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

Andrés Leonardo Alarcón Salcedo

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización En Seguridad Informática

2025

Dedicatoria

A mi madre, por su ejemplo de vida, por inculcarme desde temprana edad los valores del respeto, la responsabilidad y el compromiso. Su apoyo incondicional ha sido una guía constante en mi formación personal y académica.

A mi esposa, por su compañía leal y su fortaleza durante cada etapa de este proceso. Su comprensión, paciencia y aliento fueron fundamentales para alcanzar este objetivo.

A mis hijos, razón esencial de mi esfuerzo diario. Que este logro represente para ustedes un testimonio del valor del estudio, la perseverancia y el trabajo honesto como camino hacia la superación personal y profesional.

Agradecimientos

A Dios, por concederme la vida, la salud y la fortaleza para culminar esta etapa académica, y por ser guía constante en cada paso del camino.

A la Universidad Nacional Abierta y a Distancia – UNAD, por brindar un modelo educativo inclusivo, flexible y de alta calidad, que permite el acceso al conocimiento y el desarrollo profesional en distintos contextos.

A los docentes y tutores del programa de Especialización en Seguridad Informática, por su orientación académica, compromiso y disposición permanente para apoyar la formación integral de los estudiantes.

A mi familia, por su respaldo emocional y su confianza en mis capacidades. En especial a mi madre, esposa e hijos, quienes han sido el motor de este logro y cuyo amor y apoyo han sido determinantes en la culminación de este proceso.

A mis compañeros de estudio, por el intercambio de conocimientos, la colaboración y el compañerismo que enriquecieron significativamente esta experiencia académica.

A todas las personas y entidades que, directa o indirectamente, aportaron a la construcción de este trabajo, mi más sincero agradecimiento.

Resumen

El presente informe consolida los hallazgos obtenidos durante las Etapas 2, 3 y 4 del proceso evaluativo desarrollado para SecureNova Labs, integrando el análisis de los aspectos legales, la ejecución de operaciones ofensivas tipo Red Team y la evaluación de la defensa operativa desde el enfoque Blue Team. En la Etapa 2 se examinó el marco ético y normativo aplicable, identificando inconsistencias en el Acuerdo de Confidencialidad propuesto por la organización y su conflicto con la Ley 1273 de 2009 y los lineamientos del COPNIA. Posteriormente, en la Etapa 3 se llevó a cabo un ataque controlado que permitió evidenciar una fuga de información en Host-A, la explotación de una vulnerabilidad crítica (CVE-2014-6287), el acceso no autorizado mediante Metasploit y el movimiento lateral hacia Host-B, demostrando el compromiso integral del entorno. Finalmente, en la Etapa 4 se analizó la respuesta defensiva ante el incidente, documentando acciones de contención, análisis en tiempo real, procesos de hardenización y la aplicación de controles CIS, SIEM y herramientas especializadas de contención. El informe presenta una visión integral del ciclo de ciberseguridad, resaltando debilidades técnicas, fallos de control y recomendaciones estratégicas orientadas a fortalecer la postura de seguridad y la madurez organizacional frente a amenazas reales.

Palabras clave: Blue Team, Contención, Legalidad, Red Team, Vulnerabilidad

Abstract

This report consolidates the findings obtained during Stages 2, 3, and 4 of the evaluative process conducted for SecureNova Labs, integrating the analysis of legal aspects, the execution of offensive Red Team operations, and the assessment of operational defense from a Blue Team perspective. In Stage 2, the applicable ethical and regulatory framework was examined, identifying inconsistencies in the proposed Non-Disclosure Agreement and its conflict with Law 1273 of 2009 and COPNIA guidelines. Subsequently, in Stage 3, a controlled attack was carried out, revealing an information leak on Host-A, the exploitation of a critical vulnerability (CVE-2014-6287), unauthorized access through Metasploit, and lateral movement toward Host-B, demonstrating a full compromise of the environment. Finally, in Stage 4, the defensive response to the incident was analyzed, documenting containment actions, real-time analysis, hardening processes, and the application of CIS Controls, SIEM solutions, and specialized containment tools. The report provides a comprehensive view of the cybersecurity lifecycle, highlighting technical weaknesses, control failures, and strategic recommendations aimed at strengthening the security posture and organizational maturity against real-world threats.

Keywords: Blue Team, Containment, Legality, Red Team, Vulnerability

Tabla de Contenido

Glosario 12

Introducción 15

Justificación 16

Objetivos 17

Objetivo General 17

Objetivos Específicos 17

CAPÍTULO 1. 18

ASPECTOS LEGALES Y ÉTICOS EN LA OPERACIÓN DE CIBERSEGURIDAD 18

Introducción al Marco Normativo en Ciberseguridad 18

Análisis del Acuerdo de Confidencialidad Presentado por SecureNova Labs 19

Vulneración de la Ley 1273 de 2009 20

Impacto Ético Según el COPNIA 21

Riesgos Penales para el Profesional Firmante 21

Responsabilidad Corporativa y Gobernanza en Seguridad 22

Importancia del Cumplimiento Normativo en Organizaciones de Ciberseguridad 22

Análisis Crítico del Caso SecureNova Labs 23

Conclusión Parcial 24

Relación Entre Responsabilidad Profesional y Responsabilidad Penal 24

Deber de Denuncia y Protección del Interés Público 25

Análisis por Uso de Software Potencialmente Ilegal 25

Ética Organizacional y Cultura Corporativa en Seguridad Informática 26

Riesgos de Contratos Abusivos en la Industria de la Ciberseguridad 27

Análisis Comparativo con Normas Internacionales de Buenas Prácticas 28

Riesgos para Terceros y Responsabilidad Civil 28
Relevancia de la Ética Profesional Frente a Incentivos Económicos 29
Conclusión 29
CAPÍTULO 2 31
OPERACIONES RED TEAM Y ANÁLISIS OFENSIVO 31
Introducción al escenario Ofensivo 31
Preparación del Entorno de Ataque 31
Reconocimiento Inicial: Identificación de Dispositivos y Servicios 32
Identificación del servicio vulnerable en Host-A 33
Explotación del Servicio Rejetto HFS (CVE-2014-6287) 35
Validación del Nivel de Acceso y Escalamiento de Privilegios 36
Post-Explotación: Recolección Inicial de Evidencias 37
Pivoting: Movimiento Lateral hacia Host-B 37
Compromiso de Host-B: Ejecución de Prueba de Concepto 39
Análisis Forense del Vector Inicial de Compromiso 40
Reconstrucción de la Cadena de Ataque (Cyber Kill Chain) 41
Evidencia del Comando y Control Establecido 42
Recolección de Información de Valor (LOOTING) 43
Uso de Módulos de Post-Explotación en Host-A 44
Análisis del Movimiento Lateral hacia Host-B 44
Persistencia en Host-B 45
Documentación Final de la Operación Ofensiva 45
Evaluación de la Superficie de Exposición 46
Riesgos Asociados a la Falta de Segmentación 46

Riesgos Asociados al Uso de Aplicaciones Desactualizadas 47
Riesgos Derivados de Permisos Elevados en Servicios Windows 48
Impacto Global del Ataque 49
Metodología Utilizada 50
Relación entre la Operación Red Team y la Respuesta Blue Team 51
Conclusión del Capítulo 2 52
CAPÍTULO 3 54
ANÁLISIS DEFENSIVO: OPERACIÓN BLUE TEAM 54
Introducción al Enfoque Defensivo 54
Reconstrucción inicial del incidente y análisis de evidencias 54
Identificación del vector de ataque 56
Detección del escalamiento de privilegios 56
Movimiento lateral y compromiso del segundo host 57
Indicadores de Ataque e Indicadores de Compromiso 58
Detección tardía y respuesta inicial del equipo defensor 59
Validación del nivel real del compromiso 59
Protección de la evidencia digital y cadena de custodia 61
Análisis en tiempo real frente a análisis post incidente 61
Identificación de mecanismos de persistencia 62
Aislamiento de los sistemas comprometidos 63
Eliminación de cuentas creadas por el atacante 64
Dificultades derivadas de la falta de herramientas de seguridad 65
Impacto operativo del incidente 65
Lecciones estratégicas obtenidas del incidente 66

Importancia del análisis posterior al incidente 67

Aplicación de medidas de hardenización..... 67

Necesidad de segmentación interna y Zero Trust..... 68

Incorporación de indicadores de compromiso e indicadores de ataque 68

El papel del CIS como marco de referencia defensivo..... 69

Integración de un sistema SIEM dentro de la infraestructura..... 69

Uso de herramientas especializadas para contención de ataques 70

Mejoras estructurales en la respuesta a incidentes..... 70

Conclusión del Capítulo 3 71

Evidencias de Sustentación.....72

Conclusiones.....73

Recomendaciones 74

Referencias Bibliográficas.....76

Apéndices.....78

Lista de Figuras

Figura 1. *Verificación de comunicación entre Parrot y Host-A.* 32

Figura 2. *Resultado del escaneo Nmap de la red 192.168.56.0/24.* 33

Figura 3. *Identificación del Servicio Rejetto HFS* 34

Figura 4. *Configuración del exploit* 35

Figura 5. *Sesión Meterpreter (sysinfo - getuid)* 36

Figura 6. *Escalamiento de privilegios y verificación de sesión privilegiada.* 36

Figura 7. *Autoroute* 38

Figura 8. *Configuración de autoroute y port forwarding para pivoting* 38

Figura 9. *Movimiento Lateral* 39

Figura 10. *Creacion de usuario AndresAlarcon1982* 39

Figura 11. *Evidencia del servicio HFS ejecutándose en el sistem*a 41

Figura 12. *Control de la máquina* 43

Figura 13. *getsystem o uid = NT AUTHORITY\SYSTEM.* 48

Figura 14. *Flujo metodológico Red Team* 51

Figura 15. *Event Viewer o ejecución sospechosa en Host-A* 55

Figura 16. *Escalamiento de privilegios* 57

Figura 17. *Esquema grafico de Pivoting* 58

Figura 18. *comandos o evidencia de ejecución tardía del análisis.* 59

Figura 19. *Creación de usuario en Host-B.* 60

Figura 20. *Persistencia creada en Host-B* 63

Figura 21. *Procedimiento utilizado para aislamiento.* 64

Figura 22. *Cuentas Administradores* 64

Figura 23. *Eliminación de usuario creado* 65

Lista de Apéndices

Apéndice A.. 78

Glosario

Acceso no autorizado:

Acción mediante la cual un usuario o proceso ingresa a un sistema informático sin los permisos correspondientes, ya sea por explotación de una vulnerabilidad o por uso indebido de credenciales.

Amenaza persistente avanzada (APT):

Tipo de ataque desarrollado por actores con alta capacidad técnica que buscan mantener presencia prolongada dentro de un sistema con fines de espionaje, exfiltración o sabotaje.

Ataque lateral (Lateral Movement):

Técnica utilizada por un atacante que, tras comprometer un equipo inicial, se desplaza a través de la red interna para obtener acceso a otros sistemas y recursos.

Blue Team:

Equipo especializado en la defensa de infraestructuras tecnológicas mediante monitoreo, detección, contención y respuesta a incidentes de ciberseguridad.

Cadena de custodia:

Procedimiento legal y técnico mediante el cual la evidencia digital es recolectada, almacenada y preservada, garantizando su validez y autenticidad durante procesos de análisis o investigación judicial.

Ciberseguridad:

Conjunto de técnicas, políticas y herramientas enfocadas en la protección de sistemas informáticos, datos, redes y usuarios frente a amenazas internas o externas.

Confidencialidad:

Principio de seguridad orientado a garantizar que la información solo puede ser accedida por personas autorizadas.

Contención:

Conjunto de acciones técnicas que buscan detener temporalmente un ataque para evitar su expansión o reinfección dentro de una infraestructura.

CVE (Common Vulnerabilities and Exposures):

Sistema de referencia internacional que identifica y publica vulnerabilidades conocidas en software y hardware.

Escalada de privilegios:

Procedimiento mediante el cual un atacante incrementa su nivel de acceso dentro de un sistema hasta obtener permisos administrativos o de sistema.

Explotación (Exploit):

Fase del ataque donde se ejecuta una vulnerabilidad con el fin de comprometer un sistema, modificar su funcionamiento o instalar software malicioso.

Hardenización:

Proceso mediante el cual un sistema operativo o aplicación es ajustado para reducir la superficie de ataque, eliminar servicios innecesarios y reforzar sus medidas de protección.

Indicador de ataque (IoA):

Evidencia técnica que permite identificar actividades relacionadas con la ejecución actual de un ataque dentro de un sistema.

Indicador de compromiso (IoC):

Evidencia observable que demuestra que un sistema ha sido previamente comprometido, por ejemplo archivos modificados, conexiones sospechosas o creación de usuarios no autorizados.

Intrusión:

Cualquier acción no autorizada que permite ingresar a un sistema o red, vulnerando las políticas de seguridad establecidas.

Movimiento lateral:

Técnica ofensiva que permite al atacante desplazarse desde un sistema comprometido hacia otras máquinas dentro de la misma red interna.

Persistencia:

Capacidad del atacante para mantener acceso continuo a un sistema incluso después de reinicios, acciones defensivas o eliminación de software malicioso.

Pivoting:

Método empleado por un atacante para utilizar un equipo ya comprometido como puente hacia otros sistemas dentro de la red interna.

Red Team:

Equipo dedicado a realizar actividades ofensivas controladas con el objetivo de evaluar la seguridad de una infraestructura, identificar vulnerabilidades y simular ataques reales.

Segmentación de red:

Mecanismo mediante el cual se divide una red en segmentos independientes para limitar la propagación de amenazas y reducir la exposición interna.

SIEM (Security Information and Event Management):

Herramienta especializada que centraliza eventos de seguridad, correlaciona comportamientos sospechosos y genera alertas automáticas frente a incidentes.

Vulnerabilidad:

Debilidad técnica, lógica o de configuración que puede ser aprovechada por un atacante para comprometer sistemas, datos o usuarios.

Introducción

El presente informe técnico consolida los resultados obtenidos durante las Etapas 2, 3 y 4 del proceso desarrollado para SecureNova Labs, en el marco del seminario Red Team & Blue Team. Su propósito es analizar los aspectos legales observados en la documentación entregada, reconstruir la operación ofensiva ejecutada durante la fase Red Team y examinar la respuesta defensiva aplicada desde la perspectiva del Blue Team. (Congreso de la República, 2009; COPNIA, 2008).

