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

Beatriz Lorena Duarte Burgos

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

Dedico este trabajo, en primer lugar, a mí misma, por la perseverancia, el compromiso y la disciplina demostrados a lo largo de este proceso académico. Cada desafío enfrentado durante esta especialización representó una oportunidad de crecimiento personal y profesional, reafirmando la importancia de la constancia para alcanzar las metas propuestas.

A mi familia, por su apoyo incondicional, comprensión y acompañamiento durante esta etapa. Su confianza, paciencia y motivación fueron fundamentales para superar las dificultades y mantener el entusiasmo necesario para culminar este importante logro.

De manera especial, dedico también este trabajo a mi compañero de cuatro patas, cuya compañía silenciosa estuvo presente durante largas jornadas de estudio, lectura y desarrollo de actividades. Su presencia constante brindó tranquilidad y equilibrio en los momentos de mayor exigencia académica.

Finalmente, dedico este logro a todas las personas que, de una u otra forma, contribuyeron a mi formación y crecimiento, motivándome a continuar aprendiendo y fortaleciendo mis conocimientos en el campo de la Seguridad Informática.

Agradecimientos

Expreso mi sincero agradecimiento a la Universidad Nacional Abierta y a Distancia (UNAD) por brindar las oportunidades, recursos y espacios académicos que hicieron posible el desarrollo de esta especialización y el fortalecimiento de mis competencias profesionales en el área de la Seguridad Informática.

Agradezco de manera especial al docente Eduvin Trigos Sánchez, director del Seminario Red Team & Blue Team, por su orientación, acompañamiento y valiosos aportes durante el desarrollo de este proceso académico. Su experiencia y retroalimentación contribuyeron significativamente a la consolidación de los conocimientos adquiridos y a la elaboración de este trabajo.

Así mismo, expreso mi reconocimiento a la educación pública y de calidad, que permite a miles de personas acceder a oportunidades de formación y crecimiento profesional. Gracias a este modelo educativo fue posible continuar fortaleciendo mis conocimientos y avanzar en el cumplimiento de una importante meta académica y personal.

A mi familia, gracias por su apoyo incondicional, comprensión y motivación constante durante este camino. Su confianza y acompañamiento fueron fundamentales para superar los retos presentados y culminar satisfactoriamente esta etapa de formación.

Finalmente, agradezco a todas las personas que, de una u otra manera, aportaron a mi crecimiento personal y profesional, acompañándome durante este proceso y motivándome a seguir aprendiendo y construyendo nuevos desafíos.

Resumen

La ciberseguridad representa un componente estratégico para las organizaciones debido al incremento de amenazas que afectan la confidencialidad, integridad y disponibilidad de la información. El presente desarrolla un análisis integral de operaciones Red Team y Blue Team aplicado al escenario propuesto por SecureNova Labs, con el fin de identificar vulnerabilidades, validar técnicas de explotación controlada y formular estrategias de contención y fortalecimiento de la seguridad informática. El desarrollo integra fundamentos conceptuales, metodologías de pentesting, herramientas ofensivas y defensivas, así como aspectos éticos y legales relacionados con delitos informáticos y protección de datos personales en Colombia. Posteriormente, se ejecuta un ejercicio práctico basado en la metodología PTES, permitiendo realizar actividades de reconocimiento, análisis de vulnerabilidades, explotación, escalamiento de privilegios y movimiento lateral dentro de un entorno controlado. Finalmente, se plantea un análisis de impacto y riesgos, complementado con estrategias Blue Team orientadas a la respuesta y contención de incidentes mediante hardening, controles CIS, monitoreo SIEM y medidas preventivas enfocadas en fortalecer la postura de seguridad organizacional.

***Palabras clave*:** Blue team, ciberseguridad, pentesting, red team, vulnerabilidades.

Abstract

Cybersecurity represents a strategic component for organizations due to the increasing number of threats affecting confidentiality, integrity, and availability of information. This work develops a comprehensive analysis of Red Team and Blue Team operations applied to the scenario proposed by SecureNova Labs, aiming to identify vulnerabilities, validate controlled exploitation techniques, and formulate containment and security strengthening strategies. The study integrates conceptual foundations, penetration testing methodologies, offensive and defensive tools, as well as ethical and legal aspects related to cybercrime and personal data protection in Colombia. Subsequently, a practical exercise based on the PTES methodology is carried out, including reconnaissance, vulnerability analysis, exploitation, privilege escalation, and lateral movement within a controlled environment. Finally, an impact and risk analysis is presented, complemented by Blue Team strategies focused on incident response and containment through hardening, CIS Controls, SIEM monitoring, and preventive measures aimed at strengthening the organizational security posture.

Keywords**:** Blue team, cybersecurity, penetration testing, red team, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Active Response:

Capacidad de algunas herramientas de seguridad para ejecutar acciones automáticas de contención frente a eventos maliciosos detectados, como bloqueo de direcciones IP, finalización de procesos o aislamiento de equipos comprometidos.

Blue Team:

Equipo encargado de la defensa de la infraestructura tecnológica de una organización mediante actividades de monitoreo, detección, análisis, respuesta y contención de incidentes de ciberseguridad.

Ciberseguridad:

Conjunto de prácticas, controles, tecnologías y procedimientos orientados a proteger sistemas, redes, aplicaciones y datos frente a amenazas, ataques o accesos no autorizados.

CVE (Common Vulnerabilities and Exposures):

Sistema de identificación pública de vulnerabilidades de seguridad informática que permite clasificar y documentar fallos conocidos presentes en software, sistemas o aplicaciones.

EDR (Endpoint Detection and Response):

Solución de seguridad enfocada en la detección, análisis y respuesta ante amenazas que afectan dispositivos finales como computadores y servidores.

Exploit:

Código, técnica o procedimiento utilizado para aprovechar una vulnerabilidad existente en un sistema con el objetivo de obtener acceso no autorizado o ejecutar acciones maliciosas.

Hardening:

Proceso de fortalecimiento de un sistema informático mediante la reducción de vulnerabilidades, deshabilitación de servicios innecesarios y aplicación de configuraciones seguras.

Host:

Equipo o dispositivo conectado a una red que puede actuar como origen o destino de comunicaciones y servicios.

IOC (Indicator of Compromise):

Evidencia o señal que permite identificar que un sistema pudo haber sido comprometido por una amenaza o ataque informático.

Payload:

Componente de un exploit encargado de ejecutar una acción específica sobre el sistema comprometido, como establecer una conexión remota o ejecutar comandos.

Pentesting:

Proceso de pruebas de penetración controladas orientado a identificar y validar vulnerabilidades en sistemas, redes o aplicaciones mediante técnicas similares a las utilizadas por atacantes reales.

Pivoting:

Técnica de post-explotación que permite utilizar un sistema comprometido como punto de acceso para alcanzar otros equipos internos dentro de la red.

PTES (Penetration Testing Execution Standard):

Metodología de pruebas de penetración que establece fases y lineamientos para ejecutar ejercicios de pentesting de manera estructurada y controlada.

Red Team:

Equipo especializado en simular ataques reales contra una infraestructura tecnológica con el propósito de identificar vulnerabilidades y evaluar la capacidad defensiva de la organización.

SIEM (Security Information and Event Management):

Plataforma orientada a la recopilación, correlación y análisis de eventos de seguridad provenientes de diferentes dispositivos y sistemas dentro de una organización.

Vulnerabilidad:

Debilidad o fallo presente en un sistema, aplicación o configuración que puede ser aprovechado por un atacante para comprometer la seguridad de la información.

Introducción

Actualmente, las organizaciones enfrentan un incremento constante de amenazas cibernéticas que ponen en riesgo la seguridad de la información y la continuidad de sus operaciones. Debido a esto, la ciberseguridad se ha convertido en un elemento fundamental para la identificación, prevención y mitigación de vulnerabilidades dentro de las infraestructuras tecnológicas. En este contexto, los equipos Red Team y Blue Team cumplen un papel clave al permitir evaluar las capacidades ofensivas y defensivas de una organización frente a posibles ataques informáticos.

El presente trabajo desarrolla un análisis integral basado en el escenario propuesto por SecureNova Labs, abordando actividades relacionadas con pentesting, explotación controlada de vulnerabilidades, análisis de riesgos y estrategias de respuesta y contención de incidentes de seguridad. Así mismo, se integran aspectos éticos y legales relacionados con delitos informáticos y protección de datos personales en Colombia, permitiendo contextualizar el ejercicio desde una perspectiva técnica y profesional.

A lo largo del documento se presentan fundamentos conceptuales, evidencias técnicas, estrategias defensivas y medidas de fortalecimiento orientadas a mejorar la postura de seguridad de la infraestructura tecnológica. Finalmente, se plantean conclusiones y recomendaciones enfocadas en la prevención y mitigación de incidentes de ciberseguridad dentro de entornos organizacionales.

Justificación

El desarrollo del presente surge de la necesidad de comprender y fortalecer las capacidades ofensivas y defensivas relacionadas con la ciberseguridad dentro de los entornos organizacionales modernos, ya que actualmente, las organizaciones dependen ampliamente de infraestructuras tecnológicas para el almacenamiento, procesamiento y transmisión de información crítica, situación que ha incrementado considerablemente la exposición frente a amenazas cibernéticas, explotación de vulnerabilidades y ataques dirigidos contra sistemas informáticos.

De acuerdo con lo anterior, la implementación de estrategias Red Team y Blue Team se ha convertido en un componente fundamental para evaluar la postura de seguridad y mejorar los mecanismos de prevención, detección y respuesta ante incidentes informáticos. Así mismo, las pruebas de penetración y ejercicios controlados de simulación de ataques permiten identificar debilidades técnicas antes de que estas puedan ser aprovechadas por actores maliciosos.

Según IBM (s.f), las metodologías de pentesting contribuyen significativamente a la identificación de vulnerabilidades presentes en redes, aplicaciones y sistemas, permitiendo fortalecer la seguridad organizacional mediante procesos de evaluación continua. De igual manera, el uso de metodologías estructuradas como PTES facilita el desarrollo ordenado de actividades de reconocimiento, explotación y análisis de impacto dentro de escenarios controlados de ciberseguridad.

Por otra parte, este presente también resulta relevante debido a la importancia de integrar estrategias Blue Team orientadas a la respuesta, contención y mitigación de incidentes de seguridad informática, ya que de acuerdo con Cranford (2023), la colaboración entre equipos Red Team y Blue Team permite mejorar las capacidades defensivas de las organizaciones mediante ejercicios que simulan escenarios reales de ataque y fortalecen los procesos de

monitoreo y respuesta, por tanto, la aplicación de controles CIS, herramientas SIEM, hardening y mecanismos de monitoreo continuo representan elementos clave para reducir riesgos y fortalecer la protección de la infraestructura tecnológica.

Adicionalmente, el análisis desarrollado incorpora aspectos éticos y legales relacionados con delitos informáticos, protección de datos personales y responsabilidad profesional en actividades de ciberseguridad. Normativas como la Ley 1273 de 2009 y la Ley 1581 de 2012 establecen lineamientos fundamentales para la protección de la información y el tratamiento adecuado de datos personales en Colombia (Función Pública, 2009; Función Pública, 2012) razón por la cual resulta indispensable que los profesionales del área desarrollen competencias técnicas acompañadas de criterios éticos y normativos.

Finalmente, este informe permite consolidar los conocimientos adquiridos durante el seminario mediante la integración de fundamentos conceptuales, actividades prácticas, análisis de vulnerabilidades y estrategias de remediación aplicadas en el escenario propuesto por SecureNova Labs. Los resultados obtenidos pueden servir como referencia para futuros ejercicios académicos y profesionales relacionados con ciberseguridad ofensiva y defensiva, contribuyendo al fortalecimiento de buenas prácticas de seguridad dentro de entornos organizacionales.

Objetivos

Objetivo General

Analizar las estrategias ofensivas y defensivas implementadas en un escenario de ciberseguridad basado en operaciones Red Team y Blue Team, con el fin de identificar vulnerabilidades, evaluar riesgos y proponer medidas de contención y fortalecimiento de la seguridad informática en entornos organizacionales.

Objetivos Específicos

Identificar vulnerabilidades presentes en los sistemas y servicios del entorno de laboratorio mediante la aplicación de metodologías de pentesting, técnicas de reconocimiento y herramientas especializadas de ciberseguridad.

Analizar el impacto de la explotación de vulnerabilidades a través de actividades controladas de acceso, escalamiento de privilegios y movimiento lateral, permitiendo evidenciar los riesgos asociados a la seguridad de la infraestructura tecnológica.

Evaluar estrategias Blue Team orientadas a la detección, contención y mitigación de incidentes de ciberseguridad mediante la implementación de hardening, controles de seguridad, monitoreo y herramientas defensivas.

Relacionar los aspectos éticos y legales asociados a las operaciones de ciberseguridad, considerando la normativa colombiana sobre delitos informáticos, protección de datos personales y responsabilidad profesional en el desarrollo de actividades de pentesting y análisis de seguridad.

Fundamentos Conceptuales de Ciberseguridad

Ciberseguridad Ofensiva y Defensiva

La transformación digital ha permitido que las organizaciones integren tecnologías cada vez más avanzadas dentro de sus procesos operativos, administrativos y estratégicos. Sin embargo, este crecimiento tecnológico también ha incrementado la exposición frente a amenazas cibernéticas orientadas a comprometer la confidencialidad, integridad y disponibilidad de la información, por tanto, la ciberseguridad surge como un conjunto de prácticas, estrategias y mecanismos orientados a proteger los activos digitales frente a accesos no autorizados, explotación de vulnerabilidades y ataques informáticos.

Dentro de la ciberseguridad moderna, las estrategias ofensivas y defensivas desempeñan un papel fundamental para evaluar y fortalecer la postura de seguridad de las organizaciones, ya que según Cranford (2023), los ejercicios Red Team y Blue Team permiten simular escenarios reales de ataque y defensa con el propósito de identificar debilidades, validar controles de seguridad y mejorar las capacidades de detección y respuesta ante incidentes informáticos.

La integración de capacidades ofensivas y defensivas se ha convertido en una práctica ampliamente utilizada en organizaciones que buscan fortalecer sus mecanismos de protección frente a amenazas avanzadas. El enfoque Red Team se basa en la ejecución de actividades ofensivas controladas que simulan el comportamiento de un atacante real sobre una infraestructura tecnológica, su principal objetivo consiste en identificar vulnerabilidades, validar vectores de ataque y evidenciar posibles impactos derivados de la explotación de fallos de seguridad.

De acuerdo con IBM (s.f), este tipo de ejercicios permite evaluar la capacidad de resistencia de los sistemas frente a amenazas reales mediante técnicas de reconocimiento, análisis de vulnerabilidades, explotación y post-explotación. Así mismo, González (2024) señala

que los equipos Red Team desarrollan procesos orientados a reproducir escenarios de intrusión controlada con el fin de detectar debilidades que puedan comprometer la seguridad organizacional.

Entre las actividades más comunes desarrolladas por un equipo Red Team se encuentran el reconocimiento de infraestructura, identificación de servicios vulnerables, explotación de fallos de seguridad, escalamiento de privilegios y movimiento lateral dentro de la red.

Estas actividades permiten simular técnicas utilizadas por atacantes reales para comprometer sistemas y acceder a información sensible, por tanto, las pruebas de penetración o pentesting representan una de las metodologías más utilizadas para validar la seguridad de redes, aplicaciones y servicios tecnológicos mediante ataques controlados y autorizados.

Por otra parte, el enfoque Blue Team se encuentra orientado a la protección y defensa de la infraestructura tecnológica mediante actividades de monitoreo, análisis, contención, respuesta ante incidentes de seguridad informática y su objetivo principal consiste en detectar actividades maliciosas, reducir riesgos y fortalecer la capacidad defensiva de la organización frente a posibles amenazas.

De acuerdo con González (2024), los equipos Blue Team implementan mecanismos de vigilancia continua, correlación de eventos, análisis de registros y fortalecimiento de controles de seguridad con el propósito de prevenir y mitigar ataques cibernéticos.

Dentro de las funciones desarrolladas por un equipo Blue Team se destacan la implementación de controles de seguridad, monitoreo de eventos, análisis de indicadores de compromiso (IOC), gestión de vulnerabilidades y aplicación de procesos de hardening sobre sistemas y servicios críticos, así mismo, herramientas tecnológicas como SIEM, EDR y plataformas de monitoreo permiten fortalecer las capacidades de detección y respuesta ante incidentes de seguridad informática.

