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

Wilson Dario Rojas Martinez

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

Este informe técnico presenta un análisis integral del caso SecureNova Labs, desarrollado a través de cinco fases consecutivas que integran aspectos legales, éticos y operativos propios de la ciberseguridad contemporánea. El estudio examina las funciones del Red Team y del Blue Team mediante la simulación de un ciclo completo de ataque y defensa, que incluye la identificación de vulnerabilidades, la explotación de servicios expuestos, la aplicación de técnicas de pivoting y movimiento lateral, así como actividades de análisis forense, contención y mitigación. Asimismo, el documento articula el marco jurídico colombiano, en particular la Ley 1273 de 2009 y la normativa de protección de datos personales, con procedimientos de pruebas de penetración, el uso de herramientas ofensivas especializadas y la implementación de controles defensivos orientados al monitoreo, la preservación de evidencias y el fortalecimiento del perímetro de seguridad. Los resultados obtenidos permiten identificar debilidades críticas, reconocer patrones de ataque recurrentes y proponer estrategias de endurecimiento basadas en marcos de referencia reconocidos, concluyendo con recomendaciones orientadas a fortalecer la postura de seguridad en organizaciones con características similares.

Palabras clave: blue team, ciberseguridad, pentesting, pivoting, red team.

Abstract

This technical report presents a comprehensive analysis of the SecureNova Labs case, developed through five consecutive phases that integrate legal, ethical, and operational aspects relevant to modern cybersecurity. The study examines the roles of the Red Team and Blue Team by simulating a complete attack-and-defense cycle, including vulnerability identification, exploitation of exposed services, pivoting techniques, lateral movement, as well as forensic analysis, containment, and mitigation activities. Additionally, the document aligns the Colombian legal framework, particularly Law 1273 of 2009 and data protection regulations, with penetration testing procedures, the use of specialized offensive tools, and the implementation of defensive controls focused on monitoring, evidence preservation, and perimeter security strengthening. The findings identify critical weaknesses, highlight common attack patterns, and propose hardening strategies based on recognized cybersecurity frameworks, concluding with recommendations aimed at improving the security posture of organizations operating under similar conditions.

Keywords**:** *blue team, cybersecurity, pentesting, pivoting, red team.*

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Ataque lateral (Lateral Movement):

Técnica utilizada por un atacante para desplazarse entre sistemas dentro de una red interna después de comprometer un equipo inicial.

Autoroute:

Módulo de Metasploit que permite enrutar tráfico a través de una sesión comprometida para habilitar pivoting.

Blue Team:

Equipo encargado de la defensa activa, detección, monitoreo, respuesta a incidentes y preservación de evidencias.

CVE (Common Vulnerabilities and Exposures):

Identificador estándar que categoriza vulnerabilidades de seguridad conocidas.

Exploit:

Método o código que aprovecha una vulnerabilidad para ejecutar acciones no autorizadas.

HFS (HttpFileServer):

Aplicación utilizada para compartir archivos vía HTTP; versiones antiguas como 2.3 son vulnerables a ejecución remota de código.

Meterpreter:

Payload avanzado de Metasploit que permite control remoto, postexplotación, escalamiento y pivoting.

Nmap:

Herramienta de escaneo de red utilizada para descubrir puertos, servicios y versiones.

Pivoting:

Técnica que permite usar un host comprometido como puente hacia redes internas no accesibles directamente.

Red Team:

Equipo ofensivo encargado de simular ataques reales para evaluar la postura de seguridad de la organización.

Introducción

Teniendo en cuenta el contexto actual en donde las organizaciones dependen cada vez mas de infraestructuras tecnológicas sólidas y a la vanguardia, esto reviste una complejidad más alta para operar los servicios críticos, la gestión de la información sensible y mantenimiento continua del negocio. El aumento de la superficie de ataque en las infraestructuras tecnológicas modernas ha favorecido el uso de técnicas avanzadas como el pivoting y el movimiento lateral, lo que hace indispensable la articulación de equipos ofensivos y defensivos dentro de las organizaciones (Álvarez, 2018; Arroyo, 2025). En este contexto, los enfoques Red Team y Blue Team permiten evaluar de forma realista la postura de seguridad y fortalecer los mecanismos de detección y respuesta ante incidentes.

El desarrollo del seminario se hizo en torno al caso de SecureNove Labs permitiendo con ello el poder abordar de manera progresiva, un conjuntos de escenarios prácticos en donde ser simularon el ciclo completo de un incidentes de seguridad que comprende desde la identificación de vulnerabilidades en la arquitectura de servicios expuesto, pasando por la explotación técnica de servicios expuestos como se vio en la etapa 3 que involucrar Red Team, hasta la contención y repuesta estructurada ante el ataque en la etapa 4 con el equipo Blue Team, sin dejar de lado que en las etapas iniciales se realizó el análisis ético legal asociado con el manejo de información y al uso de herramientas de ciberseguridad.

En este informe se presenta una síntesis técnica, analítica y reflexiva de todo proceso, con el objetivo de integrar y ofrecer una visión integral del caso de SecureNova Labs. Las estrategias Red Team y Blue Team aplicados fueron documentados, a la par se realizó el análisis de los vectores de ataque y las fallas de seguridad, para tal fin se integraron los marcos normativos

relevantes para el caso y se formulan recomendaciones concretas que aportan al diseño de estrategias de seguridad robustas de defensa y respuesta a incidentes.

Justificación

El análisis de los incidentes de seguridad o aislamiento de vulnerabilidades suele ser insuficientes para comprender la complejidad real de los ataques contemporáneos. En la experiencia del caso con SecureNova Labs demuestra que un incidente exitoso rara vez se explica por un único fallo técnico, combinado con la utilización de software desactualizados, configuraciones inseguras, las falencias de los controles de monitoreo, la debilidad organizacional y algunos casos, decisiones éticas cuestionables.

Un informe técnico de cierre tiene sentido por tres razones principales:

Necesidad de integrar las lecciones aprendidas de las etapas 1 a la 4 permite comprender el incidente no solo desde la arquitectura de servicios, la respuesta defensiva y las implicaciones normativas. La adopción de marcos de referencia reconocidos permite comprender el incidente desde una perspectiva integral, superando el análisis puramente técnico e incorporando dimensiones organizacionales, legales y éticas (NIST, 2022; ISO/IEC, 2022).

Fortalecimiento de la madurez organizacional consolidado sirve como insumo para la alta dirección y para analistas, facilitando la toma de decisiones informadas respecto a inversión en controles, definición de políticos y priorización de riesgos.

Para un especialista en ciberseguridad de articulación Red Team, Blue y aspectos legales en un mismo informe contribuye a desarrollar una lógica de trabajo para superar la visión meramente técnica y se alinea con los principios responsabilidades sociales, de ética profesional y cumplimiento normativos.

Por esta razón el informe final se orienta a proporcionar no la reconstrucción técnica de lo ocurrido en SecureNova LAbs, sino también un conjunto de recomendaciones estratégicas que

eleven el nivel de madurez en ciberseguridad de cualquier organización con características similares.

Objetivos

Objetivo General

Elaborar un informe técnico completo que detalle y evalúe las tácticas utilizadas por los equipos Red Team y Blue Team en el caso SecureNova Labs, integrando las consideraciones legales y éticas detectadas, con el propósito de proponer recomendaciones orientadas a fortalecer la seguridad institucional y optimizar los procesos de gestión de incidentes de ciberseguridad.

Objetivos Específicos

Documentar el proceso técnico de ataque ejecutado por el Red Team, mediante la descripción detallada de las fases de reconocimiento, explotación inicial, pivoting y movimiento lateral, las herramientas empleadas y los resultados obtenidos sobre la infraestructura de SecureNova Labs.

Analizar la respuesta del Blue Team frente al incidente, a partir de la identificación y evaluación de las acciones de detección, contención, preservación de evidencias, remediación y hardening implementadas durante el escenario simulado.

Relacionar el caso práctico con los marcos legales y éticos aplicables a la ciberseguridad, mediante el análisis de la Ley 1273 de 2009 y del Código de Ética profesional, identificando posibles implicaciones normativas y responsabilidades asociadas.

Comparar y articular las estrategias ofensivas y defensivas aplicadas, a través de la sistematización de hallazgos y lecciones aprendidas, con el fin de contribuir a la madurez de las capacidades de Red Team y Blue Team en entornos reales.

Proponer recomendaciones técnicas y organizacionales, sustentadas en marcos de referencia internacionales como OWASP, CIS Controls, NIST e ISO/IEC 27001, orientadas al endurecimiento de la seguridad y a la prevención de incidentes de características similares.

Desarrollo del Informe

Panorama General de los Escenarios Trabajados

El proceso formativo se estructuró en cuatro etapas principales:

Etapa 1 TecnoSYS Inc.: Se analizó la infraestructura de una empresa proveedora de servicios de gestión empresarial, almacenamiento en la nube y comercio electrónico. Se identificaron activos críticos y vulnerabilidades asociadas a configuraciones por defecto, falta de segmentación, ausencia de hardening y debilidades en autenticación, tomando como referencia el CWE Top 25, OWASP, NIST e ISO/IEC 27001. Aunque se trata de un caso distinto, las conclusiones son extrapolables al escenario de SecureNova Labs, especialmente en lo que respecta a gestión de vulnerabilidades y arquitectura segura.

Etapa 2 Ciberespionaje y Ética en SecureNova Labs: Se revisaron cláusulas contractuales que inducían a la aceptación y ocultamiento de actividades ilícitas, tales como interceptación de información y acceso abusivo a sistemas informáticos, vulnerando la Ley 1273 de 2009 y el Código de Ética de COPNIA. Esta etapa reforzó la idea de que la ciberseguridad no puede desligarse del marco jurídico ni de la responsabilidad profesional.

Etapa 3 Red Team SecureNova Labs: Se ejecutó un ataque controlado contra Host A, explotando la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3, obteniendo una sesión Meterpreter, realizando escalamiento de privilegios y configurando pivoting hacia Host B, donde se explotó MS17-010 (EternalBlue), logrando movimiento lateral y acceso a información sensible.

Etapa 4 Blue Team SecureNova Labs: Se asumió el rol defensivo frente a un ataque en curso, utilizando únicamente herramientas GPL o gratuitas. Se abordaron actividades de análisis de sistema operativo, análisis de red, contención, preservación de evidencia y diseño de un plan de remediación integral.

El informe final del Escenario 5 integra estas líneas de trabajo y las presenta como un ciclo completo de ataque y defensa, enriquecido con un marco ético-legal.

Panorama Específico De Etapa 1

Legislación Colombiana Aplicable a Ciberseguridad y Tratamiento de Datos

En Colombia, las actividades de ciberseguridad deben alinearse con el marco jurídico vigente, particularmente con la Ley 1273 de 2009, que tipifica delitos como el acceso abusivo a sistemas informáticos y la interceptación ilegal de datos (Congreso de la República de Colombia, 2009). De igual forma, el tratamiento de datos personales durante pruebas de seguridad debe ajustarse a los principios establecidos en la Ley 1581 de 2012 y su decreto reglamentario (Congreso de la República de Colombia, 2012; Decreto 1377 de 2013).

Ley 1273 de 2009 – Protección de la Información y los Datos

La Ley 1273 de 2009 incorpora al Código Penal el bien jurídico de protección de la información y tipifica delitos asociados al acceso indebido, alteración y afectación de datos y sistemas informáticos. Los artículos más relevantes para actividades de ciberseguridad incluyen:

- Art. 269A – Acceso abusivo a sistemas informáticos
- Art. 269B – Obstaculización ilegítima de sistemas o redes

- Art. 269C – Interceptación ilegal de datos informáticos
- Art. 269D – Daño informático
- Art. 269E – Uso de software malicioso
- Art. 269F – Violación de datos personales
- Art. 269G – Suplantación de sitios web
- Art. 269I y 269J – Hurto por medios informáticos y transferencia no consentida

Esta ley contextualiza los límites éticos y legales del Red Team: cualquier acción ofensiva solo puede ejecutarse con autorización, en entornos controlados y con fines defensivos, evitando afectar integridad, disponibilidad o privacidad de datos reales.

Ley 1581 de 2012 y Decreto 1377 de 2013 – Protección de Datos Personales

La Ley 1581 y su decreto reglamentario establecen principios, derechos y obligaciones en el tratamiento de datos personales, con énfasis en:

- Finalidad y legitimidad del tratamiento
- Seguridad y confidencialidad de los datos
- Derechos del titular (acceso, rectificación, supresión)
- Autorización previa e informada

Para Red Team y Blue Team, estas normas determinan:

- Qué tipo de datos pueden manipularse durante pruebas.
- Qué información debe anonimizarse o excluirse.
- Cómo se deben preservar evidencias sin vulnerar datos sensibles.

Por tanto, toda actividad técnica debe alinearse con los principios de minimización, proporcionalidad y necesidad.

Ley 1266 de 2008 – Habeas Data Financiero

Esta ley regula el manejo de información financiera, exigiendo veracidad, actualización, seguridad y circulación restringida de los datos. Es relevante para entornos corporativos donde sistemas financieros podrían ser objetivo de auditorías o pruebas de intrusión. La norma protege:

- Información crediticia
- Datos transaccionales
- Historial financiero

Equipos Red Team deben evitar manipular este tipo de información sin estrictas medidas de seguridad y consentimiento formal.

Ley 1621 de 2013 – Inteligencia y Contrainteligencia

Aunque orientada a organismos estatales, establece criterios aplicables a la gobernanza de información sensible:

- Principios de legalidad, necesidad, proporcionalidad
- Manejo de información clasificada
- Obligación de confidencialidad

Estos principios pueden extrapolarse a entornos de ciberseguridad corporativa, especialmente en:

- Gestión de logs

- Preservación de evidencia
- Acceso a documentación sensible

Etapas del Pentesting y Su Relación con Red Team / Blue Team

El pentesting constituye una práctica fundamental para la identificación controlada de vulnerabilidades, ya que simula técnicas empleadas por atacantes reales con el fin de evaluar la resiliencia de los sistemas (OWASP, 2023; NIST, 2022). Desde esta perspectiva, el Red Team reproduce tácticas ofensivas mientras que el Blue Team se enfoca en la detección, contención y mitigación del incidente, generando un proceso continuo de mejora de la seguridad organizacional (Arroyo, 2025).

La fase de reconocimiento tiene como objetivo la recopilación de información pública o accesible sobre el objetivo, sin interacción directa con los sistemas internos. En esta etapa se emplean herramientas como WHOIS, Shodan, theHarvester y escaneos básicos con Nmap, orientados a identificar dominios, rangos IP, servicios expuestos y posibles superficies de ataque. Desde la perspectiva del Blue Team, esta fase debe ser monitoreada mediante la detección de consultas DNS inusuales, múltiples solicitudes HTTP con patrones de fingerprinting y escaneos discretos dirigidos a direcciones IP corporativas. Es importante resaltar que, desde el punto de vista legal, estas actividades solo son válidas cuando existe autorización expresa, dado que un uso indebido podría derivar en responsabilidades jurídicas.

Posteriormente, en la etapa de enumeración y escaneo, el Red Team profundiza en la identificación de servicios activos, puertos abiertos, versiones de software y posibles vectores de ataque. Para ello se utilizan herramientas especializadas como Nmap con scripts NSE, Gobuster, enum4linux y Nikto, las cuales permiten obtener información más detallada sobre la arquitectura

interna y los servicios desplegados. Frente a estas acciones, el Blue Team debe analizar picos anómalos de tráfico SYN a nivel de firewall o IDS, detectar intentos de exploración de directorios y rutas web, así como registrar consultas inusuales dirigidas a servicios como SMB, LDAP o FTP, que suelen ser indicativas de actividades de reconocimiento avanzado.

La fase de análisis de vulnerabilidades se orienta a identificar debilidades conocidas asociadas a las versiones y configuraciones detectadas previamente. En este punto se emplean herramientas como OpenVAS, Nessus o WPScan, cuya salida incluye la identificación de vulnerabilidades catalogadas como CVE, priorizadas generalmente mediante métricas como el CVSS, junto con evidencia técnica que respalda los hallazgos. El rol del Blue Team en esta etapa consiste en validar el estado real de los parches, evaluar el riesgo considerando el contexto y la exposición efectiva de los activos, e integrar los CVE identificados dentro del inventario institucional de vulnerabilidades para su posterior gestión y mitigación.

La explotación, siempre realizada bajo autorización explícita, busca validar si un vector identificado puede ser utilizado para comprometer efectivamente un sistema. En esta fase se emplean herramientas como Metasploit, sqlmap o Burp Suite, procurando en todo momento respetar principios éticos fundamentales, como evitar acciones destructivas, no generar interrupciones de servicio y preservar la evidencia técnica obtenida. Desde la óptica defensiva, el Blue Team debe detectar la ejecución de payloads sospechosos, como comandos en PowerShell o procesos anómalos, monitorear la creación de sesiones remotas no autorizadas y generar alertas basadas en firmas de explotación conocidas mediante sistemas IDS/IPS como Snort o Suricata.

Una vez logrado el acceso inicial, la fase de post-explotación permite evaluar el impacto real del compromiso, incluyendo la obtención de privilegios elevados, la persistencia y el movimiento lateral dentro de la red. Para estas actividades se utilizan herramientas como Meterpreter, PowerShell Empire y BloodHound, las cuales facilitan la exploración de relaciones de confianza y credenciales. El Blue Team, por su parte, debe concentrarse en la detección de escalamiento de privilegios, la identificación de conexiones laterales entre sistemas y la revisión de eventos críticos en los registros del sistema, como los eventos 4624, 4672 y 7045 en entornos Windows, que suelen reflejar accesos y cambios relevantes.

Finalmente, la etapa de limpieza y reporte representa el cierre formal del ejercicio de pentesting. En esta fase se eliminan cuentas creadas durante las pruebas, se borran artefactos temporales, se restauran configuraciones alteradas y se documentan de manera detallada los hallazgos obtenidos. El Blue Team debe validar la integridad del entorno posterior a las pruebas, actualizar indicadores de compromiso (IOC), ajustar reglas defensivas y fortalecer los playbooks de respuesta a incidentes, garantizando que las lecciones aprendidas se traduzcan en mejoras concretas de la postura de seguridad organizacional.

Herramientas Clave en Ciberseguridad

Para cumplir el llamado del tutor a sintetizar, esta sección se resume en los elementos esenciales:

Metasploit Framework

Framework modular para explotación controlada. Útil para validar CVEs, demostrar impacto y documentar ruta de compromiso.

Blue Team: obtiene IOC, analiza comportamiento de payloads, desarrolla reglas de detección.

Nmap

Fundamental para descubrimiento y enumeración.

Blue Team: detecta patrones de escaneo y anomalías de red.

OpenVAS

Escáner de vulnerabilidades basado en NVT actualizables.

Blue Team: prioriza parches y seguridad preventiva.

Exploit-DB y CVE

Repositorios de vulnerabilidades y PoC.

Blue Team: usa CVE/CVSS para priorizar riesgos; crea detecciones basadas en PoC (sin ejecutarlas en producción).

Síntesis Final de la Etapa 1

La legislación colombiana establece un marco robusto que regula la actuación segura y ética de profesionales en ciberseguridad. El pentesting, como proceso sistemático, permite simular ataques con el fin de identificar fallas reales en infraestructuras tecnológicas, siempre bajo autorización expresa. Las herramientas técnicas complementan las fases metodológicas, pero deben usarse con responsabilidad y trazabilidad.

Esta etapa permite comprender que la seguridad no depende únicamente de las capacidades ofensivas o defensivas, sino de la integración coherente entre marco legal, buenas prácticas técnicas y un enfoque ético-profesional.

El uso de herramientas como Metasploit, Nmap y OpenVAS se encuentra ampliamente documentado en guías técnicas y repositorios de vulnerabilidades, los cuales facilitan la identificación, validación y priorización de riesgos en entornos corporativos (Exploit-DB, s.f.; CVE, s.f.).

Conclusiones Parciales de La Etapa 1

El estudio realizado permitió reconocer la importancia del enfoque complementario entre los equipos Red Team y Blue Team dentro de la ciberseguridad contemporánea. Mientras el Red Team reproduce de forma controlada las técnicas utilizadas por actores maliciosos para identificar vulnerabilidades reales, el Blue Team se centra en la defensa activa mediante la detección, mitigación y manejo de incidentes. Esta interacción crea un proceso continuo de retroalimentación que fortalece la protección de los sistemas y activos digitales.

En el contexto colombiano, el marco normativo sobre delitos informáticos y tratamiento de datos personales integrado por leyes como la 1273 de 2009, 1581 de 2012, 1266 de 2008 y 1621 de 2013 define las pautas éticas y legales bajo las cuales deben operar los especialistas en seguridad. La observancia de estas disposiciones es fundamental para garantizar que las pruebas de penetración y auditorías se realicen de manera legítima y respetuosa de los derechos de los usuarios.

Las fases del pentesting, desde la preparación hasta la elaboración del informe final, conforman un procedimiento metódico que facilita la identificación de fallos y la valoración de su impacto. Dominar estas etapas permite desarrollar procesos ordenados, verificables y alineados con lineamientos internacionales y la OWASP Testing Guide.

Las herramientas empleadas en el análisis entre ellas Metasploit, Nmap, OpenVAS, ExploitDB y los repositorios de CVE resultan fundamentales para detectar, verificar y comprender vulnerabilidades. Su aplicación controlada en entornos de práctica contribuye a fortalecer las capacidades técnicas del analista y a que el Blue Team pueda anticiparse a amenazas mediante una adecuada gestión de alertas, parches y eventos de seguridad.

El uso de un laboratorio virtual en VirtualBox, con sistemas como Parrot OS o Kali Linux en conjunto con Windows, ofrece un espacio seguro para experimentar, simular ataques y aplicar defensas sin comprometer entornos reales. Este tipo de infraestructura resulta clave para afianzar el aprendizaje práctico y comprobar los conceptos abordados durante el curso.

En conjunto, la actividad permitió articular los componentes legales, técnicos y éticos de la ciberseguridad, promoviendo una perspectiva crítica y responsable del papel del profesional encargado de proteger la información. A su vez, se fortalecieron las competencias de trabajo conjunto entre equipos ofensivos y defensivos, contribuyendo a la construcción de ambientes digitales más robustos, confiables y resilientes.

Panorama Específico de Etapa 2

Análisis Ético Y Legal

Tras la revisión integral del Anexo 2 Escenario y del Anexo 3 Acuerdo, es posible identificar la presencia de cláusulas que constituyen prácticas contrarias al ordenamiento jurídico colombiano y vulneran principios éticos profesionales. En el Escenario se advierte desde el inicio la existencia de inconsistencias contractuales elaboradas por un funcionario removido por malas prácticas, lo cual genera dudas sobre la legitimidad del documento.

Esta sospecha se confirma al analizar el Acuerdo, donde se observan disposiciones que:

Normalizan actividades ilícitas, como “interceptación de información, acceso abusivo a sistemas informáticos y manipulación de datos”, conductas tipificadas en los artículos 269A y 269D de la Ley 1273 de 2009.