En primer lugar, se evaluaron los elementos normativos presentes en los documentos de la organización, evidenciando posibles infracciones a la Ley 1273 de 2009 y discrepancias con los principios éticos del ejercicio profesional. Posteriormente, se llevó a cabo una operación ofensiva controlada que permitió comprometer Host-A mediante la explotación de una vulnerabilidad crítica, escalar privilegios y realizar movimiento lateral hacia Host-B, demostrando la debilidad estructural de la infraestructura evaluada. Finalmente, desde la defensa, se analizaron los mecanismos de detección, contención y respuesta, resaltando la ausencia de monitoreo, herramientas preventivas y políticas adecuadas para mitigar incidentes en tiempo real.

El informe integra estas perspectivas con el fin de aportar una visión completa del incidente y establecer recomendaciones que permitan fortalecer la postura de ciberseguridad de SecureNova Labs frente a futuras amenazas.

Justificación

Este informe es necesario para evaluar de forma integral las capacidades técnicas, legales y operativas aplicadas durante las Etapas 2, 3 y 4 del proceso en SecureNova Labs. La revisión del marco ético y normativo permite identificar riesgos legales asociados a prácticas inapropiadas dentro de la organización. El desarrollo ofensivo Red Team demuestra la importancia de detectar vulnerabilidades reales mediante explotación controlada, mientras que el análisis Blue Team evidencia la capacidad de responder, contener y mitigar un incidente activo.

La integración de estos tres componentes justifica la elaboración del informe, al ofrecer una visión completa del ciclo de ciberseguridad y aportar insumos clave para fortalecer la postura defensiva y operativa de SecureNova Labs.

Objetivos

Objetivo General

Analizar el impacto de los aspectos legales, las actividades ofensivas Red Team y las acciones defensivas Blue Team dentro de los escenarios evaluados en SecureNova Labs, con el fin de comprender las causas del incidente, sus efectos sobre la infraestructura y las soluciones estratégicas necesarias para fortalecer la postura de ciberseguridad de la organización.

Objetivos Específicos

Identificar los factores legales, técnicos y operativos que contribuyeron al incidente de seguridad presentado en SecureNova Labs, a partir de la revisión de la normativa vigente y la documentación analizada en la Etapa 2.

Describir las vulnerabilidades explotadas, las técnicas de ataque empleadas y el impacto generado durante la operación Red Team, con base en el análisis de las evidencias obtenidas en la Etapa 3.

Evaluar las acciones de detección, contención y respuesta implementadas en el ejercicio Blue Team, considerando los procedimientos documentados en la Etapa 4, con el fin de proponer medidas de mejora y fortalecimiento de la postura defensiva de la organización.

CAPÍTULO 1.

ASPECTOS LEGALES Y ÉTICOS EN LA OPERACIÓN DE CIBERSEGURIDAD

Introducción al Marco Normativo en Ciberseguridad

El ámbito de la ciberseguridad corporativa requiere una comprensión clara de las obligaciones legales, éticas y profesionales que rigen la interacción con sistemas informáticos, datos sensibles y plataformas tecnológicas. La Etapa 2 del proceso evaluativo para SecureNova Labs puso en evidencia la necesidad de analizar documentos internos y contratos con la rigurosidad que exige la legislación colombiana, especialmente al considerar que las organizaciones pueden incurrir en prácticas que comprometen la legalidad y la integridad profesional de sus analistas.

El acuerdo presentado en los anexos incluía disposiciones que contradecían principios fundamentales de la Ley 1273 de 2009, la cual define y sanciona los delitos informáticos en Colombia. Asimismo, planteaba cláusulas que pretendían limitar el derecho del profesional a informar irregularidades, lo que representa un riesgo ético significativo para cualquier especialista en seguridad. (Congreso de la República de Colombia, 2009).

Desde el punto de vista ético, estas prácticas vulneran los principios establecidos en el **Código de Ética Profesional del Ingeniero**, el cual exige que el ejercicio de la ingeniería se realice con integridad, responsabilidad social y respeto por el marco legal vigente (Consejo Profesional Nacional de Ingeniería [COPNIA], 2008).

Este capítulo desarrolla un análisis exhaustivo del marco normativo aplicable, las cláusulas irregulares del acuerdo, los riesgos penales asociados y los principios éticos comprometidos según el COPNIA.

Análisis del Acuerdo de Confidencialidad Presentado por SecureNova Labs

El documento entregado para evaluación contenía múltiples elementos que, desde un punto de vista jurídico y técnico, representan riesgos legales tanto para el firmante como para la organización. No solo se describían actividades consideradas delitos informáticos, sino que se pretendía clasificarlas como información confidencial, obligando al aspirante a mantener silencio frente a posibles actos ilícitos.

Entre los puntos más relevantes se identificaron:

1. Inclusión de términos que normalizan actividades ilegales.

El acuerdo hace referencias explícitas a “datos de chuzadas”, “interceptación de información” y “accesos abusivos a sistemas”. Estos elementos coinciden directamente con definiciones tipificadas en la Ley 1273 de 2009. La clasificación de actividades ilícitas como información protegida constituye una manipulación conceptual que intenta encubrir delitos bajo la Figura de confidencialidad corporativa.

2. Prohibición de denuncia ante autoridades.

Frases como “abstenerse de denunciar actividades sospechosas de espionaje” buscan impedir el ejercicio del deber ciudadano de denunciar conductas ilegales. Un acuerdo que limita la acción legal del profesional lo expone a ser cómplice, sin protección jurídica.

3. Traslado de responsabilidad penal al aspirante.

El documento estipulaba que, en caso de encontrarse información ilegal en manos del estudiante, este debía eximir de responsabilidad a la empresa, lo que constituye una práctica contractual abusiva.

Estas irregularidades justifican un análisis profundo de los artículos vulnerados y del impacto profesional para el aspirante.

Vulneración de la Ley 1273 de 2009

La Ley 1273 creó un nuevo bien jurídico tutelado: la protección de datos y la información. Esta norma define múltiples delitos informáticos y establece sanciones para quienes lleven a cabo manipulaciones no autorizadas de sistemas y datos.

Dentro del acuerdo cuestionado, se identifican vulneraciones a los siguientes artículos:

Artículo 269A – Acceso abusivo a un sistema informático.

El documento de SecureNova Labs describe como "información confidencial" actividades que implican acceso a sistemas sin autorización. Al exigir que esta información sea encubierta, se incurre en complicidad indirecta.

Artículo 269B – Interceptación de datos informáticos.

El término "chuzadas" hace referencia a interceptaciones ilegales. Clasificarlas como información interna viola directamente este artículo.

Artículo 269E – Violación de datos personales.

Dar trato confidencial a actividades de apropiación de información de terceros implica validar una conducta tipificada como delito.

Artículo 269F – Transferencia no consentida de activos.

La fuga de información, propia del escenario evaluado, también relaciona este artículo.

Las actividades descritas no pueden ser legitimadas mediante acuerdos privados. Esto posiciona al aspirante en una situación de riesgo jurídico, pues su firma podría interpretarse como aceptación o complicidad en prácticas criminales.

Impacto Ético Según el COPNIA

El Código de Ética Profesional del COPNIA establece que los ingenieros —incluyendo aquellos especializados en ciberseguridad— deben actuar con integridad, responsabilidad social y respeto por el marco legal. Los principios fundamentales incluyen:

- Actuar siempre en defensa del bienestar público.
- No participar en actividades ilícitas, fraudulentas o contrarias al interés general.
- Denunciar prácticas que representen riesgo para la sociedad.

El acuerdo analizado en Etapa 2 contradice estos principios, pues no solo intenta normalizar actividades ilegales, sino que solicita explícitamente que no se denuncien. Esto implica un conflicto ético insalvable para cualquier profesional responsable.

El aspirante que firme dicho acuerdo compromete su reputación profesional, su integridad ética y su cumplimiento legal, elementos clave en la práctica de la ingeniería y la seguridad informática.

Riesgos Penales para el Profesional Firmante

Firmar un acuerdo con contenido ilegal no exime de responsabilidad penal al firmante. De hecho, podría generar:

1. Complicidad en delitos informáticos.

   La omisión de denuncia o el encubrimiento pueden ser interpretados como participación no directa.

2. Pérdida de credenciales profesionales.

   Un proceso disciplinario en el COPNIA puede inhabilitar al profesional.

3. Riesgo reputacional severo.

   Participar en actividades informáticas ilícitas afecta la credibilidad ante cualquier organización seria de ciberseguridad.

4. Sanciones económicas o privación de libertad.

   La Ley 1273 contempla penas que pueden alcanzar varios años de prisión.

Por tanto, la no aceptación de las condiciones del acuerdo no es solo una postura ética, sino una necesidad legal.

Responsabilidad Corporativa y Gobernanza en Seguridad

Más allá del análisis individual, este escenario expone una debilidad severa de gobernanza interna en SecureNova Labs, donde documentos corporativos contradicen la legislación vigente. Los aspectos observados sugieren:

- Falta de cultura ética.
- Riesgos reputacionales críticos.
- Debilidad en el cumplimiento normativo (compliance).
- Políticas mal implementadas o inexistentes.
- Deficiencias en roles y responsabilidades internas.

Una organización que valide actividades ilegales compromete también su solvencia a nivel operativa, contractual y regulatoria.

Importancia del Cumplimiento Normativo en Organizaciones de Ciberseguridad

Las empresas dedicadas a la ciberseguridad deben ser modelos de cumplimiento. No solo manipulan información sensible, sino que tienen acceso privilegiado a datos y sistemas de terceros.

Por ello, deben garantizar:

- Transparencia operativa.
- Procesos éticos de manejo de información.
- Respeto estricto de la ley.
- Auditorías internas frecuentes.
- Documentación contractual sin ambigüedades.

El acuerdo evaluado viola estos principios, lo cual genera dudas sobre la madurez organizacional de SecureNova Labs.

Análisis Crítico del Caso SecureNova Labs

El caso presentado revela un choque entre la imagen corporativa que la empresa desea proyectar y las prácticas reales sugeridas en su documentación interna. Una compañía que aspira a reclutar expertos en seguridad no puede simultáneamente solicitar acciones que violen leyes nacionales o principios profesionales.

Esto permite identificar problemas estructurales como:

- Falta de liderazgo ético.
- Procesos de selección manipulativos o coercitivos.
- Posibles actividades extra legales dentro del entorno operativo.
- Uso indebido de Figuras legales como los acuerdos de confidencialidad.

Este análisis es esencial para comprender los riesgos asociados al ejercicio del rol en dicha organización.

Conclusión Parcial

El estudio del acuerdo y del marco normativo evidencia una grave incongruencia entre las prácticas esperadas de una entidad de ciberseguridad y los estándares legales y éticos que deben regir su actuación. Las cláusulas analizadas violan disposiciones de la Ley 1273 de 2009, contradicen los lineamientos del COPNIA y exponen al aspirante a riesgos significativos.

Este capítulo establece la base legal y ética para comprender la gravedad del escenario, permitiendo una transición hacia el análisis técnico desarrollado en las etapas posteriores.

Relación Entre Responsabilidad Profesional y Responsabilidad Penal

En el ámbito de la ciberseguridad, la delgada línea entre la responsabilidad profesional y la responsabilidad penal se vuelve crítica cuando un analista participa, directa o indirectamente, en actividades que pueden ser tipificadas como delito. La Etapa 2 permitió identificar cómo un documento aparentemente administrativo puede comprometer al profesional, aun sin que este realice directamente una acción ilícita. En derecho penal moderno, la complicidad, la omisión de denuncia y el encubrimiento son conductas claramente sancionables bajo la legislación colombiana.

La responsabilidad profesional, por otra parte, implica la obligación de ejercer la ingeniería de manera ética, competente y dentro del marco normativo aplicable. Al firmar documentos con cláusulas irregulares, el profesional estaría demostrando una falta grave a su deber de diligencia. Esta combinación de responsabilidades —profesional y penal— convierte la aceptación del acuerdo en un riesgo de dimensiones mucho mayores que las consecuencias propias de un simple incumplimiento contractual.

Deber de Denuncia y Protección del Interés Público

Uno de los elementos más problemáticos del acuerdo radica en la instrucción explícita de omitir la denuncia sobre actividades sospechosas de espionaje o apropiación indebida de información. En Colombia, tanto el Código Penal como la Ley 1273 y múltiples normas administrativas exigen que los ciudadanos informen a las autoridades cuando conozcan hechos que puedan constituir delito.

El deber de denunciar no es solo un principio ético, sino también una obligación legal en casos que involucren vulneración de datos, acceso no autorizado, fuga de información o manipulación ilícita de sistemas. Obligar contractualmente al aspirante a callar constituye un acto contrario al orden jurídico colombiano y un intento de manipular el ejercicio regular de la justicia.

Además, desde la perspectiva de la seguridad nacional y corporativa, la omisión de denuncia favorece la continuidad de delitos informáticos, afecta la cadena de custodia de la evidencia y puede derivar en consecuencias graves tanto para la empresa víctima como para terceros afectados. Este tipo de cláusulas coloca a SecureNova Labs en una posición riesgosa frente a auditorías, investigaciones judiciales y regulaciones sectoriales.

Análisis por Uso de Software Potencialmente Ilegal

El escenario planteado también permite reflexionar sobre las implicaciones legales del uso de herramientas, software o procedimientos que puedan ser catalogados como indebidos. La referencia dentro del acuerdo a realizar actividades de interceptación, acceso abusivo o manipulación de datos sin autorización sugiere prácticas incompatibles con los marcos regulatorios actuales.

Las empresas que emplean personal especializado en ciberseguridad deben estar alineadas con estándares internacionales de cumplimiento, auditoría y gobernanza. No hacerlo implica riesgos como:

- Procesos sancionatorios de entes reguladores.
- Pérdida de certificaciones y acreditaciones.
- Cierre de contratos comerciales con entidades públicas y privadas.
- Demandas por negligencia, omisión o mala práctica.
- Sanciones penales por actividades relacionadas con delitos informáticos.

El uso inapropiado de herramientas de ciberseguridad especialmente cuando se aplican fuera de un marco autorizado puede constituir delito, incluso si se realiza en entornos internos o presuntamente controlados.