De acuerdo con lo indicado por Fortinet (s.f) quien define las soluciones EDR como mecanismos orientados a la detección y respuesta frente a amenazas que afectan dispositivos finales, mientras que las plataformas SIEM permiten centralizar y correlacionar eventos de seguridad provenientes de múltiples fuentes dentro de la infraestructura tecnológica.

En la actualidad, las organizaciones no solo requieren capacidades ofensivas o defensivas aisladas, sino estrategias integradas que permitan evaluar continuamente la efectividad de sus controles de seguridad. De acuerdo con Sehga & Thymianis (2023), la integración entre Red Team y Blue Team fortalece significativamente la preparación organizacional frente a ataques avanzados, permitiendo mejorar los procesos de detección temprana, respuesta y remediación de incidentes de ciberseguridad, lo cual, favorece la identificación de debilidades técnicas y la validación de mecanismos defensivos dentro de escenarios controlados y realistas.

Adicionalmente, el concepto de defensa activa ha tomado gran relevancia dentro de las estrategias modernas de ciberseguridad, esta se basa en la implementación de mecanismos capaces de detectar, analizar y responder de manera dinámica frente a actividades sospechosas o comportamientos maliciosos dentro de la infraestructura tecnológica. Su enfoque incorpora herramientas de monitoreo continuo, correlación de eventos, automatización de respuestas y mecanismos de inteligencia de amenazas que permiten reducir los tiempos de detección y contención frente a posibles ataques.

De acuerdo con lo anterior, los Security Operations Center (SOC) desempeñan un papel fundamental en la protección de las organizaciones, este corresponde a un centro especializado encargado del monitoreo continuo de eventos de seguridad, análisis de incidentes y coordinación de actividades de respuesta frente a amenazas cibernéticas. Según Palo Palo Alto Networks (s.f), los SOC integran herramientas SIEM, inteligencia de amenazas y capacidades analíticas

orientadas a identificar comportamientos anómalos y responder oportunamente ante incidentes de seguridad informática.

Finalmente, la integración de estrategias ofensivas y defensivas dentro de los procesos de ciberseguridad permite fortalecer la postura de seguridad organizacional mediante ejercicios de simulación, análisis de riesgos y validación de controles de protección. La articulación entre Red Team, Blue Team y mecanismos de defensa activa constituye un componente esencial para enfrentar amenazas cibernéticas cada vez más sofisticadas y proteger adecuadamente los activos tecnológicos y la información crítica de las

Metodologías de Pentesting

Las pruebas de penetración o pentesting constituyen uno de los procesos más utilizados dentro de la ciberseguridad ofensiva para identificar vulnerabilidades y evaluar el nivel de seguridad presente en infraestructuras tecnológicas, aplicaciones y redes corporativas, estos ejercicios permiten simular ataques controlados sobre sistemas autorizados con el propósito de detectar debilidades que puedan ser aprovechadas por actores maliciosos.

Según DragonSec (2025), el pentesting consiste en la ejecución planificada de técnicas de intrusión orientadas a descubrir vulnerabilidades antes de que puedan ser explotadas en escenarios reales de ataque.

Con el fin de garantizar resultados organizados, controlados y técnicamente estructurados, las pruebas de penetración suelen desarrollarse bajo metodologías reconocidas que establecen fases, procedimientos y lineamientos específicos para la ejecución de actividades ofensivas, estas metodologías permiten definir procesos claros de reconocimiento, análisis, explotación y documentación de hallazgos, facilitando la evaluación integral de la postura de seguridad de una organización.

Una de las metodologías más utilizadas dentro de los ejercicios de ciberseguridad ofensiva es PTES (Penetration Testing Execution Standard), la cual establece un marco estructurado para el desarrollo de pruebas de penetración mediante diferentes fases orientadas a la identificación y validación de vulnerabilidades. De acuerdo con Future Learning (s.f), PTES contempla etapas relacionadas con reconocimiento, recopilación de información, análisis de vulnerabilidades, explotación, post-explotación y generación de reportes técnicos, esta metodología busca garantizar que las actividades ofensivas sean ejecutadas de manera controlada, organizada y alineada con objetivos específicos de seguridad.

La fase de reconocimiento representa una de las etapas más importantes dentro del pentesting, ya que permite obtener información relacionada con la infraestructura objetivo, servicios activos, direcciones IP, puertos abiertos y tecnologías implementadas. Según López (2024), esta etapa facilita la identificación de posibles vectores de ataque y constituye la base para el desarrollo de actividades posteriores de análisis y explotación, durante esta fase suelen utilizarse herramientas de escaneo y enumeración orientadas a recopilar información técnica del entorno evaluado.

Posteriormente, se desarrolla la fase de análisis de vulnerabilidades, en la cual se identifican fallos de seguridad presentes en sistemas, aplicaciones o servicios expuestos dentro de la infraestructura tecnológica. Lozano (2023) afirma que esta etapa permite detectar debilidades que podrían comprometer la seguridad de la organización si son aprovechadas por atacantes, para ello, se emplean herramientas de análisis automatizado, revisión manual y validación de configuraciones inseguras con el propósito de determinar el nivel de exposición frente a amenazas cibernéticas.

Una vez identificadas las vulnerabilidades, se procede a la fase de explotación, cuyo objetivo consiste en validar técnicamente si las debilidades detectadas pueden ser aprovechadas

para obtener acceso no autorizado o comprometer sistemas. Según IBM (s.f), esta fase permite comprobar el impacto real de las vulnerabilidades identificadas y determinar las posibles consecuencias derivadas de un ataque exitoso. Dentro de este proceso se utilizan exploits, payloads y herramientas especializadas orientadas a reproducir escenarios reales de intrusión bajo condiciones controladas y autorizadas.

Posteriormente, la fase de post-explotación se enfoca en analizar el alcance del compromiso obtenido sobre la infraestructura tecnológica, en esta etapa se realizan actividades relacionadas con escalamiento de privilegios, movimiento lateral, persistencia y recopilación de información sensible dentro de la red comprometida. Hernández (2022) señala que esta fase resulta fundamental para comprender el impacto potencial de un ataque y evaluar hasta qué punto un atacante podría comprometer los activos críticos de una organización.

Otra metodología ampliamente reconocida dentro del ámbito de la ciberseguridad es OWASP, orientada principalmente a la evaluación de vulnerabilidades en aplicaciones web. Esta metodología proporciona lineamientos y buenas prácticas para identificar fallos de seguridad relacionados con autenticación, control de acceso, exposición de datos y validación de entradas. Según Hernández (2022) OWASP permite estructurar pruebas de seguridad enfocadas en aplicaciones web mediante procesos organizados de identificación y explotación de vulnerabilidades comunes presentes en entornos web.

Así mismo, OSSTMM (Open Source Security Testing Methodology Manual) representa una metodología orientada a la evaluación integral de seguridad mediante pruebas técnicas, análisis de procesos y validación de controles de protección, esta metodología busca establecer procedimientos estructurados para evaluar redes, sistemas, comunicaciones y entornos físicos desde una perspectiva ofensiva y defensiva. Su aplicación permite obtener resultados medibles

relacionados con el nivel de exposición y capacidad de protección de una organización frente a posibles amenazas (ISECOM, 2010).

En la actualidad, las metodologías de pentesting desempeñan un papel fundamental dentro de los procesos de gestión de vulnerabilidades y fortalecimiento de la seguridad organizacional, por tanto, la aplicación de marcos metodológicos como PTES, OWASP y OSSTMM permite desarrollar ejercicios de seguridad de manera controlada, ética y técnicamente organizada, contribuyendo a la identificación temprana de debilidades y a la implementación de estrategias de mitigación orientadas a reducir riesgos dentro de las infraestructuras tecnológicas.

Herramientas de Ciberseguridad

Las herramientas de ciberseguridad representan un componente fundamental dentro de los procesos de análisis, evaluación y fortalecimiento de la seguridad informática en las organizaciones, estas herramientas permiten ejecutar actividades relacionadas con reconocimiento, análisis de vulnerabilidades, explotación controlada, monitoreo y gestión de incidentes, facilitando la identificación de debilidades presentes en infraestructuras tecnológicas. Dentro de los ejercicios de pentesting y operaciones Red Team, el uso de herramientas especializadas resulta indispensable para desarrollar pruebas técnicas de manera organizada y eficiente.

Actualmente, existe una amplia variedad de herramientas orientadas a diferentes áreas de la ciberseguridad ofensiva y defensiva, dependiendo, algunas permiten identificar hosts activos y servicios expuestos, mientras que otras facilitan la detección de vulnerabilidades, explotación de fallos de seguridad y validación de riesgos asociados a sistemas comprometidos. Así mismo, plataformas de información pública como CVE y ExploitDB proporcionan repositorios actualizados de vulnerabilidades y exploits utilizados ampliamente dentro de los procesos de

análisis y gestión de riesgos. De acuerdo con este contexto, a continuación, se mencionan algunas de las herramientas más relevantes:

Nmap

Nmap (Network Mapper) es una de las herramientas de reconocimiento y escaneo de redes más utilizadas dentro del ámbito de la ciberseguridad. Su principal función consiste en identificar hosts activos, detectar puertos abiertos y recopilar información relacionada con servicios y versiones presentes dentro de una infraestructura tecnológica. Según Campus Internacional Ciberseguridad (s.f), Nmap permite obtener información detallada sobre dispositivos conectados a una red, facilitando la identificación de posibles vectores de ataque y debilidades de seguridad.

Dentro de los procesos de pentesting, Nmap es utilizado principalmente durante la fase de reconocimiento, permitiendo identificar servicios expuestos, sistemas operativos y configuraciones de red que podrían representar riesgos para la organización, por tanto, la información obtenida mediante esta herramienta constituye una base fundamental para las etapas posteriores de análisis de vulnerabilidades y explotación controlada. Así mismo, Nmap incorpora funciones avanzadas relacionadas con detección de versiones, identificación de sistemas operativos y ejecución de scripts orientados a la enumeración de servicios y validación de configuraciones inseguras, lo anterior, convierte a Nmap en una herramienta ampliamente utilizada tanto por equipos Red Team como Blue Team dentro de procesos de evaluación y monitoreo de seguridad.

OpenVAS

OpenVAS es una herramienta orientada al análisis automatizado de vulnerabilidades en sistemas, aplicaciones y servicios de red, su objetivo principal consiste en identificar debilidades de seguridad presentes en infraestructuras tecnológicas mediante procesos de escaneo y

validación automatizada. Según Ciberseguridad (s.f), OpenVAS permite detectar vulnerabilidades conocidas, configuraciones inseguras y servicios expuestos que podrían ser aprovechados por atacantes. Esta herramienta utiliza bases de datos actualizadas de vulnerabilidades para comparar configuraciones y versiones de software presentes en los sistemas evaluados y partir de este análisis, OpenVAS genera reportes técnicos que incluyen información relacionada con criticidad, nivel de riesgo y posibles medidas de remediación asociadas a las vulnerabilidades detectadas.

Dentro de los ejercicios de pentesting, OpenVAS resulta especialmente útil durante la fase de análisis de vulnerabilidades, ya que facilita la identificación temprana de fallos de seguridad presentes en la infraestructura objetivo y su capacidad para clasificar vulnerabilidades según niveles de criticidad permite priorizar procesos de remediación y fortalecimiento de la seguridad organizacional.

Metasploit

Metasploit es uno de los frameworks de explotación más reconocidos dentro del ámbito de la ciberseguridad ofensiva y las pruebas de penetración y su principal función consiste en facilitar la validación controlada de vulnerabilidades mediante el uso de exploits, payloads y módulos especializados orientados a simular ataques reales sobre sistemas autorizados. Según Ciberseguridad (s.f), Metasploit representa una herramienta fundamental para los procesos de pentesting debido a su capacidad para automatizar actividades relacionadas con explotación y post-explotación. Dentro de las funcionalidades de Metasploit se encuentra la posibilidad de ejecutar exploits asociados a vulnerabilidades conocidas, establecer sesiones remotas, realizar escalamiento de privilegios y ejecutar tareas de post-explotación sobre sistemas comprometidos, estas capacidades permiten evaluar el impacto real de las vulnerabilidades detectadas y comprender las posibles consecuencias derivadas de un ataque exitoso.

Metasploit también incorpora módulos auxiliares orientados a escaneo, enumeración y recopilación de información, permitiendo complementar las fases de reconocimiento y análisis de vulnerabilidades dentro de un ejercicio Red Team. Debido a su amplio uso dentro de la comunidad de ciberseguridad, esta herramienta se ha convertido en un referente para la validación técnica de fallos de seguridad en entornos controlados.

CVE

CVE (Common Vulnerabilities and Exposures) corresponde a un sistema de identificación pública de vulnerabilidades de seguridad informática utilizado internacionalmente para clasificar y documentar fallos presentes en software, sistemas y aplicaciones, de acuerdo con lo indicado por RedHat (2021), los identificadores CVE permiten estandarizar el registro y consulta de vulnerabilidades conocidas, facilitando el intercambio de información entre organizaciones, investigadores y fabricantes de tecnología. Cada vulnerabilidad registrada dentro de CVE recibe un identificador único que permite consultar información relacionada con el fallo de seguridad, productos afectados y posibles riesgos asociados, esta clasificación facilita los procesos de gestión de vulnerabilidades y remediación dentro de las organizaciones, permitiendo priorizar acciones correctivas según el nivel de criticidad de cada amenaza.

El uso de CVE resulta fundamental dentro de las actividades de pentesting y análisis de vulnerabilidades, ya que proporciona información técnica relacionada con debilidades conocidas que podrían ser aprovechadas por atacantes. Así mismo, plataformas como NIST y MITRE complementan esta información mediante bases de datos orientadas al análisis técnico y evaluación de impacto de vulnerabilidades registradas.

ExploitDB

ExploitDB es una base de datos pública orientada al almacenamiento y consulta de exploits asociados a vulnerabilidades conocidas en sistemas y aplicaciones, su objetivo principal

consiste en proporcionar información técnica y pruebas de concepto relacionadas con fallos de seguridad que pueden ser utilizados dentro de procesos de investigación y pruebas de penetración. Según Holm Security (2025), ExploitDB permite acceder a exploits desarrollados para validar vulnerabilidades presentes en diferentes tecnologías y servicios.

Dentro de los ejercicios de pentesting, ExploitDB representa una fuente importante de información para la identificación de posibles vectores de explotación asociados a vulnerabilidades conocidas, ya que los exploits disponibles en esta plataforma permiten validar técnicamente si un fallo de seguridad puede ser aprovechado dentro de un entorno controlado y autorizado. Así mismo, ExploitDB facilita actividades de investigación y análisis técnico relacionadas con vulnerabilidades críticas, contribuyendo a fortalecer los procesos de gestión de riesgos y remediación dentro de las organizaciones. Su integración con herramientas como Metasploit y plataformas de análisis de vulnerabilidades convierte a esta base de datos en un recurso ampliamente utilizado por profesionales de ciberseguridad ofensiva y defensiva.

Gestión de Vulnerabilidades

La gestión de vulnerabilidades es un proceso fundamental dentro de la ciberseguridad, ya que permite identificar, analizar y corregir debilidades presentes en sistemas, aplicaciones y servicios tecnológicos antes de que puedan ser aprovechadas por actores maliciosos, este proceso busca reducir la superficie de ataque y fortalecer la seguridad de la infraestructura tecnológica mediante actividades continuas de evaluación y remediación.

Uno de los principales mecanismos utilizados para la identificación de vulnerabilidades corresponde al sistema CVE (Common Vulnerabilities and Exposures), el cual permite clasificar y documentar fallos de seguridad conocidos mediante identificadores únicos estandarizados. Según Fortinet (s.f), este sistema facilita el intercambio de información técnica relacionada con vulnerabilidades presentes en software, sistemas operativos y aplicaciones, permitiendo a las

organizaciones identificar riesgos asociados a tecnologías específicas. De forma complementaria, plataformas como el National Vulnerability Database (NVD) proporcionan información relacionada con niveles de criticidad, vectores de ataque e impacto potencial de las vulnerabilidades registradas.

Dentro de este contexto, la explotación de vulnerabilidades hace referencia al aprovechamiento de un fallo de seguridad con el propósito de obtener acceso no autorizado, ejecutar código malicioso o comprometer la integridad de un sistema. Por esta razón, las organizaciones deben realizar procesos constantes de evaluación y análisis de riesgos que permitan determinar la probabilidad e impacto asociado a cada vulnerabilidad identificada. Así mismo, la criticidad de una vulnerabilidad depende de factores como facilidad de explotación, nivel de acceso obtenido y afectación potencial sobre la infraestructura tecnológica. Según RedHat (2021), la correcta clasificación de vulnerabilidades facilita la priorización de actividades de remediación y fortalecimiento de la seguridad organizacional.

