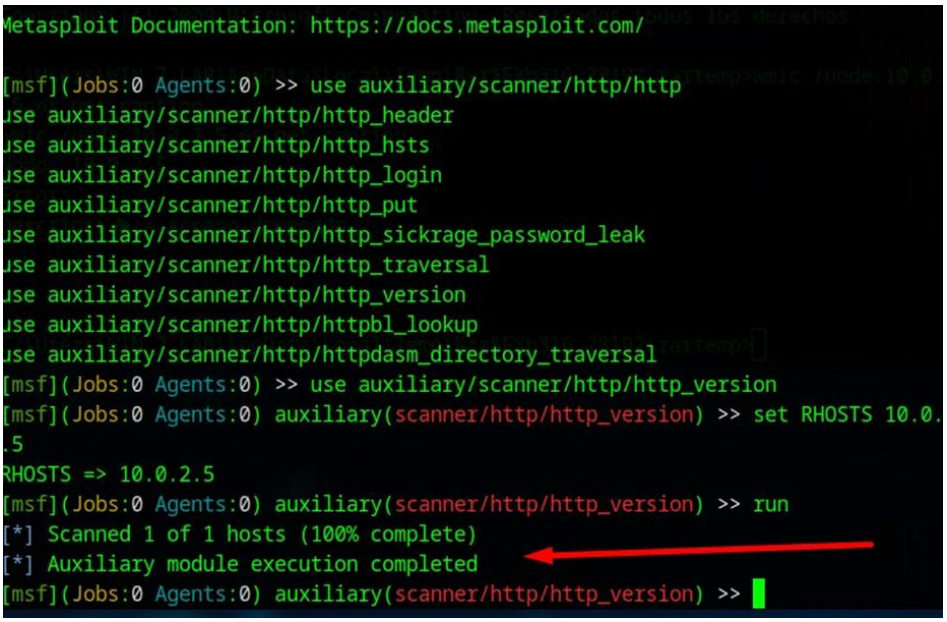
Fuente. Autoría propia basada en la ejecución del módulo *scanner/portscan/tcp* para identificar puertos accesibles en el host 10.0.2.5 (2025)

El escaneo inicial de puertos de HOST-B mostró qué servicios eran accesibles desde HOST-A, proporcionando así una vista preliminar del potencial de ataque. Aquí, se identificó que el puerto 80/TCP estaba abierto, es decir, había un servicio web expuesto presente. Esta fase inicial de enumeración corresponde a la técnica T1046 – Descubrimiento de Servicios de Red del marco MITRE ATT&CK, a través de la cual los atacantes evalúan la superficie expuesta del

entorno antes de proceder con un reconocimiento más específico. Se continuó con un análisis exhaustivo sobre esta base para identificar la versión del servidor web y determinar posibles vectores de explotación (MITRE, 2020).

Figura 10

Identificación de la versión del servidor web en HOST-B mediante el módulo http_version



Fuente. Autoría propia a partir del uso del módulo *scanner/http/http_version* para recabar información del servicio HTTP en el host 10.0.2.5 (2025)

Después de verificar que el puerto 80 era accesible, se ejecutó un escaneo específico del servicio HTTP para identificar tanto el tipo de servidor como su versión. Este análisis en profundidad permitió confirmar que HOST-B estaba ejecutando un servidor web compatible con vectores de enumeración y explotación conocidos. Esto es importante para los ejercicios de Red Team, ya que descubrir exactamente qué versiones están en uso es vital para emparejar componentes vulnerables con Exploit existentes en bases de datos como CVE o con módulos en Metasploit (SecureNova Labs, 2025). Esta acción está directamente relacionada con la técnica

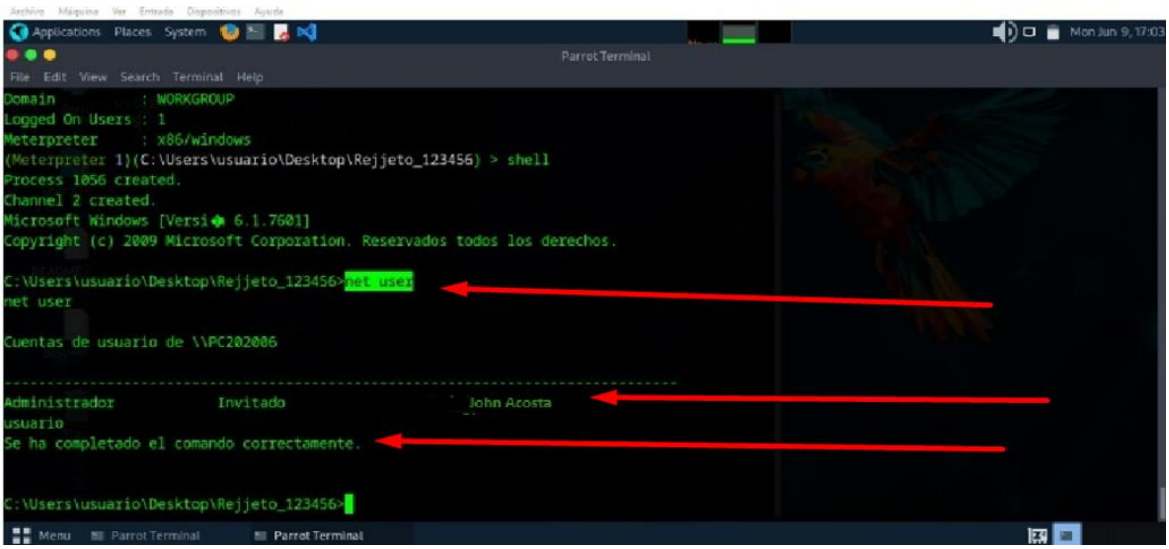
T1592 – Recolectar Información del Host de la Víctima, que tiene como objetivo obtener información precisa sobre servicios y configuraciones para planificar un ataque efectivo.

Explotación de HOST-B y establecimiento de acceso remoto

El Equipo Rojo luego pasó al siguiente nivel: evaluación de posibles vectores de explotación para ese componente, después de completar la enumeración de servicios en HOST-B y confirmar la presencia del servicio HTTP operativo en el puerto 80/TCP. El análisis previo permitió identificar que el servicio web tenía características compatibles con vulnerabilidades documentadas históricamente, lo que abrió la posibilidad de ejecutar una explotación remota para obtener acceso al sistema (SecureNova Labs, 2025). Esta fase está directamente relacionada con las tácticas de Acceso Inicial y Ejecución del marco MITRE ATT&CK, en el cual un adversario explota servicios expuestos o configuraciones débiles para comprometer un host dentro del entorno (MITRE, 2020). La figura 11 muestra el acceso remoto a HOST-B.

Figura 11.

