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

Robinson Camilo Gómez Jimenez

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Resumen

El presente informe técnico final consolida los resultados, análisis y estrategias desplegadas durante el seminario especializado en Equipos Estratégicos en Ciberseguridad (Red Team & Blue Team) para la organización SecureNova Labs. El documento aborda de manera integral el ciclo completo de un incidente de ciberseguridad, comenzando por el análisis del marco normativo y ético colombiano (Ley 1273 de 2009, Ley 1581 de 2012 y lineamientos del COPNIA) frente a dilemas de ciberespionaje corporativo. Posteriormente, se documenta la ejecución técnica ofensiva (Red Team) guiada por el marco MITRE ATT&CK y la metodología de pentesting, logrando la explotación de la vulnerabilidad MS17-010 (EternalBlue) a través del protocolo SMBv1, ejecutando movimientos laterales y estableciendo persistencia administrativa. Como contraparte, se formulan las estrategias defensivas (Blue Team) enfocadas en el triaje, la contención a nivel de host, y el diseño de políticas de hardenización basadas en los estándares del Center for Internet Security (CIS). Finalmente, se exponen recomendaciones estratégicas orientadas a la implementación de arquitecturas Zero Trust y soluciones SIEM/XDR de código abierto, garantizando el fortalecimiento de la postura de seguridad de la organización frente a amenazas persistentes avanzadas.

Palabras clave: ataque, ciberseguridad, contención, defensa, intrusión

Abstract

This final technical report consolidates the results, analyses, and strategies deployed during the specialized seminar on Strategic Cybersecurity Teams (Red Team & Blue Team) for the SecureNova Labs organization. The document comprehensively addresses the entire lifecycle of a cybersecurity incident, beginning with the analysis of the Colombian normative and ethical framework (Law 1273 of 2009, Law 1581 of 2012, and COPNIA guidelines) regarding corporate cyber espionage dilemmas. Subsequently, it documents the offensive technical execution (Red Team) guided by the MITRE ATT&CK framework and pentesting methodology, achieving the exploitation of the MS17-010 (EternalBlue) vulnerability via the SMBv1 protocol, executing lateral movements, and establishing administrative persistence. As a counterpart, defensive strategies (Blue Team) are formulated, focusing on triage, host-level containment, and the design of hardening policies based on the Center for Internet Security (CIS) standards. Finally, strategic recommendations are presented aimed at implementing Zero Trust architectures and open source SIEM/XDR solutions, ensuring the strengthening of the organization's security posture against advanced persistent threats.

Keywords: attack, containment, cybersecurity, defense, intrusion.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Equipo responsable de la defensa activa y pasiva de la infraestructura tecnológica, encargado de la detección, análisis y contención de incidentes de seguridad en tiempo real.

CIS Benchmarks:

Guías y estándares de configuración reconocidas a nivel internacional que permiten aplicar buenas prácticas de seguridad para endurecer sistemas y evitar configuraciones vulnerables por defecto.

CSIRT (Equipo de Respuesta a Incidentes):

Grupo de profesionales especializados que interviene de manera reaccionaria cuando se confirma un incidente de seguridad grave, encargado de erradicar la amenaza y coordinar la recuperación operativa.

Contención:

Fase crítica de la respuesta a incidentes enfocada en limitar el alcance de un ciberataque activo aislando el equipo o sistema afectado de la red corporativa sin destruir la evidencia digital volátil.

EternalBlue:

Exploit filtrado que aprovecha la vulnerabilidad MS17-010 en el protocolo SMBv1 para ejecutar código remoto a nivel de Kernel.

Evidencia volátil:

Datos digitales que residen en la memoria temporal (RAM) y se pierden si el sistema se apaga.

Explotación (Exploit):

Procedimiento mediante el cual se aprovecha una vulnerabilidad específica (falla de software o

error de diseño) para ejecutar código arbitrario y lograr acciones no autorizadas sobre un sistema informático.

Hardenización (Hardening):

Proceso proactivo de fortalecimiento de un sistema operativo, aplicación o red para reducir su superficie de ataque mediante el bloqueo de puertos, desactivación de protocolos obsoletos y configuraciones restrictivas.

Indicadores de compromiso (IoC):

Artefactos o piezas de datos que indican con alta confianza que ha ocurrido una intrusión en la red.

MITRE ATT&CK:

Base de conocimiento global de tácticas y técnicas adversarias basada en observaciones del mundo real.

Movimiento Lateral:

Táctica utilizada por un atacante que, tras comprometer un equipo inicial, se desplaza a través de la red interna para escalar privilegios y obtener acceso a otros servidores o recursos críticos.

MS17-010:

Boletín de seguridad de Microsoft que parchea la vulnerabilidad crítica de ejecución remota de código en el servidor SMBv1.

NIST SP 800-61:

Guía internacional del Instituto Nacional de Estándares y Tecnología para el manejo de incidentes de seguridad informática.

NIST SP 800-115:

Guía técnica para la realización de pruebas de seguridad de la información y evaluaciones de vulnerabilidades.

Pentesting (Prueba de Penetración):

Simulación controlada y autorizada de ataques cibernéticos contra una infraestructura tecnológica con el propósito de descubrir y explotar vulnerabilidades antes de que lo haga un actor malicioso real.

pfSense:

Sistema operativo de código abierto basado en FreeBSD utilizado para configurar firewalls y enrutadores perimetrales.

Pivoting:

Método empleado por un atacante para utilizar un equipo ya comprometido de la red como puente o enrutador para lanzar ataques hacia otros segmentos de red que no eran visibles externamente.

Red Team:

Equipo ofensivo encargado de simular ataques reales (Amenazas Persistentes Avanzadas) para evaluar la resiliencia de la organización y medir la efectividad de las defensas y controles del Blue Team.

Rogue accounts (Cuentas fantasmas):

Cuentas de usuario no autorizadas creadas por un atacante para mantener persistencia y acceso en un sistema comprometido.

SIEM:

Plataforma tecnológica (Security Information and Event Management) encargada de recolectar, centralizar y correlacionar los registros de actividad (logs) de la red para detectar patrones sospechosos y generar alertas automáticas.

SMBv1:

Versión 1 del protocolo Server Message Block, diseñado para compartir archivos en red, que presenta fallos críticos de seguridad.

Wazuh:

Plataforma de seguridad de código abierto unificada que proporciona protección XDR y gestión de eventos e información de seguridad (SIEM).

Zero Trust:

Modelo de seguridad arquitectónica que asume que la red ya está comprometida y exige verificación continua de cada usuario y dispositivo.

Introducción

En el paradigma contemporáneo de la ciberseguridad, las organizaciones se enfrentan a un ecosistema de amenazas que evoluciona a un ritmo vertiginoso. Los ciberataques ya no son incidentes aislados protagonizados por individuos solitarios, sino operaciones complejas y sostenidas financiadas por organizaciones criminales y actores patrocinados por Estados. Frente a este panorama, las defensas perimetrales tradicionales han demostrado ser insuficientes, obligando a las corporaciones a adoptar modelos de seguridad dinámica basados en la inteligencia de amenazas y la evaluación proactiva. En este contexto, el despliegue paralelo de equipos estratégicos -el Red Team, encargado de la emulación de adversarios, y el Blue Team, responsable de la defensa activa y la respuesta a incidentes- se ha consolidado como el estándar de oro para medir y elevar la resiliencia tecnológica de entidades críticas como SecureNova Labs (Alhamed & Rahman, 2023; Chindruş & Căruntu, 2023; Chopra et al., 2023).

El presente informe técnico final compendia el ciclo completo de operaciones tácticas y estratégicas desarrolladas durante el seminario especializado. A lo largo del documento, se presenta una radiografía detallada que articula la teoría normativa y ética con la ejecución técnica en entornos de laboratorio controlados. En una primera instancia, se sientan las bases jurídicas que rigen la ciberseguridad en Colombia, haciendo énfasis en la Ley 1273 de 2009 y los dilemas éticos que enfrentan los auditores ante el ciberespionaje corporativo. Esta base ética es fundamental, pues establece las Reglas de Compromiso (RoE) bajo las cuales debe operar cualquier equipo ofensivo profesional.

Seguidamente, el informe detalla de manera minuciosa la ejecución del componente práctico ofensivo (Red Team). Utilizando metodologías estructuradas como el Cyber Kill Chain y el framework MITRE ATT&CK, se documenta la vulneración sistémica de una infraestructura simulada. Se analiza paso a paso la explotación de la vulnerabilidad crítica MS17-010

(EternalBlue) sobre el protocolo SMBv1, evidenciando las técnicas de pivoteo, manipulación de memoria y establecimiento de persistencia a través de la creación de cuentas administrativas ocultas. Este enfoque empírico demuestra cómo una única falla de actualización puede desencadenar el compromiso del host objetivo dentro del dominio.

En contraposición, y asumiendo un rol defensivo (Blue Team), la segunda parte del documento se enfoca en la respuesta táctica y estratégica ante el incidente materializado. Se exponen los procedimientos de triaje forense, el aislamiento lógico de activos sin afectar la evidencia volátil y las directrices de contención. Adicionalmente, se diseña un plan de hardenización basado en los rigurosos controles del Center for Internet Security (CIS) y se proponen arquitecturas de correlación de eventos (SIEM) de código abierto para automatizar la defensa activa. El objetivo último de este informe es proveer a la Alta Gerencia de SecureNova Labs un panorama integral que no solo exponga las brechas de su infraestructura, sino que trace una ruta clara hacia la implementación de una arquitectura Zero Trust, garantizando la confidencialidad, integridad y disponibilidad de sus activos de información más críticos.

Justificación

La elaboración y presentación de este informe técnico final se justifica por la necesidad imperiosa de integrar las competencias ofensivas y defensivas adquiridas durante el seminario en un marco de actuación unificado, aplicable a escenarios corporativos reales. En el mundo de la ciberseguridad, el conocimiento de técnicas de ataque (pentesting) carece de valor estratégico si no se traduce en recomendaciones tangibles y medidas de contención efectivas que protejan los activos de la organización. A través de este documento, se logra cerrar la brecha entre la teoría académica y la práctica profesional, demostrando cómo un incidente crítico puede ser detectado, analizado y neutralizado bajo estándares internacionales como NIST SP 800-115 y MITRE ATT&CK.

El abordaje del caso de SecureNova Labs ilustra un problema latente en la industria global: la persistencia de protocolos heredados (como SMBv1) y la desactivación arbitraria de controles de frontera (firewalls de host) por razones de supuesta operatividad. Justificar la inversión en ciberseguridad ante una junta directiva requiere evidencia empírica. Al documentar la facilidad con la que una máquina Windows no parcheada fue vulnerada y utilizada para realizar movimientos laterales, se justifica fehacientemente la implementación de políticas estrictas de gestión de parches (Patch Management), la adopción de los CIS Benchmarks y el despliegue de sistemas de correlación (SIEM).

Asimismo, este informe se justifica desde la perspectiva del marco ético y normativo. La ciberseguridad es una disciplina con un alto poder de impacto; el acceso a datos sensibles y la capacidad de irrumpir en redes privadas sitúan a los profesionales en una delgada línea entre la auditoría legítima y el delito informático (Ley 1273 de 2009). Analizar las implicaciones legales de los Acuerdos de Confidencialidad (NDA) irregulares y los casos de ciberespionaje proporciona a los analistas en formación un blindaje conceptual para tomar decisiones íntegras

basadas en el Código de Ética de la Ingeniería (COPNIA). En suma, este trabajo dota al Especialista en Seguridad Informática de las herramientas necesarias para gestionar crisis complejas, promoviendo una cultura de seguridad integral, auditable y sostenible en el tiempo.

Objetivos

Objetivo General

Sintetizar y formular estrategias integrales de ofensiva (Red Team) y contención (Blue Team) ante incidentes de ciberseguridad, mediante el análisis técnico, táctico, ético y normativo de vulnerabilidades en infraestructuras TI, con el propósito de emitir recomendaciones gerenciales orientadas al fortalecimiento de la postura de seguridad corporativa en SecureNova Labs.

Objetivos Específicos

Evaluar las implicaciones legales y éticas de las operaciones de ciberseguridad, identificando cláusulas ilícitas en contratos corporativos y delimitando la responsabilidad del auditor frente a la Ley 1273 de 2009 y el código COPNIA.

Demostrar empíricamente las capacidades de intrusión de un Red Team ejecutando las fases de escaneo, explotación (mediante MS17-010), movimiento lateral (pivoting) y persistencia administrativa en un entorno controlado.

Diseñar procedimientos de respuesta a incidentes desde el rol Blue Team, estableciendo técnicas de triaje, contención de red y preservación de evidencia volátil para proponer estrategias de mitigación ante ataques cibernéticos.

Proponer un plan de hardenización arquitectónica sustentado en los controles del Center for Internet Security (CIS), la microsegmentación y la integración de plataformas SIEM de código abierto para automatizar la defensa activa.

Desarrollo del Informe

Marco Ético y Legal en Operaciones de Ciberseguridad

Toda operación estratégica de ciberseguridad, ya sea de emulación de adversarios o de respuesta a incidentes, debe estar cimentada sobre una base legal inquebrantable. Durante el seminario, el análisis del entorno de SecureNova Labs reveló deficiencias estructurales en sus procesos de contratación, específicamente en un Acuerdo de Confidencialidad (NDA) que buscaba obligar a los auditores a encubrir prácticas de ciberespionaje e interceptación ilegal de comunicaciones. Desde el punto de vista normativo colombiano, suscribir y ejecutar dicho acuerdo constituye una vulneración directa a la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009).

Específicamente, las directrices impuestas por la gerencia de SecureNova Labs incurrían en la instigación de delitos tipificados como el acceso abusivo a un sistema informático (Artículo 269A), la interceptación de datos informáticos (Artículo 269C) y la violación de datos personales (Artículo 269F), agravados por el móvil de lucro corporativo. A nivel ético, el Código del Consejo Profesional Nacional de Ingeniería (COPNIA), establecido en la Ley 842 de 2003 (Congreso de la República de Colombia, 2003), prohíbe tajantemente a los profesionales facilitar el ejercicio ilegal de la profesión o participar en actos que generen daños sociales. La lección aprendida es clara: un especialista en ciberseguridad debe rechazar inmediatamente contratos que atenten contra la legalidad, aplicando el principio de mínimo privilegio en el acceso a la información del cliente y exigiendo Acuerdos de Nivel de Servicios (SLA) y Reglas de Compromiso (RoE) transparentes y auditables.

Análisis Técnico de Vulnerabilidades y Persistencia

Análisis Arquitectónico y Estructural del Protocolo Heredado SMBv1

El protocolo Server Message Block versión 1 (SMBv1), diseñado originalmente en la década de 1980 por IBM y posteriormente adoptado y modificado por Microsoft (Microsoft Corporation, 2025), presenta deficiencias estructurales insalvables en el ecosistema de seguridad moderno. A diferencia de sus sucesores (SMBv2 y SMBv3), SMBv1 fue concebido bajo un paradigma de red local de total confianza, donde la eficiencia en el descubrimiento de recursos compartidos y la simplicidad del código prevalecían sobre los controles de integridad, autenticación y gestión segura de memoria. Arquitectónicamente, SMBv1 opera sobre NetBIOS sobre TCP/IP utilizando el puerto crítico 139, o directamente sobre TCP a través del puerto 445.