Finalmente, la remediación corresponde al conjunto de acciones implementadas para corregir o mitigar vulnerabilidades detectadas dentro de un entorno tecnológico. De acuerdo con Randall (2026), este proceso puede incluir aplicación de parches, hardening, segmentación de redes, actualización de sistemas y fortalecimiento de controles de seguridad, por tanto, la gestión de vulnerabilidades representa un componente esencial para reducir riesgos y mejorar la capacidad de protección frente a amenazas cibernéticas cada vez más sofisticadas.

Hardening y Seguridad Defensiva

La seguridad defensiva comprende el conjunto de estrategias, controles y mecanismos orientados a prevenir, detectar y reducir el impacto de amenazas cibernéticas sobre la infraestructura tecnológica de una organización. Dentro de este enfoque, el hardening representa uno de los procesos más importantes para fortalecer la seguridad de sistemas, servicios y

dispositivos mediante configuraciones seguras y reducción de vulnerabilidades. Según Pandora FMS Team (2024), el hardening busca disminuir la superficie de ataque a través de la deshabilitación de servicios innecesarios, actualización de componentes y aplicación de configuraciones de seguridad adecuadas.

Así mismo, la implementación de controles de seguridad permite establecer medidas preventivas orientadas a proteger los activos tecnológicos frente a posibles ataques informáticos. En este contexto, los CIS Controls proporcionan un conjunto de buenas prácticas enfocadas en gestión de vulnerabilidades, control de accesos y protección de sistemas críticos dentro de las organizaciones (CIS, s.f). En la misma línea, las organizaciones requieren mecanismos de monitoreo que permitan identificar actividades sospechosas y eventos relacionados con incidentes de seguridad informática. Para ello, las plataformas SIEM facilitan la recopilación y análisis centralizado de registros y eventos provenientes de diferentes dispositivos y sistemas, contribuyendo a mejorar la capacidad de detección de amenazas (Fortinet, s.f). De manera complementaria, las soluciones EDR permiten monitorear y analizar comportamientos asociados a dispositivos finales con el propósito de identificar posibles actividades maliciosas dentro de la infraestructura tecnológica.

Marco Ético y Legal

Delitos Informáticos en Colombia

El crecimiento de las tecnologías de la información y la transformación digital han generado nuevos riesgos relacionados con el uso indebido de sistemas informáticos, acceso no autorizado a información y afectación de activos tecnológicos, debido a esto, Colombia ha desarrollado un marco normativo orientado a sancionar conductas que comprometen la seguridad de la información y los sistemas informáticos.

En primer lugar, una de las principales normas relacionadas con delitos informáticos corresponde a la Ley 1273 de 2009, la cual incorporó al Código Penal Colombiano el bien jurídico denominado “protección de la información y de los datos”, de acuerdo con Función Pública (2009), esta ley tipifica conductas relacionadas con acceso abusivo a sistemas informáticos, interceptación de datos, daño informático, uso de software malicioso y violación de datos personales. Así mismo, la Policia Nacional (2009) señala que esta normativa establece sanciones penales y económicas frente a actividades que afecten la confidencialidad, integridad y disponibilidad de la información. Dentro de los delitos contemplados por esta ley se encuentra el acceso abusivo a sistemas informáticos, el cual hace referencia al ingreso no autorizado a plataformas, redes o sistemas protegidos con el propósito de obtener información o ejecutar acciones indebidas sobre la infraestructura tecnológica, de igual manera, la interceptación de datos informáticos corresponde a la captura, monitoreo o acceso no autorizado a comunicaciones o información transmitida mediante medios digitales.

Por otra parte, la Ley 599 de 2000, correspondiente al Código Penal Colombiano, establece lineamientos relacionados con conductas punibles y responsabilidades jurídicas frente a diferentes tipos de delitos, esta normativa también contempla obligaciones relacionadas con el deber de denuncia frente a actividades ilícitas, aspecto especialmente relevante dentro del ámbito

de la ciberseguridad y el manejo de información sensible (Función Pública, 2000). Entendiéndose lo anterior, el marco legal colombiano busca proteger tanto los sistemas tecnológicos como los derechos asociados a la información y los datos personales, estableciendo mecanismos jurídicos orientados a prevenir, sancionar y controlar actividades relacionadas con delitos informáticos dentro de entornos digitales.

Protección de Datos Personales

La protección de datos personales constituye un componente fundamental dentro de la seguridad de la información, debido a la necesidad de garantizar la privacidad y el adecuado tratamiento de la información de los ciudadanos. En Colombia, una de las principales normas relacionadas con esta materia es la Ley 1581 de 2012, la cual establece disposiciones generales para la protección de datos personales y el ejercicio del derecho constitucional de Habeas Data. Según Función Pública (2012), esta ley reconoce el derecho que tienen las personas a conocer, actualizar y rectificar la información almacenada en bases de datos públicas o privadas y establece principios relacionados con legalidad, finalidad, libertad, confidencialidad y seguridad en el tratamiento de la información personal.

El Habeas Data corresponde al derecho que poseen los titulares de datos personales para controlar el uso de su información y solicitar correcciones, actualizaciones o eliminación cuando sea necesario, por tanto, las organizaciones que administran información personal deben implementar medidas orientadas a proteger la confidencialidad y seguridad de los datos recolectados.

Por otra parte, la Superintendencia de Industria y Comercio (SIC) actúa como autoridad encargada de la vigilancia y control del cumplimiento de la normativa relacionada con protección de datos personales en Colombia, de acuerdo con MinCIT (2012), las organizaciones deben establecer políticas y procedimientos adecuados para garantizar el correcto tratamiento de

la información y prevenir accesos no autorizados o usos indebidos de datos personales. En consecuencia, la protección de datos personales representa un elemento esencial dentro de los procesos de ciberseguridad organizacional, especialmente en entornos donde se almacena y procesa información sensible de usuarios, clientes o entidades.

Ética Profesional en Ciberseguridad

El ejercicio profesional en ciberseguridad no solo requiere competencias técnicas relacionadas con análisis de vulnerabilidades, pruebas de penetración y gestión de incidentes, sino también el cumplimiento de principios éticos orientados a garantizar el uso responsable de herramientas y conocimientos especializados, debido al impacto que pueden generar las actividades ofensivas sobre sistemas y datos sensibles, resulta indispensable que los profesionales actúen bajo criterios de legalidad, confidencialidad y responsabilidad profesional.

En Colombia, el COPNIA establece lineamientos éticos relacionados con el ejercicio responsable de las profesiones de ingeniería y áreas afines, según COPNIA (s.f), los profesionales deben actuar con honestidad, transparencia y responsabilidad frente al manejo de información y el desarrollo de actividades que puedan afectar a personas, organizaciones o infraestructuras tecnológicas. En el ámbito de la ciberseguridad, el deber ético implica ejecutar actividades de análisis y pruebas de penetración únicamente sobre sistemas autorizados y bajo condiciones previamente definidas, así mismo, la confidencialidad representa un principio fundamental debido a que los profesionales pueden tener acceso a información sensible durante auditorías, evaluaciones de seguridad o investigaciones relacionadas con incidentes informáticos.

De igual manera, los especialistas en ciberseguridad deben evitar el uso indebido de herramientas ofensivas o técnicas de intrusión con fines no autorizados, ya que este tipo de acciones podría generar consecuencias legales, operacionales y reputacionales para las organizaciones involucradas, por tanto, la ética profesional constituye un componente esencial

para garantizar el desarrollo responsable de actividades relacionadas con seguridad informática y protección de la información.

Análisis Ético del Caso SecureNova Labs

El caso planteado por SecureNova Labs presenta un escenario orientado al desarrollo de actividades de ciberseguridad ofensiva y defensiva dentro de un entorno organizacional simulado, permitiendo analizar aspectos técnicos, éticos y legales relacionados con la identificación de vulnerabilidades, explotación controlada de sistemas y aplicación de estrategias de contención. Este tipo de ejercicios resulta fundamental para fortalecer las capacidades de prevención y respuesta frente a amenazas informáticas; sin embargo, también implica responsabilidades asociadas al manejo adecuado de herramientas de seguridad y al cumplimiento de principios legales y éticos durante el desarrollo de las actividades.

Dentro del escenario propuesto se evidencian situaciones relacionadas con el acceso a información sensible, uso de herramientas de análisis ofensivo y posibles restricciones asociadas a la divulgación de actividades internas de la organización, por lo anterior, resulta necesario considerar que las actividades de pentesting y análisis de seguridad únicamente deben ejecutarse bajo autorización expresa y dentro de límites previamente establecidos, garantizando el respeto por la confidencialidad, integridad y disponibilidad de la información evaluada.

Así mismo, el caso permite reflexionar sobre los riesgos asociados al uso indebido de herramientas de ciberseguridad, ya que, tecnologías utilizadas para análisis de vulnerabilidades, explotación controlada o monitoreo pueden convertirse en mecanismos de afectación si son empleadas fuera de contextos autorizados o con fines diferentes a los establecidos dentro de los procesos de seguridad informática, por ello, los profesionales del área deben actuar bajo principios de responsabilidad, transparencia y confidencialidad durante el desarrollo de actividades técnicas relacionadas con sistemas y datos sensibles.

Por otra parte, el escenario también plantea implicaciones relacionadas con posibles cláusulas o acuerdos que podrían limitar el deber ético y legal de reportar actividades irregulares o ilícitas identificadas durante el ejercicio profesional, en Colombia, el marco normativo relacionado con delitos informáticos y responsabilidad profesional establece la importancia de actuar conforme a principios legales y éticos frente al manejo de información y conocimiento técnico especializado.

Así mismo, el análisis del caso evidencia la necesidad de que las organizaciones implementen políticas claras de seguridad, control de accesos y supervisión sobre el uso de herramientas de ciberseguridad, especialmente en entornos donde se realizan actividades ofensivas y defensivas de manera controlada, esto permite reducir riesgos asociados a abuso de privilegios, exposición de información sensible o utilización inadecuada de capacidades técnicas avanzadas.

Finalmente, el caso SecureNova Labs permite comprender la importancia de integrar criterios éticos, legales y profesionales dentro de los procesos de ciberseguridad organizacional. La correcta aplicación de principios de confidencialidad, responsabilidad y legalidad resulta indispensable para garantizar que las actividades de análisis, pentesting y respuesta a incidentes se desarrollen de manera segura, autorizada y alineada con la normativa vigente.

Metodología del Ejercicio

El escenario planteado por SecureNova Labs fue diseñado para desarrollar un ejercicio práctico orientado al análisis de operaciones Red Team y Blue Team dentro de un entorno controlado de ciberseguridad, a través de un laboratorio se buscó simular un contexto organizacional vulnerable frente a posibles amenazas informáticas, permitiendo aplicar técnicas de reconocimiento, análisis de vulnerabilidades, explotación controlada y estrategias de contención sobre diferentes sistemas conectados dentro de una red virtual.

El ejercicio práctico se enfocó en evaluar el impacto que puede generar la explotación de vulnerabilidades presentes en servicios y configuraciones inseguras, así como la importancia de implementar mecanismos defensivos orientados a fortalecer la seguridad de la infraestructura tecnológica. Para ello, se utilizaron herramientas especializadas de pentesting, análisis de vulnerabilidades y monitoreo, permitiendo integrar capacidades ofensivas y defensivas dentro de un mismo escenario de evaluación.

Así mismo, el laboratorio permitió recrear diferentes fases de un posible incidente de seguridad informática, incluyendo reconocimiento de infraestructura, identificación de servicios vulnerables, acceso inicial, escalamiento de privilegios y movimiento lateral entre sistemas comprometidos, lo cual facilitó el análisis técnico de riesgos asociados a vulnerabilidades explotables y la validación de estrategias de respuesta y fortalecimiento de la seguridad organizacional.

Por tanto, la metodología implementada dentro del escenario SecureNova Labs se desarrolló bajo principios de ejecución controlada, análisis técnico y evaluación estructurada de vulnerabilidades, permitiendo integrar conocimientos relacionados con pentesting, gestión de riesgos, seguridad defensiva y respuesta ante incidentes de ciberseguridad.

Descripción del Entorno de Laboratorio

Para el desarrollo del ejercicio práctico se implementó un entorno de laboratorio controlado orientado a la ejecución de actividades de ciberseguridad ofensiva y defensiva bajo condiciones seguras y autorizadas. Este entorno permitió simular escenarios reales de ataque y análisis de incidentes mediante la utilización de máquinas virtuales, herramientas de pentesting y configuraciones de red aisladas del entorno productivo.

La infraestructura utilizada fue implementada mediante Oracle VirtualBox, plataforma de virtualización que permitió la creación y administración de máquinas virtuales destinadas a las actividades del ejercicio, ya que el uso de entornos virtualizados facilita la simulación de ataques controlados y la validación de vulnerabilidades sin comprometer sistemas reales o infraestructuras externas.

Dentro del laboratorio se configuró una máquina atacante basada en Kali Linux o Parrot Security OS, distribuciones especializadas en ciberseguridad que incorporan herramientas orientadas a reconocimiento, análisis de vulnerabilidades, explotación y monitoreo de sistemas. Estas distribuciones son ampliamente utilizadas en procesos de pentesting debido a la integración de herramientas ofensivas y defensivas orientadas a pruebas de seguridad controladas.

Así mismo, se configuraron dos equipos objetivo-identificados como Host-A y Host-B, los cuales representaban sistemas vulnerables dentro del escenario propuesto por SecureNova Labs con la siguiente distribución:

Tabla 1

Distribución de equipos

Máquina	Rol	Sistema Operativo	Función
Kali/Parrot	Atacante	Linux	Pentesting

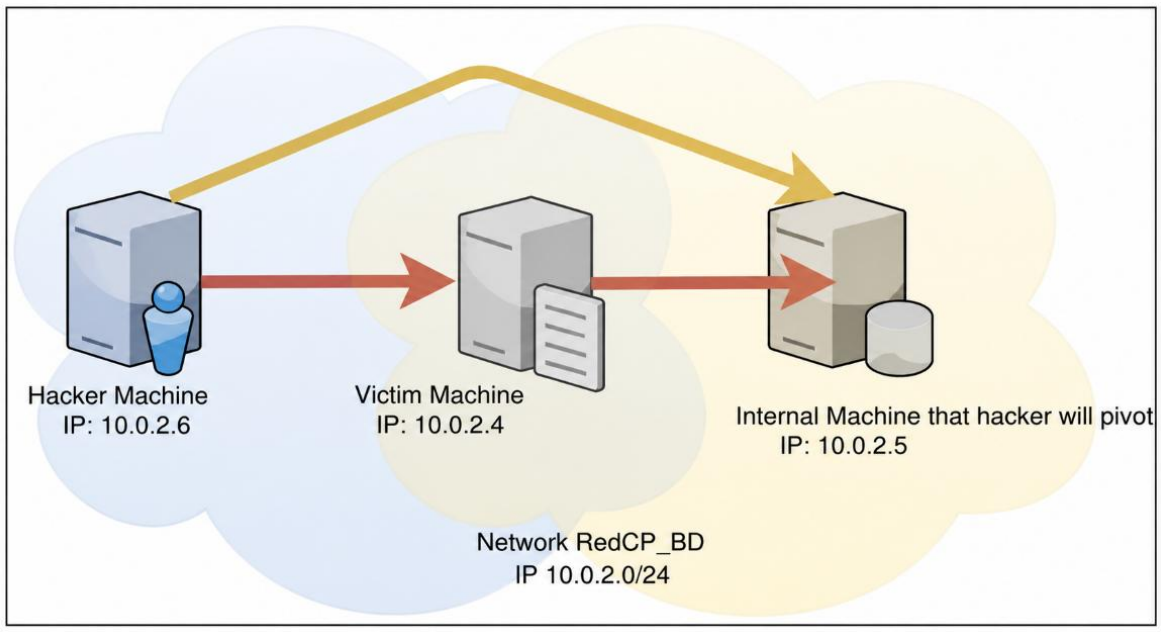
Host-A	Objetivo	Windows/Linux	Sistema vulnerable
Host-B	Objetivo	Windows/Linux	Movimiento lateral

Nota: Se presenta el resumen general de las máquinas virtuales utilizadas y su función dentro del laboratorio.