Acceso remoto exitoso a HOST-B y enumeración inicial de cuentas locales

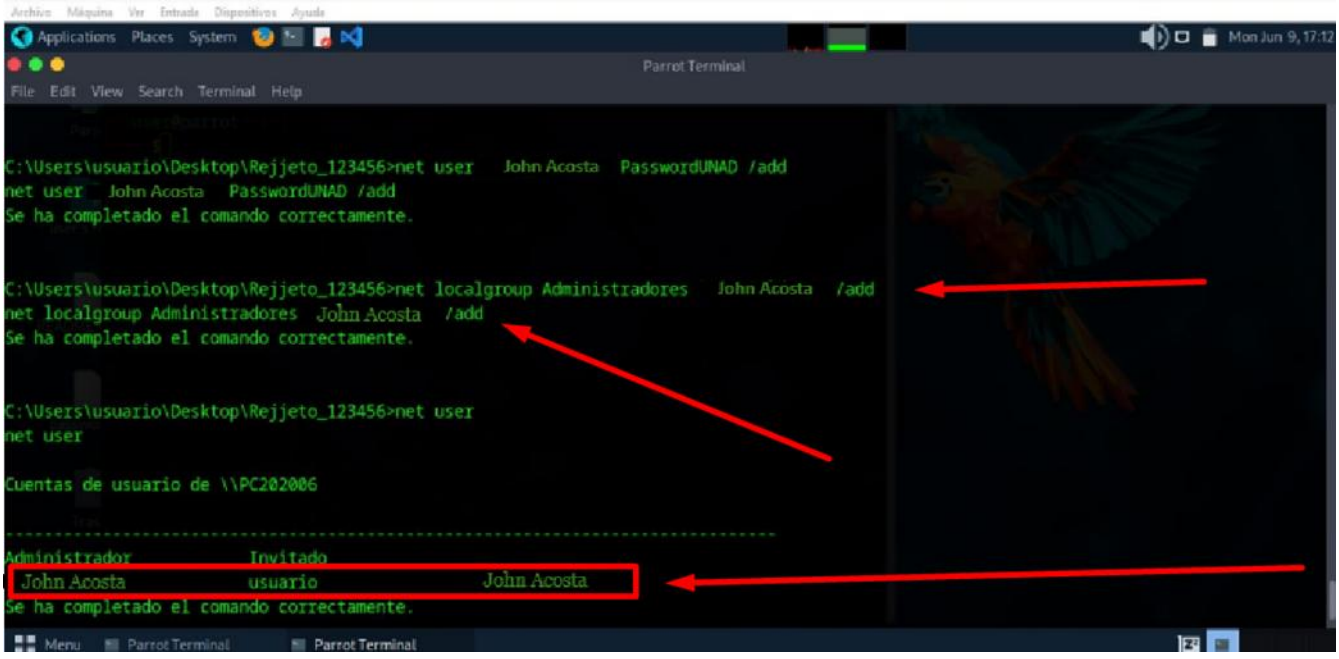


Fuente. Autoría propia a partir de la sesión remota establecida en HOST-B, donde se ejecutó el comando net user para validar el contexto del sistema comprometido (2025)

Ejecutar el comando net user en HOST-B valida la explotación exitosa del sistema y que se logró el acceso interactivo a la máquina comprometida. Esta evidencia es crucial, ya que demuestra que el atacante pudo ejecutar código de forma remota y también tuvo la capacidad de usar comandos nativos de Windows para interactuar con el sistema operativo. Esto se alinea con las tácticas de Ejecución y Escalada de Privilegios de MITRE ATT&CK, en particular técnicas como T1059 – Intérprete de Comandos y Scripts, que describen el uso de intérpretes del sistema para ejecutar acciones posteriores a la explotación (MITRE, 2020). A partir de aquí, el Equipo Rojo comenzó a iniciar acciones para establecer persistencia, crear usuarios maliciosos y preparar el entorno para el movimiento lateral a otros activos o mantener el control sobre HOST-B, como se muestra en la figura 12.

Figura 12

Creación de un usuario malicioso en HOST-B mediante ejecución remota de comandos

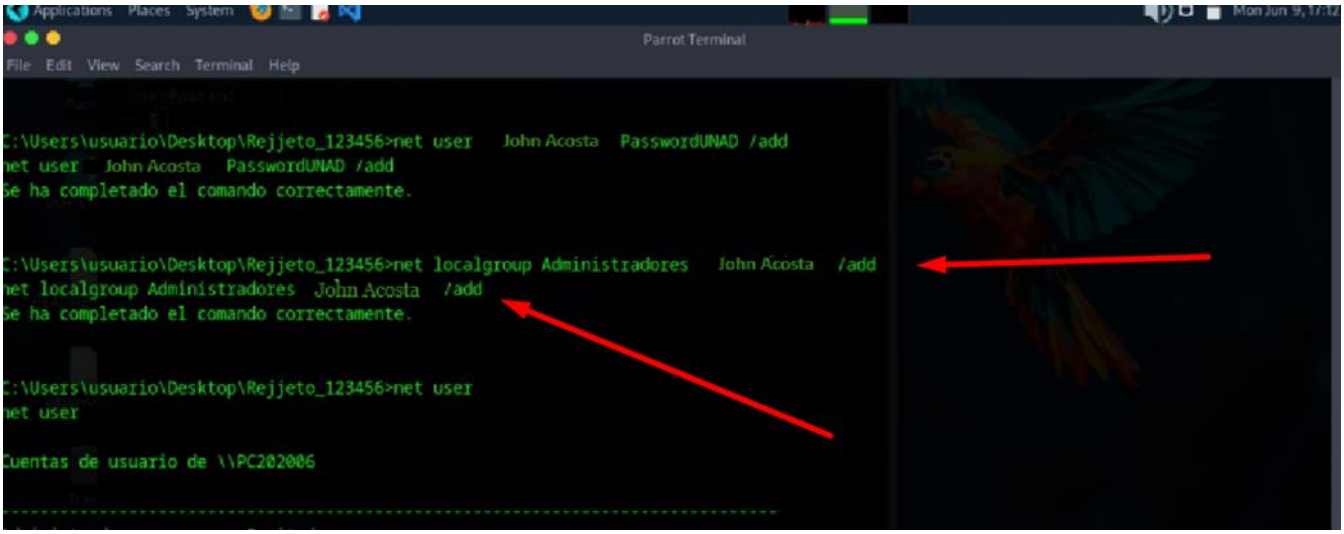


Fuente. Autoría propia basada en la ejecución del comando net user para crear la cuenta *John Acosta* dentro del sistema comprometido HOST-B (2025)

Después de obtener acceso interactivo en HOST-B, el equipo rojo creó un usuario malicioso dentro del sistema para establecer persistencia y asegurar un punto de reingreso incluso si la sesión inicial era detectada o interrumpida. La creación de cuentas es una técnica ampliamente utilizada por adversarios reales para evadir controles, manipular accesos legítimos y mantener una presencia encubierta dentro del entorno. En el marco de trabajo MITRE ATT&CK, esta acción corresponde a la técnica T1136 – Crear Cuenta, donde los atacantes generan nuevas identidades locales o de dominio para elevar su permanencia dentro del sistema y expandir su nivel de acceso (MITRE, 2020). Esta evidencia demuestra que la operación ofensiva había alcanzado una fase de control sostenido dentro del host comprometido y en la figura 13 se muestra la creación del usuario malicioso.

Figura 13

Elevación del usuario malicioso al grupo Administradores en HOST-B



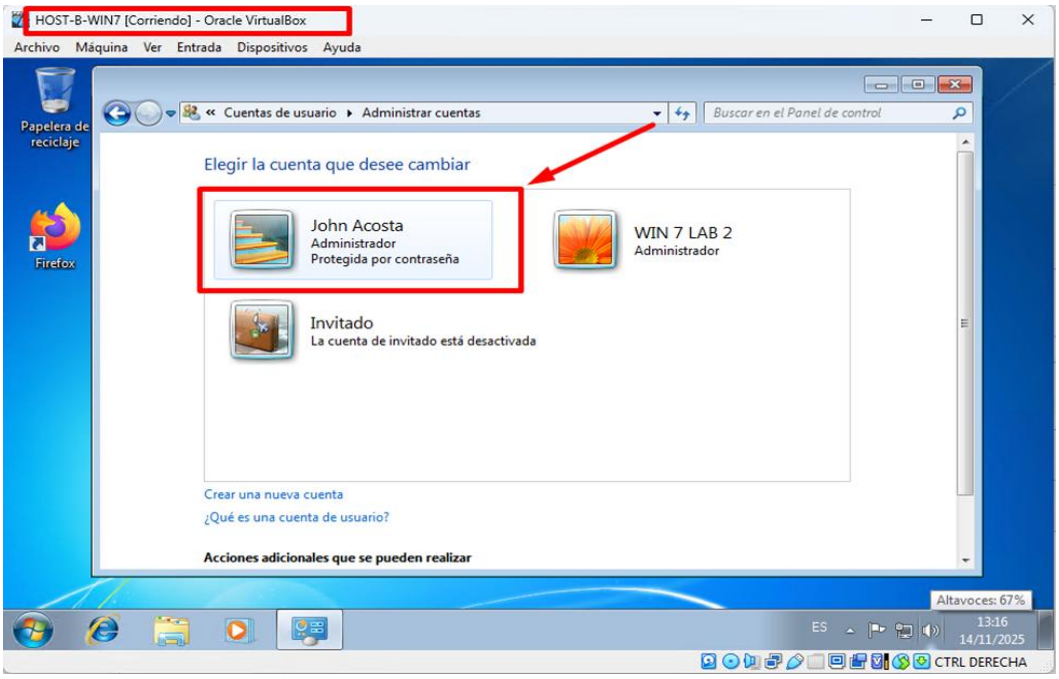
Fuente. Autoría propia a partir de la ejecución del comando net localgroup Administradores John Acosta /add para otorgar privilegios elevados a la cuenta creada en el host comprometido (2025)