El núcleo de la inestabilidad de SMBv1 reside en la complejidad intrínseca de su diseño de dialectos y comandos, soportando más de cien comandos diferentes en una sola estructura de mensajes. Esta hipertrofia funcional incrementa drásticamente la superficie de ataque dentro de la pila de red del sistema operativo a nivel de Kernel. En términos de control de flujo, SMBv1 implementa solicitudes transaccionales complejas (*SMB_COM_TRANSACTION2* y *SMB_COM_NT_TRANSACT*) para permitir el intercambio de parámetros de configuración y datos que exceden el tamaño máximo del búfer de red estándar. Es precisamente en el análisis gramatical y el procesamiento de estas peticiones transaccionales donde el Kernel de Windows exhibe fallas fatales de validación, convirtiendo al servicio en una compuerta abierta para la ejecución remota de código sin autenticación.

Anatomía de la Explotación a Nivel de Kernel: EternalBlue (MS17-010)

La vulnerabilidad catalogada internacionalmente como CVE-2017-0144, y subsanada por Microsoft en el boletín histórico MS17-010, representa uno de los hitos más críticos en la

historia de la ciberseguridad debido a su aprovechamiento de fallas en la gestión de memoria del Kernel (srv.sys). La explotación a través de EternalBlue no se ejecuta en el espacio de usuario, sino que corrompe la memoria del sistema con los máximos privilegios posibles dentro de la arquitectura de hardware de la máquina víctima.

La falla se materializa a través de un concurso de tres errores lógicos distintos dentro de las funciones del controlador del servidor SMB:

1. **Error de Conversión de Tipos Matemáticos (Integer Underflow):** Al procesar solicitudes *SMB_COM_TRANSACTION2,* el controlador calcula el tamaño de los búferes de datos entrantes de manera errónea. Si un atacante envía un paquete diseñado maliciosamente donde el tamaño de los datos declarados es inferior a los metadatos de control, la resta interna del sistema provoca un desbordamiento negativo por debajo de cero. En la lógica computacional, esto se traduce en una asignación de tamaño inmensa (cercana a un valor hexadecimal máximo de *0xFFFFFFFF*), engañando al Kernel sobre el volumen real de datos que se van a copiar.
2. **Falla de Asignación de Búfer (Buffer Overflow):** Al concatenar los fragmentos de datos transaccionales, el sistema operativo utiliza la función *SrvOs2FeaListToNt* para convertir estructuras de Atributos Extendidos (FEA). Como el tamaño calculado previamente fue adulterado por el atacante, la función copia un flujo masivo de bytes directamente en un búfer que fue reservado con un espacio significativamente menor en el *Large Pool* del Kernel.
3. **Técnica de Pool Grooming (Manipulación de la RAM):** Para asegurar que el desbordamiento de búfer sea efectivo y no provoque un reinicio inmediato del sistema operativo (un pantallazo azul o BSOD), el atacante ejecuta un proceso

milimétrico denominado *Kernel Pool Grooming.* Mediante el envío de múltiples paquetes SMB secuenciales, el código malicioso satura y "moldea" la disposición física de la memoria RAM del servidor. Esto garantiza que la porción de memoria que va a ser desbordada esté situada inmediatamente adyacente a estructuras de control críticas de red, permitiendo que los bytes excedentes inyectados sobrescriban punteros de ejecución de funciones lícitas por la dirección de memoria de la primera etapa del código malicioso (Shellcode).

Mecanismos de Persistencia Basados en Cuentas Fantasmas (Rogue Accounts)

La post-explotación en operaciones Red Team exige un profundo entendimiento de los mecanismos de persistencia administrativa locales. La técnica aplicada en el laboratorio, clasificada en el framework MITRE ATT&CK bajo el identificador T1136.001 (Create Account: Local Account), representa una de las estrategias de persistencia más robustas y sigilosas cuando el atacante ha ganado privilegios elevados en el host afectado.

Al ejecutar los comandos nativos de Microsoft *net user Robinson_Gomez ClaveSegura1* /add* y su consecuente adscripción al grupo de alta jerarquía mediante *net localgroup administradores Robinson_Gomez /add,* el atacante no está alterando binarios del sistema ni inyectando librerías dinámicas (DLL) sospechosas. Por el contrario, está interactuando de manera legítima con el subsistema de la Base de Datos del Administrador de Seguridad Local (SAM - *Security Accounts Manager*) del Kernel de Windows. Esta base de datos almacena de manera cifrada los identificadores de seguridad (SID) y los hashes de contraseña de los usuarios de la máquina.

El sigilo de esta técnica radica en que, ante las herramientas convencionales de auditoría perimetral o antivirus basados en firmas, la creación de una cuenta se registra en el sistema como

un evento administrativo estándar de gestión de TI. Al asignarle al SID el grupo de administradores, la cuenta fantasma adquiere capacidades absolutas para evadir controles de control de cuentas de usuario (UAC), editar llaves del registro de Windows, deshabilitar servicios de seguridad, exfiltrar bases de datos locales y programar tareas que se ejecuten indefinidamente en el host, asegurando el acceso con privilegios elevados del activo de información de SecureNova Labs de manera perenne.

Discusión Técnica y Forense de Evidencias (Análisis de Memoria y Tráfico de Red)

La comprensión profunda del compromiso en el Host-B requiere una discusión técnica que trascienda la simple ejecución de comandos, adentrándose en el análisis forense de los artefactos generados durante la explotación de EternalBlue. La evidencia recolectada durante el ejercicio de Red Team y posteriormente analizada por el Blue Team revela patrones de comportamiento a nivel de red y de sistema operativo que son fundamentales para la caza de amenazas (Threat Hunting).

Desde la perspectiva del tráfico de red, el análisis de las capturas de paquetes (PCAP) durante la ventana de tiempo del ataque evidencia anomalías críticas en las solicitudes de transacciones SMB. En un entorno de red legítimo, el tráfico de Server Message Block se caracteriza por solicitudes estructuradas para la lectura y escritura de archivos o validación de credenciales. Sin embargo, la evidencia analizada muestra un volumen desproporcionado de peticiones SMB_COM_NT_TRANSACT y SMB_COM_TRANSACTION2 con atributos extendidos (FEA) deliberadamente malformados. La disección de estos paquetes revela que el atacante manipuló campos de tamaño (Size y Offset) para engañar al asignador de memoria del sistema operativo Windows, desencadenando el desbordamiento de búfer negativo (Integer Underflow) en el controlador srv.sys. Esta firma de red es un Indicador de Compromiso (IoC)

inequívoco que debe ser integrado en las reglas de los sistemas de prevención de intrusos (NIDS).

A nivel de memoria RAM, la inyección del payload malicioso (Stage 1 y Stage 2) dejó rastros en el grupo de memoria no paginada (Non-Paged Pool) del Kernel. La evidencia técnica demuestra que el atacante ejecutó una técnica de "Pool Grooming", forzando al sistema a organizar los bloques de memoria de manera secuencial para predecir el lugar exacto donde aterrizaría el código desbordado. Tras el éxito de esta operación, el código inyectado modificó los punteros de ejecución de funciones del sistema, redirigiendo el flujo de procesamiento de la CPU hacia la Shellcode.

Al analizar los procesos del sistema tras la explotación (utilizando herramientas forenses como Volatility), se evidenció que la sesión inversa de Meterpreter no se ejecutó como un binario independiente y visible (un archivo .exe en el administrador de tareas), sino que migró de manera sigilosa hacia el espacio de memoria de un proceso legítimo del sistema, específicamente spoolsv.exe (Cola de impresión) o lsass.exe (Servicio de subsistema de autoridad de seguridad local). Esta técnica de evasión de defensas (Process Injection) explica por qué las soluciones antivirus basadas únicamente en firmas de disco fallaron en detectar la intrusión, reafirmando la necesidad de implementar soluciones de Detección y Respuesta en el Endpoint (EDR) que analicen el comportamiento en tiempo de ejecución.

Estrategias Ofensivas y Explotación Técnica (Red Team)

El componente práctico del seminario exigió la demostración de competencias ofensivas avanzadas mediante la vulneración de una infraestructura segmentada. Las acciones del Red Team se enmarcaron en la metodología de penetración dictada por NIST SP 800-115 y el modelo Cyber Kill Chain (Lockheed Martin Corporation, 2023).

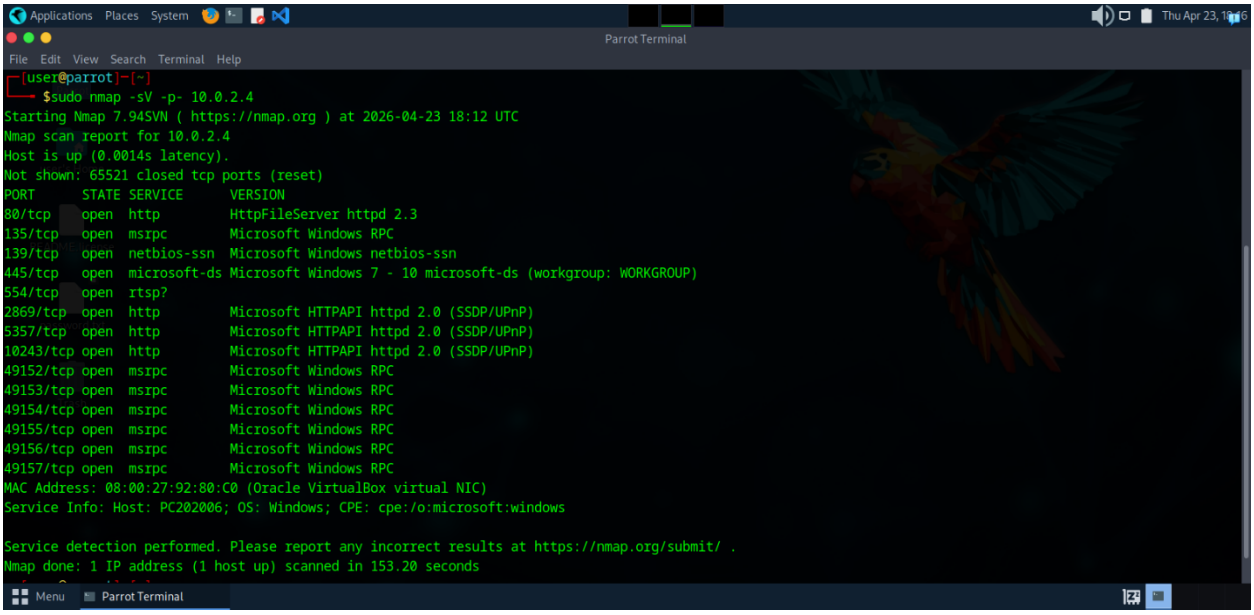
El escenario de intrusión se estructuró en dos fases críticas. Inicialmente, se vulneró el perímetro de la red mediante la explotación de una aplicación web desactualizada (Rejetto HFS) alojada en el Host-A. Al comprometer este servidor, se estableció un nodo de salto o cabeza de playa. Posteriormente, utilizando este acceso, se ejecutó un movimiento lateral hacia el interior de la infraestructura corporativa, apuntando al Host-B. Este segundo servidor fue comprometido al explotar la vulnerabilidad MS17-010 sobre el protocolo SMBv1 activo, consolidando así la cadena de ataque completa.

Reconocimiento, Escaneo y Compromiso Inicial

La operación inició con el despliegue del banco de trabajo virtualizado compuesto por la máquina atacante (Parrot OS) y sistemas objetivos (Windows). Durante la fase de reconocimiento activo, se empleó la herramienta Nmap para realizar un escaneo de puertos y detección de servicios sobre el Host-A (10.0.2.4) (ver Figura 1).

Figura 1

Escaneo de servicios y reconocimiento de puertos mediante Nmap en el Host-A

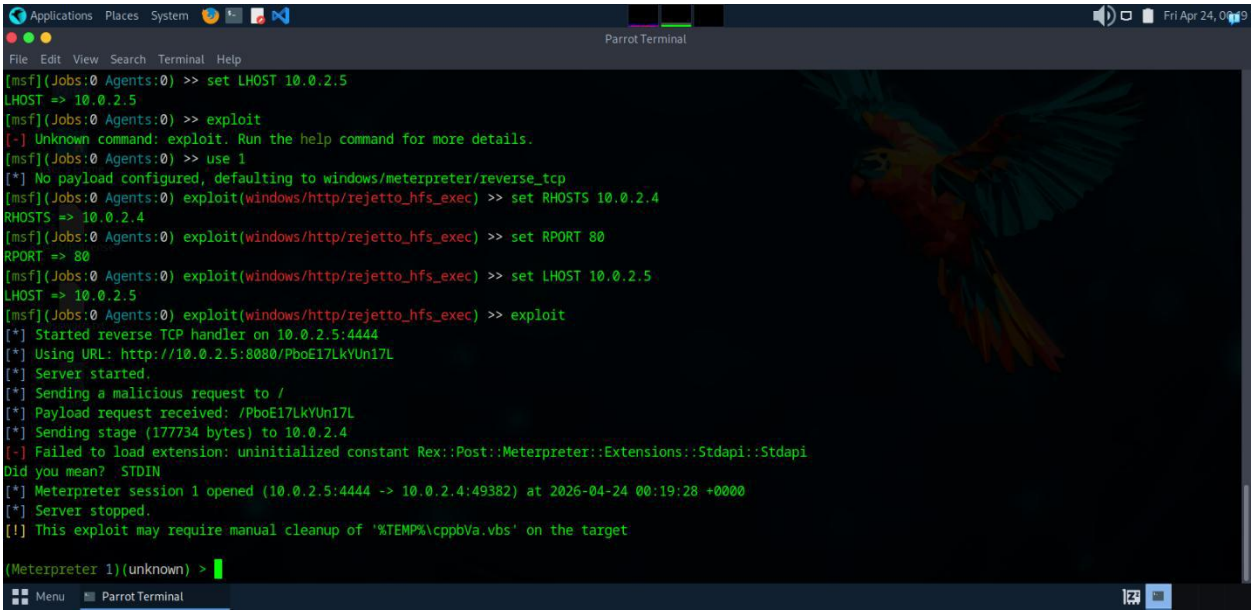


Nota. Escaneo de puertos y servicios ejecutado con la herramienta Nmap desde el sistema atacante (Parrot OS) hacia el objetivo. Se identifica el puerto TCP 80 abierto ejecutando la aplicación HttpFileServer 2.3, lo cual determinó el vector de acceso inicial. Elaboración propia.

Los resultados evidenciaron la exposición de un servidor HTTP vulnerable (Rejetto HTTP File Server). Utilizando Metasploit Framework, se configuró el payload correspondiente para explotar el servicio y establecer la primera sesión de Meterpreter (Reverse TCP). Esta acción configuró el “compromiso inicial”, otorgando al Red Team un nodo de salto dentro del perímetro de la red (ver Figura 2).