Restringen la denuncia ante autoridades competentes, lo cual contradice el Código de Ética Profesional del COPNIA (Art. 31, lit. f) que obliga al ingeniero a reportar cualquier irregularidad o conducta delictiva.

Pretenden eximir de responsabilidad penal a la empresa, trasladándola al profesional, en contravía del artículo 6 de la Constitución Política, que establece la responsabilidad individual frente a la ley.

El ejercicio del pentesting y del análisis forense debe estar guiado no solo por criterios técnicos, sino también por principios éticos profesionales, como los establecidos en el Código de Ética del COPNIA, los cuales exigen actuar con integridad, legalidad y responsabilidad social (COPNIA, 2014).

En consecuencia, el Acuerdo presenta irregularidades graves, que comprometerían la responsabilidad penal, disciplinaria y ética del profesional firmante y vulneran principios como integridad, legalidad y responsabilidad social.

Precisión al explicar los artículos de la Ley 1273 vulnerados

Versión optimizada

El Anexo 3 vulnera directamente los siguientes artículos de la Ley 1273 de 2009:

Artículo 269A – Acceso abusivo a sistemas informáticos:

Las actividades mencionadas en el acuerdo (“accesos no autorizados”, “copias de datos” o “manipulación de información”) encajan plenamente en esta conducta punible.

Artículo 269D – Interceptación de datos informáticos:

La referencia explícita a prácticas de “interceptación” o “chuzadas” constituye un delito sancionado con penas de prisión y multas.

Adicionalmente, la prohibición de denunciar actividades ilegales describe una conducta que facilita la continuidad delictiva y convierte al profesional en coautor o cómplice, según los principios del Código Penal Colombiano.

Mejora de la postura ética frente a la oferta laboral

A pesar del atractivo económico ofertado, aceptar un contrato que contiene cláusulas ilegales y antiéticas sería incompatible con la responsabilidad profesional. El documento exige omitir denuncias, participar en prácticas ilícitas y asumir responsabilidades penales ajenas, lo cual contraviene:

el Código de Ética del COPNIA, los principios fundamentales de la ciberseguridad (confidencialidad, integridad y legalidad), y la dignidad profesional del ingeniero.

Por ello, la decisión responsable es rechazar la oferta, ya que ningún beneficio económico justifica comprometer los principios éticos ni asumir riesgos penales.

Reflexión Personal

El caso de SecureNova Labs evidencia una contradicción profunda entre la imagen de una empresa líder en ciberseguridad y la inclusión de cláusulas contractuales que vulneran la ley y los principios éticos. Este tipo de prácticas deteriora la confianza, compromete la transparencia organizacional y expone a los profesionales a riesgos legales y disciplinarios injustificados.

La ciberseguridad, como disciplina, se fundamenta en la protección de derechos fundamentales, el manejo legítimo de datos y la integridad profesional; por ello, cualquier

acuerdo que promueva conductas ilícitas pone en riesgo la credibilidad de la organización y del sector en general.

Límites Del Acceso A Información

El acceso a información sensible debe limitarse estrictamente a lo requerido para cumplir el alcance definido de la auditoría o prueba de seguridad. Esto debe estar documentado, autorizado y sometido a controles como:

- acuerdos de confidencialidad válidos y auditables,
- registros de trazabilidad,
- segmentación de funciones,
- auditorías externas independientes,
- políticas internas de ética y responsabilidad profesional.

Ninguno de estos mecanismos puede impedir la denuncia de actividades ilegales, pues ello constituye una obligación ética y jurídica.

Mecanismos de Supervisión Interna

Para evitar abusos en el uso de herramientas forenses, la empresa debe establecer:

- Controles preventivos: mínimo privilegio, necesidad de saber, segregación de funciones.
- Controles detectivos: monitoreo continuo, auditoría de registros, sistemas de alerta.
- Controles correctivos: sanciones disciplinarias, comités de ética, revocación de privilegios.

- Controles independientes: auditorías bajo ISO 27001, 27037 y 27043.
- Controles culturales: formación ética permanente y cultura organizacional de integridad.

El Rol del Estado Y Las Instituciones

Cuando se confirma que una empresa contratada incurre en ciberespionaje, el Estado debe iniciar:

- investigación penal y administrativa,
- preservación forense de evidencia,
- supervisión mediante entidades como la Fiscalía o unidades de delitos informáticos.

Las organizaciones afectadas deben:

- rescindir el contrato,
- denunciar ante las autoridades,
- realizar auditorías externas,
- regenerar credenciales y reforzar sus controles internos.

Para restablecer la confianza, se deben implementar:

- evaluaciones independientes periódicas,
- certificaciones obligatorias,
- mejoras en la gobernanza de proveedores,
- políticas de integridad y transparencia.

Conclusiones Parciales De La Etapa 2

El análisis del caso evidencia que el Anexo 3 – Acuerdo presentado por SecureNova Labs incluye disposiciones que podrían facilitar la comisión de conductas tipificadas como delitos informáticos en la Ley 1273 de 2009, particularmente aquellas referentes al acceso no autorizado, la interceptación de datos y el encubrimiento de actividades irregulares. Estas cláusulas también contradicen los principios del Código de Ética Profesional, el cual exige denunciar acciones ilícitas, actuar en beneficio de la sociedad y preservar la integridad en el ejercicio profesional. De esta manera, el documento pone de manifiesto que la ética en la ciberseguridad no es un elemento accesorio, sino un pilar indispensable para garantizar prácticas responsables y la adecuada protección de la información.

Asimismo, se establece que el manejo de información sensible en procesos de auditoría debe regirse por los principios de mínimo privilegio, separación de funciones, trazabilidad y controles de auditoría tanto internos como externos. Ante el riesgo de un uso inadecuado de herramientas forenses, las organizaciones están obligadas a fortalecer sus mecanismos de gobernanza, supervisión y cumplimiento, apoyándose en estándares como ISO/IEC 27001, 27037 y 27047.

Finalmente, ante incidentes de ciberespionaje, tanto los gobiernos como las instituciones deben responder mediante investigaciones formales, posibles terminaciones contractuales, sanciones, auditorías independientes y estrategias de comunicación transparente. Estas acciones buscan recuperar la confianza pública y fomentar una cultura de responsabilidad profesional que impida la reincidencia de conductas similares.

Panorama Específico de Etapa 3

Herramientas Software Utilizadas

Para el desarrollo del Escenario 3 – Red Team, se emplearon herramientas propias de un proceso de intrusión estructurado, siguiendo las fases del pentesting: reconocimiento, enumeración, explotación, post-explotación y pivoting. A continuación, se describen las herramientas, sus funciones, los comandos utilizados y los resultados obtenidos.

Maquinas empleadas para la implementación.

Parrot OS – Máquina Atacante (Red Team)

Descripción:

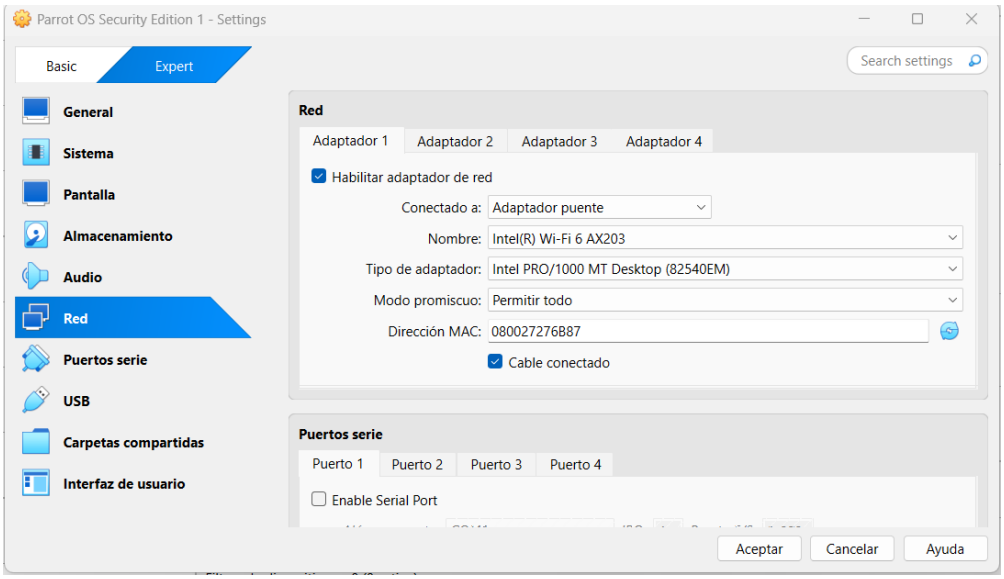
En el apartado de configuración de red de VirtualBox, la máquina virtual Parrot OS Security Edition se ha configurado con un adaptador de red en modo “Adaptador puente”. Este adaptador se asocia a la interfaz física Intel(R) Wi-Fi 6 AX203 del host, permitiendo que la máquina virtual obtenga una dirección IP directamente en la misma red que el equipo físico.

Esta configuración facilita la comunicación directa entre el equipo atacante (Parrot OS) y las máquinas objetivo Windows (Host-A y Host-B), sin necesidad de NAT adicional, lo que resulta apropiado para simular escenarios de Red Team en un entorno controlado de laboratorio.

Como se observa en la Figura 1, el equipo atacante Parrot OS se conecta a la red mediante un adaptador puente, compartiendo segmento con los hosts Windows.

Figura 1

Configuración del adaptador de red de la máquina virtual Parrot OS en VirtualBox en modo "Adaptador puente".

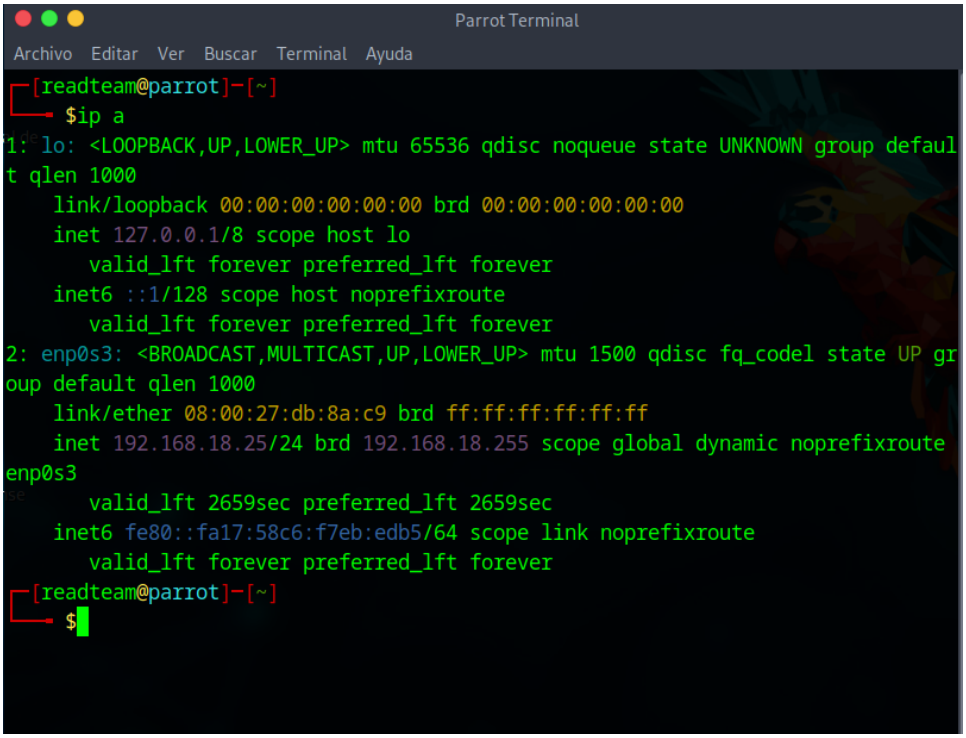


Nota. Configuración del adaptador de red de la máquina virtual Parrot OS 1 en modo adaptador de red; fuente propia (2025).

A continuación, se muestra la comprobación de la dirección IP asignada a la máquina virtual Parrot OS mediante el comando ip a, con el fin de validar su conectividad dentro del laboratorio

Figura 2

Salida del comando ip a en Parrot OS mostrando la dirección IP asignada



Nota. Se observa la dirección IP 192.168.18.25/24, asignada mediante el adaptador puente configurado previamente en VirtualBox. Esta información confirma la conectividad del atacante dentro del laboratorio virtual. Fuente propia (2025).

Ejecutar el reconocimiento inicial.

Explorar vulnerabilidad en Rejjeto alojado en Host-A.

Iniciar el pivoting hacia la red interna.

Host-A – Máquina Intermedia Vulnerable (Windows 7)

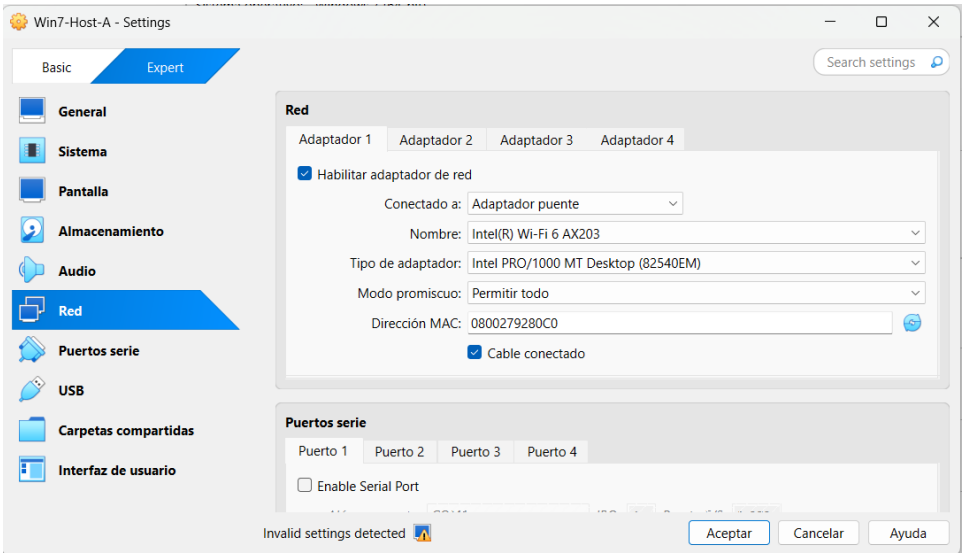
Descripción:

Es la máquina Windows donde se instaló Rejjeto, la aplicación vulnerable obligatoria del escenario. Funciona como punto de entrada del atacante y como puente hacia la red interna donde se encuentra el servidor final (Host-B).

En la siguiente figura se observa la configuración del adaptador de red asignado a la máquina virtual Windows 7 (Host-A) dentro de VirtualBox, empleando el modo adaptador puente para garantizar su integración con la red del laboratorio.

Figura 3

Configuración del adaptador de red de la máquina virtual Windows 7 Host-A en modo adaptador puente.



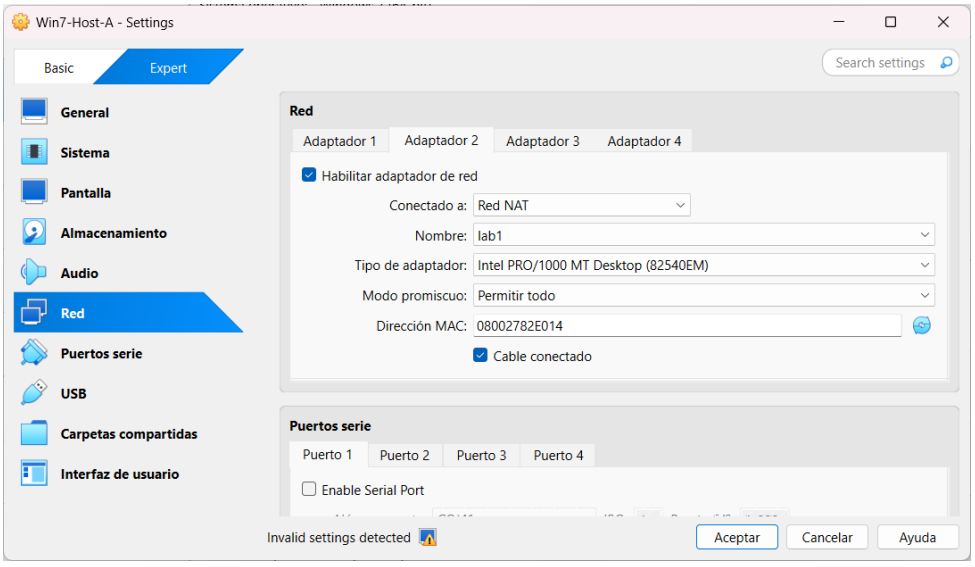
Nota. La imagen muestra la habilitación del adaptador de red de Host-A, configurado en modo adaptador puente y con modo promiscuo en “Permitir todo”, lo cual permite su comunicación directa con la red física del laboratorio. Fuente propia (2025).

Seguidamente se presenta la configuración de Host-A cuando se utiliza NAT como alternativa al adaptador puente, permitiendo validar ambos esquemas de conectividad dentro del laboratorio

A continuación, se detalla la configuración alternativa del adaptador de red de la máquina virtual Windows 7 Host-A, en la cual se emplea el modo Red NAT para permitir conectividad controlada hacia el exterior mientras se mantiene el aislamiento del entorno interno del laboratorio.

Figura 4

Configuración del adaptador de red de la máquina virtual Windows 7 Host-A en modo Red NAT.



Nota. La figura muestra el adaptador de red configurado en modo Red NAT,Esta configuración permite que la máquina virtual acceda a Internet a través del host sin exponerse directamente a la red física. Fuente propia (2025).

Función:

Recibir el ataque directo desde Parrot.

Ser comprometida mediante Rejjeto y entregar shell remota.

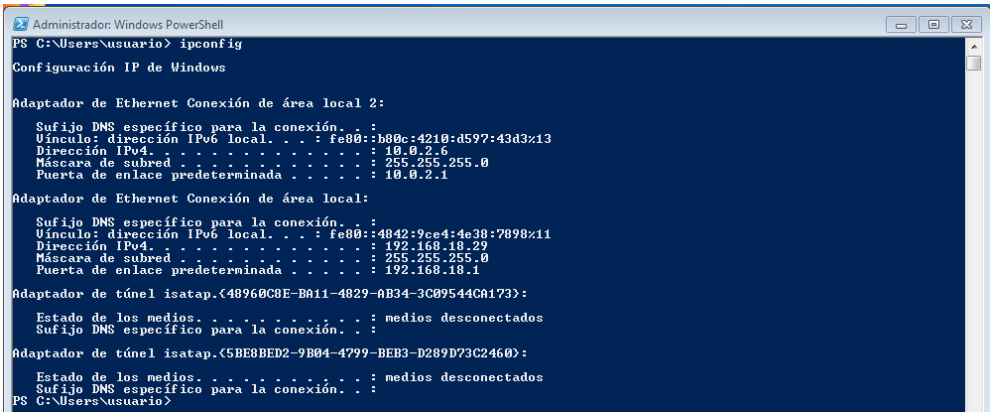
Permitir pivoting hacia Host-B gracias a sus dos interfaces.

Una vez configurado el adaptador de red del Host-A, se verifica la asignación de direcciones IP internas y la correcta detección de sus interfaces de red mediante el comando

ipconfig ejecutado en la consola de PowerShell, como se puede ver en siguiente figura. Esta verificación permite identificar las subredes a las que pertenece la máquina y confirmar la interoperabilidad entre los adaptadores virtuales configurados en VirtualBox.

Figura 5

Salida del comando ipconfig en Windows 7 Host-A, mostrando las interfaces de red activas y sus direcciones asignadas.



Nota. La figura muestra los adaptadores de red del Host-A, incluyendo la interfaz configurada en la red interna 10.0.2.6 y la dirección asignada por la red puente 192.168.18.29. para enlazar correctamente con el Host-B y validar el escenario de pivoting. Fuente propia (2025).

Host-B – Servidor Interno (Windows 7)

Descripción:

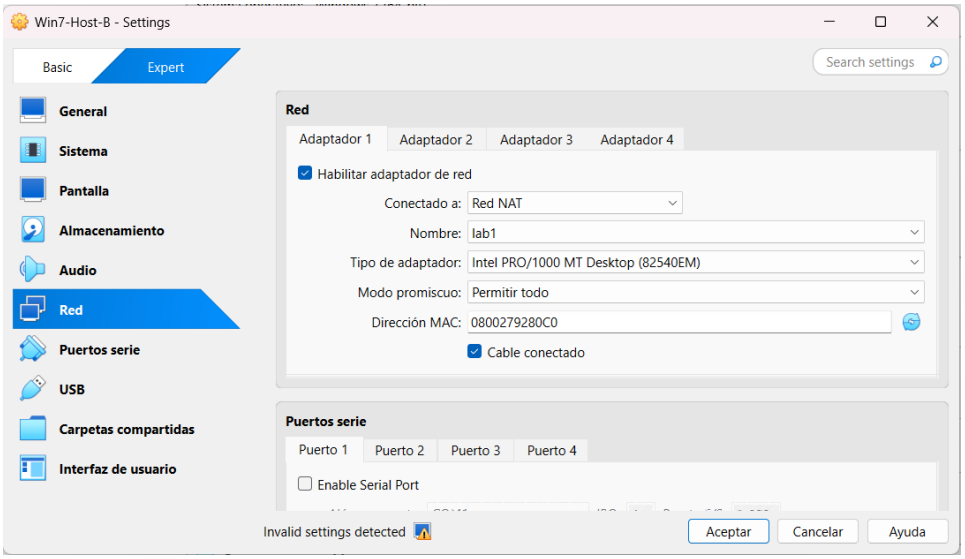
Es la máquina objetivo final del ejercicio. Representa un servidor interno de la organización en el cual se debe realizar la prueba de concepto controlada, que consiste en crear y eliminar un usuario administrativo efímero una vez obtenido acceso mediante pivoting.

En el caso del Host-B, se emplea una configuración de red distinta a la del Host-A, manteniéndolo en un segmento controlado mediante la opción Red NAT. Este aislamiento permite simular correctamente el escenario forense donde el atacante pivotó desde Host-A hacia

Host-B a través de rutas internas, asegurando un entorno reproducible para el análisis del movimiento lateral. Como se ve en la figura a continuación.

Figura 6

Configuración del adaptador de red de Host-B en VirtualBox utilizando el modo Red NAT.



Nota. La configuración del adaptador de Host-B en modo Red NAT permite situar esta máquina en una subred virtual aislada. Este ajuste es crucial para controlar el flujo de red entre Host-A y Host-B durante las pruebas de pivoting. Fuente propia (2025).