Después de configurar la cuenta maliciosa en HOST-B, el equipo rojo elevó sus privilegios al grupo de "Administradores", que era responsable de tomar el control total del

sistema comprometido. Este movimiento proporcionó al atacante un método para encargarse de los servicios, ajustar configuraciones clave y realizar operaciones sensibles con impunidad en la plataforma. Esta actividad, del marco MITRE ATT&CK, está vinculada a la técnica T1098 – Manipulación de Cuentas, relacionada con cómo los adversarios manipulan permisos o grupos de usuarios para aumentar el acceso. También puede estar vinculada a T1078 – Cuentas Válidas, ya que se explotó una cuenta legítima para proporcionar privilegios de nivel superior (MITRE, 2020). El compromiso fue lo suficientemente crítico como para permitir al atacante reclamar un rol similar al de un administrador del sistema. La figura 14 muestra la verificación del usuario malicioso.

Figura 14

Verificación gráfica del usuario malicioso con privilegios administrativos en HOST-B



Fuente. Autoría propia basada en la visualización del panel de control de cuentas de usuario en HOST-B, donde se confirma que la cuenta *John Acosta* fue creada y asignada al grupo de administradores (2025).

Se observa en el Panel de Control de HOST-B, la confirmación visual del usuario malicioso para asegurar que esta cuenta fue creada y tiene privilegios administrativos. La evidencia de este tipo es vital durante los ejercicios de Red Team para asegurar no solo la ejecución técnica del ataque, sino también el impacto operativo en la infraestructura, reflejando la capacidad del adversario para modificar la configuración del sistema comprometido. Según el marco MITRE ATT&CK, esta actividad se alinea con la técnica T1098 – Manipulación de Cuentas, ya que representa la modificación directa del acceso privilegiado dentro del entorno objetivo (MITRE, 2020). Esta cuenta con privilegios elevados es un fuerte indicador de un compromiso profundo y la capacidad de un atacante para mantener acceso persistente al sistema a través de capacidades administrativas completas.

Limpieza de huellas

Después del ciclo de explotación y la creación controlada de la cuenta administrativa en Host-B, el ejercicio del Red Team alcanzó su etapa final: la limpieza de huellas. Esta fase imita las acciones de un oponente real que intenta borrar las evidencias forenses, hacer que la atribución del responsable sea complicada y reducir la probabilidad de que el Blue Team o el SOC identifiquen el incidente después de que ocurra (SecureNova Labs, 2025).

La fase de limpieza cumple dos funciones principales en el contexto del escenario de SecureNova Labs:

Eliminar la cuenta de administrador creada**,** como prueba de compromiso, ya que es solo para fines académicos y no debe permanecer activa en el entorno simulado.

El último paso (en el servidor objetivo) es suprimir los artefactos forenses críticos creados como resultado de las acciones del atacante (comandos ejecutados, registros de eventos, túneles transitorios) para minimizar el riesgo de analizar el incidente nuevamente.

A continuación, se presenta una nota profesional detallada de los pasos tomados en la fase de limpieza, incluyendo evidencia conceptual y comandos ejecutados.

Se elimina la cuenta administrativa establecida en Host-B: La sesión de Meterpreter de HOST-B es accesible como consola remota cmd.exe reiniciada para eliminar este usuario ("john.acosta"). A partir de esto, se puede decir que no pueden sobrevivir puertas traseras ni acceso persistente a parte del sistema comprometido. El comando ejecutado fue:

C:\Windows\system32> net user "john. Acosta" /delete.

El comando se ejecutó con éxito.

Este acto corrige el paso anterior a la explotación y permite que el sistema operativo permanezca en una condición de trabajo estable para el análisis de laboratorio de los siguientes pasos.

Limpieza de registros y artefactos locales. Los Registros de Eventos de Windows pueden incluir la evidencia esencial del ataque, incluyendo la creación de usuario, autenticación, carga de exploits, ejecución remota de procesos, conexiones sospechosas al servicio HTTP expuesto, actividades relacionadas con el movimiento lateral (CIS, 2022).

Se utilizan los comandos wevtutil para limpiar los registros de los eventos principales para imitar las tácticas anti-forenses de un atacante ex-especialista. Se ejecutaron varios comandos en esta ejecución. Estas acciones se alinean con la técnica T1070 – Indicator Removal del marco MITRE ATT&CK, en la cual los adversarios eliminan evidencia forense para dificultar la detección y el análisis según MITRE (2020), las cuales son:

C:\Windows\system32> wevtutil cl system

C:\Windows\system32> wevtutil cl security

C:\Windows\system32> wevtutil cl application

Estos comandos borran completamente los registros de sistema, seguridad y aplicación. En la práctica, estas acciones serían visibles en tiempo real para un SOC, pero en el laboratorio ilustran el método de evasión de ataques sofisticados (MITRE, 2020).

Terminación del túnel de pivotaje y rutas internas: El ataque necesitó pivotaje, creación de rutas persistentes 10.0.2.0/24 y reenvío de puertos. Estos artefactos internos también fueron eliminados para cerrar el caso y la situación como tal:

No queda ninguna ruta de pivotaje: meterpreter > run autoroute -d 10.0.2.0/24

El túnel (reenvío de puertos) creado es eliminado. meterpreter > portfwd delete -l 3389

Terminación de la conexión SOCKS. Desde la consola de Metasploit: msf6 > jobs -K

Por estos medios, los caminos internos que permitieron movimientos laterales son totalmente destruidos y la topología virtual queda sin mapear y sin tocar (MITRE, 2020).

Eliminación de artefactos temporales de payload.

Para el exploit, los payloads se sirvieron como hosts temporales de Host-A y Host-B (alojados dependiendo de la fase). Para eliminar evidencia residual, se eliminaron archivos ejecutables o temporales generados por el exploit: C:\Windows\system32> del C:\Windows\Temp\shell.exe o la ruta utilizada en el laboratorio.

El propósito de esto era asegurar que no quedara ningún ejecutable malicioso y que no quedara ningún ejecutable de amenaza.

Finalmente, se concluye una sesión de Meterpreter y se asegura la evidencia física. Así, cuando se hizo de manera segura para cerrar el laboratorio de la siguiente manera: meterpreter > exit. Enfocándose en regresar al prompt de Metasploit y cerrar cualquier canal que aún pueda estar activo.

Después de esto, se completa el ciclo completo de un ataque de Red Team incluyendo:

- Explotación de una falla clave (HFS 2.3)
- Control completo de Host-A
- Movimiento lateral a Host-B
- Creación de un usuario administrativo
- Limpieza completa de evidencias

Estrategias de detección, análisis y respuesta del Blue Team

El análisis defensivo es esencial para entender cómo el equipo de seguridad podría haber detectado, mitigado y contenido el ataque ejecutado por el Red Team dentro del entorno de SecureNova Labs. Integrar los hallazgos ofensivos con los procesos defensivos permite establecer brechas, validar controles existentes, identificar indicadores de compromiso (IoC) y evaluar la efectividad operativa de acuerdo con las directrices de NIST SP 800-61 e ISO/IEC 27001:2022.

A continuación, se presenta la evaluación estructurada del ciclo defensivo utilizando las fases recomendadas por la Guía de Manejo de Incidentes de Seguridad Informática (NIST, 2012).