Ética Organizacional y Cultura Corporativa en Seguridad Informática

La ética organizacional es un pilar central para cualquier entidad dedicada a servicios de ciberseguridad. Si la empresa no mantiene una cultura basada en transparencia, cumplimiento legal y gobernanza clara, su personal queda expuesto a incertidumbres operativas y riesgos penales. De manera preocupante, el acuerdo analizado refleja una cultura basada en el secretismo y la normalización de actividades contrarias a la ley.

Una cultura ética sólida en ciberseguridad debe incluir:

- Protocolos formales de manejo de incidentes.
- Líneas claras de divulgación de irregularidades.
- Procesos internos de auditoría y control.
- Capacitación continua en compliance y legislación vigente.
- Canal de denuncias seguro y protegido contra represalias.

- Documentación interna aprobada por áreas jurídicas competentes.

La ausencia de estos elementos abre la puerta a vulneraciones legales, fraudes, abuso de poder y manipulación de responsabilidades. Una organización que opera en el sector de ciberseguridad tiene la obligación de ser ejemplo de integridad, especialmente debido a la naturaleza confidencial y estratégica de la información que maneja.

Riesgos de Contratos Abusivos en la Industria de la Ciberseguridad

Los contratos abusivos son aquellos que establecen obligaciones desproporcionadas o ilegales para una de las partes. En el caso del acuerdo analizado, se identifican elementos que podrían ser considerados abusivos, tales como:

- Exigencia de confidencialidad sobre actividades ilegales.
- Renuncia obligada a mecanismos de protección legal.
- Exoneración total de responsabilidad penal para la empresa.
- Transferencia injustificada de culpa hacia el profesional.
- Cláusulas que contradicen derechos fundamentales.

Este tipo de prácticas no solo es ilegal, sino que también amenaza la estabilidad emocional y profesional del aspirante, quien podría verse obligado a elegir entre mantener su integridad o conservar un empleo.

Existen precedentes legales en los cuales contratos de esta naturaleza han sido declarados nulos, ya que ninguna entidad puede utilizar documentos privados para amparar actividades ilícitas.

Análisis Comparativo con Normas Internacionales de Buenas Prácticas

Las normas internacionales en ciberseguridad como ISO 27001, NIST 800-53, la RGPD europea o la norma ISO 27701 establecen principios que contradicen completamente lo propuesto en el acuerdo evaluado. Estas normas exigen:

- Protección adecuada de datos personales.
- Procesos auditables y transparentes.
- Documentación clara, lícita y verificable.
- Clasificación legítima de la información.
- Prohibición absoluta de ocultar actividades ilícitas.

SecureNova Labs, al presentar un acuerdo de estas características, contradice todos estos marcos, lo que indica una falta profunda de gobernanza corporativa y un desconocimiento de estándares internacionales que son obligatorios para empresas del sector.

Riesgos para Terceros y Responsabilidad Civil

Además del impacto directo sobre el profesional firmante, este tipo de acuerdos puede generar un impacto significativo sobre terceros, incluyendo clientes, socios comerciales y usuarios finales. Una empresa que normaliza actividades ilegales pone en riesgo:

- La privacidad de ciudadanos y empleados.
- Los contratos vigentes con entes gubernamentales.
- La confianza de clientes internacionales.
- El cumplimiento con regulaciones sectoriales.
- La estabilidad financiera en caso de sanciones.

La responsabilidad civil derivada de incidentes de fuga de información, espionaje o accesos indebidos puede alcanzar valores millonarios. Esto agrava la incertidumbre laboral del

profesional, quien podría terminar involucrado en procesos legales extensos sin protección jurídica.

Relevancia de la Ética Profesional Frente a Incentivos Económicos

El escenario plantea un sueldo atractivo y un contrato vitalicio, intentado mostrar un conflicto ético entre un beneficio económico y el cumplimiento legal. Sin embargo, aceptar una oferta que obliga a participar en actividades ilícitas no solo es contrario a la ética profesional, sino que además constituye un riesgo irreversible para la carrera del analista.

En la práctica, ningún incentivo económico justifica:

- La complicidad en delitos informáticos.
- El ocultamiento de actividades ilegales.
- La firma de contratos abusivos.
- La renuncia a principios esenciales del COPNIA.

Este análisis subraya la importancia de que las decisiones laborales en ciberseguridad se basen en valores éticos sólidos y no en beneficios económicos superficiales.

Conclusión

El análisis legal y ético realizado demuestra que el acuerdo presentado por SecureNova Labs vulnera múltiples disposiciones de la Ley 1273 de 2009, contradice los lineamientos del COPNIA y coloca al profesional en una posición de riesgo penal, civil y reputacional. Más allá del análisis técnico, este capítulo evidencia que las operaciones de ciberseguridad deben estar enmarcadas en principios de transparencia, legalidad y protección del interés público.

Este capítulo finaliza estableciendo un marco conceptual que permitirá comprender, en los capítulos siguientes, cómo estas irregularidades legales se conectan directamente con las vulnerabilidades técnicas explotadas en el entorno corporativo y la respuesta defensiva requerida.

CAPÍTULO 2

OPERACIONES RED TEAM Y ANÁLISIS OFENSIVO

Introducción al escenario Ofensivo

El Capítulo 2 desarrolla el análisis completo de la operación Red Team realizada durante la Etapa 3, cuyo propósito fue identificar, explotar y documentar una vulnerabilidad crítica en la infraestructura simulada de SecureNova Labs. El ejercicio permitió comprometer el Host-A mediante la explotación del servicio vulnerable Rejetto HFS 2.3.x, escalar privilegios, obtener una sesión remota Meterpreter y ejecutar técnicas de pivoting hacia Host-B.

Este capítulo describe detalladamente cada una de las fases del ataque, desde el reconocimiento inicial hasta la prueba de concepto final, en donde se logró crear un usuario administrativo efímero en Host-B. El proceso se abordó siguiendo la metodología tradicional del hacking ético, la cual contempla de manera estructurada las fases de reconocimiento, enumeración, explotación, post-explotación y movimiento lateral. Esta metodología permite evaluar de forma sistemática la superficie de ataque, identificar vulnerabilidades técnicas y comprender el impacto real que podría alcanzar un adversario dentro de una infraestructura comprometida (Harris, 2020).

Preparación del Entorno de Ataque

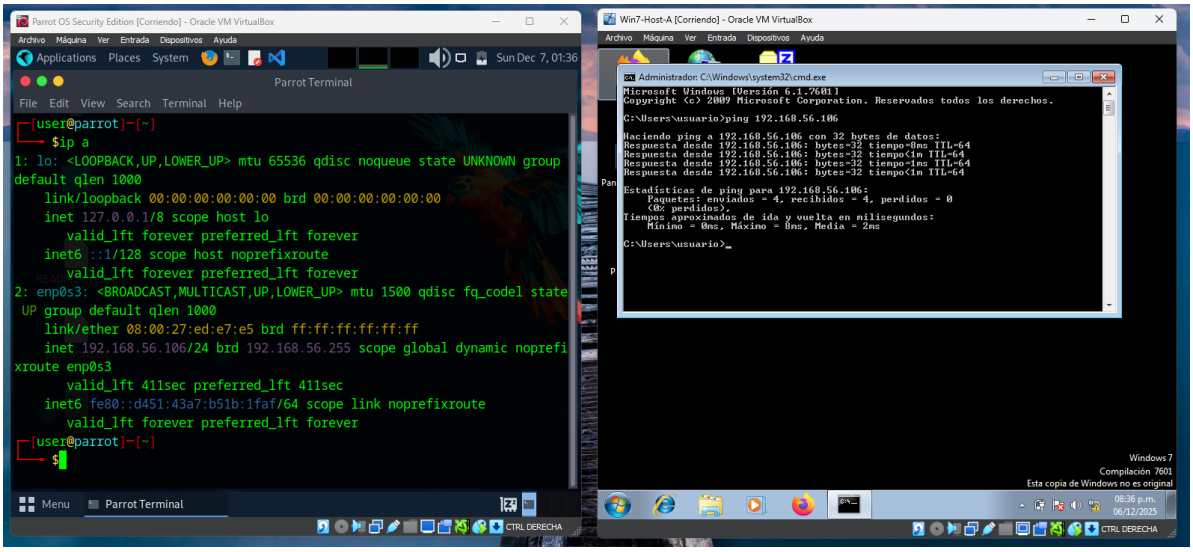
Antes de iniciar la operación ofensiva, se verificó la disponibilidad y correcta comunicación entre las máquinas virtuales del entorno de prueba. Para la ejecución del ataque se utilizó:

- Parrot OS Security Edition como equipo atacante.
- Host-A (Windows 7) como estación vulnerable.
- Host-B (Windows 7/Server) como objetivo secundario para movimiento lateral.

Se realizaron validaciones iniciales de red mediante ping y análisis de conectividad entre los hosts.

Figura 1.

Verificación de comunicación entre Parrot y Host-A.



Nota: Se verifica que tengamos comunicación entre la máquina Parrot OS y el Host-A

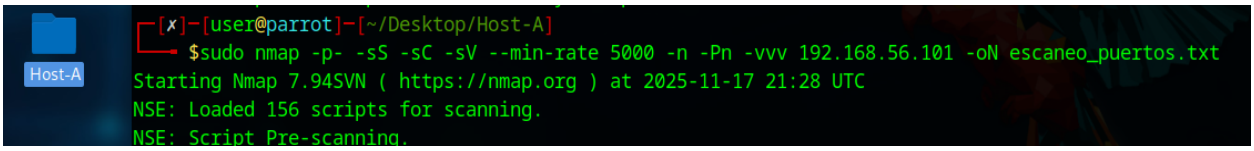
Reconocimiento Inicial: Identificación de Dispositivos y Servicios

El reconocimiento constituye la fase inicial dentro de un proceso formal de pentesting, y tiene como propósito delimitar el entorno tecnológico sobre el cual se desarrollarán las acciones ofensivas posteriores. En esta etapa se busca identificar los dispositivos presentes en la red, determinar su disponibilidad, observar posibles mecanismos de filtrado y comprender de manera general la superficie de ataque.

En el escenario propuesto, se empleó la herramienta Nmap para efectuar un escaneo de descubrimiento sobre la subred asignada, permitiendo detectar los hosts activos y los puertos expuestos en cada uno de ellos. Esta exploración inicial constituye un paso esencial, ya que proporciona una visión preliminar del entorno y posibilita establecer los vectores de ataque potencialmente aprovechables durante las siguientes fases del ejercicio ofensivo.

Figura 2.

Resultado del escaneo Nmap de la red 192.168.56.0/24.



Nota: Realizamos un escaneo de la red con Nmap 192.168.56.0/24

Durante el escaneo inicial se identificaron los siguientes hosts relevantes:

- Host-A: 192.168.56.101
- Atacante: 192.168.56.106

El análisis inicial de los resultados obtenidos evidenció que Host-A presentaba varios puertos abiertos, entre los cuales resultaba especialmente relevante el puerto 80/tcp. Dicho puerto correspondía a un servicio HTTP que, tras la fase de enumeración detallada, fue identificado como Rejetto HFS en una versión vulnerable. Esta aplicación es reconocida en la literatura especializada por poseer una vulnerabilidad crítica que permite la ejecución remota de código, situación que la convierte en un vector de ataque altamente viable dentro del presente escenario ofensivo.

Identificación del servicio vulnerable en Host-A

El análisis inicial de los resultados obtenidos evidenció que Host-A presentaba varios puertos abiertos, entre los cuales resultaba especialmente relevante el puerto 80/tcp. Dicho puerto correspondía a un servicio HTTP que, tras la fase de enumeración detallada, fue identificado como Rejetto HFS en una versión vulnerable. Esta aplicación es reconocida en la literatura especializada por poseer una vulnerabilidad crítica que permite la ejecución remota de código,

situación que la convierte en un vector de ataque altamente viable dentro del presente escenario ofensivo (OWASP Foundation, 2021).

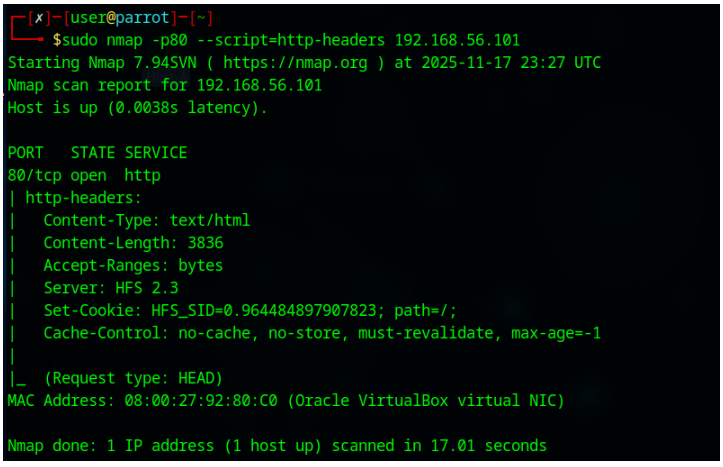
Tras identificar el puerto 80/tcp abierto, el siguiente paso consistió en determinar qué servicio se encontraba en ejecución. Se utilizó nuevamente Nmap, esta vez con scripts de enumeración:

sudo nmap -sV -p80 --script=http-headers 192.168.56.101

El análisis de los encabezados del servicio permitió observar de manera explícita que se trataba de Rejetto HFS en su versión 2.3.x, software que ha sido ampliamente documentado en la comunidad de ciberseguridad debido a la vulnerabilidad **CVE-2014-6287**, la cual posibilita la ejecución remota de código sin necesidad de autenticación previa. Este tipo de vulnerabilidades evidencian la falta de procesos formales de gestión de parches y control de software, situación ampliamente documentada en escenarios reales de compromiso (Mandiant, 2022).

Figura 3.

Identificación del Servicio Rejetto HFS



Nota: Identificamos del servicio Rejetto HFS la vulnerabilidad CVE-2014-6287

Explotación del Servicio Rejetto HFS (CVE-2014-6287)

Una vez identificado el servicio vulnerable, se procedió a emplear Metasploit Framework como plataforma principal para la explotación. Esta herramienta constituye un estándar dentro de los entornos ofensivos profesionales, dado que integra módulos específicos para el análisis, explotación y post-explotación de vulnerabilidades conocidas, permitiendo automatizar procedimientos y asegurar una ejecución técnica controlada durante las pruebas.

