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

Alexander Cuellar Herrera

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Resumen

El presente informe técnico documenta el desarrollo integral de un ejercicio práctico de ciberseguridad ejecutado en cinco etapas, abordando actividades ofensivas (Red Team), defensivas (Blue Team) y análisis legales y éticos aplicados a escenarios corporativos simulados en “SecureNova Labs”. Durante la fase ofensiva se realizó el reconocimiento de infraestructura, identificación de vulnerabilidades críticas y explotación controlada de los sistemas Host-A y Host-B mediante técnicas de pivoting, movimiento lateral y post-explotación. Se evidenció la explotación de la vulnerabilidad CVE-2014-6287 asociada a Rejetto HFS 2.3 y la vulnerabilidad MS17-010 EternalBlue, permitiendo demostrar el impacto de sistemas desactualizados, segmentación insuficiente y configuraciones inseguras. Posteriormente, desde la perspectiva Blue Team, se plantearon estrategias de remediación orientadas a fortalecer la seguridad organizacional mediante gestión de vulnerabilidades, hardening, segmentación de red, monitoreo continuo, implementación de SIEM, EDR/XDR, así como la aplicación de controles basados en el principio de mínimo privilegio para reducir riesgos asociados a accesos innecesarios. Adicionalmente, se desarrolló un análisis jurídico y ético relacionado con acuerdos de confidencialidad, deber de denuncia, protección de datos y responsabilidad profesional en ciberseguridad, concluyendo que ninguna organización puede justificar prácticas ilegales mediante cláusulas contractuales contrarias al orden público colombiano. Finalmente, el informe consolida recomendaciones estratégicas alineadas con estándares internacionales y buenas prácticas de seguridad, orientadas al fortalecimiento de la resiliencia organizacional frente a amenazas cibernéticas actuales y futuras.

***Palabras clave*:** Ciberseguridad, hardening, pentesting, pivoting, vulnerabilidad.

Abstract

This technical report documents the comprehensive development of a practical cybersecurity exercise conducted in five stages, encompassing offensive (Red Team) and defensive (Blue Team) activities, as well as legal and ethical analyses applied to simulated corporate scenarios within “SecureNova Labs”. During the offensive phase, infrastructure reconnaissance, identification of critical vulnerabilities, and controlled exploitation of the Host-A and Host-B systems were performed using pivoting, lateral movement, and post-exploitation techniques. The exploitation of the CVE-2014-6287 vulnerability associated with Rejetto HFS 2.3 and the MS17-010 EternalBlue vulnerability demonstrated the impact of outdated systems, insufficient network segmentation, and insecure configurations. Subsequently, from the Blue Team perspective, remediation strategies were proposed to strengthen organizational security through vulnerability management, system hardening, network segmentation, continuous monitoring, the implementation of SIEM and EDR/XDR solutions, and the application of least-privilege access controls to reduce risks associated with unnecessary access permissions. Additionally, a legal and ethical analysis was conducted concerning confidentiality agreements, the duty to report unlawful activities, data protection, and professional responsibility in cybersecurity, concluding that no organization can justify illegal practices through contractual clauses that contravene Colombian public policy. Finally, the report consolidates strategic recommendations aligned with international standards and cybersecurity best practices, aimed at enhancing organizational resilience against current and emerging cyber threats.

***Keywords*:** Cybersecurity, hardening, pentesting, pivoting, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Acceso abusivo a un sistema informático:

Conducta delictiva que consiste en ingresar, permanecer o interactuar con un sistema informático sin autorización legítima o excediendo los permisos otorgados. En Colombia, este comportamiento se encuentra tipificado en la Ley 1273 de 2009.

ARP (Address Resolution Protocol):

Protocolo de red utilizado para asociar direcciones IP con direcciones MAC dentro de una red local. En pruebas de penetración, se emplea para identificar dispositivos activos y realizar procesos de reconocimiento interno.

Blue Team:

Equipo encargado de proteger la infraestructura tecnológica de una organización mediante actividades de monitoreo, detección, análisis y respuesta ante incidentes de seguridad informática.

Ciberseguridad:

Conjunto de prácticas, procesos, tecnologías y controles orientados a proteger sistemas, redes, aplicaciones y datos frente a accesos no autorizados, ataques informáticos y amenazas digitales.

CIS Benchmarks:

Son estándares de configuración reconocidos mundialmente que ayudan a las organizaciones a proteger sus sistemas y datos contra amenazas cibernéticas, (Susnjara & Smalley, 2024).

Escaneo de vulnerabilidades:

Proceso automatizado o manual mediante el cual se identifican debilidades de seguridad presentes en sistemas, aplicaciones o redes, con el fin de evaluar riesgos y priorizar acciones de mitigación.

EternalBlue (MS17-010):

Exploit desarrollado sobre una vulnerabilidad crítica del protocolo SMBv1 en sistemas Windows, ampliamente utilizado para la ejecución remota de código y movimientos laterales dentro de redes corporativas (BetaFred, 2024).

Exploit:

Código, técnica o procedimiento diseñado para aprovechar una vulnerabilidad específica con el propósito de ejecutar acciones no autorizadas sobre un sistema informático.

Exploit-DB:

Repositorio público de vulnerabilidades y exploits utilizado por profesionales de ciberseguridad para actividades de investigación, pruebas de penetración y análisis de seguridad.

Firewall:

Mecanismo de seguridad que controla y filtra el tráfico de red entrante y saliente de acuerdo con políticas previamente definidas, con el fin de prevenir accesos no autorizados.

Hardening:

Proceso de fortalecimiento de la seguridad de un sistema mediante la deshabilitación de servicios innecesarios, aplicación de configuraciones seguras y reducción de la superficie de ataque.

Host-A:

Equipo comprometido inicialmente durante el ejercicio práctico, utilizado posteriormente como punto de pivote para acceder a la red interna.

Host-B:

Servidor ubicado en una red interna segmentada que fue comprometido mediante técnicas de movimiento lateral y explotación remota.

IDS/IPS (Intrusion Detection System / Intrusion Prevention System):

Herramientas de seguridad encargadas de detectar y, en algunos casos, bloquear actividades sospechosas o ataques dentro de una red informática.

Lateral Movement (Movimiento lateral):

Técnica utilizada por un atacante para desplazarse entre sistemas dentro de una red comprometida con el objetivo de ampliar el acceso y obtener control sobre otros activos.

Meterpreter:

Payload avanzado de Metasploit que proporciona una consola interactiva sobre el sistema comprometido, permitiendo ejecutar comandos, transferir archivos y realizar actividades de post-explotación.

MSFconsole:

Interfaz principal de línea de comandos de Metasploit Framework utilizada para gestionar exploits, payloads, módulos auxiliares y sesiones activas.

Nmap (Network Mapper):

Herramienta de código abierto utilizada para el descubrimiento de hosts, escaneo de puertos, identificación de servicios y auditoría de seguridad en redes informáticas.

OpenVAS:

Herramienta de código abierto orientada al análisis y gestión de vulnerabilidades mediante pruebas automatizadas sobre sistemas, aplicaciones y redes.

Payload:

Componente de un exploit encargado de ejecutar la acción maliciosa o controlada sobre el sistema objetivo una vez la vulnerabilidad ha sido explotada.

Pentesting (Prueba de penetración):

Evaluación de seguridad autorizada que simula ataques reales con el propósito de identificar vulnerabilidades y medir el nivel de exposición de una infraestructura tecnológica.

Pivoting:

Técnica mediante la cual un atacante utiliza un sistema previamente comprometido como puente para acceder a otros segmentos o redes internas que originalmente no eran accesibles.

Portproxy:

Funcionalidad de Windows que permite redirigir tráfico de red entre diferentes direcciones IP y puertos, utilizada en escenarios de pivoting y movimiento lateral.

Post-explotación:

Fase posterior a la explotación de una vulnerabilidad en la que el atacante busca mantener acceso, recolectar información, escalar privilegios o desplazarse lateralmente dentro de la red.

Privilege Escalation (Escalada de privilegios):

Proceso mediante el cual un atacante obtiene permisos superiores a los inicialmente concedidos, alcanzando privilegios administrativos o de sistema.

Red Team:

Equipo especializado en ejecutar simulaciones controladas de ataques reales con el objetivo de evaluar la postura de seguridad, capacidades defensivas y nivel de resiliencia de una organización.

Rejetto HFS:

Servidor HTTP ligero para compartición de archivos que presenta vulnerabilidades críticas en versiones desactualizadas, como la ejecución remota de comandos asociada al CVE-2014-6287.

Reverse Shell:

Conexión remota iniciada desde el sistema comprometido hacia el equipo atacante, utilizada para evadir restricciones de red y establecer control sobre el objetivo.

Segmentación:

Técnica de seguridad que divide una red en subredes aisladas para controlar el tráfico y limitar el movimiento lateral de amenazas, reduciendo así la superficie de ataque y mejorando la capacidad de contención ante incidentes. (Cisco, 2026)

SIEM (Security Information and Event Management):

Plataforma de seguridad que centraliza, correlaciona y analiza eventos y registros provenientes de múltiples dispositivos y sistemas para detectar incidentes de seguridad.

SMB (Server Message Block):

Protocolo de comunicación utilizado principalmente en entornos Windows para compartir archivos, impresoras y recursos de red.

Vulnerabilidad:

Debilidad presente en un sistema, aplicación, red o proceso que puede ser explotada para comprometer la confidencialidad, integridad o disponibilidad de la información.

Wazuh:

La plataforma de ciberseguridad de código abierto más utilizada, que unifica XDR y SIEM en una sola solución. Analiza datos de seguridad en endpoints, nubes y redes para detectar amenazas, responder a incidentes y garantizar el cumplimiento normativo".

Introducción

El presente informe técnico consolida el desarrollo integral de un ejercicio práctico de ciberseguridad ejecutado en cinco etapas dentro de un entorno controlado de laboratorio propuesto por “SecureNova Labs”. El objetivo principal fue evaluar escenarios ofensivos y defensivos mediante la aplicación de técnicas de Red Team, Blue Team y análisis jurídico–ético asociados a la seguridad informática y la protección de infraestructuras tecnológicas.

Durante el desarrollo del ejercicio se realizaron actividades de reconocimiento, análisis de vulnerabilidades, explotación controlada, pivoting, movimiento lateral y post-explotación sobre sistemas Windows vulnerables, utilizando herramientas especializadas como Nmap, Metasploit Framework, OpenVAS y Exploit-DB. Asimismo, se documentaron los hallazgos relacionados con vulnerabilidades críticas como CVE-2014-6287 y MS17-010 EternalBlue, evidenciando riesgos asociados a sistemas desactualizados, segmentación deficiente y configuraciones inseguras.

De igual manera, el informe aborda estrategias defensivas orientadas a la mitigación de riesgos, fortalecimiento de controles de seguridad y adopción de buenas prácticas alineadas con estándares internacionales. Finalmente, se incorporan consideraciones legales y éticas relacionadas con la protección de datos, responsabilidad profesional y cumplimiento normativo en el contexto colombiano.

Justificación

El desarrollo del presente ejercicio de ciberseguridad se justifica por la necesidad de fortalecer las capacidades técnicas, defensivas y analíticas frente al incremento constante de amenazas informáticas que afectan a las organizaciones modernas. En la actualidad, vulnerabilidades críticas, configuraciones inseguras y sistemas desactualizados representan un alto riesgo para la confidencialidad, integridad y disponibilidad de la información corporativa.

A través de la ejecución de actividades de Red Team y Blue Team, este proyecto permitió comprender de manera práctica el ciclo completo de un ataque informático, desde las fases de reconocimiento y explotación hasta el movimiento lateral y la post-explotación, evidenciando cómo una vulnerabilidad puede comprometer múltiples activos dentro de una infraestructura tecnológica. Asimismo, el análisis defensivo facilitó la formulación de estrategias de mitigación basadas en hardening, segmentación de red, monitoreo continuo y gestión de vulnerabilidades.

De igual manera, el ejercicio incorporó un enfoque legal y ético orientado al cumplimiento normativo y a la responsabilidad profesional en ciberseguridad, resaltando la importancia de actuar conforme a la legislación colombiana y los principios de integridad profesional. En conjunto, el desarrollo de este informe contribuye al fortalecimiento de competencias técnicas y estratégicas aplicables a escenarios reales de seguridad informática.

Objetivos

Objetivo General

Evaluar la seguridad de una infraestructura tecnológica mediante técnicas de Red Team, Blue Team y análisis legal, con el fin de identificar vulnerabilidades y proponer medidas de mitigación.

Objetivos Específicos

Examinar las implicaciones legales y éticas asociadas a las actividades de ciberseguridad realizadas en el ejercicio.

Identificar y explotar vulnerabilidades en los sistemas Host-A y Host-B utilizando herramientas de ciberseguridad.

Analizar debilidades de seguridad relacionadas con configuraciones inseguras, segmentación de red y sistemas desactualizados.

Proponer estrategias de mitigación y fortalecimiento defensivo basadas en buenas prácticas de seguridad informática.

Lineamientos de Operación de Equipos Red Team y Blue Team

En el marco de los lineamientos de Operaciones Red Team y Blue Team, se consolidó un conjunto de documentos técnicos y normativos orientados a establecer las bases conceptuales, legales y operativas para la ejecución de pruebas de penetración y la gestión de vulnerabilidades con una metodología de acuerdo al texto "Una mirada a metodologías para pruebas de penetración en ciberseguridad" Palomo Luna, D. F., Zambrano Hernández, L. F., Moreno Molano, S. X., & Peña Hidalgo, H. J. (2024).

Los productos generados abordan el marco normativo colombiano aplicable a delitos informáticos y protección de datos, la metodología estructurada del proceso de pentesting, así como el análisis de herramientas fundamentales utilizadas en ciberseguridad ofensiva y defensiva de acuerdo con el contexto "Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield" de Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023).

En esta primera etapa, se abordó el marco normativo sobre delitos informáticos y protección de datos personales en Colombia. Si bien el ordenamiento jurídico colombiano ha desarrollado un sistema normativo integral (Constitución Política, Ley 1581 de 2012, Ley 1273 de 2009, entre otros), el análisis crítico permite cuestionar la brecha entre la norma y su aplicación efectiva en entornos empresariales y gubernamentales.

Por ejemplo, aunque la Ley 1273 de 2009 tipifica conductas como el acceso abusivo a sistemas informáticos (Art. 269A) o el hurto por medios informáticos (Art. 269I), la experiencia práctica muestra que muchas organizaciones aún no implementan controles técnicos suficientes para mitigar estos riesgos. Asimismo, la Resolución 500 de 2021 (MinTIC) y el Modelo de

Seguridad y Privacidad de la Información (MSPI) ofrecen directrices MINTIC. (2022), pero su adopción sigue siendo heterogénea, especialmente en el sector privado.

No basta con conocer las leyes y estándares (ISO/IEC 27001, CONPES 3854, etc.); el verdadero desafío radica en traducir estos lineamientos en procesos operativos sostenibles. Durante la etapa, se evidenció que muchas entidades se limitan a cumplir requisitos formales (como tener una política de tratamiento de datos) sin implementar mecanismos reales de verificación, auditoría continua o respuesta a incidentes. Esta desconexión entre el marco normativo y la práctica cotidiana representa un riesgo mayor que la ausencia total de regulación, pues genera una falsa sensación de seguridad.

Proceso de pentesting: análisis de etapas y limitaciones prácticas

El pentesting o prueba de penetración se desarrolló siguiendo la metodología estructurada de cinco fases (reconocimiento, escaneo, explotación, post-explotación y reporte), tal como se describe en la literatura especializada de Lozano (2023).

Figura 1

Etapas del pentesting

Nota: Las diferentes etapas del pentesting y sus herramientas Open Source y comerciales, Autoría propia

Reconocimiento y escaneo: la importancia de la interpretación humana

Frente al tema, Estefania.dominguez. (2026) afirma que la herramienta apropiada se encuentra Nmap para identificar puertos abiertos, servicios y versiones de software. Si bien la herramienta facilita un barrido rápido de la superficie de ataque, el análisis crítico revela dos limitaciones fundamentales:

Falsos positivos/negativos: Como se advierte en el texto, los resultados automatizados requieren interpretación por parte del analista. En la práctica, un puerto abierto no siempre es vulnerable, y un servicio actualizado no garantiza seguridad.

Dependencia de firmas conocidas: Tanto Nmap como Nessus se basan en bases de datos de vulnerabilidades conocidas (CVE), lo que los hace ineficaces frente a vulnerabilidades de día cero (zero-day) o configuraciones propietarias no documentadas.

Estas herramientas son necesarias, pero no suficientes. Un profesional debe complementarlas con análisis manual y contexto del negocio. La automatización no reemplaza el juicio experto.

Explotación y post-explotación: entre la validación y el riesgo

Se emplean herramientas como Metasploit y SQLMap para validar vulnerabilidades. Si bien su uso permite demostrar impacto real, se identificaron riesgos operativos:

Explotación inestable: Algunos exploits pueden afectar la disponibilidad del sistema objetivo, lo que en entornos productivos es inaceptable.

Escalamiento de privilegios limitado: Herramientas como Mimikatz funcionan bien en entornos Windows legacy, pero su efectividad disminuye ante configuraciones modernas (Windows Defender, AMSI, etc.).

La fase de post-explotación es a menudo subestimada. En el ejercicio, se evidenció que obtener acceso inicial (ej. mediante inyección SQL) es solo el primer paso; moverse lateralmente y mantener persistencia requiere un conocimiento profundo de la infraestructura objetivo, algo que ninguna herramienta automatizada resuelve por sí sola.

Reporte y mitigación: el eslabón más débil

Se encuentra Dradis para organizar hallazgos y generar reportes. Sin embargo, desde una perspectiva crítica:

Los informes técnicos suelen ser extensos y poco accionables para la alta dirección.

Las recomendaciones genéricas (ej. "aplicar parches") ignoran las restricciones operativas de las organizaciones (ventanas de mantenimiento, compatibilidad, recursos económicos).

En esta etapa, se recomienda priorizar la criticidad de los hallazgos según el contexto del negocio y proponer planes de remediación por fases, no solo listados de vulnerabilidades.

Herramientas de ciberseguridad

Metasploit: Plataforma para desarrollo y ejecución de exploits. Su facilidad de uso puede generar una falsa sensación de dominio. Muchos usuarios ejecutan exploits sin comprender el impacto real en el sistema objetivo. Además, su efectividad depende de la actualización constante de módulos, lo que requiere suscripción a versiones Pro o acceso a comunidades activas.

Nmap: Escaneo de puertos, servicios y OS fingerprinting. Es una herramienta poderosa, pero el ruido en redes modernas (firewalls, IDS/IPS, balanceadores de carga) puede distorsionar los resultados. El uso de técnicas sigilosas (como decoy scans) es útil, pero no infalible.

OpenVAS: Frente al tema, Estefania.dominguez. (2026) afirma que el escaneo automatizado de vulnerabilidades. Su principal limitación es la alta tasa de falsos positivos, lo que obliga a invertir tiempo en validación manual. Además, su curva de aprendizaje es más compleja que la de alternativas comerciales (Nessus, Qualys).

Exploit-DB: Repositorio público de exploits y PoCs. Si bien es un recurso valioso para investigación, su uso en pruebas reales implica riesgos legales y operativos. Asimismo, para Molina, P. (2024) no todos los exploits están validados; algunos pueden causar daños colaterales.

CVE: Sistema de identificación estandarizado de vulnerabilidades. La asignación de un CVE no garantiza que exista un parche o una solución disponible. Además, los tiempos entre la divulgación pública y la corrección pueden ser extensos, dejando sistemas expuestos.

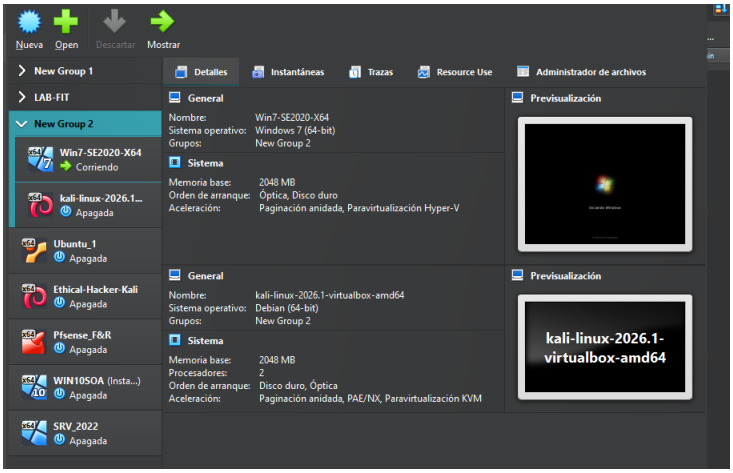
El uso de herramientas de ciberseguridad no puede desligarse del contexto organizacional y del nivel de madurez del equipo técnico. Una herramienta avanzada en manos de un usuario sin experiencia puede generar más riesgos que beneficios. La etapa permitió comprender que la eficacia del pentesting no reside en las herramientas en sí mismas, sino en la capacidad de interpretar sus resultados y traducirlos en acciones de mejora continua.

Configuración laboratorio

Una vez analizado el marco normativo y revisadas algunas de las herramientas más relevantes en el ámbito de la ciberseguridad, se procederá a la preparación del entorno de laboratorio mediante la descarga, instalación y configuración inicial de las máquinas virtualizadas, así como la validación de conectividad y funcionamiento entre los diferentes componentes del entorno.

Figura 2

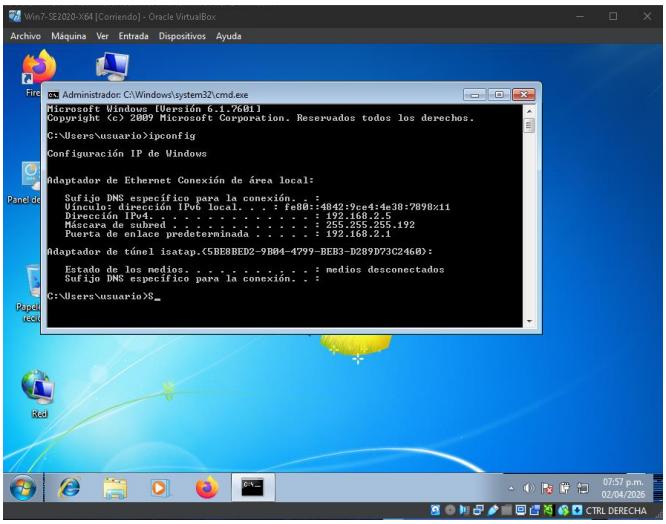
Máquinas virtuales agrupadas en new grupo2



Nota: La imagen presenta la instalación y configuración de las máquinas virtuales Host-A, Host-B y Kali Linux en el entorno de virtualización Oracle VM VirtualBox, las cuales conforman la infraestructura utilizada para el desarrollo de las actividades de análisis, explotación y validación de seguridad realizadas durante el laboratorio. Autoría propia.

Figura 3

Verificación de la ip asignada a la máquina virtual de windows

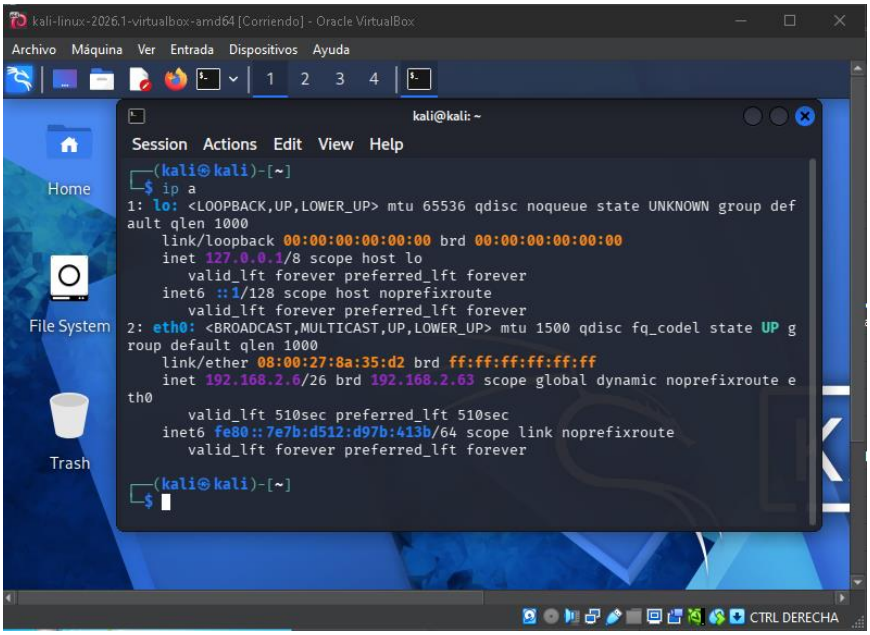


Nota: Acceso a la consola de comandos (CMD) y verificación de los parámetros de configuración de red mediante la ejecución del comando ipconfig, con el fin de identificar la

dirección IP, la máscara de subred, la puerta de enlace predeterminada y demás configuraciones de red del sistema. Autoría propia

Figura 4

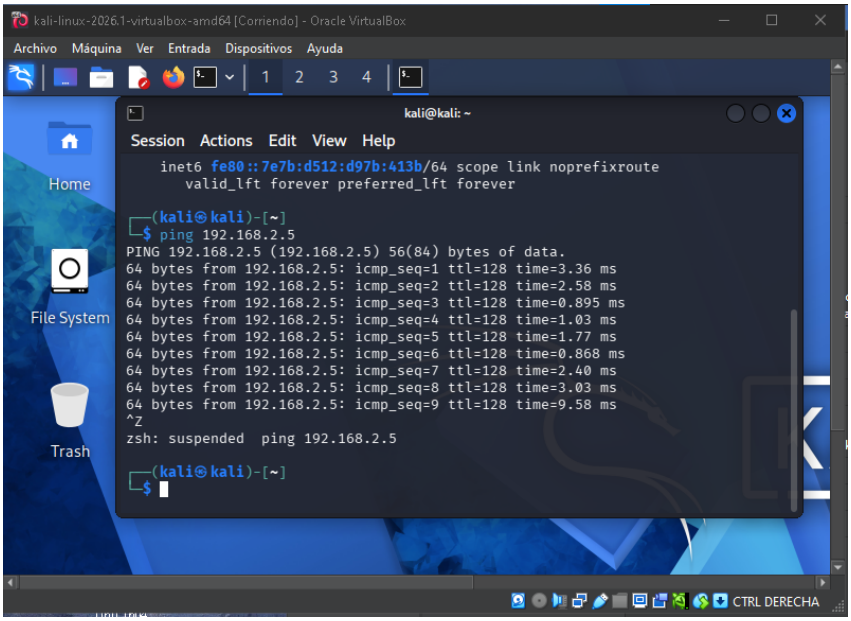
Verificación de la ip asignada a la máquina virtual de kali linux



Nota: Se realizó la verificación de la dirección IP correspondiente a la máquina virtual Kali Linux, cuyo registro se documenta en la imagen adjunta. Autoría propia

Figura 5

Respuesta de conexión del ping realizado a la ip asignada a la máquina virtual de windows



Nota: Se verificó la conectividad a través del comando ping hacia la dirección IP correspondiente a la máquina virtual Windows, obteniendo respuesta exitosa. Autoría propia

Responsabilidad Profesional y Marco Legal en Ciberseguridad

El acuerdo de confidencialidad analizado presenta múltiples inconsistencias tanto en su redacción como en su validez jurídica dentro del ordenamiento colombiano. En primer lugar, se evidencian errores formales, tales como numeración incorrecta y cláusulas incompletas, lo que afecta su claridad e interpretación. Sin embargo, el aspecto más crítico radica en que varias de sus disposiciones contravienen normas constitucionales y legales, lo que podría acarrear su nulidad total o parcial.

En relación con la Cláusula Primera, se establece la prohibición de divulgar información confidencial, incluso aquella relacionada con posibles actividades ilegales dentro de la organización. Esta disposición resulta contraria al orden jurídico colombiano, ya que la Constitución Política de Colombia (1991) establece el deber ciudadano de denunciar conductas delictivas, en particular en su artículo 95. En este sentido, ningún acuerdo privado puede limitar u obstaculizar una obligación de carácter constitucional, lo que convierte esta cláusula en jurídicamente inválida.

Por su parte, la Cláusula Segunda, numeral 2, incluye dentro de la información confidencial datos relacionados con prácticas como interceptaciones ilegales, accesos no autorizados a sistemas informáticos y otras conductas tipificadas como delito. Estas acciones están contempladas en la Ley 1273 de 2009, específicamente en los artículos 269A y 269C. En consecuencia, pretender otorgar carácter confidencial a información obtenida mediante actividades ilícitas implica un objeto ilegal, lo cual genera nulidad desde su origen.

Asimismo, la Cláusula Cuarta, numeral 3, impone la obligación de no reportar ante las autoridades posibles actividades de espionaje o apropiación indebida de información. Esta disposición no solo vulnera nuevamente el deber constitucional de denuncia, sino que también

podría interpretarse como una forma de obstrucción a la justicia. De acuerdo con el Código de Procedimiento Penal Colombiano (Ley 906 de 2004), existe la obligación de informar sobre la comisión de delitos, y su incumplimiento podría derivar en responsabilidades penales, incluso por conductas como el encubrimiento.

De manera similar, la Cláusula Cuarta, numeral 4, insiste en prohibir la denuncia o divulgación de información ilegal conocida por el receptor. Esta disposición refuerza la ilegalidad del acuerdo, ya que pretende limitar derechos y deberes fundamentales, lo cual no es permitido dentro del marco jurídico colombiano.

Finalmente, la Cláusula Octava, en su segunda parte, establece la exoneración de responsabilidad legal y penal de la empresa. Esta afirmación carece de validez jurídica, dado que el principio de responsabilidad penal es personal e intransferible, conforme al Código Penal Colombiano (Ley 906 de 2004). En consecuencia, ninguna persona natural o jurídica puede ser eximida de responsabilidad penal mediante acuerdos privados.

Revisión de los anexos orientada a determinar posibles infracciones a la Ley 1273 y conductas no autorizadas.

Tras revisar el acuerdo de confidencialidad presentado como anexo a la propuesta laboral, se identifican múltiples disposiciones que podrían constituir una vulneración directa del marco normativo colombiano en materia de delitos informáticos. En particular, varias cláusulas hacen referencia a la obligación de mantener en reserva información relacionada con prácticas como interceptación de comunicaciones, accesos no autorizados a sistemas o apropiación indebida de datos, las cuales están tipificadas como conductas delictivas en la Ley 1273 de 2009.

Desde un enfoque jurídico, resulta improcedente establecer acuerdos que pretendan encubrir o dar tratamiento confidencial a información obtenida mediante actividades ilícitas,

tales como “chuzadas” o accesos abusivos a sistemas informáticos. Estas conductas se encuentran sancionadas por la normativa penal vigente, por lo que cualquier disposición contractual que busque protegerlas carece de validez y podría considerarse nula desde su origen.

Asimismo, el acuerdo incluye cláusulas que restringen la posibilidad de denunciar hechos ilícitos ante las autoridades competentes. Esta situación no solo contradice el deber constitucional de denuncia, sino que también podría interpretarse como una forma de encubrimiento o favorecimiento de conductas delictivas. En consecuencia, el documento no solo presenta inconsistencias legales, sino que además expone al firmante a posibles responsabilidades jurídicas.

En síntesis, el análisis permite concluir que el acuerdo contiene elementos que vulneran principios fundamentales del derecho colombiano, especialmente en lo relacionado con la protección de la información y la persecución de delitos informáticos de acuerdo al texto “La naturaleza jurídica de los delitos informáticos en Colombia” de Guarnizo Portela, M. P. (2024), lo que lo convierte en un instrumento de alto riesgo legal.

Estudio de la propuesta laboral enfocado en los aspectos legales y éticos relacionados con su ejecución.

En relación con la propuesta laboral ofrecida, se identifican aspectos que deben ser evaluados tanto desde la legalidad como desde la ética profesional. Aunque la remuneración ofrecida ($15.000.000 mensuales) resulta altamente competitiva, esto no constituye un elemento suficiente para validar condiciones contractuales contrarias a la ley.

En primer lugar, la mención de un “contrato vitalicio” carece de sustento jurídico en el ordenamiento laboral colombiano. La legislación vigente únicamente reconoce figuras como el contrato a término fijo, indefinido o por obra o labor, por lo que la promesa de estabilidad

permanente no tiene respaldo legal y podría interpretarse como una práctica engañosa o imprecisa.

Desde una perspectiva ética, la aceptación de esta oferta implicaría comprometer principios fundamentales del ejercicio profesional. De acuerdo con los lineamientos del COPNIA (2015), el ejercicio de la ingeniería debe regirse por valores como la honestidad, la responsabilidad y el respeto por la ley. En este sentido, firmar un acuerdo que obligue a ocultar actividades ilícitas o a abstenerse de denunciarlas vulnera directamente estos principios.

Adicionalmente, aceptar condiciones que impliquen el manejo o encubrimiento de información obtenida de manera ilegal podría acarrear sanciones disciplinarias, incluyendo la suspensión o cancelación de la matrícula profesional. Esto evidencia que el riesgo no es únicamente legal, sino también reputacional y ético.

Examen del Caso "Ciberespionaje y Ética en SecureNova Labs" bajo Perspectivas Normativas, Legales y Éticas desde la Posición Organizacional.

El análisis del caso de "SecureNova Labs" evidencia la existencia de prácticas contrarias al ordenamiento jurídico colombiano, tales como acuerdos que buscan encubrir información ilícita, restringir la denuncia de delitos o evadir responsabilidades legales. Este tipo de actuaciones no solo carecen de validez jurídica, sino que además representan un riesgo significativo para cualquier profesional vinculado al ámbito de la ciberseguridad. En este contexto, garantizar que el acceso a la información no sea utilizado de manera indebida implica establecer controles estrictos basados en la legalidad, la técnica y la ética profesional.

En primer lugar, desde el punto de vista normativo, el acceso a la información debe regirse por los principios establecidos en la Ley 1581 de 2012. Entre estos principios se destacan la finalidad, que exige que el acceso tenga un propósito legítimo y previamente definido; la

proporcionalidad, que limita el tratamiento a la información estrictamente necesaria; el consentimiento informado, que obliga a contar con autorización expresa del titular de los datos; y la seguridad, que impone la implementación de medidas técnicas y organizativas para proteger la información. Estos elementos constituyen la base legal para evitar el uso indebido de datos sensibles.

Adicionalmente, existen límites claros que no pueden ser vulnerados bajo ninguna circunstancia. De acuerdo con la Ley 1273 de 2009, conductas como el acceso abusivo a sistemas, la interceptación de datos o el daño informático están tipificadas como delitos. Por lo tanto, ninguna organización puede justificar el acceso o tratamiento de información obtenida de manera ilegal, ni mucho menos encubrir este tipo de prácticas mediante acuerdos contractuales.

En segundo lugar, la garantía frente a posibles abusos requiere la implementación de instrumentos contractuales sólidos. Entre ellos, el Acuerdo de Nivel de Servicio (SLA) permite definir condiciones operativas claras, como tiempos de respuesta y responsabilidades; el Acuerdo de Confidencialidad (NDA) regula el tratamiento de la información sensible, estableciendo quién puede acceder y bajo qué condiciones; y la Declaración de Trabajo (SOW) delimita el alcance de las actividades a realizar, evitando excesos o desviaciones en el uso de la información. Estos mecanismos permiten formalizar controles y responsabilidades entre las partes involucradas.

Desde la perspectiva técnica, es indispensable aplicar medidas de seguridad que reduzcan la posibilidad de explotación indebida. Entre las más relevantes se encuentra el principio de privilegio mínimo, que limita los accesos únicamente a los recursos necesarios; la segregación de datos, que protege la información crítica mediante anonimización o uso de entornos controlados; el registro y trazabilidad, que permite auditar todas las acciones realizadas; y el cifrado de la información, tanto en tránsito como en almacenamiento. Asimismo, es fundamental garantizar la

eliminación segura de los datos una vez finalizado el proceso, mediante mecanismos de destrucción certificada.

Finalmente, desde una perspectiva ética, el profesional de ciberseguridad debe actuar conforme a los principios establecidos por el COPNIA (2015), los cuales incluyen la honestidad, la integridad, la responsabilidad y el respeto por la ley. Esto implica no acceder a información sin autorización, no utilizarla para fines distintos a los establecidos y, especialmente, no encubrir actividades ilícitas bajo el argumento de la confidencialidad.

Mecanismos de supervisión y control de ciberseguridad

La prevención del uso no autorizado o éticamente cuestionable de herramientas avanzadas de análisis forense en entornos de ciberseguridad no puede depender de una única medida aislada. Por el contrario, requiere la implementación de un sistema integral de control que articule componentes normativos, técnicos, organizativos y éticos. La ausencia de estos mecanismos, como se evidenció en el caso “SecureNova Labs”, no solo incrementa los riesgos legales, sino que además desvirtúa el propósito esencial de la ciberseguridad: proteger la información y no vulnerarla.

En primer lugar, desde el ámbito normativo, es fundamental establecer instrumentos contractuales claros y exigibles. Documentos como los acuerdos de confidencialidad (NDA), acuerdos de nivel de servicio (SLA) y declaraciones de trabajo (SOW) deben definir con precisión el alcance del acceso, las responsabilidades del personal y las restricciones en el uso de herramientas forenses. Estos instrumentos deben alinearse con principios legales como los establecidos en la Ley 1581 de 2012, garantizando el tratamiento adecuado de la información, y con la Ley 1273 de 2009, que tipifica las conductas relacionadas con el uso indebido de sistemas informáticos.

En segundo lugar, es indispensable implementar controles técnicos robustos que permitan limitar, monitorear y auditar el uso de estas herramientas. Entre las medidas más relevantes se encuentran la aplicación del principio de privilegio mínimo, el uso de sistemas de registro y trazabilidad (logs), la integración con plataformas de monitoreo como SIEM para detectar comportamientos anómalos y la ejecución de procesos de eliminación segura de la información una vez finalizadas las actividades (*SIEM Evaluation Tool | SANS Institute*, 2025). Estos controles permiten no solo prevenir abusos, sino también detectar y responder oportunamente ante posibles incidentes.

Desde la perspectiva organizacional, la gobernanza juega un papel clave. Las empresas deben establecer estructuras de supervisión que incluyan auditorías internas periódicas, controles cruzados entre equipos y la designación de responsables como oficiales de cumplimiento o ética. Estas figuras garantizan que las actividades se desarrollen conforme a la normativa y los estándares profesionales, fortaleciendo la transparencia y la rendición de cuentas.

Adicionalmente, la formación continua del personal es un elemento esencial. Los profesionales deben recibir capacitación constante en aspectos legales, técnicos y éticos, con el fin de comprender no solo cómo funcionan las herramientas forenses, sino también cuáles son los límites de su uso. En este sentido, los lineamientos del COPNIA (2015) refuerzan la importancia de actuar con integridad, responsabilidad y respeto por la ley en el ejercicio profesional.

Finalmente, es imprescindible contar con mecanismos efectivos de denuncia, como líneas éticas confidenciales, políticas de protección al denunciante y procedimientos claros para reportar irregularidades tanto a nivel interno como ante las autoridades competentes. Estos canales permiten detectar prácticas indebidas y actuar de manera oportuna, evitando que situaciones irregulares se perpetúen.

Medidas del descubrimiento de actos de ciberespionaje

El hallazgo de prácticas de ciberespionaje en una empresa de ciberseguridad representa una grave vulneración de la confianza, así como un incumplimiento de principios legales y éticos fundamentales. En este contexto, la respuesta institucional debe ser inmediata, integral y proporcional a la gravedad de los hechos, articulándose en cuatro fases clave: contención, investigación, reparación y prevención.

En primer lugar, la respuesta inmediata debe centrarse en la contención del daño y la preservación de la evidencia digital. Esto implica suspender de forma preventiva los accesos comprometidos, aislar los sistemas afectados y activar protocolos de gestión de incidentes según lo menciona en el texto “The 6 Phases of an Incident Response Plan” de Netalit. (2024). Asimismo, la recolección adecuada de evidencias resulta esencial para garantizar su validez en eventuales procesos judiciales, en concordancia con las conductas tipificadas en la Ley 1273 de 2009, que sanciona el acceso abusivo, la interceptación de datos y otras prácticas ilícitas en entornos digitales.

En segundo lugar, la fase de investigación y sanción debe desarrollarse bajo criterios de transparencia y debido proceso. Es necesario adelantar investigaciones internas y, de ser pertinente, poner los hechos en conocimiento de las autoridades competentes. Las sanciones pueden abarcar ámbitos penales, disciplinarios y contractuales, dependiendo de la responsabilidad individual y organizacional. En este sentido, el deber de denunciar se fundamenta en la Constitución Política de Colombia (1991), el cual no puede ser limitado por acuerdos privados.

En tercer lugar, la reparación y restauración busca mitigar los daños ocasionados a las víctimas y recuperar la confianza afectada. Esto puede incluir la notificación a los titulares de los datos comprometidos, la implementación de medidas correctivas, la compensación por los

perjuicios causados y la adopción de mejores prácticas en el tratamiento de la información, conforme a los principios establecidos en la Ley 1581 de 2012.

Finalmente, la fase de prevención de recurrencia implica una revisión estructural de los procesos internos de la organización. Esto incluye el fortalecimiento de controles técnicos, la actualización de políticas de seguridad, la implementación de auditorías periódicas y la capacitación continua del personal en aspectos legales y éticos. Además, se deben eliminar prácticas irregulares como la inclusión de cláusulas contractuales que pretendan encubrir actividades ilícitas o limitar la denuncia de delitos, ya que estas son contrarias al orden público y carecen de validez jurídica.

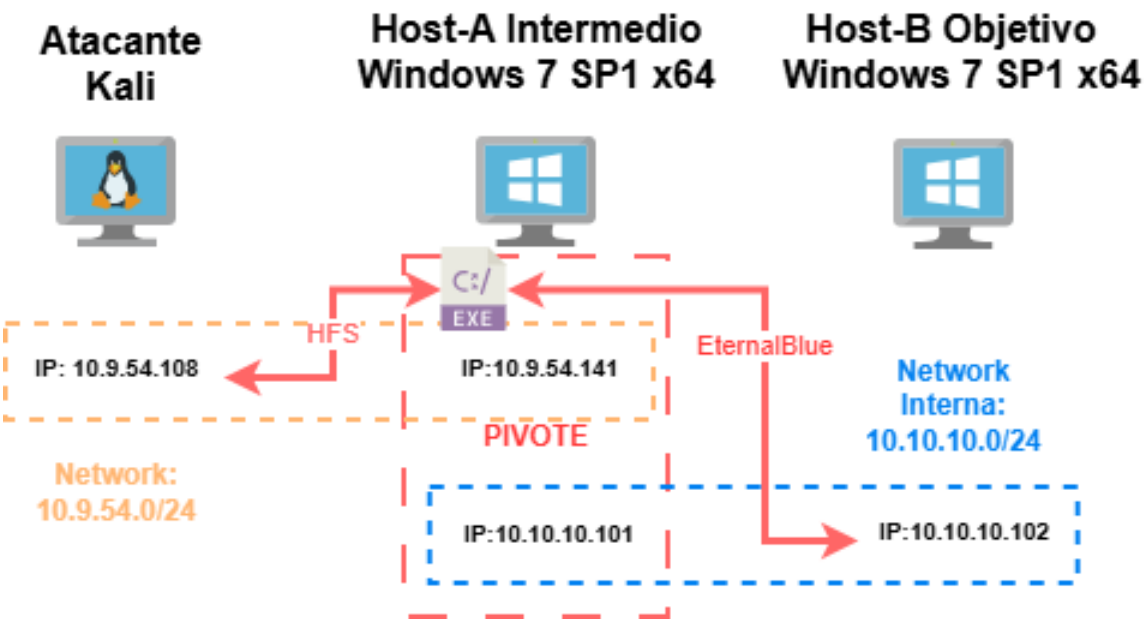
Componente Aplicado: Simulación de Escenarios de Seguridad

En esta fase, el análisis estará orientado al estudio de los entornos Host-A y Host-B con el sistema operativo Windows 7, ambos implementados en VirtualBox, junto con un host Kali. El objetivo será identificar posibles vectores de fuga de información mediante la explotación controlada de una aplicación vulnerable, validando escenarios de escalamiento de privilegios y técnicas de movimiento lateral (pivoting) dentro del entorno simulado es una técnica empleada para expandir el compromiso dentro de una infraestructura corporativa.

Laboratorio "SecureNova Labs"

Figura 6

Topología de red "SecureNova Labs"

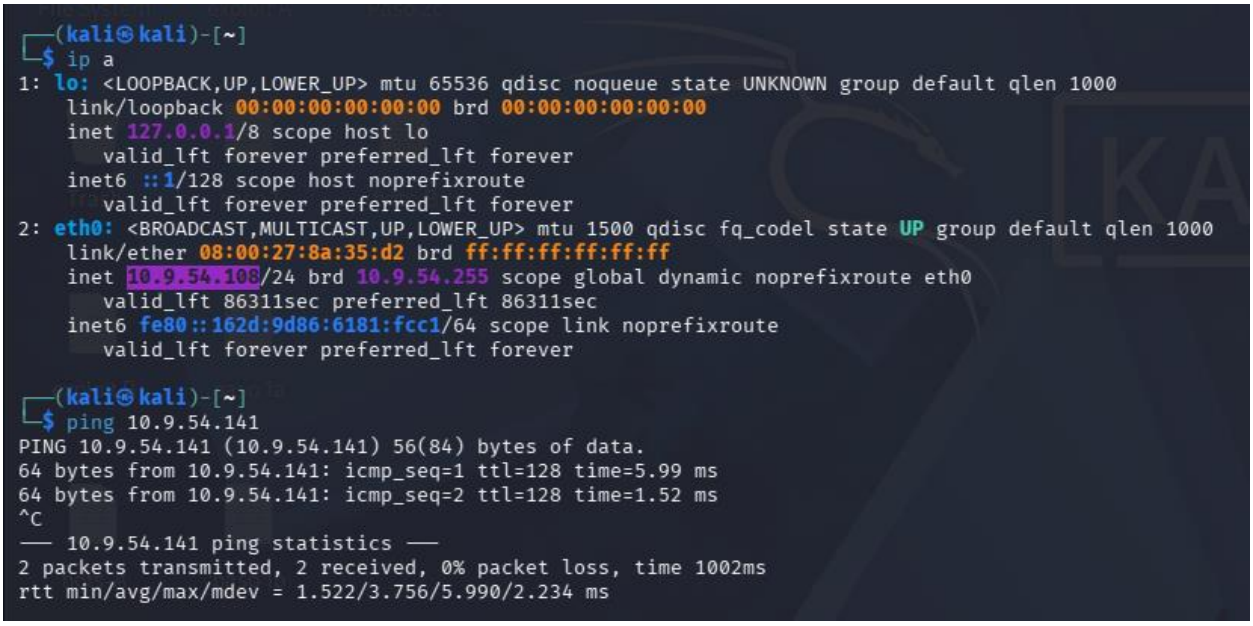


Nota. Esta imagen ilustra el concepto de pivoting. A partir de ella, se identifican tres equipos dentro del escenario: una máquina atacante con dirección IP 10.9.54.108, una primera víctima (Host A) con IP 10.9.54.141, y una segunda víctima (Host B) con IP 10.10.10.102. Autoría propia.

El Host A, correspondiente a la primera víctima, presenta una vulnerabilidad asociada a Rejetto HFS (rejetto_hfs_exec), la cual puede ser explotada para obtener acceso inicial y, posteriormente, facilitar el desplazamiento lateral hacia otros sistemas dentro de la red.

Figura 7

Configuración de red de la máquina atacante kali

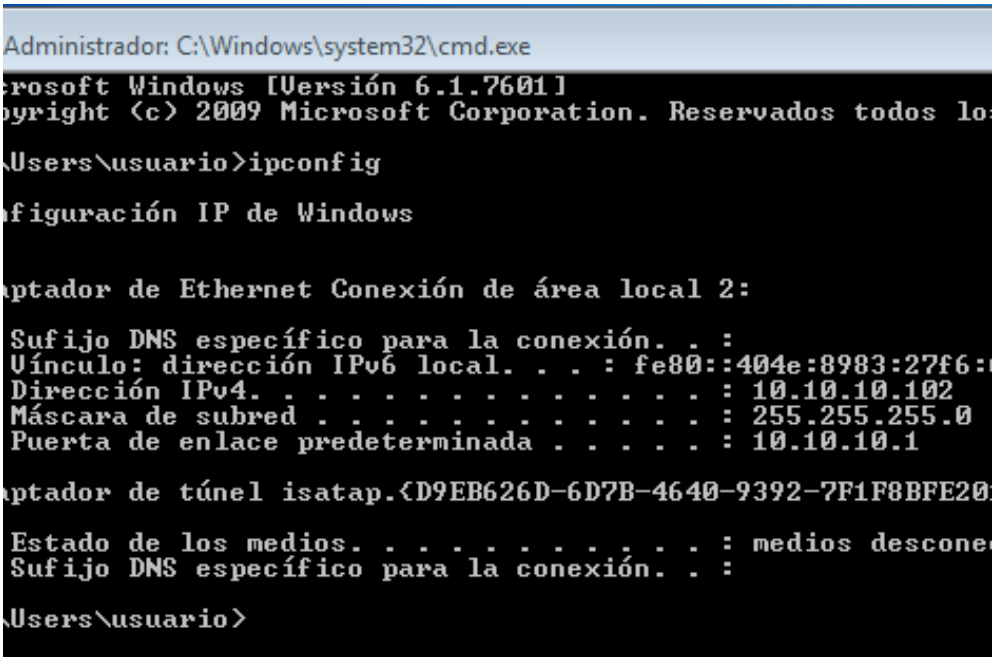


Nota. Se observa que la interfaz eth0 del equipo atacante tiene asignada la dirección IP 10.9.54.108/24. Desde la máquina Kali se realiza un escaneo de la red con el fin de identificar los dispositivos activos, utilizando el comando arp -a. Como resultado, se detecta la máquina víctima 1 (Host A) con dirección IP 10.9.54.141.

Posteriormente, se ejecuta una prueba de conectividad mediante ping, confirmando que Kali tiene comunicación directa con Host A. La imagen presentada es de autoría propia.

Figura 8

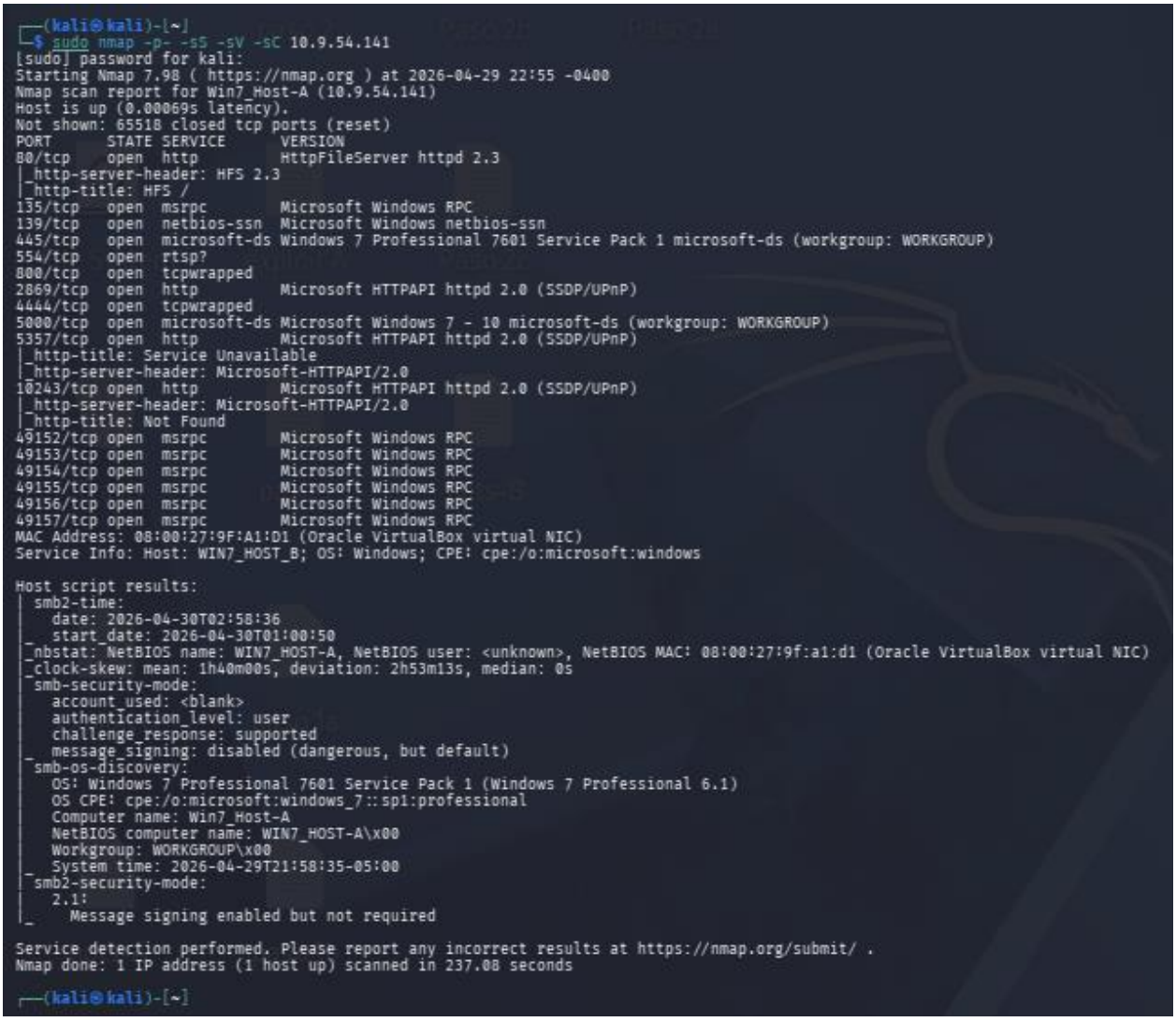
Configuración de red de la máquina host-b



Nota. Se identifica la dirección IP de la máquina víctima 2 (Host B), correspondiente a 10.10.10.102, la cual pertenece a una red interna aislada a la que el equipo Kali no tiene acceso directo. La imagen es de autoría propia.

Figura 9

Escaneo completo de puertos con nmap



Nota. Se presenta la salida del comando nmap ejecutado desde la máquina Kali, donde se identifica el puerto 80 abierto con el servicio HFS 2.3. Asimismo, el puerto 445 se encuentra abierto, lo que sugiere que el sistema operativo corresponde a Windows 7 Professional (versión 7601 con Service Pack 1).

Como información adicional del equipo, se identifica el host PC-HOST-A con dirección IP 10.9.54.141, perteneciente al grupo de trabajo WORKGROUP. La imagen es de autoría propia.

Tabla 1

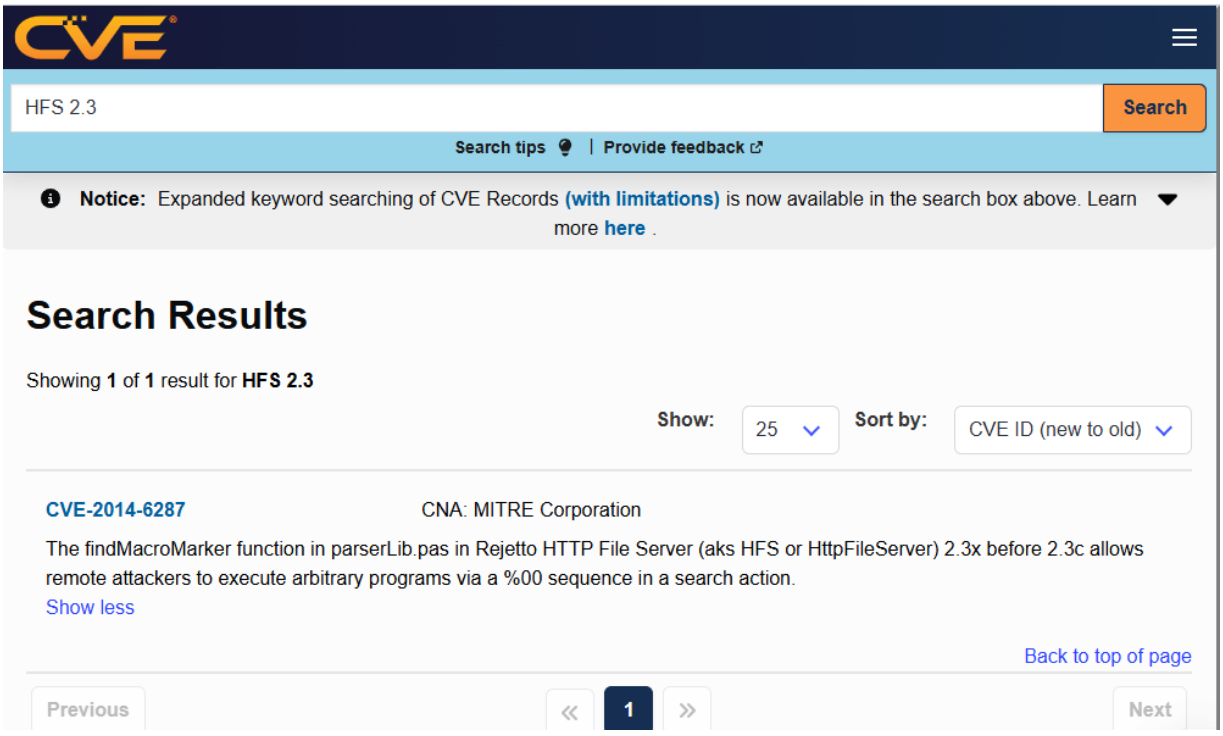
Hallazgos del reconocimiento de puertos

Puertos	Servicios	Observación
80	HTTP (HFS 2.3)	Vector de entrada principal
135, 139, 445	SMB / RPC	Posible escalamiento
5000	microsoft-ds	Alternativo para SMB

Nota. El vector de fuga más probable es la vulnerabilidad de Rejetto HFS 2.3, que permite ejecutar comandos en el sistema remoto.

Figura 10

Búsqueda en la bases de datos de seguridad cve



Nota. En el sitio oficial del programa Common Vulnerabilities and Exposures (CVE) se realizó la búsqueda de la vulnerabilidad asociada a HFS 2.3, considerando que el Host A tenía el puerto

80 abierto ejecutando Rejetto HFS. Como resultado, se identificó la vulnerabilidad CVE-2014-6287, la cual permite a un atacante ejecutar programas de manera arbitraria en el sistema. La imagen es de autoría propia.

HttpFileServer (HFS) versión 2.3 es un servidor web ligero utilizado para compartir archivos. Sin embargo, esta versión presenta una vulnerabilidad crítica que permite la ejecución remota de comandos sin autenticación (CVE-2014-6287). Esto significa que un atacante puede enviar una petición HTTP especialmente manipulada para ejecutar comandos en el sistema afectado sin necesidad de credenciales, comprometiendo completamente su seguridad.

Tabla 2

Hallazgos del reconocimiento del host-a

Elemento identificado	Resultado
IP	10.9.54.141
HOST	PC-HOST-A
Sistema Operativo	Windosws 7 SP1 Profesional
Servicio expuesto	El puerto 80/TCP abierto
Reconocimiento	Identificación de servicio vulnerable HFS 2.3 en Host-A

Nota. Durante la fase de reconocimiento se llevó a cabo la identificación de activos, servicios expuestos y posibles vectores de ataque en el objetivo inicial (Host-A). Los resultados obtenidos permiten establecer con claridad el punto de entrada utilizado posteriormente en la intrusión.

Con el vector de entrada identificado, se procedió a explotar HFS 2.3 utilizando Metasploit. El módulo exploit/windows/http/rejetto_hfs_exec se configuró con los parámetros adecuados y se ejecutó, obteniendo una sesión de Meterpreter en Host-A.

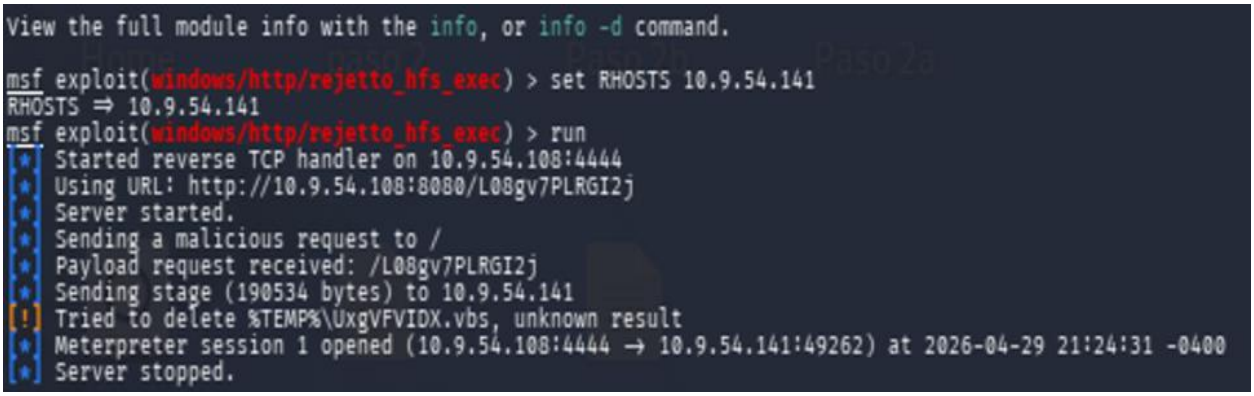
Figura 11

Búsqueda en metasploit framework

Nota. Se realiza la búsqueda de Rejetto HFS en el Metasploit Framework mediante el comando search rejetto, identificando el módulo exploit/windows/http/rejetto_hfs_exec como la primera opción disponible. Posteriormente, se procede a su utilización para la explotación de la vulnerabilidad. La imagen es de autoría propia.

Figura 12

Explotación con metasploit rejetto y la configuración del módulo



Nota. Se configura el módulo estableciendo la opción RHOSTS con la dirección IP de Host A (10.9.54.141). Posteriormente, se verifican los parámetros mediante el comando show options y, una vez confirmada la configuración, se procede a explotar la vulnerabilidad utilizando el comando run o exploit. La imagen es de autoría propia.

El exploit envió una petición HTTP maliciosa al servidor HFS, que ejecutó un script VBS en la carpeta %TEMP%. Este script descargó e inyectó el payload de Meterpreter, estableciendo una conexión reversa (reverse shell) hacia Kali.

Figura 13

Verificación del ingreso a la máquina

Nota. Se realiza la verificación del sistema comprometido mediante Meterpreter, utilizando el comando sysinfo para identificar el sistema operativo y el nombre de la máquina víctima.

Asimismo, se ejecuta el comando ipconfig con el fin de identificar las interfaces de red disponibles. Como resultado, se observa la interfaz 13 con dirección IP 10.10.10.101/24, lo que evidencia la existencia de una red interna adicional susceptible de ser explorada. La imagen es de autoría propia.

El Host A fue comprometido exitosamente mediante la explotación de la vulnerabilidad de Rejetto HFS, estableciendo una sesión activa de Meterpreter:

```
Meterpreter session 1 opened (10.9.54.108:4444 -> 10.9.54.141:49262)
meterpreter > sysinfo
Computer        : WIN7_HOST-A
OS              : Windows 7 (6.1 Build 7601, Service Pack 1)
Architecture    : x64
Meterpreter     : x86/Windows
```

El proceso de explotación se llevó a cabo de la siguiente manera:

El exploit envía una petición HTTP maliciosa al servidor HFS.

El servidor ejecuta un script VBS en la carpeta temporal %TEMP%.

Dicho script descarga e inyecta el payload de Meterpreter.

Finalmente, el Host A establece una conexión de retorno (reverse shell) hacia la máquina Kali, permitiendo el control remoto del sistema comprometido.

La obtención de una sesión de Meterpreter confirmó que la vulnerabilidad era explotable y que el atacante ya tenía control sobre Host-A. Sin embargo, los privilegios iniciales eran limitados (usuario estándar), lo que motivó la necesidad de escalar para ejecutar acciones administrativas.

El acceso inicial permitió ejecutar comandos internos como ipconfig y arp -a, lo que reveló la existencia de una segunda interfaz de red y de un equipo adicional en la red interna (Host-B). Este descubrimiento abrió la puerta al movimiento lateral.

Figura 14

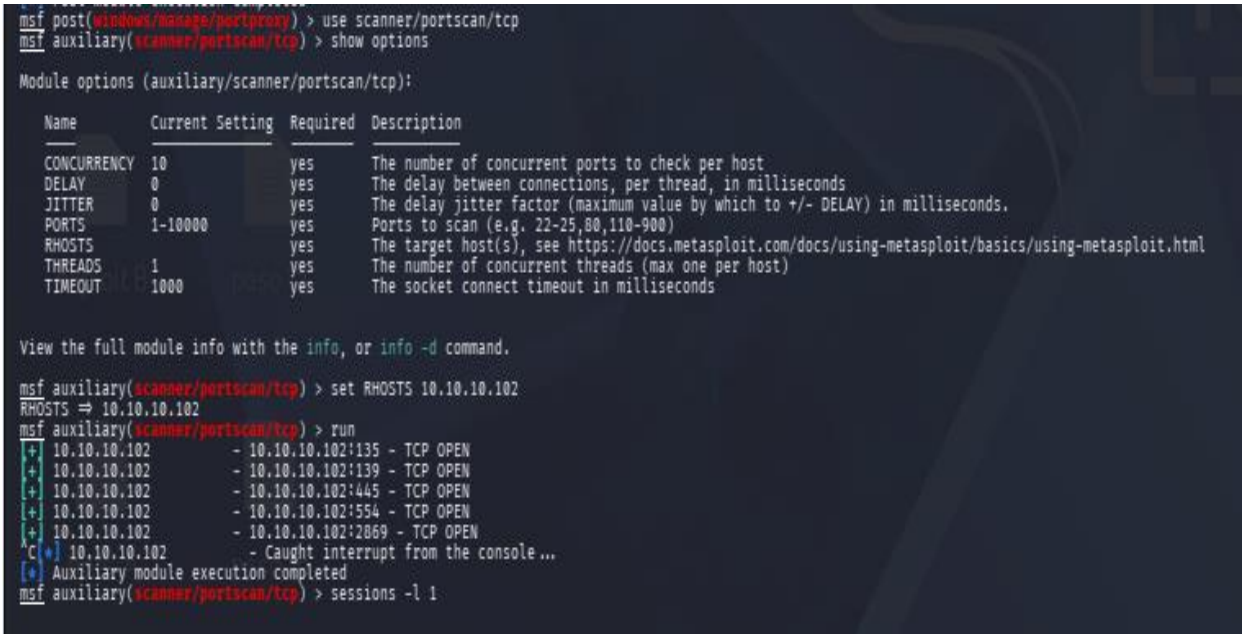
Meterpreter arp -a

Nota. Como parte de la fase de pos-explotación, se realiza la verificación y reconocimiento de redes disponibles desde Host A mediante Meterpreter. Para ello, se utiliza el comando arp -a, el cual permite identificar otros dispositivos con los que el sistema ha tenido comunicación. Como resultado del análisis, se detecta la dirección IP 10.10.10.102, correspondiente a una red interna, lo que permite descubrir la existencia de Host B como un servidor secundario dentro de la infraestructura. Este hallazgo confirma la presencia de un nuevo objetivo potencial para la exploración lateral.

Finalmente, se procede a colocar la sesión en segundo plano utilizando el comando background. La imagen es de autoría propia.

Figura 15

Escaneo de puertos a host-b



Nota. La captura evidencia la fase de reconocimiento activo durante el movimiento lateral, específicamente el escaneo de puertos del Host B a través del pivote previamente establecido en Host A. Para ello, se utiliza el módulo use scanner/portscan/tcp, configurando RHOSTS 10.10.10.102 y ejecutando el comando run.

Como resultado, se identifica el puerto 445/TCP en estado open, asociado a un servicio potencialmente vulnerable a EternalBlue. La imagen es de autoría propia.

Host-A actúa como un punto de pivote (pivot) que conecta la red externa con una red interna no accesible directamente desde Kali.

Figura 16

Preparación del movimiento lateral

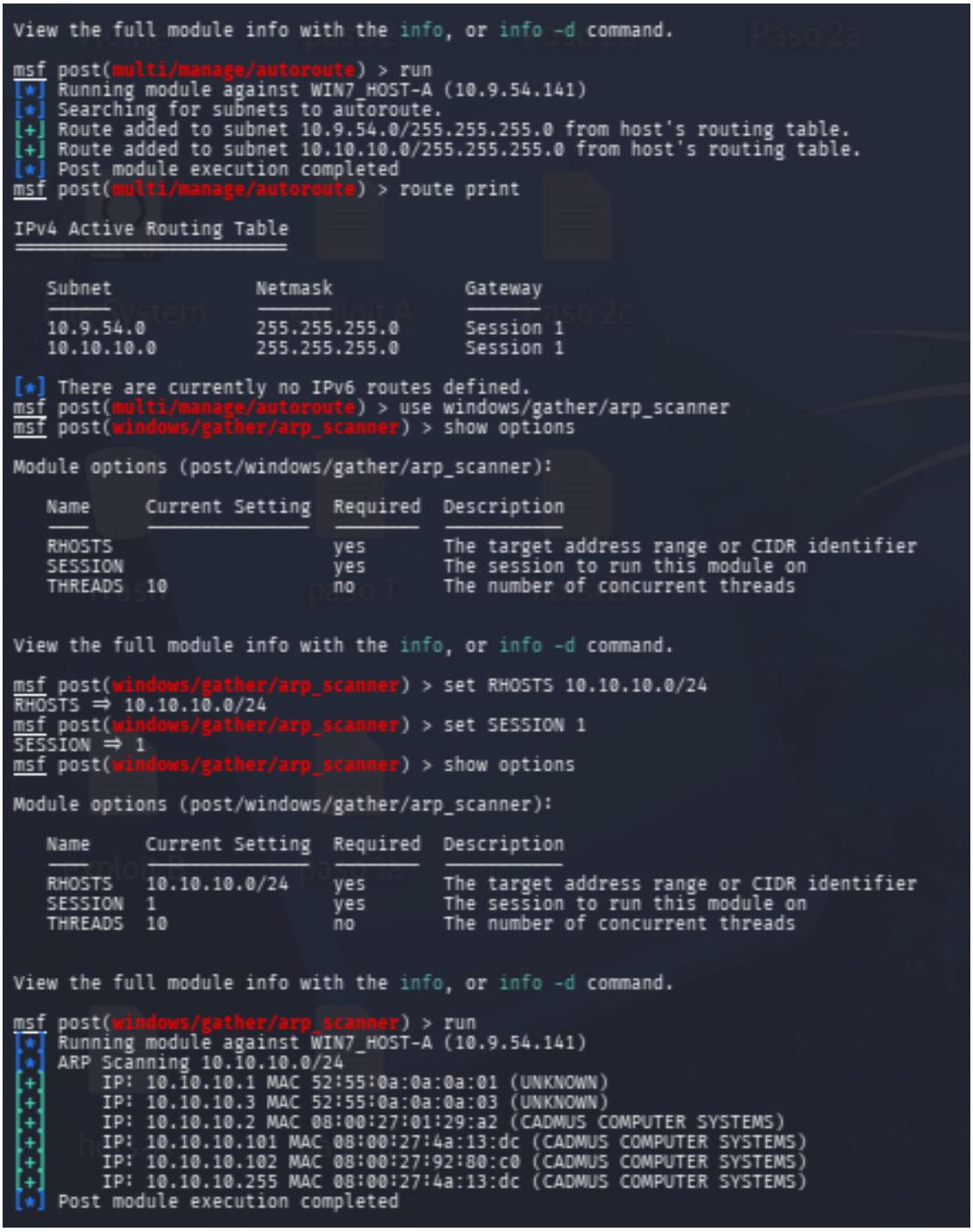
Nota. La captura muestra la fase de preparación del movimiento lateral, específicamente la configuración del módulo autoroute para enrutar el tráfico de Metasploit hacia la red interna 10.10.10.0/24, donde se encuentra el Host B. La imagen es de autoría propia.

El módulo post/windows/manage/autoroute permite agregar las rutas necesarias para que Metasploit pueda alcanzar redes internas no accesibles directamente desde la máquina atacante. En este caso, se han configurado rutas estáticas que indican a Metasploit cómo llegar a la red 10.10.10.0/24 a través de la sesión 1, correspondiente a Host A.

Este procedimiento es fundamental para el pivoting, ya que la máquina Kali no tiene acceso directo a dicha red. Sin embargo, Host A sí dispone de conectividad mediante su interfaz 10.10.10.101, lo que lo convierte en un punto intermedio o puente. En consecuencia, la ruta configurada le indica a Metasploit que, para acceder a cualquier dirección 10.10.10.x, debe utilizar la sesión establecida en Host A como canal de comunicación.

Figura 17

Módulos autoroute y arp



Nota. Se realiza la selección del módulo post/windows/gather/arp_scanner, el cual permite ejecutar un escaneo ARP desde Host A hacia la red especificada. Este tipo de escaneo utiliza el

protocolo ARP (Address Resolution Protocol) para identificar direcciones IP y MAC de los dispositivos activos dentro de la misma red.

Como resultado del análisis, se observa que todas las direcciones MAC comienzan con 08:00:27, lo que confirma que los equipos del laboratorio se encuentran ejecutándose en un entorno de VirtualBox. La imagen es de autoría propia.

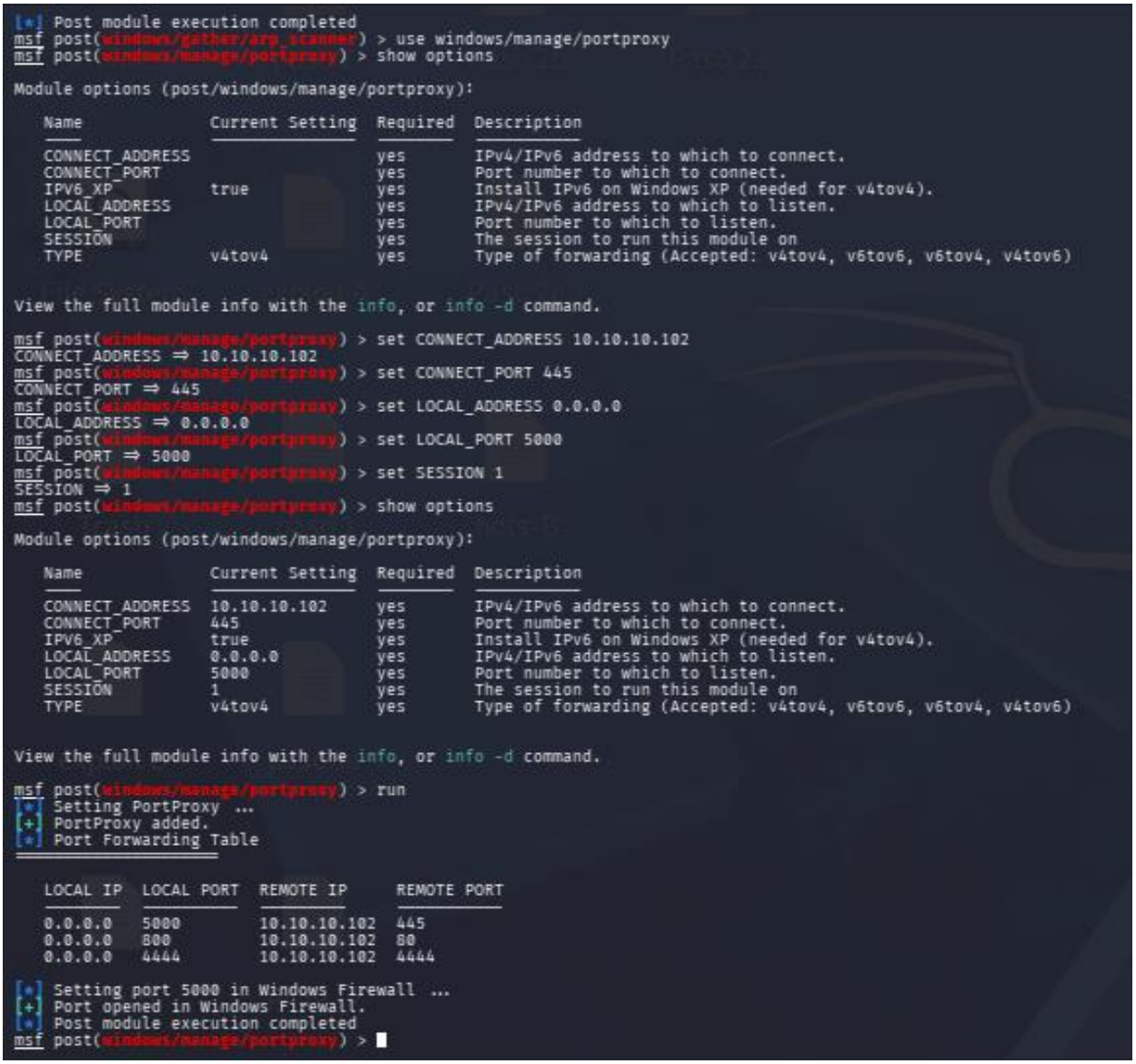
La red interna 10.10.10.0/24 está mal segmentada, permitiendo que un equipo externo comprometido tenga visibilidad y alcance hacia servidores internos sensibles.

La identificación de Host-B justificó la configuración de un mecanismo de redirección de puertos (portproxy) para dirigir tráfico hacia Host-B, habilitando así el movimiento lateral.

Para establecer un túnel hacia Host-B, se utilizó el módulo post/windows/manage/portproxy, que crea reglas de redirección de puertos utilizando el comando nativo netsh interface portproxy. La regla configurada redirigía el tráfico del puerto 5000 de Host-A al puerto 445 de Host-B.

Figura 18

Módulo portproxy



Nota. La captura muestra la configuración exitosa de portproxy en Host A, un paso crítico para el movimiento lateral hacia Host B. Esta acción permite redirigir el tráfico SMB desde Host A hacia Host B, facilitando así la explotación remota. La imagen es de autoría propia.

Para ello, se utiliza el módulo post/windows/manage/portproxy, el cual permite crear reglas de redirección de puertos de forma nativa en el sistema operativo Windows. Este mecanismo constituye una técnica de pivoting que no requiere herramientas externas.

La correcta configuración de los parámetros es fundamental para establecer la conexión y verificar el redireccionamiento del puerto 445, potencialmente vulnerable a EternalBlue. Adicionalmente, el módulo crea una regla de entrada en el firewall de Windows de Host A, permitiendo que las conexiones externas (desde Kali) lleguen al puerto configurado; sin esta regla, el tráfico sería bloqueado.

Los parámetros configurados son los siguientes:

CONNECT_ADDRESS: 10.10.10.102 → Corresponde a Host B en la red interna.

CONNECT_PORT: 445 → Puerto SMB potencialmente vulnerable.

LOCAL_ADDRESS: 0.0.0.0 → Escucha en todas las interfaces de Host A.

LOCAL_PORT: 5000 → Puerto al que Kali enviará el ataque.

SESSION: 1 → Utiliza la sesión activa de Meterpreter.

Esta configuración permite que cualquier conexión dirigida al puerto 5000 de Host A sea redirigida internamente al puerto 445 de Host B, habilitando así el acceso indirecto al objetivo dentro de la red aislada.

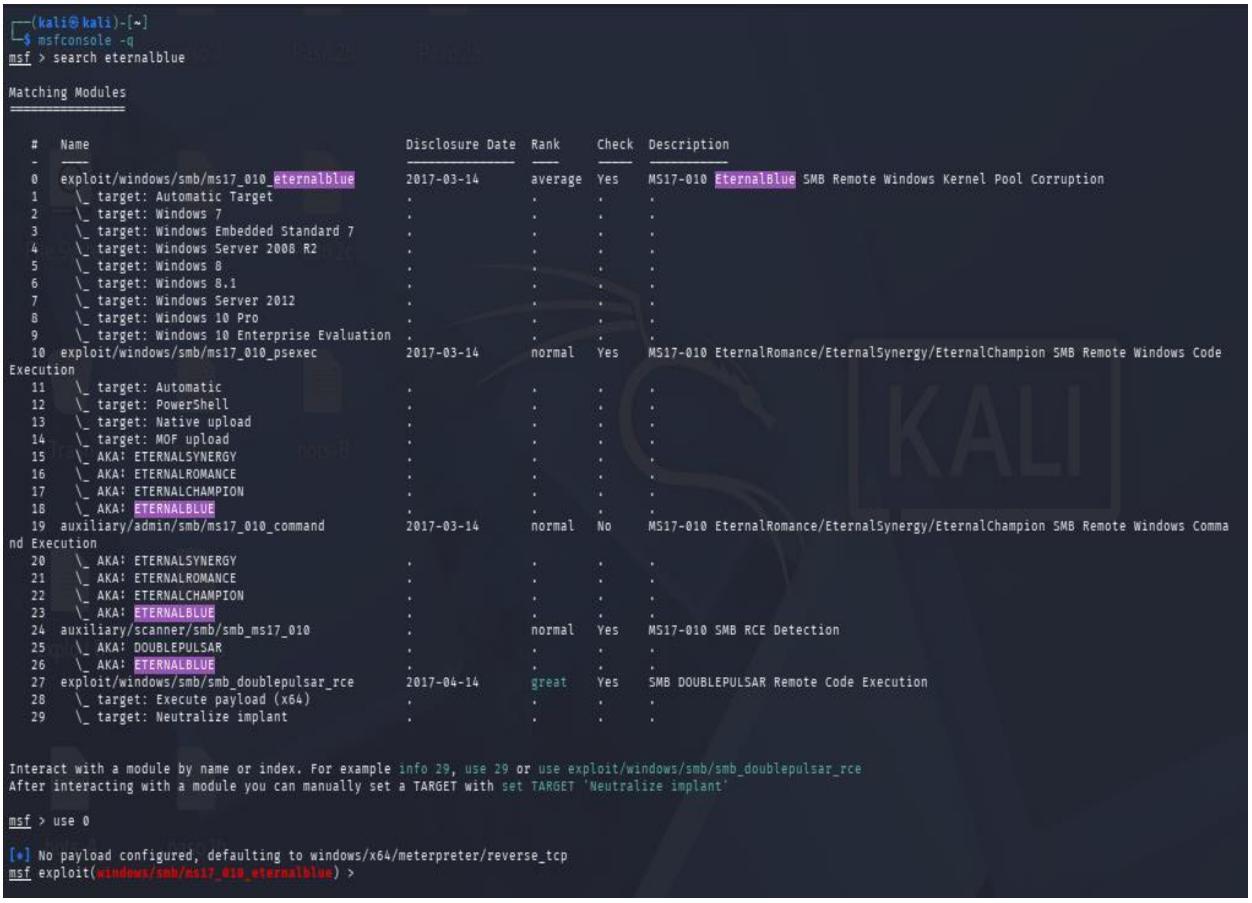
Este paso convirtió a Host-A en un proxy, habilitando el acceso indirecto a Host-B. Sin esta configuración, el atacante no habría podido interactuar con Host-B debido a la falta de conectividad directa.

Con el portproxy activo, el siguiente paso lógico fue atacar el servicio SMB de Host-B utilizando EternalBlue, aprovechando que el puerto 445 estaba abierto y probablemente vulnerable.

Desde una nueva terminal de Metasploit, se ejecutó el exploit exploit/windows/smb/ms17_010_eternalblue apuntando a 10.9.54.141:5000, Figuras 19 y 20. El portproxy redirigió el tráfico hacia 10.10.10.102:445.

Figura 19

Exploit eternalBlue en metasploit



Nota. Esta captura representa el inicio de la fase de movimiento lateral hacia Host B, específicamente la búsqueda del módulo EternalBlue y la preparación del ataque, aprovechando la configuración previa de portproxy en Host A. La imagen es de autoría propia.

Dado que el portproxy ya se encuentra configurado en Host A (0.0.0.0:5000 → 10.10.10.102:445), el siguiente paso consiste, desde otra terminal, en realizar la búsqueda del

exploit EternalBlue dentro de Metasploit. Esto permite preparar el ataque contra Host B a través del canal previamente establecido.

Como resultado, se obtiene una lista de módulos asociados a la vulnerabilidad MS17-010, seleccionando el módulo exploit/windows/smb/ms17_010_eternalblue, el cual será utilizado para la explotación. Este procedimiento forma parte esencial de la fase de movimiento lateral dentro del proceso de intrusión.

Figura 20

Configuración exploit eternalBlue

Nota. La captura muestra la configuración final del exploit EternalBlue para atacar al Host B a través del portproxy previamente establecido en Host A. La imagen es de autoría propia.

En esta configuración, el ataque se dirige hacia Host-A a través del puerto 5000, el cual redirige internamente al Host-B (puerto 445). Se emplea un payload de tipo reverse_tcp, permitiendo que la conexión remota retorne hacia la máquina Kali, la cual se encuentra a la escucha en el puerto 5555.

Con esta preparación, se procede a ejecutar el exploit y completar el proceso de movimiento lateral, comprometiendo el Host B desde el acceso previamente obtenido en Host A.

Figura 21

Establecimiento de conexión

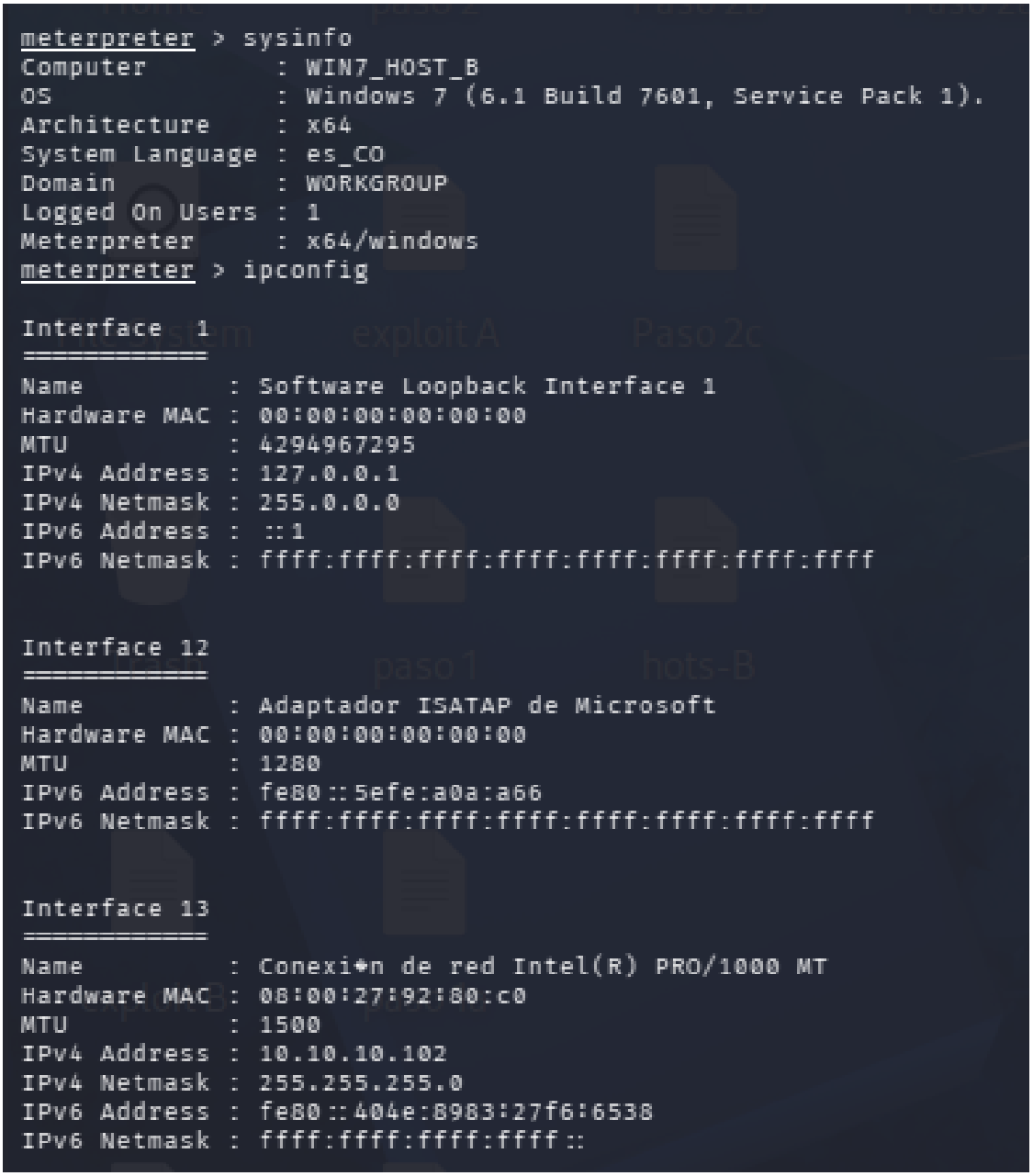
Nota. La captura evidencia la ejecución exitosa del exploit EternalBlue contra Host-B a través del portproxy configurado en Host-A. En consecuencia, el proceso de movimiento lateral se ha completado satisfactoriamente. La imagen es de autoría propia.

Se abrió una sesión de Meterpreter en Host-B, confirmando el control total sobre el servidor interno.

Este hallazgo demostró que: Host-B carecía del parche de seguridad MS17-010, a pesar de ser un sistema crítico. La segmentación de red era insuficiente, permitiendo que un atacante comprometiera un servidor interno a través de un equipo periférico. El movimiento lateral era viable, confirmando la escalabilidad del ataque dentro de la organización

Figura 22

Meterpreter sysinfo

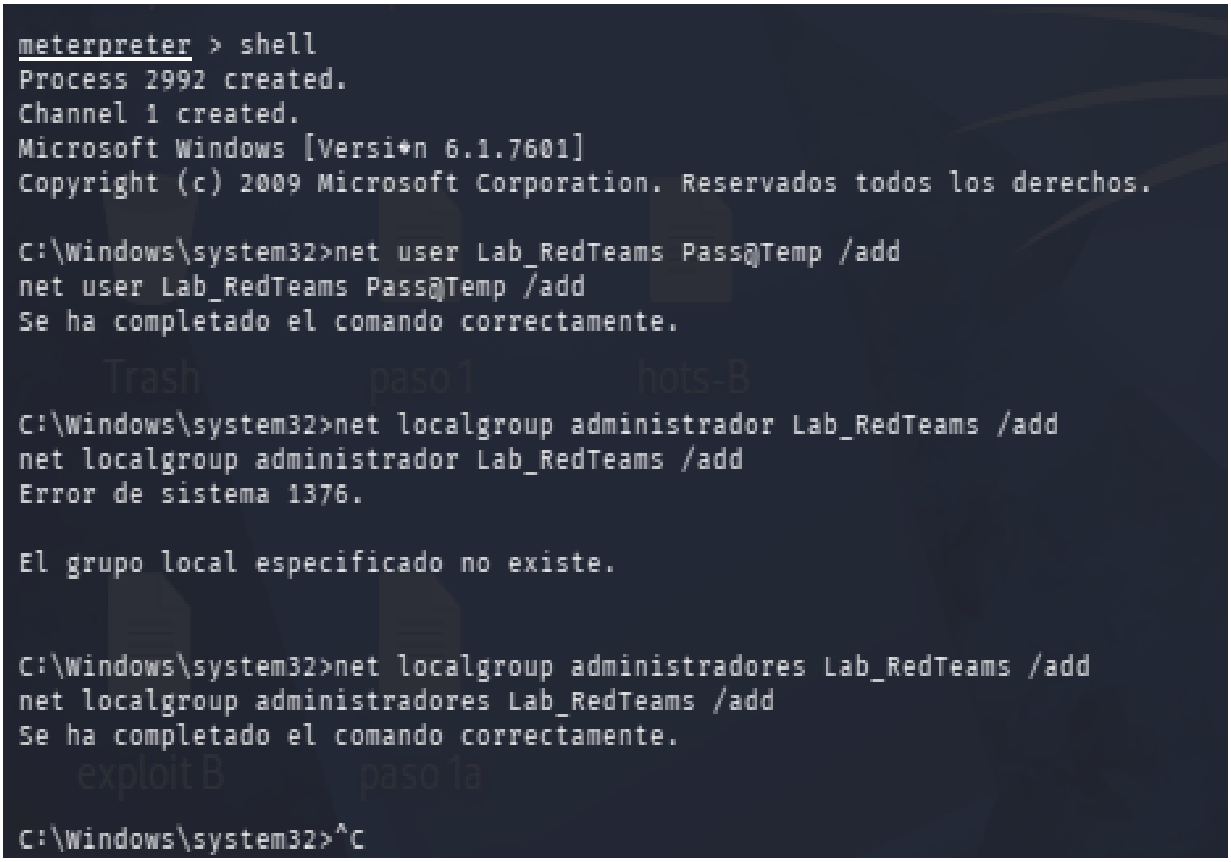


Nota. La captura muestra la fase de pos-explotación en Host-B, confirmando que el movimiento lateral se realizó con éxito y que se ha obtenido control sobre la máquina objetivo. La imagen es de autoría propia.

Como paso final, se ejecutó una prueba de concepto controlada: la creación de una cuenta administrativa en Host-B con el formato Lab_RedTeams,

Figura 23

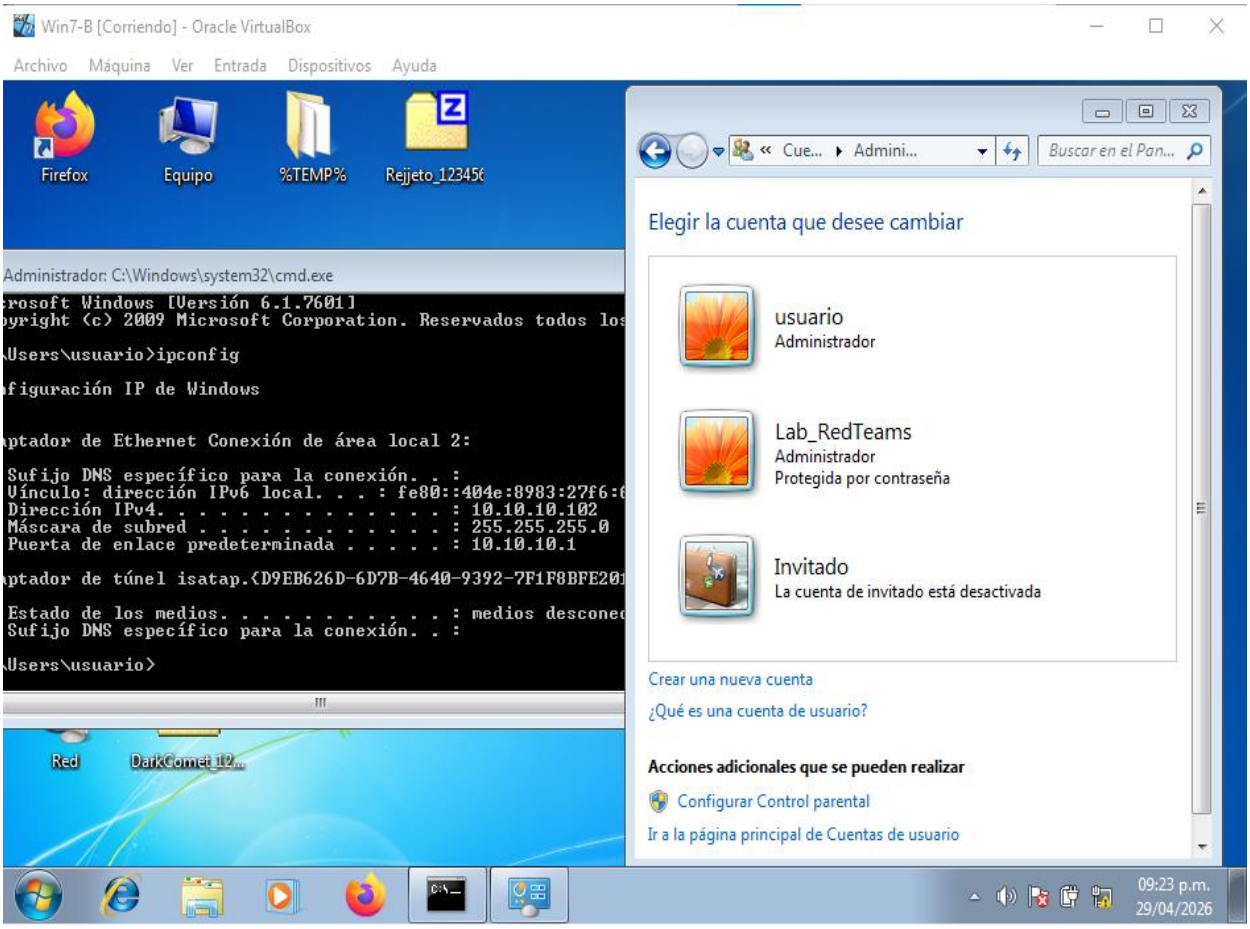
Creación del usuario en host-b



Nota. La captura muestra la fase final de pos-explotación en Host B, donde se ejecuta la prueba de concepto (PoC) solicitada por “SecureNova Labs”, consistente en la creación de una cuenta con privilegios administrativos denominada Lab_RedTeams. La imagen es de autoría propia.

Figura 24

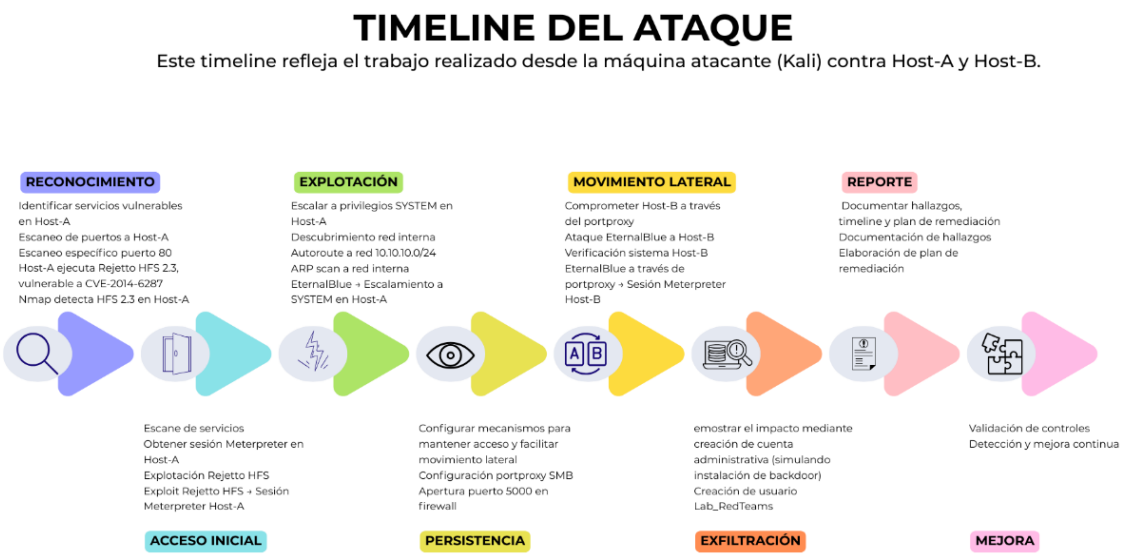
Windows host-b



Nota. La captura muestra la verificación visual, en el escritorio de Host-B, de que la cuenta Lab_RedTeams fue creada exitosamente y cuenta con privilegios de administrador, cumpliendo así con la prueba de concepto (PoC) solicitada por “SecureNova Labs”. La imagen es de autoría propia.

Figura 25

Timeline



Nota. En la línea de tiempo (timeline) se evidencia el avance estructurado del ataque: desde el reconocimiento del servicio HFS 2.3, el acceso inicial mediante la explotación de Rejetto, la escalada de privilegios utilizando EternalBlue hasta obtener acceso como SYSTEM, la configuración de portproxy, el movimiento lateral hacia otros sistemas y, finalmente, la creación de un usuario con privilegios administrativos. La imagen es de autoría propia.

Estrategias De Remediación Del Equipo Blue Team

Con base en la cadena de ataque demostrada en el laboratorio, se recomienda la implementación de un conjunto de estrategias integrales orientadas a remediar las vulnerabilidades identificadas y prevenir incidentes futuros. Estas acciones deben abordarse desde un enfoque técnico, organizacional y preventivo.

Es fundamental establecer un programa continuo de gestión de vulnerabilidades que incluya escaneos periódicos, priorización de riesgos críticos y aplicación oportuna de parches de seguridad. En este contexto, se recomienda:

- Eliminar o actualizar Rejetto HFS a una versión parcheada (superior a 2.3).
- Aplicar los parches de seguridad KB4012212 / KB4012215 en todos los sistemas Windows.
- Deshabilitar el protocolo SMBv1 en toda la infraestructura.
- Migrar sistemas Windows 7 a versiones con soporte vigente.

Se debe implementar una arquitectura de red segmentada que limite el movimiento lateral y reduzca la superficie de ataque. Para ello:

- Separar las redes en zonas: externa, DMZ, interna y crítica.
- Implementar firewalls perimetrales e internos con reglas específicas y restrictivas.
- Monitorear y auditar configuraciones como portproxy.
- Restringir la modificación de configuraciones de red únicamente a administradores autorizados.

El endurecimiento (hardening) de los sistemas operativos debe realizarse siguiendo estándares reconocidos como CIS Benchmarks y Microsoft Security Baselines. Entre las acciones clave se incluyen:

- Deshabilitar servicios inseguros o innecesarios (SMBv1, NetBIOS, entre otros).
- Configurar el Windows Firewall con reglas de entrada restrictivas.
- Establecer políticas seguras para la ejecución de scripts (PowerShell, VBS).

- Implementar políticas de contraseñas robustas y mecanismos de bloqueo de cuentas.
- Habilitar auditorías de eventos de seguridad (creación de usuarios, cambios en grupos, modificaciones del firewall).

Es recomendable implementar un Centro de Operaciones de Seguridad (SOC), ya sea interno o externalizado, con capacidades de monitoreo continuo (24/7) y herramientas avanzadas de detección:

- Implementar solución EDR/XDR (CrowdStrike, SentinelOne, Microsoft Defender for Endpoint).
- Configurar reglas de correlación para alertar sobre: accesos anómalos a puertos administrativos, creación de cuentas no autorizadas (Event ID 4720), cambios en grupos privilegiados (Event ID 4728/4732), modificaciones en firewall y portproxy (Event ID 5157).
- Establecer un proceso de respuesta a incidentes con tiempos definidos (detección, contención, erradicación, recuperación).
- Alinear la gestión de seguridad con estándares internacionales como ISO 27001 y NIST.

La gestión de identidades y accesos debe basarse en el principio de mínimo privilegio, complementado con esquemas de acceso temporal:

- Auditar periódicamente las cuentas locales y los miembros del grupo de administradores.
- Eliminar cuentas inactivas o no autorizadas.

- Implementar cuentas de servicio administradas para evitar el uso de credenciales estáticas.
- Habilitar autenticación multifactor (MFA) en todas las cuentas, especialmente las privilegiadas.
- Monitorear la creación y modificación de usuarios mediante eventos de seguridad

Gestión y mitigación de amenazas de seguridad informática

Investigación y Contención

Basado en el Plan de Respuesta a Incidentes alineado con el "NIST Cybersecurity Framework (CSF) 2.0 NIST SP 800-61 Rev. 3 (2025)", el enfoque del equipo Blue Team de "SecureNova Labs" se orienta a la prevención, detección, contención, erradicación y recuperación frente a amenazas de ciberseguridad, cubriendo las funciones de Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. Este modelo permite gestionar incidentes de manera estructurada, garantizando la continuidad operativa, el resguardo de la información y el mantenimiento íntegro de la evidencia digita.

Como parte inicial del proceso, ante la detección de un posible incidente, se procede a la creación de un evento o ticket mediante la plataforma de Help Desk o sistema de gestión de incidencias, donde el caso es registrado, categorizado y priorizado de acuerdo con su criticidad, impacto y nivel de urgencia. Posteriormente, se realiza el análisis del comportamiento anómalo con el fin de determinar si se trata de un falso positivo o de un incidente real que pueda comprometer los principios de Confidencialidad, Integridad y Disponibilidad (CID) de la información.

Una vez confirmada la incidencia, se define el tipo de evento de seguridad y se clasifica conforme a los procedimientos establecidos por el equipo de respuesta. En esta fase se determina el nivel de severidad (alto, medio o bajo), el alcance del incidente, la posible propagación, persistencia y afectación sobre los activos tecnológicos y servicios críticos. De igual manera, se identifican los sistemas afectados, aplicaciones sensibles y dependencias operativas, activando formalmente el Plan de Respuesta a Incidentes y el protocolo de comunicación hacia las partes interesadas.

Como medida inmediata de contención, se solicita autorización a las áreas responsables para ejecutar acciones de aislamiento y sanitización. Técnicamente, esto implica desconectar el sistema comprometido de la red para evitar movimiento lateral, exfiltración de información o escalamiento del ataque. Dependiendo de la criticidad del incidente, puede realizarse la segmentación temporal del entorno afectado mediante reglas restrictivas en firewalls, redirección controlada del tráfico o bloqueo total de comunicaciones externas, validando además que no existan canales alternos físicos o lógicos que permitan persistencia o fuga de información.

De manera complementaria, se procede al aislamiento de los activos críticos y de la información sensible comprometida, así como al bloqueo de accesos, revocación y cambio de credenciales, fortalecimiento de los mecanismos de autenticación y aplicación inmediata de parches de seguridad. En caso de evidenciarse movimiento lateral, se refuerzan las políticas de segmentación de red que limita la propagación de amenazas entre entornos críticos y control de accesos con el fin de contener la propagación de la amenaza dentro de la infraestructura tecnológica. Asimismo, si la arquitectura de seguridad lo permite, pueden implementarse mecanismos como DNS Sinkholing para redirigir el tráfico malicioso hacia direcciones controladas, facilitando su análisis y mitigación. Finalmente, el incidente debe escalarse oportunamente al equipo especializado CIRT/CSIRT para dar continuidad al proceso de respuesta, análisis forense y recuperación.

Todas las actividades de contención deben ejecutarse preservando la integridad de la evidencia digital. Por ello, antes de alterar el sistema comprometido, se realiza la recolección de evidencia volátil y no volátil para su posterior análisis forense. La adquisición de evidencia incluye la captura de memoria RAM mediante herramientas como Volatility o FTK Imager, así como la clonación bit a bit de discos duros utilizando herramientas forenses certificadas, garantizando una copia exacta del medio original.

Posteriormente, las evidencias recolectadas son aseguradas mediante funciones criptográficas hash, tales como MD5, SHA-1 o SHA-256, con el propósito de preservar la integridad, autenticidad y cadena de custodia de la información digital. Este procedimiento resulta fundamental para soportar procesos legales, regulatorios, auditorías o investigaciones internas derivadas del incidente.

Superada la fase de contención, se inicia el proceso de erradicación, orientado a eliminar completamente la amenaza de los sistemas afectados. Esto incluye la remoción de malware mediante herramientas antivirus, EDR o XDR, eliminación manual de artefactos maliciosos, aplicación de actualizaciones de seguridad, hardening de sistemas operativos y servicios, cierre de puertos innecesarios y reinstalación controlada de equipos comprometidos cuando sea requerido. Así mismo, se valida que las copias de seguridad utilizadas para restauración no hayan sido afectadas por el incidente antes de su puesta en producción.

La fase de recuperación tiene como objetivo restablecer los servicios afectados garantizando que el entorno se encuentre completamente seguro y estable. Durante esta etapa se valida el correcto funcionamiento de aplicaciones, servicios y procesos críticos, se monitorean eventos de seguridad, se revisan logs y se verifican posibles cuentas no autorizadas, procesos anómalos o mecanismos de persistencia que puedan comprometer nuevamente la operación.

Finalmente, en la etapa de posincidente y lecciones aprendidas, se realiza la consolidación de bitácoras, evidencias, indicadores y acciones ejecutadas durante todo el ciclo de atención. El propósito de esta fase es identificar causas raíz, evaluar la efectividad de la respuesta, documentar oportunidades de mejora y fortalecer los controles preventivos y correctivos para evitar incidentes similares en el futuro. Como resultado, se genera un informe técnico de posincidente que retroalimenta el Plan de Respuesta a Incidentes, actualiza

procedimientos internos y comunica formalmente los hallazgos y recomendaciones a las partes interesadas.

Estrategias para Prevenir Recurrencia de Ataques

Teniendo en cuenta el ejercicio desarrollado por el equipo Red Team y los hallazgos identificados durante la simulación de ataque, el enfoque del Blue Team debe orientarse al fortalecimiento de la postura defensiva mediante estrategias de hardening, segmentación de red y reducción de la superficie de ataque como lo contempla en el texto "Blue team red team approach to hardware trust assessment" de Rajendran, J., Jyothi, V., & Karri, R. (2011). El objetivo principal es minimizar la probabilidad de explotación de vulnerabilidades, limitar el movimiento lateral dentro de la infraestructura y fortalecer los controles de acceso y monitoreo de la organización.

Como medida prioritaria, se recomienda la implementación de una arquitectura de microsegmentación de red soportada por firewalls de nueva generación (NGFW), permitiendo aislar servicios críticos y controlar el tráfico este-oeste entre segmentos internos. Esta estrategia debe complementarse con la adopción de un modelo de seguridad Zero Trust, bajo el principio de "nunca confiar, siempre verificar", garantizando validación continua de usuarios, dispositivos y aplicaciones antes de permitir el acceso a recursos corporativos.

Adicionalmente, resulta fundamental realizar una evaluación técnica de la configuración de los equipos de red, sistemas operativos y versiones de firmware instaladas, identificando configuraciones inseguras, software obsoleto y vulnerabilidades conocidas que puedan ser utilizadas como vectores de ataque. En este contexto, se recomienda fortalecer la seguridad perimetral mediante un esquema de defensa en profundidad, incorporando múltiples capas de protección tales como firewalls, IDS/IPS, WAF, segmentación lógica, filtrado DNS y controles de acceso centralizados.

Desde la perspectiva de gestión de identidades y accesos, se debe ejecutar una revisión integral de credenciales, eliminando cuentas no autorizadas, cuentas huérfanas o privilegios excesivos. Es indispensable implementar mecanismos de autenticación multifactor (MFA) y restringir el uso de cuentas con privilegios administrativos únicamente a personal autorizado y bajo esquemas de control y trazabilidad. Así mismo, se recomienda aplicar estrictamente el Principio de Menor Privilegio (Least Privilege), auditando periódicamente qué usuarios y aplicaciones tienen acceso a recursos críticos y ajustando los permisos conforme a las funciones reales de cada rol.

En cuanto al endurecimiento de infraestructura (hardening), se recomienda deshabilitar puertos, protocolos y servicios innecesarios tanto en estaciones de trabajo como en servidores y dispositivos de red. La segmentación lógica mediante VLANs permitirá separar entornos administrativos, operativos, servidores y usuarios finales, reduciendo el riesgo de propagación de amenazas dentro de la organización. De igual forma, se sugiere restringir o deshabilitar el uso de dispositivos USB y medios removibles, mitigando riesgos asociados a malware, fuga de información o ejecución de código malicioso.

Otro componente crítico corresponde a la actualización y estandarización tecnológica de la plataforma corporativa. Se recomienda mantener sistemas operativos, aplicaciones y firmware permanentemente actualizados, aplicando políticas de gestión de parches y remediación de vulnerabilidades. Como referencia técnica, es recomendable adoptar los lineamientos del “Center for Internet Security” (CIS) para la implementación de configuraciones seguras basadas en benchmarks reconocidos internacionalmente.

Finalmente, para fortalecer las capacidades de detección y respuesta, se recomienda el despliegue de una plataforma SIEM “Security Information and Event Management” que permita

centralizar logs, correlacionar eventos de seguridad y generar alertas tempranas ante comportamientos anómalos. Esta solución debe complementarse con la validación periódica del licenciamiento, estado operativo de antivirus/EDR y controles de monitoreo continuo, asegurando una visibilidad integral sobre la infraestructura tecnológica y mejorando la capacidad de respuesta ante incidentes de ciberseguridad.

Blue Team Proactivo vs. Equipo de Respuesta Reactivo en Ciberseguridad

El Blue Team, o línea defensiva de ciberseguridad, tiene un enfoque preventivo y continúo orientado a fortalecer la postura de seguridad de la organización mediante la implementación de controles de protección, monitoreo, detección, contención y remediación de amenazas (NIST, 2023). Su función principal consiste en reducir la superficie de ataque, supervisar constantemente la infraestructura tecnológica, identificar comportamientos anómalos y aplicar medidas de hardening, segmentación, gestión de vulnerabilidades y monitoreo de eventos de seguridad para prevenir incidentes antes de que impacten la operación.

Por otro lado, un equipo de Respuesta a Incidentes Informáticos (CIRT/CSIRT) corresponde a un grupo especializado con un enfoque principalmente reactivo, encargado de gestionar incidentes de ciberseguridad una vez estos han sido detectados o confirmados. Sus responsabilidades incluyen la investigación técnica del incidente, análisis forense, contención avanzada, erradicación de la amenaza, recuperación de servicios y preservación de evidencias digitales, garantizando además la coordinación de la respuesta técnica, operativa y comunicacional frente a eventos que comprometan la seguridad de la información.

En este contexto, mientras el Blue Team trabaja de forma permanente en la prevención y defensa proactiva de la infraestructura, el CIRT/CSIRT actúa como un componente especializado

de respuesta y recuperación ante incidentes confirmados, complementando la estrategia integral de ciberseguridad de la organización.

CIS Benchmarks en el Hardening Defensivo

Resulta fundamental que el equipo Blue Team adopte y aplique los estándares y buenas prácticas definidas por el Center for Internet Security (CIS), orientadas al hardening y fortalecimiento de la seguridad de la infraestructura tecnológica. La implementación de los CIS Controls y CIS Benchmarks permite reducir significativamente la superficie de ataque y mitigar amenazas cibernéticas mediante configuraciones seguras aplicadas sobre sistemas operativos, servidores, estaciones de trabajo, dispositivos de red, aplicaciones y entornos en la nube.

Estas prácticas de endurecimiento contribuyen a disminuir brechas de seguridad derivadas de configuraciones inseguras, servicios innecesarios, privilegios excesivos y vulnerabilidades conocidas, fortaleciendo así la postura defensiva de la organización. Adicionalmente, los lineamientos CIS se encuentran alineados con marcos internacionales y estándares de seguridad reconocidos, como ISO/IEC 27001, NIST “Cybersecurity Framework” (CSF) y NIST SP 800-53, facilitando la adopción de controles de seguridad consistentes, medibles y auditables dentro de los procesos de gestión de ciberseguridad.

La aplicación de CIS Benchmarks permite reducir la superficie de ataque, tenido un impacto directo en los hallazgos críticos:

La desactivación de servicios innecesarios y protocolos obsoletos, como SMBv1, recomendada por los CIS Benchmarks, habría impedido la explotación de la vulnerabilidad MS17-010 (EternalBlue), evitando el escalamiento de privilegios a SYSTEM en Host-A y el posterior movimiento lateral hacia Host-B.

La configuración segura de servicios web, conforme a los CIS Benchmarks, habría mitigado el riesgo asociado a Rejetto HFS 2.3 (CVE-2014-6287), bloqueando el vector de acceso inicial que permitió al atacante obtener control remoto sobre Host-A.

Funciones Clave y Características Esenciales en Gestión de Seguridad en el SIEM

Los Sistemas de Gestión de Información y Eventos de Seguridad SIEM “Security Information and Event Management” según Stellar Cyber. (2026), son plataformas especializadas que complementan el ecosistema de ciberseguridad junto con tecnologías como EDR “Endpoint Detection and Response” y XDR “Extended Detection and Response”. Su función principal es centralizar, correlacionar y analizar grandes volúmenes de registros (logs) y eventos de seguridad provenientes de múltiples fuentes, tales como servidores, firewalls, aplicaciones, endpoints, dispositivos de red, servicios cloud y herramientas de seguridad.

Frente al tema, Moreno, P. (2015) a firma que el SIEM proporciona capacidades avanzadas de monitoreo continuo, detección temprana de amenazas y gestión de incidentes en tiempo real, permitiendo identificar comportamientos anómalos y posibles indicadores de compromiso (IoC). Mediante motores de correlación, reglas de análisis y capacidades de inteligencia de amenazas, estas plataformas ayudan a detectar actividades maliciosas que podrían pasar desapercibidas de manera aislada, fortaleciendo así la capacidad de respuesta y visibilidad de la organización.

La implementación de un SIEM es determinante para detectar en tiempo real las acciones ejecutadas por el atacante en el ejercicio de “SecureNova Labs”:

La creación no autorizada de la cuenta "Lab_RedTeams" en Host-B y su posterior adición al grupo de administradores habrían generado alertas inmediatas en un SIEM, permitiendo al Blue Team contener el incidente antes de que el atacante consolidara su persistencia.

La ejecución de comandos de redirección de puertos mediante netsh interface portproxy habría quedado registrada en los logs del sistema, y un SIEM con reglas de correlación adecuadas habría detectado este comportamiento anómalo como un indicio de movimiento lateral.

Los intentos de explotación de EternalBlue contra Host-B, que implican patrones específicos de tráfico SMB, habrían sido correlacionados con los logs de red y de endpoints, generando una alerta temprana que habría permitido aislar Host-B antes de que el atacante obtuviera control total.

La descarga y ejecución de payloads desde el servidor web de Kali (actividad sospechosa en el puerto 8080) habría sido identificada como tráfico no autorizado, activando mecanismos de bloqueo y notificación al equipo de respuesta.

Adicionalmente, los SIEM facilitan la generación de reportes de cumplimiento normativo y auditoría, alineándose con marcos regulatorios y estándares como ISO/IEC 27001, NIST, PCI DSS y SOC. Esto permite identificar áreas de alto riesgo y enfocar de manera proactiva las estrategias de mitigación, reduciendo tiempos de detección, costos operativos y tiempos de respuesta ante incidentes de seguridad.

Entre los eventos y alertas más comunes que puede detectar un SIEM se encuentran:

- Múltiples intentos fallidos de autenticación.
- Bloqueo o uso indebido de cuentas.
- Comportamientos sospechosos de usuarios o privilegios elevados.
- Detección de malware, ransomware o virus.
- Tráfico de red inusual o conexiones no autorizadas.
- Intentos de intrusión y explotación de vulnerabilidades.

- Fuga o pérdida de información sensible.
- Caídas o indisponibilidad de servicios críticos.
- Actividades anómalas en aplicaciones y servicios cloud.

Desde el punto de vista técnico, un SIEM integra componentes de recolección, normalización y almacenamiento de logs, motores de correlación de eventos, análisis basado en reglas e inteligencia artificial, dashboards de monitoreo y capacidades de automatización e integración con plataformas SOAR. Estas funcionalidades permiten mejorar significativamente la detección, investigación y respuesta ante amenazas avanzadas, fortaleciendo la gestión integral de seguridad y la resiliencia operativa de la organización.

Herramientas Clave para Contención Activa de Ataques en Ciberseguridad

Para fortalecer la capacidad de contención y respuesta ante ataques informáticos en "SecureNova Labs", se recomienda la implementación integrada de herramientas de seguridad de código abierto bajo licencia GPL "General Public License", las cuales proporcionan capacidades avanzadas de monitoreo, detección, segmentación y control de acceso. Entre las soluciones más relevantes se destacan Wazuh, Suricata y la integración de pfSense con PacketFence, conformando un ecosistema robusto de defensa en profundidad capaz de detectar, responder y mitigar amenazas internas y externas.

Suricata – NIDS/NIPS para análisis y protección de red

Frente al tema, Fajardini, J. (2024) afirma que Suricata es una solución de "Network Intrusion Detection and Prevention System NIDS/NIPS" enfocada en el monitoreo y análisis del tráfico de red mediante técnicas de Inspección Profunda de Paquetes DPI "Deep Packet

Inspection". Esta herramienta permite identificar actividades maliciosas, tráfico anómalo, malware, ataques de red y patrones asociados a amenazas avanzadas.

En el contexto del laboratorio, Suricata habría detectado:

Los intentos de explotación de Rejetto HFS (CVE-2014-6287) mediante firmas IDS específicas, bloqueando las peticiones HTTP maliciosas antes de que alcanzaran Host-A.

Los patrones de tráfico SMB asociados a EternalBlue (MS17-010), permitiendo alertar y bloquear el movimiento lateral desde Host-A hacia Host-B.

El tráfico de red inusual generado por la configuración de portproxy y las conexiones reversas desde los hosts comprometidos hacia Kali.

Desde el punto de vista técnico, Suricata soporta análisis multihilo de alto rendimiento, firmas IDS/IPS, detección basada en comportamiento y protocolos de red modernos, proporcionando visibilidad en tiempo real sobre las comunicaciones de la infraestructura.

Como referencia, "Suricata es un software de análisis de redes y detección de amenazas de alto rendimiento y código abierto, utilizado por la mayoría de las organizaciones privadas y públicas, e integrado por los principales proveedores para proteger sus activos" (Fajardini, 2024).

Wazuh – Plataforma XDR/SIEM/HIDS para monitoreo y correlación

Wazuh es una plataforma de ciberseguridad de código abierto que integra capacidades de HIDS (Host-based Intrusion Detection System), SIEM y XDR, enfocándose en la protección de endpoints, servidores y entornos cloud. Su funcionalidad permite recolectar y correlacionar logs, detectar cambios en archivos críticos mediante File Integrity Monitoring (FIM), identificar actividades sospechosas y automatizar procesos de respuesta ante incidentes.

En relación con los hallazgos del laboratorio:

La creación de la cuenta "Lab_RedTeams" y su adición al grupo "administradores" habrían sido capturadas por Wazuh, generando alertas de alta criticidad sobre cambios en la gestión de identidades.

La modificación de la configuración de red mediante netsh interface portproxy (asociada al pivoting y movimiento lateral) habría sido identificada como un cambio crítico en la configuración del sistema.

La presencia de conexiones reversas hacia direcciones IP no autorizadas (Kali) habría sido correlacionada con eventos de red, activando alertas sobre posible actividad de malware o backdoor.

Adicionalmente, Wazuh facilita la gestión centralizada de eventos de seguridad, monitoreo continuo, análisis de vulnerabilidades y cumplimiento normativo, integrándose con herramientas de visualización y motores de inteligencia de amenazas.

Según su documentación oficial, “Wazuh es la plataforma de ciberseguridad de código abierto más utilizada, que unifica XDR y SIEM en una sola solución. Analiza datos de seguridad en endpoints, nubes y redes para detectar amenazas, responder a incidentes y garantizar el cumplimiento normativo” (Wazuh, 2025).

pfSense y PacketFence – Firewall y NAC para segmentación y control de acceso

La integración de pfSense con PacketFence proporciona una arquitectura sólida de seguridad perimetral y control de acceso a la red.

Por un lado, pfSense actúa como firewall y router de nueva generación basado en FreeBSD, permitiendo implementar reglas avanzadas de filtrado, VPN, segmentación de red, NAT, IDS/IPS y políticas de seguridad adaptativas. Su enfoque modular y de código abierto facilita la expansión de funcionalidades sin incrementar innecesariamente la superficie de ataque.

De acuerdo con la documentación oficial, “El software pfSense® es una distribución gratuita y de código abierto de FreeBSD, diseñada específicamente para funcionar como cortafuegos y enrutador, y gestionada completamente mediante una interfaz web” (Learn About the pfSense Project, 2026).

Por otro lado, PacketFence funciona como una solución NAC (Network Access Control) orientada a la autenticación, autorización y control de dispositivos conectados a la red. Permite aplicar políticas de acceso basadas en perfiles, segmentar usuarios mediante VLAN dinámicas, gestionar portales cautivos y controlar dispositivos corporativos y BYOD bajo estándares como 802.1X.

Como lo indica su documentación, “PacketFence es una solución de control de acceso a la red (NAC) de código abierto. Ofrece una amplia gama de funciones, como un portal cautivo para registro y corrección de problemas, gestión centralizada de redes cableadas e inalámbricas y compatibilidad con 802.1X” (PacketFence Gateway, 2026).

Beneficios técnicos de la integración

La implementación conjunta de estas herramientas permite construir una estrategia de seguridad multicapa alineada con modelos de defensa en profundidad y Zero Trust, aportando beneficios como:

- Monitoreo continuo de endpoints, servidores y tráfico de red.
- Detección temprana de amenazas y movimientos laterales.
- Segmentación dinámica y control de acceso basado en identidad.
- Correlación de eventos y análisis centralizado de logs.
- Automatización de alertas y respuesta ante incidentes.
- Reducción de superficie de ataque y fortalecimiento del hardening.

- Cumplimiento de buenas prácticas alineadas con marcos como ISO/IEC 27001, NIST y CIS Controls.

En conjunto, estas soluciones proporcionan a “SecureNova Labs” una capacidad sólida y escalable para fortalecer su postura de ciberseguridad, incrementar la visibilidad operativa y mejorar significativamente los tiempos de detección y respuesta ante incidentes de seguridad informática.

Evaluación, Documentación y Divulgación de Hallazgos Técnicos

El presente informe técnico consolida los hallazgos, estrategias y lecciones aprendidas durante el ejercicio integral de ciberseguridad realizado en “SecureNova Labs”, abarcando las etapas de reconocimiento, acceso inicial, explotación, persistencia, movimiento lateral, respuesta a incidentes y análisis legal. El ejercicio fue ejecutado bajo los roles de Red Team (equipo ofensivo) y Blue Team (equipo defensivo), con el objetivo de evaluar la postura de seguridad de la organización, identificar vulnerabilidades críticas y proponer medidas de remediación alineadas con marcos internacionales como NIST CSF 2.0, NIST SP 800-61 Rev. 3, ISO/IEC 27001 y estándares CIS.

Desde la perspectiva del Red Team, se documentó de manera estructurada la cadena completa de ataque ejecutada en el laboratorio, iniciando con la fase de reconocimiento y enumeración de servicios vulnerables mediante herramientas como Nmap y Metasploit Framework. Durante el proceso se identificó el servicio vulnerable Rejetto HFS 2.3 asociado a la vulnerabilidad CVE-2014-6287, permitiendo la obtención de acceso inicial al Host-A mediante explotación remota. Posteriormente, se ejecutaron técnicas de post-explotación, pivoting y movimiento lateral hacia el Host-B mediante la configuración de rutas internas, portproxy y explotación de la vulnerabilidad MS17-010 EternalBlue, logrando acceso privilegiado y control administrativo del entorno objetivo.

La documentación técnica incluyó evidencias asociadas a:

- Descubrimiento de hosts y servicios expuestos.
- Identificación de vulnerabilidades críticas.
- Configuración de rutas para pivoting.
- Movimiento lateral entre segmentos internos.

- Explotación de EternalBlue.
- Escalamiento de privilegios.
- Persistencia mediante creación de cuentas administrativas.
- Validación de acceso y control sobre los sistemas comprometidos.

Cada actividad fue acompañada de capturas de pantalla, comandos ejecutados, direcciones IP involucradas, puertos identificados y análisis técnico de impacto, permitiendo garantizar trazabilidad y reproducibilidad de los hallazgos obtenidos durante el ejercicio ofensivo.

Desde la perspectiva del Blue Team, el análisis se enfocó en identificar las debilidades de seguridad que facilitaron el compromiso de la infraestructura, evaluando la efectividad de los controles existentes y proponiendo estrategias de remediación y fortalecimiento defensivo. En este contexto, se evidenció la necesidad de implementar mecanismos de hardening, segmentación de red, monitoreo continuo, gestión de vulnerabilidades y principios de Zero Trust para reducir la superficie de ataque y limitar el movimiento lateral dentro de la organización. En particular, se identificó que la ausencia de controles específicos permitió que cada fase del ataque impactara los principios CID:

Confidencialidad: La explotación de Rejetto HFS y el acceso a Host-B expusieron información sensible de la organización, incluyendo configuraciones internas, credenciales y datos almacenados en el servidor secundario.

Integridad: La ejecución de comandos mediante scripts VBS, la modificación de la configuración de red con portproxy y la creación de cuentas administrativas alteraron el estado esperado de los sistemas, afectando su integridad operativa y de configuración.

Disponibilidad: La explotación de EternalBlue, al ser un ataque dirigido al kernel, presenta un riesgo significativo de inestabilidad del sistema. Adicionalmente, la persistencia establecida mediante cuentas administrativas podría ser utilizada para realizar acciones destructivas que afecten la disponibilidad de los servicios.

Como parte de la evaluación defensiva, se recomendó:

- Actualizar o eliminar servicios vulnerables como Rejetto HFS 2.3.
- Aplicar parches de seguridad críticos asociados a EternalBlue.
- Deshabilitar SMBv1 en toda la infraestructura.
- Implementar segmentación de red mediante VLAN y firewalls internos.
- Adoptar controles de acceso basados en el principio de mínimo privilegio.
- Habilitar autenticación multifactor (MFA).
- Implementar soluciones EDR/XDR y plataformas SIEM.
- Fortalecer la auditoría y monitoreo de eventos de seguridad.
- Aplicar lineamientos de hardening basados en CIS Benchmarks.

Adicionalmente, se evaluó la importancia de contar con capacidades de monitoreo y correlación de eventos mediante soluciones SIEM, permitiendo detectar comportamientos anómalos, intentos de explotación, creación de cuentas no autorizadas y actividades asociadas a movimiento lateral. En este sentido, se destacó la relevancia de plataformas como Wazuh, Suricata y pfSense integradas con mecanismos NAC como PacketFence para fortalecer las capacidades de detección, contención y respuesta ante incidentes de seguridad.

En relación con los aspectos legales y éticos evaluados durante el ejercicio, se concluyó que cualquier actividad de pruebas de penetración debe ejecutarse bajo principios de legalidad, autorización expresa, proporcionalidad y trazabilidad. Se identificaron riesgos asociados a cláusulas contractuales irregulares que pretendían restringir la denuncia de actividades ilícitas o proteger información obtenida ilegalmente, situaciones contrarias a la legislación colombiana y a los principios éticos del ejercicio profesional en ciberseguridad.

Por lo anterior, se enfatizó la necesidad de:

- Implementar acuerdos de confidencialidad alineados con la legislación vigente.
- Garantizar supervisión legal y ética de las actividades ofensivas.
- Mantener controles de auditoría y trazabilidad sobre herramientas forenses y de explotación.
- Establecer mecanismos de denuncia y cumplimiento normativo.
- Aplicar principios de responsabilidad profesional y deber de reporte ante actividades ilícitas.

Estos aspectos legales y éticos son fundamentales para preservar la Confidencialidad de la información del cliente, la Integridad de los procesos de auditoría y la Disponibilidad de los servicios, al garantizar que las actividades de seguridad se realicen dentro de un marco de confianza y responsabilidad.

Como resultado de esta evaluación integral, se concluye que el ejercicio permitió evidenciar de manera práctica cómo vulnerabilidades críticas, configuraciones inseguras y deficiencias de segmentación pueden facilitar compromisos completos de infraestructura mediante técnicas de explotación y movimiento lateral. El impacto sobre los principios de Confidencialidad, Integridad y Disponibilidad fue demostrado en cada fase del ataque: la explotación de Rejetto HFS y el pivoting hacia Host-B comprometieron la Confidencialidad al

exponer información sensible; la ejecución de comandos y la creación de cuentas administrativas afectaron la Integridad de los sistemas; y la presencia de EternalBlue y la persistencia establecida representaron un riesgo significativo para la Disponibilidad de los servicios críticos.

Asimismo, se demostró la importancia de integrar capacidades ofensivas y defensivas dentro de una estrategia madura de ciberseguridad orientada a la prevención, detección, respuesta y mejora continua.

Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/Zk_Lifs4zro

Conclusiones

El ejercicio integral de ciberseguridad realizado en “SecureNova Labs” permitió evidenciar la complejidad de la gestión de incidentes y la necesidad de adoptar un enfoque holístico que integre las capacidades ofensivas del Red Team, las defensivas del Blue Team y el cumplimiento normativo desde los aspectos legales.

El acuerdo de confidencialidad analizado contiene cláusulas ilegales que contravienen la Constitución Política de Colombia, la Ley 1273 de 2009 y el Código Penal. Específicamente, se identificaron disposiciones que pretendían prohibir la denuncia de actividades ilícitas, proteger información obtenida mediante "chuzadas" o interceptaciones ilegales, y eximir de responsabilidad penal a la organización, lo que expone a “SecureNova Labs” y a los firmantes a riesgos legales y éticos significativos. Este hallazgo evidencia la necesidad de revisar y alinear los acuerdos de confidencialidad con el marco normativo colombiano, garantizando que no se limiten derechos fundamentales como el deber constitucional de denuncia.

El Red Team demostró que un atacante con acceso inicial a un equipo aparentemente no crítico (Host-A) puede escalar privilegios a SYSTEM mediante Rejjetto, configurar mecanismos de persistencia como portproxy y moverse lateralmente hacia servidores internos sensibles (Host-B) mediante EternalBlue, comprometiendo la confidencialidad, integridad y disponibilidad de la información. La prueba de concepto con la creación de la cuenta Lab_RedTeams evidencia el impacto real de la cadena de ataque, confirmando que ambas máquinas fueron comprometidas exitosamente y que las vulnerabilidades identificadas son explotables en el entorno actual de la organización.

El Blue Team, por su parte, identificó brechas significativas en las capacidades de detección, contención y respuesta a incidentes. La ausencia de un SIEM, la falta de monitoreo continuo y la desactivación del firewall de Windows permitieron que los ataques pasaran

desapercibidos. Asimismo, se evidenció que la segmentación de red era insuficiente, ya que Host-A actuaba como un puente entre la red externa y la red interna (10.10.10.0/24), facilitando el movimiento lateral hacia Host-B. La presencia de SMBv1 habilitado y la ausencia de parches críticos (MS17-010) confirmaron que las configuraciones inseguras y los sistemas desactualizados representan vectores de ataque viables y de alto impacto.

Se formularon recomendaciones específicas orientadas a cerrar las brechas identificadas. Entre ellas se destacan: la actualización o eliminación de servicios vulnerables como Rejetto HFS 2.3, la aplicación de parches críticos, la deshabilitación de SMBv1 en toda la infraestructura, la implementación de segmentación de red mediante VLAN y firewalls internos, la adopción del principio de mínimo privilegio y autenticación multifactor (MFA), el despliegue de soluciones EDR/XDR y plataformas SIEM para monitoreo continuo, y la aplicación de lineamientos de hardening basados en CIS Benchmarks. Estas estrategias, alineadas con marcos como NIST CSF 2.0, ISO/IEC 27001 y CIS Controls, permitirán a “SecureNova Labs” reducir significativamente su superficie de ataque y fortalecer su postura defensiva.

Frente al tema, Larson, M. (2025, August 13) afirma que la implementación de un plan de respuesta a incidentes basado en NIST SP 800-61 Rev. 3 y la preservación de evidencia digital mediante hash criptográficos (MD5, SHA-256) demostraron ser fundamentales para la gestión estructurada del incidente, garantizando la cadena de custodia y la integridad de la evidencia para futuros procesos legales o auditorías.

Finalmente, se destaca que la solución de los problemas identificados no depende exclusivamente de un solo actor dentro de “SecureNova Labs”, sino que requiere la colaboración entre la dirección de tecnología, los equipos de seguridad (Red y Blue Team), los administradores de sistemas, los responsables de cumplimiento normativo y la alta gerencia. Solo a través del trabajo conjunto entre estas áreas será posible avanzar hacia una postura de

seguridad sólida, sostenible y resiliente, implementando de manera efectiva las estrategias de remediación propuestas y estableciendo una cultura de mejora continua basada en ejercicios periódicos de Purple Team.

Recomendaciones

Como acciones de carácter urgente, se recomienda eliminar o actualizar el servicio Rejetto HFS 2.3, vulnerable a CVE-2014-6287, y aplicar el parche MS17-010 (KB4012212/KB4012215) para mitigar EternalBlue, deshabilitando simultáneamente el protocolo SMBv1 en toda la infraestructura. Estas medidas deben complementarse con la restricción del puerto 445 mediante reglas de firewall y la eliminación de cuentas no autorizadas, como la cuenta "Lab_RedTeams" creada durante el ejercicio. Para verificar la efectividad de estas acciones, se recomienda ejecutar escaneos con Nmap u OpenVAS que confirmen la ausencia de los servicios vulnerables, así como revisar los logs de seguridad (Event ID 4720, 4732) para garantizar que no persisten cuentas no autorizadas. La reactivación del firewall de Windows con reglas de entrada restrictivas debe ser validada mediante pruebas de conectividad desde la red externa, asegurando que únicamente los puertos necesarios permanezcan abiertos.

En el mediano plazo, resulta indispensable implementar una plataforma SIEM, como Wazuh, que permita centralizar y correlacionar eventos de seguridad, configurando reglas específicas para detectar creación de cuentas no autorizadas (Event ID 4720), cambios en grupos privilegiados (4728, 4732) y modificaciones en la configuración de red (5157). Complementariamente, se recomienda desplegar soluciones EDR/XDR, como CrowdStrike o SentinelOne, en todos los endpoints para fortalecer la detección de actividades maliciosas. La segmentación de la red mediante VLAN y firewalls internos, bajo un modelo de Zero Trust, debe ser validada mediante pruebas de conectividad que confirmen el aislamiento entre segmentos. Asimismo, se sugiere aplicar hardening basado en CIS Benchmarks, verificando el cumplimiento mediante herramientas como OpenSCAP o CIS-CAT, y habilitar autenticación multifactor

(MFA) bajo el principio de mínimo privilegio, auditando periódicamente los permisos de cuentas y servicios.

Desde una perspectiva estratégica, se recomienda establecer un programa continuo de gestión de vulnerabilidades que incluya escaneos automáticos semanales con herramientas como OpenVAS o Nessus, priorizando la remediación de vulnerabilidades críticas en un plazo no superior a 48 horas. La consolidación de un Blue Team permanente y un equipo CSIRT/CIRT, con roles y procedimientos documentados, permitirá gestionar incidentes de manera estructurada, complementándose con ejercicios periódicos de Purple Team que simulen escenarios de ataque y validen la efectividad de los controles implementados. Adicionalmente, resulta fundamental capacitar al personal en ciberseguridad, con énfasis en ingeniería social, midiendo la efectividad mediante pruebas de phishing simuladas y el registro de asistencia y aprobación de cursos. Finalmente, la organización debe alinear su estrategia de ciberseguridad con marcos internacionales como ISO/IEC 27001, NIST CSF 2.0 y CIS Controls, manteniendo un sistema de gestión de seguridad de la información (SGSI) que demuestre mejora continua a través de auditorías internas periódicas.

Desde el ámbito legal y ético, se recomienda revisar y corregir el acuerdo de confidencialidad para eliminar cláusulas que contravengan la Constitución Política de Colombia (Art. 95), la Ley 1273 de 2009 y el Código Penal, garantizando que se incluya una cláusula explícita que exceptúe de la confidencialidad las denuncias de delitos ante autoridades competentes. Toda actividad ofensiva, incluyendo pruebas de penetración, ejercicios Red Team y análisis forense, debe ejecutarse bajo autorización formal, alcance definido y estricto cumplimiento de la legislación vigente, documentando y archivando las autorizaciones firmadas para cada ejercicio. Asimismo, se debe mantener un registro de trazabilidad de todas las actividades realizadas, incluyendo fechas, alcance, herramientas utilizadas y resultados

obtenidos, garantizando así la supervisión legal y ética de las operaciones de ciberseguridad. Finalmente, se recomienda establecer mecanismos de denuncia y cumplimiento normativo, así como aplicar principios de responsabilidad profesional y deber de reporte ante actividades ilícitas, alineados con el Código de Ética del COPNIA.

Referencias Bibliográficas

BetaFred. (2024, March 18). *Boletín de seguridad de Microsoft MS17-010: crítico.Microsoft.Com*. https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS. Universidad Nacional Abierta y a Distancia – UNAD* (Versión 1.0, pp. 531). https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoración_y_evaluación_de_riesgos_de_ciberseguridad__Pag_publicado.pdf

Cisco. (2026). *What Is Network Segmentation?* https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html

Congreso de la República de Colombia. (2003, 14 de octubre). *Ley 842 de 2003. Código de Ética para el ejercicio de la ingeniería... Consejo Profesional Nacional de Ingeniería* (COPNIA). https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Congreso de la República de Colombia. (2009, 5 de enero*). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —de la protección de la información y de los datos— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, y se dictan otras disposiciones.* Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

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. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4998

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

Constitución Política de Colombia. (1991, 7 de julio). *Artículos 15 y 20.* Funcionpublica.Gov.Co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Estefania.dominguez. (2026). *Nmap en ciberseguridad | Escaneo y análisis de red. Campus Internacional de Ciberseguidad*. https://www.campusciberseguridad.com/blog/como-ayuda-nmap-con-la-seguridad-de-la-red/

Estefania.dominguez. (2026). *OpenVAS | Escaneo profesional de vulnerabilidades. Campus Internacional de Ciberseguidad*. https://www.campusciberseguridad.com/blog/escaneo-de-vulnerabilidades-usando-openvas/

Fajardini, J. (2024). *What is Suricata - Suricata. Suricata*. https://suricata.io/2024/04/15/what-is-suricata/

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

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). *Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. International Journal of Scientific Research in Engineering and Management* , 7(12), 1–11. https://doi.org/10.55041/IJSREM27675

Larson, M. (2025, August 13). NIST SP 800-61 Rev 3: *New Incident Response Framework Guide. Linford & Company LLP*. https://linfordco.com/blog/nist-sp-800-61/

Lozano, P. A. (2023). *Fases del pentesting: Pasos para asegurar tus sistemas. OpenWebinars.net*. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (2022). *Políticas de Privacidad y Condiciones de Uso.* https://www.mintic.gov.co/portal/inicio/Secciones

Molina, P. (2024). *Desentrañando la Esencia de Exploit-DB: Una Herramienta Vital en Ciberseguridad. InSys*. https://www.gotoinsys.com/actualidades/desentra%C3%B1ando-la-esencia-de-exploit-db-una-herramienta-vital-en-ciberseguridad

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management).* USFQ (pp. 31–63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Netalit. (2024). *The 6 Phases of an Incident Response Plan. Check Point Software*. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-incident-response/the-6-phases-of-an-incident-response-plan/

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

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

Ribeiro, A., & Ribeiro, A. (2025, April 4). *NIST publishes SP 800-61 Rev. 3, overhauling incident response guidance for CSF 2.0 - Industrial Cyber. Industrial Cyber.* https://industrialcyber.co/nist/nist-publishes-sp-800-61-rev-3-overhauling-incident-response-guidance-for-csf-2-0/

SANS Institute. (2025). *SIEM Evaluation Tool | SANS Institute*. https://www.sans.org/tools/siem-evaluation

Stellar Cyber. (2026). *¿Qué es SIEM Componentes, capacidades y arquitectura?* https://stellarcyber.ai/es/learn/what-is-siem/

Susnjara, S., & Smalley, I. (2024, November 6). *Puntos de referencia de CIS. Ibm.Com.* https://www.ibm.com/es-es/think/topics/cis-benchmarks

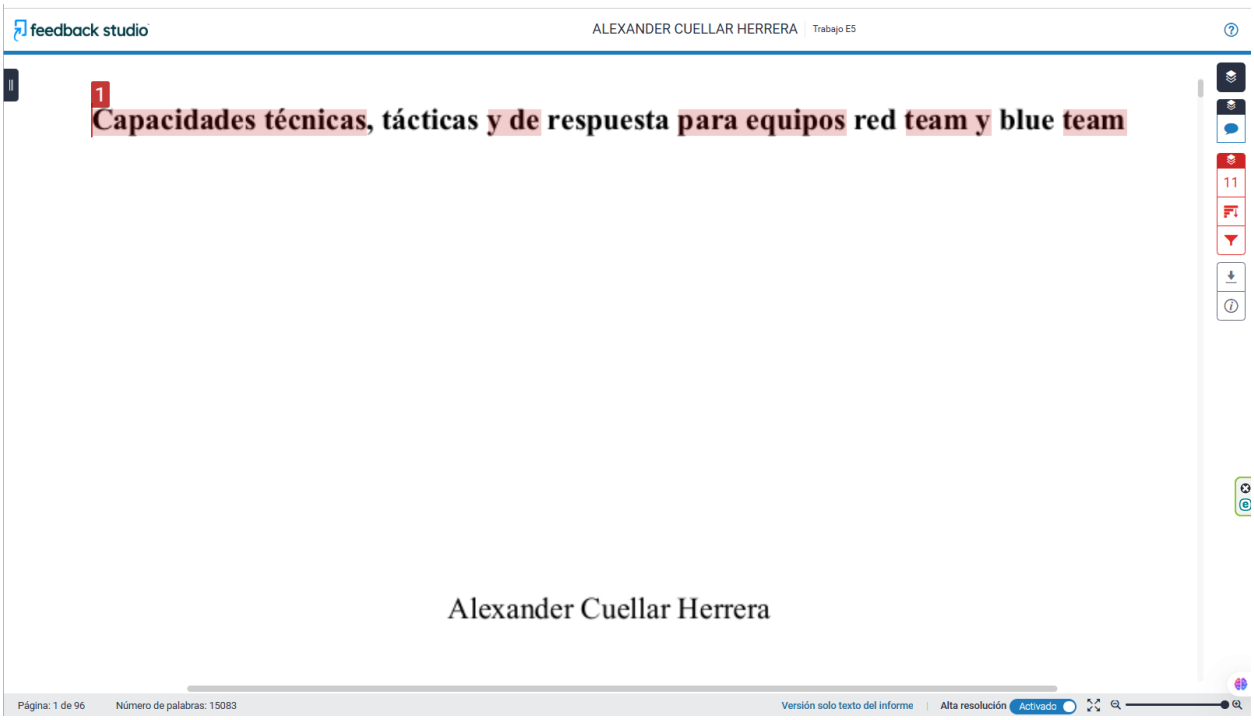
Top 10 Routinely Exploited Vulnerabilities | CISA. (2020). *Cybersecurity and Infrastructure Security Agency CISA*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-133a

Zambrano Hernández, Peña Hidalgo, H. J., & Cárdenas Corral. (2024). *Guía para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello* Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Apéndices

Apéndice A

Resultado de revisión en turnitin



Nota. Autoría propia.