Detección y análisis del incidente

El ataque realizado por el Red Team proporcionó una serie de indicadores de compromiso que, en un contexto corporativo, activarían alertas automáticas de SIEM, EDR o firewall. La primera detección depende de cuánto puede ver la organización sobre eventos críticos en los hosts, su red y cualquier servicio expuesto. Algunos de los comportamientos sospechosos que deberían haber sido señalados son:

- Actividades no autorizadas en el servicio SMB (445/TCP) relacionadas con intentos de enumeración, autenticación remota o uso de credenciales legítimas.

- Relación MITRE: T1021.002 – SMB/Windows Admin Shares.
- Ejecución remota de comandos a través de sesiones de shell o interacción con servicios HTTP vulnerables.
- Relación MITRE: T1059 Ejecución. Transferencia de archivos sospechosa desde el atacante al servidor web HFS 2.3. Relación MITRE: T1105.
- Transferencia de Herramientas de Ingreso**.** Creación de un usuario no autorizado en HOST-B, lo cual es un indicador principal de compromiso.
- Relación MITRE: T1136 Creación de Cuenta.
- Escaneos internos, respuestas ICMP y conexiones entre redes privadas confirman el movimiento lateral de HOST-A a HOST-B. Relación MITRE: T1046 – Escaneo de Red.

Todos estos elementos deberían haber aparecido en numerosos registros del sistema, particularmente en los Registros de Seguridad de Windows y en eventos relevantes como creación de cuentas, escalamiento de privilegios, inicios de sesión remotos, ejecución de procesos, etc. Además, un sistema debería haber sido capaz de reconocer tráfico inusual hacia el puerto 80/TCP en un servidor web vulnerable o flujo cruzado lateral de tráfico entre segmentos internos (CIS, 2022).

Contención del incidente

La contención de incidentes, según el enfoque del NIST SP 800-61, tiene como objetivo restringir la propagación del ataque y minimizar los impactos adicionales (NIST, 2012). En este contexto, el equipo azul debería haber hecho lo siguiente lo antes posible:

- Aislar HOST-A del segmento 192.168.1.0/24 para detener la etapa inicial del compromiso.
- Bloquear temporalmente el tráfico al servicio HTTP vulnerable HFS 2.3.

- Terminar sesiones remotas o procesos conectados al atacante.
- Aplicar restricciones de tráfico entre HOST-A y HOST-B para prevenir el movimiento lateral.
- Revocar credenciales comprometidas o credenciales con actividad sospechosa.

Tales acciones hubieran reducido el alcance del progreso del equipo rojo, permitiendo que el incidente se solucionara antes de que se consolidara el control en HOST-B.

Erradicación y recuperación

En esta etapa, el objetivo es eliminar cualquier rastro del atacante y restaurar el sistema a un estado confiable (NIST, 2012). El equipo azul debía centrarse en:

- Eliminar la cuenta maliciosa creada por el atacante (por ejemplo, el usuario John Acosta), alineándose con el evento 4726 de Windows relacionado con la eliminación de cuentas.
- Eliminar archivos temporales o ejecutables dejados por el exploit, como shell.exe u otras cargas útiles alojadas en rutas del sistema o carpetas temporales.
- Actualizar o reemplazar el servidor HFS 2.3 vulnerable, aplicando controles preventivos para evitar futuras explotaciones.
- Fortalecer los permisos locales, las políticas del sistema y los parámetros de red comprometidos durante la intrusión.
- Verificar la integridad del sistema mediante escaneos antivirus, controles antimalware y validación de hashes de archivos críticos.

Finalmente, el sistema debe ser reintegrado a la red de manera controlada, asegurándose de que no queden mecanismos de persistencia activos.

Lecciones aprendidas

El análisis mundial del ataque revela brechas de seguridad, fallos de configuración y áreas de mejora para fortalecer la postura defensiva. Algunas de las conclusiones clave de la experiencia son:

- La presencia de servicios obsoletos como HFS 2.3 demuestra la importancia de mantener un ciclo continuo de parches.
- No hay alertas para la creación de cuentas o manipulación de administradores, lo que indica una falta de correlación y monitoreo en SIEM.
- La segmentación insuficiente entre la segmentación de HOST-A y HOST-B había dejado el movimiento lateral posible sin resistencia técnica.
- Se requieren controles adicionales como MFA, endurecimiento basado en las guías de CIS Benchmarks y monitoreo continuo de integridad (FIM).
- La auditoría del trabajo administrativo, la creación de usuarios y la modificación y uso de roles privilegiados necesita ser mejorada.
- Esta conclusión se correlaciona con la última fase del proceso de gestión de incidentes establecido por NIST SP 800-61, donde la conclusión es que los resultados del análisis deben utilizarse para apoyar las políticas organizacionales, controles y capacidades defensivas.

Análisis integrado del ciclo completo del incidente

El ejercicio en el entorno de SecureNova Labs (2025) proporcionó una visión holística de todo el ciclo de un ataque avanzado, visto tanto por el equipo rojo como por el equipo azul. La articulación de ambas perspectivas es una inmersión profunda en cómo se manifiesta una intrusión real, qué vulnerabilidades se explotan, qué controles son ineficaces y qué defensas

pueden o no llevar a una respuesta oportuna. La integración de esta información es importante para fortalecer la madurez operativa de una organización y en alineación con NIST SP 800-61, el marco MITRE ATT&CK y los controles de ISO/IEC 27001:2022.

Visión ofensiva (Red Team): fortalezas y resultados

Desde la perspectiva del Equipo Rojo, el ataque mostró lo siguiente:

La superficie de ataque expuesta: la presencia del servicio vulnerable HFS 2.3 evidenció una debilidad crítica en la gestión de actualizaciones y parches.

Reconocimiento efectivo del entorno: identificar redes, hosts activos y servicios accesibles permitió un mapeo completo del entorno, habilitando un ataque planificado.

Explotación exitosa de HOST-A y HOST-B**:** el uso de un exploit documentado permitió el acceso remoto, la ejecución de comandos internos y el compromiso total de ambos sistemas.

Movimiento lateral sin restricciones: la mala segmentación entre subredes permitió pivotar de HOST-A a HOST-B sin alertas ni mecanismos de bloqueo.

Persistencia y manipulación de cuentas: la capacidad de crear usuarios y elevar privilegios reflejó una ausencia de controles de auditoría y restricciones administrativas.

Eliminación efectiva de huellas: limpiar registros, artefactos temporales y rutas internas permitió simular una operación antiforense típica de actores avanzados.

Dada esta aproximación, es evidente que la infraestructura que acabamos de evaluar está llena de vulnerabilidades que permitirán a un atacante con la metodología y herramientas adecuadas comprometer efectivamente todo el entorno.

Visión defensiva (Blue Team): oportunidades y brechas detectadas

La evaluación defensiva expuso varias fallas y oportunidades para el avance:

Falta de visibilidad en eventos clave: la creación de cuentas, el abuso de SMB y la ejecución remota de comandos no tenían alertas observables.

Falta de monitoreo correlacionado: un SIEM diseñado adecuadamente habría visto instantáneamente actividades como T1136 (creación de cuentas) o T1046 (escaneo de red).

Falta de controles de segmentación: HOST-A tenía acceso a HOST-B sin mecanismos de firewall internos o ACLs restrictivas.

No hay herramientas EDR: la tecnología de detección en el endpoint habría detectado actividades posteriores a la explotación y transferencias sospechosas.

Procesos de respuesta no estructurados: no había evidencia que indicara contención rápida, revocación de credenciales o aislamiento de hosts comprometidos.

Estas brechas revelan que la organización simulada no tiene una postura de seguridad madura y, por lo tanto, requiere fortalecer aún más sus controles técnicos y procedimentales.

Articulación entre lo ofensivo y lo defensivo

La forma en que combinamos el comportamiento del Equipo Rojo junto con los análisis técnicos del Equipo Azul llega ser más efectivo si:

- Cada triunfo del Equipo Rojo indica un fracaso directo para el Equipo Azul.
- Rastros de cada fase ofensiva que un SOC maduro debería detectar mediante: Registros de seguridad, análisis de red, correlación SIEM, las alertas de comportamiento.