Estos hosts fueron utilizados para simular actividades relacionadas con reconocimiento, explotación de vulnerabilidades, escalamiento de privilegios y movimiento lateral dentro de la red virtual implementada para el ejercicio. La comunicación entre las máquinas virtuales se realizó mediante una red virtual interna configurada dentro de VirtualBox, permitiendo establecer conectividad controlada entre los diferentes dispositivos del laboratorio. Esta arquitectura facilitó la ejecución de pruebas de seguridad y análisis de tráfico dentro de un entorno aislado y seguro para el desarrollo del ejercicio práctico. De acuerdo con lo anterior se presenta en la Figura 1 la topología utilizada:

Figura 1

Topología de red



Nota: Se presenta la topología de red para el escenario de laboratorio. Tomado de Campus Virtual UNAD. (2026). *Guía para el desarrollo de componente práctico - Etapa 3 - Componente práctico.* https://campus146.unad.edu.co/ses55/mod/resource/view.php?id=2679

Arquitectura del Escenario

El entorno implementado para el ejercicio práctico estuvo compuesto por una arquitectura de red virtual orientada a simular un escenario organizacional básico con diferentes sistemas interconectados, lo que permitió desarrollar actividades de reconocimiento, análisis de vulnerabilidades, explotación controlada y movimiento lateral entre hosts comprometidos dentro de un entorno seguro y aislado.

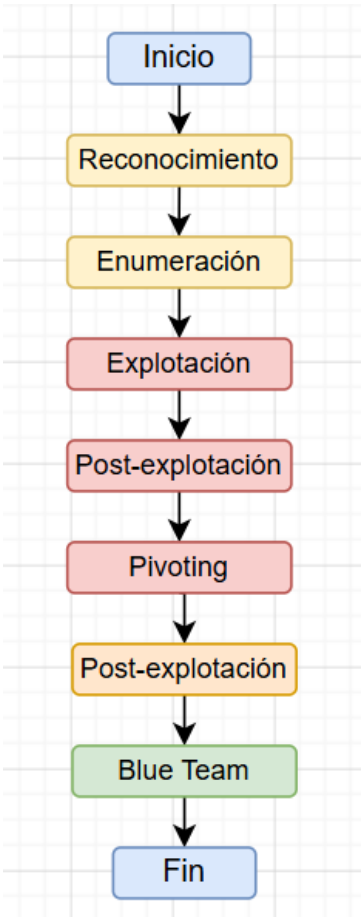
La topología del laboratorio estuvo conformada por una máquina atacante encargada de ejecutar actividades ofensivas y dos hosts vulnerables conectados mediante una red virtual interna. Esta arquitectura facilitó la simulación de diferentes etapas de un posible incidente de

ciberseguridad, permitiendo validar el impacto derivado de vulnerabilidades presentes en servicios expuestos y configuraciones inseguras.

El flujo general del ataque inició con actividades de reconocimiento y enumeración sobre Host-A, seguido de la identificación de vulnerabilidades asociadas a servicios activos dentro del sistema. Posteriormente, se ejecutaron procesos de explotación controlada y establecimiento de acceso remoto, permitiendo desarrollar actividades de post-explotación y movimiento lateral hacia otros dispositivos presentes en la red virtual, a continuación, se muestra el flujo mencionado en la Figura 2:

Figura 2

Flujo general del ataque



Nota: Se presentan la secuencia de acciones realizadas durante el ataque.

Metodología PTES Aplicada

Para el desarrollo del ejercicio práctico se implementó la metodología PTES (Penetration Testing Execution Standard), la cual establece fases estructuradas orientadas a la ejecución controlada de pruebas de penetración y análisis de seguridad informática (Future Learning, s.f). La aplicación de esta metodología permitió organizar las actividades ofensivas desarrolladas dentro del escenario SecureNova Labs y mantener una secuencia lógica durante el ejercicio.

La primera fase correspondió al reconocimiento, etapa orientada a la recopilación de información relacionada con la infraestructura objetivo mediante procesos de identificación de hosts activos, descubrimiento de servicios y análisis inicial de la superficie de ataque. Posteriormente, se desarrolló la fase de enumeración y análisis de vulnerabilidades, permitiendo identificar servicios vulnerables y configuraciones inseguras presentes en los hosts evaluados.

Una vez identificadas las vulnerabilidades, se ejecutó la fase de explotación mediante el uso de herramientas y exploits orientados a validar técnicamente los fallos de seguridad detectados. Esta etapa permitió obtener acceso controlado sobre sistemas vulnerables y evidenciar el impacto potencial derivado de un ataque exitoso.

Posteriormente, se realizaron actividades de post-explotación relacionadas con escalamiento de privilegios, recopilación de información y validación del alcance del compromiso obtenido sobre la infraestructura tecnológica. Finalmente, se ejecutaron actividades de pivoting o movimiento lateral con el propósito de utilizar sistemas comprometidos como punto de acceso hacia otros dispositivos dentro de la red virtual. A continuación, en la Tabla 2 se presenta el resumen de la aplicación de la metodología:

Tabla 2

Implementación de la metodología PTES

Fase PTES	Actividad realizada	Herramienta utilizada
Reconocimiento	Escaneo de red	Nmap
Enumeración	Identificación de servicios	Nmap/OpenVAS
Explotación	Ejecución de exploit	Metasploit
Post-explotación	Escalamiento de privilegios	Meterpreter
Pivoting	Movimiento lateral	Metasploit/Proxychains

Nota: Se presentan las actividades y herramientas utilizadas en cada etapa ejecutada.

Estrategias de Red Team

El ejercicio Red Team desarrollado en el escenario SecureNova Labs tuvo como propósito reproducir de manera controlada un posible incidente de seguridad informática, partiendo de la identificación de un sistema vulnerable hasta la demostración del impacto potencial derivado de su explotación. Para ello se aplicó la metodología PTES, permitiendo estructurar las actividades de reconocimiento, análisis de vulnerabilidades, explotación, post-explotación y movimiento lateral sobre una infraestructura virtual compuesta por dos sistemas Windows y una máquina atacante basada en Parrot OS.

El desarrollo del ejercicio permitió validar la vulnerabilidad CVE-2014-6287 (MITRE, 2014) presente en el servicio HTTP File Server (HFS) (ASEC, 2024), obtener acceso remoto sobre el sistema comprometido y analizar la posibilidad de propagación hacia otros activos de la red. Los resultados obtenidos constituyen evidencia técnica de cómo una vulnerabilidad conocida puede ser utilizada como punto de entrada para comprometer una infraestructura tecnológica y afectar la confidencialidad, integridad y disponibilidad de la información.

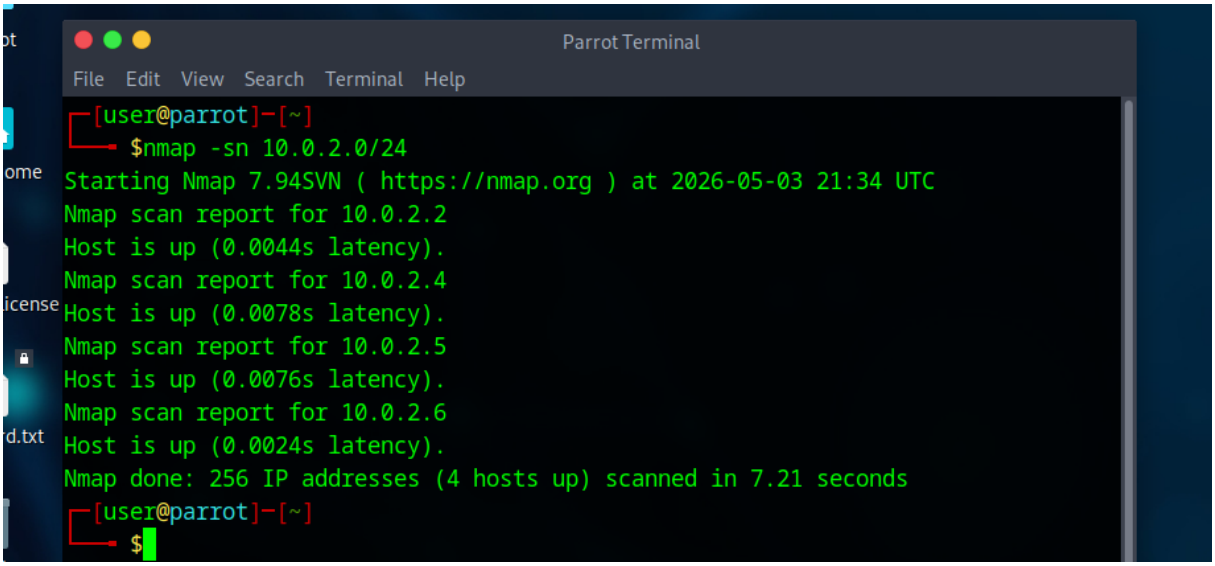
Reconocimiento y Descubrimiento

La fase de reconocimiento tuvo como objetivo identificar los activos presentes dentro de la red virtual y determinar posibles vectores de ataque asociados a los sistemas objetivo. Esta etapa constituye el punto de partida de cualquier ejercicio de pentesting, ya que permite obtener información relevante sobre la superficie de ataque antes de iniciar procesos de explotación.

Inicialmente se realizó un escaneo de descubrimiento utilizando Nmap sobre el segmento de red 10.0.2.0/24, permitiendo identificar los dispositivos activos dentro del entorno de laboratorio. Como resultado se detectaron tres equipos principales: la máquina atacante, Host-A y Host-B, los cuales forman parte del escenario planteado por SecureNova Labs:

Figura 3

Identificación de hosts activos dentro de la red virtual



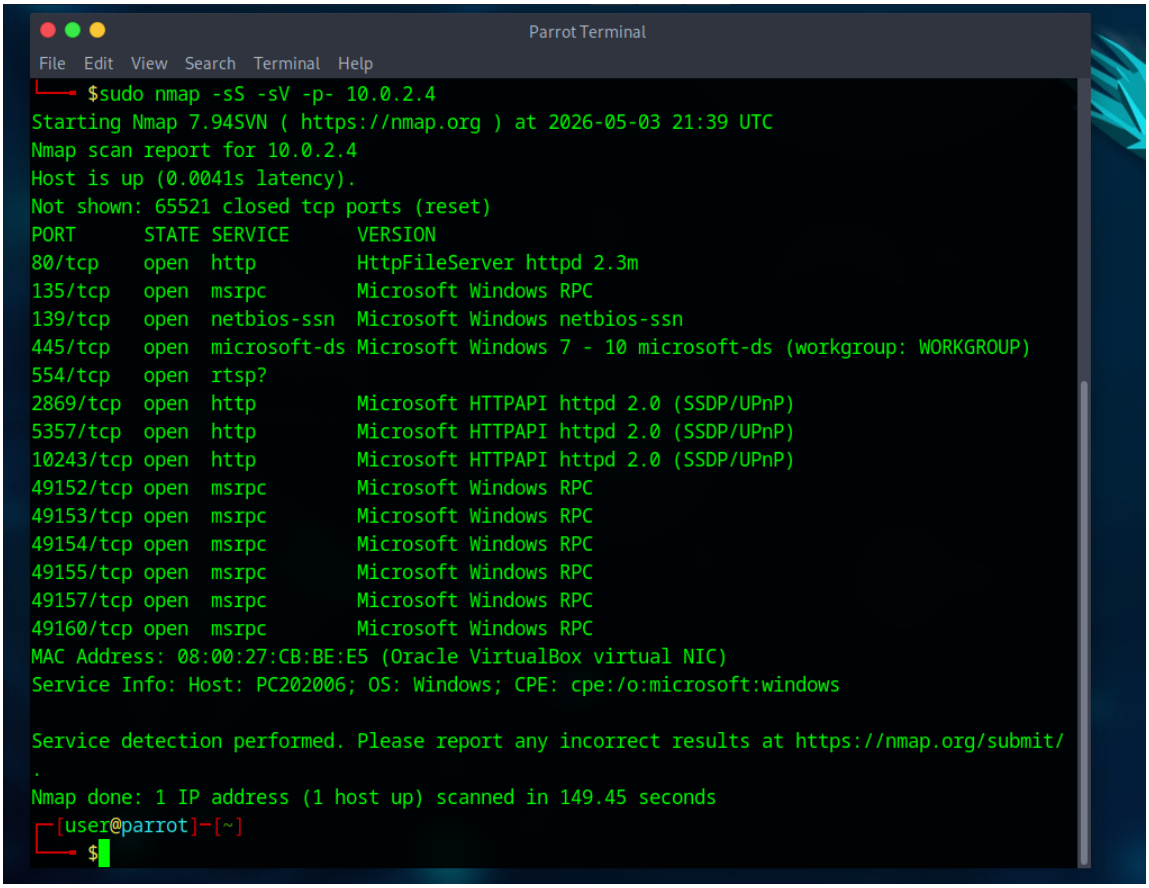
Nota: Se presenta la detección de equipos dentro de la red desde Host-A

Como se observa en la Figura 3, el proceso de descubrimiento permitió identificar los sistemas disponibles dentro de la red y establecer el objetivo principal del ejercicio. Esta información sirvió de base para orientar las siguientes actividades de enumeración y análisis de vulnerabilidades.

Posteriormente se realizó un escaneo exhaustivo sobre Host-A con el propósito de identificar puertos abiertos, servicios activos y versiones asociadas a cada servicio detectado. La información obtenida permitió conocer con mayor detalle la configuración del sistema objetivo y determinar posibles vectores de explotación:

Figura 4

Enumeración de puertos y servicios identificados en Host-A



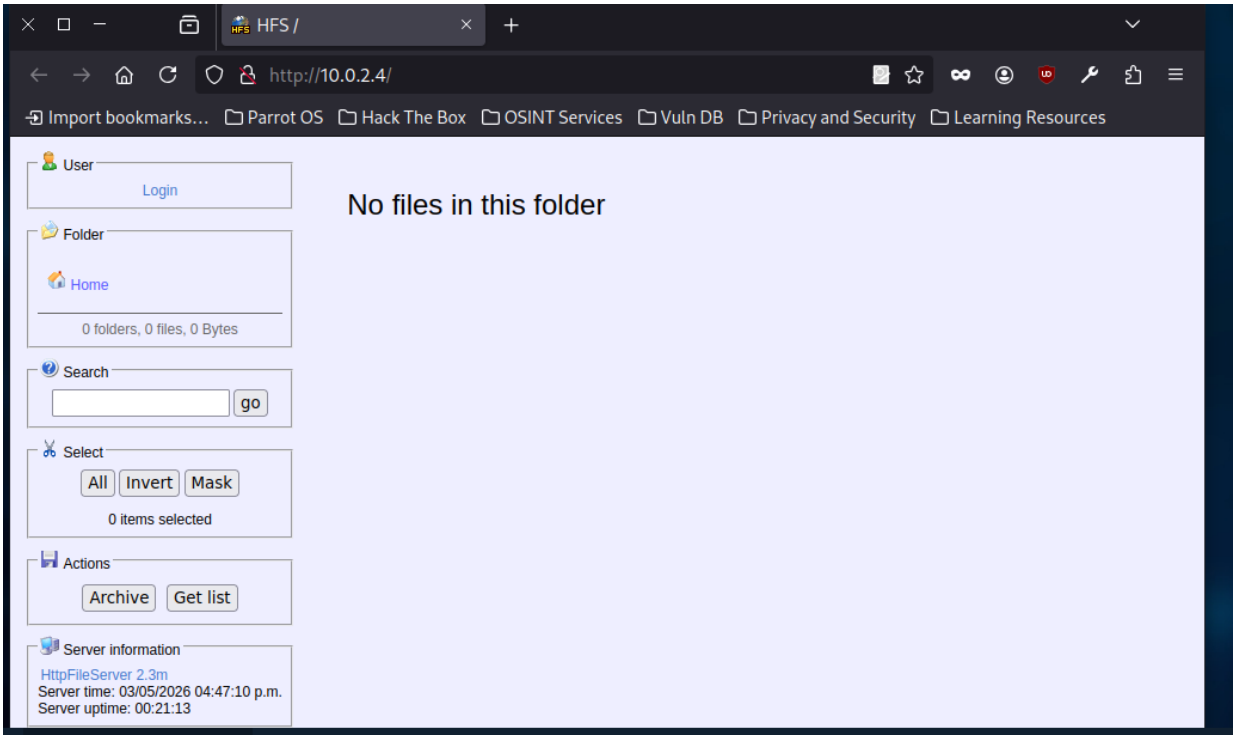
Nota: Se muestra la revisión a detalle de los equipos identificados.