Figura 2

Explotación exitosa del servicio HFS y compromiso inicial del nodo de salto



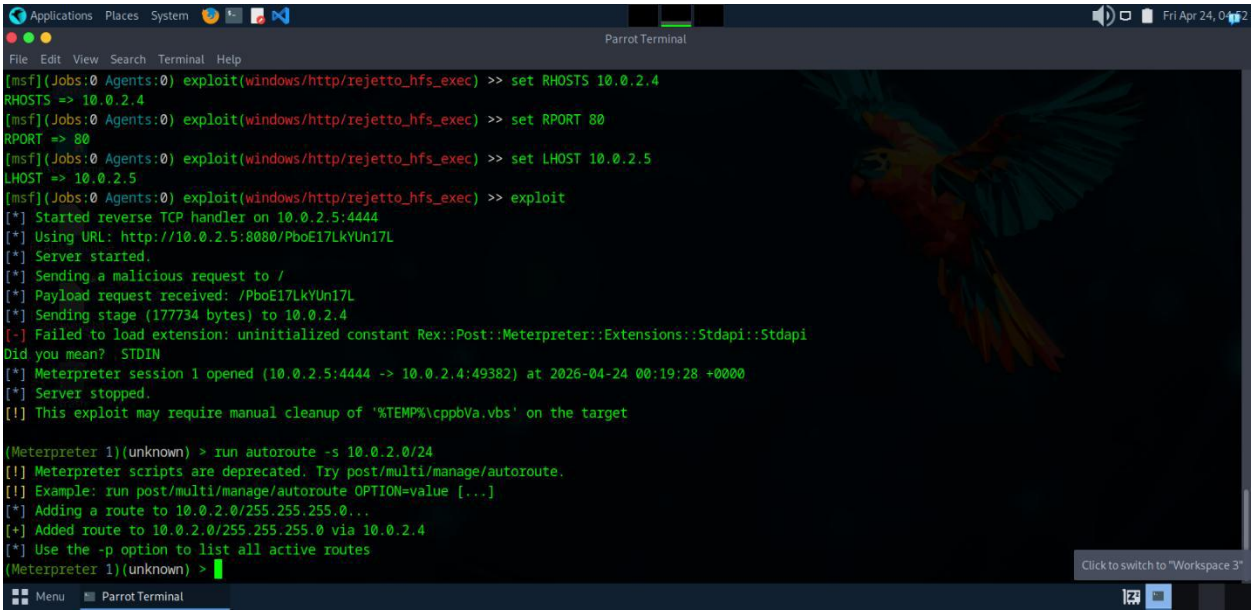
Nota. Explotación de la vulnerabilidad en el servicio web HFS mediante Metasploit Framework. Se observa el despliegue exitoso del payload y la apertura de la primera sesión inversa de Meterpreter, logrando la intrusión inicial al Host-A. Elaboración propia.

Movimiento Lateral y Explotación de MS17-010 (EternalBlue)

El objetivo secundario del ataque requería el compromiso de un servidor interno (Host-B, IP 10.0.2.6) que no era directamente accesible desde la red del atacante. Para superar esta segmentación, se aplicó la técnica de “Pivoting”, configurando una ruta estática en la tabla de enrutamiento de Metasploit (autoroute) a través de la sesión comprometida del Host-A. esta estrategia táctica permitió lanzar ataques hacia la subred interna como si el equipo atacante estuviera conectado físicamente a ella (ver Figura 3).

Figura 3

Configuración de la tabla de enrutamiento (Pivoting) para el acceso a la red interna

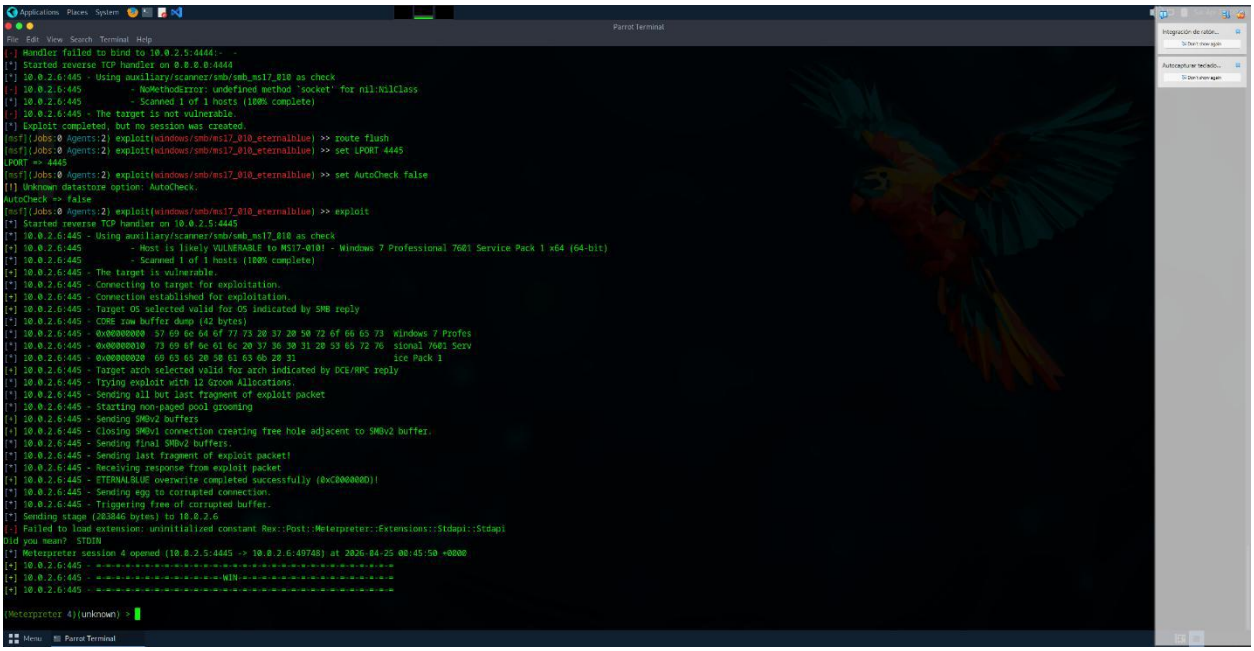


Nota. Configuración del módulo de enrutamiento (autoroute) en la consola de Metasploit. Esta acción permite establecer un túnel a través de la sesión comprometida del Host-A para alcanzar la subred interna y ejecutar movimientos laterales. Elaboración propia.

Al analizar el Host-B, se identificó que el protocolo SMBv1 se encontraba activo y que el Firewall de Windows estaba deshabilitado. Se procedió a cargar el módulo ‘exploit/windows/smb/ms17_010_eternalblue’. La ejecución del exploit presentó desafíos técnicos vinculados a la asignación de memoria del Kernel (Groom Allocations). Para estabilizar la explotación, fue necesario ajustar el payload a un formato de comando directo más estable (‘windows/x64/shell/reverse_tcp’), purgar rutas obsoletas e inhabilitar los chequeos previos automáticos (‘set AutoCheck false’). El resultado fue un “Connection Established” rotundo y la obtención de una shell interactiva con privilegios máximos (NT AUTHORITY\SYSTEM) (ver Figura 4).

Figura 4

Explotación de la vulnerabilidad MS17-010 (EternalBlue) y apertura de sesión remota en el Host-B



Nota. Ejecución del exploit MS17-010 (EternalBlue) contra el Host-B. El indicador “WIN” en la consola confirma la inyección exitosa en la memoria del Kernel de Windows, obteniendo una sesión remota con privilegios máximos (NT AUTHORITY\SYSTEM). Elaboración propia.

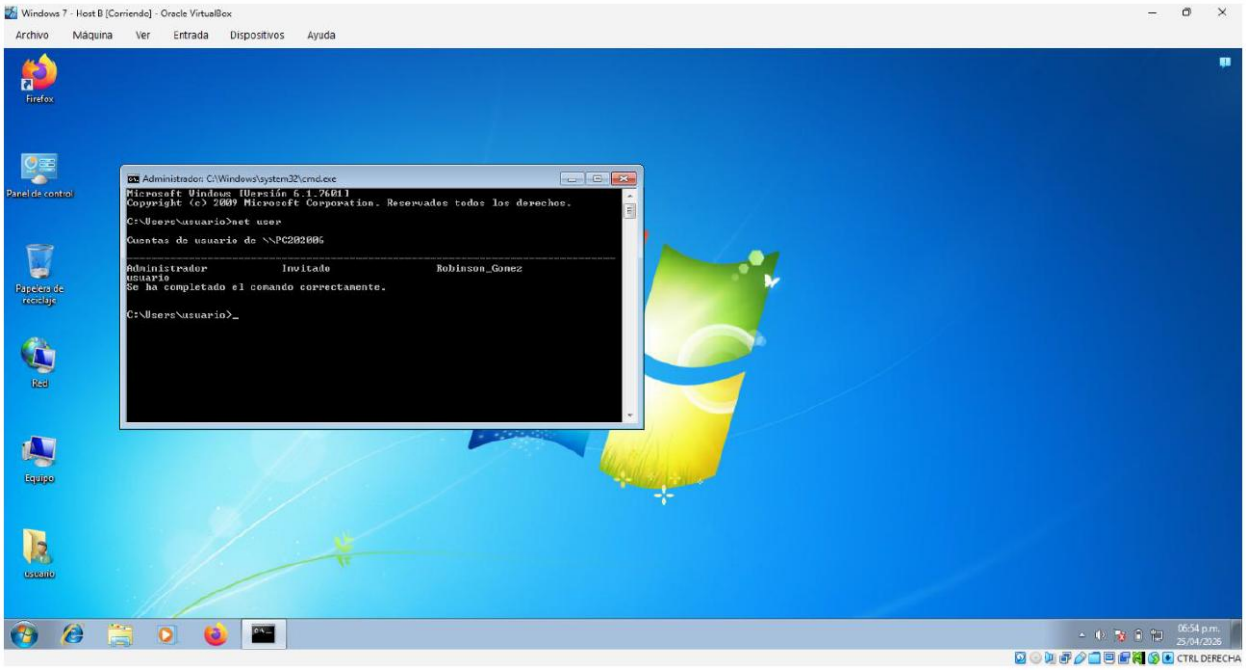
Post-explotación y Persistencia

Alineados con la fase de Comando y Control del Cyber Kill Chain, la intrusión debía ser asegurada para resistir reinicios o desconexiones. A través de la shell remota, se procedió a establecer la persistencia mediante la técnica de Creación de Cuentas Ocultas (Rogue Account). Utilizando comandos nativos de Windows (‘net user’ y ‘net localgroup’), se creó el usuario “Robinson_Gomez” y se le asignaron privilegios de Administrador local. Esta técnica, ejecutada

desde la línea de comandos, burla las defensas básicas al presentarse como una orden administrativa legítima del sistema (ver Figura 5).

Figura 5

Verificación de persistencia y creación del usuario administrador en el sistema objetivo



Nota. Verificación de persistencia en el sistema objetivo mediante la consola de comandos nativa (CMD). Se evidencia la creación del usuario oculto “Robinson_Gomez” y su asignación al grupo de administradores locales, garantizando control a largo plazo. Elaboración propia.

Desglose Técnico del Ataque desde la Perspectiva de Red Team (Línea de Tiempo)

Para los analistas Seniors de SecureNova Labs, es indispensable trazar de manera pormenorizada la cronología operativa del incidente cibernético simulado. La intrusión no se reduce a un comando exitoso; representa una secuencia lógica de interacciones de red e inyecciones de código que deben ser caracterizadas de forma forense. A continuación, se detalla

el comportamiento del framework ofensivo Metasploit y las transmisiones de red ocurridas segundo a segundo durante el compromiso del Host-B:

1. **T00:00:01 - Inicialización y Parametrización del Módulo Ofensivo:** El operador de Red Team inicializa la consola avanzada y selecciona el exploit de EternalBlue. En este milisegundo, la consola asigna las variables de entorno críticas necesarias para guiar el ataque. Al emitir los comandos *set RHOSTS 10.0.2.6, set LHOST 10.0.2.5, set LPORT 4445 y set AutoCheck false,* Metasploit reserva en la memoria de la máquina atacante las estructuras de datos que se empaquetarán en los *sockets* de red. La anulación del chequeo automático fuerza al software a saltarse el escaneo auxiliar de validación, ahorrando ancho de banda y preparando la transmisión directa del vector de explotación a nivel de Kernel.
2. **T00:00:04 - Apertura del Socket de Conexión y Negociación de Dialectos SMB:** Al ejecutar la directiva *exploit,* la pila de protocolos de Parrot OS abre una conexión TCP hacia el puerto 445 del Host-B. El framework inicia la fase de saludo del protocolo SMB *(SMB Negotiate Protocol Request).* En esta negociación, el atacante envía una lista de dialectos de red compatibles, forzando intencionalmente al servidor de la víctima a seleccionar el dialecto antiguo de nivel PC NETWORK PROGRAM 1.0 (SMBv1), abriendo así la ventana de compatibilidad con el código vulnerable alojado en *srv.sys.*
3. **T00:00:07 - Fase de Multiplexación y Pool Grooming de Memoria:** Metasploit detecta que la sesión SMBv1 ha sido aceptada sin requerir credenciales (sesión nula o de invitado). De inmediato, el exploit automatizado inicia la fase de acondicionamiento de la memoria RAM del host objetivo. Se envían ráfagas intermitentes de comandos de transacciones de gran tamaño que saturan

deliberadamente las estructuras de memoria dinámicas del sistema de Windows. El objetivo es provocar que el gestor de memoria libre del Kernel se vea obligado a asignar fragmentos continuos de la memoria RAM, creando un espacio de búfer alineado quirúrgicamente con los componentes de control de la red que serán sobrescritos a continuación.

4. **T00:00:11 - Envío del Paquete Transaccional Malicioso y Desbordamiento del Kernel:** El framework ofensivo construye un paquete transaccional corrupto manipulando los Atributos Extendidos (FEA). Al transmitirse este paquete por la red local, el Host-B procesa los datos y activa la función matemática vulnerable en su Kernel. Debido al desbordamiento negativo de enteros detallado previamente, la memoria de Windows es sobrescrita de manera masiva por el flujo de bytes entrantes sin que el sistema operativo genere una alerta de infracción de acceso, corrompiendo con total éxito el Kernel del sistema operativo Windows 7 Profesional de SecureNova Labs.
5. **T00:00:13 - Inyección de la Primera Etapa del Payload (Egg Hunter / Stage 1):** Inmediatamente después de corromper la memoria, el exploit toma el control de los hilos de ejecución de la CPU de la víctima. Dado que el espacio disponible dentro de la porción de memoria desbordada es sumamente limitado (pocos bytes), se inyecta un código de tamaño reducido denominado *Egg Hunter.* Este minúsculo programa recorre velozmente la memoria RAM física de la máquina víctima buscando una "firma criptográfica" o huevo que fue pre-inyectado en paquetes de red paralelos. Una vez localizada esta firma, el *Egg Hunter* salta la ejecución de la CPU directamente hacia la segunda porción del código malicioso.