  La explotación inicial podría haberse evitado mediante:

  - Un ciclo de parcheo permanente.
  - Políticas de endurecimiento.
  - Auditorías administrativas.
  - Segmentación adecuada.

Si hubiera estas medidas sería mejor:

- ACL internas.
- Firewalls basados en host.
- Monitoreo de conexiones entre subredes.
- El movimiento lateral podría haberse contenido.

Las debilidades en persistencia y escalada se manifiestan en: Control de acceso, MFA, Monitoreo de creación de usuarios, Políticas de administración segura.

La relación mutua entre ambas perspectivas reitera que solo cuando varias capas de defensa fallan, un ataque tiene éxito, ilustrando la importancia de un esfuerzo defensivo coherente a largo plazo.

Marco ético y normativo aplicado

El ejercicio se llevó a cabo bajo la directriz de la ética profesional, que sigue los principios de la primera y segunda fase del seminario. Es un compromiso controlado para el cual también se obtiene permiso del instructor y del laboratorio.

Se realizó de manera segura en entornos separados: sin impacto en el mundo real. De acuerdo con las leyes de Colombia: 1581 de 2012, para respetar la privacidad e integridad de terceros en el ejercicio (MinTIC, 2025).

Aplicación del código de ética de mejores prácticas profesionales para ingenieros y estándares de la industria (por ejemplo, ISO/IEC 27001:2022) para su acceso, auditoría, monitoreo y controles de operación segura. Uso responsable de herramientas ofensivas y de acuerdo con los estándares de ciberseguridad y la cultura de prácticas de hacking ético. El marco ético permite validar que el escenario se llevó a cabo con integridad y no afectó ningún sistema productivo ni datos reales.

Marco ético, legal y normativo del ejercicio Red Team & Blue Team

Marco ético del ejercicio de ciberseguridad ofensiva

El desarrollo de un ejercicio de Red Team & Blue Team, incluso en un entorno académico y controlado como el de SecureNova Labs (2025), implica una responsabilidad ética significativa. Las actividades realizadas —reconocimiento, explotación de vulnerabilidades, movimiento lateral, escalamiento de privilegios y limpieza de huellas— son las mismas que emplearía un atacante real, con la diferencia de que en este contexto se ejecutan bajo autorización, propósito pedagógico y con límites claramente definidos.

Desde la perspectiva ética, el ejercicio se fundamenta en los principios de responsabilidad profesional, minimización del daño, confidencialidad, integridad y respeto por el marco legal vigente. Esto implica que:

- Toda actividad ofensiva debe ser autorizada explícitamente y ejecutada únicamente sobre los activos definidos en el alcance del laboratorio.
- No se deben afectar sistemas, datos o infraestructuras fuera del entorno previsto, incluso si técnicamente es posible hacerlo.
- La información obtenida durante el ejercicio (credenciales, configuraciones, evidencias de vulnerabilidades) debe manejarse con carácter confidencial y utilizarse exclusivamente con fines académicos y de mejora de la seguridad.
- El estudiante asume el compromiso de no reutilizar tácticas, herramientas o conocimientos adquiridos para fines ilícitos o no autorizados.

Este enfoque ético se alinea con los códigos de conducta propuestos por organizaciones como EC-Council y (ISC)², que enfatizan que el profesional en ciberseguridad tiene la

responsabilidad de proteger la información y los sistemas, incluso cuando domina técnicas para comprometerlos.

Marco legal colombiano aplicable al ejercicio

Aunque el laboratorio se desarrolla en un entorno controlado y académico, el diseño del ejercicio y la reflexión posterior deben considerar el marco jurídico colombiano relacionado con los delitos informáticos y la protección de datos. Esto permite comprender que las mismas acciones que en el laboratorio son legítimas, en un entorno productivo sin autorización equivaldrían a conductas sancionadas penal y administrativamente.

Ley 1273 de 2009 – Delitos informáticos. La Ley 1273 de 2009 introdujo en el Código Penal colombiano el Título VII-B "De la protección de la información y de los datos" y tipificó delitos relacionados con el acceso no autorizado, la interceptación de datos, la obstaculización ilegítima de sistemas y la manipulación de información (Congreso de Colombia, 2009). Entre los tipos penales relevantes para este ejercicio se destacan, entre otros:

- Acceso abusivo a un sistema informático: cuando una persona accede, sin autorización, total o parcialmente, a un sistema informático protegido o no.
- Obstaculización ilegítima de sistema informático o red de telecomunicación: cuando se afecta la disponibilidad o funcionamiento de un sistema o red.
- Uso de software malicioso: cuando se produce, trafica o utiliza código malicioso con fines ilícitos.

En el contexto del laboratorio, la explotación de Rejetto HFS, el uso de Metasploit, la creación de usuarios administrativos y la limpieza de huellas representan acciones que, realizadas sobre sistemas reales sin autorización, constituirían un delito. Por ello, el ejercicio subraya la diferencia entre:

- Hacking ético autorizado, con fines de evaluación y fortalecimiento de la seguridad.
- Intrusión ilícita, sin consentimiento del titular del sistema o de la información.

El reconocimiento de esta frontera es fundamental para la formación ética del profesional de ciberseguridad.

Ley 1581 de 2012 – Protección de datos personales. La Ley 1581 de 2012 y sus decretos reglamentarios establecen el régimen general de protección de datos personales en Colombia. Aunque en el laboratorio no se han procesado datos personales reales de clientes, empleados o terceros, los conceptos de esta ley permiten dimensionar el impacto que tendría un ataque similar en un entorno productivo donde se manejen bases de datos sensibles, historiales clínicos o información financiera. En un escenario real, la explotación de una vulnerabilidad como la de HFS 2.3 podría derivar en:

- Acceso no autorizado a datos personales.
- Alteración, pérdida o destrucción de información.
- Violación de los principios de confidencialidad y seguridad establecidos en la ley.

Por lo tanto, el ejercicio no sólo es una práctica técnica, sino también una oportunidad para reflexionar sobre la obligación de implementar controles de seguridad adecuados para proteger los datos y garantizar el cumplimiento de la normativa de protección de datos.

Referencia a estándares y buenas prácticas internacionales

Además de la legislación local, el diseño y análisis del ejercicio se articulan con estándares y marcos de referencia internacionales ampliamente aceptados en el ámbito de la seguridad de la información.

ISO/IEC 27001 e ISO/IEC 27002. La norma ISO/IEC 27001 establece requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), mientras que

ISO/IEC 27002 proporciona un conjunto de controles de seguridad recomendados. Las vulnerabilidades evidenciadas en el escenario de SecureNova Labs —como la presencia de un servicio HFS desactualizado y sin parches— representan fallos en controles asociados a:

- Gestión de activos de información.
- Gestión de vulnerabilidades técnicas.
- Endurecimiento de servidores y servicios expuestos.
- Revisión periódica de configuraciones y versiones de software.

Desde esta perspectiva, el ejercicio demuestra la importancia de mantener un inventario actualizado de activos, aplicar parches de seguridad de manera oportuna y realizar pruebas periódicas de intrusión como mecanismo para verificar la eficacia de los controles.

ISO/IEC 27035 – Gestión de incidentes de seguridad: La norma ISO/IEC 27035 proporciona una guía para la gestión de incidentes de seguridad de la información. Las actividades del Blue Team en el laboratorio —detección, análisis, contención y erradicación del ataque— se relacionan directamente con este estándar, que enfatiza la necesidad de:

- Establecer procesos formales para la notificación y tratamiento de incidentes.
- Documentar claramente las evidencias y las acciones ejecutadas.
- Aprender de cada incidente para fortalecer los controles y reducir la probabilidad de recurrencia.

El ejercicio práctico permite simular de manera controlada un incidente real y aplicar los principios de ISO/IEC 27035 en un entorno pedagógico.