Los resultados evidenciaron la existencia de múltiples puertos accesibles, destacándose el puerto 80/TCP asociado a un servicio web HTTP. La identificación de este servicio resultó especialmente relevante debido a que posteriormente se determinó que correspondía a una versión vulnerable de HTTP File Server (HFS).

Con el fin de validar manualmente la información obtenida mediante el escaneo, se accedió al servicio web desde un navegador, confirmando la presencia de la aplicación HFS sobre el sistema objetivo:

Figura 5

Validación manual del servicio HTTP File Server.



Nota: Se evidencia la validación del servicio vulnerable en funcionamiento.

La verificación visual permitió corroborar la presencia de la aplicación vulnerable y confirmar la información recopilada durante la fase de reconocimiento. Esta evidencia constituyó el punto de partida para el análisis de vulnerabilidades desarrollado en la siguiente etapa.

Análisis de Vulnerabilidades

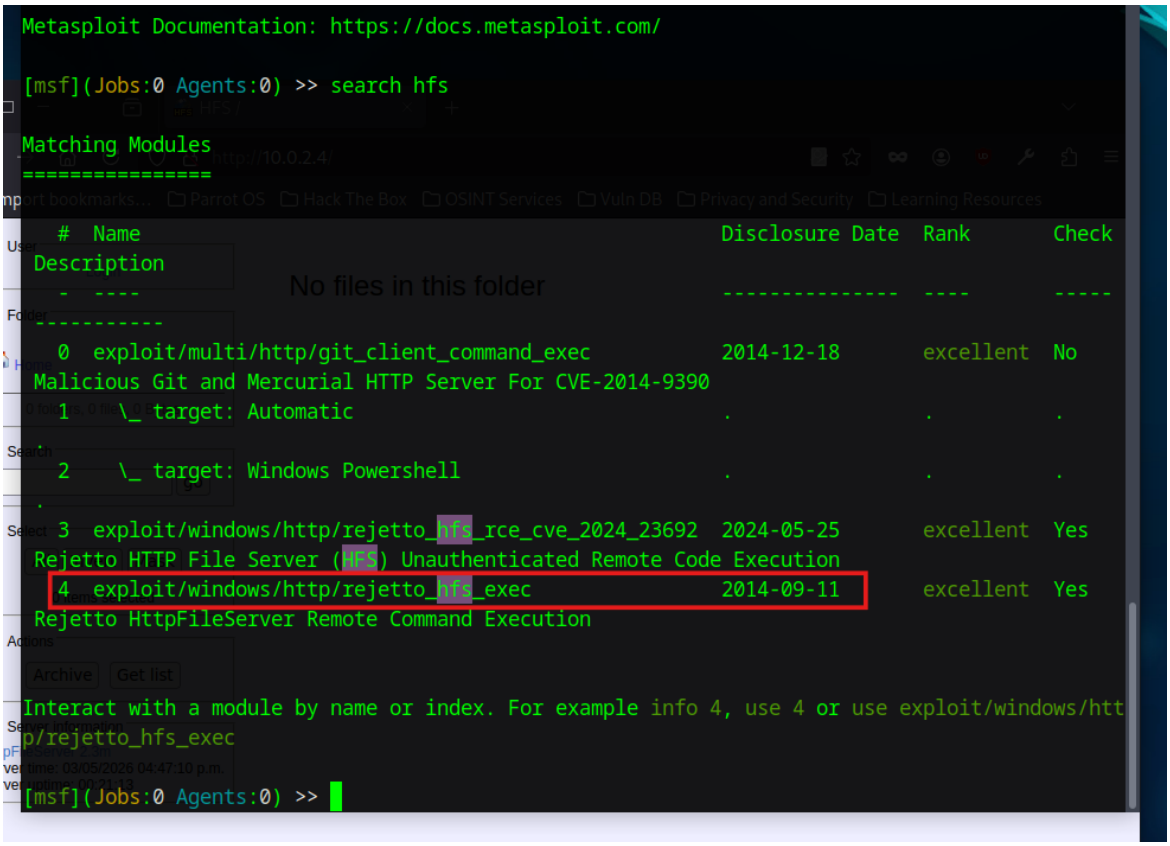
Una vez identificado el servicio HTTP File Server (HFS) versión 2.3m, se procedió a realizar el análisis de vulnerabilidades con el propósito de determinar si existían fallos de seguridad conocidos que permitieran comprometer el sistema objetivo.

Para ello se consultaron bases de datos públicas de vulnerabilidades y módulos disponibles dentro del framework Metasploit, identificando la existencia de un exploit asociado a la vulnerabilidad CVE-2014-6287. Esta vulnerabilidad corresponde a una falla de ejecución

remota de código que afecta versiones específicas de HFS y permite a un atacante ejecutar comandos arbitrarios sobre el sistema afectado:

Figura 6

Módulo de explotación asociado a HFS.



Nota: Se presenta la identificación del exploit a utilizar para el ejercicio.

La identificación del exploit confirmó que la vulnerabilidad disponía de mecanismos públicos de explotación, incrementando significativamente el nivel de riesgo asociado al servicio expuesto.

Posteriormente se realizó un análisis detallado del módulo de explotación con el fin de verificar su compatibilidad con el entorno de laboratorio y comprender su funcionamiento técnico, como se muestra en la Figura 7:

Figura 7

Información técnica del módulo asociado a CVE-2014-6287.

Nota: Se presenta el detalle del análisis del módulo de explotación.

El análisis confirmó que el módulo se encontraba diseñado específicamente para explotar la vulnerabilidad identificada, permitiendo ejecutar código remoto sobre sistemas Windows que ejecutaran versiones vulnerables de HFS. Esta validación permitió avanzar hacia la fase de explotación con un alto grado de confianza respecto a la viabilidad del ataque.

Explotación del Sistema Objetivo

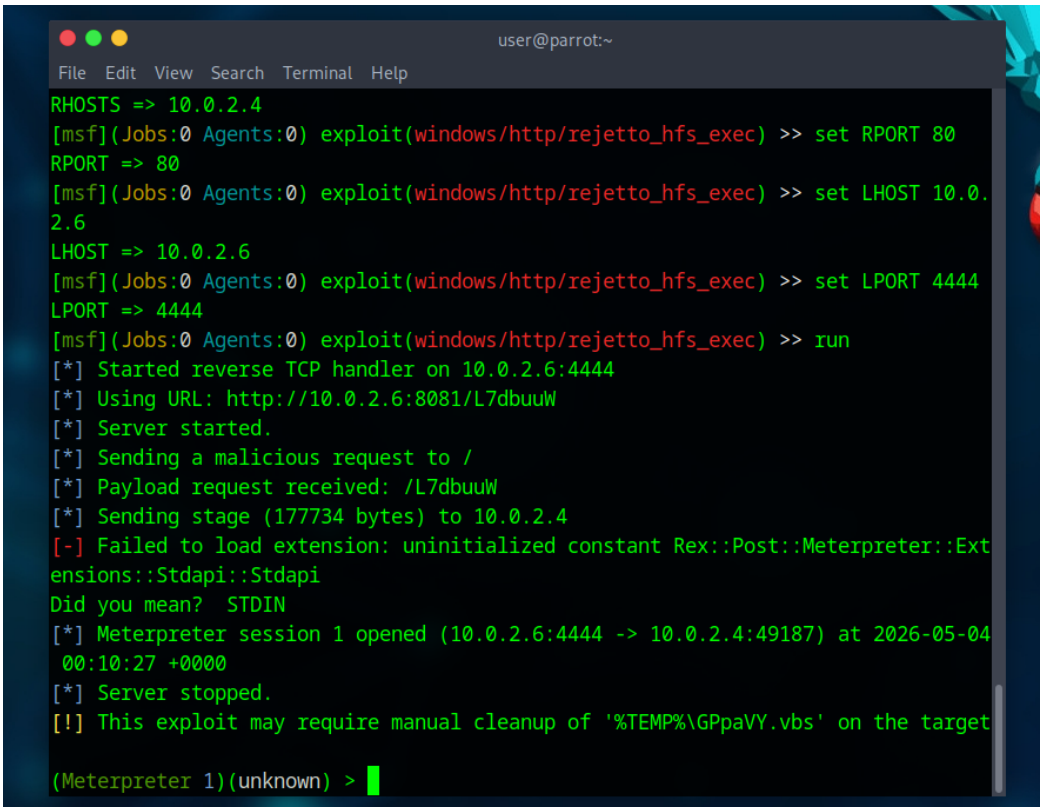
La fase de explotación tuvo como propósito validar técnicamente la vulnerabilidad identificada mediante la obtención de acceso remoto sobre Host-A. Para ello se utilizó el framework Metasploit, configurando el exploit correspondiente y definiendo un payload

orientado al establecimiento de una sesión remota desde el sistema comprometido hacia la máquina atacante.

Durante las pruebas iniciales se identificaron limitaciones asociadas a la configuración de red del laboratorio, las cuales impedían el establecimiento de la conexión remota. Una vez realizados los ajustes necesarios en la arquitectura de red virtual, fue posible completar exitosamente el proceso de explotación:

Figura 8

Ejecución exitosa del exploit y establecimiento de sesión remota.



Nota: Se evidencia el funcionamiento del explot y el acceso obtenido mediante el mismo.

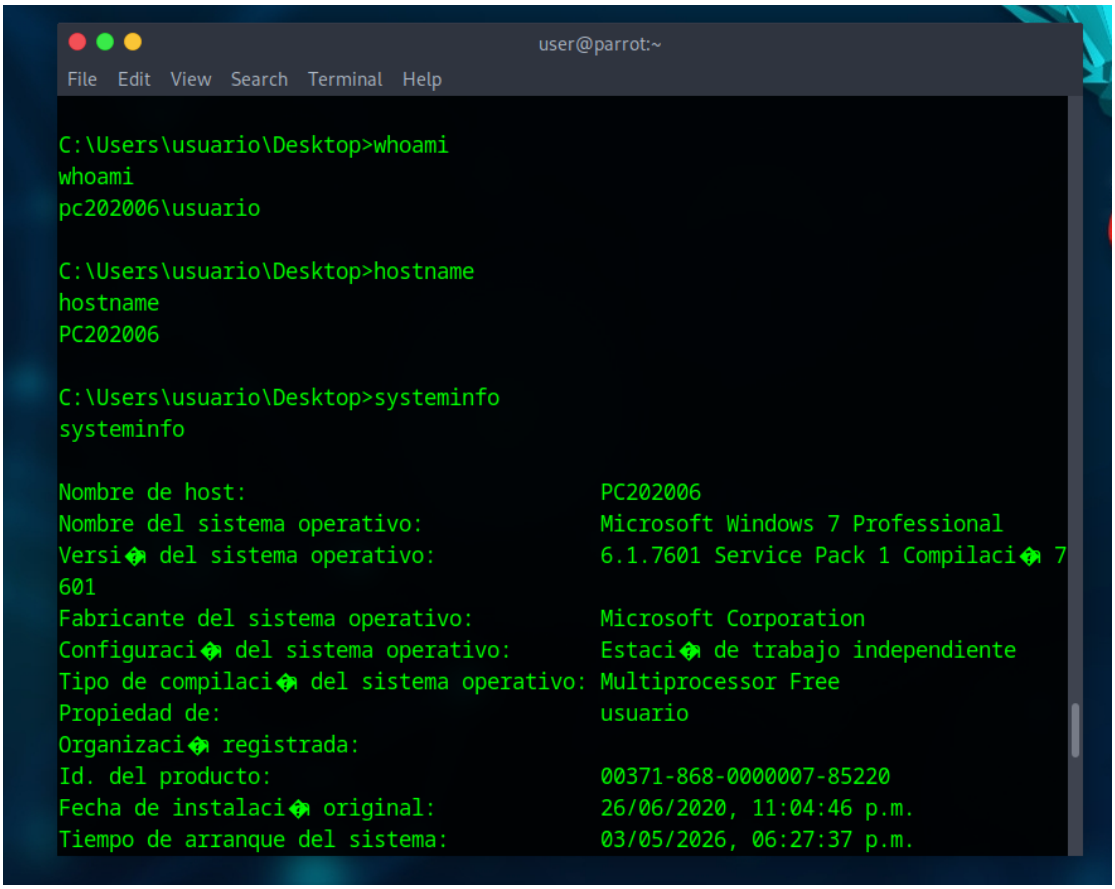
Como se evidencia en la Figura 8, el exploit logró transferir correctamente el payload al sistema objetivo, obteniendo una sesión remota funcional. Este resultado confirmó la explotación

exitosa de la vulnerabilidad CVE-2014-6287 y demostró la posibilidad de comprometer el sistema sin necesidad de credenciales válidas.

Una vez obtenido el acceso inicial, se ejecutaron comandos de reconocimiento local con el propósito de validar el control sobre el sistema comprometido y recopilar información relacionada con el entorno operativo:

Figura 9

Validación del acceso obtenido sobre Host-A.



Nota: Se muestra la validación de información técnica del host atacado.

Los resultados obtenidos en la Figura 9 permitieron confirmar la ejecución remota de comandos, validar el acceso al sistema operativo y recopilar información relevante para el desarrollo de las actividades de post-explotación.

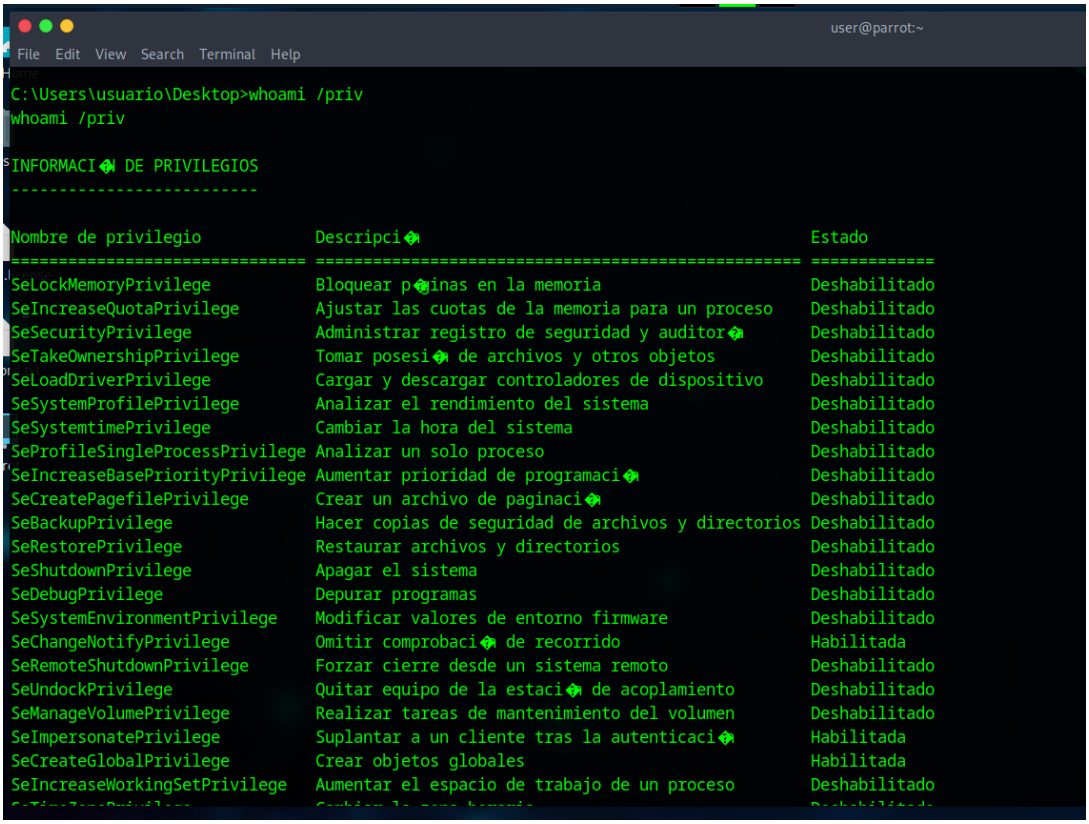
Escalamiento de Privilegios

Una vez comprometido el sistema objetivo, se desarrollaron actividades orientadas a identificar privilegios disponibles y posibles oportunidades de escalamiento. El objetivo de esta etapa fue determinar el nivel de acceso alcanzado y evaluar la posibilidad de incrementar los privilegios dentro del sistema comprometido.