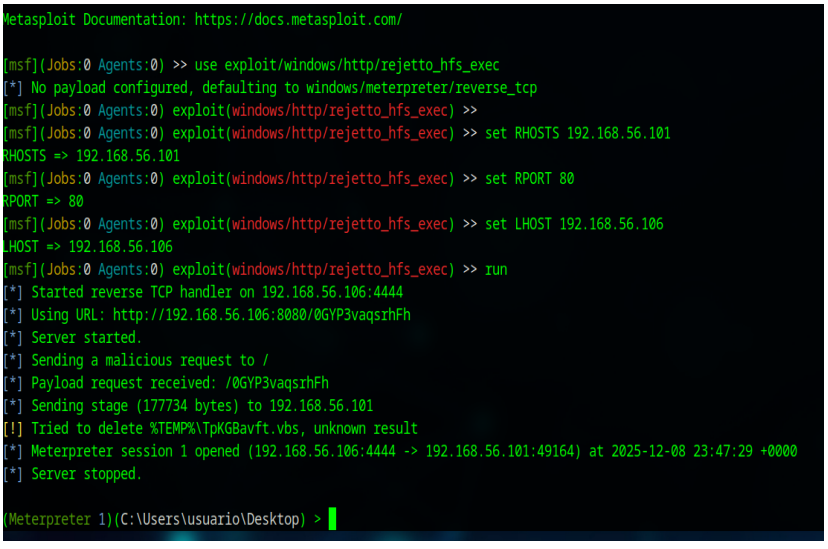
Sudo mfsconsole

Los parámetros configurados fueron:

- RHOSTS → IP del Host-A
- LHOST → IP del equipo atacante
- Payload → Meterpreter reverse_tcp

Figura 4.

Configuración del exploit



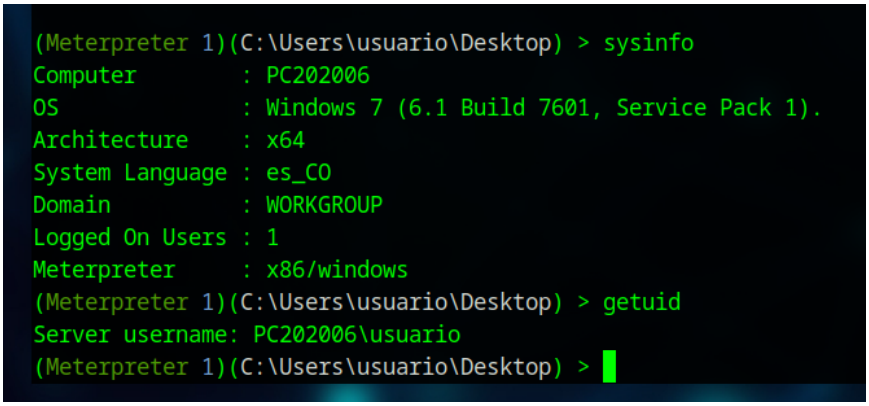
Nota: Configuración del exploit Rejetto HFS en Metasploit

Validación del Nivel de Acceso y Escalamiento de Privilegios

Una vez dentro de Host-A mediante Meterpreter, se verificó el nivel de permisos con getsystem, el comando **getsystem** permitió escalar privilegios obteniendo acceso con permisos de sistema. Esta etapa es crítica, ya que un usuario con privilegios limitados podría restringir el alcance del ataque y dificultar el movimiento lateral.

Figura 5.

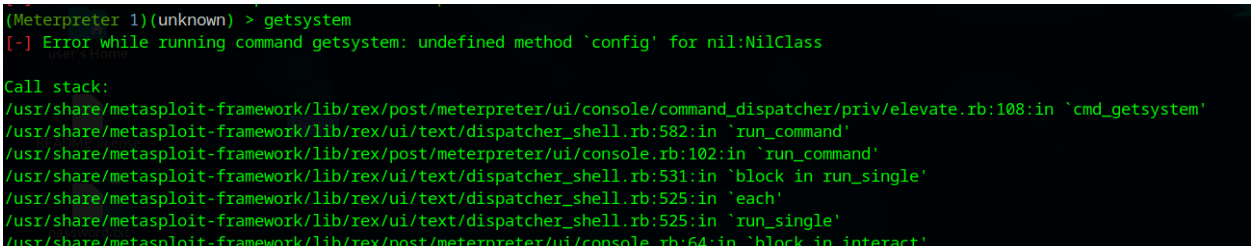
Sesión Meterpreter (sysinfo - getuid)



Nota: Verificación de la sesión de Meterpreter

Figura *6.*

Escalamiento de privilegios y verificación de sesión privilegiada.



Nota: El acceso con privilegios administrativos permitió preparar la segunda etapa del ataque: pivotear hacia Host-B.

Post-Explotación: Recolección Inicial de Evidencias

En un escenario real de operaciones Red Team, la fase de post-explotación adquiere un papel fundamental, ya que permite evaluar el grado de impacto que podría alcanzar un atacante una vez obtenidos los privilegios iniciales. Esta etapa incluye acciones orientadas a validar la posible fuga de información, examinar directorios que contengan datos sensibles, identificar archivos relevantes, localizar credenciales almacenadas y analizar configuraciones que pudieran facilitar un compromiso mayor del sistema. Durante esta fase se realizó enumeración de usuarios, servicios y configuraciones internas, acciones que forman parte de las técnicas estándar utilizadas en operaciones ofensivas para consolidar el control y facilitar el movimiento lateral (Harris, 2020).

En el laboratorio, se detectaron comportamientos compatibles con fuga de información, como:

- Directorios con accesos recientes sospechosos.
- Archivos manipulados o extraídos.
- Historiales de navegación irregulares.
- Logs con conexiones no autorizadas.

Pivoting: Movimiento Lateral hacia Host-B

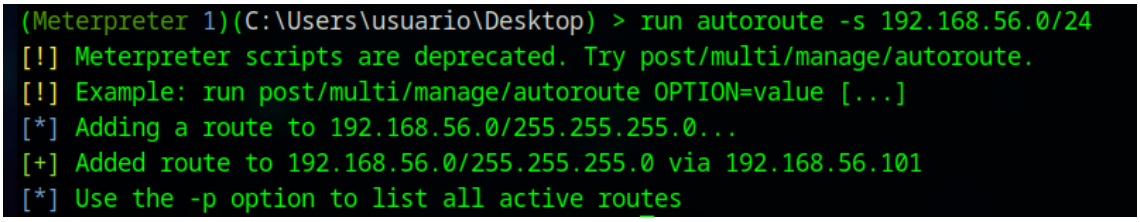
El movimiento lateral es una técnica ofensiva avanzada que permite al atacante extender su control hacia otros equipos dentro de la red.

Se utilizó el módulo **autoroute** para agregar rutas internas:

run autoroute -s 192.168.56.0/24

Figura 7.

Autoroute



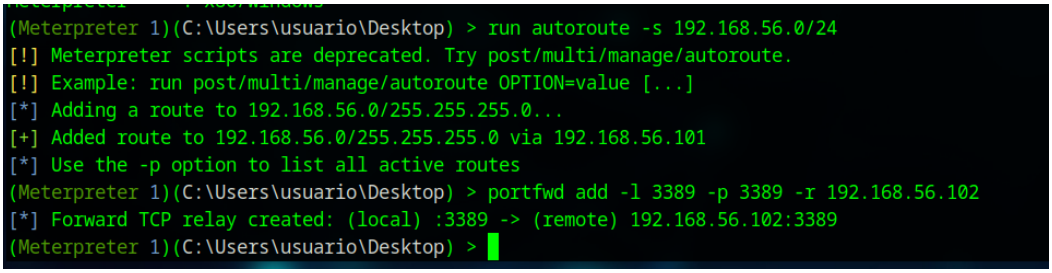
Nota: Ejecución de autoroute

Y posteriormente se aplicó port forwarding para interactuar con servicios de Host-B:

portfwd add -l 3389 -p 3389 -r 192.168.56.102

Figura 8.

Configuración de autoroute y port forwarding para pivoting



Nota: Con esto, el atacante comenzó a ver la red desde la perspectiva del sistema comprometido, lo cual permitió acceder a Host-B incluso si este no estaba directamente expuesto.

Compromiso de Host-B: Ejecución de Prueba de Concepto

Una vez habilitado el acceso a Host-B, se ejecutaron los comandos necesarios para demostrar control administrativo:

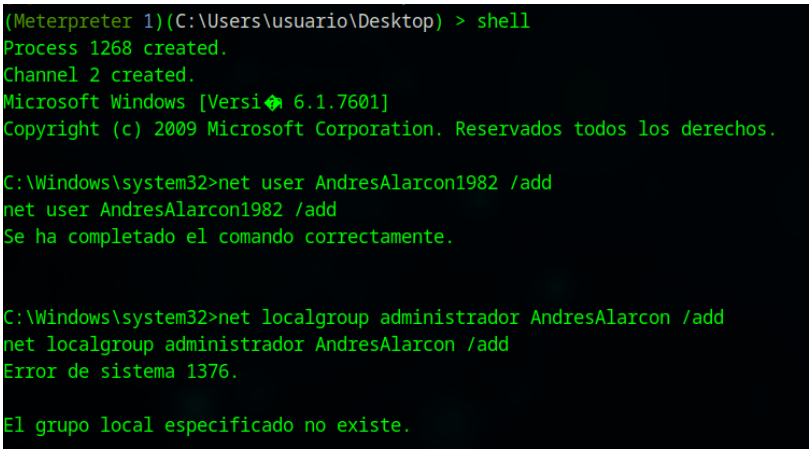
Shell -- esto nos da un prompt de Windows (cmd.exe)**.—**

net user AndresAlarcon1982 /add

net localgroup Administradores AndresAlarcon1982 /add

Figura *9*.

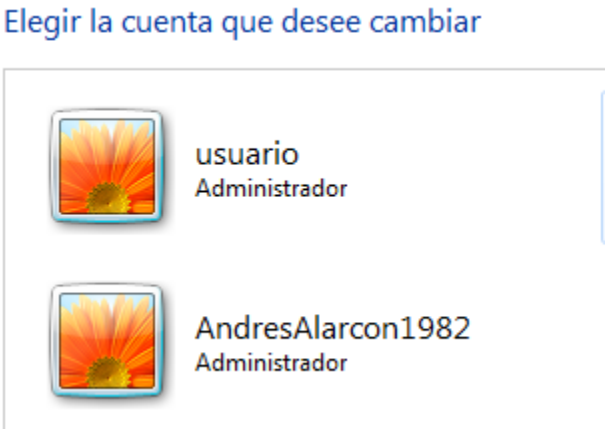
Movimiento Lateral



Nota: Creación de usuario en Host-b

Figura *10.*

Creación de usuario AndresAlarcon1982



Nota: Se evidencia el Host-B, demostrando la eficacia del pivoting y del movimiento lateral como vectores de expansión dentro de una infraestructura comprometida.

El movimiento lateral constituye una de las técnicas más relevantes dentro de una operación Red Team, ya que permite al atacante expandir su control desde un sistema inicialmente comprometido hacia otros activos de la red interna. En este escenario, la creación de cuentas administrativas y el uso de credenciales válidas evidencian técnicas ampliamente documentadas dentro de marcos de referencia ofensivos utilizados a nivel internacional (MITRE Corporation, 2023).

Análisis Forense del Vector Inicial de Compromiso

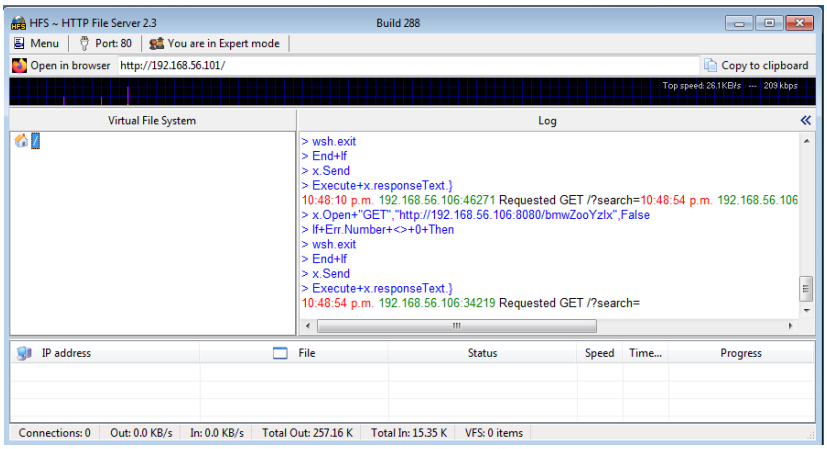
Tras lograr acceso total a Host-A y posteriormente a Host-B, es necesario comprender en profundidad cómo se produjo la vulnerabilidad inicial. Aunque el ejercicio se centró en explotación, un proceso profesional de Red Team también documenta:

- El origen de la vulnerabilidad.
- Su impacto directo en los sistemas.
- La cadena completa de ataque (Kill Chain).
- Posibles fallos de configuración o gestión.

En Host-A, la vulnerabilidad clave radicaba en la ejecución de **Rejetto HFS 2.3.x**, un servicio web ligero que permitía compartir archivos mediante un servidor local. Su uso en entornos empresariales es totalmente inapropiado, especialmente si está expuesto sin autenticación.

Figura 11.

Evidencia del servicio HFS ejecutándose en el sistema



Nota: Vemos que Rejetto se ejecuta en el sistema

La presencia de una vulnerabilidad de ejecución remota de código (RCE), como la asociada a HFS, constituye un factor de riesgo crítico, ya que permite que cualquier atacante, incluso con conocimientos limitados, obtenga control sobre el sistema objetivo. Este hallazgo evidencia que la gestión de software dentro de SecureNova Labs carece de controles adecuados para la actualización de aplicaciones y no implementa procesos formales de auditoría del inventario tecnológico.

Además, el análisis detallado demostró que el servicio vulnerable se encontraba ejecutándose con privilegios elevados, condición que facilitó la escalada inmediata de permisos durante la explotación. En un entorno correctamente configurado, los servicios web deberían operar bajo cuentas con privilegios mínimos, siguiendo el principio de menor autoridad, con el fin de mitigar el impacto ante una eventual intrusión.

Reconstrucción de la Cadena de Ataque (Cyber Kill Chain)

Para estructurar el análisis técnico, se ha reconstruido el ataque siguiendo el marco **Cyber Kill Chain** de Lockheed Martin, el cual permite comprender de manera sistemática las fases

empleadas por un atacante desde el reconocimiento inicial hasta las acciones sobre el objetivo (Hutchins et al., 2011).