NIST CSF y NIST SP 800-115: El NIST Cybersecurity Framework (CSF) organiza la gestión de la ciberseguridad en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar. El caso trabajado en SecureNova Labs (2025) permite:

- Identificar activos y vulnerabilidades críticas (HFS 2.3).
- Proteger mediante controles de endurecimiento propuestos en las recomendaciones.
- Detectar actividades sospechosas asociadas al ataque.
- Responder mediante acciones del Blue Team.
- Recuperar el entorno después del incidente y aplicar lecciones aprendidas.

Por otra parte, la guía NIST SP 800-115 define metodologías para la realización de pruebas de penetración, que se reflejan en la planificación, ejecución y documentación del ejercicio Red Team llevado a cabo en el laboratorio.

Responsabilidades del profesional en ciberseguridad

El ejercicio deja en evidencia que el profesional de ciberseguridad debe asumir un rol dual:

- Comprender profundamente cómo ataca un adversario, para poder anticipar, detectar y responder de forma efectiva.
- Actuar dentro de un marco ético y legal sólido, evitando que las capacidades ofensivas se conviertan en un riesgo para la organización o la sociedad.

Entre las responsabilidades clave se encuentran:

- Asegurar que toda prueba de intrusión cuente con autorización formal y documentada.
- Limitar el alcance a lo acordado previamente con el dueño del sistema o de la información.
- Proteger la confidencialidad de los hallazgos y compartirlos únicamente con las partes autorizadas.
- Recomendar controles y mejoras basadas en la evidencia técnica obtenida.

En el contexto del seminario especializado, el estudiante asume temporalmente el rol de un especialista en Red Team y Blue Team, y este rol exige no sólo capacidad técnica, sino también criterio ético y conocimiento normativo.

Reflexión ética final sobre el uso de capacidades ofensivas

Finalmente, el laboratorio demuestra que las mismas herramientas que pueden ser empleadas para fortalecer la seguridad —como Nmap, Metasploit o técnicas de pivoting— pueden causar daños significativos si se utilizan sin autorización o sin controles adecuados (NIST, 2012). La formación en ciberseguridad no puede limitarse a la dimensión técnica; debe incluir una reflexión constante sobre:

- El impacto de los ataques en la vida real.
- El potencial daño a organizaciones y personas.
- La responsabilidad de quienes poseen las habilidades para realizar este tipo de acciones.

Integrar las dimensiones ética, legal y normativa dentro del informe final permite entregar no solo un resultado técnico sólido, sino también un documento maduro, alineado con las expectativas profesionales de la industria y con el enfoque académico de la Universidad Nacional Abierta y a Distancia.

Análisis de impacto y riesgo del compromiso técnico

El ejercicio de Red Team permitió comprometer completamente la infraestructura simulada, iniciando desde un servicio vulnerable expuesto en HOST-A y extendiéndose hasta el control total de HOST-B (NIST, 2020). Este conjunto de acciones no solo demuestra la efectividad técnica del ataque, sino que también permite analizar su impacto operativo, su criticidad y las consecuencias que un evento similar podría tener en un entorno corporativo real.

Desde una perspectiva de gestión de riesgos, cada fase del ataque representa una vulnerabilidad explotada, una falla en los controles de seguridad y un riesgo materializado. El análisis que se presenta a continuación se construye bajo los lineamientos del NIST SP 800-30, la ISO/IEC 27005, el NIST Cybersecurity Framework (CSF) y el modelo de amenazas MITRE ATT&CK. De esta forma, se articula una visión integral que combina lo técnico con una lectura estratégica del riesgo organizacional.

Impacto del compromiso inicial de HOST-A

El acceso inicial mediante la explotación de Rejetto HFS 2.3 permitió al Red Team obtener control remoto del sistema con privilegios suficientes para ejecutar comandos, enumerar el entorno y manipular recursos internos (SecureNova Labs, 2025). En un ambiente corporativo real, esta fase equivaldría a una violación de la barrera perimetral, constituyendo la materialización de:

- Pérdida de confidencialidad: el atacante logra leer e interceptar información sensible.
- Pérdida de integridad: el atacante puede modificar archivos, servicios, usuarios o configuraciones.
- Pérdida de disponibilidad: comprometen la capacidad operativa si deciden afectar servicios críticos.

El modelo CIA (Confidencialidad, Integridad y Disponibilidad) se ve afectado desde el primer minuto, incluso sin que existan aún acciones destructivas.

Desde MITRE ATT&CK, esta fase se asocia a:

- T1190 – Exploit Public-Facing Application
- TA0001 – Initial Access

Impacto del pivoteo y descubrimiento de la red interna

Tras comprometer HOST-A, el atacante logró descubrir la existencia de la red 10.0.2.x, la cual no era accesible desde el exterior. La capacidad de pivotar hacia nuevos segmentos representa un riesgo crítico, porque significa que:

- La segmentación de red no está adecuadamente protegida.
- No existen controles para monitorear rutas anómalas.
- El atacante puede moverse lateralmente sin restricciones.

En términos de riesgo técnico y operativo, el movimiento lateral tiene un impacto directo

- Robo de información alojada en sistemas internos.
- Compromiso de estaciones de trabajo adicionales.
- Escalada hacia servidores críticos (AD, bases de datos, aplicaciones internas).
- Propagación de malware o ransomware dentro de la red.

Dentro de ATT&CK, estas acciones corresponden a:

- TA0007 – Discovery
- TA0008 – Lateral Movement
- T1021 – Remote Services
- T1080 – Command Execution via Pivoting

Desde la perspectiva de negocio, el movimiento lateral de un atacante representa uno de los peores escenarios, ya que permite pasar de un incidente aislado a un ataque generalizado.

Impacto del compromiso total de HOST-B

HOST-B representaba un sistema ubicado en la red interna, sin relación de exposición directa al exterior (SecureNova Labs, 2025). El hecho de que el atacante lograra:

- Acceder al sistema

- Crear un usuario administrativo
- Manipular el grupo de administradores locales
- Mantener una sesión operativa

pone en evidencia que la empresa (simulada) no contaba con:

- Controles de autenticación robustos
- Políticas de monitoreo de creación de usuarios
- Alertas ante cambios de permisos privilegiados
- Registros protegidos o auditados de eventos críticos

Desde la perspectiva de ciberseguridad, el compromiso de HOST-B implica:

- Acceso total a datos internos
- Control total sobre una máquina de la red interna
- Capacidad de instalar malware, ejecutar herramientas, modificar archivos
- Riesgo crítico de continuidad del negocio

Este impacto constituye una violación grave y directa a los principios del SGSI establecidos en ISO/IEC 27001.

Impacto de la limpieza de huellas y evasión de auditorías

La eliminación de logs en Windows (eventos de seguridad, sistema y aplicación), así como la eliminación de la cuenta creada, representa un escenario crítico para cualquier organización. Esta fase evidencia el riesgo de:

- Pérdida total de trazabilidad
- Imposibilidad de reconstruir el incidente
- Evasión de auditorías internas y externas
- Falsos negativos en el SOC

En entornos reales, la evasión de registros es una técnica utilizada por grupos APT y ransomware antes de cifrar o exfiltrar datos. Desde ATT&CK:

- TA0005 – Defense Evasion
- T1070 – Clear Windows Event Logs

Impacto general del ataque a nivel organizacional

La sumatoria de las fases del ejercicio evidencia un escenario de **compromiso completo** de la infraestructura. Aunque el laboratorio es un entorno controlado, este resultado permite inferir el alto impacto que un ataque real podría tener sobre:

- La operación del negocio
- La continuidad del servicio
- La confidencialidad de la información
- La reputación de la organización
- El cumplimiento normativo y legal
- La relación con clientes, proveedores y entes reguladores

Si este ataque ocurriera en una empresa real, implicaría:

- Parada operacional de varios días
- Riesgo de extorsión o ransomware
- Pérdida de confianza de clientes
- Posibles investigaciones judiciales
- Multas por incumplimiento normativo

Evaluación del riesgo total

Usando una matriz de probabilidad vs impacto, el ataque ejecutado se clasifica como:

- Probabilidad: Alta (el servicio era vulnerable)

- Impacto: Crítico (compromiso total de la red interna)
- Nivel de riesgo: Extremo

Este análisis justifica la importancia de:

- Actualizar servicios expuestos
- Configurar políticas de monitoreo
- Implementar controles de acceso
- Mantener un SGSI actualizado
- Realizar pruebas de seguridad periódicas

Respuesta avanzada del Blue Team frente al ataque

Aunque el laboratorio se diseñó principalmente para evaluar la capacidad ofensiva del Red Team, este mismo escenario permite realizar un análisis exhaustivo sobre la eficacia que habría tenido un Blue Team real para detectar, contener y responder a las actividades ejecutadas durante el ejercicio. Este análisis defensivo, estructurado bajo marcos internacionales como NIST CSF, MITRE ATT&CK y MITRE, permite identificar brechas de visibilidad, fallos de monitoreo, ausencia de controles y oportunidades de mejora en los procesos de seguridad operativa (MITRE, 2020).