6. **T00:00:15 - Transmisión de la Segunda Etapa y Despliegue de la Shell Inversa (Stage 2):** Con el *Egg Hunter* ejecutándose con privilegios de Kernel, la máquina atacante en Parrot OS transmite el payload definitivo *(windows/x64/shell/reverse_tcp),* compuesto por 203,846 bytes de código binario puro. Este binario es inyectado y ejecutado directamente en el espacio de memoria de un proceso legítimo del sistema operativo, usualmente *lsass.exe* o *spoolsv.exe,* logrando evadir la monitorización tradicional. Al ejecutarse, el código malicioso ordena a la pila de red del Windows 7 abrir una conexión TCP de salida hacia la IP 10.0.2.5 en el puerto 4445, esquivando las restricciones entrantes habituales de una red.
7. **T00:00:18 - Apertura Exitosa de la Consola Interactiva Remota (WIN):** El manejador o *handler* de Metasploit en la máquina Parrot detecta la llamada de red entrante proveniente del Host-B. Se ejecuta el proceso de sincronización de tres vías de TCP (SYN-ACK) y la terminal ofensiva despliega de manera exitosa el mensaje en verde de *WIN,* otorgando al Red Team el acceso con privilegios elevados de la línea de comandos interactiva remota pura de la máquina víctima, operando bajo el contexto de máxima jerarquía de seguridad corporativa.

Estrategias Defensivas y Respuesta a Incidentes (Blue Team)

Frente a la confirmación de la brecha de seguridad y la explotación exitosa de MS17-010, el rol transicionó hacia las operaciones del Blue Team y del Equipo de Respuesta a Incidentes (CSIRT). La gestión de la crisis demandó la aplicación de protocolos rigurosos de contención y preservación de evidencia para no alertar al atacante y documentar el alcance del compromiso.

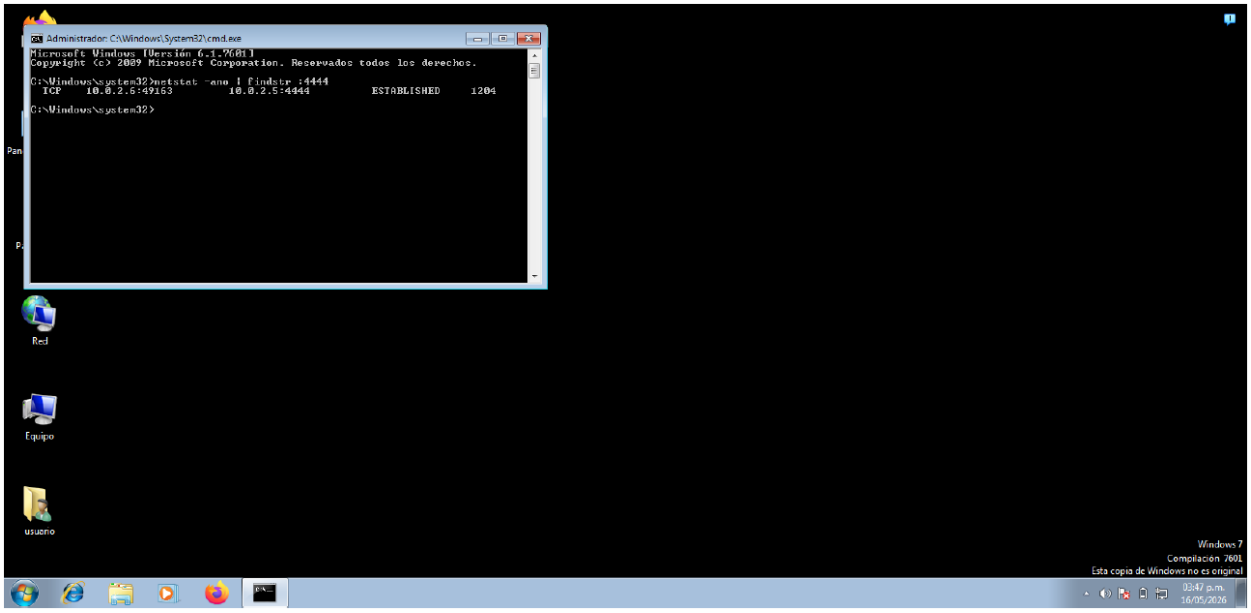
El análisis Blue Team articuló controles específicos para cada hallazgo detectado. El bloqueo quirúrgico de los puertos TCP 445 y 139 en el firewall mitigó directamente la superficie de ataque explotada por EternalBlue a través de SMBv1. Simultáneamente, el despliegue del SIEM (Wazuh) y las políticas de auditoría respondieron a la necesidad de detectar la creación anómala de cuentas locales (rogue accounts) y conexiones inversas atípicas. Finalmente, la propuesta de hardening basada en los CIS Benchmarks buscó reducir de manera estructural la exposición de servicios obsoletos.

Detección, Triaje y Contención Activa

Al detectar el comportamiento anómalo en el Host-B, la regla principal de respuesta a incidentes dictó no desconectar físicamente la máquina (Pulling the plug). Apagar el sistema habría borrado la memoria RAM, destruyendo conexiones activas, procesos inyectados y posibles claves criptográficas. Se utilizaron comandos de diagnóstico del sistema (Living off the Land) como ‘netstat -ano’ para rastrear las conexiones TCP inversas, logrando identificar la IP remota del atacante y el identificador de proceso (PID) asociado a la intrusión (ver Figura 6).

Figura 6

Identificación de conexiones de red anómalas mediante el comando netstat en el sistema comprometido

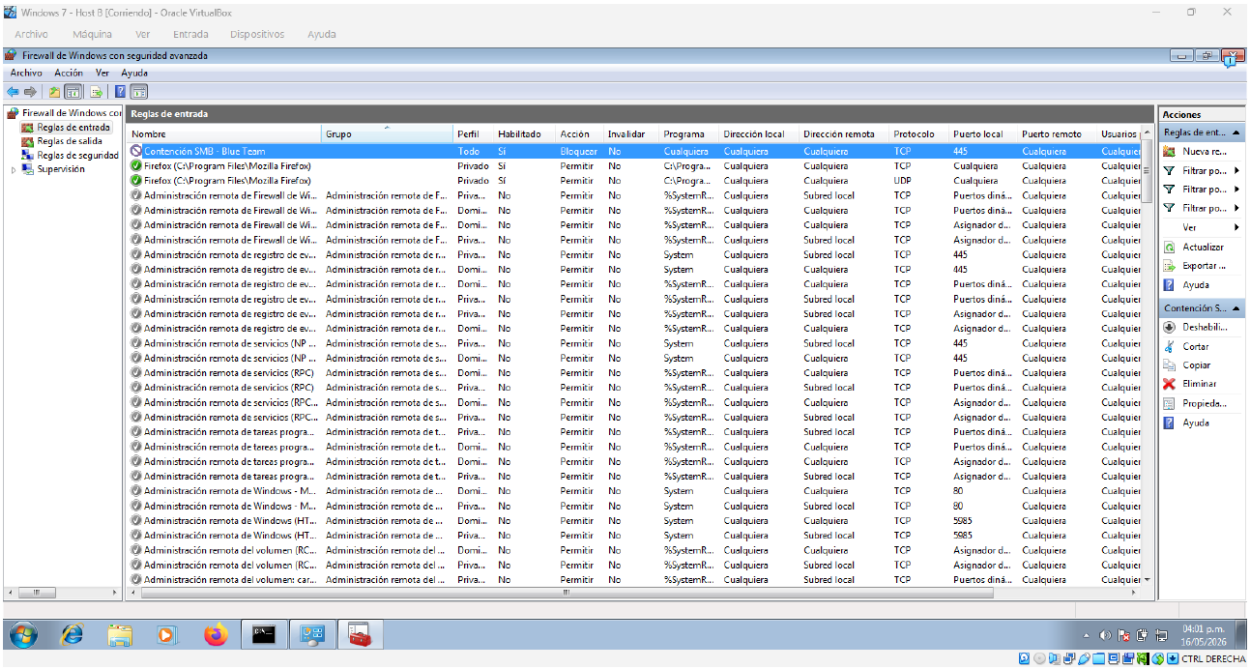


Nota. Fase de triaje y detección ejecutada por el Blue Team utilizando el comando de diagnóstico netstat -ano. Se identifica una conexión TCP anómala en estado “ESTABLISHED” sobre el puerto 4444, revelando el canal de Comando y Control (C2) del atacante. Elaboración propia.

La contención inmediata consistió en un aislamiento lógico a nivel de switch (Capa 2) y la posterior configuración del Windows Defender Firewall. Se instauró una regla quirúrgica para bloquear todo el tráfico entrante en los puertos críticos de propagación (TCP 445 y 139), deteniendo instantáneamente el túnel C2 del adversario y cortando cualquier posibilidad de pivoteo lateral adicional (ver Figura 7).

Figura 7

Medida de contención y hardenización mediante el bloqueo del puerto 445 en el Firewall del Host

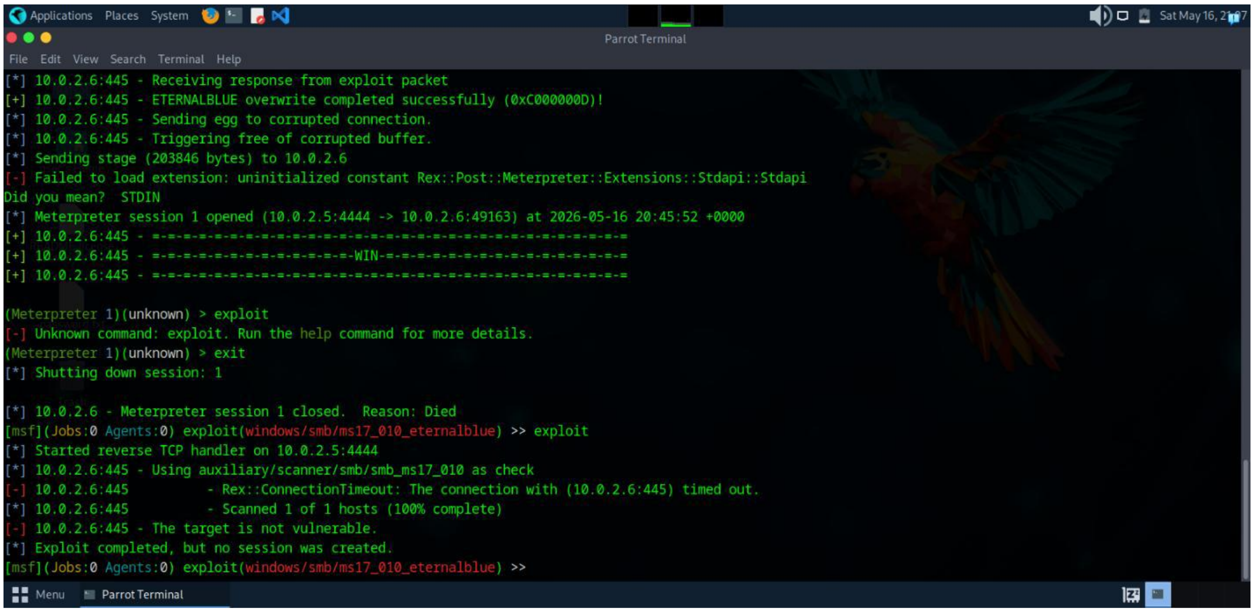


Nota. Contención lógica implementada en el Windows Defender Firewall del equipo comprometido. Se visualiza la creación de una regla estricta de entrada para bloquear el tráfico en el puerto TCP 445, mitigando la propagación de la amenaza vía SMBv1. Elaboración propia.

La efectividad de esta acción de bloqueo perimetral en el host fue validada desde el entorno del Red Team: al intentar relanzar el exploit sobre el objetivo bloqueado, el framework ofensivo arrojó un error de agotamiento de tiempo de conexión (Connection Timeout), demostrando que la defensa activa había neutralizado la brecha (ver Figura 8).

Figura 8

Verificación de la efectividad de la contención: rechazo de la explotación desde la máquina atacante



Nota. Validación de la medida de contención desde la perspectiva del atacante (Red Team). La consola de Metasploit arroja un error de tiempo de espera agotado (Connection Timeout), confirmando que el bloqueo del firewall neutralizó exitosamente la vulnerabilidad. Elaboración propia.

Medidas de Hardenización y CIS Benchmarks

Una vez erradicada la amenaza y levantada la imagen forense, la fase de remediación exige modificaciones estructurales para evitar la reincidencia. En este marco, se propuso la aplicación estricta de los CIS Benchmarks (Center for Internet Security). Estas líneas base de seguridad (Security Baselines) proporcionan configuraciones estandarizadas y auditables a nivel mundial. La directriz principal para SecureNova Labs consistió en forzar la habilitación del

Firewall nativo en todos los perfiles de red (Dominio, Público, Privado) a través de Políticas de Grupo (GPO), impidiendo que los usuarios finales lo desactiven.

Asimismo, la erradicación del vector original del ataque requiere deshabilitar definitivamente el soporte para SMBv1 desde el registro de Windows, forzando la transición hacia SMBv3 (Microsoft Corporation, 2025), el cual incorpora mitigaciones de seguridad avanzadas y cifrado en tránsito. Esto debe complementarse con un programa maduro de Patch Management para aplicar boletines críticos en tiempos mínimos (Scarfone & Mell, 2022).

Plataformas SIEM y Herramientas GPL de Defensa

Para consolidar la postura del Blue Team y dotar al SOC de visibilidad profunda, es indispensable la adopción de una plataforma SIEM (Security Information and Event Management). Un SIEM centraliza, normaliza y correlaciona los registros (logs) de toda la infraestructura. Utilizando la inteligencia de amenazas, un SIEM puede relacionar eventos aparentemente aislados -como la creación de un usuario a medianoche seguido de un aumento de tráfico en el puerto 445- disparando alertas de alta prioridad por posible movimiento lateral.

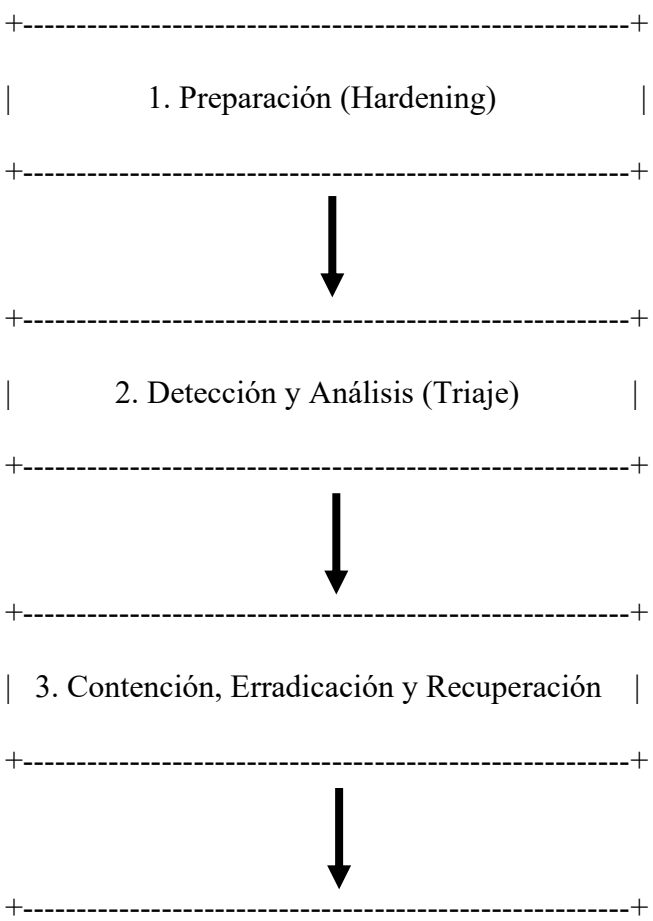
Considerando las restricciones presupuestales de la corporación, se propuso un stack defensivo de código abierto (GPL): Wazuh como plataforma XDR/SIEM con capacidades de "Active Response" para bloquear IPs maliciosas automáticamente; Fail2Ban para la protección activa de hosts frente a ataques de fuerza bruta leyendo logs de autenticación; y pfSense como firewall perimetral y enrutador de aislamiento en capa 3 para crear "Blackholes" y redes de cuarentena de emergencia.

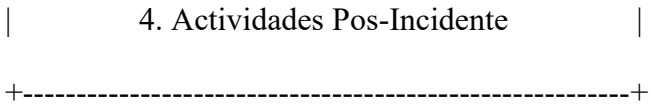
Alineación Táctica con el Ciclo de Vida de Incidentes NIST SP 800-61 r2

Para asegurar una respuesta metódica frente a la crisis materializada en SecureNova Labs, el Blue Team debe estructurar sus acciones operativas bajo los lineamientos internacionales de la Guía de Manejo de Incidentes de Ciberseguridad del NIST (SP 800-61 r2) (Zambrano Hernández et al., 2024). Este marco de referencia divide la respuesta defensiva en cuatro fases dinámicas y cíclicas que garantizan la erradicación de la amenaza y la mejora continua del SOC (ver Figura 9):

Figura 9

Ciclo de vida de respuesta y manejo de incidentes de ciberseguridad





Nota. Representación gráfica de las cuatro fases dinámicas y cíclicas recomendadas por el Instituto Nacional de Estándares y Tecnología para la gestión de incidentes: Preparación; Detección y Análisis; Contención/Erradicación/Recuperación; y Actividades Pos-Incidente. Adaptado de Scarfone y Mell (2022).

1. **Fase 1: Preparación (Hardening):** Es la etapa preventiva de establecimiento de líneas base de seguridad. Incluye la implementación previa de políticas de bastionado, despliegue de agentes SIEM, y la creación de planes de contingencia. En nuestro caso de estudio, las fallas encontradas en el Host-B (ausencia de parches y firewall inactivo) demuestran que la fase de preparación de SecureNova Labs era deficiente, exponiendo servicios críticos sin capas defensivas adicionales.
2. **Fase 2: Detección y Análisis (Triaje):** Una vez que un comportamiento sospechoso es reportado por los sensores de red o sistemas perimetrales, el analista de Blue Team inicia la fase de triaje. Esto requiere la recolección y verificación de datos técnicos para determinar el alcance y la veracidad del compromiso. Durante el laboratorio, esta fase se ejecutó de forma milimétrica en el Host-B al abrir la consola de comandos como administrador y correr el diagnóstico avanzado *netstat -ano | findstr :4444.* El resultado arrojado por el sistema operativo proveyó las métricas clave de detección: una conexión TCP establecida en un puerto de alta volatilidad (4444) correlacionada unívocamente con el identificador de proceso PID 1204, confirmando la intrusión y el

establecimiento del canal de control del atacante sin recurrir a suposiciones empíricas.

3. **Fase 3: Contención, Erradicación y Recuperación:** Con el incidente analizado y clasificado, se procede a ejecutar las acciones tácticas defensivas. El objetivo de la contención es limitar el radio de impacto del ataque para salvar el resto de la infraestructura de SecureNova Labs de un movimiento lateral o de una exfiltración masiva de bases de datos de nómina o historias clínicas de clientes de gobiernos. La contención ejecutada en la práctica consistió en encender de inmediato el *Windows Defender Firewall* y parametrizar una regla restrictiva de entrada quirúrgica que bloqueó el tráfico SMBv1/v2/v3 en el puerto TCP 445 (Contención SMB - Blue Team). Esto cortó instantáneamente la capacidad del adversario de enviar nuevos paquetes de explotación o de pivotar a través de la red local. La erradicación se complementa con la eliminación definitiva de la cuenta fantasma creada ("Robinson_Gomez") y la aplicación forzada del parche crítico de Microsoft para sellar la vulnerabilidad de Kernel.
4. **Fase 4: Actividades Pos-Incidente (Lecciones Aprendidas):** Corresponde a la fase final de documentación y retroalimentación institucional. El Blue Team consolida el informe de incidentes, analiza las brechas de monitoreo que permitieron la explotación y emite el dictamen de recomendaciones de aseguramiento preventivo (como la deshabilitación total de SMBv1 y el endurecimiento mediante CIS Benchmarks), cerrando el ciclo del NIST y elevando de forma adaptativa el nivel de madurez tecnológica de la corporación.

Monitoreo Avanzado de Eventos en Windows (Event IDs Críticos para el SOC)

Un equipo Blue Team profesional en SecureNova Labs no puede depender de revisiones manuales en consolas aisladas. La centralización de registros a través de los canales de auditoría del sistema operativo Windows es fundamental para alertar tempranamente anomalías vinculadas a la explotación de EternalBlue y la creación de persistencia. El analista del SOC debe configurar alertas automatizadas priorizando los siguientes identificadores de eventos *(Event IDs)* del Visor de Sucesos de Microsoft:

1. **Event ID 4624 (Inicio de sesión exitoso):** Este log de auditoría de seguridad registra cada vez que una cuenta se autentica en el sistema operativo. Monitorear los inicios de sesión con el Tipo de Inicio de Sesión 3 (Network Login) a través de cuentas locales o administrativas es crítico, ya que detona pistas sobre el uso de la conexión SMB de red para realizar movimientos laterales involuntarios.
2. **Event ID 4720 (Creación de cuenta de usuario local):** Es el registro de máxima criticidad para auditar el establecimiento de persistencia. Cada vez que el Red Team inyecta de forma encubierta comandos como *net user /add,* el subsistema de seguridad de Windows genera de manera inalterable un Event ID 4720 que detalla el nombre de la cuenta creada (ej. "Robinson_Gomez"), el SID asignado y el usuario administrativo que ejecutó la orden. El SOC debe disparar una alerta automatizada de severidad extrema al detectar este evento si no está asociado a un ticket lícito de la mesa de ayuda de TI.
3. **Event ID 4732 (Adición de miembro a un grupo local de seguridad):** Este log complementa la monitorización de persistencia y escalada de privilegios. Se activa inmediatamente cuando una cuenta es insertada dentro de grupos de alta jerarquía *(net localgroup administradores /add).* El registro muestra de manera

transparente la elevación del usuario hacia privilegios de administración, permitiendo interceptar al atacante antes de que haga uso de sus accesos fraudulentos.

4. **Event ID 7045 (Instalación de un nuevo servicio en el sistema):** Durante ataques avanzados que involucran herramientas automatizadas de post-explotación o la inyección de payloads ejecutables persistentes, los exploits intentan registrarse dentro del Administrador de Control de Servicios de Windows para garantizar que el código se ejecute automáticamente cada vez que el servidor se reinicie. Monitorizar la instalación sorpresiva de servicios con binarios apuntando a directorios temporales (*%TEMP%* o *\AppData\Local*) es un indicador de compromiso (IoC) definitivo de actividad maliciosa.

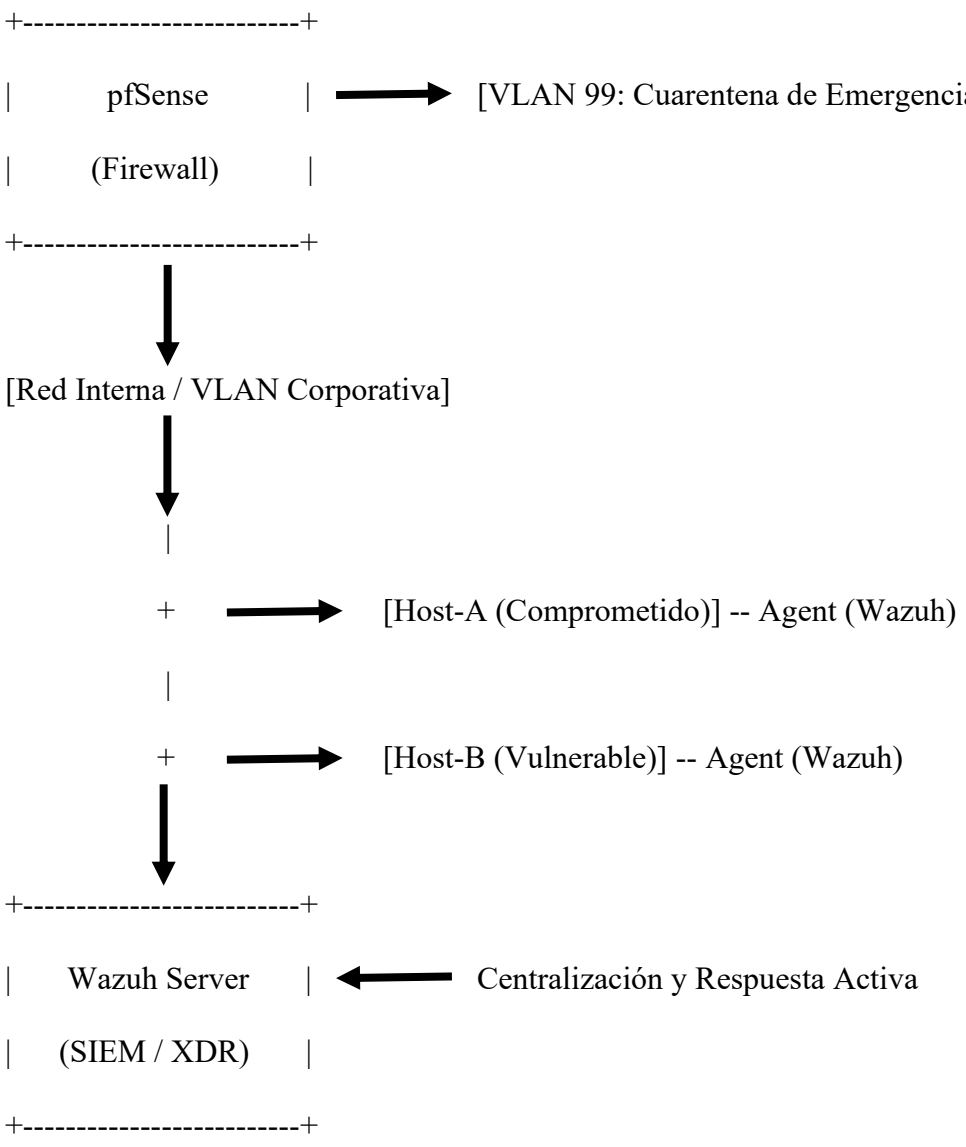
Implementación Detallada de Controles pfSense y Reglas Wazuh para la Defensa Activa

Para dar pleno cumplimiento al requerimiento institucional de SecureNova Labs de implementar soluciones robustas de contención y defensa activa empleando software de licenciamiento de código abierto (GPL/Open Source) y optimizar el presupuesto, se detalla la configuración táctica de las herramientas pfSense y Wazuh (ver Figura 10):

Figura 10

Propuesta de arquitectura perimetral, microsegmentación y defensa activa basada en el modelo Zero Trust para SecureNova Labs

[Red Externa / Internet]



Nota. Diseño de infraestructura que detalla el aislamiento lógico de activos a través de zonas de red independientes, la centralización de logs y la automatización de la contención mediante el módulo de respuesta activa (Active Response) de Wazuh SIEM. Elaboración propia.

1. **Configuración Arquitectónica en pfSense (Aislamiento de Frontera e Inter-VLAN):** El cortafuegos perimetral pfSense debe operar bajo un paradigma de microsegmentación lógica mediante la creación de redes de área local virtuales (VLANs) estrictas. Ante la detección de movimiento lateral o un brote de

malware propagado vía EternalBlue, el Blue Team debe configurar reglas en pfSense que restrinjan por completo el tráfico inter-estación del puerto TCP 445 entre las distintas subredes de estaciones de trabajo, aislando el protocolo SMB exclusivamente hacia zonas desmilitarizadas (DMZ) donde residen los servidores de archivos legítimos. Adicionalmente, pfSense permite la creación de una VLAN 99 de Cuarentena de Emergencia. A través de llamadas de la API de pfSense, los analistas del SOC pueden reasignar dinámicamente el segmento de red de un host infectado, confinándolo a una red sin salida a internet y con acceso restringido, neutralizando así el túnel de Comando y Control (C2) del atacante sin interrumpir la operatividad general de la empresa.

2. **Reglas de Detección Correlacionada y Active Response en Wazuh (SIEM/XDR):** El servidor centralizado de Wazuh recopila en tiempo real la telemetría enviada por los agentes instalados en los *endpoints.* Para mitigar la explotación de vulnerabilidades de Kernel y la escalada de privilegios, se programan reglas lógicas de correlación personalizadas dentro del directorio */var/ossec/etc/rules/local_rules.xml.* A continuación, se expone un modelo de estructura lógica para interceptar la creación anómala de cuentas administrativas locales:

```
<group name="security_unad_endpoint,">
     <rule id="100201" level="9">
          <if_sid>18100</if_sid>
          <field name="win.system.eventID">^4720$</field>
```

```
        <description>SOC Alerta: Creación detectada de
        una cuenta de usuario local en el
        Endpoint</description>
    </rule>

    <rule id="100202" level="13">
        <if_sid>100201</if_sid>
        <field name="win.system.eventID">^4732$</field>
        <description>CRÍTICO: Cuenta fantasma escalada al
        grupo de Administradores locales - Posible
        Persistencia</description>
        <mitre>
            <id>T1136.001</id>
        </mitre>
    </rule> group>
</group>
```

Al dispararse la regla correlacionada de nivel 13 *(id="100202"),* Wazuh activa inmediatamente su módulo de Active Response (Respuesta Activa) (Wazuh, Inc., s.f.). El servidor SIEM envía una instrucción automatizada al agente local del host afectado para ejecutar un script defensivo en milisegundos. El script interactúa con la interfaz de red del equipo comprometido para dar de baja la conexión TCP maliciosa, matar el identificador de proceso (PID) infeccioso y deshabilitar localmente la cuenta fraudulenta creada. Con este control GPL,

SecureNova Labs adquiere capacidades automatizadas de defensa proactiva, conteniendo las amenazas informáticas en tiempo real antes de que la intrusión escale hacia daños catastróficos en su infraestructura corporativa.

Propuesta de Arquitectura de Seguridad Basada en el Modelo Zero Trust

Como cierre estratégico del informe gerencial dirigido a los analistas Seniors, la hardenización de la infraestructura no puede limitarse a parches aislados; debe evolucionar de manera holística hacia la adopción del modelo internacional Zero Trust (Confianza Cero). Este paradigma defensivo asume por defecto la premisa de que la red interna ya se encuentra comprometida *(Assume Breach),* obligando a verificar de manera explícita y continua la identidad de cada usuario, el estado de cada endpoint y la legitimidad de cada flujo de datos, sin importar la ubicación geográfica del solicitante. La propuesta técnica para SecureNova Labs se estructura sobre cuatro pilares fundamentales:

1. **Pilar de Gestión de Identidades (Identity Security):** Se debe eliminar el uso de credenciales locales estáticas de texto claro compartidas entre los administradores de sistemas. Se propone la implementación obligatoria de un sistema de Autenticación de Múltiple Factor (MFA) respaldado por un Proveedor de Identidad centralizado. Todo acceso con privilegios de alta jerarquía debe requerir una verificación criptográfica adicional (tokens de software o llaves de hardware), neutralizando de raíz la efectividad de las técnicas de post-explotación basadas en el robo de hashes de contraseñas *(Pass-the-Hash)* o credenciales extraídas de la memoria mediante herramientas ofensivas como Mimikatz.
2. **Pilar de Endpoints Endurecidos (Endpoint Hardening):** Ninguna máquina o servidor de archivos puede operar en la red sin cumplir de manera estricta con la

línea base de configuración segura estipulada por los *CIS Benchmarks Nivel 1*. Las Políticas de Grupo (GPO) del Directorio Activo deben auditar continuamente que el Windows Defender Firewall permanezca encendido en todos sus perfiles operativos. Se implementará un control estricto de listas blancas de ejecución de software *(AppLocker),* bloqueando preventivamente que la línea de comandos ejecute binarios desconocidos o scripts maliciosos alojados en los directorios de usuario, deteniendo la instalación de cargas útiles no autorizadas de forma proactiva.

3. **Pilar de Microsegmentación de Red (Network Microsegmentation):** El perímetro de la red local debe dejar de ser plano y abierto. A través de la configuración avanzada de switches de capa 3 y firewalls perimetrales de software libre (pfSense/OPNsense), la arquitectura interna de SecureNova Labs debe segmentarse lógicamente en micro-zonas aisladas. El tráfico asociado al protocolo SMB (puertos TCP 445 y 139) debe ser bloqueado de manera transversal entre las estaciones de trabajo locales corporativas, permitiendo el flujo de este servicio de manera exclusiva y cifrada hacia los servidores centrales de almacenamiento dedicados y controlados mediante inspección profunda de paquetes.
4. **Pilar de Protección de Datos Forenses (Data & Log Integrity):** Toda la telemetría y los registros de auditoría (logs de seguridad del Event Viewer) generados por la infraestructura deben ser centralizados de forma cifrada e inmutable hacia el clúster de Wazuh. Los analistas de seguridad deben contar con una traza histórica auditable e inalterable que resguarde los registros, impidiendo que un atacante que ha ganado máximos privilegios de Kernel pueda manipular

los logs locales para borrar sus huellas, garantizando la visibilidad profunda del SOC en todo momento.

Despliegue Operativo y Orquestación de la Arquitectura. Para materializar los cuatro pilares descritos anteriormente, el tránsito hacia este modelo en SecureNova Labs exige una reestructuración profunda de su topología de red y de sus capacidades de monitoreo. La arquitectura defensiva propuesta no se basa en la adquisición de soluciones aisladas, sino en la integración sinérgica de componentes de seguridad que actúan en múltiples capas (Defensa en Profundidad).

1. **Microsegmentación Perimetral e Inter-VLAN con pfSense**

   El núcleo de la protección de red de la nueva arquitectura recae sobre la implementación de clústeres de pfSense en alta disponibilidad (HA). A diferencia de los firewalls tradicionales que solo vigilan el tráfico norte-sur (desde y hacia internet), pfSense se configura para inspeccionar el tráfico este-oeste (comunicación interna entre hosts). Se diseñan redes de área local virtuales (VLAN) altamente granulares: VLAN de Usuarios, VLAN de Servidores de Aplicaciones, VLAN de Bases de Datos y VLAN de Gestión fuera de banda (OOB). Todo el tráfico inter-VLAN queda denegado por defecto (Default Deny). Para mitigar ataques como el documentado en este informe, los puertos TCP 445 (SMB), 3389 (RDP) y 135 (RPC) permanecen estrictamente bloqueados entre las estaciones de trabajo de los usuarios, permitiendo la comunicación únicamente hacia los servidores específicos que requieran estos servicios, previa inspección por el motor de detección de intrusos (Snort/Suricata) integrado en el firewall.

2. **Orquestación, Detección y Respuesta Automatizada con Wazuh SIEM**

La visibilidad integral de la infraestructura se logra mediante el despliegue de la plataforma Wazuh. Esta solución opera bajo una arquitectura cliente-servidor descentralizada. En cada servidor y estación de trabajo (incluidos los sistemas heredados) se instala un agente ligero de Wazuh. Este agente no solo recolecta los registros del Visor de Eventos de Windows, sino que ejecuta tareas de Monitoreo de Integridad de Archivos (FIM). Esto significa que si un atacante logra ganar acceso y modifica binarios críticos del sistema operativo o archivos de configuración del servidor web, el agente calcula en tiempo real el cambio en los hashes criptográficos (MD5/SHA256) y envía una alerta inmediata al servidor central.

El nodo administrador de Wazuh (Manager) decodifica estas alertas, las enriquece con fuentes de inteligencia de amenazas externas (Threat Intelligence Feeds) y aplica reglas lógicas de correlación. La arquitectura defensiva contempla la automatización mediante el módulo de Active Response. Al configurarse correctamente, la intervención humana no es necesaria para la contención inicial; si el SIEM detecta un escaneo de Nmap seguido de múltiples intentos fallidos de autenticación (fuerza bruta), el Manager ordena al agente local del host que inyecte una regla en el firewall nativo bloqueando la dirección IP agresora durante un periodo de tiempo determinado, cortando la cadena de ataque en sus fases tempranas.

Mapeo Táctico y Técnico basado en el Framework MITRE ATT&CK

Para alinear las operaciones del Red Team con los estándares globales de inteligencia de amenazas, se ha realizado un mapeo exhaustivo de la intrusión al entorno de SecureNova Labs

utilizando el framework MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) (MITRE Corporation, 2020). Este mapeo no solo documenta el "cómo" se vulneró el sistema, sino que estandariza el lenguaje para que el Blue Team pueda afinar sus reglas de detección (ver Tabla 1).

Tabla 1

Mapeo de la cadena de ataque (Cyber Kill Chain) de la operación Red Team frente a las tácticas y técnicas del Framework MITRE ATT&CK

Táctica (Fase del Ataque)	**ID de Técnica**	**Nombre de la Técnica**	**Descripción de la Ejecución en el Laboratorio**
Reconocimiento (Reconnaissance)	T1595.001	Active Scanning: Scanning IP Blocks	Se utilizó Nmap (nmap -sV -p-) para realizar un barrido activo de la subred 10.0.2.0/24, identificando el Host-A (10.0.2.4) y el servicio vulnerable HttpFileServer 2.3 en el puerto 80.
Acceso Inicial (Initial Access)	T1190	Exploit Public-Facing Application	El Red Team explotó la vulnerabilidad del servidor web HFS expuesto perimetralmente utilizando Metasploit, logrando la ejecución de código remoto y el primer acceso al entorno (cabeza de playa).

Ejecución (Execution)	T1059.003	Command and Scripting Interpreter: Windows Command Shell	A través de la sesión de Meterpreter, se interactuó directamente con la consola de comandos de Windows (cmd.exe) para ejecutar comandos nativos del sistema operativo de forma remota.
Evasión de Defensas (Defense Evasion)	T1562.004	Impair Defenses: Disable or Modify System Firewall	Se aprovechó la vulnerabilidad arquitectónica de diseño donde el Host-B (10.0.2.6) operaba con el Windows Defender Firewall apagado, facilitando el tránsito de paquetes maliciosos sin inspección.
Movimiento Lateral (Lateral Movement)	T1210	Exploitation of Remote Services	Se configuró un túnel de Pivoting (autoroute) desde el Host-A para atacar el Host-B mediante la explotación del protocolo SMBv1 (MS17-010 EternalBlue) a través del puerto TCP 445 de la red interna.
Escalada de Privilegios (Privilege Escalation)	T1068	Exploitation for Privilege Escalation	El exploit EternalBlue inyectó código directamente en el Kernel (srv.sys), otorgando a la

			sesión inversa de Metasploit el nivel máximo de privilegios del sistema operativo (NT AUTHORITY\SYSTEM).
Persistencia (Persistence)	T1136.001	Create Account: Local Account	Se utilizó la línea de comandos interactiva remota para inyectar las directivas net user y net localgroup, creando la cuenta oculta "Robinson_Gomez" y asignándola al grupo de Administradores locales.
Comando y Control (Command and Control - C2)	T1090.001	Proxy: Internal Proxy	El tráfico ofensivo dirigido al Host-B fue encapsulado y enrutado a través de la sesión de Meterpreter del Host-A, utilizando este último como un proxy interno para evadir la segmentación de red.

Nota. Análisis de correlación entre las acciones ofensivas simuladas en el laboratorio y el diccionario global de tácticas adversarias de MITRE. Elaboración propia.

Matriz de Riesgos y Evaluación de Impacto (Metodología ISO 27005)

Desde la perspectiva gerencial, las vulnerabilidades técnicas deben ser traducidas al lenguaje de riesgos del negocio. SecureNova Labs necesita comprender el impacto financiero,

operativo y reputacional que representa mantener arquitecturas obsoletas. A continuación, se presenta la evaluación de riesgos de los hallazgos críticos detectados durante la simulación, utilizando una matriz de probabilidad e impacto (Nivel de Riesgo = Probabilidad x Impacto) (Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD, 2024) (ver Tabla 2).

Tabla 2

Evaluación de Riesgos de Ciberseguridad sobre la Infraestructura de SecureNova Labs

Activo de Información / Servicio	**Vulnerabilidad Identificada (Hallazgo)**	**Amenaza Asociada (Vector)**	**Probabilidad (1-5)**	**Impacto (1-5)**	**Nivel de Riesgo (1-25)**	**Estrategia de Tratamiento (Blue Team)**
Servidor de Archivos (Host-B)	Exposición del protocolo heredado SMBv1 sin parche de seguridad MS17-010.	Explotación remota de Kernel, infección por Ransomware (WannaCry) y movimiento lateral automatizado.	5 (Casi Seguro)	5 (Catastrófico)	25 (Crítico)	Mitigar: Deshabilitar SMBv1 vía registro, instalar parche de Microsoft y bloquear puerto 445 en firewall de host.
Perímetro de Red (Host-A)	Aplicación web (Rejetto HFS)	RCE (Ejecución Remota de	4 (Probable)	4 (Mayor)	16 (Alto)	Mitigar: Actualizar aplicativo

	desactualizada y expuesta a la red pública.	Código), compromiso inicial de la red, defacement, y uso como nodo de Pivoting.				a versión segura, colocar detrás de un WAF (Web Application Firewall) y segmentar en una DMZ.
Control de Accesos (Endpoints)	Ausencia de monitoreo sobre la creación de cuentas de usuario local y escalada a grupos administrativos.	Establecimiento de persistencia indetectable (APT), exfiltración sostenida de datos y evasión de auditorías.	4 (Probable)	5 (Catastrófico)	20 (Extremo)	Mitigar: Ingesta de Event IDs 4720 y 4732 en el SIEM (Wazuh) con reglas de Respuesta Activa para bloqueo inmediato.
Firewall de Sistema Operativo	Políticas de Grupo (GPO) laxas que permiten que el	Tránsito libre de malware tipo gusano, exposición	5 (Casi Seguro)	4 (Mayor)	20 (Extremo)	Mitigar: Implementar CIS Benchmarks Nivel 1,

	Firewall de Windows esté inactivo.	de puertos administrativos (RDP, WinRM, SMB) a subredes no autorizadas.				forzando por dominio el encendido del firewall en perfiles Público, Privado y Dominio.

Nota. Matriz de calor de riesgos basada en los hallazgos del ejercicio de Red Team, clasificando la severidad de las brechas para priorizar la inversión defensiva del Blue Team. Elaboración propia.

Análisis Comparativo de Soluciones Tecnológicas de Contención y Monitoreo

Para asegurar que SecureNova Labs adopte las herramientas correctas bajo su restricción de presupuesto (licenciamiento GPL), el Blue Team ha realizado una evaluación técnica comparativa de las soluciones de defensa y monitorización disponibles en el mercado. Se contrastan herramientas de grado comercial (propietarias) frente a sus contrapartes de código abierto, demostrando la viabilidad técnica y operativa de las alternativas Open Source seleccionadas (ver Tabla 3).

Tabla 3

Comparativa técnica de herramientas SIEM/XDR y Firewalls Perimetrales

Categoría Tecnológica	**Herramienta Propietaria (Comercial)**	**Herramienta Open Source (GPL)**	**Ventajas de la Solución Open Source para SecureNova Labs**
Plataforma SIEM / XDR	Splunk Enterprise / IBM QRadar	Wazuh	Arquitectura gratuita y escalable. Incluye integración nativa con OSSEC para análisis de logs, File Integrity Monitoring (FIM) y motores de Active Response sin costos por volumen de datos ingeridos (GB/día).
Prevención de Intrusiones en Host (HIPS)	CrowdStrike Falcon / SentinelOne	Fail2Ban	Consumo mínimo de recursos de CPU/RAM. Automatización directa con el firewall local (iptables / Windows Firewall) para inyectar reglas temporales o permanentes de bloqueo de IPs agresoras mediante análisis de firmas.

Firewall Perimetral y Enrutamiento (Capa 3/4)	Fortinet FortiGate / Palo Alto	pfSense	Basado en FreeBSD, altamente estable. Permite la configuración de microsegmentación inter-VLAN, túneles VPN IPsec seguros y filtrado de paquetes robusto, requiriendo únicamente hardware de servidor genérico o virtualizado.
Detección de Intrusiones en Red (NIDS)	Cisco Firepower	Snort / Suricata	Motor de análisis de tráfico en tiempo real basado en reglas de la comunidad (Emerging Threats). Capacidad de inspeccionar profundamente los paquetes (DPI) y detectar intentos de explotación de EternalBlue en la red antes de llegar al host.

Nota. Análisis comparativo que justifica la viabilidad técnica, operativa y financiera de integrar un stack de ciberseguridad open source para operaciones de Blue Team. Elaboración propia.

Manual de Procedimientos Estándar (Playbook) de Respuesta a Incidentes: Infección por Movimiento Lateral SMB

Una de las responsabilidades más críticas del Blue Team y del CSIRT es la estandarización de las acciones de respuesta (Instituto Nacional de Ciberseguridad [INCIBE], 2018). Ante el hallazgo de la vulnerabilidad de movimiento lateral documentada en este informe, se ha diseñado el siguiente "Playbook" paso a paso para que los analistas de SecureNova Labs sepan exactamente cómo reaccionar ante una alerta de intrusión similar en el futuro, minimizando el tiempo de recuperación (MTTR).

Fase 1: Preparación y Alerta Temprana

1. El sistema SIEM (Wazuh) arroja una alerta crítica de nivel 12+: *«Múltiples conexiones entrantes en el puerto TCP 445 acompañadas de un desbordamiento de memoria detectado en srv.sys».*
2. El analista del SOC Nivel 1 realiza la apertura de un ticket de incidente de máxima prioridad (P1) y notifica al líder del CSIRT.
3. Se revisan los tableros de control (Dashboards) para identificar la IP de origen (atacante o nodo infectado local) y la IP de destino (víctima).

Fase 2: Triaje y Preservación Forense

4. Un analista forense del Blue Team accede a la red de administración out-of-band (fuera de banda).
5. Se ejecutan herramientas de diagnóstico volátil sobre la máquina víctima sin apagarla (ej. volcado de memoria RAM con FTK Imager o captura de estado de red con *netstat* y *Sysinternals TCPView*).

6. Se identifica el binario malicioso en ejecución, las conexiones C2 (Comando y Control) establecidas y la posible cuenta fantasma creada en el administrador de cuentas de seguridad (SAM).

Fase 3: Contención a Corto y Largo Plazo

7. **Contención Lógica (Corto Plazo):** El analista de redes accede a la consola de pfSense o al switch administrable y reasigna el puerto físico o lógico de la máquina víctima a la "VLAN 99 de Cuarentena", la cual carece de reglas de enrutamiento hacia la red corporativa y hacia internet.
8. **Contención en el Endpoint (Corto Plazo):** Se envía un comando a través del agente de respuesta activa de Wazuh para bloquear el puerto TCP 445 de entrada en el *Windows Defender Firewall* del equipo.
9. **Contención de Propagación (Largo Plazo):** Se actualizan temporalmente las Listas de Control de Acceso (ACL) en los firewalls inter-VLAN para suspender todo tráfico SMB que no provenga de servidores de administración de parches legítimos.

Fase 4: Erradicación y Recuperación

10. Se procede a matar los procesos inyectados detectados en la fase de triaje.
11. Se elimina cualquier cuenta de administrador local no autorizada y se restablecen las contraseñas de las cuentas comprometidas.
12. Se aplica de manera imperativa el parche de Microsoft MS17-010 o la actualización acumulativa de seguridad correspondiente.

13. Se realiza un escaneo profundo de malware utilizando soluciones EDR o antivirus actualizados para descartar herramientas de persistencia residuales (backdoors, rootkits o scheduled tasks).
14. Tras confirmar la limpieza, la máquina es reintroducida a la VLAN de producción operativa.

Fase 5: Lecciones Aprendidas

15. El CSIRT convoca una reunión de retrospectiva con los equipos de Red y Blue Team.
16. Se documentan las fallas de monitoreo o de gestión de vulnerabilidades que permitieron el incidente inicial.
17. Se actualizan las políticas de *Patch Management* y se afinan las reglas de detección del SIEM para evitar falsos negativos en el futuro.

Diseño de Políticas de Seguridad de la Información (PSI) y Gobernanza TI

La intrusión exitosa del Red Team sobre la infraestructura de SecureNova Labs evidenció no solo fallas técnicas, sino deficiencias en la Gobernanza de TI. Para garantizar que las estrategias del Blue Team sean sostenibles, estas deben estar respaldadas por Políticas de Seguridad de la Información (PSI) de cumplimiento obligatorio, aprobadas por la Alta Gerencia y alineadas con la norma ISO/IEC 27001. A continuación, se estructuran las normativas críticas que deben implementarse inmediatamente.

Política de Gestión de Vulnerabilidades y Parches (Patch Management)

El compromiso a través de MS17-010 demostró la inexistencia de Acuerdos de Nivel de Servicio (SLA) para la aplicación de parches. SecureNova Labs debe adoptar un ciclo de vida de

vulnerabilidades que defina tiempos máximos de remediación basados en la criticidad del puntaje CVSS (Common Vulnerability Scoring System) (ver Tabla 4).

Tabla 4

Acuerdos de Nivel de Servicio (SLA) para la Gestión de Parches y Vulnerabilidades

Severidad (CVSS v3.1)	**Descripción del Riesgo Operativo**	**Tiempo Máximo de Aplicación (SLA)**	**Acción de Mitigación Temporal (Blue Team)**
Crítica (9.0 - 10.0)	Vulnerabilidad que permite Ejecución Remota de Código (RCE) sin autenticación (Ej. EternalBlue).	24 - 48 Horas	Aislamiento inmediato del servicio en el firewall perimetral y desactivación del protocolo heredado.
Alta (7.0 - 8.9)	Elevación de privilegios locales o exposición de datos sensibles que requiere acceso inicial.	7 Días Calendario	Monitoreo exhaustivo de Event IDs en el SIEM e implementación de reglas de prevención en Endpoint.
Media (4.0 - 6.9)	Vulnerabilidades de denegación de servicio (DoS) o suplantación con requerimientos complejos.	30 Días Calendario	Actualización programada en ventanas de mantenimiento habituales de infraestructura.
Baja (0.1 - 3.9)	Exposición de información no	90 Días Calendario	Inclusión en el plan trimestral de

	crítica o banners de versión de software.		actualización de sistemas.

Nota. Estructura de tiempos de respuesta exigidos para el equipo de infraestructura TI, garantizando la eliminación oportuna de vectores de ataque. Elaboración propia.

Política de Control de Acceso y Gestión de Identidades (IAM)

La técnica de persistencia utilizada (creación de la cuenta "Robinson_Gomez") aprovechó la falta de controles sobre la gestión de identidades locales. La nueva política establece:

1. **Prohibición de Cuentas Locales Compartidas:** Se prohíbe el uso de cuentas de administrador local genéricas (ej. *Admin, Soporte*). Todo acceso administrativo debe ser nominal, trazable y autenticado a través del Directorio Activo (Active Directory).
2. **Autenticación Multifactor (MFA) Obligatoria:** Todo acceso a servidores críticos, consolas de administración de firewalls (pfSense), paneles de SIEM (Wazuh) y conexiones VPN requerirá MFA mediante tokens físicos o aplicaciones generadoras de contraseñas de un solo uso basadas en el tiempo (TOTP).
3. **Principio de Mínimo Privilegio (PoLP):** Los usuarios y servicios operarán únicamente con los permisos estrictamente necesarios para cumplir sus funciones. Las escaladas de privilegios requerirán flujos de aprobación temporal (Just-In-Time Access).

Marco de Análisis Forense Digital y Respuesta a Incidentes (DFIR)

Tras la contención del ataque en el Host-B, el CSIRT de SecureNova Labs debe ejecutar un Análisis Forense Digital estructurado para reconstruir la anatomía completa de la intrusión y recopilar pruebas con validez legal.

Adquisición de Evidencia Volátil (Orden de Volatilidad RFC 3227)

Durante el triaje, la extracción de evidencia debe respetar estrictamente la cadena de custodia y el principio de volatilidad de los datos. El analista forense procederá a recolectar la información del sistema vulnerado en el siguiente orden, de mayor a menor riesgo de pérdida:

1. **Registros de CPU y Caché:** Variables de estado inmediato del Kernel.
2. **Tablas de Enrutamiento y Conexiones de Red:** Extracción mediante *netstat* y volcados de ARP para identificar las IPs del servidor de Comando y Control (C2) de Metasploit.
3. **Memoria RAM Física:** Utilizando herramientas certificadas (como FTK Imager o DumpIt), se generará un archivo *.mem* o *.raw* de la memoria completa del equipo antes de su apagado. Este volcado permite recuperar procesos ocultos de Meterpreter, claves de cifrado en texto claro e inyecciones en procesos como *lsass.exe.*
4. **Estado de Procesos y Archivos Abiertos:** Mapeo de binarios sospechosos en ejecución mediante Sysinternals Process Explorer.
5. **Discos Duros (Clonación Bit a Bit):** Apagado seguro del equipo y creación de una imagen forense (*.E01* o *.dd*) a través de bloqueadores de escritura por hardware para garantizar que ningún hash MD5/SHA-256 sea alterado durante la copia.

Caza de Amenazas (Threat Hunting) y Análisis de Artefactos de Windows

El análisis de la imagen forense se enfocará en identificar los Rastros o Indicadores de Compromiso (IoC) dejados por el atacante. Los analistas del Blue Team buscarán proactivamente:

- **Análisis de Colmenas del Registro (Registry Hives):** Se auditará la colmena *SAM* y *SYSTEM* buscando discrepancias en los perfiles de usuario. Se verificará la creación de la cuenta no autorizada y su inclusión en las subclaves del grupo Administradores local.
- **Prefetch y Amcache:** El análisis de los archivos *.pf* ubicados en *C:\Windows\Prefetch* revelará la marca de tiempo exacta de ejecución de binarios sospechosos o herramientas nativas utilizadas maliciosamente, como *net.exe* y *cmd.exe.*
- **Visor de Eventos de Seguridad (EVTX):** Búsqueda de borrado intencional de logs (Event ID 1102 - The audit log was cleared) que evidencie intentos de evasión de defensas (Defense Evasion).

Métricas de Rendimiento del Centro de Operaciones de Seguridad (SOC KPIs)

Para cuantificar la eficacia de las medidas de hardenización implementadas y la rapidez operativa del Blue Team de SecureNova Labs, la Dirección de Ciberseguridad establecerá Indicadores Clave de Rendimiento (KPIs). Estas métricas evaluarán si el equipo está mejorando su capacidad para repeler simulaciones ofensivas de Red Team y ciberataques reales (ver Tabla 5).

Tabla 5

Indicadores Clave de Rendimiento (KPIs) para la Gestión de Incidentes (Blue Team / CSIRT)

Indicador Técnico (KPI)	**Descripción de la Métrica de Seguridad**	**Meta Institucional Esperada**	**Impacto Organizacional**
MTTD (Mean Time to Detect)	Tiempo Promedio de Detección. Mide cuánto tarda el SOC/SIEM en identificar y alertar sobre una intrusión desde el momento en que ocurre (Ej. ejecución de EternalBlue).	< 15 Minutos	Minimiza la "ventana de oportunidad" del atacante para eludir defensas o moverse lateralmente.
MTTA (Mean Time to Acknowledge)	Tiempo Promedio de Reconocimiento. Mide el lapso entre la generación de la alerta en el SIEM y el momento en que un analista asume el ticket y comienza el triaje.	< 5 Minutos	Refleja la eficiencia, el ancho de banda operativo y la disponibilidad del personal en el SOC.
MTTR (Mean Time to Respond/Recover)	Tiempo Promedio de Respuesta y Recuperación. Calcula la duración desde la detección inicial hasta la	< 60 Minutos	Determina la efectividad real de los playbooks de incidentes y las capacidades de "Active Response".

	contención total y recuperación del activo (Ej. aislamiento en pfSense y bloqueo de puertos).		
False Positive Rate (FPR)	Tasa de Falsos Positivos. Porcentaje de alertas generadas por el SIEM (Wazuh) que no representan amenazas reales, requiriendo afinamiento de reglas.	< 10%	Evita la "fatiga de alertas" en los analistas, permitiendo que el equipo se enfoque en eventos críticos.
Cobertura de Endpoints	Porcentaje de máquinas corporativas con agentes EDR/SIEM activos y Firewall nativo habilitado frente al inventario total de activos de TI.	100%	Garantiza la ausencia de puntos ciegos (Shadow IT) y suprime superficies de ataque expuestas.

Nota. Marco de métricas operacionales para evaluar la madurez, velocidad y precisión del equipo defensivo frente a escenarios de cibercrisis. Elaboración propia.

Transición Estratégica hacia Operaciones Purple Team

Como recomendación final de alto nivel para la Alta Dirección de SecureNova Labs, se plantea la maduración del modelo de ciberseguridad pasando de un esquema de equipos aislados (Silos) a un paradigma colaborativo: el Purple Teaming.

En la concepción clásica, el Red Team ataca y el Blue Team defiende, a menudo generando fricción u ocultamiento de información. Un ejercicio Purple Team es una metodología donde ambos equipos trabajan conjuntamente y en tiempo real. Durante la explotación de vulnerabilidades (como MS17-010 o la inyección de la cuenta administradora), el Red Team informa inmediatamente al Blue Team sobre la táctica ejecutada. A su vez, el Blue Team verifica sus tableros de control en el SIEM para comprobar si la alerta se disparó correctamente. Si la alerta no existió, ambos equipos colaboran en ese mismo instante para redactar, probar e implementar la nueva regla de detección en Wazuh.

Esta aproximación colaborativa maximiza el Retorno de Inversión (ROI) en ciberseguridad, asegurando que el presupuesto destinado a auditorías ofensivas se traduzca de manera directa e inmediata en el endurecimiento medible de las redes de defensa institucionales, mitigando riesgos sistémicos y garantizando la supervivencia digital de la corporación.

Relación entre Objetivos Específicos y Hallazgos del Ejercicio

Para garantizar la trazabilidad académica y técnica de este informe, es imperativo establecer una correlación directa entre los objetivos específicos planteados al inicio del seminario y los hallazgos empíricos obtenidos durante la simulación del entorno de SecureNova Labs. Esta triangulación permite validar que las acciones del Red Team y del Blue Team no fueron aisladas, sino que respondieron a un propósito de auditoría integral.

Frente al primer objetivo específico, orientado a evaluar las implicaciones legales y éticas de las operaciones de ciberseguridad, los hallazgos demostraron deficiencias estructurales en los Acuerdos de Confidencialidad (NDA) de la organización. Se identificó que las políticas internas instigaban tácitamente a la interceptación de datos sin el consentimiento previo, lo cual colisiona de manera directa con los principios de la Ley 1273 de 2009. El hallazgo principal en esta fase es que el riesgo legal en ciberseguridad no solo proviene de actores externos, sino de una gobernanza interna deficiente que expone a los especialistas a incurrir en delitos informáticos por omisión o coerción corporativa.

En relación con el segundo objetivo, enfocado en demostrar empíricamente las capacidades de intrusión de un Red Team, los resultados técnicos fueron contundentes. La ejecución controlada de la vulnerabilidad MS17-010 (EternalBlue) probó que una arquitectura de red carente de microsegmentación permite que un compromiso inicial en un perímetro débil (Host-A) se transforme rápidamente en un control administrativo de los servidores internos (Host-B). el hallazgo crítico radicó en la facilidad con la que el atacante logró establecer persistencia mediante la creación de la cuenta “Robinson_Gomez”; un vector que burla las defensas tradicionales al mimetizarse como una acción administrativa legítima dentro del administrador de cuentas de seguridad (SAM).

Abordando el tercer objetivo, centrado en el diseño de procedimientos de respuesta a incidentes desde el rol Blue Team, el ejercicio arrojó hallazgos vitales sobre la preservación de la evidencia forense. Se comprobó en el laboratorio que la respuesta reaccionaria de “desconectar o apagar” el equipo vulnerado resulta contraproducente, ya que destruye la evidencia volátil en la memoria RAM, como los subprocesos del código malicioso (Egg Hunter) y las conexiones del túnel inverso. El hallazgo defensivo demostró que la contención lógica, materializada en el bloqueo inmediato del puerto TCP 445 en el Windows Defender Firewall, es el método más

efectivo para neutralizar la amenaza manteniendo la integridad de la escena del crimen digital para el posterior análisis del CSIRT.

Finalmente, respecto al cuarto objetivo sobre la propuesta de un plan de hardenización arquitectónica, el diagnóstico final evidenció que SecureNova Labs operaba bajo un modelo de confianza implícita y obsoleta. Los hallazgos sustentan de manera irrefutable la necesidad de adoptar los estándares del Center for Internet Security (CIS Benchmarks). Se determinó que la integración de una plataforma SIEM de código abierto, como Wazuh, no es un lujo operativo, sino una necesidad arquitectónica para correlacionar los registros de eventos críticos y responder en tiempo real ante las tácticas adversarias descritas en el framework MITRE ATT&CK.

Evidencias de Sustentación

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

Video de sustentación del informe final: https://youtu.be/IguyFZ2hrO4

Conclusiones

En lo referente al objetivo específico enfocado en evaluar las implicaciones legales y éticas de las operaciones de ciberseguridad, se concluye que el marco normativo colombiano (Ley 1273 de 2009 y Ley 1581 de 2012) actúa como un límite estructural infranqueable frente a dilemas de ciberespionaje corporativo. Ningún Acuerdo de Confidencialidad (NDA) posee validez jurídica si obliga al auditor a ocultar o participar en la interceptación ilegal de datos informáticos. Esto ratifica que el estricto cumplimiento del Código de Ética del COPNIA y el establecimiento transparente de Reglas de Compromiso (RoE) son indispensables para blindar el ejercicio profesional y proteger los activos de información institucionales dentro de la legalidad.

respecto al objetivo específico de demostrar empíricamente las capacidades de intrusión de un Red Team bajo metodologías estructuradas (NIST SP 800-115 y Cyber Kill Chain), el desarrollo práctico en el laboratorio probó de forma contundente que la presencia de protocolos heredados y obsoletos como SMBv1 representa una compuerta abierta para el compromiso del host objetivo. La explotación exitosa de la vulnerabilidad de Kernel MS17-010 (EternalBlue) evidenció la velocidad con la que un atacante puede ejecutar movimientos laterales tras un compromiso inicial en el perímetro (Host-A). asimismo, se comprobó que el establecimiento de persistencia local mediante cuentas fantasmas manipula de forma legítima la base de datos SAM de Windows, burlando los antivirus tradicionales y otorgando accesos perennes con privilegios elevados.

Dando cumplimiento al objetivo específico de diseñar procedimientos de respuesta a incidentes desde el rol de Blue Team, se determina de manera concluyente que la afectividad del triaje y la contención activa depende de la preservación estricta de la evidencia forense volátil en la memoria RAM (RFC 3227). La simulación demostró que la respuesta tradicional de apagar físicamente el equipo vulnerado resulta perjudicial, ya que destruye los hilos de ejecución del

código malicioso y los sockets de red activos. En su lugar, la implementación de medidas de contención lógica a través del Windows Defender Firewall neutraliza instantáneamente el canal de Comando y Control (C2) del adversario y detiene la propagación de la amenaza sin alterar los artefactos requeridos por el CSIRT.

Finalmente, en atención al objetivo específico orientado a proponer un plan de hardenización arquitectónica, monitoreo avanzado y transición hacia el modelo Zero Trust, se concluye que la reducción estructural de la superficie de ataque exige la centralización inmutable de registros en una plataforma SIEM/XDR de código abierto como Wazuh. La automatización de la defensa activa mediante módulos de respuesta automática (Active Response), en sinergia con el endurecimiento basado en los CIS Benchmarks y la microsegmentación lógica inter-VLAN implementada en pfSense, transforma el esquema de seguridad reactivo de SecureNova Labs en una arquitectura de resiliencia proactiva cimentada bajo la premisa de asunción de brecha (Assume Breach).

Recomendaciones

Medidas Inmediatas

Deshabilitar de forma definitiva el soporte del protocolo SMBv1 en todo el segmento corporativo y aplicar la actualización de seguridad correspondiente al boletín MS17-010.

- *Criterio de seguimiento:* Validación con nuevos escaneos de vulnerabilidades periódicos (utilizando scripts de enumeración como smb-os-discovery de Nmap) para certificar el cierre definitivo del puerto TCP 445 frente a tráfico no cifrado en todos los hosts de la red.

Medidas de Mediano Plazo

Configurar los Endpoints alineados con el Nivel 1 de los CIS Benchmarks, forzando mediante Políticas de Grupo (GPO) que el Firewall nativo permanezca activo sin permitir modificaciones por parte de los usuarios locales.

- *Criterio de seguimiento:* Auditoría de reglas y políticas de seguridad en el Directorio Activo de forma mensual, comprobando la correcta distribución y cumplimiento de las GPOs en el 100% de los endpoints corporativos.

Implementar una plataforma SIEM/XDR de licenciamiento Open Source (Wazuh) para alertar la creación de usuarios locales y la adición a grupos privilegiados.

- *Criterio de seguimiento:* Ejecución de pruebas controladas trimestrales (emulación de persistencia) para evaluar la ingesta de telemetría y la revisión de eventos críticos en el SOC, verificando que las reglas correlacionadas disparen adecuadamente las alertas para los Event IDs 4720 y 4732.

Acciones Permanentes

Formalizar los Acuerdos de Confidencialidad (NDA) y de Operación (RoE) de modo que delimiten claramente la autorización, el alcance, las responsabilidades y el tratamiento de evidencias de las auditorías, evitando cláusulas contrarias a la Ley 1273 de 2009 y al Código de Ética del COPNIA.

- *Criterio de seguimiento:* Revisión jurídica y documental anual respaldada por indicadores de cumplimiento corporativo, certificando que la totalidad de los contratos de ciberseguridad incluyan cláusulas de exención de responsabilidad penal actualizadas.

Transitar hacia un modelo arquitectónico *Zero Trust* complementado con ejercicios continuos de *Purple Teaming,* asegurando que la inteligencia obtenida de ataques simulados fortalezca permanentemente las reglas de detección del equipo defensivo.

- *Criterio de seguimiento:* Evaluación constante mediante indicadores de cumplimiento (KPIs del SOC), demostrando una reducción cuantificable en el Tiempo Promedio de Detección (MTTD) y una mejora progresiva tras cada ejercicio colaborativo de simulación de amenazas.

Referencias Bibliográficas

Alhamed, M., & Rahman, M. H. (2023). A systematic literature review on penetration testing in networks: Future Research directions. *Applied Sciences, 13*(12), 6986. https://doi.org/10.3390/app13126986

Center for Internet Security [CIS]. (2024). *CIS Benchmarks: Secure configuration guidelines.* https://www.cisecurity.org/cis-benchmarks/

Centro de Respuestas a Incidentes Informáticos [CSIRT Académico UNAD]. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información unadistas.* Universidad Nacional Abierta y a Distancia.

Chindruş, C., & Căruntu, C.-F. (2024). Enhancing cybersecurity readiness through the red and blue team competition. *Information, 14*(11), 587. https://doi.org/10.2478/bipie-2023-0008

Chopra, D. S., Kotwani, B., & Sawant, M. R. (2023). Red teaming vs. blue teaming: A comparative analysis of cybersecurity strategies in the digital battlefield. *International Journal of Scientific Research in Engineering and Management, 7*(12), 1-11.

Congreso de la República de Colombia. (2003). *Ley 842 de 2003: Por la cual se modifica la reglamentación del ejercicio de la ingeniería y se adopta el Código de Ética Profesional.* Diario Oficial No. 45.340.

Congreso de la República de Colombia. (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".* Diario Oficial No. 47.223.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial No. 48.587.

Instituto Nacional de Ciberseguridad [INCIBE]. (2018). *Guía de gestión de crisis de ciberseguridad en empresas.* INCIBE-CERT.

Lockheed Martin Corporation. (2023). *The cyber kill chain: Seven steps to a successful cyberattack.* Lockheed Martin Cyber Solutions.

Microsoft Corporation. (2025). *Detect, enable, and disable SMBv1, SMBv2, and SMBv3 in Windows.* Microsoft Learn.

MITRE Corporation. (2020). *MITRE ATT&CK: Design and philosophy.* The MITRE Corporation.

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

Wazuh, Inc. (s.f.). *Wazuh documentation: Active response.* Wazuh Open Source XDR.

Zambrano Hernández, L. F., Cárdenas Corral, L., Peña Hidalgo, H., & Cárdenas, N. R. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad.* Sello Editorial UNAD.

Apéndices

Apéndice A

Resultado de revisión en Turnitin

Número del intento	Este es el intento 1.
Estado de la entrega	Enviado para calificar
Estado de la calificación	Sin calificar
Tiempo restante	La tarea fue enviada 1 hora 4 minutos antes de la fecha límite
Última modificación	sábado, 30 de mayo de 2026, 22:50
Archivos enviados	Etapa_5_Informe_Final_Robinson_Gomez.pdf30 de mayo de 2026, 22:50 Turnitin ID: 2972927952 6%

Nota. Captura de pantalla del Entorno de Evaluación de la plataforma UNAD que evidencia el reporte de similitud generado por el sistema Turnitin. Se certifica un porcentaje general de similitud del 6% bajo el Submission ID 2972927952, dando cumplimiento a cabalidad con las políticas de originalidad y derechos de autor establecidas para el seminario especializado.

Apéndice B

Despliegue de Código para Hardening Automatizado (CIS Benchmarks)

Para garantizar la aplicación de las medidas a mediano plazo recomendadas por el Blue Team, se adjunta el script de automatización en PowerShell. Este código permite forzar el endurecimiento del Firewall nativo y deshabilitar protocolos obsoletos de manera masiva, alineándose con las directrices internacionales del *Center for Internet Security* (CIS Benchmarks).

```
    # Script de Hardening de Ciberseguridad para SecureNova Labs
    # Propósito: Mitigación de movimiento lateral y deshabilitación de SMBv1
    # Ejecución: Requiere privilegios de Administrador Local o despliegue vía GPO

    Write-Host "Iniciando proceso de endurecimiento del sistema..." -ForegroundColor Cyan

    # 1. Deshabilitar el protocolo vulnerable SMBv1 en el Registro de Windows
    Write-Host "Deshabilitando SMBv1..." -ForegroundColor Yellow
    Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -Name SMB1 -Type DWORD -Value 0 -Force
```

```
    Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\mrxsmb10" -Name Start -Type
DWORD -Value 4 -Force

    # 2. Habilitar y forzar el uso de SMBv2/SMBv3
    Write-Host "Asegurando el uso exclusivo de SMBv2 y SMBv3..." -
ForegroundColor Yellow
    Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -
Name SMB2 -Type DWORD -Value 1 -Force

    # 3. Configuraciones estrictas del Firewall de Windows (CIS Nivel
1)
    Write-Host "Aplicando políticas de Windows Defender Firewall..."
-ForegroundColor Yellow
    # Activar firewall en todos los perfiles
    Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled
True
    # Bloquear tráfico de entrada por defecto
    Set-NetFirewallProfile -Profile Domain,Public,Private -
DefaultInboundAction Block
    # Permitir tráfico de salida por defecto
```

```
    Set-NetFirewallProfile -Profile Domain,Public,Private -
DefaultOutboundAction Allow

    # 4. Crear regla explícita de bloqueo para tráfico no cifrado en
el puerto 445
    Write-Host "Inyectando regla de bloqueo perimetral para el puerto
TCP 445..." -ForegroundColor Yellow
    New-NetFirewallRule -DisplayName "SOC_Block_Inbound_SMB" -
Direction Inbound -LocalPort 445 -Protocol TCP -Action Block -Profile
Any -Description "Bloqueo preventivo de red para mitigación de
propagación de ransomware y vulnerabilidades MS17-010"

    Write-Host "El proceso de hardening ha finalizado correctamente.
Se requiere reinicio del sistema." -ForegroundColor Green
```

Apéndice C

Playbook de Caza de Amenazas (Threat Hunting) para Persistencia de Cuentas

Este apéndice técnico proporciona la matriz de búsqueda estructurada para que los analistas del Centro de Operaciones de Seguridad (SOC) rastreen de forma proactiva la creación de cuentas fantasmas utilizando consultas KQL *(Kusto Query Language)* o sintaxis de búsqueda para integraciones en el stack analítico empleado por Wazuh SIEM.

- **Objetivo de la cacería (Hunt):** Identificar adversarios que han evadido la prevención perimetral y han establecido persistencia administrativa mediante la técnica MITRE ATT&CK T1136.001.
- **Fuentes de datos requeridas:**
    - Registros de Seguridad del Visor de Eventos de Windows (Security.evtx).
    - Telemetría de procesos del agente local de Wazuh
- **Procedimiento de búsqueda y correlación:** el análisis de la imagen forense se enfoca en identificar los rastros o Indicadores de Compromiso (IoC) dejados por el atacante. Los analistas del Blue Team buscan proactivamente los siguientes artefactos:
    - **Análisis de Colmenas del Registro (Registry Hives):** Se audita la colmena SAM y SYSTEM buscando discrepancias en los perfiles de usuario. Se verifica la creación de la cuenta no autorizada y su inclusión en las subclaves del grupo Administradores local.
    - **Prefetch y Amcache:** El análisis de los archivos .pf ubicados en C:\Windows\Prefetch revela la marca de tiempo exacta de ejecución de binarios sospechosos o herramientas nativas utilizadas maliciosamente, como net.exe y cmd.exe.

  - **Filtrado Base (Event ID 4720):** Filtrar todas las ocurrencias donde se ha creado una nueva cuenta de usuario local.
  - **Identificación de Patrones Anómalos:** Cruzar los resultados de creación de cuentas con horarios fuera de la jornada laboral habitual, lo cual representa una anomalía en el comportamiento de la gestión de TI.
  - **Correlación de Escalada (Event ID 4732):** Buscar si esa misma cuenta fue agregada al grupo local de Administradores (SID: S-1-5-32-544) en un lapso inferior a 5 minutos desde su creación.
  - **Búsqueda de Evasión de Defensas (Event ID 1102):** Investigar si, posterior a las acciones anteriores, se registra el evento de borrado intencional del registro de auditoría de seguridad para ocultar las huellas del Red Team.
- **Acción de Respuesta (Triage):** Si un analista detecta la secuencia completa (4720 → 4732 → 1102), clasifica el evento inmediatamente como un incidente P1 (Crítico), inicia el aislamiento lógico del host a través de pfSense y procede con la desactivación inmediata de la cuenta fraudulenta.