Para ello se ejecutaron diferentes procesos de enumeración relacionados con privilegios, grupos locales y usuarios disponibles dentro del sistema:

Figura 10

Enumeración de privilegios disponibles en Host-A.

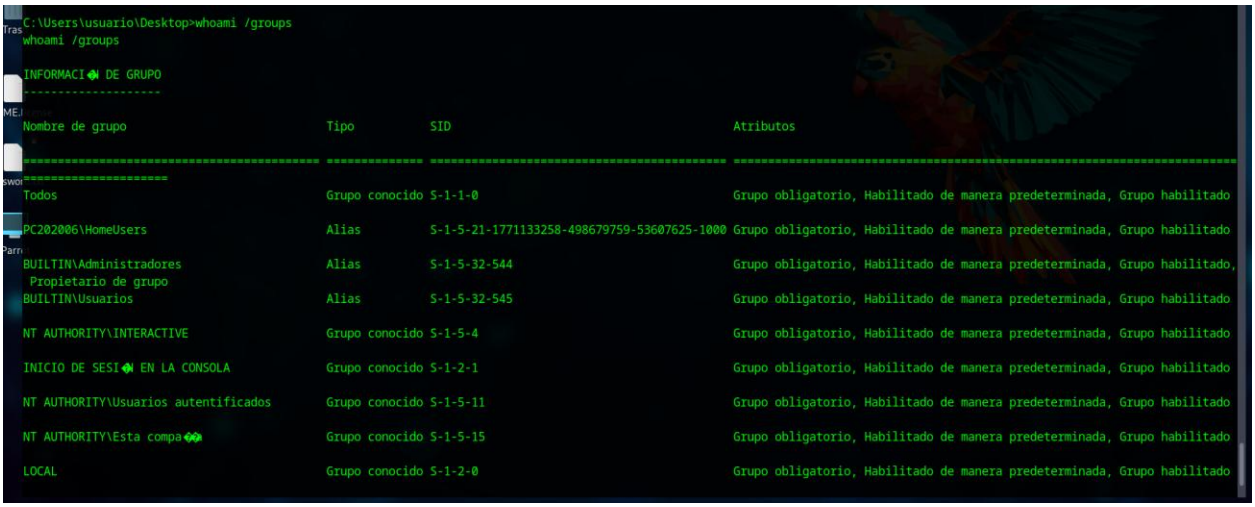


Nota: Se indica la numeración de privilegios del host atacado.

Adicionalmente, se realizó la revisión de grupos asociados al usuario comprometido como se muestra en la Figura 11:

Figura 11

Enumeración de grupos locales y privilegios asociados.



```
C:\Users\usuario\Desktop>whoami /groups
whoami /groups

INFORMACI◆N DE GRUPO
--------------------
Nombre de grupo                            Tipo             SID                                           Atributos
========================================== ================ ============================================= ==================================================
Todos                                      Grupo conocido   S-1-1-0                                       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
PC202006\HomeUsers                         Alias            S-1-5-21-1771133258-498679759-53607625-1000   Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Administradores                    Alias            S-1-5-32-544                                  Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado,
 Propietario de grupo
BUILTIN\Usuarios                           Alias            S-1-5-32-545                                  Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\INTERACTIVE                   Grupo conocido   S-1-5-4                                       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
INICIO DE SESI◆N EN LA CONSOLA             Grupo conocido   S-1-2-1                                       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Usuarios autentificados       Grupo conocido   S-1-5-11                                      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Esta compa◆◆                   Grupo conocido   S-1-5-15                                      Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
LOCAL                                      Grupo conocido   S-1-2-0                                       Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
```

Nota: Se presenta la validación de grupos dentro del usuario comprometido.

Los resultados evidenciaron la existencia de capacidades elevadas dentro del contexto analizado, confirmando que el sistema comprometido presentaba condiciones favorables para el desarrollo de actividades posteriores relacionadas con movimiento lateral y acceso a otros recursos de la red.

Pivoting y Movimiento Lateral

Una vez validado el acceso sobre Host-A, se procedió a analizar la posibilidad de utilizar dicho sistema como punto de pivote hacia otros activos presentes dentro de la red. Esta etapa resulta especialmente relevante dentro de ejercicios Red Team debido a que permite simular escenarios reales de propagación y expansión del compromiso.

La primera actividad consistió en identificar dispositivos accesibles desde el sistema comprometido mediante el análisis de la tabla ARP como se presenta en la Figura 12:

Figura 12

Identificación de sistemas accesibles desde Host-A.

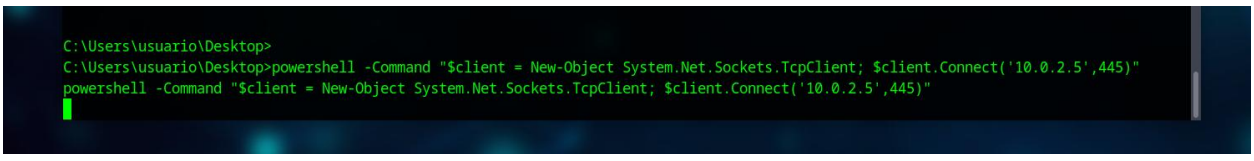
Nota: Se muestra la validación de los sistemas accesibles desde Host atacado.

Los resultados permitieron identificar la dirección IP correspondiente a Host-B, evidenciando conectividad entre ambos sistemas y demostrando la posibilidad de utilizar Host-A como punto de acceso hacia otros dispositivos internos.

Posteriormente se validó la disponibilidad de servicios internos sobre Host-B, específicamente el servicio SMB asociado al puerto 445/TCP:

Figura 13

Validación de conectividad hacia servicios internos de Host-B.



Nota: Se presenta la comprobación de conectividad del puerto 445 vía TCP.

La validación mostrada en la Figura 13 confirmó la existencia de conectividad efectiva entre ambos sistemas y demostró la viabilidad técnica del movimiento lateral dentro del entorno

evaluado. Aunque las limitaciones propias del laboratorio impidieron implementar mecanismos avanzados de acceso remoto persistente, las evidencias obtenidas permitieron demostrar la factibilidad del desplazamiento entre activos comprometidos.

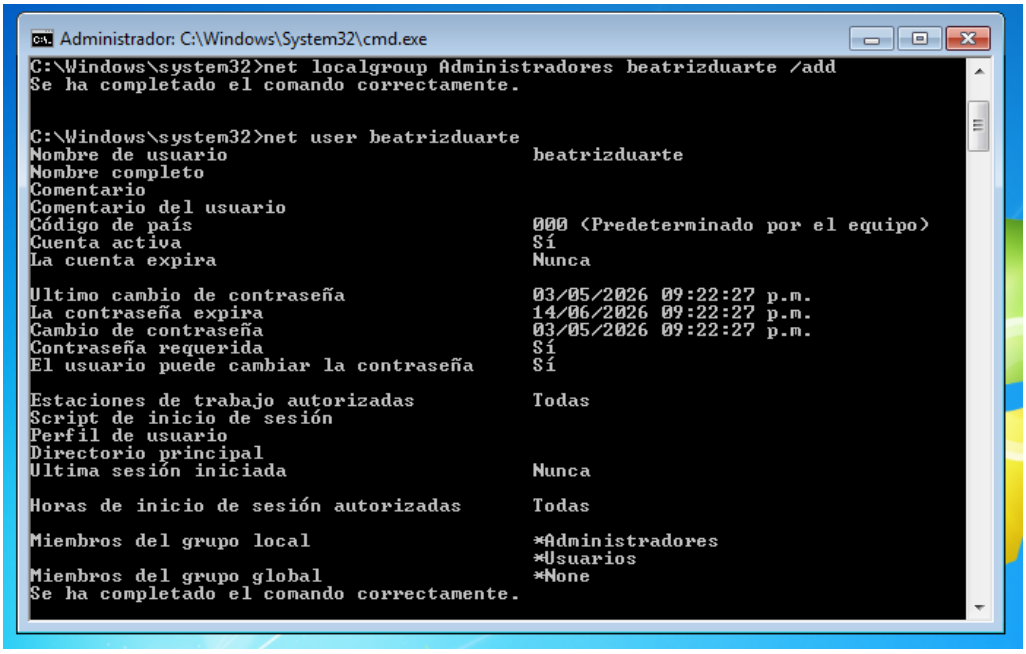
Evidencia del Impacto del Ataque

Con el propósito de demostrar el impacto potencial derivado de la explotación exitosa del sistema, se validó la ejecución de acciones administrativas sobre el entorno comprometido. Estas actividades permitieron evidenciar cómo un atacante podría modificar la configuración del sistema y mantener acceso persistente dentro de la infraestructura.

La evidencia principal del impacto consistió en la creación y validación de una cuenta con privilegios administrativos sobre el sistema objetivo como de presenta en la Figura 14:

Figura 14

Evidencia de Impacto del Ataque



Nota: Se presenta la evidencia del impacto de la ejecución del ataque.

La creación de cuentas privilegiadas constituye una de las técnicas más utilizadas por actores maliciosos para garantizar persistencia dentro de entornos comprometidos. Esta acción demuestra el riesgo que representa la explotación exitosa de vulnerabilidades críticas y evidencia el potencial impacto sobre la integridad y seguridad de los sistemas afectados.

Timeline Forense del Incidente

Con el fin de reconstruir cronológicamente las actividades desarrolladas durante el ejercicio, se elaboró un timeline forense que documenta cada una de las fases observadas desde el reconocimiento inicial hasta la evidencia final del impacto generado sobre la infraestructura.

El análisis cronológico permitió identificar la secuencia lógica del ataque, relacionando las actividades de descubrimiento, enumeración, análisis de vulnerabilidades, explotación, acceso remoto, post-explotación y movimiento lateral. Esta información resulta fundamental para comprender el comportamiento del atacante, evaluar el alcance del incidente y facilitar futuras actividades de respuesta y contención. A continuación, se presenta la Tabla 3 con el orden cronológico del ejercicio:

Tabla 3

Timeline forense consolidado del incidente SecureNova Labs

Fase	Orden	Actividad realizada	Herramienta utilizada	Evidencia obtenida	Resultado
Reconocimiento	1	Descubrimiento de hosts activos en la red virtual	Nmap	Identificación de Host-A y Host-B	Definición de objetivos del ejercicio

Fase	Orden	Actividad realizada	Herramienta utilizada	Evidencia obtenida	Resultado
Reconocimiento	2	Enumeración de puertos y servicios	Nmap	Puertos 80/TCP y 445/TCP abiertos	Identificación de superficie de ataque
Análisis de vulnerabilidades	3	Validación del servicio HTTP File Server (HFS)	Navegador Web	Confirmación de HFS 2.3m	Servicio potencialmente vulnerable
Análisis de vulnerabilidades	4	Consulta de vulnerabilidades conocidas	CVE, ExploitDB	Identificación de CVE-2014-6287	Vulnerabilidad crítica confirmada
Explotación	5	Configuración del exploit y payload	Metasploit	Parámetros de explotación definidos	Preparación del ataque
Explotación	6	Ejecución del exploit	Metasploit	Sesión Meterpreter obtenida	Acceso remoto exitoso
Post-explotación	7	Enumeración del sistema comprometido	Meterpreter	Información de usuarios y sistema operativo	Validación del compromiso

Fase	Orden	Actividad realizada	Herramienta utilizada	Evidencia obtenida	Resultado
Post-explotación	8	Análisis de privilegios	Meterpreter / Windows	Privilegio SeImpersonatePrivilege identificado	Posibilidad de escalamiento
Movimiento lateral	9	Identificación de otros activos internos	ARP	Descubrimiento de Host-B	Expansión potencial del ataque
Movimiento lateral	10	Validación de conectividad SMB	SMB / Meterpreter	Puerto 445/TCP accesible	Viabilidad de pivoting
Impacto	11	Creación y validación de usuario administrativo	Windows	Persistencia demostrada	Compromiso de integridad del sistema
Cierre	12	Consolidación de evidencias y análisis	Registro del ejercicio	Documentación técnica del incidente	Elaboración de plan de remediación

Nota: La tabla presenta una a una las actividades realizadas durante el ataque bajo la metodología PTES.

El timeline consolidado permitirá presentar una visión integral del incidente y servirá de insumo para el análisis de riesgos, estrategias Blue Team y medidas de remediación que serán desarrolladas en los capítulos siguientes.

Análisis Técnico de las Etapas e Impacto

La explotación exitosa de la vulnerabilidad CVE-2014-6287 dentro del entorno SecureNova Labs permitió demostrar cómo una debilidad técnica aparentemente puntual puede convertirse en un incidente con capacidad de afectar múltiples dimensiones de la seguridad de la información. A partir de los resultados obtenidos durante el ejercicio Red Team, es posible evaluar el impacto potencial sobre los principios fundamentales de confidencialidad, integridad y disponibilidad, así como los riesgos organizacionales derivados de un compromiso de seguridad.

El análisis presentado en este capítulo toma como referencia las evidencias obtenidas durante las fases de explotación, post-explotación y movimiento lateral, con el propósito de determinar el alcance que podría tener un incidente similar en un entorno corporativo real.

Impacto sobre la Confidencialidad

La confidencialidad constituye uno de los pilares fundamentales de la seguridad de la información y se refiere a la protección de los datos frente a accesos no autorizados. Durante el ejercicio realizado se logró obtener acceso remoto sobre Host-A mediante la explotación de una vulnerabilidad crítica, permitiendo la ejecución de comandos y la consulta de información interna del sistema.

Si este escenario se presentara en un entorno productivo, un atacante podría acceder a información sensible almacenada en el servidor comprometido, incluyendo credenciales, documentos corporativos, configuraciones de red, información financiera o datos personales de clientes y empleados. De acuerdo con la Ley 1581 de 2012, las organizaciones tienen la obligación de proteger adecuadamente la información personal bajo su custodia, por lo que un incidente de este tipo podría derivar en incumplimientos regulatorios y sanciones legales (Función Pública, 2012).

Adicionalmente, la capacidad de identificar otros activos internos mediante técnicas de reconocimiento posterior a la explotación evidencia que la exposición de información no se limita únicamente al sistema inicialmente comprometido, ya que un atacante podría utilizar la información obtenida para ampliar el alcance del ataque y acceder a recursos adicionales dentro de la infraestructura.

Desde la perspectiva organizacional, la pérdida de confidencialidad representa uno de los impactos más críticos debido a que afecta directamente la confianza de clientes, proveedores y demás partes interesadas.

Impacto sobre la Integridad

La integridad busca garantizar que la información y los sistemas no sean alterados de manera no autorizada, durante el ejercicio práctico se validó la posibilidad de ejecutar comandos sobre el sistema comprometido y realizar modificaciones administrativas, incluyendo la creación de usuarios con privilegios elevados.

Estas capacidades demuestran que un atacante podría modificar configuraciones críticas del sistema, alterar registros, instalar software malicioso o manipular información almacenada dentro de la infraestructura, la creación de cuentas privilegiadas constituye un ejemplo claro de afectación a la integridad, ya que modifica el estado original del sistema y facilita el mantenimiento de accesos persistentes.

La alteración indebida de información puede generar impactos significativos sobre la operación organizacional, especialmente cuando afecta datos financieros, registros de auditoría, sistemas de gestión o bases de datos corporativas. Desde el ámbito legal colombiano, este tipo de acciones pueden estar relacionadas con conductas tipificadas dentro de la Ley 1273 de 2009, particularmente aquellas asociadas con daño informático y acceso abusivo a sistemas informáticos (Policia Nacional, 2009).

Impacto sobre la Disponibilidad

La disponibilidad garantiza que los sistemas y servicios permanezcan accesibles cuando son requeridos por usuarios autorizados, y aunque el ejercicio desarrollado tuvo como objetivo principal demostrar la explotación y el acceso al sistema, las capacidades obtenidas permiten inferir posibles afectaciones sobre este principio de seguridad.

Un atacante con acceso administrativo podría detener servicios críticos, modificar configuraciones esenciales o ejecutar acciones que provoquen interrupciones parciales o totales de la operación tecnológica. En entornos empresariales, este tipo de incidentes puede afectar la continuidad del negocio, generar indisponibilidad de servicios y ocasionar pérdidas económicas derivadas de interrupciones operativas.

La existencia de vulnerabilidades conocidas y explotables incrementa significativamente la probabilidad de afectaciones a la disponibilidad, especialmente cuando los sistemas carecen de mecanismos adecuados de monitoreo, hardening y respuesta ante incidentes. Por esta razón, organismos como CIS recomiendan implementar controles de seguridad orientados a reducir la superficie de ataque y fortalecer la resiliencia de la infraestructura tecnológica (CIS, s.f; ManageEngine, s.f). La afectación de la disponibilidad suele ser uno de los impactos más visibles para la organización debido a que repercute directamente sobre la prestación de servicios y la experiencia de los usuarios.

Riesgos Organizacionales

Más allá del impacto técnico sobre los sistemas, un incidente de seguridad puede generar consecuencias significativas para la organización en distintos ámbitos, por tanto, a continuación, se presentan los principales riesgos asociados:

Riesgo Reputacional

La divulgación pública de un incidente de seguridad puede afectar la imagen corporativa y disminuir la confianza de clientes, socios comerciales e inversionistas, así mismo, la percepción de falta de controles adecuados puede deteriorar la credibilidad de la organización y afectar su posicionamiento dentro del mercado.

Riesgo Financiero

Los incidentes de seguridad suelen generar costos asociados a actividades de investigación, recuperación de sistemas, implementación de controles correctivos y atención de requerimientos regulatorios, además de que se pueden producir pérdidas derivadas de interrupciones operativas y afectaciones sobre los procesos de negocio.

Riesgo Operativo

La indisponibilidad de sistemas críticos o la alteración de información puede impactar directamente la capacidad operativa de la organización. Dependiendo de la criticidad de los activos comprometidos, el incidente podría afectar procesos estratégicos, administrativos o productivos.

Riesgo Legal y Regulatorio

El tratamiento inadecuado de información personal o la falta de controles de seguridad suficientes podría generar incumplimientos frente a la normativa vigente en materia de protección de datos y delitos informáticos. Esto puede derivar en investigaciones, sanciones administrativas y responsabilidades legales para la organización (Función Pública, 2009; Función Pública, 2012).

En conjunto, estos riesgos evidencian que los incidentes de ciberseguridad no deben analizarse únicamente desde una perspectiva tecnológica, sino también desde una visión integral que contemple sus implicaciones organizacionales y estratégicas.

Riesgo Asociado al Movimiento Lateral

Uno de los hallazgos más relevantes del ejercicio fue la demostración de la posibilidad de identificar y acceder a otros activos internos a partir del compromiso inicial de Host-A. Esta situación evidencia el riesgo asociado al movimiento lateral, técnica ampliamente utilizada por actores maliciosos para expandir progresivamente el alcance de un ataque dentro de una organización.Durante las actividades de post-explotación se logró identificar Host-B y validar la existencia de servicios internos accesibles desde el sistema comprometido.

Aunque el escenario fue desarrollado en un laboratorio controlado, los resultados obtenidos reflejan una situación frecuente en entornos corporativos donde la segmentación de red es insuficiente o los controles internos presentan debilidades.

El movimiento lateral incrementa considerablemente el nivel de riesgo debido a que transforma un incidente localizado en un compromiso potencialmente masivo, un atacante que obtiene acceso inicial a un único sistema puede utilizarlo como plataforma para descubrir nuevos activos, comprometer servidores adicionales y acceder a información de mayor valor estratégico.

Desde la perspectiva Blue Team, este riesgo justifica la implementación de controles como segmentación de red, monitoreo continuo mediante SIEM, detección avanzada mediante EDR, hardening de sistemas y mecanismos de respuesta automatizada que permitan identificar comportamientos anómalos antes de que el ataque alcance otros segmentos de la infraestructura (CrowdSec, s.f).

En el caso de SecureNova Labs, el movimiento lateral constituye el riesgo técnico más relevante identificado durante el ejercicio, ya que evidencia cómo una vulnerabilidad inicialmente localizada puede convertirse en un incidente con capacidad de comprometer múltiples activos organizacionales y afectar significativamente la postura de seguridad de la empresa.

Estrategias Blue Team

Una vez identificadas las vulnerabilidades explotadas y analizados los riesgos derivados del compromiso de Host-A, resulta necesario definir las acciones defensivas que permitirían contener, detectar y prevenir incidentes similares dentro de SecureNova Labs. Desde la perspectiva Blue Team, la gestión de incidentes no se limita a responder ante un ataque ya materializado, sino que busca fortalecer continuamente la postura de seguridad mediante mecanismos de monitoreo, control, detección y endurecimiento de la infraestructura.

Las estrategias presentadas en este capítulo toman como referencia las evidencias obtenidas durante el ejercicio Red Team y se encuentran orientadas a reducir la probabilidad de explotación de vulnerabilidades, limitar el movimiento lateral y mejorar la capacidad de detección temprana frente a futuras amenazas.

Respuesta Inicial Ante Incidentes

Ante la detección de un incidente de seguridad, las primeras acciones ejecutadas por el equipo Blue Team resultan determinantes para limitar el alcance del ataque y preservar evidencias útiles para el proceso de investigación. En el escenario analizado, la explotación de la vulnerabilidad CVE-2014-6287 permitió la obtención de acceso remoto sobre Host-A. Frente a una situación real, la respuesta inicial debería comenzar con la identificación de indicadores de compromiso (IOC), tales como conexiones inusuales, ejecución de procesos sospechosos, creación de cuentas no autorizadas o modificaciones inesperadas en los registros del sistema.

Posteriormente, se debe realizar la recopilación y análisis de logs provenientes de sistemas operativos, servicios de red, soluciones EDR y plataformas de monitoreo, con el propósito de determinar el alcance del incidente y reconstruir la secuencia de eventos ocurridos. IBIS Computer (2026) señala que estas primeras acciones deben priorizar la contención, la preservación de evidencias y la identificación del alcance del compromiso. Una vez clasificado

el incidente según su criticidad, el equipo de respuesta debe proceder al aislamiento controlado de los sistemas afectados para evitar la propagación hacia otros activos de la infraestructura, esta acción permite contener la amenaza mientras se desarrollan las actividades de análisis y remediación (Abdul, 2026). A continuación, se presenta en la Tabla 4 el objetivo de cada acción inicial:

Tabla 4

Acciones iniciales de respuesta ante incidentes.

Acción	Objetivo
Identificación de IOC	Detectar actividad maliciosa
Recolección de logs	Preservar evidencia
Clasificación del incidente	Determinar criticidad
Aislamiento del sistema	Evitar propagación
Notificación interna	Activar respuesta organizacional

Nota: Se presentan las acciones de respuesta y el objetivo de cada una.

Estrategias de Contención

Una vez confirmado el incidente, las acciones de contención buscan limitar la capacidad del atacante para continuar interactuando con los sistemas comprometidos. En el caso de SecureNova Labs, la principal prioridad consistiría en impedir que el compromiso inicial sobre Host-A evolucione hacia otros sistemas internos. Para ello, BBVA (2025) recomienda implementar mecanismos de segmentación de red que limiten la comunicación entre servidores, estaciones de trabajo y recursos críticos, así mismo, los firewalls perimetrales e internos deben configurarse para restringir conexiones innecesarias y bloquear puertos asociados a servicios vulnerables o no autorizados.

El uso de listas de control de acceso (ACL) permite reforzar estas restricciones y reducir la superficie de exposición, en la misma línea, cuando se detecte un sistema comprometido, es recomendable aplicar procedimientos de cuarentena mediante soluciones EDR o herramientas de respuesta automatizada, aislando temporalmente el equipo afectado mientras se desarrollan actividades de análisis y remediación. Estas medidas permiten reducir significativamente la probabilidad de movimiento lateral y minimizar el impacto organizacional del incidente.

Estrategias de Hardening

Los resultados obtenidos durante el ejercicio evidenciaron que la principal causa del compromiso fue la existencia de un servicio vulnerable expuesto dentro de la infraestructura. En consecuencia, una de las estrategias más efectivas para reducir el riesgo consiste en fortalecer los sistemas mediante procesos de hardening.

La primera medida recomendada es la actualización y aplicación periódica de parches de seguridad sobre sistemas operativos, aplicaciones y servicios críticos. En el escenario evaluado, la vulnerabilidad CVE-2014-6287 se encontraba asociada a una versión obsoleta de HFS, situación que podría haberse mitigado mediante una adecuada gestión de actualizaciones.

Igualmente, se recomienda eliminar o deshabilitar servicios innecesarios, reducir puertos expuestos, restringir accesos administrativos y aplicar el principio de mínimo privilegio sobre usuarios y aplicaciones. La implementación de medidas de hardening disminuye significativamente la superficie de ataque y dificulta las actividades de explotación realizadas por actores maliciosos como lo indica Pandora FMS Team (2024).

Implementación de Controles CIS

Los Controles CIS constituyen uno de los marcos de referencia más utilizados para fortalecer la postura de seguridad de una organización. A partir de los hallazgos identificados durante el ejercicio Red Team, se recomienda priorizar la implementación de controles

orientados a la gestión de activos, vulnerabilidades, privilegios y monitoreo continuo. Entre los controles más relevantes para SecureNova Labs se destacan:

- Inventario y control de activos empresariales.
- Inventario y control de software autorizado.
- Gestión continua de vulnerabilidades.
- Control de privilegios administrativos.
- Gestión segura de configuraciones.
- Monitoreo y análisis continuo de registros.
- Respuesta y recuperación ante incidentes.

De acuerdo con ManageEngine (s.f) la adopción de estos controles permitiría reducir significativamente las condiciones que facilitaron la explotación observada durante el ejercicio y fortalecer la capacidad defensiva de la organización.

SIEM y Monitoreo de Eventos

Uno de los principales desafíos observados durante el ejercicio es la necesidad de detectar oportunamente actividades sospechosas antes de que evolucionen hacia compromisos de mayor alcance. Las plataformas SIEM permiten centralizar registros provenientes de múltiples fuentes, correlacionar eventos de seguridad y generar alertas cuando se detectan patrones asociados a comportamientos maliciosos (Fortinet, s.f). De esta manera, actividades como múltiples intentos de acceso, ejecución de procesos inusuales o conexiones entre sistemas internos pueden ser identificadas de forma temprana.

La correlación de eventos facilita además la construcción de líneas de tiempo de incidentes y mejora la capacidad de respuesta de los equipos Blue Team. En escenarios similares al desarrollado en SecureNova Labs, un SIEM podría detectar actividades relacionadas con la explotación de HFS, la apertura de sesiones remotas y los intentos de movimiento lateral entre

activos internos como lo indica Palo Alto Networks, (s.f). El monitoreo continuo constituye uno de los pilares fundamentales para fortalecer la capacidad de detección y respuesta frente a amenazas avanzadas.

Herramientas Blue Team

Wazuh

Wazuh es una plataforma open source orientada a la monitorización de seguridad, detección de amenazas y respuesta automatizada, su capacidad para recopilar registros, generar alertas y ejecutar acciones automáticas permite fortalecer significativamente la visibilidad sobre la infraestructura tecnológica (Wazuh, s.f). Dentro de SecureNova Labs, Wazuh podría utilizarse para identificar modificaciones sospechosas en sistemas, monitorear eventos críticos y activar respuestas automáticas frente a actividades maliciosas detectadas.

CrowdSec

CrowdSec es una solución colaborativa de detección y bloqueo de amenazas basada en inteligencia colectiva, su funcionamiento permite identificar comportamientos asociados a ataques y bloquear automáticamente direcciones IP consideradas maliciosas (CrowdSec, s.f). La integración de CrowdSec permitiría reducir intentos de explotación repetitivos y fortalecer los mecanismos preventivos frente a amenazas externas.

Pfsense

PfSense constituye una solución de firewall ampliamente utilizada para el control de tráfico, segmentación de redes y aplicación de políticas de acceso (PfSense, s.f). Su implementación dentro de SecureNova Labs facilitaría la separación de segmentos críticos de la infraestructura, limitando las posibilidades de movimiento lateral observadas durante el ejercicio y mejorando el control sobre las comunicaciones internas

Solución EDR

Las soluciones EDR (Endpoint Detection and Response) permiten monitorear continuamente los dispositivos finales, identificar actividades anómalas y responder rápidamente ante incidentes de seguridad (Fortinet, s.f). Estas herramientas proporcionan visibilidad detallada sobre procesos, conexiones y comportamientos sospechosos, permitiendo detectar actividades similares a las ejecutadas durante el ejercicio Red Team y facilitando la contención temprana de amenazas.

Integración Red Team vs Blue Team

Uno de los principales aprendizajes obtenidos durante el desarrollo del seminario es que la seguridad organizacional no depende exclusivamente de capacidades ofensivas o defensivas aisladas y la efectividad de una estrategia de ciberseguridad se incrementa cuando los equipos Red Team y Blue Team trabajan de manera coordinada y complementaria.

Mientras el Red Team identifica vulnerabilidades y simula escenarios reales de ataque, el Blue Team fortalece los mecanismos de detección, respuesta y recuperación, lo cual permite validar controles existentes, descubrir debilidades operativas y mejorar continuamente la postura de seguridad organizacional (Cranford, 2023).

Adicionalmente, la incorporación de plataformas SOAR (Security Orchestration, Automation and Response) permite automatizar procesos de análisis, correlación y respuesta ante incidentes, reduciendo tiempos de reacción y mejorando la eficiencia operativa de los equipos defensivos. Los ejercicios conjuntos, simulaciones periódicas y programas de mejora continua facilitan el fortalecimiento de capacidades técnicas, fomentan la colaboración interdisciplinaria y permiten que las organizaciones evolucionen desde modelos reactivos hacia esquemas de seguridad proactivos y resilientes.

En el caso de SecureNova Labs, la integración entre Red Team y Blue Team representa el mecanismo más efectivo para transformar los hallazgos identificados durante el ejercicio práctico en oportunidades de mejora continua, fortaleciendo la capacidad de prevención, detección y respuesta frente a futuras amenazas.

Plan de Remediación

Como resultado del ejercicio Red Team desarrollado sobre el entorno SecureNova Labs, se identificaron vulnerabilidades y debilidades de seguridad que permitieron la obtención de acceso remoto, la ejecución de comandos sobre sistemas comprometidos y la posibilidad de movimiento lateral dentro de la infraestructura evaluada. Los hallazgos evidenciaron la existencia de riesgos asociados a la exposición de servicios vulnerables, la falta de actualización de componentes críticos, la presencia de privilegios que podrían facilitar escenarios de escalamiento y la posibilidad de afectar múltiples activos a partir de un compromiso inicial. Adicionalmente, el análisis realizado permitió identificar impactos potenciales sobre la confidencialidad, integridad y disponibilidad de la información, así como riesgos operativos, reputacionales y legales para la organización.

En este contexto, la remediación constituye una fase fundamental dentro del proceso de gestión de vulnerabilidades, ya que permite implementar acciones correctivas orientadas a eliminar o reducir las condiciones que favorecen la materialización de amenazas y la explotación de debilidades de seguridad. De acuerdo con Randall (2026), un proceso efectivo de remediación no solo busca corregir vulnerabilidades identificadas, sino también fortalecer los controles existentes y reducir la probabilidad de recurrencia de incidentes similares.

Con el propósito de reducir los riesgos identificados y fortalecer la postura de seguridad de SecureNova Labs, se plantea el siguiente plan de remediación priorizado, orientado a corregir las condiciones que facilitaron el compromiso de los sistemas y a establecer una base para la

mejora continua de las capacidades de protección y respuesta frente a incidentes de ciberseguridad (Randall, 2026).

La Tabla 5 presenta los principales hallazgos identificados durante el ejercicio, así como su nivel de criticidad y prioridad de atención:

Tabla 5

Hallazgos Priorizados

Hallazgo identificado	**Riesgo asociado**	**Prioridad**
Vulnerabilidad CVE-2014-6287 en HFS	Ejecución remota de código	Crítica
Posibilidad de movimiento lateral	Compromiso de otros activos internos	Alta
Exceso de privilegios en el sistema comprometido	Escalamiento de privilegios	Alta
Exposición de servicios innecesarios	Incremento de superficie de ataque	Media
Limitado monitoreo de eventos de seguridad	Detección tardía de incidentes	Media

Nota: Se presentan los hallazgos identificados junto con el respectivo riesgo asociado y la prioridad para dar tratamiento.

A partir de los hallazgos identificados, se definieron en la Tabla 6 las acciones correctivas orientadas a eliminar o reducir los riesgos detectados durante el ejercicio:

Tabla 6

Plan de tratamiento de hallazgos

Hallazgo	**Acción de remediación**	**Prioridad**
CVE-2014-6287	Actualizar o reemplazar el servicio vulnerable	Alta
Movimiento lateral	Implementar segmentación de red	Alta
Exceso de privilegios	Aplicar principio de mínimo privilegio	Alta
Servicios innecesarios	Realizar hardening y reducción de exposición	Media
Falta de monitoreo	Fortalecer capacidades de detección y monitoreo	Media

Nota: Se presentan las acciones correctivas para las debilidades identificadas.

Las acciones propuestas deben ejecutarse de acuerdo con el nivel de riesgo asociado y el impacto potencial sobre la organización como se indica en la Tabla 7:

Tabla 7

Priorización de implementación

Acción	**Horizonte de ejecución**
Corrección de vulnerabilidades críticas	Inmediato
Aplicación de parches de seguridad	Corto plazo
Segmentación de red	Corto plazo
Hardening de sistemas	Mediano plazo
Fortalecimiento de monitoreo	Mediano plazo
Revisión periódica de controles	Continuo

Nota: Se presenta el horizonte de ejecución de las acciones a ejecutar en el proceso de remediación.

Con la implementación de estas acciones, SecureNova Labs podrá reducir significativamente la exposición frente a amenazas informáticas, fortalecer su postura de seguridad y mejorar su capacidad de prevención y respuesta ante incidentes de ciberseguridad. El detalle de las recomendaciones técnicas, organizacionales y de mejora continua se presenta en el apartado de “Recomendaciones” del presente documento.

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/sG3_yKrq8ck

Conclusiones

La evaluación realizada sobre el escenario SecureNova Labs permitió evidenciar que la combinación de capacidades Red Team y Blue Team constituye un mecanismo efectivo para identificar debilidades de seguridad, validar riesgos reales y fortalecer la postura defensiva de una organización. El análisis confirmó que la seguridad informática requiere un enfoque integral que combine actividades ofensivas de evaluación con capacidades permanentes de monitoreo, detección y respuesta.

Los resultados obtenidos demostraron que la presencia de vulnerabilidades conocidas, servicios expuestos y configuraciones inseguras puede facilitar el compromiso inicial de un sistema y convertirse en un punto de partida para ataques de mayor alcance. Esto permitió comprobar que la gestión continua de vulnerabilidades y la aplicación oportuna de medidas de fortalecimiento son factores determinantes para reducir la superficie de ataque y minimizar la probabilidad de incidentes de seguridad.

El análisis de impacto evidenció que la explotación exitosa de una vulnerabilidad crítica puede afectar simultáneamente la confidencialidad, integridad y disponibilidad de la información, generando además consecuencias operativas, financieras, reputacionales y legales para la organización. Este hallazgo confirma que los riesgos de ciberseguridad trascienden el ámbito tecnológico y deben ser gestionados como parte de la estrategia organizacional.

De igual manera, se concluyó que la implementación de controles de seguridad, segmentación de redes, monitoreo continuo y procesos de hardening fortalece significativamente la capacidad de prevención, detección y contención frente a amenazas cibernéticas. La adopción de estas medidas contribuye a incrementar la resiliencia organizacional y a mejorar la capacidad de respuesta ante incidentes de seguridad.

Desde la perspectiva ética y legal, se evidenció que las actividades de pentesting y análisis de seguridad deben desarrollarse bajo principios de responsabilidad profesional, confidencialidad y cumplimiento normativo. El estudio permitió reconocer la importancia de la legislación colombiana sobre delitos informáticos y protección de datos personales como marco de referencia para el ejercicio responsable de la ciberseguridad.

Finalmente, el seminario permitió consolidar competencias técnicas, analíticas y estratégicas relacionadas con la identificación de vulnerabilidades, análisis de riesgos y fortalecimiento de controles de seguridad. Como principal aprendizaje, se concluye que la protección efectiva de los activos tecnológicos depende de la integración permanente entre capacidades ofensivas, defensivas y procesos de mejora continua orientados a la gestión del riesgo.

Recomendaciones

Las recomendaciones presentadas a continuación se formulan a partir de los resultados obtenidos durante el ejercicio desarrollado en SecureNova Labs y buscan fortalecer la madurez organizacional en materia de ciberseguridad. Más que acciones correctivas puntuales, estas recomendaciones están orientadas a consolidar una cultura de gestión del riesgo, resiliencia operativa y mejora continua frente a las amenazas que afectan actualmente a las organizaciones.

Recomendaciones Técnicas

Se recomienda adoptar un enfoque basado en riesgo para la toma de decisiones relacionadas con la protección de activos tecnológicos, priorizando los recursos y esfuerzos de seguridad sobre aquellos sistemas que soportan procesos críticos para la organización.

Igualmente, resulta conveniente fortalecer la integración entre las diferentes herramientas de seguridad utilizadas dentro de la infraestructura tecnológica, permitiendo una mayor visibilidad sobre los eventos de seguridad y una mejor capacidad de correlación entre incidentes potencialmente relacionados.

Así mismo, se recomienda incorporar procesos periódicos de validación técnica mediante ejercicios controlados de simulación de ataques y revisión de controles de seguridad, con el fin de evaluar continuamente la efectividad de las medidas implementadas y detectar oportunidades de mejora antes de que sean aprovechadas por actores maliciosos.

Recomendaciones Organizacionales

La ciberseguridad debe consolidarse como un componente estratégico dentro de la gestión organizacional y no limitarse exclusivamente al ámbito tecnológico. En este sentido, se recomienda fortalecer la participación de la alta dirección en los procesos relacionados con gestión de riesgos, continuidad del negocio y protección de la información.

De igual manera, resulta conveniente promover mecanismos de coordinación entre áreas técnicas, administrativas y de gestión, favoreciendo una visión integral de la seguridad que facilite la toma de decisiones y la adecuada asignación de recursos para la protección de los activos institucionales.

Adicionalmente, se recomienda fomentar una cultura organizacional orientada a la seguridad de la información, en la cual la protección de los activos digitales sea entendida como una responsabilidad compartida entre todos los niveles de la organización.

Recomendaciones de Monitoreo

Se recomienda evolucionar progresivamente desde modelos reactivos de supervisión hacia esquemas de monitoreo basados en análisis continuo y detección temprana de amenazas. Para ello, es importante establecer mecanismos que permitan identificar tendencias, comportamientos anómalos y posibles indicadores de compromiso antes de que estos se materialicen en incidentes de seguridad.

Así mismo, resulta conveniente definir métricas e indicadores de desempeño asociados a la gestión de eventos de seguridad, permitiendo medir de forma objetiva la efectividad de los controles implementados y la capacidad de respuesta de la organización frente a incidentes. La información obtenida mediante los procesos de monitoreo debe convertirse en un insumo permanente para la toma de decisiones y la actualización de estrategias de protección.

Recomendaciones de Mejora Continua

La evolución constante de las amenazas informáticas exige que las organizaciones adopten modelos de mejora continua que permitan revisar periódicamente sus capacidades de prevención, detección, respuesta y recuperación. En este contexto, se recomienda establecer ciclos regulares de evaluación de riesgos y revisión de controles de seguridad, incorporando los resultados obtenidos como parte de los procesos de planeación y fortalecimiento institucional.

Así mismo, Adonis Partners (2025) destaca la importancia de mantener espacios de aprendizaje y actualización frente a nuevas tendencias, tecnologías y técnicas utilizadas por actores maliciosos, favoreciendo la adaptación de la organización a un entorno digital en constante transformación. Finalmente, se recomienda promover ejercicios colaborativos entre capacidades ofensivas y defensivas, permitiendo que los hallazgos identificados durante actividades de evaluación se conviertan en oportunidades de mejora para fortalecer progresivamente la postura de seguridad y la resiliencia organizacional.

Referencias Bibliográficas

Pandora FMS Team. (2024). System Hardening: porque requerimos fortalecer la ciberseguridad en nuestros sistemas. https://pandorafms.com/blog/es/hardening/

Abdul, S. (2026). How to respond to cyber hacks and security breaches. (C. Guide, Ed.). https://cybersecurityguide.org/resources/cyber-incident-guide/

Adonis Partners. (2025). White Paper: Enhancing Cybersecurity Through Continuous Improvement Methodologies. https://adonispartners.com/enhancing-cybersecurity-continuous-improvement/

ASEC. (2024). Attack Cases Against HTTP File Server (HFS) (CVE-2024-23692). https://asec.ahnlab.com/en/76436/

BBVA. (2025). Técnicas de 'hardening' para blindar tu empresa ante los ciberatacantes. https://www.bbva.com/es/empresas/tecnicas-de-hardening-para-blindar-tu-empresa-ante-los-ciberatacantes/

Campus Internacional Ciberseguridad. (s.f.). ¿Cómo ayuda Nmap con la seguridad de la red? Recuperado el 28 de mayo de 2026, de https://www.campusciberseguridad.com/blog/como-ayuda-nmap-con-la-seguridad-de-la-red/

Campus Internacional Ciberseguridad. (s.f.). Escaneo de vulnerabilidades usando OpenVAS. Recuperado el 28 de mayo de 2026, de https://www.campusciberseguridad.com/blog/escaneo-de-vulnerabilidades-usando-openvas/

Campus Internacional Ciberseguridad. (s.f.). Metasploit. La herramienta esencial en ciberseguridad. Recuperado el 28 de mayo de 2026, de

https://www.campusciberseguridad.com/blog/metasploit-herramienta-esencial-ciberseguridad/

CIS. (s.f.). Controles de seguridad críticos de CIS. Recuperado el 27 de mayo de 2026, de https://www.cisecurity.org/controls

COPNIA. (s.f.). Código de ética. Recuperado el 27 de mayo de 2026, de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Cranford, J. (2023). Red Team vs Blue Team in Cybersecurity. (CrowdStrike, Ed.). https://www.crowdstrike.com/en-us/cybersecurity-101/advisory-services/red-team-vs-blue-team/

CrowdSec. (s.f). Conocemos las direcciones IP que te atacan, ¿ y tú?. Recuperado el 28 de mayo, de 2026 de https://www.crowdsec.net/cyber-threat-intelligence

DragonSec. (2025). Pentesting. Qué es, fases y cómo lo aplicamos en dragonsec.io. https://dragonsec.io/es/pentesting-que-es

Future Learning. (s.f). Penetration Testing Execution Standard (PTES). Recuperado el 26 de mayo de 2026, de https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71523

Fortinet. (s.f). ¿Qué es la detección y respuesta de endpoint (EDR)? Recuperado el 28 de mayo de 2026, de https://www.fortinet.com/lat/resources/cyberglossary/what-is-edr?utm_source=chatgpt.com

Fortinet. (s.f). ¿Qué es SIEM. Recuperado el 26 de mayo de 2026, de https://www.fortinet.com/lat/resources/cyberglossary/what-is-siem

Fortinet. (s.f). ¿Qué es una CVE? Vulnerabilidades y exposiciones comunes definidas. Recuperado el 26 de mayo de 2026, de https://www.fortinet.com/lat/resources/cyberglossary/cve

Función Pública. (2000). Ley 599 de 2000. Por la cual se expide el Código Penal Colombiano. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Función Pública. (2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Función Pública. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

González, M. M. (2024). Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team. (U. N. UNAD, Ed.) https://repository.unad.edu.co/bitstream/handle/10596/65956/mmauryg.pdf?sequence=3

Hernandez, M. (2022). Pentesting con OWASP: fases y metodología. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Holm Security. (2025). ¿Qué es la base de datos Exploit-db? https://support-holmsecurity-com.translate.goog/knowledge/what-is-exploit-db-database?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wa

IBIS Computer. (2026). Qué hacer durante las primeras 24 horas tras un ciberataque. https://ibiscomputer.com/que-hacer-tras-un-ciberataque/

IBM. (s.f). Metodologías y estándares de pruebas de penetración. Recuperado el 27 de mayo de 2026, de https://www.ibm.com/mx-es/think/insights/pen-testing-methodology

ISECOM. (2010). OSSTMM 3. https://www.isecom.org/OSSTMM.3.pdf

López, M. M. (2024). Fases de un pentest. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

Lozano, P. A. (2023). Fases del pentesting: Pasos para asegurar tus sistemas. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

ManageEngine. (s.f.). ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)? Recuperado el 28 de mayo de 2026, de https://www.manageengine.com/es/cis-critical-security-controls/

MinCIT. (2012). Protección de datos personales. https://www.mincit.gov.co/minindustria/estrategia-transversal/regulacion/proteccion-de-datos-personales

MITRE. (2014). CVE-2014-6287. https://www.cve.org/CVERecord?id=CVE-2014-6287

Palo Alto Networks. (s.f). ¿Qué es SIEM? Recuperado el 28 de mayo de 2026, de https://www.paloaltonetworks.lat/cyberpedia/what-is-siem

PfSense. (s.f). Realice una visita guiada. Recuperado el 28 de mayo de 2026, de https://www.pfsense.org/getting-started/

Policia Nacional. (2009). Normatividad sobre delitos informáticos: Ley 1273 de 2009. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Randall, M. (2026). ¿Qué es la remediación en ciberseguridad y por qué es importante? https://onspring-com.translate.goog/resources/blog/what-is-remediation-in-cybersecurity-and-why-does-it-matter/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

RedHat. (2021). Los CVE. https://www.redhat.com/es/topics/security/what-is-cve

Sehga, K., & Thymianis, N. (2023). Cybersecurity Blue Team Strategies. Packt Publishing. https://books.google.com.co/books?hl=es&lr=&id=ojWxEAAAQBAJ&oi=fnd&pg=PP1&dq=blue+team+cyber+security&ots=5W9rlxU1dq&sig=-

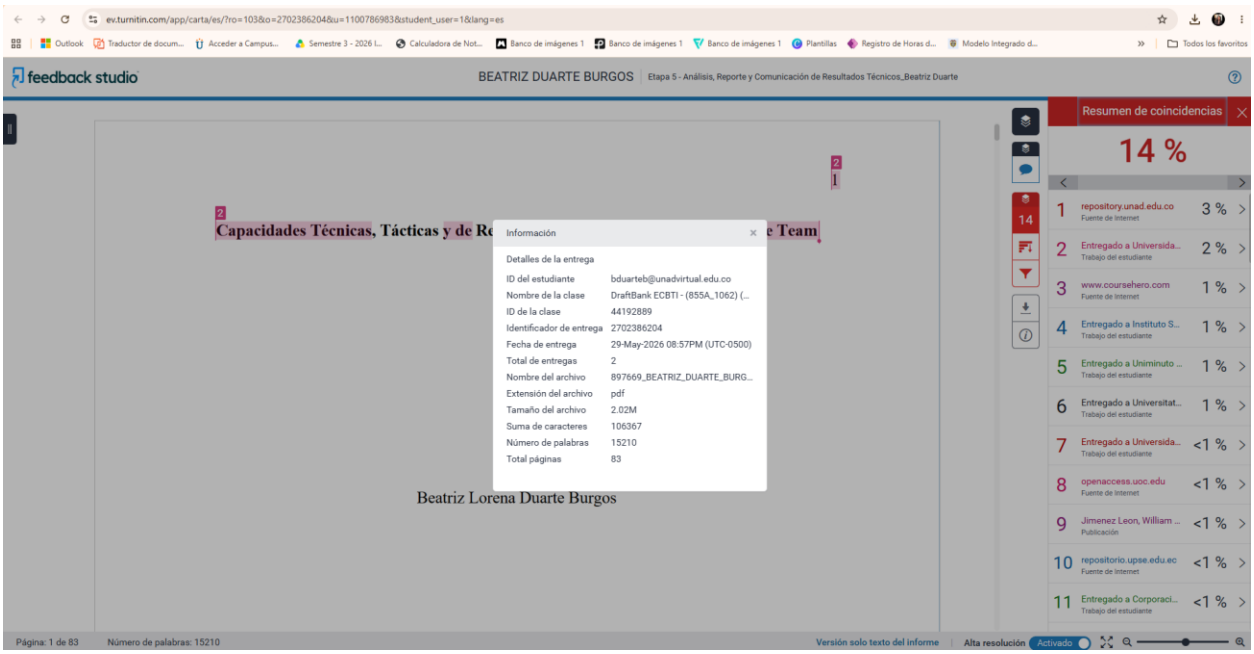
Tburml7bB2kIBCFKluOX5jNyZo&redir_esc=y#v=onepage&q=blue%20team%20cyber%20security&f=false

Wazuh. (s.f). Active Response. Recuperado el 28 de mayo de 2026, de https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Reporte de similitud generado mediante la herramienta Turnitin para la validación de originalidad del Informe Técnico Final. El resultado presentado corresponde a la versión final del documento sometida a revisión antes de su entrega y publicación en el repositorio institucional con un 14% de similitud.