El objetivo principal del Blue Team es detectar el ataque lo más temprano posible, contenerlo antes de que se expanda y generar un análisis forense que permita comprender el alcance del compromiso. A continuación, se presenta un abordaje avanzado que evalúa cómo un SOC maduro habría enfrentado este ataque.

Visibilidad y monitoreo del entorno: capacidades mínimas requeridas

Para que un Blue Team detecte actividades maliciosas en los hosts del laboratorio, es indispensable que exista una infraestructura mínima de monitoreo, incluyendo:

- Event Viewer habilitado y con logs sin depurar (seguridad, sistema, aplicación).
- Auditoría avanzada de Windows activada.
- Reglas de auditoría para creación de cuentas, inicios de sesión, cambios en grupos locales.
- Solución EDR (Endpoint Detection and Response) capaz de monitorear procesos y conexiones.
- SIEM configurado con correlación de eventos (Splunk, QRadar, Elastic, etc.).
- Reglas Sigma o detecciones personalizadas para TTPs comunes.

El escenario del laboratorio evidenció que ninguno de estos controles estaba habilitado, lo que permitió al adversario llevar a cabo el ataque sin generar alertas visibles.

Detección del reconocimiento y actividad de escaneo

El Red Team realizó escaneos activos utilizando Nmap. En un entorno real, estos escaneos habrían generado tráfico anómalo identificable por el Blue Team a través de:

✓ Registros de firewall:

- Conexiones múltiples en un corto intervalo.
- Paquetes SYN consecutivos hacia puertos cerrados.

✓ Eventos de red:

- Trazas de escaneo horizontal detectado como “port scanning behaviour”.

✓ Alertas basadas en firmas o comportamiento:

- “Host scanning detected”
- “Service enumeration anomaly”

✓ Controles MITRE D3FEND aplicables:

- D3-NCP: Network Connection Pattern Analysis

- D3-NTC: Network Traffic Correlation

Detección de la explotación del servicio vulnerable Rejetto HFS

Durante la explotación HFS, Metasploit envió una petición HTTP especialmente construida. Un sistema defensivo habría podido detectar:

✓ Comportamiento anómalo en el servidor

- Procesos inesperados iniciados por HFS.exe
- Creación de conexiones reversas inusuales

✓ Alertas EDR

Un EDR habría detectado:

- Ejecución de código no firmado
- Payload de Meterpreter en memoria
- Conexiones reversas a puertos no autorizados
- Comandos ejecutados desde cmd.exe o PowerShell

Esto se relaciona con:

- T1059 – Command and Scripting Interpreter
- T1105 – Ingress Tool Transfer

Detección del movimiento lateral hacia HOST-B

El Blue Team debería ser capaz de detectar:

✓ Nuevas rutas internas

- "Autoroute" habría generado tráfico anómalo entre 192.168.1.x → 10.0.2.x

✓ Escaneos internos

- Consultas ICMP, SMB y RDP desde HOST-A hacia HOST-B

✓ Conexiones entre hosts que normalmente no se comunican

Esto es D3FEND:

- D3-SCA: Subnet and Host Communication Analysis

✓ **Eventos Windows que deberían activar alertas T00123**

Detección de la creación del usuario malicioso en HOST-B

La creación del usuario "john.acosta" y su elevación al grupo Administradores debería activar servicios críticos.

Un SOC bien configurado tiene reglas de correlación obligatorias sobre estos eventos, ya que son signos claros de escalación de privilegios (ATT&CK: T1068).

Detección de la limpieza de huellas

Cuando el atacante ejecutó:

- wevtutil cl security
- wevtutil cl system
- wevtutil cl application

Un SOC real habría recibido una alerta inmediata por:

✓ Eliminación de logs de seguridad

✓ "Event Clearing Behavior"

✓ Cambios inesperados en auditoría

IDS/EDR lo relaciona con:

- T1070 – Clear Windows Event Logs

Este evento debe activar:

- Alerta crítica
- Ticket inmediato
- Escalamiento a equipos forenses

Correlación general del ataque en un SIEM real

Un SIEM moderno correlacionaría:

1. Escaneo inicial de puertos
2. Explotación RCE en HFS
3. Conexión reversa desde HOST-A → atacante
4. Descubrimiento de red y pivoting
5. Movimiento lateral hacia HOST-B
6. Creación de usuario y escalación
7. Limpieza de registros

La correlación genera un incidente de severidad crítica:

ATAQUE AVANZADO – Compromiso total de 2 hosts internos.

Vector inicial: Exploit HFS 2.3

Evidencias: Escaneo, RCE, movimiento lateral, creación de usuario, limpieza de logs.

Aplicación del ciclo NIST CSF desde el Blue Team

✓ Detect

- Ningún sistema detectó el ataque → falla crítica

✓ Respond

El Blue Team debería:

1. Contener la actividad (aislar HOST-A)
2. Cortar conexiones reversas
3. Resetear credenciales
4. Revocar sesiones activas
5. Tomar evidencias forenses

6. Inhabilitar túneles (autoroute, portfwd)

✓ Recover

Debería:

- Restaurar HOST-A desde backup
- Cambiar claves del dominio
- Revisar logs de red
- Endurecer servicios expuestos

Conclusión defensiva

Si este ataque ocurriera en una red real, un Blue Team maduro habría detectado múltiples señales, especialmente:

- La explotación HFS
- La creación del usuario malicioso
- La limpieza de logs
- El movimiento lateral inesperado
- La ejecución de procesos anómalos

La falta de detecciones demuestra por qué la defensa debe ser:

- Proactiva
- Basada en comportamiento
- Integrada con SIEM/EDR
- Totalmente auditada

Recomendaciones

Tras una evaluación exhaustiva del ejercicio, se derivaron muchas recomendaciones, centrándose en aumentar la postura de seguridad de la organización y los procesos operativos para garantizar que incidentes como este puedan ser prevenidos, identificados y gestionados de manera oportuna. Basadas en los hallazgos de las diferentes fases del ciclo del incidente, y con referencia a los buenos fundamentos de ciberseguridad y el marco regulatorio internacional,

Se generan estas recomendaciones. Esto requiere un enfoque sistemático para la gestión de vulnerabilidades, así como escaneos regulares, priorización basada en riesgos y aplicación de parches. El aprovechamiento del servicio HFS 2.3 hizo evidente los riesgos inherentes de un sistema obsoleto y la necesidad de implementar una política de actualizaciones continuas y reemplazar sistemas que no están respaldados por el entorno de seguridad actual.

En una nota relacionada, se recomienda mejorar la segmentación y el filtrado interno, ya que el movimiento lateral entre HOST-A y HOST-B fue desenfrenado e imperceptible. Si el diseño de la red se basara en conceptos de Zero Trust, las listas de control de acceso (ACL), la microsegmentación y los cortafuegos internos reducirían en gran medida la superficie de ataque para el adversario y su capacidad para atravesar la infraestructura.

Sin embargo, implementar o mejorar significativamente un SIEM a través del monitoreo y la correlación de eventos también es esencial. Eventos como la creación de cuentas, la ejecución remota de comandos y la manipulación de privilegios deberían generar alertas de alta criticidad. Para tales incidentes, la visibilidad y la capacidad de detección temprana son un elemento clave en la remediación exitosa, particularmente en entornos donde se pueden usar varios vectores al mismo tiempo.