Red Interna LAN

Función:

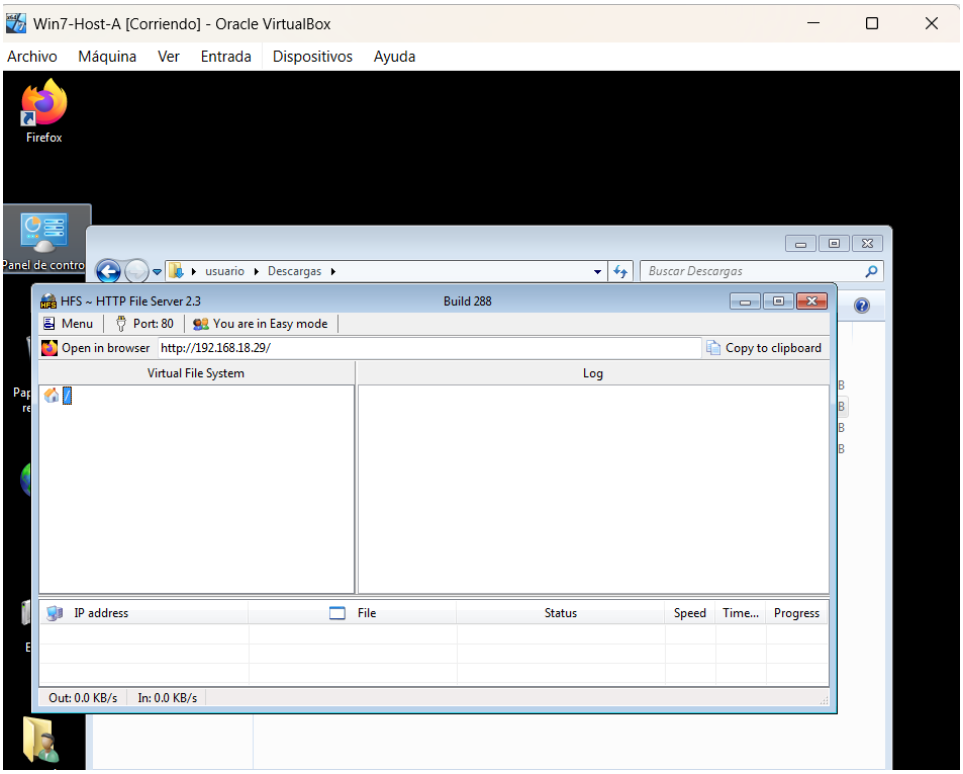
Ser alcanzado únicamente mediante pivoting desde Host-A.

Validar el compromiso mediante la creación y eliminación del usuario efímero.

Generar evidencias en los logs de Windows para análisis forense.

Figura 7

Encendido de la Aplicación HFS para inicio vulnerabilidad rejetto

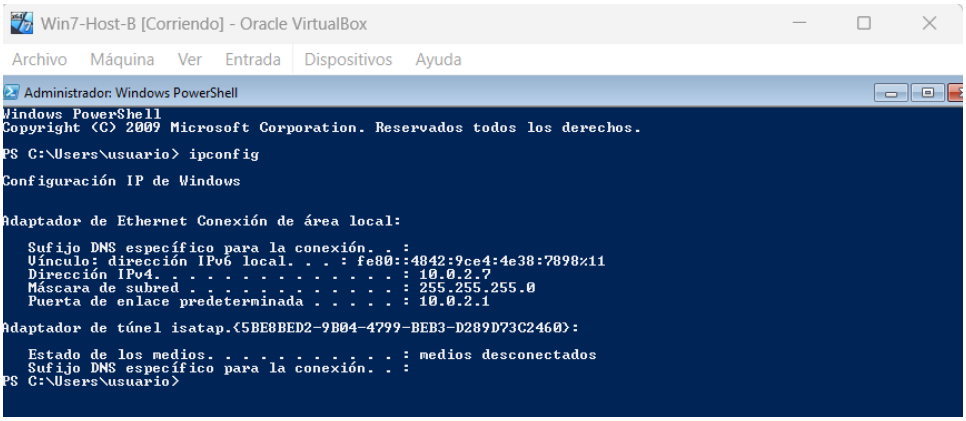


Nota. La configuración del Host-A para inicio de la vulnerabilidad por medio del encendio de la aplicación HFS 2.3. Fuente propia (2025).

Tras configurar el adaptador de red del Host-B en modo Red NAT, se verifica la asignación de parámetros de red dentro de la subred virtual. Esta comprobación garantiza que el Host-B se encuentra correctamente ubicado en el segmento 10.0.2.0/24, lo cual es fundamental para reproducir el escenario de pivoting desde Host-A hacia Host-B.

Figura 8

Resultado del comando ipconfig en Host-B, mostrando la asignación de la dirección IPv4 10.0.2.7 dentro de la red virtual.



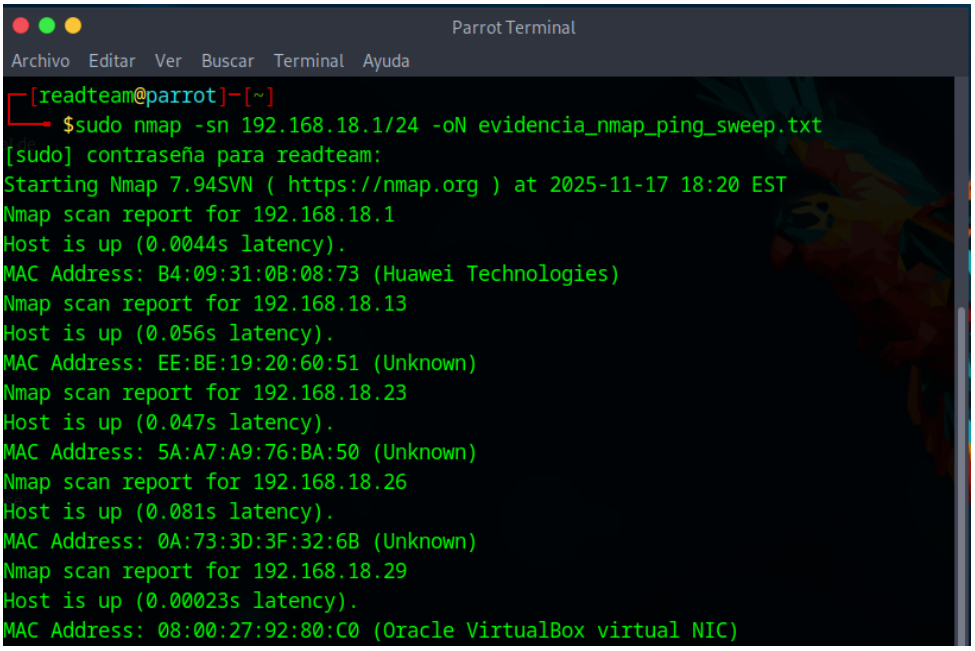
Nota. La salida del comando ipconfig confirma que el Host-B recibió la dirección IP 10.0.2.7 con puerta de enlace 10.0.2.1. (2025).

Reconocimiento inicial con Nmap (Ping Sweep)

Como parte de la fase de reconocimiento activo, se ejecutó un escaneo tipo *ping sweep* sobre la red 192.168.18.0/24 utilizando Nmap. Esta técnica permite identificar qué hosts se encuentran activos antes de proceder con enumeración de servicios o explotación. Los resultados obtenidos revelan múltiples dispositivos conectados, incluyendo la máquina Host-A (192.168.18.29), cuya dirección MAC coincide con un adaptador virtual de VirtualBox.

Figura 9

Resultado del escaneo Nmap tipo ping sweep sobre la red 192.168.18.0/24 desde Parrot OS.



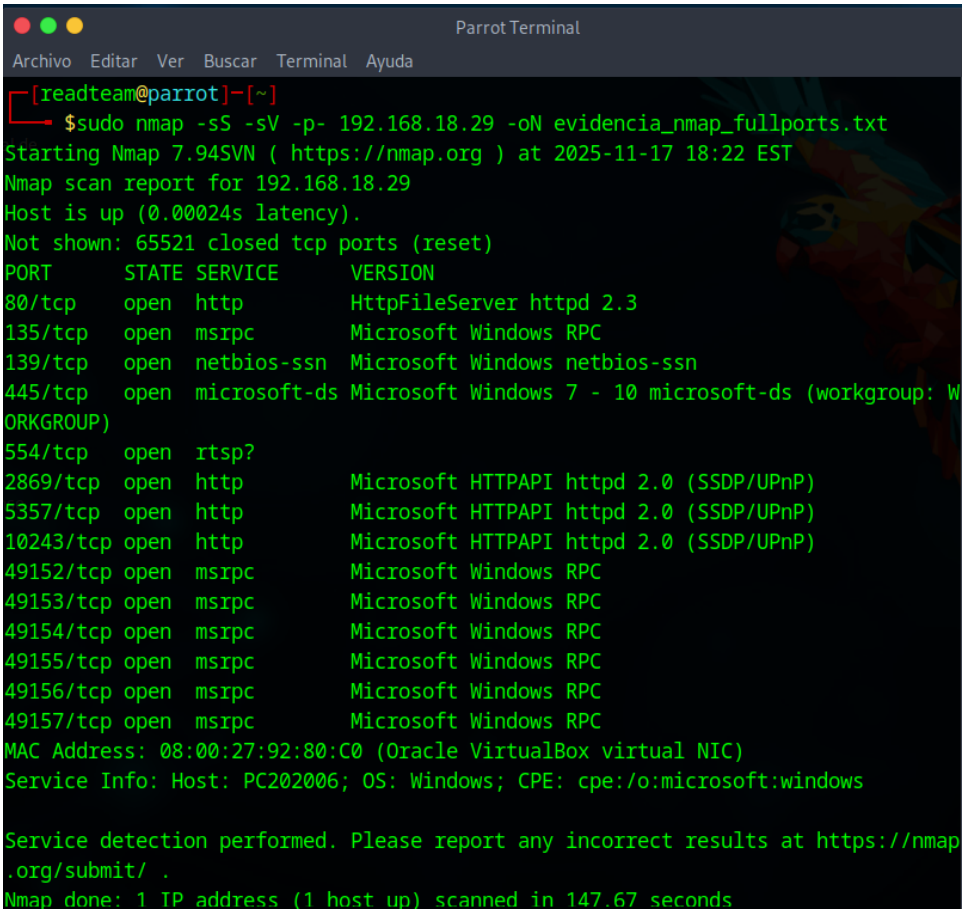
Nota. La ejecución del comando sudo nmap -sn 192.168.18.1/24 -oN evidencia_nmap_ping_sweep.txt. Destaca la detección de la máquina 192.168.18.29, correspondiente al Host-A comprometido, cuya dirección MAC concuerda con una interfaz virtual de Oracle VirtualBox. Fuente propia (2025).

Escaneo exhaustivo de puertos y detección de servicios en Host-A

En este paso se realiza un escaneo completo de puertos TCP sobre el Host-A (192.168.18.29) utilizando Nmap con técnicas de detección de servicios (-sV) y escaneo SYN (-sS). Este procedimiento permite identificar qué puertos se encuentran abiertos, qué servicios se ejecutan en ellos y qué versiones específicas están activas. La información obtenida es fundamental para determinar posibles vectores de ataque, validar vulnerabilidades conocidas (como HttpFileServer 2.3) y confirmar la superficie de exposición del sistema comprometido. Comando utilizado sudo nmap -sS -sV -p- 192.168.18.29 -oN evidencia_nmap_fullports.txt

Figura 10

Resultado del escaneo exhaustivo de puertos y servicios en Host-A mediante Nmap.



Nota. Captura de pantalla del comando sudo nmap -sS -sV -p- 192.168.18.29 -oN evidencia_nmap_fullports.txt ejecutado en Parrot OS para identificar puertos TCP abiertos y servicios activos en el Host-A (fuente propia, 2025).

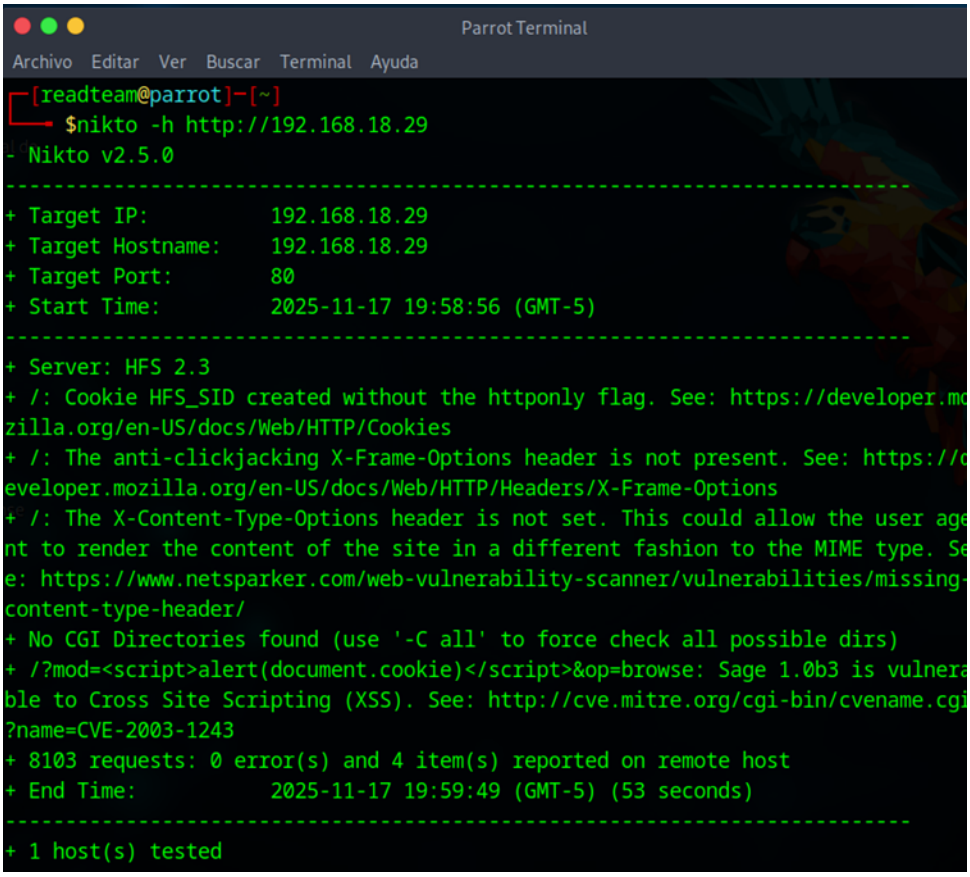
Identificación del servicio vulnerable HFS 2.3 mediante análisis automatizado con Nikto

En este paso se empleó la herramienta Nikto, un escáner de vulnerabilidades web de código abierto, para confirmar la presencia del servicio HttpFileServer (HFS) versión 2.3 en el Host-A. Este análisis es fundamental para validar el vector de entrada identificado previamente mediante Nmap y cURL, permitiendo corroborar tanto la versión del software como la existencia de cabeceras inseguras y configuraciones deficientes asociadas a vulnerabilidades conocidas. La

detección explícita del banner “Server: HFS 2.3” confirma que el sistema ejecuta una versión vulnerable asociada al CVE-2014-6287, utilizada con frecuencia para lograr ejecución remota de comandos.

Figura 11

Detección del servidor HFS 2.3 en el Host-A mediante escaneo Nikto



Nota. Resultado del análisis de seguridad ejecutado con Nikto sobre la dirección IP del Host-A (192.168.18.29), en el cual se identifica el banner del servidor **HFS 2.3** y múltiples cabeceras HTTP inseguras asociadas a vulnerabilidades reportadas. Captura de pantalla de elaboración propia (2025).

Se realizó una verificación OSINT para confirmar si la versión del servicio identificado (HFS 2.3) presenta vulnerabilidades conocidas. En los resultados de búsqueda se evidencian

referencias a la vulnerabilidad **CVE-2014-6287**, asociada a ejecuciones remotas de código en versiones 2.3 y 2.3a de HFS (Figura 12).

Inicialización de Metasploit Framework para la verificación de vulnerabilidades en el servicio HFS 2.3

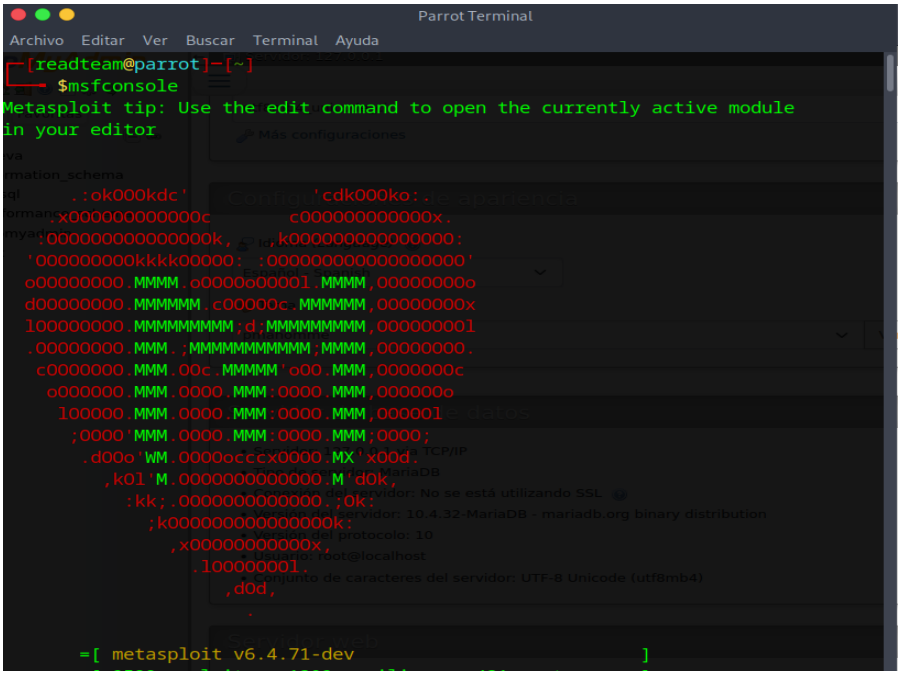
En esta etapa se inicializa Metasploit Framework desde Parrot OS con el fin de utilizar módulos de explotación y verificación asociados al servicio vulnerable HFS 2.3, previamente identificado en el Host-A (192.168.18.29).

La herramienta Metasploit permite realizar un análisis especializado mediante el módulo rejetto_hfs_exec, asociado a la vulnerabilidad CVE-2014-6287, la cual habilita la ejecución remota de comandos (RCE) (Rapid7, s.f.).

Este paso es fundamental para confirmar si el servicio identificado es efectivamente explotable y para continuar con la fase de intrusión controlada solicitada por la guía académica.

Figura 12

Inicialización de Metasploit Framework desde Parrot OS para el análisis del servicio HFS 2.3.



Nota. Resultados de Searchsploit mostrando exploits disponibles para las versiones 2.3.x de HFS, entre ellos varios de ejecución remota de código (RCE). Captura de pantalla realizada por el autor (2025).

Selección del módulo Rejetto HFS en Metasploit para la explotación de la vulnerabilidad CVE-2014-6287

Una vez inicializado Metasploit Framework, se procede a buscar los módulos disponibles relacionados con el servicio Rejetto HTTP File Server (HFS) utilizando el comando search rejetto.

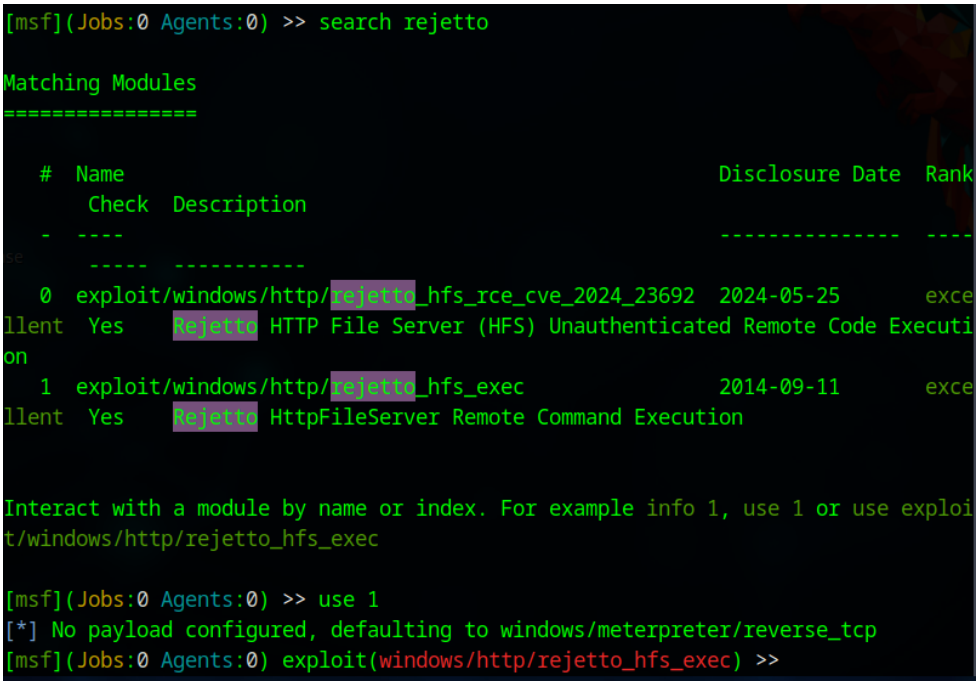
La búsqueda devuelve dos módulos principales: uno asociado a la vulnerabilidad reciente CVE-2024-23692 y otro correspondiente a la vulnerabilidad histórica CVE-2014-6287, la cual afecta directamente a las versiones 2.3.x del servicio HFS, coincidentes con la versión identificada previamente en el Host-A (192.168.18.29).

Para cumplir con los objetivos del ejercicio Red Team, se selecciona el módulo exploit/windows/http/rejetto_hfs_exec, que permite la ejecución remota de comandos (RCE) sobre el servidor vulnerable. Esto se realiza mediante la instrucción use 1, la cual carga el módulo correspondiente y prepara el entorno para continuar con la verificación y explotación controlada.

Este paso es fundamental, ya que confirma y habilita la interacción directa con el vector de entrada identificado en etapas previas. Como se ve en la siguiente figura.

Figura 13

Selección del módulo rejetto_hfs_exec en Metasploit para la explotación del servicio HFS 2.3 vulnerable.



Nota. Selección del módulo Metasploit asociado a la vulnerabilidad CVE-2014-6287 en HFS 2.3 mediante el comando search rejetto, seguida de la carga del módulo rejetto_hfs_exec mediante use 1. Captura de pantalla de elaboración propia (2025)

Revisión de parámetros del módulo rejetto_hfs_exec antes de la explotación

Una vez cargado el módulo rejetto_hfs_exec en Metasploit, se utiliza el comando show options para visualizar los parámetros de configuración requeridos antes de ejecutar la explotación.

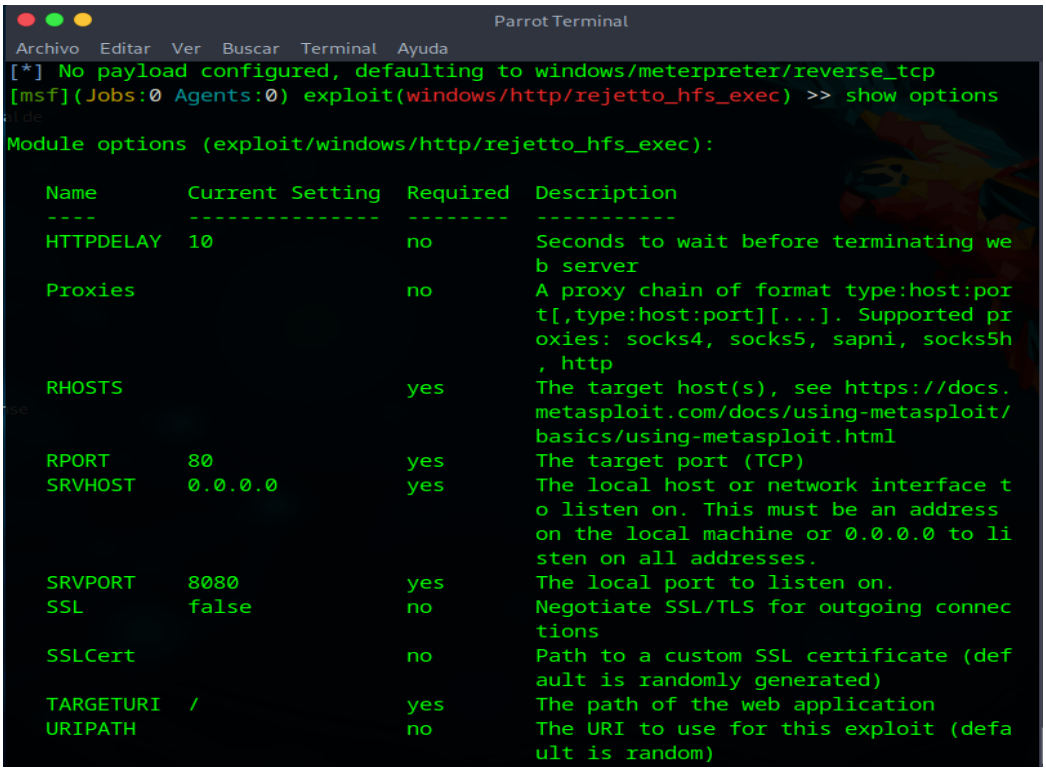
El módulo presenta valores por defecto tanto para el puerto objetivo (RPORT = 80) como para el puerto local asociado al servidor del payload (SRVPORT = 8080). Asimismo, aparece el campo RHOSTS, el cual debe configurarse explícitamente con la dirección IP del Host-A

vulnerable (192.168.18.29) para permitir la comunicación con el servicio HFS 2.3 previamente identificado.

Este paso es esencial, ya que garantiza que el módulo está correctamente parametrizado y que la explotación se dirigirá al objetivo adecuado. Además, permite verificar los parámetros adicionales como el uso de SSL, rutas de URI y opciones del servidor local, asegurando que la ejecución sea controlada y reproducible dentro del entorno de laboratorio.

Figura 14

Parámetros del módulo rejetto_hfs_exec mostrados mediante el comando show options en Metasploit.



Nota. Configuración predeterminada y parámetros requeridos del módulo exploit/windows/http/rejetto_hfs_exec en Metasploit, visualizados mediante el comando show options antes de establecer el objetivo de explotación. Captura de pantalla de elaboración propia (2025).

Configuración del objetivo y validación del servicio HFS 2.3 en Metasploit

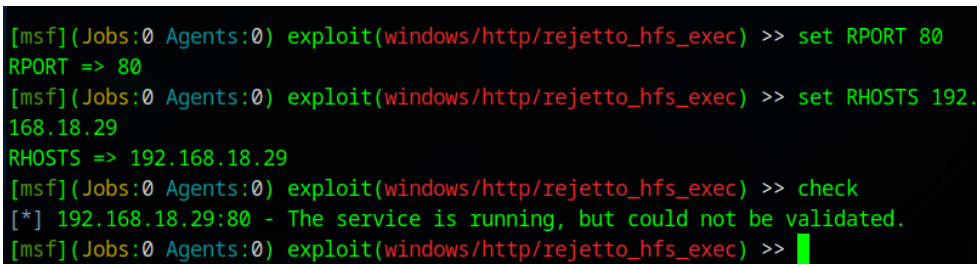
En este paso se establece la configuración necesaria para dirigir el módulo de explotación hacia el Host-A vulnerable. Mediante el comando set RPORT 80, se define el puerto donde se encuentra expuesto el servicio HFS 2.3, mientras que set RHOSTS 192.168.18.29 asigna explícitamente la dirección IP objetivo identificada durante la fase de reconocimiento.

Posteriormente, se ejecuta el comando check, el cual valida si el servicio objetivo responde. En este caso, Metasploit indica que el servicio está activo ("The service is running"), aunque no puede verificar automáticamente si es vulnerable. Esta limitación es normal en módulos antiguos, y la explotación continúa basándose en la evidencia previa obtenida mediante Nmap, Nikto y GoBuster, que confirmaron la presencia del servidor vulnerable Rejetto HFS 2.3 (Rapid7, s.f.).

Este procedimiento es fundamental para asegurar que la herramienta está apuntando correctamente al vector de ataque antes de proceder con la explotación. Como lo muestra en la figura a continuación

Figura 15

Configuración del puerto y dirección IP objetivo en Metasploit, seguida de validación del servicio mediante el comando check.



Nota. Validación del servicio HFS 2.3 mediante el comando check y configuración de los parámetros RPORT y RHOSTS en el módulo exploit/windows/http/rejetto_hfs_exec de Metasploit. Captura de pantalla de elaboración propia (2025).

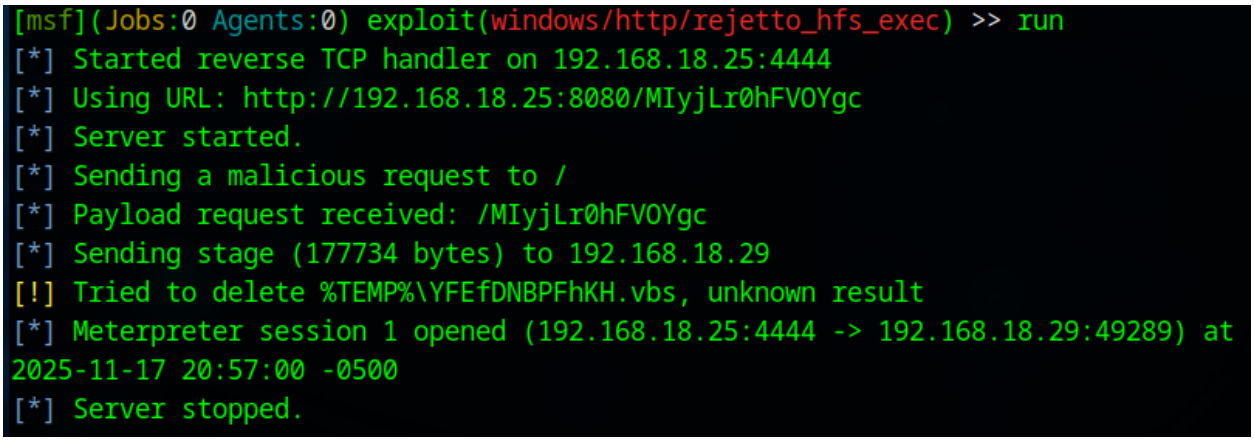
Explotación remota de Rejetto HFS 2.3 mediante Metasploit Framework

En este paso se llevó a cabo la explotación de la vulnerabilidad conocida como CVE-2014-6287, la cual afecta al servidor web Rejetto HTTP File Server (HFS) versión 2.3.x. Esta vulnerabilidad permite la ejecución remota de comandos (RCE) sin autenticación, ocasionada por un manejo inseguro de las plantillas (“template vulnerability”).

Se empleó el módulo exploit/windows/http/rejetto_hfs_exec del framework Metasploit, configurando adecuadamente los parámetros RHOSTS y RPORT, para posteriormente ejecutar la carga útil por defecto (windows/meterpreter/reverse_tcp). El servidor víctima respondió a la solicitud maliciosa y devolvió una sesión Meterpreter activa, lo que confirma el compromiso del Host-A. como se ve en la siguiente figura.

Figura 16

Ejecución del módulo rejetto_hfs_exec y apertura de la sesión Meterpreter en el Host-A



Nota. Explotación remota del servicio HFS 2.3 en el Host-A mediante Metasploit Framework, evidencia propia (2025).

Validación de acceso remoto y recopilación inicial de información del sistema comprometido, Verificación de interfaces de red en Host-A mediante shell desde Meterpreter

En esta etapa se ingresa desde la sesión Meterpreter a una shell del sistema operativo comprometido (Host-A) con el fin de verificar nuevamente las interfaces de red y confirmar su rol dentro del pivoting (Rapid7, s.f.). El comando ipconfig permite identificar que Host-A posee dos adaptadores activos:

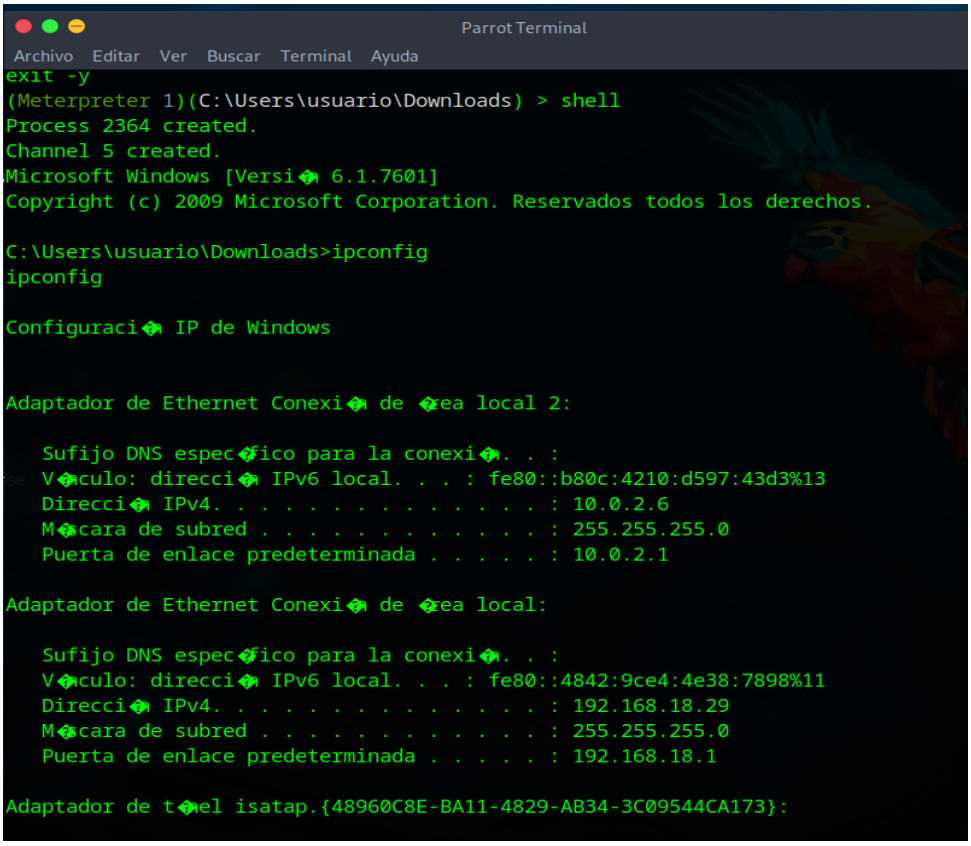
Uno perteneciente a la red 10.0.2.0/24 (donde se encuentra Host-B).

Otro perteneciente a la red 192.168.18.0/24, utilizada entre el atacante (Parrot OS) y Host-A.

Esta confirmación es fundamental para sustentar técnicamente que Host-A funciona como puente entre ambas redes, lo cual valida la pertinencia del pivoting y el movimiento lateral hacia Host-B.

Figura 17

Salida del comando ipconfig ejecutado desde la shell de Host-A



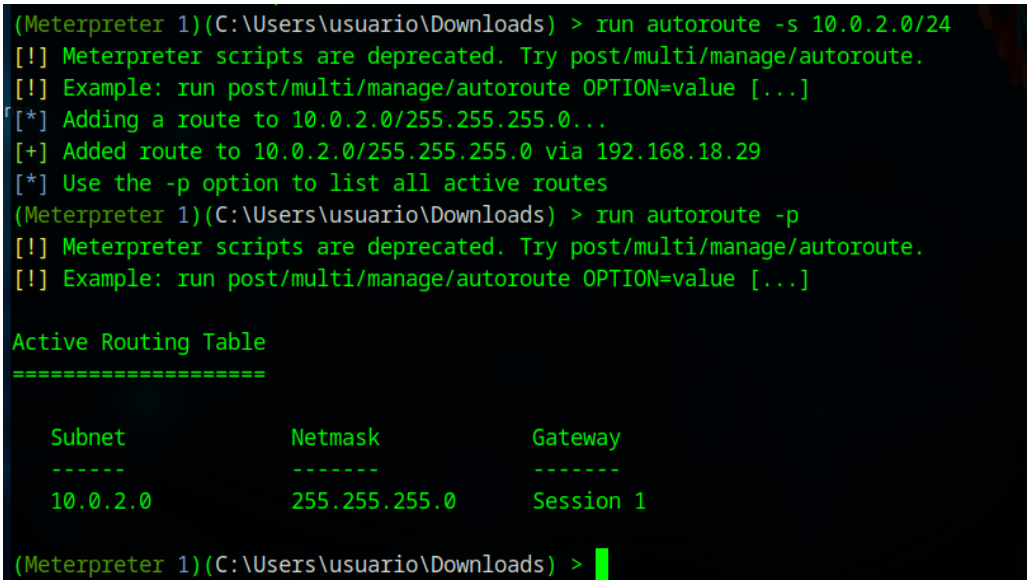
Nota. Visualización de las interfaces de red del Host-A mediante la ejecución del comando ipconfig desde la shell abierta a través de Meterpreter. Captura de pantalla propia (2025).

Configuración de ruta interna mediante autoroute en Meterpreter

Para permitir que la máquina comprometida Host-A funcione como punto de pivoting hacia la red interna donde se encuentra Host-B, se utilizó el módulo autoroute de Meterpreter (Rapid7, s.f.). Este proceso agrega una ruta persistente dentro del framework Metasploit, posibilitando que todo el tráfico dirigido a la subred interna 10.0.2.0/24 sea redirigido a través de la sesión activa. Esta acción es esencial para la fase de movimiento lateral exigida en el escenario del Anexo 4, dado que Host-A actúa como puente entre ambas redes.

Figura 18

Configuración exitosa de la ruta hacia la subred interna (10.0.2.0/24) utilizando autoroute en Meterpreter.



Nota. Salida del comando run autoroute -s 10.0.2.0/24 seguido de run autoroute -p, donde se verifica la incorporación de la ruta hacia la red interna a través de la sesión Meterpreter establecida en Host-A (fuente propia, 2025).

Escaneo ARP de la red interna 10.0.2.0/24 mediante pivoting desde la sesión Meterpreter

En este paso se procede a identificar los equipos activos dentro de la red interna descubierta desde el host comprometido (10.0.2.0/24).

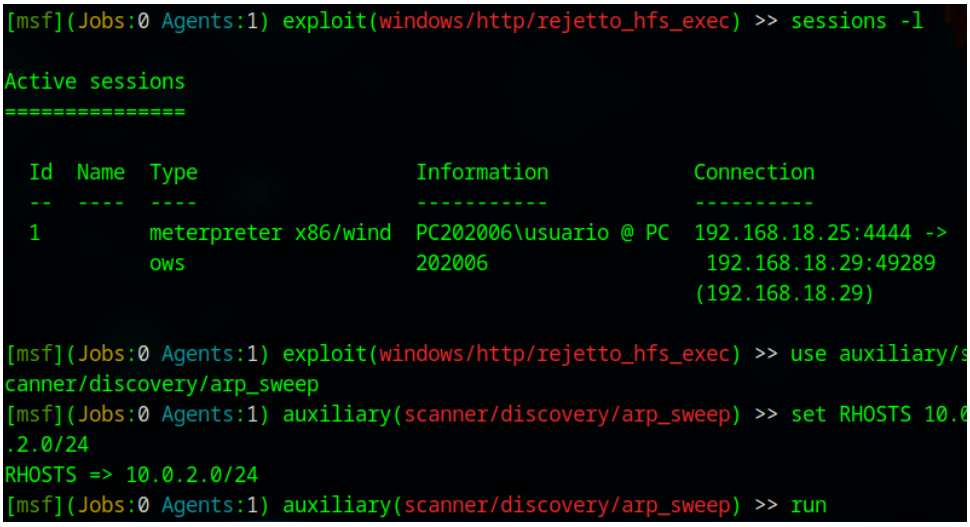
Para ello, se utiliza el módulo auxiliary/scanner/discovery/arp_sweep de Metasploit, el cual permite realizar un escaneo ARP a través de la sesión Meterpreter previamente establecida.

Este procedimiento es esencial en un entorno real, ya que el atacante normalmente no conoce la IP del Host-B, por lo que primero debe descubrir qué dispositivos están presentes en la red pivotada.

Una vez configurado el rango de direcciones (RHOSTS 10.0.2.0/24), el módulo detecta los hosts activos, lo que permite continuar con el reconocimiento y futuros escaneos de puertos sobre los sistemas encontrados.

Figura 19

Ejecución del módulo ARP Sweep para identificar dispositivos activos en la red interna 10.0.2.0/24.



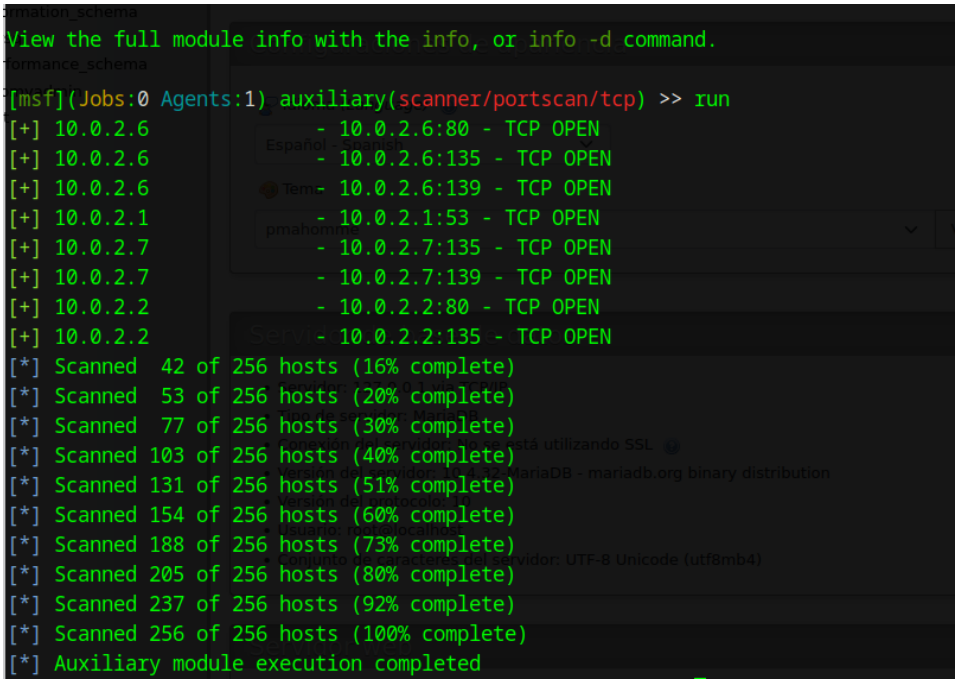
Nota. Escaneo ARP realizado desde Metasploit para descubrir hosts activos en la red interna 10.0.2.0/24 mediante pivoting desde la sesión Meterpreter. Fuente propia (2025).

Escaneo de puertos en la red interna 10.0.2.0/24 mediante pivoting desde Host-A comprometido

Tras establecer pivoting mediante Metasploit, se ejecutó un escaneo de puertos TCP sobre toda la red interna 10.0.2.0/24 utilizando el módulo auxiliary/scanner/portscan/tcp. Este análisis permitió identificar hosts activos y sus servicios accesibles a través del túnel pivotado, evidenciando la visibilidad de Host-B (10.0.2.7) desde la sesión comprometida en Host-A. El resultado confirma la correcta propagación del tráfico a través del canal lateral creado mediante autoroute. Como lo muestra en la siguiente figura.

Figura 20

Escaneo de puertos internos mediante Metasploit después de habilitar pivoting



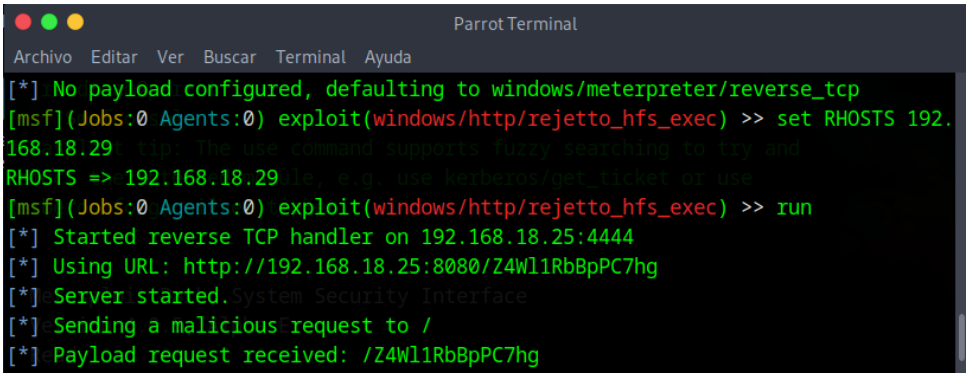
Nota. Los resultados muestran múltiples servicios abiertos en los hosts identificados (por ejemplo, 80/tcp, 135/tcp, 139/tcp en 10.0.2.6 y 10.0.2.7). Estos hallazgos verifican que el pivoting está funcionando correctamente, ya que la máquina atacante puede escanear redes a las que no tendría acceso directo sin la sesión comprometida en Host-A.

Ejecución del exploit Rejetto HFS para obtener acceso remoto

En este paso se ejecuta el módulo exploit/windows/http/rejetto_hfs_exec de Metasploit con el fin de comprometer el host objetivo que ejecuta Rejetto HFS 2.3. Al configurar la dirección RHOSTS y lanzar el ataque, Metasploit inicia un handler de reverse TCP, envía la solicitud maliciosa al servicio vulnerable y transfiere las etapas del payload Meterpreter. Como resultado, se logra la apertura de múltiples sesiones remotas desde la host víctima hacia el atacante, evidenciando un compromiso exitoso. Como se ve en la figura 25.

Figura 21

Ejecución del exploit Rejetto HFS 2.3 y apertura de sesiones Meterpreter



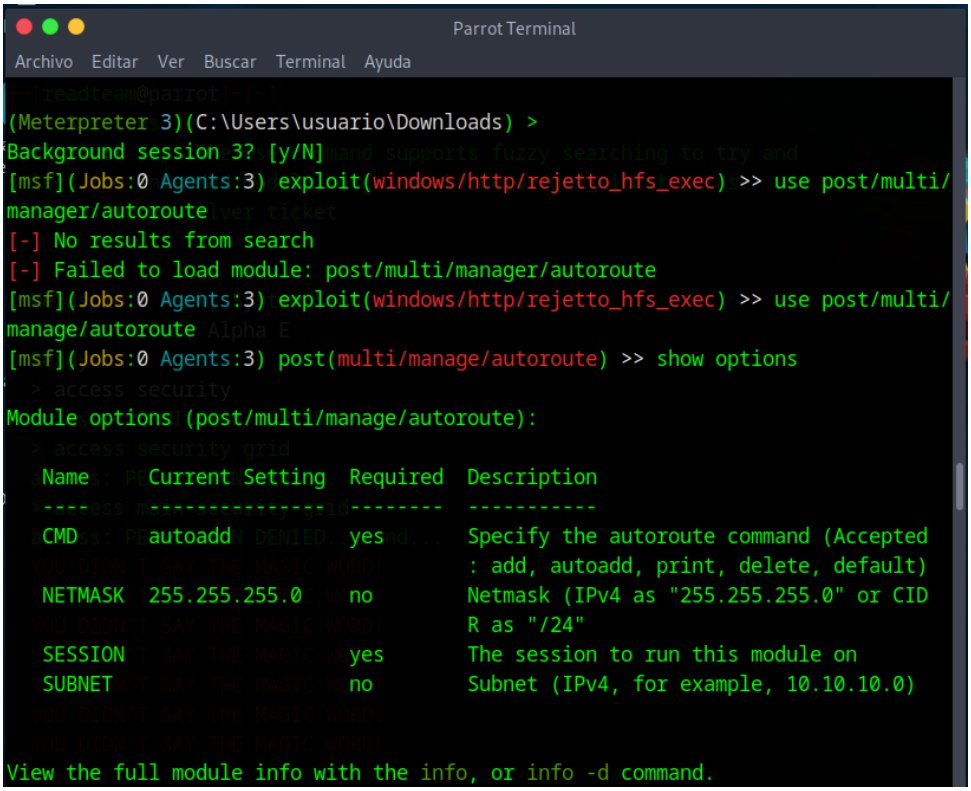
Nota. La figura muestra el proceso completo del ataque: inicialización del handler, envío de la solicitud maliciosa, transferencia del payload y apertura de tres sesiones Meterpreter desde el host comprometido (192.168.18.29) hacia el atacante (192.168.18.25). Fuente propia (2025).

Carga del módulo Autoroute para habilitar pivoting

En este paso se intenta cargar el módulo post/multi/manage/autoroute desde la sesión Meterpreter comprometida, con el propósito de añadir rutas internas y permitir el pivoting hacia otras subredes. Inicialmente, Metasploit genera errores al no encontrar o cargar el módulo; sin embargo, al especificarlo correctamente, se muestran las opciones disponibles, incluyendo el comando autoadd, la máscara de red y la sesión sobre la cual se ejecutará el módulo. Este procedimiento permite establecer rutas a través del host comprometido para continuar con el reconocimiento y movimiento lateral.

Figura 22

Ejecución y configuración del módulo Autoroute en Metasploit



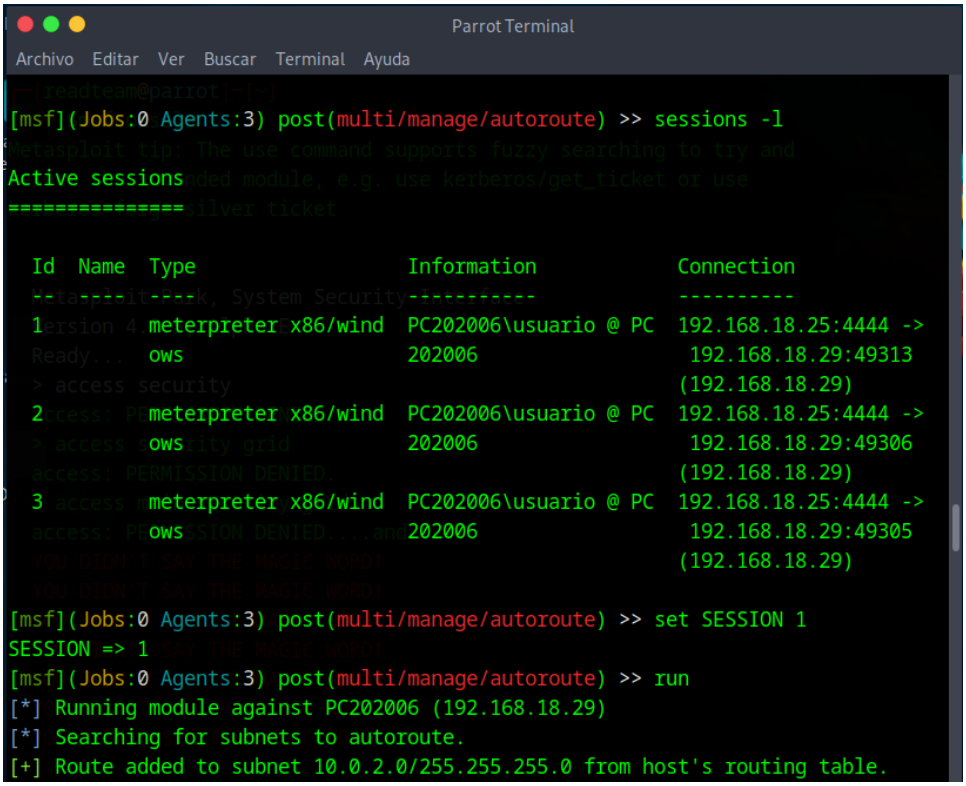
Nota. Proceso de carga del módulo post/multi/manage/autoroute, junto con los errores iniciales y la visualización de las opciones configurables. Este módulo es esencial para establecer rutas a través de la sesión comprometida y habilitar el pivoting hacia otras redes internas. Fuente propia (2025).

Selección de sesión activa y ejecución de Autoroute

En esta etapa se listan las sesiones Meterpreter activas obtenidas tras la explotación del servicio vulnerable. A continuación, se selecciona la sesión número 1 como la sesión objetivo para ejecutar el módulo autoroute. Luego, se ejecuta el módulo, el cual analiza las subredes disponibles desde el host comprometido y agrega una nueva ruta hacia la red interna 10.0.2.0/24. Con este proceso, se habilita la capacidad de pivoting, permitiendo que el atacante enrute tráfico hacia subredes internas previamente inaccesibles.

Figura 23

Ejecución de Autoroute en la sesión seleccionada y adición de rutas internas



Nota. Tres sesiones Meterpreter activas, la selección de la sesión 1 y la ejecución exitosa del módulo autoroute, que agrega una ruta hacia la subred 10.0.2.0/24 desde la tabla de enrutamiento del host comprometido. Fuente propia (2025).

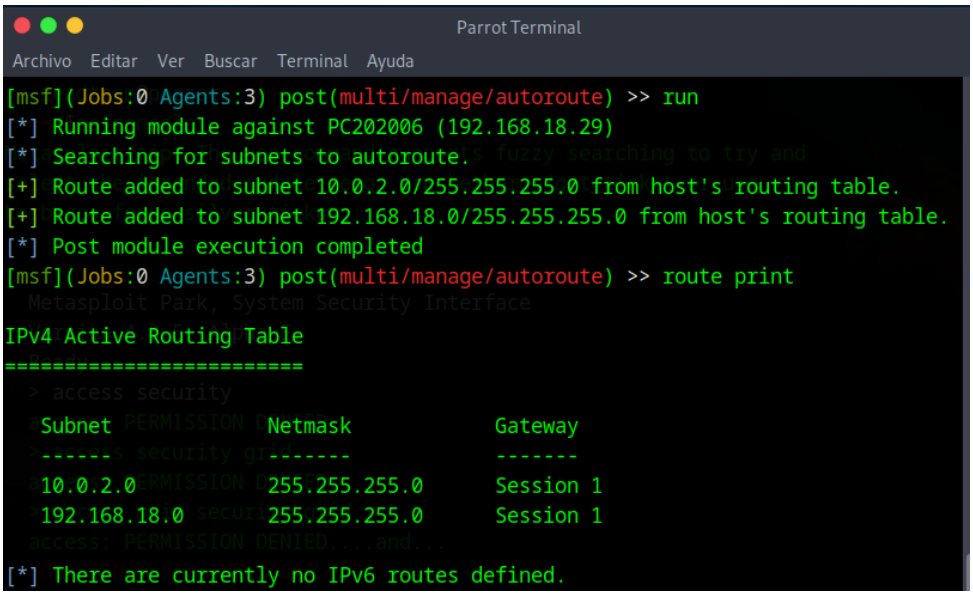
Verificación de rutas agregadas mediante Autoroute

Después de ejecutar el módulo autoroute, se validan las rutas añadidas consultando la tabla de enrutamiento activa en Metasploit mediante el comando route print. En este paso, se observa que el módulo ha identificado las subredes accesibles desde el host comprometido y ha agregado correctamente las rutas hacia 10.0.2.0/24 y 192.168.18.0/24, ambas utilizando la sesión 1 como gateway. Esta verificación confirma que el pivoting está habilitado y que es posible

dirigir tráfico hacia redes internas a través del sistema comprometido. Como lo muestra la figura 28.

Figura 24

Rutas agregadas automáticamente al ejecutar Autoroute y verificación mediante route print



Nota. La ejecución del módulo autoroute, la incorporación de dos subredes detectadas en la tabla de enrutamiento del host víctima y la impresión de la tabla de rutas IPv4, donde ambas redes aparecen asociadas a la sesión 1. Fuente propia (2025).

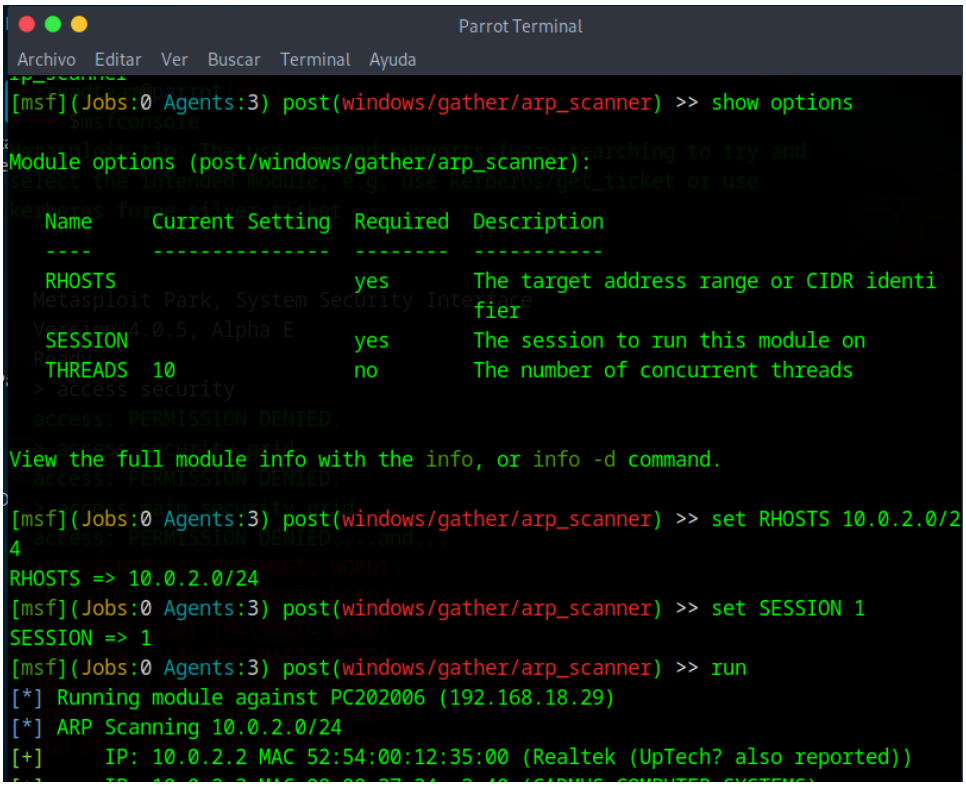
Escaneo de la subred descubierta mediante el módulo ARP Scanner

Tras haber configurado correctamente las rutas internas mediante autoroute, en este paso se utiliza el módulo post/windows/gather/arp_scanner para identificar dispositivos activos dentro de la subred 10.0.2.0/24. Primero se revisan las opciones del módulo, donde se especifican los parámetros obligatorios: el rango de direcciones objetivo (RHOSTS) y la sesión a utilizar (SESSION). Luego se establecen estos valores, seleccionando la red descubierta y la sesión 1 como punto de pivoting. Al ejecutar el módulo, Metasploit realiza el escaneo ARP desde el host

comprometido, identificando los equipos disponibles en la red interna, incluyendo direcciones IP y direcciones MAC.

Figura 25

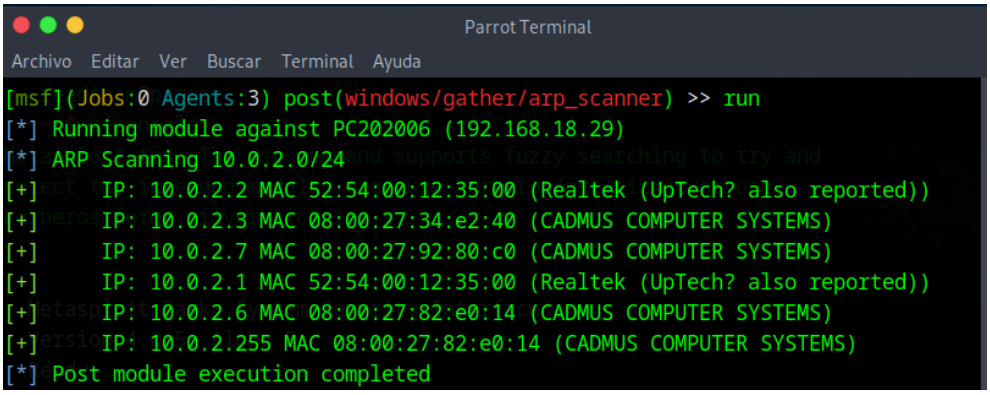
Configuración y ejecución del módulo ARP Scanner para identificar hosts en la red 10.0.2.0/24



Nota. Configuración del módulo arp_scanner, el establecimiento de la subred objetivo y la ejecución exitosa del escaneo, donde se detecta un host activo con dirección IP 10.0.2.2 y dirección MAC 52:54:00:12:35:00. Fuente propia (2025).

Figura 26

Resultados del módulo ARP Scanner mostrando hosts activos en la subred interna



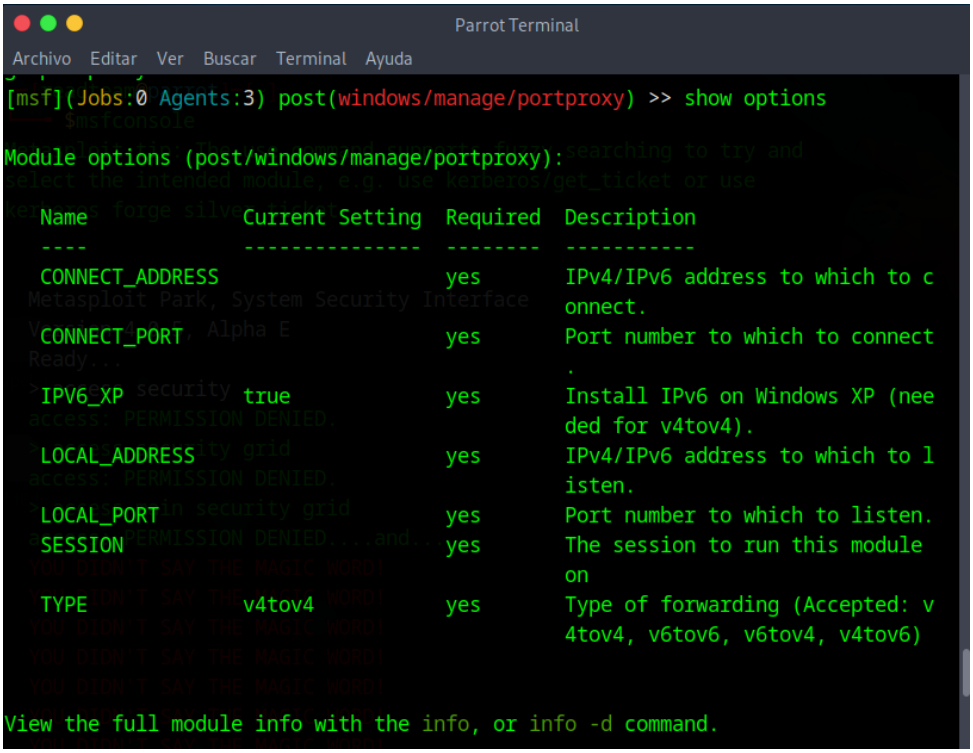
Nota. Muestra múltiples direcciones IP activas en la subred 10.0.2.0/24, junto con sus direcciones MAC, incluyendo dispositivos identificados como Realtek y CADMUS COMPUTER SYSTEMS. La ejecución finaliza exitosamente, confirmando la detección de varios hosts internos. Fuente propia (2025).

Revisión de opciones del módulo PortProxy para establecer reenvío de puertos

En este paso se inspeccionan las opciones del módulo post/windows/manage/portproxy, utilizado para configurar reglas de reenvío de puertos (port forwarding) en el host Windows comprometido. Este módulo permite crear túneles entre una dirección local y una dirección remota, lo cual es fundamental para acceder a servicios internos que no están expuestos directamente a la red del atacante. Dentro de las opciones del módulo se definen parámetros clave como la dirección y puerto de conexión (CONNECT_ADDRESS y CONNECT_PORT), la dirección y puerto local donde se escuchará el tráfico (LOCAL_ADDRESS y LOCAL_PORT), así como el tipo de redirección (TYPE) y la sesión Meterpreter donde se ejecutará la configuración.

Figura 27

Opciones del módulo PortProxy para la configuración de reenvío de puertos



Nota. Las opciones disponibles del módulo post/windows/manage/portproxy, incluyendo los parámetros necesarios para establecer un túnel entre direcciones IPv4/IPv6 locales y remotas. Esta configuración permite al atacante redirigir tráfico hacia servicios internos de la red comprometida mediante pivoting. Fuente propia (2025).

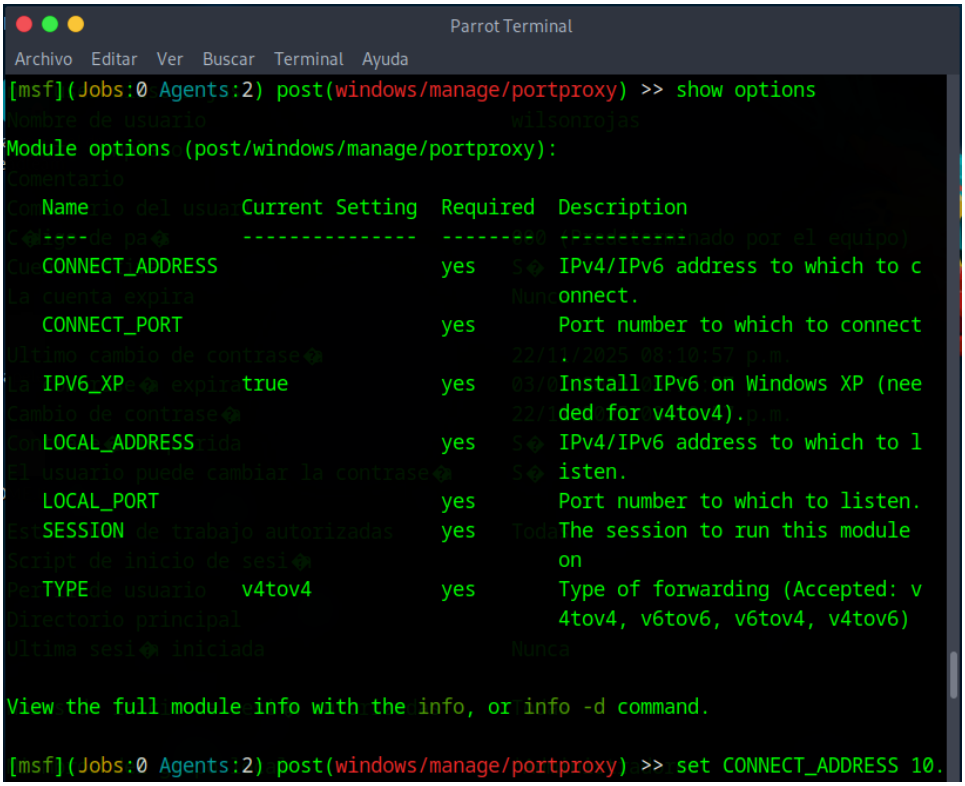
Configuración inicial del módulo PortProxy para establecer un túnel interno

En este paso como muestra la figura 32 se visualizan nuevamente las opciones del módulo post/windows/manage/portproxy con el objetivo de preparar el reenvío de puertos entre el host comprometido y un servicio interno de la red. El módulo permite definir la dirección remota a la cual conectar (CONNECT_ADDRESS), el puerto destino (CONNECT_PORT), así como la dirección y puerto locales que actuarán como punto de escucha (LOCAL_ADDRESS y

LOCAL_PORT). También se especifica el tipo de conversión de tráfico (TYPE), en este caso de IPv4 a IPv4, y la sesión Meterpreter que ejecutará la acción. Esta configuración es esencial para acceder a servicios internos sin exponerlos directamente.

Figura 28

Opciones del módulo PortProxy previo a la configuración del túnel interno



Nota. Parámetros requeridos por el módulo portproxy, incluyendo las direcciones locales y remotas, los puertos involucrados, el tipo de reenvío y la sesión activa. Esta etapa prepara el entorno para establecer un túnel hacia un servicio interno descubierto durante el reconocimiento de la red comprometida. Fuente propia (2025).

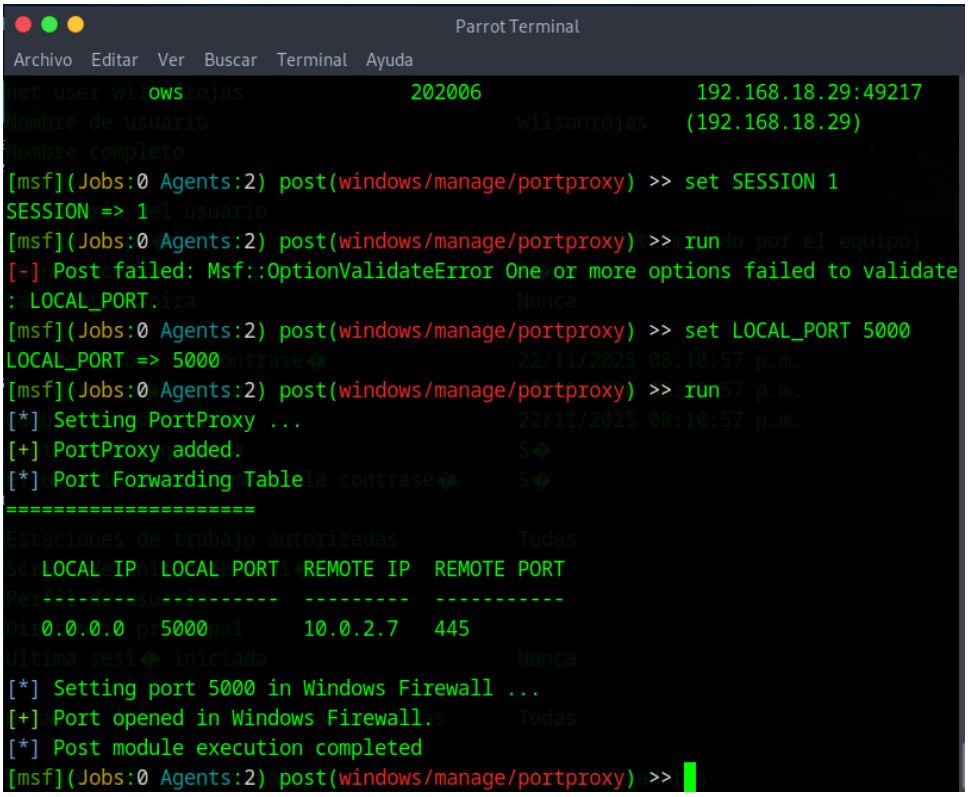
Configuración del túnel PortProxy hacia el servicio SMB del host interno

A continuación, como se muestra en la figura 33 se procede a configurar los parámetros necesarios del módulo post/windows/manage/portproxy para redirigir tráfico hacia el servicio

SMB (puerto 445) del host identificado previamente en la red interna (10.0.2.7). Para ello, se establece la dirección remota objetivo (CONNECT_ADDRESS), se define el puerto del servicio al cual se quiere acceder (CONNECT_PORT), y finalmente se configura la dirección local (LOCAL_ADDRESS) desde donde el atacante escuchará la conexión. Tras definir estos valores, se listan nuevamente las sesiones Meterpreter activas para seleccionar la adecuada y así aplicar la regla de reenvío. Esta configuración permitirá acceder al servicio SMB del host interno a través del pivoting, incluso cuando dicho servicio no es accesible desde la red del atacante.

Figura 29

Parámetros configurados en PortProxy para redirigir tráfico al puerto 445 del host interno



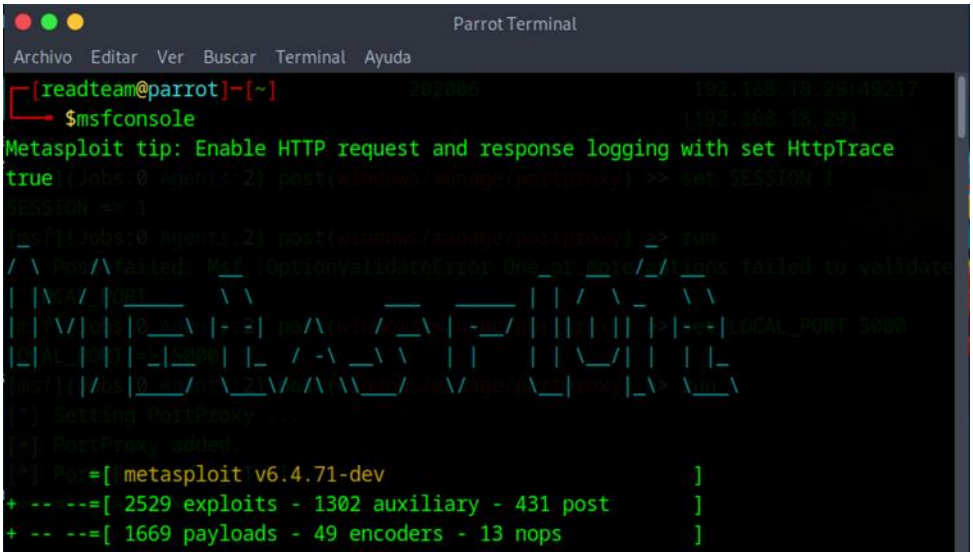
Nota. Asignación del host interno 10.0.2.7 como destino del túnel, el puerto 445 como servicio objetivo, y la dirección local 0.0.0.0 como punto de escucha. También se listan las sesiones activas que pueden ser utilizadas para ejecutar la regla de redirección. Fuente propia (2025).

Reinicio de Metasploit desde un nuevo terminal para continuar con la explotación

En la figura 34 se puede observar que se abre un nuevo terminal dentro de la misma máquina Parrot para reiniciar Metasploit Framework mediante el comando msfconsole (Rapid7, s.f.). Este procedimiento permite continuar con la explotación sin interferir con la consola previa donde se estableció el túnel PortProxy y las sesiones Meterpreter. Una vez cargado Metasploit, se verifica la versión activa del framework y se confirma que el entorno está listo para ejecutar nuevos módulos. Finalmente, se realiza una búsqueda del exploit relacionado con EternalBlue, lo que prepara el entorno para evaluar si el host interno identificado previamente mediante ARP Scanner y pivoting es vulnerable a esta técnica de explotación.

Figura 30

Inicio de Metasploit en un nuevo terminal y búsqueda del exploit EternalBlue



Nota. La ejecución de msfconsole en una sesión separada dentro de la misma máquina Parrot OS, la carga

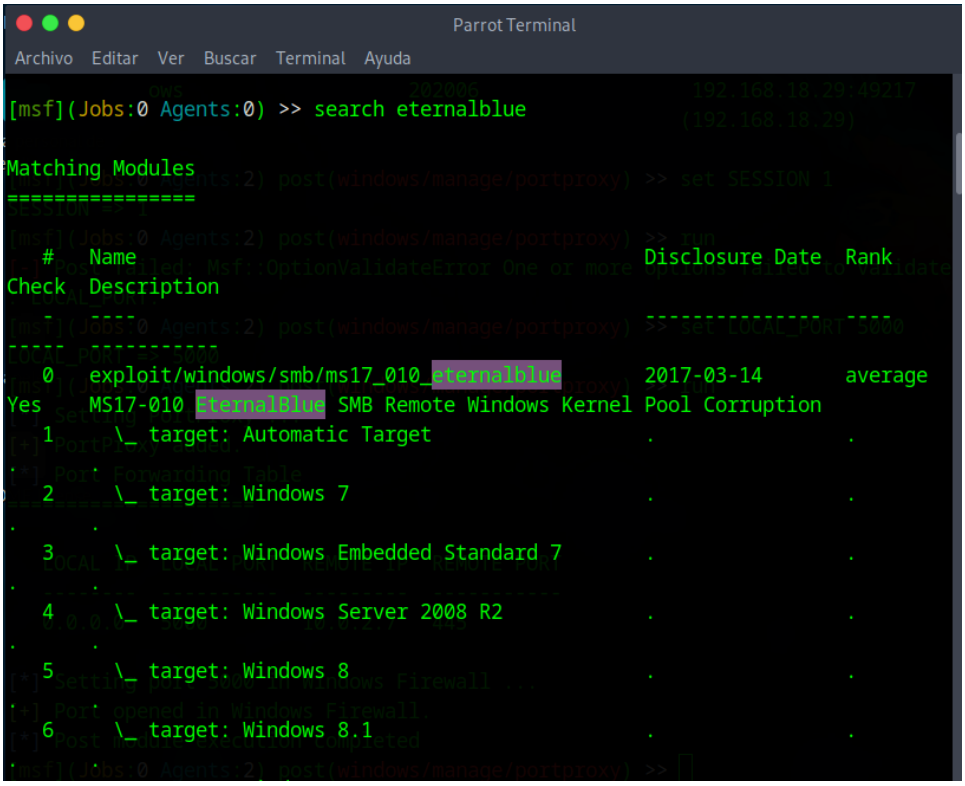
del framework Metasploit 6.4.71-dev y la búsqueda del módulo “eternalblue”. Esto permite trabajar en paralelo mientras se mantienen activos el pivoting y las sesiones previamente configuradas. Fuente propia (2025).

Identificación del exploit EternalBlue compatible con el entorno destino

Después de iniciar Metasploit en un nuevo terminal, se procede a buscar el exploit correspondiente a la vulnerabilidad MS17-010, conocida como EternalBlue. Al ejecutar el comando search eternalblue, el framework devuelve los módulos disponibles relacionados con esta vulnerabilidad crítica que afecta múltiples versiones de Windows. El resultado muestra el exploit exploit/windows/smb/ms17_010_eternalblue, junto con sus objetivos soportados, como Windows 7, Windows 8, Windows Server 2008 R2, entre otros. Esta búsqueda permite verificar si el host descubierto durante el pivoting coincide con alguno de los sistemas vulnerables enumerados (Microsoft, 2017).

Figura 31

Listado del exploit MS17-010 EternalBlue y sistemas compatibles



Nota. Módulo exploit/windows/smb/ms17_010_eternalblue, su descripción, la fecha de divulgación (14 de marzo de 2017) y los sistemas operativos objetivo compatibles. Esta información es crucial para determinar si el host interno identificado previamente puede ser explotado mediante EternalBlue.. Fuente propia (2025).

Configuración y ejecución del exploit EternalBlue mediante pivoting

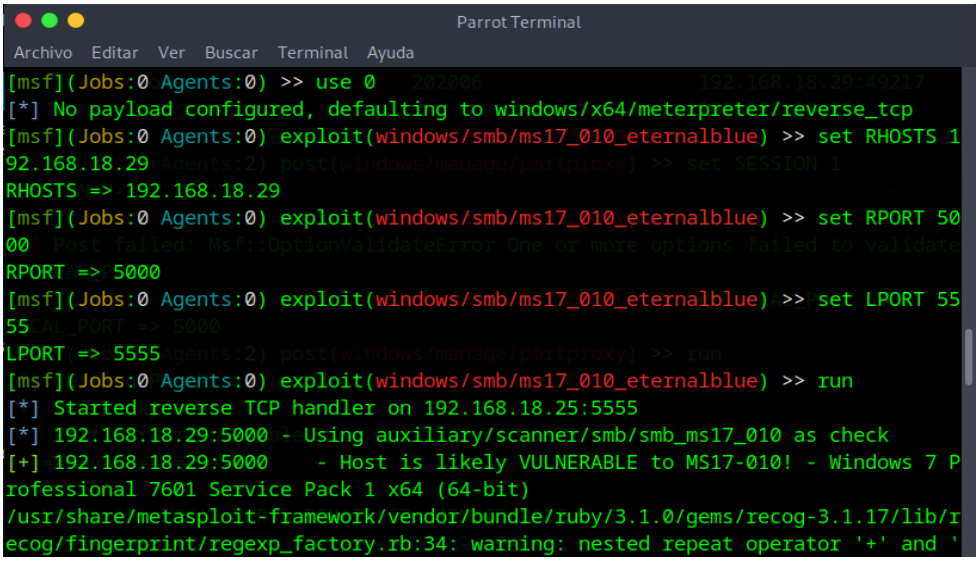
En la figura 36 a continuación se carga el módulo exploit/windows/smb/ms17_010_eternalblue y se configuran los parámetros necesarios para dirigirse al host interno comprometido a través del túnel PortProxy previamente configurado.

Se define la dirección del objetivo (RHOSTS), el puerto remoto expuesto a través del túnel (RPORT 5000), así como el puerto local para recibir la sesión Meterpreter (LPORT 5555).

Luego se ejecuta el módulo, que automáticamente utiliza el verificador smb_ms17_010 para determinar si el sistema es vulnerable. El resultado confirma que el host ejecuta Windows 7 Professional Service Pack 1 x64 y es vulnerable a MS17-010, permitiendo proceder con la explotación del desbordamiento de memoria del kernel SMB (Microsoft, 2017).

Figura 32

Ejecución del exploit EternalBlue y validación de vulnerabilidad del host interno



Nota. Proceso de configuración del módulo EternalBlue, la validación automática de vulnerabilidad y la confirmación de un objetivo vulnerable. Se observa que el host responde como Windows 7 SP1 x64, lo cual coincide con los sistemas afectados por MS17-010.Fuente propia (2025).

Obtención de acceso remoto mediante Meterpreter tras la explotación de EternalBlue

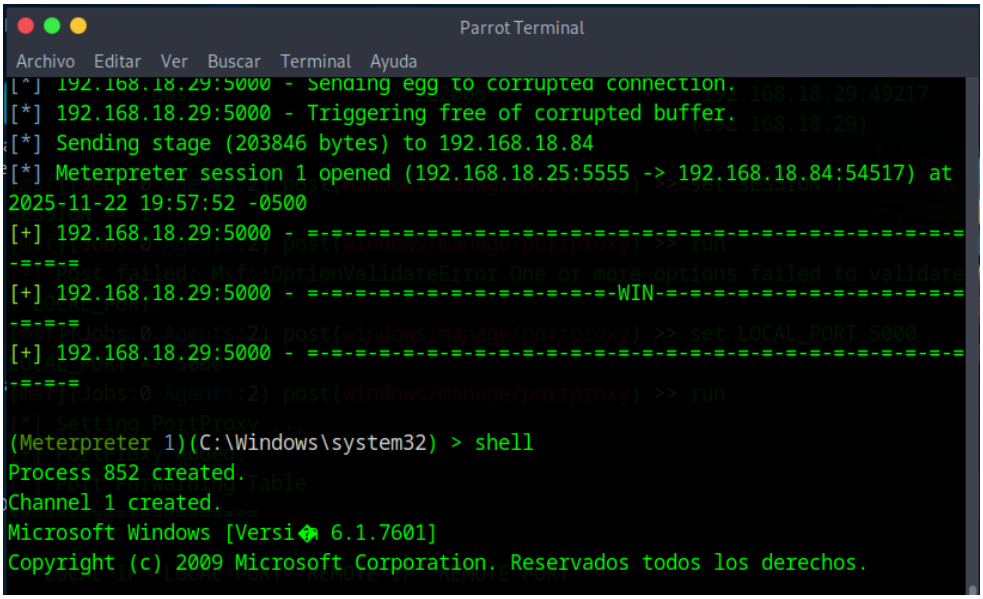
Luego de ejecutar con éxito el exploit MS17-010 EternalBlue a través del túnel establecido por PortProxy, Metasploit envía la etapa final del payload y establece una nueva sesión Meterpreter con el host interno vulnerable.

El exploit completa el proceso de corrupción del buffer SMB, envía la carga útil y, finalmente, abre una sesión Meterpreter procedente del host víctima.

A partir de esta sesión, se utiliza el comando shell para crear un proceso remoto y obtener un intérprete de comandos de Windows directamente en el sistema comprometido, confirmando así el control total sobre la máquina interna. cómo se puede ver en la figura 37 a continuación.

Figura 33

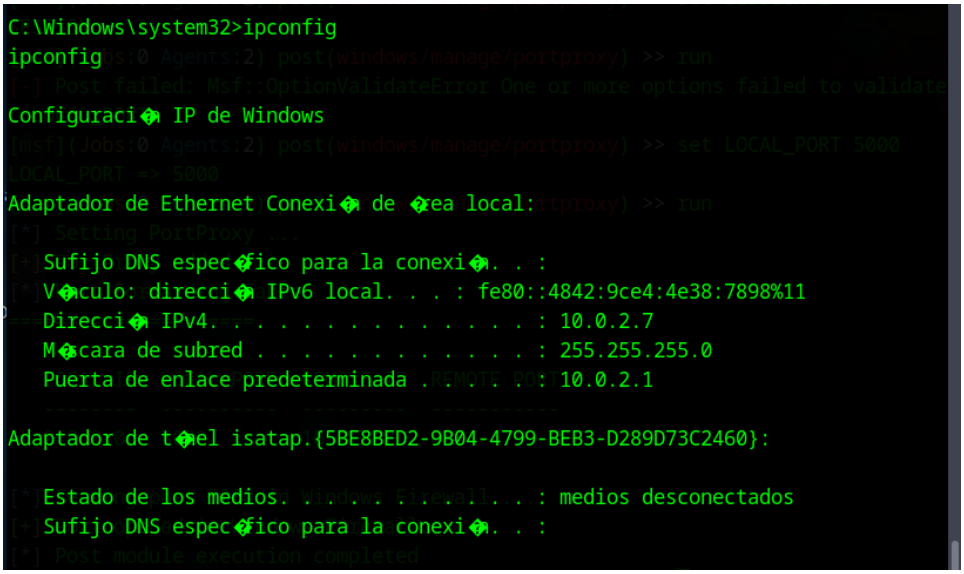
Apertura de sesión Meterpreter y obtención de shell del sistema tras explotar EternalBlue


Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[*] 192.168.18.29:5000 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.18.84
[*] Meterpreter session 1 opened (192.168.18.25:5555 -> 192.168.18.84:54517) at 2025-11-22 19:57:52 -0500
[+] 192.168.18.29:5000 - =-=-=-=

Los datos revelan su dirección IPv4, la máscara de subred y su puerta de enlace predeterminada dentro del entorno de red interna comprometida. Esta información permite comprender la topología donde se está operando, así como validar la comunicación efectiva a través del pivoting establecido. Como lo muestra la figura 38.

Figura 34

Configuración IP del host interno 10.0.2.7 obtenida mediante ipconfig



Nota. Muestra que el equipo comprometido posee dirección IPv4 10.0.2.7, máscara 255.255.255.0 y puerta de enlace 10.0.2.1, lo cual coincide con la estructura de red identificada previamente mediante autoroute y arp_scanner, confirmando que se ha tomado control del host correcto. Fuente propia (2025).

Creación del usuario “wilsonrojas” y asignación a administradores desde la sesión comprometida

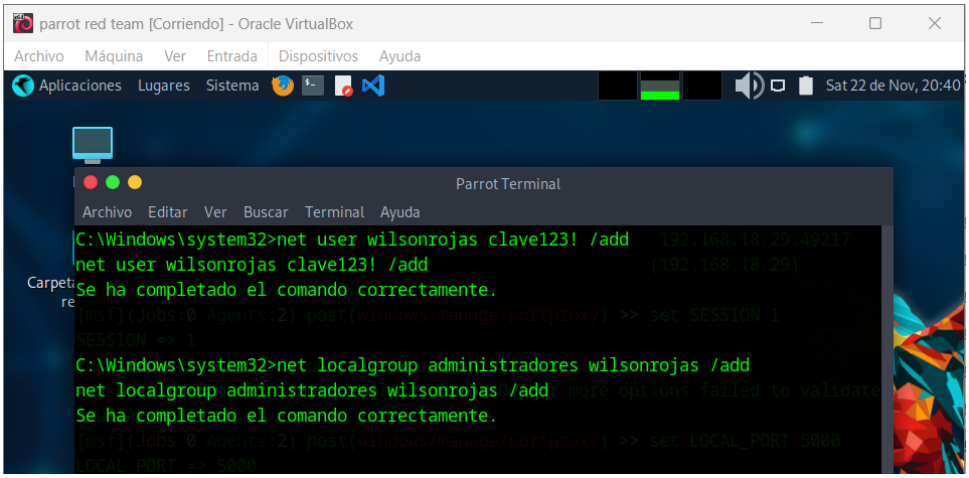
En la figura 39 se muestra ya dentro de la sesión interactiva del host interno comprometido mediante Meterpreter, se ejecutan comandos de Windows para crear un nuevo usuario local con privilegios elevados, siguiendo el objetivo controlado del ejercicio Red Team.

¡Primero se crea la cuenta wilsonrojas con la contraseña “clave123!”. Luego, se añade esta cuenta al grupo de Administradores, otorgándole permisos totales en el sistema.

Este procedimiento demuestra la capacidad del atacante para modificar la configuración del sistema víctima después del movimiento lateral exitoso.

Figura 35

Creación y elevación del usuario “wilsonrojas” en el host comprometido



Nota. Ejecución de los comandos net user wilsonrojas clave123! /add y net localgroup administradores wilsonrojas /add, confirmando que la cuenta fue creada y promovida correctamente a administrador. Fuente propia (2025).

Verificación de cuentas locales en Host-B tras el movimiento lateral

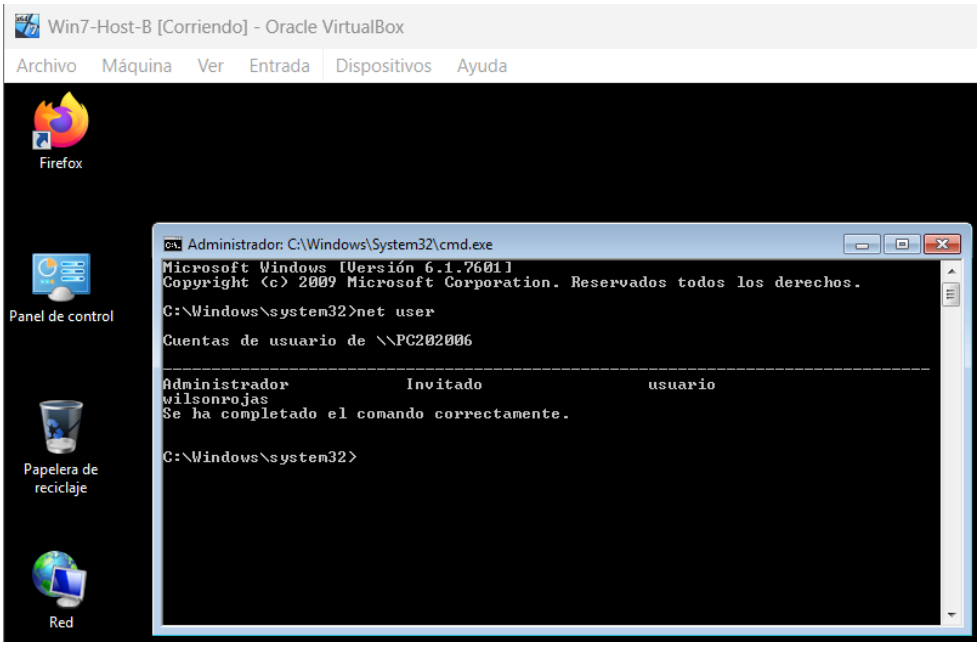
Posteriormente, desde la consola del propio Host-B en VirtualBox, se ejecuta el comando net user para comprobar que la cuenta creada desde el ataque realmente existe en el sistema.

La salida confirma que wilsonrojas aparece dentro de la lista de usuarios locales junto a las cuentas predeterminadas de Windows.

Esta validación directa desde Host-B prueba que la explotación, el pivoting y la modificación del sistema objetivo se llevaron a cabo de forma exitosa. Como se muestra en la siguiente figura 40.

Figura 36

Comprobación de la existencia de la cuenta "wilsonrojas" en Host-B



Nota. La ejecución de net user dentro de Host-B, donde aparece la cuenta "wilsonrojas" creada durante la fase de explotación y movimiento lateral. Esto confirma el acceso real y persistente en el sistema comprometido. Fuente propia (2025).

Confirmación gráfica de la creación del usuario mediante la consola de administración local (lusrmgr.msc)

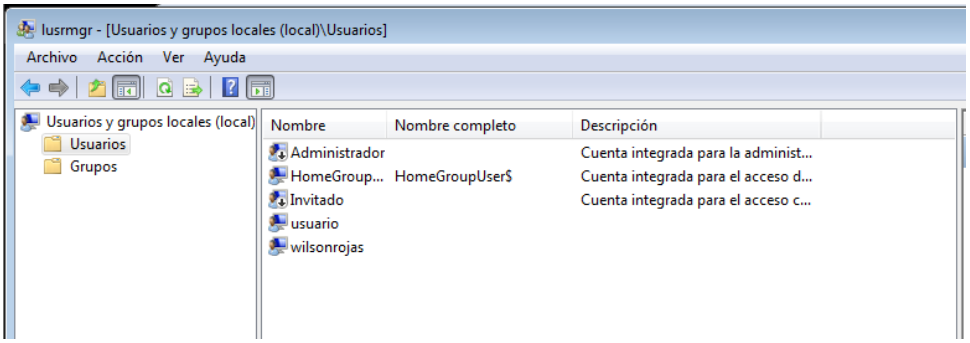
Después de crear la cuenta wilsonrojas desde la sesión remota y verificarla en consola mediante net user, se procede a validar visualmente su existencia desde la herramienta gráfica de administración local de Windows (lusrmgr.msc).

Este paso permite comprobar, con una interfaz gráfica nativa de Windows 7, que la cuenta ha sido efectivamente añadida al sistema y aparece dentro del contenedor Usuarios junto a las cuentas integradas del sistema.

Esta validación complementa la verificación en línea de comandos y demuestra de manera irrefutable que el atacante posee la capacidad de crear cuentas locales persistentes en el host interno comprometido.

Figura 37

Visualización de la cuenta "wilsonrojas" en la consola gráfica de administración de usuarios locales (lusrmgr.msc)



Nota. La consola Usuarios y grupos locales del sistema Host-B, donde se aprecia la cuenta "wilsonrojas" junto a las cuentas predeterminadas (Administrador, Invitado, usuario). Esto confirma la persistencia de la cuenta creada mediante el ataque y su integración en la estructura de usuarios locales del sistema. Fuente propia (2025).

Eliminación de la cuenta creada durante el ejercicio Red Team

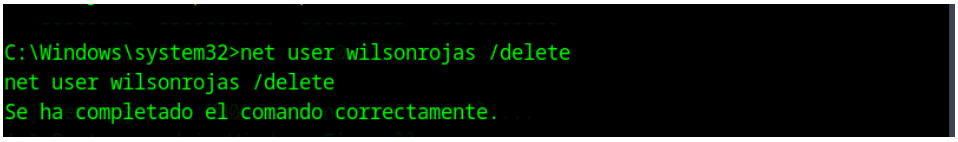
Como parte del cierre controlado del laboratorio, se procede a eliminar la cuenta wilsonrojas que fue creada durante el movimiento lateral en el Host-B.

Desde la consola del sistema comprometido, se ejecuta el comando net user wilsonrojas /delete, lo que remueve la cuenta local y revierte el cambio realizado previamente.

Esta acción forma parte de las buenas prácticas de los ejercicios Red Team controlados, asegurando que no queden cuentas persistentes o artefactos que puedan alterar el entorno original. Como lo muestra la figura 42 a continuación.

Figura 38

Eliminación de la cuenta local "wilsonrojas" mediante línea de comandos en Host-B



Nota. La ejecución exitosa del comando net user wilsonrojas /delete, con el mensaje "Se ha completado el comando correctamente.", confirmando que la cuenta creada para el ejercicio ha sido eliminada del sistema. Fuente propia (2025).

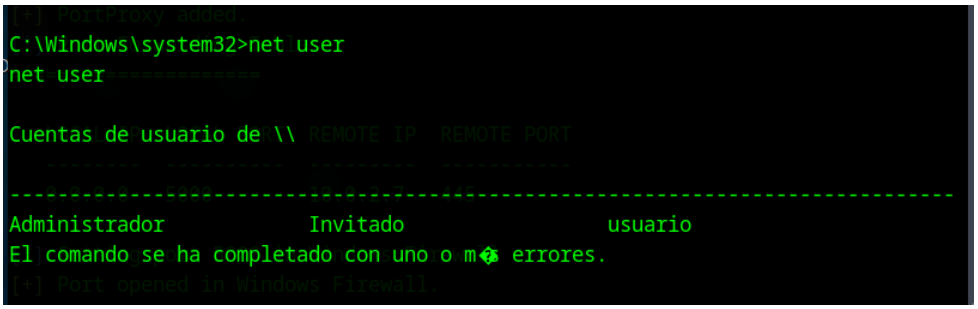
Verificación final de la eliminación de la cuenta en el sistema comprometido

Después de ejecutar la eliminación de la cuenta wilsonrojas, se realiza una verificación final utilizando el comando net user desde la consola del Host-B comprometido.

En esta salida se observa que únicamente permanecen las cuentas predeterminadas del sistema: Administrador, Invitado y usuario, lo que confirma que la cuenta creada durante el ejercicio Red Team ha sido eliminada exitosamente.

Figura 39

Verificación de cuentas locales tras la eliminación de "wilsonrojas"



Nota. La cuenta "wilsonrojas" ya no aparece en la lista de cuentas locales, confirmando su eliminación. El mensaje de advertencia mostrado no invalida el resultado principal del comando. Fuente propia (2025).

Análisis del Ataque por Máquina

Host-A: Vector de Entrada

Host-A fue comprometido debido a la presencia del servicio vulnerable Rejetto HFS 2.3 (CVE-2014-6287), que permite ejecución remota de código sin autenticación. El reconocimiento inicial (Nmap, curl, nikto) evidenció la exposición del puerto 80/tcp, confirmando la versión vulnerable.

El uso del módulo rejetto_hfs_exec de Metasploit permitió obtener una sesión Meterpreter y realizar post-explotación básica: revisión de interfaces, procesos y subredes internas. Este análisis reveló una ruta hacia la red 10.0.2.0/24, lo cual convirtió a Host-A en un punto estratégico para establecer pivoting y acceder a otros activos internos.

Conclusión sintetizada: Host-A actuó como el punto de compromiso inicial por falta de parches, exposición innecesaria de servicios y ausencia de controles perimetrales.

Host-B: Movimiento Lateral

Una vez comprometido Host-A, se identificó Host-B (10.0.2.7) mediante escaneo interno. La exposición de SMB y RPC (135/139/445) permitió inferir que el sistema era vulnerable a métodos estándar de ejecución remota.

El movimiento lateral se realizó con PsExec, aprovechando credenciales válidas, lo cual confirma dos fallas claves:

Reutilización de credenciales

Segmentación interna deficiente

Con el acceso obtenido, el atacante pudo manipular el sistema, demostrando capacidad de impacto sin explotar vulnerabilidades adicionales.

Conclusión sintetizada: Host-B fue comprometido debido a configuraciones inseguras y administración débil de credenciales.

Relación Host-A & Host-B

El compromiso de Host-B solo fue posible gracias al control previo de Host-A. La ausencia de segmentación, monitoreo y restricciones inter-VLAN facilitó el movimiento lateral sin ser detectado.

Conclusión sintetizada: La red presenta una falla estructural: una única vulnerabilidad perimetral comprometió dos máquinas internas, demostrando un riesgo grave de escalamiento lateral.

Herramientas Utilizadas

Las herramientas se agrupan según las fases del pentesting.

Reconocimiento Externo

Nmap: identificación de hosts y puertos expuestos.

Curl / Nikto: validación del servicio HFS 2.3.

Gobuster: enumeración de rutas internas del servidor web.

Enumeración y Análisis de Vulnerabilidades

Searchsploit: confirmación del exploit CVE-2014-6287.

Metasploit (auxiliares): escaneo SMB, ARP y configuración del servidor SOCKS.

Explotación

Módulo rejetto_hfs_exec para Host-A.

PsExec para movimiento lateral en Host-B.

Post-Explotación

Meterpreter: inventario del sistema, obtención de rutas y análisis del entorno.

Autoroute: inclusión de rutas internas para habilitar el pivoting.

Pivoting y Movimiento Lateral

ProxyChains + Servidor SOCKS: enrutamiento del tráfico hacia 10.0.2.0/24.

PortProxy: túnel SMB para acceso remoto a Host-B.

Persistencia

PsExec y cmd.exe: creación y eliminación controlada de un usuario temporal.

lusrmgr.msc: verificación visual en Host-B.

Validación y Evidencia

Visor de Eventos de Windows: confirmación de creación/eliminación de cuentas y accesos del atacante.

Recomendaciones Técnicas

Host-A

Eliminar o actualizar HFS 2.3.

Restringir puertos públicos mediante firewall.

Aplicar hardening del sistema operativo.

Implementar IDS/IPS para detectar patrones de explotación.

Monitorear actividad anómala en el servicio web.

Host-B

Restringir SMB solo a administradores autorizados.

Implementar segmentación fina.

Prohibir la reutilización de credenciales.

Activar auditoría de ejecuciones remotas.

MFA para cuentas administrativas.

Infraestructura Global

Implementar Zero Trust.

Utilizar SIEM para correlación de eventos.

Realizar escaneos continuos de vulnerabilidades.

Aplicar gestión centralizada de parches.

Capacitar al personal en detección y respuesta a incidentes.

Conclusiones parciales de la etapa 3

La realización de este ejercicio permitió observar, dentro de un laboratorio controlado, toda la cadena de explotación correspondiente a un escenario realista que abarca el acceso inicial, el reconocimiento interno, las técnicas de pivoting y el movimiento lateral dentro de una red empresarial. A partir de la vulnerabilidad CVE-2014-6287 presente en Rejetto HFS 2.3, fue posible obtener acceso remoto al Host-A mediante la ejecución de un payload Meterpreter, demostrando cómo un servicio expuesto y desactualizado puede convertirse en un punto de entrada crítico para un actor malicioso.

Tras establecer la sesión en Host-A, se aplicaron técnicas de pivoting para alcanzar la red 10.0.2.0/24, lo que permitió evidenciar la importancia de segmentar adecuadamente las redes internas y restringir la visibilidad de equipos sensibles. El uso del módulo **autoroute** posibilitó enrutar el tráfico a través del sistema comprometido, facilitando la ejecución de escaneos internos y habilitando posteriormente acciones de movimiento lateral.

Finalmente, la ejecución de PsExec sobre SMB para comprometer Host-B demostró que un atacante puede aprovechar credenciales legítimas incluso aquellas temporales o con permisos

limitados para expandir su presencia dentro de la infraestructura. Este resultado destaca la necesidad de implementar mecanismos como autenticación robusta, políticas estrictas sobre cuentas privilegiadas y monitoreo continuo frente a intentos de desplazamiento lateral.

Panorama Específico De La Etapa 5

Metodología

La metodología empleada en este informe se fundamenta en un enfoque técnico y operativo, alineado con las fases del ciclo de respuesta a incidentes establecido por el NIST SP 800-61 y con las buenas prácticas de defensa contempladas en los CIS Controls v8. Todo ello fue adaptado a un entorno donde se exige el uso exclusivo de herramientas de software libre o bajo licencia GPL.

La ruta metodológica se organiza de la siguiente manera:

Preparación y comprensión del entorno

Se analizó el escenario entregado por SecureNova Labs para reconocer los activos afectados —Host A y Host B—, los vectores de compromiso potenciales y las herramientas utilizadas por el atacante.

Identificación del incidente

Se efectuó la validación inicial del compromiso mediante la revisión de procesos inusuales, servicios no autorizados, registros de eventos, sesiones activas y artefactos sospechosos detectados en el sistema.

Los indicadores de compromiso (IoC) fueron comparados con los resultados obtenidos en la actividad previa de Red Team.

Análisis del escenario SecureNova Labs

SecureNova Labs ha informado que se ha visto involucrada en un ataque activo en curso dirigido contra sus estaciones de trabajo Windows, previamente analizadas en las actividades anteriores. La organización debe dar una respuesta inmediata, dado que esta amenaza compromete de manera significativa la integridad, disponibilidad y confiabilidad de sus recursos internos. En este contexto, se activa el equipo Blue Team, cuya misión es contener el ataque en curso, identificar su alcance y evitar la persistencia del daño dentro de la infraestructura, haciendo uso de herramientas de código abierto o con licencia GPL, debido a que la organización no dispone de recursos para la adquisición de software comercial

Existen evidencias preliminares de explotación remota del Host A, posible escalamiento de privilegios y establecimiento de mecanismos de persistencia, lo cual habría facilitado el movimiento lateral hacia otros sistemas de la infraestructura, incluidos servidores que gestionan información sensible. En consecuencia, el análisis se enfoca en dos dimensiones principales: el análisis del sistema operativo y el análisis de red.

Análisis del sistema operativo (Windows)

El primer eje de análisis consiste en evaluar el compromiso a nivel del sistema operativo. Desde la perspectiva del Blue Team, se debe iniciar con la identificación de procesos maliciosos o anómalos, utilizando herramientas como Sysinternals Process Explorer, Process Hacker y comandos nativos como tasklist y taskkill. Estas acciones permiten listar procesos sospechosos, revisar su consumo de CPU y memoria, verificar configuraciones de inicio automático y validar firmas digitales.

De manera complementaria, se realiza el análisis de servicios y mecanismos de persistencia, empleando herramientas como Autoruns y sc.exe, así como la revisión de claves críticas del registro de Windows, incluyendo Winlogon y Run/RunOnce. El objetivo es detectar servicios creados recientemente o modificaciones orientadas a mantener acceso persistente, registrando evidencia gráfica para su posterior inclusión en el informe forense.

Asimismo, se lleva a cabo la revisión de los registros de eventos del sistema, mediante Event Viewer, wevtutil y la herramienta Chainsaw para análisis avanzado de logs. En esta etapa se analizan eventos asociados a inicios de sesión exitosos y fallidos (4624 y 4625), elevación de privilegios (4672), creación de usuarios (4720), adición a grupos administrativos (4732) y eliminación de registros de auditoría (1102), con el fin de identificar patrones anómalos o actividades maliciosas recurrentes.

Análisis de red

El segundo eje de análisis se orienta a verificar si el equipo comprometido está siendo utilizado como punto de pivoting o si genera tráfico malicioso hacia otros activos internos. Para ello se realiza la inspección de conexiones activas mediante netstat -ano y TcpView, con el objetivo de identificar conexiones persistentes hacia puertos comúnmente asociados a canales de comando y control, como 4444, 8080, 135, 139, 445 y 3389.

Adicionalmente, se efectúa la captura y análisis del tráfico de red utilizando Wireshark y Tcpdump, lo que permite detectar patrones de explotación sobre servicios SMB, RDP o HTTP, identificar intentos de escaneo de puertos y reconocer posibles comportamientos de beaconing o transferencia de payloads maliciosos.

Como parte del endurecimiento defensivo, se procede a la validación de reglas de firewall y controles de seguridad, revisando configuraciones del Firewall de Windows y registros de Defender a través de PowerShell. Estas acciones permiten identificar reglas alteradas por el atacante, bloquear direcciones IP maliciosas y habilitar mecanismos de registro extendido para fortalecer la visibilidad del entorno.

contención del ataque (Blue Team)

La contención inicial de un ataque activo constituye el primer paso crítico dentro del ciclo de respuesta a incidentes. Cuando el analista Blue Team confirma que un host ha sido comprometido, como en el caso de la estación Windows analizada en SecureNova Labs, es fundamental ejecutar acciones orientadas a preservar la integridad de la evidencia y evitar la propagación del ataque hacia otros activos sensibles.

El proceso inicia con la identificación inmediata del alcance del ataque, evaluando la existencia de procesos sospechosos, conexiones remotas activas, intentos de autenticación inusuales, elevaciones de privilegios y creación de cuentas no autorizadas. La correlación de estos indicadores permite determinar si el atacante mantiene acceso interactivo o si se ha establecido persistencia en el sistema.

Una vez confirmado el compromiso, se procede al aislamiento controlado del host afectado, con el fin de interrumpir la comunicación con el atacante y prevenir movimientos laterales. Entre las acciones aplicables se encuentra la deshabilitación temporal del adaptador de red mediante PowerShell, la aplicación de reglas de firewall que bloqueen todo el tráfico entrante

y saliente, y, en entornos virtualizados, la remoción del adaptador de red interna asociado a la máquina comprometida.

Detener procesos maliciosos en ejecución n

Una vez aislado el host comprometido, se procede a la interrupción inmediata de cualquier carga útil activa con el fin de evitar que el atacante mantenga el control remoto del sistema. Esta acción inicia con la identificación de procesos sospechosos mediante herramientas como tasklist o Process Hacker, permitiendo reconocer el identificador único de cada proceso (PID), validar sus rutas de ejecución y verificar firmas digitales. Posteriormente, los procesos confirmados como maliciosos son finalizados de manera controlada utilizando el comando taskkill /F /PID, minimizando el impacto sobre el sistema. La detección temprana de estos procesos resulta clave para impedir la persistencia del ataque y limitar su propagación.

bloque de mecanismos de persistencia

El siguiente paso consiste en mitigar posibles reingresos del atacante al sistema mediante la revisión exhaustiva de los mecanismos de persistencia. Para ello se analizan claves críticas del registro, como Run y RunOnce, servicios creados recientemente a través de sc query y Autoruns, tareas programadas sospechosas mediante schtasks /query y cuentas de usuario agregadas sin autorización utilizando net user. Toda persistencia identificada debe ser eliminada de forma inmediata, documentando detalladamente cada acción realizada, con el fin de respaldar el informe técnico y garantizar la trazabilidad del proceso de contención.

conservación de evidencias

Aunque la prioridad inicial es detener el ataque en curso, el analista Blue Team debe asegurar la preservación adecuada de la evidencia forense, garantizando la posibilidad de un análisis posterior sin comprometer la cadena de custodia. Esto incluye la recolección de copias de registros relevantes del sistema, como Security, System y Application, la exportación de eventos mediante wevtutil, la captura de memoria RAM utilizando herramientas GPL como Winpmem o Belkasoft RAM Capture, y la obtención de capturas de pantalla de procesos, conexiones activas y configuraciones alteradas. Estas medidas permiten conservar información crítica para la investigación forense y la toma de decisiones estratégicas posteriores.

Comunicación y escalamiento

De manera paralela a las acciones técnicas, el analista debe comunicar de forma inmediata la situación al equipo de respuesta a incidentes y coordinar acciones adicionales. Esto implica validar la existencia de otros hosts comprometidos, verificar si se produjo exfiltración de información sensible y mantener un monitoreo continuo de la red interna para detectar actividad residual o intentos de reexplotación. Una comunicación oportuna y estructurada resulta fundamental para una respuesta coordinada y efectiva.

Conclusiones de la contención.

Ante un ataque activo, el Blue Team debe actuar con rapidez y precisión para identificar la naturaleza del ataque, aislar el host comprometido, bloquear procesos y mecanismos de persistencia, preservar la evidencia forense y coordinar la respuesta con el equipo de gestión de incidentes. Estas acciones inmediatas permiten contener la amenaza antes de que comprometa

activos críticos y facilitan la recuperación del control del entorno sin pérdida de información relevante para el análisis forense.

Acciones de hardenización para evitar la Repetición de ataque.

El análisis del ejercicio de Red Team evidenció que la estación Windows comprometida presentaba múltiples debilidades que facilitaron la explotación remota, el escalamiento de privilegios y el movimiento lateral hacia otros activos internos. Para prevenir la repetición de ataques bajo condiciones similares, se deben implementar medidas de hardening orientadas a reducir la superficie de ataque, fortalecer la configuración del sistema operativo y limitar la explotación de vulnerabilidades conocidas.

Gestión de parches y Actualizaciones críticas.

El ejercicio permitió identificar vulnerabilidades asociadas a software desactualizado dentro de la infraestructura de SecureNova Labs. El Host A fue comprometido mediante la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3, mientras que el Host B fue afectado a través de la vulnerabilidad MS17-010 (EternalBlue), relacionada con versiones obsoletas del protocolo SMB en Windows 7. La mitigación efectiva de estos vectores exige una gestión de parches integral que contemple ambos escenarios.

En el caso del Host A, Rejetto HFS 2.3 corresponde a una aplicación descontinuada, vulnerable a ejecución remota de código y no apta para entornos productivos. Las medidas de hardening incluyen su desinstalación completa, la sustitución por software con soporte y actualizaciones activas (como Apache, NGINX o IIS), la prohibición del uso de aplicaciones portables no autorizadas y la aplicación de políticas de control de ejecución para prevenir el uso

de binarios inseguros. La implementación de estas medidas habría evitado el compromiso inicial del sistema.

Para el Host B, la explotación de EternalBlue se debió a la ausencia del parche MS17-010 y al uso activo de SMBv1, un protocolo inseguro y obsoleto. Las acciones recomendadas incluyen la aplicación de parches acumulativos necesarios, la desactivación de SMBv1, la configuración segura de SMB para mitigar ataques de intermediario y la adopción de políticas de actualización automática mediante Windows Update o WSUS. Estas medidas habrían bloqueado completamente la explotación lateral observada.

Tabla 1

Medidas preventivas

Host afectado	Vulnerabilidad explotada	Medida preventiva clave
Host A	Rejetto HFS 2.3 – CVE-2014-6287	Eliminación de software vulnerable, control de aplicaciones
Host B	MS17-010 (EternalBlue)	Parcheo SMB, deshabilitar SMBv1, actualización del sistema

Nota. El cuadro describe las medidas preventivas para los Host afectados, vulnerabilidad explotada. Fuente propia (2025).

Diferencias entre el Blue Team y el Equipo de Respuesta a Incidentes

La distinción entre el Blue Team y el equipo de respuesta a incidentes resulta fundamental dentro de una estrategia integral de ciberseguridad. El Blue Team desarrolla una

labor proactiva y continua, orientada al fortalecimiento de la postura defensiva mediante monitoreo permanente, hardening, detección temprana de anomalías y reducción de la superficie de ataque. En contraste, el equipo de respuesta a incidentes actúa de forma reactiva, interviniendo cuando un incidente ya ha sido detectado o confirmado, con el objetivo de contener, erradicar la amenaza, restaurar la operación y preservar la evidencia forense.

Mientras el Blue Team se enfoca en la prevención y el mantenimiento de la confidencialidad, integridad y disponibilidad de los activos, el equipo de respuesta a incidentes concentra sus esfuerzos en la contención del ataque en curso, la identificación del alcance del compromiso, la erradicación del adversario y la coordinación de las acciones de recuperación. Ambas funciones son complementarias y esenciales para un ecosistema de seguridad resiliente.

Pertinencia del uso de Center for Internet Security dentro del Blue Team

La adopción de los Center for Internet Security (CIS) Controls resulta altamente pertinente para el Blue Team, ya que proporciona una guía estructurada, priorizada y basada en evidencia para el fortalecimiento de la postura defensiva. Estos controles permiten estandarizar procesos de seguridad, alinear las prácticas con estándares internacionales y garantizar coherencia entre medidas de defensa, monitoreo y respuesta.

La organización de los CIS Controls en niveles de implementación (IG1, IG2 e IG3) facilita la priorización de acciones defensivas, permitiendo fortalecer primero los controles esenciales y escalar progresivamente según el nivel de madurez requerido. Además, su enfoque en defensa en profundidad abarca aspectos críticos como inventario de activos, gestión de

vulnerabilidades, configuración segura, monitoreo continuo, respuesta a incidentes y protección de datos, lo que contribuye a una reducción significativa de la superficie de ataque.

En el contexto específico de SecureNova Labs, la aplicación de los CIS Controls habría permitido estructurar una defensa coherente y eficaz, reduciendo la probabilidad de explotación exitosa y fortaleciendo la capacidad de detección y respuesta ante incidentes de ciberseguridad.

Funciones Y Características Principales De Un SIEM

Security Information and Event Management es una plataforma fundamental dentro de la seguridad organizacional, especialmente para los equipos Blue Team. Su propósito en centralizar, correlacionar y analizar los eventos de seguridad que se generan por múltiples sistemas, con el fin de detectar actividades de origen malicioso, para con ello responder a incidentes y mejorar la visibilidad general del entorno.

Funciones Principales De Un SIEM

a) recolección y agregación de logs.

El Security Information and Event Management recibe y almacena eventos de diversas fuentes, como:

- Servidores Windows y Linux
- Firewalls y sistemas IDS/IPS
- Equipos de red
- Aplicaciones críticas
- Servicios en la nube
- Endpoints y antivirus

Esta centralización permite una visión unificada del comportamiento de la infraestructura.

b) Correlación de eventos

Security Information and Event Management analiza patrones y relaciones entre distintos eventos para identificar actividades que, de forma aislada, podría parecer benignas, pero en conjunto evidencia un ataque como, por ejemplo:

- Escaneos previos seguidos de intentos de autenticación
- Conexiones remotas inusuales después de ejecutar un proceso sospechoso
- Eventos correlacionados de movimiento lateral

La correlación permite detectar ataques complejos como ransomware, intrusiones avanzadas o campañas de phishing.

c) Detección temprana de amenazas

- Indicadores de Compromiso
- Actividades anómalas
- Intentos fallidos repetitivos
- Cambios no autorizados en configuraciones
- Ejecución de procesos maliciosos

La mejora de la capacidad del Blue Team para la actuación de manera oportuna.

a) Análisis forense y trazabilidad

El SIEM conserva registros históricos, lo que permite:

- Reconstruir la secuencia de un ataque.
- Analizar la propagación de la intrusión.
- Determinar que usuarios, sistemas o datos fueron afectados.

- Documentar evidencia para auditoria o investigación legal.

b) Reporte y cumplimiento normativo

Muchos estándares como ISO/IEC 27001, NIST y PCI-DSS requiere monitoreo y retención de registro. Un Security Information and Event Management facilita:

- Generación de reporte en forma automática.
- Cumplimiento de requisitos legal y de auditoría.
- La evidencia para revisiones internas y externas.

Características principales de un Security Information and Event Management (SIEM)

- Centralización del monitoreo en donde integra la seguridad de toda organización en un solo punto.
- Escalabilidad permite administrar grandes volúmenes de logs inclusive en infraestructuras distribuidas o en la nube.
- Integración con múltiples tecnologías al conectarse con firewals, antivirus, AD, endpoints, proxies, VPN, entre otros.
- Alertamiento avanzado donde incluye reglas predefinidas, aprendizaje automático y heurísticas.
- Dashboards interactivos facilitando al Blue Team la visualización en tiempo real del estado de los sistemas, alertas y tendencias de ataques.
- Capacidad de automatización para permitir la ejecución de acciones automáticas, tales como bloqueo de IP, cierre de sesión comprometida, Aislamiento de endpoint.

Importancia del SIEM para SecureNova Labs

Las principales relaciones que tiene SIEM con el caso objeto de análisis es:

- La posibilidad de detectar la ejecución del servidor Rejetto HFS en Host A.
- Hubiese generado una alerta sobre conexiones anómalas entre Host A y Host B.
- Habría identificado la explotación de EternalBlue mediante eventos SMB.
- Permitirá al Blue Team monitorear la infraestructura en tiempo real.
- Fortalece la detección y la respuesta ante amenazas futuras.

Herramientas de Contención de Ataques Informáticos (Hardware o Software)

La contención hace parte de fase primordial de la respuesta a incidentes, cuyo objetivo es limitar la propagación de la ocurrencia de los ataques, lograr el aislar los sistemas comprometidos y que reducir que el impacto sea mayor en la infraestructura. Contiene diferencia a las herramientas de detección, la soluciones que proporcionan las soluciones de contención actúan directamente sobre los entornos para bloquear, aislar o neutralizar las actividades maliciosas.

Para la contención se puede describir tres herramientas bastantemente utilizadas:

a) Firewalls de próxima generación

Puede ser de tipo Hardware / software, herramientas como por ejemplo pfSense, FortiGate, Palo Alto Networks.

Permite aplicar controles de filtrado avanzado para contener un ataque en tiempo real. Cuyas capacidades son:

- Detección de tráfico anómalo mediante inspección profunda de paquetes (DPI).
- Integración con sistemas IDS/IPS para bloquear explotación activa.
- Bloqueo inmediato de direcciones IP maliciosas.

- Restringir puertos utilizados por el atacante (por ejemplo 4444, 445, 3389).
- Implementación de reglas de emergencia para aislar equipos comprometidos.

Para la pertinencia que tiene para el caso SecureNova Labs:

Un NGFW hubiese permitido el aislar el Host A y Host B durante el ataque, evitando movimiento lateral y la explotación de EternalBlue.

b) Endpoint Detection & Response (EDR) con capacidades de aislamiento

Es de tipo Software, herramientas como por ejemplo Wazuh (open source), Velociraptor, Microsoft Defender for Endpoint.

Los EDR modernos permiten:

- Aislar un endpoint de la red (network isolation).
- Bloquear procesos maliciosos en ejecución.
- Interrumpir conexiones utilizadas por backdoors o C2.
- Suspender actividades no autorizadas en el sistema operativo.
- Extraer evidencia para análisis forense mientras el equipo permanece controlado.

Pertinencia en el caso un EDR habría bloqueado la ejecución de servidor malicioso HFS 2.3 hubiese podido detenido la sesión Meterpreter creada por Red Team.

c) Sistemas IDS/IPS (Intrusion Detection/Prevention Systems)

El tipo: Hardware/Software herramientas recomendadas suricata (GPL), Snort (GPL), Zeek.

Estas herramientas permiten:

- Generar alertas en tiempo real sobre escaneos de puertos, tráfico inusual o beaconing.
- Aplicar acciones automáticas para detener la propagación del ataque.

- Detectar y bloquear intentos de explotación conocidos (por firmas o patrones).
- Cortar conexiones activas asociadas a ataques SMB (EternalBlue).

En el caso de estudio tiene pertinencia un IPS con reglas actualizadas habría detectado y bloqueado la explotación CVE-2014-6287 (Rejetto HFS) y la explotación MS17-010 en Host B.

Línea de Tiempo Forense del Incidente (Timeline)

La siguiente línea de tiempo reconstruye, a partir de la evidencia técnica recolectada durante el ejercicio Red Team–Blue Team, los eventos clave del compromiso de Host A, el movimiento lateral hacia Host B y las acciones posteriores del adversario:

Tabla 2

Línea de Tiempo Forense del Ataque en SecureNova Labs

TIMESTAMP (APROX.)	EVENTO IDENTIFICADO	DESCRIPCIÓN TÉCNICA DEL SUCESO	EVIDENCIA ASOCIADA
10:12 AM	Ejecución del servicio vulnerable	El usuario del Host A inicia el servicio Rejetto HFS 2.3, versión vulnerable a ejecución remota de código (CVE-2014-6287).	Captura del servicio HFS en ejecución; confirmación de versión 2.3.
10:17 AM	Descubrimiento del servicio desde Parrot OS	El atacante identifica el puerto HTTP expuesto mediante el comando *nmap -sV -sC*.	Resultado de Nmap mostrando el

			puerto 80 abierto y el servicio HFS.
10:19 AM	Explotación remota del HFS	Se utiliza el módulo *exploit/windows/http/rejetto_hfs_exec* para obtener una sesión *shell*/*meterpreter*.	Evidencia en *msfconsole* de sesión *meterpreter* activa.
10:22 AM	Escalamiento de privilegios en Host A	El atacante obtiene privilegios de nivel SYSTEM mediante técnicas de bypass de seguridad.	Registro del evento 4672 en el log de seguridad de Windows.
10:25 AM	Enumeración de red interna	Se ejecutan los comandos *ipconfig*, *route print* y *arp* para identificar rutas y segmentación de red.	Salida de comandos registrada en la sesión activa.
10:29 AM	Establecimiento de pivoting	Se ejecuta el comando *run autoroute -s 10.0.2.0/24* para enrutar tráfico hacia la red interna donde se encuentra Host B.	Salida del módulo *autoroute* en *msfconsole*.

10:32 AM	Descubrimiento de Host B	Se realiza un *ARP sweep* y un escaneo TCP para identificar el host con dirección IP 10.0.2.7.	Resultado del barrido ARP confirmando la existencia de Host B.
10:35 AM	Explotación de Host B	Se identifica y explota la vulnerabilidad MS17-010 (EternalBlue), logrando acceso remoto al sistema.	Salida del módulo EternalBlue indicando explotación exitosa.
10:38 AM	Establecimiento de persistencia en Host B	El atacante crea un usuario con privilegios administrativos siguiendo el patrón “primerNombre+primerApellido”.	Registro del evento 4720 (creación de usuario) en el log de seguridad.
10:40 AM	Movimiento lateral y acceso a información	Se realizan acciones para visualizar y potencialmente extraer archivos sensibles almacenados en Host B.	Capturas de pantalla de la sesión activa en Host B.

10:47 AM	Intento de eliminación de trazas	El atacante ejecuta comandos para borrar registros de auditoría del sistema.	Registro del evento 1102 correspondiente al borrado de logs.

Nota. La línea de tiempo forense reconstruye de manera cronológica las acciones ejecutadas durante el incidente, con base en evidencias técnicas obtenidas de registros del sistema, salidas de herramientas ofensivas y capturas de sesión, permitiendo correlacionar las fases de explotación, pivoting y persistencias observadas en el caso SecureNova Labs.

Plan de Remediación Integral

El plan de remediación tiene como objetivo eliminar la causa raíz del compromiso, fortalecer la postura de seguridad y evitar que ataques similares vuelvan a ocurrir. Las medidas se dividen en acciones correctivas inmediatas, acciones de hardening, y acciones estratégicas a mediano plazo.

Acciones Correctivas Inmediatas

a) Eliminación del software vulnerable

- Desinstalar Rejetto HFS 2.3 de Host A.
- Bloquear la instalación de software portable no autorizado.
- Establecer una política de inventario obligatorio de software.

b) Aplicación de parches críticos

- Instalar MS17-010 en Host B.
- Aplicar parches acumulativos de Windows.
- Configurar actualizaciones automáticas.

c) Eliminación de usuarios maliciosos

- Eliminar la cuenta administrativa creada por el atacante.
- Revisar grupos administrativos para detectar modificaciones no autorizadas.

d) Limpieza de persistencia

- Revisar claves Run/RunOnce, NTLM, servicios sospechosos.
- Eliminar cualquier archivo, DLL o script dejado por el atacante.

e) Aislamiento temporal de los hosts comprometidos

- Desconectar Host A y Host B de la red hasta completar el saneamiento.

Acciones de Hardening del Sistema Operativo

a) Configuración segura en Windows

- Deshabilitar SMBv1 completamente.
- Habilitar SMB Signing.
- Fuerza mínima de contraseña 12 caracteres.
- Bloqueo de cuenta tras 5 intentos fallidos.
- Habilitar Control de Cuentas de Usuario (UAC) en modo estricto.

b) Restricción de privilegios

- Implementar el principio de menor privilegio.
- Separación de cuentas administrativas y de usuario estándar.
- Deshabilitar cuentas administrativas heredadas.

c) Endurecimiento de servicios

- Deshabilitar cualquier servicio no utilizado.
- Revisar puertos expuestos (135, 139, 445, 3389).
- Restringir RDP a través de VPN y listas blancas.

Acciones de Hardening de Red

a) Configuración de firewall

- Bloquear tráfico entrante no esencial.
- Crear reglas para impedir acceso externo a servicios internos.
- Registrar y alertar conexiones hacia puertos utilizados por malware (4444, 8080, 135, 445).

b) Segmentación de red

- Separar estaciones de trabajo y servidores críticos.
- Implementar VLANs y políticas de acceso entre segmentos.
- Aislar sistemas legacy que no se puedan actualizar.

c) IDS/IPS

- Implementar Snort o Suricata con reglas actualizadas.
- Bloquear firmas asociadas a EternalBlue y CVE-2014-6287.

Acciones Estratégicas a Mediano Plazo

a) Implementación de un SIEM

- Centralizar logs.
- Automatizar alertas de escalada de privilegios, creación de usuarios y tráfico anómalo.

b) Cultura de seguridad

- Capacitación a usuarios sobre instalación de software.
- Entrenamiento del personal de TI sobre actualización de sistemas.

c) Políticas formales

- Política de gestión de vulnerabilidades.
- Política de inventario de software.
- Política de respuesta a incidentes.

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/XDO5PjXD4GY

Conclusiones

El análisis del caso SecureNova Labs evidencia que la ciberseguridad requiere un equilibrio entre capacidades ofensivas, controles defensivos, cumplimiento normativo y una conducta ética responsable. El ejercicio permitió recrear un ciclo completo de ataque y defensa, confirmando que las debilidades explotadas no se originan únicamente en fallos técnicos, sino también en deficiencias organizacionales, ausencia de controles preventivos efectivos y limitaciones en la gestión del riesgo.

En relación con el objetivo de documentar el proceso técnico de ataque ejecutado por el Red Team, se logró describir de manera detallada cada una de las fases del ataque, desde el reconocimiento inicial hasta la explotación, el pivoting y el movimiento lateral dentro de la infraestructura. Este análisis permitió identificar vectores de ataque críticos y evidenciar cómo vulnerabilidades ampliamente conocidas, como CVE-2014-6287 y MS17-010, pueden ser explotadas con alto impacto cuando no se gestionan adecuadamente los parches y configuraciones de seguridad.

Respecto al objetivo de analizar la respuesta del Blue Team, el estudio demostró la importancia del monitoreo continuo, la revisión sistemática de registros, la preservación de evidencias y la ejecución oportuna de acciones de contención. La correcta identificación de eventos críticos, el aislamiento de los hosts comprometidos y la aplicación de medidas de hardening resultaron determinantes para reducir el impacto del incidente y limitar la propagación del ataque.

En cuanto al objetivo de relacionar el caso práctico con los marcos legales y éticos aplicables, el análisis permitió evidenciar la relevancia de la Ley 1273 de 2009 y del Código de Ética profesional en la conducción de actividades de ciberseguridad. Tanto las acciones ofensivas como las defensivas deben ejecutarse bajo autorización expresa, respetando los principios de legalidad, proporcionalidad y responsabilidad en el manejo de la información.

De igual manera, el objetivo de comparar y articular las estrategias del Red Team y del Blue Team se cumplió al identificar cómo ambas funciones se complementan dentro de un modelo de defensa integral. Mientras el Red Team expone debilidades y simula escenarios de ataque realistas, el Blue Team fortalece la capacidad de detección, respuesta y recuperación, contribuyendo conjuntamente a la madurez de la postura de seguridad organizacional.

Finalmente, en relación con el objetivo de proponer recomendaciones técnicas y organizacionales, el trabajo permitió formular medidas de endurecimiento alineadas con marcos de referencia reconocidos como OWASP, CIS Controls, NIST e ISO/IEC 27001. Estas recomendaciones se orientan a la reducción de la superficie de ataque, la mejora de la gestión de vulnerabilidades y la prevención de incidentes similares, reafirmando que la madurez en ciberseguridad depende tanto de la tecnología como de procesos sólidos y una cultura organizacional orientada a la prevención y el cumplimiento normativo. La articulación efectiva entre Red Team y Blue Team, soportada por marcos internacionales y alineada con el contexto legal colombiano, constituye un elemento clave para fortalecer la madurez de la ciberseguridad organizacional y prevenir incidentes futuros (Arroyo, 2025; NIST, 2022).

Recomendaciones

A partir del análisis integral del caso SecureNova Labs, y considerando tanto la perspectiva ofensiva (Red Team) como la defensiva (Blue Team), se formulan las siguientes recomendaciones orientadas al fortalecimiento de la postura de seguridad y a la madurez organizacional. Con el fin de facilitar su implementación en contextos de recursos limitados, estas se agrupan en recomendaciones técnicas, organizacionales y formativas, priorizando aquellas de mayor impacto inmediato.

Recomendaciones técnicas (alta prioridad)

Las recomendaciones técnicas constituyen el primer nivel de acción, dado su impacto directo en la reducción de la superficie de ataque y la prevención de incidentes críticos. En primer lugar, se recomienda implementar un programa formal de gestión de vulnerabilidades, integrado al Sistema de Gestión de Seguridad de la Información (SGSI), que permita identificar, clasificar, priorizar y mitigar vulnerabilidades de manera continua. Este programa debe apoyarse en herramientas especializadas, la utilización de métricas como CVSS v3.1 y la verificación posterior a la remediación.

De manera complementaria, resulta prioritario eliminar servicios obsoletos y software vulnerable, como Rejetto HFS 2.3 y sistemas operativos sin soporte, sustituyéndolos por soluciones actualizadas y con mantenimiento activo. La ausencia de parches y el uso de aplicaciones descontinuadas fueron factores determinantes en la explotación de vulnerabilidades como CVE-2014-6287 y MS17-010.

Asimismo, se recomienda fortalecer la segmentación de red y el aislamiento de activos críticos, mediante el uso de VLAN, firewalls internos y listas de control de acceso, con el fin de limitar el movimiento lateral y reducir el impacto de un compromiso inicial. Esta medida debe complementarse con la deshabilitación de protocolos inseguros, como SMBv1, Telnet o FTP plano, y el cierre de puertos innecesarios a nivel de host y perímetro.

Finalmente, se sugiere incorporar mecanismos avanzados de monitoreo, como IDS/IPS y soluciones SIEM, que permitan detectar de forma temprana actividades anómalas, correlacionar eventos de seguridad y generar alertas oportunas. Estas capacidades son fundamentales para acortar el tiempo de detección y respuesta frente a incidentes activos.

Recomendaciones organizacionales (prioridad media)

Desde el punto de vista organizacional, se recomienda formalizar un proceso de respuesta a incidentes basado en NIST SP 800-61, definiendo roles, responsabilidades, procedimientos y canales de comunicación. Un marco metodológico claro mejora la coordinación entre áreas técnicas, directivas y legales, y reduce el impacto operativo durante incidentes reales.

Igualmente, es necesario reforzar las políticas de privilegios y separación de funciones, aplicando el principio de mínimo privilegio, mecanismos de autenticación multifactor y controles sobre cuentas administrativas. La correcta gestión de identidades y accesos limita el abuso de credenciales y reduce las posibilidades de escalamiento de privilegios.

Adicionalmente, se recomienda realizar auditorías periódicas y ejercicios controlados Red Team y Blue Team, incluyendo prácticas de Purple Team, que permitan evaluar la eficacia de los controles implementados, identificar brechas persistentes y retroalimentar continuamente el SGSI.

Recomendaciones formativas (prioridad estratégica)

Las recomendaciones formativas constituyen un eje transversal y de largo plazo, orientado a fortalecer la cultura de seguridad. Se propone desarrollar programas de capacitación continua para el personal técnico en áreas como hardening, análisis forense, gestión de vulnerabilidades y respuesta a incidentes, así como formación en principios éticos y normativos relacionados con la protección de datos personales.

De igual forma, es fundamental implementar campañas de concientización dirigidas a todo el personal, enfocadas en la prevención de amenazas comunes como phishing, ingeniería social y malas prácticas operativas. La capacitación permanente incrementa la resiliencia organizacional y complementa las medidas técnicas y organizacionales adoptadas.

Referencias Bibliográficas

Álvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos*. Semantic Scholar.

Arroyo, E. (2025). *Sinergia de equipos red team y blue team en la protección de entornos corporativos*. Universidad Nacional Abierta y a Distancia (UNAD).

CCN-CERT. (2018). *Guía de seguridad de las TIC (CCN-STIC-495): Seguridad en IPv6* (pp. 10–29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-deacceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Chindrus, C., & Caruntu, C.-F. (2023). Securing the network: A red and blue cybersecurity competition case study. *Information, 14*(11), 587. https://doi.org/10.2478/bipie-2023-0008CIS Security. (2020). *CIS benchmarks*. https://www.cisecurity.org/cis-benchmarks/

Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS* (Versión 1.0, pp. 5–31). Universidad Nacional Abierta y a Distancia. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoracion_y_evaluacion_de_riesgos_de_ciberseguridad__Pag_publicado.pdf

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009*. Diario Oficial No. 47.223.

Congreso de la República de Colombia. (2009). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”. https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2012). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. https://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

COPNIA. (2015). *Código de ética para el ejercicio de la ingeniería y sus profesiones afines y auxiliares* (pp. 3–26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia* [Monografía]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/41392

INCIBE. (2019). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas*. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red teaming vs. blue teaming: A comparative analysis of cybersecurity strategies in the digital battlefield. *International Journal of Scientific Research in Engineering and Management, 7*(12), 1–11. https://doi.org/10.55041/IJSREM27675

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Políticas de privacidad y condiciones de uso*. https://www.mintic.gov.co/portal/inicio/Secciones

Ministerio de Tecnologías de la Información y las Comunicaciones. (2013). Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security information and event management)* (pp. 31–63). Universidad San Francisco de Quito. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Palomo Luna, D. F., Zambrano Hernández, L. F., Moreno Molano, S. X., & Peña Hidalgo, H. J. (2024). Una mirada a metodologías para pruebas de penetración en ciberseguridad. *Boletín Informativo CSIRT Académico UNAD*, (28). https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

Panda Security. (2018). *Pentesting: Una herramienta muy valiosa para tu empresa*. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team–red team approach to hardware trust assessment. In *2011 IEEE 29th International Conference on Computer Design (ICCD)* (pp. 285–288). IEEE. https://doi.org/10.1109/ICCD.2011.6081410

Rapid7. (2012). *Metasploitable 2*. https://metasploit.help.rapid7.com/docs/metasploitable-2

Sanne, S. H. (2024). *Investigaciones sobre técnicas, herramientas y metodologías de pruebas de seguridad para identificar y mitigar vulnerabilidades*. URF Journals.

Zambrano Hernández, L. F., Peña Hidalgo, H. J., & Cárdenas Corral, J. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad*. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_Gestion_y_Clasificacion_de_un_Incidentes_de_Ciberseguridad.pdf

Apéndices

Apéndice A

Resultado de revisión en Turnitin

Nota. Registro de paso del trabajo de informe del seminario de Especialización, donde se registra el porcentaje de similitud con solo un 6%.