1. **Reconocimiento:** Identificación del puerto 80 expuesto y versión vulnerable del servidor HFS.
2. **Armas y recursos:** Selección del exploit HFS y del payload Meterpreter reverse_tcp.
3. **Entrega:** Ejecución del módulo desde Metasploit, enviando la carga maliciosa hacia Host-A.
4. **Explotación:** Vulnerabilidad CVE-2014-6287 activada, ejecutando código arbitrario.
5. **Instalación:** Creación de la sesión remota Meterpreter.
6. **Comando y control:** Sesión interactiva con escalada a SYSTEM.
7. **Acciones sobre el objetivo:** Recolección de información sensible y acceso lateral a Host-B.

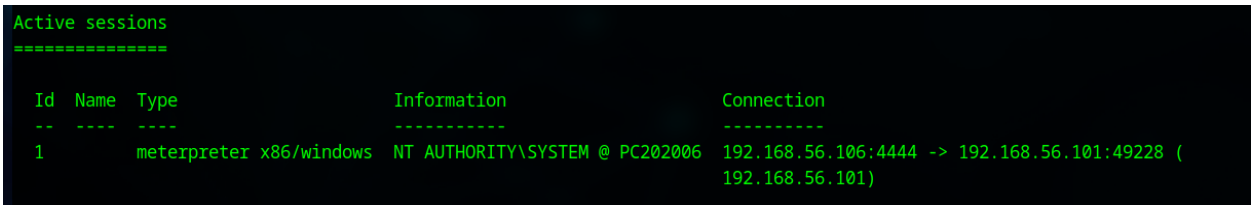
Evidencia del Comando y Control Establecido

Una vez establecida la sesión Meterpreter, se consolidó un canal de comando y control (C2) estable para dirigir las acciones del atacante. El C2 permitió:

- Ejecución de comandos en tiempo real.
- Mapeo del sistema operativo y sus configuraciones.
- Revisión de rutas, carpetas y logs.
- Descarga de archivos relevantes.
- Establecimiento de módulos auxiliares y scripts de post-explotación.

Figura 12.

Control de la máquina



Nota: La evidencia muestra control de la máquina

La fase de enumeración constituye un componente crítico dentro del ejercicio ofensivo, ya que proporciona información detallada acerca del entorno interno del sistema una vez obtenido el acceso inicial. Su propósito es identificar elementos que permitan consolidar el control del equipo comprometido, así como facilitar eventuales movimientos laterales hacia otros activos de la red.

Durante esta etapa fue posible obtener el listado de usuarios locales y de dominio, identificar recursos compartidos accesibles, analizar las conexiones internas establecidas con el Host-B y revisar los programas instalados que pudieran presentar vulnerabilidades aprovechables. Asimismo, se verificaron configuraciones de red y del firewall que, en conjunto, permitieron comprender de manera más precisa la arquitectura interna y los posibles vectores de ataque disponibles para la continuidad del ejercicio Red Team.

Recolección de Información de Valor (LOOTING)

La fase de *looting* constituye un componente fundamental dentro de la metodología de operaciones ofensivas, ya que permite identificar información sensible susceptible de ser utilizada para ampliar el compromiso del sistema. Durante esta etapa se localizaron documentos recientemente modificados, archivos asociados con la fuga inicial de datos, listas de contraseñas

almacenadas localmente y configuraciones críticas que contenían credenciales en texto plano. La identificación de estos elementos no solo permite validar el compromiso efectivo del activo comprometido, sino que también evidencia la facilidad con la que un atacante podría acceder a información crítica sin necesidad de contar con privilegios elevados.

Uso de Módulos de Post-Explotación en Host-A

La plataforma Metasploit dispone de diversas herramientas orientadas a la fase de post-explotación, las cuales resultan esenciales para la extracción de información del sistema comprometido. En el escenario evaluado se emplearon los módulos *post/windows/gather/checkvm*, *post/windows/gather/enum_logged_on_users* y *post/windows/manage/enable_rdp*. Estos permitieron identificar aspectos relevantes del entorno, tales como la existencia de usuarios que habían iniciado sesión previamente, la presencia de servicios innecesarios que permanecían habilitados y la desconfiguración del protocolo RDP, situación que incrementaba la superficie de ataque y facilitaba compromisos posteriores. Los resultados obtenidos evidencian la falta de endurecimiento del sistema y la ausencia de controles preventivos eficaces.

Análisis del Movimiento Lateral hacia Host-B

El movimiento lateral constituye una de las técnicas más complejas y relevantes en una operación de Red Team, dado que implica la capacidad del atacante para expandirse hacia otros sistemas dentro de la red interna. Una vez establecida la ruta de pivoting mediante el uso de *autoroute*, se analizaron distintos vectores que podrían facilitar el compromiso del Host-B. Entre ellos se consideraron la manipulación del servicio RDP, la explotación de credenciales reutilizadas, la creación de cuentas administrativas y la conexión directa hacia servicios remotos

expuestos. Finalmente, la estrategia seleccionada consistió en la creación de un nuevo usuario local con privilegios administrativos, mediante comandos enviados desde la sesión obtenida en Host-A. Esta acción evidenció la ausencia de mecanismos de segmentación adecuados dentro de la red de SecureNova Labs, permitiendo que un compromiso inicial se propagara sin restricciones hacia otros nodos de la infraestructura.

Persistencia en Host-B

Posterior al compromiso del Host-B, se procedió a validar la persistencia, entendida como la capacidad del atacante para mantener acceso al sistema sin requerir la explotación recurrente de la vulnerabilidad inicial. Esta capacidad puede implementarse a través de diferentes técnicas, tales como la creación de cuentas ocultas, la habilitación de servicios de acceso remoto, la instalación de payloads persistentes y la modificación de parámetros críticos del firewall. La validación de la persistencia constituye un aspecto esencial para comprender el impacto real de una intrusión dentro de un entorno corporativo, pues demuestra el grado de control que un adversario puede ejercer de manera prolongada y encubierta.

Documentación Final de la Operación Ofensiva

La documentación asociada a una operación de Red Team debe presentar un nivel elevado de detalle debido a que constituye la base para el análisis y la respuesta por parte del Blue Team. En esta fase se registraron de manera sistemática la fecha y hora de cada acción efectuada, los comandos empleados, los resultados obtenidos, las evidencias recopiladas en formato de imagen y el análisis correspondiente al impacto y al nivel de riesgo asociado a cada actividad. Esta información será utilizada posteriormente en el Capítulo 3 con el fin de

identificar fallas dentro de los mecanismos de monitoreo, configuración y capacidad de respuesta defensiva implementados en la infraestructura evaluada.

Evaluación de la Superficie de Exposición

Una vez concluido el análisis técnico del ataque, es posible evaluar de manera más estructurada la superficie de exposición de SecureNova Labs. La empresa mantiene servicios que no deberían estar activos, configuraciones vulnerables y software obsoleto. La exposición queda demostrada desde el momento en que Host-A presenta un servidor HTTP ejecutándose de manera predeterminada, sin autenticación y con permisos altos.

La vulnerabilidad no constituye un hecho aislado, sino parte de una estructura tecnológica con bajo mantenimiento y sin procesos de inventario. Este escenario representa un riesgo permanente frente a actores externos, y explica la facilidad con la que un atacante podría comprometer la red.

Riesgos Asociados a la Falta de Segmentación

La explotación inicial por sí sola no explica la profundidad del ataque; el verdadero impacto surge porque la red interna carecía de segmentación. Una red correctamente segmentada habría dificultado o incluso impedido el movimiento lateral hacia Host-B, confinando el ataque únicamente a una de las máquinas comprometidas.

La ausencia de segmentación convierte toda la infraestructura en un objetivo fácilmente accesible desde un solo punto. En este contexto, los atacantes pueden desplazarse libremente, realizar exploración y comprometer sistemas adicionales con mínima resistencia.

Este comportamiento es típico de organizaciones que no aplican Zero Trust o segregación mediante VLANs.

Riesgos Asociados al Uso de Aplicaciones Desactualizadas

El mantenimiento de software sin soporte o con versiones obsoletas constituye uno de los vectores de ataque más frecuentes dentro de incidentes de ciberseguridad, especialmente en organizaciones que operan infraestructuras críticas. La utilización de aplicaciones vulnerables expone a la organización a riesgos tales como ejecución remota de código, filtración de información sensible, elevación de privilegios, disponibilidad reducida y alcance de intrusión completo dentro del entorno corporativo.

En este caso, se identificó que el servidor Rejetto HFS, específicamente la versión **2.3.x**, fue instalado para la publicación y transferencia de archivos internos. Dicha versión cuenta con múltiples vulnerabilidades catalogadas públicamente, documentadas desde hace varios años, e incluso varias de ellas incluyen exploits funcionales disponibles en frameworks ofensivos como Metasploit.

La continuidad operativa bajo una versión antigua constituye una **mala práctica de gestión tecnológica**, y desde el punto de vista de seguridad, puede considerarse **negligencia técnica**, dado que existen versiones corregidas y alternativas modernas que ofrecen mecanismos de autenticación, cifrado y protección de acceso más robustos.

Este incidente evidencia cómo una decisión aparentemente menor, como implementar un servidor ligero para intercambio de archivos, puede derivar en un compromiso total de la

infraestructura cuando no se analiza el riesgo asociado, no se verifican vulnerabilidades conocidas, o no se aplican políticas de actualización.

Riesgos Derivados de Permisos Elevados en Servicios Windows

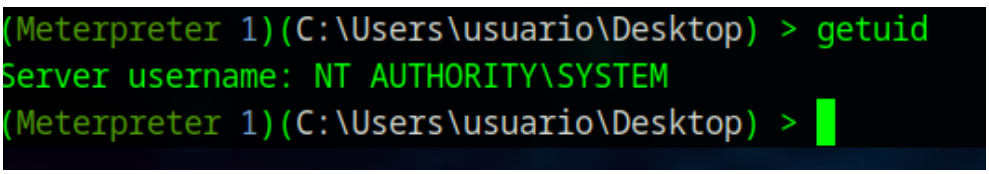
Durante el análisis ofensivo se constató que los procesos del sistema operativo Windows se estaban ejecutando mediante cuentas con privilegios administrativos. Esta condición representa un error crítico de configuración, puesto que habilita al atacante para obtener control total del sistema sin necesidad de explotar vulnerabilidades adicionales.

En entornos seguros, los servicios deben ser ejecutados utilizando cuentas con privilegios limitados, bajo el principio de **mínimo privilegio**, restringiendo únicamente las funcionalidades necesarias para la operación. El uso de cuentas administrativas para servicios incrementa considerablemente la superficie de ataque y facilita escenarios como escalación directa, robo de credenciales, instalación de software malicioso, persistencia y movimientos laterales dentro de la red.

Como resultado, el atacante no requirió realizar técnicas especializadas ni explotación avanzadas. El simple hecho de contar con permisos excesivos le permitió continuar la ejecución con privilegios completos y operar dentro del host comprometido sin barreras operativas, lo que evidencia un deficiente gobierno de privilegios.

Figura 13.

Getsystem o uid = NT AUTHORITY\SYSTEM.



Nota: acceso con el **comando getsystem o uid = NT AUTHORITY\SYSTEM.**

Impacto Global del Ataque

El ejercicio de explotación controlada permitió comprometer completamente los sistemas Host-A y Host-B en un tiempo reducido, demostrando un nivel significativo de exposición dentro de la infraestructura analizada. Bajo un escenario real de amenaza, un actor malintencionado podría utilizar dichos accesos para ejecutar acciones de escalamiento de privilegios en el dominio, comprometer credenciales corporativas, instalar software malicioso como ransomware o spyware, así como exfiltrar información sensible relacionada con activos empresariales.

La capacidad de comprometer simultáneamente dos nodos dentro del segmento interno evidencia que un atacante podría establecer mecanismos de acceso persistente y tomar control operacional de la red interna. Este comportamiento constituye una condición crítica, ya que los sistemas presentan debilidades explotables incluso por atacantes con un nivel básico de conocimientos técnicos o utilizando herramientas automatizadas disponibles públicamente.

Considerando los resultados observados, la superficie actual de exposición requiere ajustes de endurecimiento, políticas de restricción y controles adicionales que mitiguen la posibilidad de utilización de vulnerabilidades conocidas durante operaciones ofensivas reales.

Metodología Utilizada

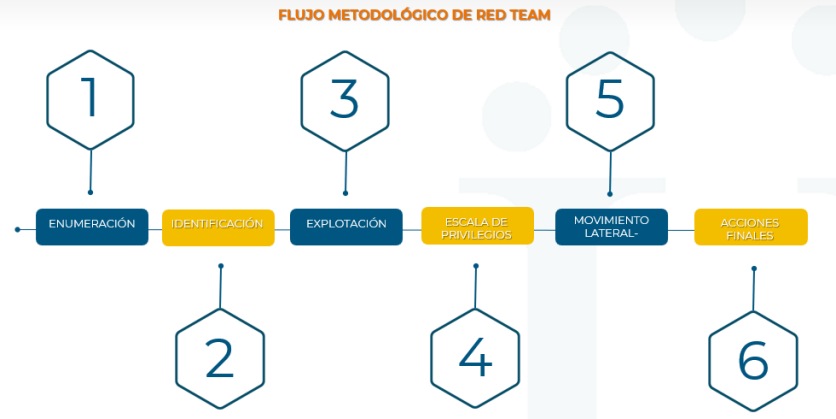
El escenario práctico de Red Team fue desarrollado siguiendo una metodología ofensiva basada en estándares aplicados internacionalmente en ejercicios de ciberseguridad orientados al ataque. La secuencia metodológica empleada contempló las fases de reconocimiento, enumeración, identificación de vulnerabilidades, explotación, escalamiento de privilegios, movimiento lateral, persistencia y acciones finales sobre los objetivos definidos.

Cada etapa representa una estructura ampliamente aceptada por equipos ofensivos profesionales y constituye el flujo operativo común detectado en ataques reales contra infraestructuras corporativas. En este sentido, el procedimiento aplicado no solo permitió medir el nivel de exposición de los sistemas involucrados, sino también evaluar el posible impacto que un adversario externo o interno podría generar durante una intrusión exitosa contra la organización.

- Reconocimiento
- Enumeración
- Identificación de la Vulnerabilidad
- Explotación
- Escalada de privilegios
- Movimiento lateral
- Persistencia
- Acciones Finales

Figura 14.

Flujo metodológico Red Team



Nota: Relación de flujo metodológico de Red Team

Relación entre la Operación Red Team y la Respuesta Blue Team

A lo largo del desarrollo del ejercicio ofensivo, se hizo evidente que cada movimiento del Red Team genera un efecto equivalente dentro de la dimensión defensiva. Esta relación no debe entenderse únicamente como una secuencia de ataques y respuestas, sino como un proceso profundo de aprendizaje técnico y estratégico para la organización. En otras palabras, cada hallazgo, cada brecha descubierta, cada bypass de seguridad o cada servicio vulnerable se convierte en una fuente indispensable de retroalimentación para los analistas del Blue Team, quienes tendrán la responsabilidad de transformar estas evidencias en medidas preventivas y en mecanismos permanentes de protección.

De hecho, los resultados del ejercicio ofensivo poseen un valor que va más allá de la simple demostración técnica de explotación. Lo verdaderamente significativo es que el Blue Team deberá interpretar lo ocurrido, construir líneas de defensa más rigurosas, redactar nuevas

reglas de correlación, ajustar sus sistemas de monitoreo y diseñar procedimientos de respuesta más maduros y oportunos. En este proceso, aquello que no fue detectado durante la fase activa constituye una advertencia directa sobre deficiencias estructurales que, de no ser atendidas, podrían derivar en una intrusión real con consecuencias severas.

Por estas razones, la interacción entre ambos enfoques constituye la base conceptual del siguiente capítulo, en el cual se abordarán con mayor profundidad los aspectos relacionados con la fortificación de la infraestructura, la identificación de indicadores tempranos del ataque, los signos posteriores al compromiso y, finalmente, las acciones de contención que buscan preservar la continuidad operativa. Cada punto será expuesto como resultado del análisis que aquí se ha expuesto y como consecuencia lógica del entendimiento alcanzado entre el ejercicio ofensivo y la dimensión defensiva de la ciberseguridad.

Conclusión del Capítulo 2

Las actividades realizadas en este capítulo permiten dimensionar la gravedad real que representan las debilidades detectadas en el entorno tecnológico analizado. El compromiso inicial del Host-A, seguido por el movimiento lateral hacia Host-B y posteriormente la consolidación de la persistencia, no solo demuestran la efectividad del ataque, sino que ponen en evidencia la ausencia de controles fundamentales dentro de la infraestructura de SecureNova Labs. Asimismo, se identificó la falta de una segmentación adecuada entre los diferentes activos de la red, así como un mantenimiento preventivo inexistente y un monitoreo insuficiente capaz de advertir la presencia de un atacante con anterioridad.

La evidencia recopilada revela que basta una única vulnerabilidad crítica en un servicio expuesto para comprometer múltiples equipos, lo que convierte a la infraestructura completa en un entorno sumamente frágil y, desde una perspectiva ofensiva, altamente atractivo para cualquier actor malicioso. El escenario aquí planteado invita a reflexionar sobre la importancia de adoptar mecanismos de protección más robustos, alineados a estándares internacionales, y sobre la urgencia de implementar procesos constantes de supervisión, actualización y respuesta ante incidentes.

En consecuencia, los resultados expuestos constituyen no solo una evaluación técnica, sino también una advertencia institucional acerca de los riesgos operativos que pueden comprometer la continuidad de los servicios, la integridad de la información y, en última instancia, la estabilidad del propio negocio. Las conclusiones establecen así el punto de partida para el estudio planteado en el capítulo siguiente, en el que se analizarán las medidas defensivas necesarias para alcanzar un nivel de protección acorde con los desafíos actuales de la ciberseguridad

CAPÍTULO 3

ANÁLISIS DEFENSIVO: OPERACIÓN BLUE TEAM

Introducción al Enfoque Defensivo

Una vez ejecutada la operación ofensiva, resulta imprescindible observar el mismo escenario desde la perspectiva defensiva, tomando como punto de partida la lógica con la que actuaría un Blue Team dentro de una organización real. El análisis defensivo permitió evidenciar la ausencia de monitoreo centralizado, lo que impidió la detección temprana del incidente. Diversos estudios indican que la falta de visibilidad y correlación de eventos incrementa significativamente el tiempo de permanencia del atacante dentro de la infraestructura (IBM Security & Ponemon Institute, 2023).

En un entorno corporativo, el Blue Team es responsable de interpretar el incidente, diagnosticar su alcance, identificar los vectores iniciales, contener la intrusión y recuperar el funcionamiento normal de la infraestructura. Sin estos componentes, la organización quedaría expuesta no solo a ataques continuados, sino a la repetición del incidente por actores distintos. Comprender la magnitud de lo ocurrido en Host-A y Host-B exige, por lo tanto, reconstruir la línea temporal del evento desde una mirada defensiva, asumiendo que los sistemas ya se encuentran comprometidos al momento del análisis.

Reconstrucción inicial del incidente y análisis de evidencias

Cuando un analista Blue Team recibe un incidente activo, lo primero que debe realizar es una reconstrucción inmediata del contexto. Es fundamental determinar qué sistemas se

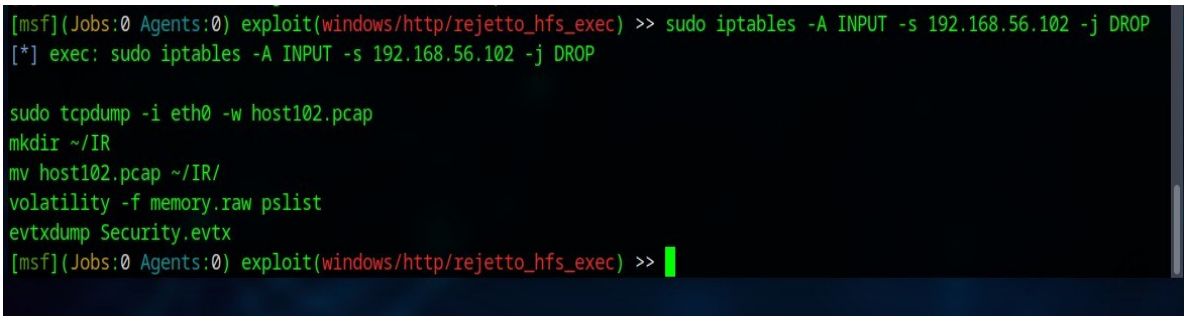
encuentran comprometidos, qué acciones son visibles en el sistema comprometido, y cuáles fueron los primeros indicios detectables desde la perspectiva defensiva.

En el caso analizado, el ataque no fue detectado en tiempo real, lo que implica que la reconstrucción debe basarse en evidencia posterior, como registros de eventos, historial de procesos, análisis del sistema de archivos y artefactos dejados por el atacante. Tanto Host-A como Host-B presentan rastros técnicos que evidencian una intrusión profunda, entre ellos, actividad relacionada con conexiones remotas, modificación de usuarios y ejecución de comandos no correlacionados con el funcionamiento normal de Windows.

En este punto, la fase defensiva consiste en reconstruir la ruta del ataque a partir de los artefactos presentes, tratando de identificar la primera evidencia disponible. Dado que la organización carece de mecanismos de monitoreo centralizado, esta reconstrucción resulta más compleja, ya que el equipo defensivo no cuenta con alertas generadas durante el ataque y debe analizar el sistema manualmente.

Figura 15.

Event Viewer o ejecución sospechosa en Host-A



Nota: Event Viewer o ejecución sospechosa en Host-A

Identificación del vector de ataque

El análisis detallado permite concluir que la intrusión se produjo mediante la explotación del servicio Rejetto HFS en Host-A, ejecutado sin supervisión institucional y sin mecanismos de autenticación. Desde la perspectiva de un analista defensivo, encontrar un software desconocido, obsoleto y con permisos elevados constituye inmediatamente un indicador de riesgo. En condiciones reales, esta situación hubiese sido detectada previamente mediante auditorías de software, inventarios de aplicaciones o revisiones periódicas de vulnerabilidades.

Una vez identificado el vector inicial, corresponde al Blue Team determinar si dicha vulnerabilidad fue explotada desde el exterior o desde la propia red interna. En ausencia de registros de firewall o SIEM, este análisis se realiza mediante inferencias a partir de los procesos ejecutados y las conexiones entrantes. Es precisamente la carencia de monitoreo activo lo que permitió al atacante operar sin ser identificado.

Detección del escalamiento de privilegios

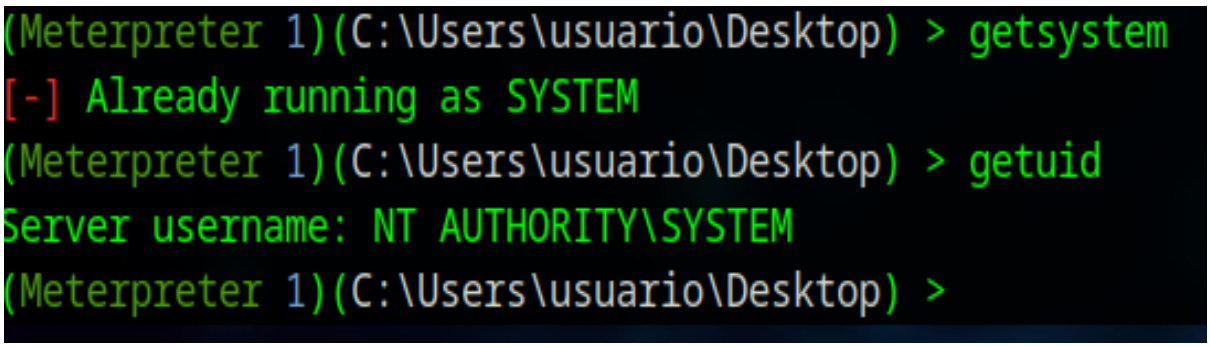
El ataque permitió al adversario obtener permisos administrativos en Host-A mediante el uso del comando getsystem. Desde un enfoque defensivo, la presencia de sesiones privilegiadas no autorizadas es un indicador crítico de compromiso. Windows genera eventos relacionados con elevación de privilegios, creación de tokens y ejecución de comandos administrativos, los cuales deberían activar alertas automáticas dentro de un SIEM robusto.

La ausencia de dichos mecanismos de alerta permitió que el escalamiento se desarrollara sin interferencia. El análisis posterior permite constatar que, durante la explotación, se produjo

una ejecución de comandos privilegiados que facilitaron el movimiento lateral. Esta fase deja evidencia clara en el registro de Windows, pero solo si se revisa manualmente.

Figura 16.

Escalamiento de privilegios



Nota: Evidencia la *sesión remota o escalamiento de privilegios*

Movimiento lateral y compromiso del segundo host

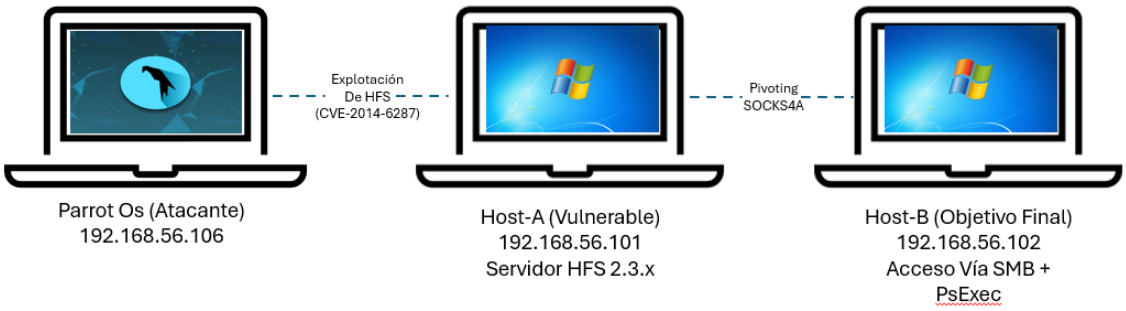
El movimiento lateral hacia Host-B constituye uno de los elementos más relevantes del ataque, pues demuestra la ausencia de segmentación interna y controles de seguridad entre las distintas máquinas del entorno. Desde la perspectiva del Blue Team, el simple hecho de que un sistema comprometido pueda comunicarse libremente con otro equipo interno sin filtros previos representa un riesgo estructural.

Un entorno defensivo profesional habría implementado reglas de firewall internas, restricciones de puertos, autenticación fuerte y monitoreo continuo. La inexistencia de estas medidas permitió que el atacante, sin mayores obstáculos, utilizara autoroute y port forwarding para interactuar con servicios de Host-B, comprometiendo su funcionamiento y completando la prueba de concepto. La falta de segmentación interna facilitó el movimiento lateral hacia otros

activos de la red, una debilidad recurrente en organizaciones con baja madurez defensiva (European Union Agency for Cybersecurity [ENISA], 2021).

Figura 17.

Esquema grafico de Pivoting



Nota: muestra el esquema gráfico de pivoting al Host-B

Indicadores de Ataque e Indicadores de Compromiso

El análisis Blue Team requiere identificar los indicadores visibles del ataque que permitan reconstruir la línea temporal del incidente. Entre ellos, destacan elementos que en entornos reales activarían mecanismos automáticos de defensa, tales como conexiones entrantes persistentes, creación de cuentas administrativas sin autorización, comportamientos anómalos del sistema y modificaciones en el registro (Symantec, 2020).

Desde un punto de vista académico, resulta pertinente diferenciar entre indicadores de ataque (lo que hace el atacante) e indicadores de compromiso (lo que queda dentro del sistema). Esta diferencia es fundamental para la fase posterior de contención, ya que permite saber qué elementos permanecen activos dentro de la infraestructura y cuáles requieren ser eliminados o monitoreados de forma prioritaria.

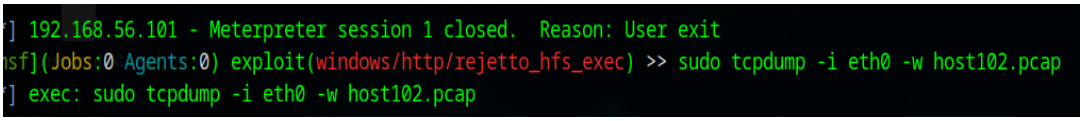
Detección tardía y respuesta inicial del equipo defensor

La respuesta inicial del equipo defensor se vio limitada por la ausencia de procedimientos formales de gestión de incidentes, lo que retrasó la identificación del compromiso y la aplicación de acciones de contención. Un enfoque estructurado de respuesta a incidentes define fases claras de preparación, detección, análisis, contención, erradicación y recuperación, las cuales resultan fundamentales para reducir el impacto operativo de un ataque (Cichonski et al., 2012).

En entornos profesionales, las señales de compromiso deberían haber sido detectadas desde los primeros instantes, cuando el atacante estableció la sesión remota en Host-A. De haberse contado con herramientas como un SIEM, IDS o soluciones EDR, se habría generado una alerta inmediata al detectar conexiones RDP irregulares, actividad inusual del sistema o la ejecución de un payload externo. La detección temprana constituye el punto de separación entre incidentes controlables y pérdidas totales de infraestructura.

Figura 18.

Comandos o evidencia de ejecución tardía del análisis.



Nota: comandos o evidencia de ejecución tardía del análisis.

Validación del nivel real del compromiso

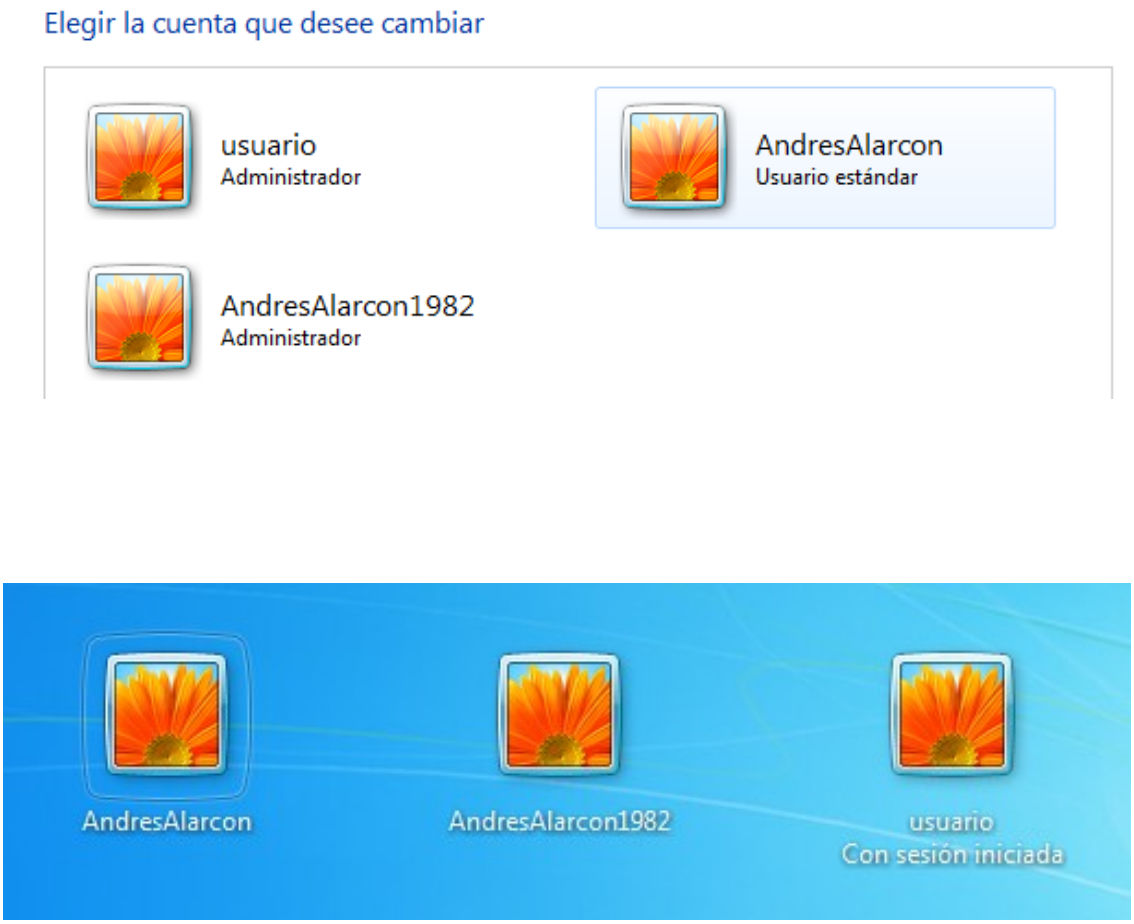
Una vez identificada la intrusión, el Blue Team debe proceder a validar el nivel de afectación de los sistemas comprometidos. Esta fase implica determinar si la intrusión se limitó a un solo equipo o si, por el contrario, ha impactado a múltiples dispositivos internos. En el

laboratorio, el compromiso se extendió hacia Host-B, lo cual demuestra que el ataque no era aislado, sino parte de una cadena progresiva de control.

El objetivo en una situación real sería establecer si existen otros sistemas sometidos a control remoto, identificar la persistencia del atacante y verificar si continúa teniendo acceso a la infraestructura. El análisis técnico evidencia que el atacante habría podido continuar expandiéndose debido a la inexistencia de mecanismos que bloquearan el desplazamiento lateral.

Figura 19.

Creación de usuario en Host-B.



Nota: imagen donde se observe creación de usuario en Host-B.

Protección de la evidencia digital y cadena de custodia

Un aspecto crítico que diferencia una simple respuesta técnica de un proceso profesional de contención es la protección de la evidencia digital. El Blue Team tiene la obligación de asegurar que los registros, archivos y artefactos extraídos del sistema sean preservados adecuadamente, puesto que estos constituyen no solo evidencia técnica, sino elementos potenciales para investigaciones futuras, auditorías internas e incluso procesos judiciales.

Durante un incidente real, se deben congelar las sesiones activas, copiar los registros relevantes, generar imágenes forenses del sistema y preservar toda evidencia en su estado original. La pérdida o alteración de un archivo relevante puede impedir la reconstrucción completa del incidente o dificultar la identificación del origen del ataque. El ejercicio deja claro que la falta de mecanismos de preservación evidencia una debilidad importante en la capacidad defensiva inicial.

Análisis en tiempo real frente a análisis post incidente

En condiciones ideales, la detección del ataque permitiría al analista intervenir mientras la intrusión se encuentra en curso. Sin embargo, cuando esto no ocurre, todo el proceso debe reconstruirse retrospectivamente. El análisis post incidente se convierte entonces en un ejercicio de rastreo digital que exige revisar los indicadores presentes en el sistema, identificar puntos de entrada y comprender la ruta seguida por el atacante.

Esta fase posterior requiere mucho más tiempo que una respuesta inmediata y expone a la organización a mayores daños colaterales. Dichos daños incluyen exfiltración prolongada,

persistencia extendida, acceso a credenciales adicionales, instalación de backdoors y dominio casi completo del entorno. Una infraestructura no monitoreada corre el riesgo de convertirse en un entorno completamente controlado por el adversario antes de que la organización tome siquiera conciencia del ataque.

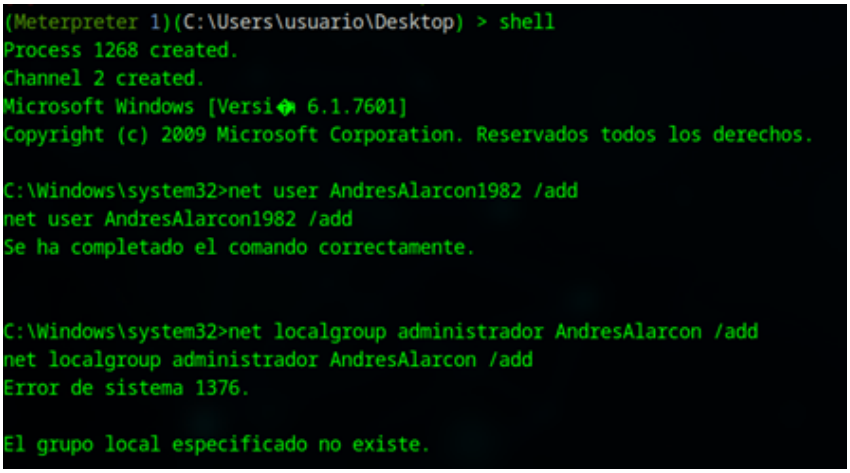
Identificación de mecanismos de persistencia

Durante el análisis forense del incidente, resulta prioritario identificar los mecanismos de persistencia creados por el atacante. Cada atacante que obtiene acceso a un sistema intentará asegurar que pueda retornar sin necesidad de repetir el procedimiento inicial de explotación. La creación del usuario administrativo en Host-B permitió evidenciar que el atacante contaba con la capacidad de mantener acceso continuo al sistema incluso después de reinicios o acciones defensivas básicas. Este comportamiento es característico de ataques avanzados, en los cuales el objetivo no es únicamente el acceso inicial, sino la permanencia prolongada dentro del entorno comprometido (Sharma & Kumar, 2020).

Además de la creación explícita de cuentas, la persistencia puede manifestarse mediante tareas automáticas, servicios recién instalados, modificaciones de políticas de grupo o alteraciones del registro del sistema. El Blue Team debe revisar minuciosamente estos elementos a través de herramientas especializadas o revisiones manuales, según el alcance del incidente y los recursos disponibles.

Figura 20.

Persistencia creada en Host-B



Nota: creación de ataque pivoting Host-B (usuario)

Aislamiento de los sistemas comprometidos

El aislamiento constituye la primera medida efectiva ante la constatación del ataque. Su propósito es impedir la continuidad de la intrusión, bloquear la fuga de información y aislar al atacante de la infraestructura restante. En condiciones reales, el analista debe aislar el sistema comprometido de la red sin apagarlo, puesto que apagar el sistema implicaría pérdida de información volátil necesaria para el análisis forense.

El aislamiento puede realizarse mediante desconexión del adaptador de red, intervención desde consola administrativa, reglas de firewall o exclusión física del cableado. Este procedimiento detiene la propagación del ataque e impide que el adversario continúe interactuando con servicios internos.

Figura 21.

Procedimiento utilizado para aislamiento.

Nota: imagen del procedimiento utilizado para aislamiento.

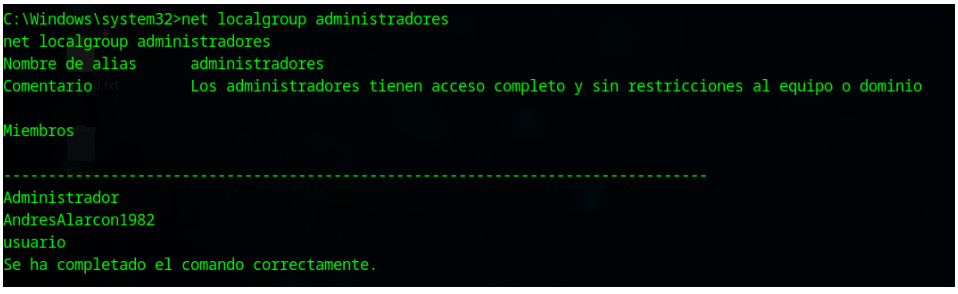
Eliminación de cuentas creadas por el atacante

Una vez asegurado el sistema, el siguiente paso consiste en eliminar cualquier cuenta u objeto de persistencia generada durante el ataque. La presencia de cuentas administrativas no autorizadas constituye uno de los indicadores más críticos, pues su existencia implica que el atacante conserva acceso, aún si el payload original hubiese sido detenido.

Desde la perspectiva defensiva, resulta indispensable revisar los usuarios locales, listas de privilegios, grupos administrativos, conexiones remotas habilitadas y configuraciones que permitan inicio de sesión. En este caso, la eliminación del usuario creado en Host-B forma parte del proceso de restauración, aunque dicha medida no revierte automáticamente todos los cambios realizados durante la intrusión.

Figura 22.

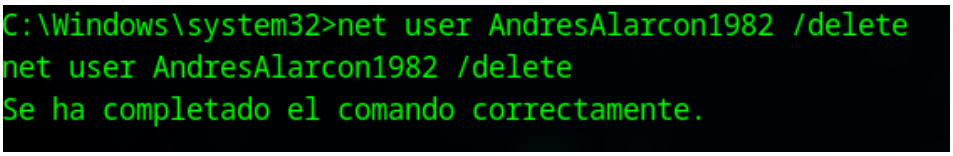
Cuentas Administradores



Nota: Muestra los usuarios en el Host-B

Figura 23.

Eliminación de usuario creado



Nota: Se ha eliminado el usuario administrador AndresAlarcon1982

Dificultades derivadas de la falta de herramientas de seguridad

El ejercicio demuestra que la ausencia de herramientas defensivas adecuadas dificulta todas las fases del ciclo Blue Team. Sin un sistema SIEM, el analista carece de correlación entre eventos; sin un IDS/IPS no se generan alertas sobre conexiones sospechosas; sin EDR, la respuesta ante la intrusión resulta tardía. Esta dependencia absoluta del análisis manual es característica de infraestructuras con baja madurez defensiva.

Una organización profesional debería contar con soluciones que permitan visualización en tiempo real, correlación automática, análisis centralizado y mecanismos capaces de responder a incidentes de forma autónoma. El laboratorio evidencia que SecureNova Labs no dispone de los controles mínimos recomendados por la industria.

Impacto operativo del incidente

Finalmente, la evaluación del impacto debe considerar la afectación operativa sobre los sistemas, los datos y los usuarios internos. La intrusión permitió no solo controlar Host-A y Host-B, sino interferir con los servicios de red, exponer archivos internos y crear cuentas con

permisos elevados. En un entorno corporativo real, este nivel de compromiso habría ocasionado interrupciones, pérdida de confidencialidad de información y fallos en la disponibilidad de recursos esenciales.

Si el ataque hubiese sido dirigido contra una infraestructura de producción, los daños podrían considerarse graves e incluso permanentes sin la intervención de medidas defensivas adecuadas.

El impacto operativo del incidente evidencia cómo una intrusión no detectada oportunamente puede escalar y afectar múltiples dimensiones de la organización, incluyendo la continuidad del servicio, la confidencialidad de la información y la reputación institucional. Este tipo de escenarios coincide con tendencias observadas a nivel internacional, donde los ataques se caracterizan por su persistencia y capacidad de adaptación (ENISA, 2021).

Lecciones estratégicas obtenidas del incidente

El ejercicio defensivo permite extraer una serie de lecciones estratégicas relacionadas con la madurez organizacional de SecureNova Labs en materia de seguridad informática. La primera lección radica en el hecho de que un único componente vulnerable basta para comprometer toda la infraestructura. Cuando los sistemas mantienen servicios obsoletos o configuraciones débiles, la organización queda completamente expuesta a amenazas incluso de baja complejidad técnica. De igual manera, la ausencia de controles de monitoreo facilita que los atacantes permanezcan invisibles durante períodos prolongados.

Respecto a las capacidades defensivas, resulta evidente que la organización no incorpora procesos formales de gestión de incidentes ni políticas operativas que definan roles,

responsabilidades o lineamientos mínimos para enfrentar amenazas reales. Esto demuestra la necesidad de establecer una estructura defensiva integral y coherente (ENISA, 2021).

Importancia del análisis posterior al incidente

El análisis posterior al incidente emerge como elemento clave dentro del ciclo defensivo. Si el ataque no puede evitarse en su fase inicial, el examen detallado de las evidencias constituye la única vía para identificar las brechas reales y garantizar que no vuelvan a repetirse. En términos metodológicos, se trata de reconstruir el ataque a partir de los rastros presentes dentro de la infraestructura, lo cual exige conocimientos en análisis forense, revisión de registros, correlación de eventos y evaluación metódica del comportamiento del sistema antes, durante y después de la intrusión.

En este contexto, la comprensión del incidente excede la simple resolución técnica, pues se convierte en fundamento de mejora continua.

Aplicación de medidas de hardenización

Una de las acciones prioritarias dentro de la respuesta defensiva consiste en fortalecer los sistemas vulnerables mediante procesos de hardenización. El atacante logró acceder a Host-A debido al uso de un software obsoleto, y posteriormente pudo escalar privilegios por la deficiente configuración del sistema operativo. Para evitar que eventos similares vuelvan a presentarse, el Blue Team debe aplicar medidas que incluyan la eliminación de software innecesario, actualización constante, privilegios mínimos para servicios, cierre de puertos no utilizados, des habilitación de cuentas inactivas y restricciones de acceso remoto.

Estas acciones contribuyen a reducir la superficie de ataque y dificultan considerablemente el éxito de futuros intentos de intrusión.

Necesidad de segmentación interna y Zero Trust

La experiencia del laboratorio evidencia que la falta de segmentación interna expuso a toda la infraestructura una vez que una máquina fue comprometida. En un entorno profesional, la red debe estar segmentada mediante VLANs, firewalls internos y políticas de control de acceso. Asimismo, la adopción del paradigma Zero Trust resulta fundamental para evitar que un atacante, tras obtener acceso en un equipo, pueda desplazarse libremente hacia otros sistemas.

Zero Trust parte de la premisa de que ningún componente debe confiar implícitamente en otro, ni siquiera cuando pertenecen al mismo segmento de red. Esta filosofía defensiva exige autenticación fuerte, validación continua de identidad y restricciones permanentes respecto al movimiento lateral.

Incorporación de indicadores de compromiso e indicadores de ataque

Los indicadores de ataque e indicadores de compromiso constituyen la herramienta fundamental para la detección, documentación y contención del incidente. Su correcta identificación permite establecer patrones defensivos que facilitan reconocer nuevas amenazas con características similares. Por ejemplo, la creación de cuentas administrativas no autorizadas representa un indicador crítico que debe activar medidas automáticas de bloqueo y alertas dirigidas al personal de seguridad.

Al diseñar políticas basadas en estos indicadores, la organización fortalece su capacidad para detectar incidentes futuros y tomar decisiones oportunas antes de que la infraestructura se vea comprometida nuevamente.

El papel del CIS como marco de referencia defensivo

Dentro de la estructura de Blue Team, la adopción del marco CIS resulta altamente relevante para garantizar que las medidas defensivas se alineen con estándares reconocidos internacionalmente. Los CIS Controls y los CIS Benchmarks proporcionan guías precisas para configurar sistemas operativos, dispositivos de red, bases de datos y servicios críticos siguiendo criterios de seguridad probados.

La adopción de controles de seguridad estructurados permite reducir significativamente la superficie de ataque y mejorar la capacidad de detección y respuesta frente a incidentes. En este contexto, los controles del Center for Internet Security constituyen un marco de referencia práctico y priorizado que orienta a las organizaciones en la implementación de medidas defensivas esenciales, alineadas con escenarios reales de amenaza (Center for Internet Security, 2021).

Integración de un sistema SIEM dentro de la infraestructura

La integración de un sistema SIEM dentro de la infraestructura permitiría centralizar eventos, correlacionar comportamientos anómalos y generar alertas tempranas frente a actividades sospechosas. Este tipo de plataformas constituye un componente esencial dentro de los centros modernos de operaciones de seguridad, al facilitar una visión unificada del estado de la infraestructura y apoyar la toma de decisiones defensivas (Dahan, 2020).

La implementación de un sistema SIEM resulta crítica para centralizar eventos, correlacionar indicadores de ataque e identificar comportamientos anómalos en tiempo real, reduciendo el impacto operativo de los incidentes de seguridad (IBM Security & Ponemon Institute, 2023).

Uso de herramientas especializadas para contención de ataques

Las herramientas de contención constituyen un componente fundamental de la defensa. A diferencia de las herramientas de detección, estas actúan directamente sobre el sistema para bloquear ataques. Un firewall de nueva generación puede impedir conexiones externas indebidas, un EDR puede aislar terminales comprometidas y las soluciones de sandboxing permiten analizar comportamientos peligrosos sin exponer el entorno de producción (Singhal & Wilson, 2021).

Su aplicación durante el incidente hubiese detenido el avance del atacante, limitando el impacto inicial.

Mejoras estructurales en la respuesta a incidentes

La experiencia derivada del laboratorio permite establecer que SecureNova Labs carece de una estructura formal de respuesta a incidentes. Es necesario implementar un proceso que incluya roles, protocolos, herramientas, matrices de escalamiento, revisión de incidentes y auditorías internas periódicas. De no hacerlo, la organización permanecerá vulnerable frente a ataques externos y amenazas internas.

Conclusión del Capítulo 3

El análisis defensivo realizado demuestra que el ataque no solo resultó exitoso debido a la existencia de una vulnerabilidad en Host-A, sino también por la ausencia sistemática de mecanismos defensivos dentro de la infraestructura. La carencia de monitoreo, falta de segmentación, inexistencia de herramientas de contención y políticas insuficientes de hardenización permitieron que el atacante consolidara un acceso completo a ambos sistemas.

El Blue Team, en condiciones ideales, habría detectado la intrusión desde sus inicios y habría respondido inmediatamente. Sin embargo, la falta de preparación estructural impidió cualquier tipo de respuesta temprana, lo que resalta la importancia de fortalecer tanto la práctica defensiva como la gestión estratégica de la seguridad.

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/ncLxKDnaAqw

Conclusiones

El análisis integral demuestra que SecureNova Labs presenta fallas críticas en tres dimensiones esenciales: el marco legal, la protección tecnológica y la capacidad operativa para responder ante incidentes. Las irregularidades contenidas en la documentación revisada evidencian riesgos éticos y normativos que comprometen a la organización y exponen al profesional a responsabilidades penales, lo cual obliga a replantear los procedimientos administrativos y contractuales utilizados internamente.

Desde la perspectiva técnica, la operación Red Team demostró que la vulnerabilidad presente en Host-A permitió un compromiso total de la infraestructura, afectando también a Host-B mediante movimiento lateral. La facilidad del ataque revela ausencia de mantenimiento, carencia de segmentación interna y falta de controles que limiten la expansión del adversario.

El análisis defensivo confirma que la organización no implementa monitoreo, herramientas de detección o mecanismos de contención. La respuesta ante el incidente solo pudo desarrollarse de manera posterior, lo que incrementa el riesgo real frente a amenazas externas.

En síntesis, la infraestructura evaluada refleja una baja madurez en materia de ciberseguridad y requiere adoptar medidas correctivas urgentes, integrando controles técnicos, políticas institucionales y procesos formales que permitan fortalecer la protección interna y garantizar una postura segura frente al panorama actual de amenazas.

Recomendaciones

La evidencia recopilada durante el desarrollo del presente informe permite formular una serie de recomendaciones estratégicas orientadas a mejorar la postura de ciberseguridad de SecureNova Labs. En primer lugar, resulta imprescindible revisar y reformular la documentación legal entregada al personal técnico y administrativo, garantizando que cualquier acuerdo contractual se encuentre alineado con la legislación nacional, los principios éticos profesionales y las buenas prácticas institucionales. Las recomendaciones propuestas se alinean con modelos modernos de operación de centros de seguridad, los cuales destacan la necesidad de integrar monitoreo continuo, respuesta a incidentes estructurada y controles técnicos bien definidos para reducir riesgos operativos (Dahan, 2020).

En segundo lugar, la infraestructura tecnológica requiere la eliminación inmediata de software obsoleto, la actualización permanente de todos los componentes y la adopción de procesos formales de inventario tecnológico. El uso de aplicaciones vulnerables representa una amenaza grave que debe ser atendida mediante controles técnicos que permitan prevenir la explotación de fallas conocidas. Adicionalmente, la segmentación interna debe convertirse en un pilar central de la arquitectura, con el fin de evitar que una intrusión aislada comprometa toda la infraestructura.

Desde el punto de vista defensivo, la empresa debe implementar soluciones tecnológicas avanzadas capaces de monitorear la actividad de los equipos, generar alertas tempranas y actuar automáticamente frente a comportamientos anómalos. Entre estas herramientas se encuentran sistemas SIEM, soluciones IDS/IPS y tecnologías EDR. La incorporación de estos componentes permitirá visibilizar incidentes, reducir tiempos de respuesta y evitar que una intrusión permanezca sin detección durante periodos prolongados.

Asimismo, la organización debe fortalecer sus procesos mediante políticas de hardenización, gestión de cuentas administrativas, restricción de accesos y eliminación de servicios innecesarios. Estas acciones deben acompañarse de mecanismos de auditoría periódica, controles internos y capacitación técnica para los equipos involucrados en la administración de sistemas críticos.

Adicionalmente, el fortalecimiento de la gobernanza de la seguridad y la adopción de prácticas de cumplimiento normativo permiten reducir impactos legales, financieros y reputacionales derivados de incidentes de seguridad (European Union, 2018).

Finalmente, es indispensable que SecureNova Labs establezca una estrategia institucional de respuesta a incidentes que contemple roles, procedimientos, escalamiento de eventos y canales formales de comunicación. Solo mediante una estructura coordinada será posible enfrentar riesgos reales de manera eficiente y garantizar la continuidad operativa de la organización. Estas recomendaciones, aplicadas de forma integral, contribuirán significativamente a elevar la madurez defensiva, proteger los activos digitales y consolidar una postura de seguridad acorde con los estándares internacionales del sector.

Referencias Bibliográficas

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

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide (SP 800-61r2).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Colombia. Congreso de la República. (2009). *Ley 1273 de 2009*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35366

COPNIA. (2008). *Código de Ética Profesional del Ingeniero*. Consejo Profesional Nacional de Ingeniería. https://www.copnia.gov.co

Dahan, I. (2020). *Modern Security Operations Center*. Apress. https://link.springer.com/book/10.1007/978-1-4842-5699-3

ENISA. (2021). *ENISA Threat Landscape*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications

European Union. (2018). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu

Harris, S. (2020). *CISSP All-in-One Exam Guide* (9th ed.). McGraw-Hill. https://www.mheducation.com/highered/product/cissp-all-one-exam-guide-harris/M9781260142648.html

Hutchins, E., Cloppert, M., & Amin, R. (2011). *Intelligence-Driven Computer Network Defense*. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/lockheed-martin-cyber-kill-chain.pdf

IBM Security. (2023). *Cost of a Data Breach Report*. IBM & Ponemon Institute. https://www.ibm.com/reports/data-breach

Mandiant. (2022). *M-Trends Report*. Mandiant Corporation. https://www.mandiant.com/resources/m-trends

Microsoft Security. (2022). *Incident Response Documentation*. https://learn.microsoft.com/en-us/security/

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

OWASP Foundation. (2021). *OWASP Top 10: Web Application Security Risks*. https://owasp.org/www-project-top-ten/

Sharma, A., & Kumar, R. (2020). Advanced persistent threats and defense mechanisms. *International Journal of Cyber Security and Digital Forensics, 9*(3), 45–58. https://sites.google.com/site/ijcsdf/

Singhal, A., & Wilson, W. (2021). *Intrusion Detection Techniques for Enterprise Environments*. Springer. https://link.springer.com/book/10.1007/978-3-030-72158-0

Symantec. (2020). *Internet Security Threat Report*. NortonLifeLock. https://www.broadcom.com/company/newsroom/press-releases

Apéndices

Apéndice A

Resultado de revisión en Turnitin

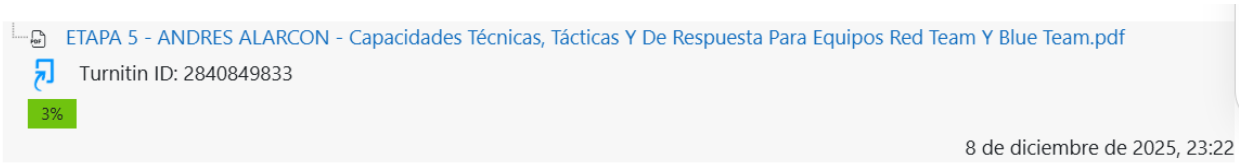
turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	ANDRES LEONARDO ALARCON SALCEDO
Título del ejercicio:	Etapa 5 - Análisis, Reporte y Comunicación de Resultados Técn...
Título de la entrega:	ETAPA 5 - ANDRES ALARCON - Capacidades Técnicas, Tácticas ...
Nombre del archivo:	136562_ANDRES_LEONARDO_ALARCON_SALCEDO_ETAPA_5_-_...
Tamaño del archivo:	5.82M
Total páginas:	73
Total de palabras:	12,928
Total de caracteres:	86,328
Fecha de entrega:	08-dic-2025 11:24p. m. (UTC-0500)
Identificador de la entrega:	2840849833



ETAPA 5 - ANDRES ALARCON - Capacidades Técnicas, Tácticas Y De Respuesta Para Equipos Red Team Y Blue Team.pdf

Turnitin ID: 2840849833

3%

8 de diciembre de 2025, 23:22

Nota. Se presenta el comprobante de revisión de Turnitin para adjuntar la evidencia en el trabajo final y cumplir con la política que exige la universidad.