Asimismo, un segundo punto importante es la necesidad de fortalecer los controles de gestión de identidad y acceso (IAM). La escalada de privilegios de cuentas no autorizadas y la creación demostraron la ausencia de cualquier sistema de supervisión o autorización. También minimizaría la oportunidad de que credenciales comprometidas o la creación de actores maliciosos sean aprovechadas mediante cuentas maliciosas si implementamos políticas de privilegio mínimo, MFA (autenticación multifactor) y revisión programada de cuentas privilegiadas.

También es esencial fomentar la implementación de soluciones de protección de endpoints (EDR). Permiten la detección de anomalías en la ejecución afectada por malware, transferencias de cargas útiles, manipulación de registros o actividad sospechosa que escaparía a la detección en software antivirus más convencional. Un EDR de última generación, que esté integrado con políticas SIEM, dará a las empresas la capacidad de responder a actividades maliciosas con considerablemente más prontitud que una solución antivirus tradicional. A nivel organizacional,

las políticas internas deben fortalecerse con la adopción de marcos de estándares de seguridad (ISO/IEC 27001:2022) y aumentarse con controles de endurecimiento basados en los Benchmarks de CIS. Hará que las configuraciones sean uniformes, definirá roles claramente definidos y establecerá una mentalidad de seguridad que abarque todas las categorías de roles en todos los niveles de la organización. Los hallazgos también refuerzan la importancia de la gestión cooperativa e interdisciplinaria de la seguridad.

El control y la contención de incidentes no pueden ser únicamente la experiencia de los equipos técnicos, sino que involucra la participación de los ejecutivos organizacionales, el personal, los profesionales regulatorios y la academia. Construir resiliencia ante nuevas

amenazas y apoyar la seguridad, sostenibilidad y adaptabilidad (al abordar el entorno actual) dependerá de la colaboración, la capacitación continua y la alineación estratégica.

Evidencias de Sustentación

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

Video de sustentación del informe final:

https://www.youtube.com/watch?v=OXnIrY0RkV4

Conclusiones

El ejercicio desarrollado dentro del entorno de SecureNova Labs permitió comprender, de manera integral, la dinámica completa de un incidente de ciberseguridad, desde la perspectiva ofensiva del Red Team hasta las actividades de detección, contención y recuperación propias del Blue Team. Esta experiencia demostró que la seguridad informática no depende únicamente de herramientas o configuraciones aisladas, sino de la interacción entre procesos, controles, monitoreo continuo y capacidad de respuesta organizada frente a amenazas reales.

El análisis evidenció que la explotación inicial no fue resultado de una vulnerabilidad única, sino de una combinación de factores como software desactualizado, configuraciones débiles, ausencia de controles de segmentación y falta de monitoreo. Estos elementos, cuando se presentan simultáneamente, permiten que un atacante avance con rapidez desde la intrusión inicial hasta el control total de los activos críticos del entorno. De esta forma, el laboratorio expuso la importancia de adoptar una visión preventiva y proactiva de la seguridad, donde el fortalecimiento de la infraestructura debe ser continuo y basado en riesgos.

Asimismo, las actividades ofensivas demostraron que el ciclo de un ataque real implica reconocimiento, explotación, movimiento lateral, escalamiento de privilegios, persistencia y eliminación de huellas, procesos que requieren no solo habilidades técnicas, sino también pensamiento estratégico y capacidad analítica. Esta aproximación permitió validar que la metodología del Red Team no busca únicamente comprometer sistemas, sino identificar vulnerabilidades estructurales que podrían representar riesgos significativos para una organización en un escenario real.

Desde la perspectiva defensiva, el análisis reveló la necesidad urgente de mejorar los procesos de detección y respuesta, la correlación de eventos mediante SIEM y la implementación de controles como EDR, MFA, gestión de privilegios mínimos y políticas estrictas de auditoría. La ausencia de estos mecanismos facilitó la operación del atacante y permitió que las acciones ejecutadas pasaran inadvertidas para el hipotético Blue Team. Esto refuerza la importancia de contar con equipos de monitoreo bien entrenados, así como con procedimientos documentados y alineados con marcos como NIST SP 800-61 e ISO/IEC 27001.

Otro elemento fundamental corresponde a la dimensión ética y normativa. El ejercicio se desarrolló bajo principios de responsabilidad profesional, respeto por las buenas prácticas del hacking ético y cumplimiento de la Ley 1581 de 2012 y normativas internacionales. Esto reafirma que las operaciones ofensivas deben ser siempre controladas, autorizadas y ejecutadas con parámetros claros que eviten daños a sistemas productivos y garanticen la integridad del entorno académico.

En síntesis, el ejercicio permitió demostrar que la ciberseguridad exige un enfoque integral donde convergen técnicas ofensivas, capacidades defensivas, análisis normativo, buenas prácticas organizacionales y cultura de seguridad. Solo mediante la articulación armónica de estos componentes es posible construir entornos digitales resilientes, capaces de enfrentar amenazas avanzadas y adaptarse a los desafíos propios de la era digital. La experiencia adquirida a través de este laboratorio constituye una base sólida para seguir profundizando en la formación profesional, fortalecer las competencias técnicas y contribuir al desarrollo de mejores prácticas dentro del campo de la seguridad informática.

Referencias Bibliográficas

Centro Criptológico Nacional. (2022). *Guía de seguridad CCN-STIC 817: Gestión de incidentes de ciberseguridad*. https://www.ccn-cert.cni.es

CIS Center for Internet Security. (2022). *CIS Controls v8*. Center for Internet Security. https://www.cisecurity.org

Congreso de Colombia. (2009). *Ley 1273. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Instituto Nacional de Ciberseguridad (INCIBE). (2021). *Guía de respuesta ante incidentes de seguridad*. https://www.incibe.es

ISO. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Organización Internacional de Normalización.

ISO. (2022). *ISO/IEC 27002:2022 – Code of practice for information security controls*. Organización Internacional de Normalización.

Microsoft. (2023). *Windows security auditing and monitoring documentation*. Microsoft Corporation. https://learn.microsoft.com

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). *Guía de gestión de incidentes de seguridad digital*. Gobierno de Colombia.

MITRE Corporation. (2020). *MITRE ATT&CK® knowledge base*. MITRE. https://attack.mitre.org

National Institute of Standards and Technology. (2012). *NIST SP 800-61 Revision 2: Computer Security Incident Handling Guide*. U.S. Department of Commerce. https://csrc.nist.gov

National Institute of Standards and Technology. (2020). *NIST SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*. U.S. Department of Commerce.

Sánchez, J., & Rojas, F. (2020). Metodologías para el análisis de incidentes de seguridad informática. *Revista Colombiana de Tecnologías de la Información*, 12(3), 45–58. https://sedici.unlp.edu.ar/bitstream/handle/10915/77276/Documento_completo.pdf?sequence=1

SANS Institute. (2021). *Incident Handler's Handbook*. SANS Institute. https://www.sans.org

SecureNova Labs. (2025). *Escenario de prácticas simuladas Red Team & Blue Team*. Material académico interno.

Rapid7. (2023). *Vulnerability management best practices*. Rapid 7 Documentation. https://www.rapid7.com

Apéndices

Apéndice A

Resultado de revisión en Turnitin

El presente apéndice contiene el reporte oficial de similitud generado por Turnitin, requerido por la Universidad Nacional Abierta y a Distancia (UNAD) como evidencia de originalidad del documento titulado

Informe Técnico Final – Seminario Especializado Red Team & Blue Team – Etapa 5.

El análisis fue realizado sobre la versión final del informe, conforme a las orientaciones del tutor, evitando múltiples cargas que pudieran aumentar artificialmente el porcentaje de similitud. Este reporte respalda la integridad académica del trabajo y certifica el cumplimiento de las normas institucionales.

A continuación, se presenta el documento correspondiente: