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

Richard Fernando Mahecha Rocha

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Dedico este trabajo a todas las personas que han contribuido a mi formación profesional y personal, especialmente a quienes, con su guía, exigencia y acompañamiento, han fortalecido mi compromiso con la ética, la responsabilidad y el aprendizaje continuo. A mi familia, por su apoyo incondicional; a mis tutores, por su dedicación; y a quienes creen en la importancia de construir un entorno digital más seguro. Este proyecto es reflejo del esfuerzo compartido y del camino recorrido con disciplina y convicción.

Agradecimientos

Agradezco profundamente a mi familia, cuyo apoyo incondicional, paciencia y confianza han sido la base que me impulsa a continuar avanzando en mi formación profesional. Su compañía en los momentos de mayor esfuerzo me ha recordado la importancia de perseverar y de valorar cada logro alcanzado. A mis docentes y tutores les expreso mi reconocimiento por su dedicación, su guía constante y la motivación que transmiten día a día. Este trabajo es también el resultado de su influencia y orientación. A quienes compartieron conmigo aprendizajes, ideas y desafíos, les agradezco por aportar a mi crecimiento académico y personal.

Resumen

El presente trabajo desarrolla un análisis integral del ciclo completo de un ejercicio Red Team – Blue Team orientado a la evaluación de la seguridad informática dentro de un entorno controlado. El estudio inicia con la construcción metodológica del laboratorio y la delimitación teórica del ataque, continúa con un examen ético y legal basado en la Ley 1273 de 2009 y los principios del COPNIA, y posteriormente avanza hacia la ejecución técnica del ataque ofensivo mediante explotación de vulnerabilidades, obtención de acceso remoto, movimiento lateral y compromiso de equipos internos (COPNIA, 2015). En paralelo, se documenta la respuesta estructurada del Blue Team, abordando procesos de detección, análisis forense inicial, contención inmediata del incidente, erradicación de artefactos maliciosos y recuperación del sistema comprometido. El análisis integrado de las cuatro etapas permite evidenciar la relación indisoluble entre técnica, ética y marco jurídico, mostrando cómo un ataque exitoso solo puede desarrollarse de manera legítima cuando existe un alcance autorizado y cómo la defensa debe ejecutarse con preservación de evidencia, rigor metodológico y apego a buenas prácticas. En conjunto, este ejercicio refleja la complejidad del trabajo en ciberseguridad moderna y la necesidad de formar profesionales capaces de comprender tanto la dimensión ofensiva como la defensiva, sin perder de vista su responsabilidad legal, social y profesional.

***Palabras clave*:** Ciberseguridad, ética, forense, incidente, vulnerabilidades.

Abstract

This paper presents an integrated analysis of a complete Red Team – Blue Team cybersecurity exercise conducted in a controlled laboratory environment. The study begins with the methodological construction of the testing infrastructure and the conceptual definition of the offensive scenario, followed by an ethical and legal examination based on Colombian Law 1273 of 2009 and the professional principles established by COPNIA. The work then advances into the technical execution of the Red Team attack, which includes vulnerability exploitation, remote access acquisition, lateral movement, and compromise of internal hosts. In parallel, the Blue Team response is documented through a structured process involving incident detection, initial forensic triage, rapid containment, eradication of malicious components, and system recovery. The integrated analysis of all stages demonstrates the essential relationship between technical proficiency, ethical responsibility, and legal compliance, highlighting that offensive operations are only legitimate when fully authorized and that defensive actions must preserve evidence and follow recognized best practices. Overall, this project illustrates the complexity of modern cybersecurity operations and emphasizes the need to train professionals capable of understanding both offensive and defensive perspectives while maintaining strong ethical and legal awareness.

Keywords: Cybersecurity, ethics, forensics. vulnerabilities, incident,

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Análisis forense digital:

Proceso de identificación, extracción, preservación y análisis de evidencia digital con el fin de reconstruir eventos, comprender la actividad de un atacante y aportar información válida en una investigación técnica o legal.

Blue Team:

Conjunto de profesionales encargados de la defensa de los sistemas informáticos. Su labor consiste en monitorear, detectar, analizar, contener y erradicar incidentes de seguridad para proteger la infraestructura tecnológica de la organización.

Cadena de ataque:

Secuencia de pasos que sigue un atacante desde el reconocimiento inicial hasta la explotación, el movimiento lateral y la obtención de control sobre sistemas adicionales dentro de una red.

Contención:

Acción tomada por el equipo defensor para limitar el alcance de un ataque activo, interrumpir la capacidad del adversario y evitar que el incidente continúe propagándose a otros sistemas.

Explotación (Exploit):

Ejecución de una técnica o herramienta diseñada para aprovechar una vulnerabilidad y obtener acceso o ejecutar acciones no autorizadas en un sistema comprometido.

Incidente de seguridad:

Evento que compromete la confidencialidad, integridad o disponibilidad de un sistema o de los datos que procesa, pudiendo ser causado por fallas técnicas, errores humanos o ataques deliberados.

Movimiento lateral (Lateral Movement):

Técnica utilizada por un atacante para desplazarse dentro de la red interna después de comprometer un equipo inicial, con el objetivo de alcanzar sistemas de mayor valor o ampliar su control.

Pivoting:

Método que permite a un atacante utilizar un equipo comprometido como puente hacia otros sistemas que no están directamente accesibles desde su máquina de origen.

Post-explotación:

Conjunto de actividades realizadas tras la explotación exitosa de una vulnerabilidad, orientadas a mantener el acceso, elevar privilegios, recolectar información o expandir el compromiso dentro de la red.

Reconocimiento:

Fase inicial de un ataque en la cual se recolecta información sobre servicios, puertos, direcciones IP o configuraciones de red para identificar posibles vías de acceso.

Red Team:

Equipo de especialistas responsables de simular ataques reales de manera controlada, empleando técnicas ofensivas para evaluar la seguridad de la organización y poner a prueba la efectividad de sus mecanismos de defensa.

Reverse Shell:

Conexión establecida desde el equipo víctima hacia el atacante, permitiendo que éste obtenga una consola remota interactiva y ejecute comandos con los privilegios del usuario comprometido.

SIEM (Security Information and Event Management):

Sistema que centraliza la recolección, normalización y análisis de registros de múltiples dispositivos, permitiendo detectar comportamientos anómalos, correlacionar eventos y generar alertas de seguridad.

Triage:

Evaluación inicial de un incidente de seguridad cuyo propósito es determinar la severidad, el impacto y las acciones inmediatas necesarias para su contención y tratamiento adecuado.

Introducción

En el contexto actual, marcado por una acelerada transformación digital y una creciente dependencia de los sistemas informáticos, la ciberseguridad se ha consolidado como un eje fundamental para el funcionamiento seguro y confiable de organizaciones públicas y privadas. La sofisticación de las amenazas, junto con la constante evolución de las tecnologías, obliga a desarrollar enfoques integrales que permitan comprender tanto los mecanismos de ataque como las estrategias de defensa que intervienen en la protección de los activos digitales. En este marco, resulta imprescindible analizar de manera estructurada cómo se ejecuta un ataque informático, cómo se detecta y cómo se responde, utilizando metodologías reconocidas y reflejando escenarios similares a los que enfrentan diariamente los equipos de seguridad.

La literatura reciente destaca que las amenazas en entornos de red evolucionan constantemente, lo que exige enfoques sistemáticos de evaluación de la seguridad que integren técnicas ofensivas y defensivas de manera controlada y documentada (Alhamed et al., 2023; Kotwani et al., 2023; Chindrus & Caruntu, 2023).

El presente documento tiene como propósito examinar de manera detallada un ejercicio práctico de ciberseguridad basado en la simulación de un ataque Red Team y la correspondiente respuesta del Blue Team dentro de un entorno controlado. Este análisis abarca desde la construcción del laboratorio y la formulación metodológica, pasando por la revisión de los aspectos legales y éticos que regulan la práctica profesional, hasta la ejecución técnica del ataque, la evidencia forense obtenida y las medidas de contención, erradicación y recuperación aplicadas durante la respuesta al incidente. El enfoque adoptado combina fundamentos teóricos, metodologías estandarizadas, herramientas especializadas y una reflexión crítica sobre la responsabilidad del profesional de ciberseguridad.

A lo largo del documento se desarrollan los principales conceptos y procedimientos asociados al ciclo de un ataque informático, la explotación de vulnerabilidades, el movimiento lateral dentro de la red, la identificación de indicadores de compromiso, la gestión del incidente y la importancia de actuar conforme al marco normativo vigente. Se destaca además la relevancia de integrar perspectivas técnicas, éticas y legales para comprender plenamente la complejidad del fenómeno y para fortalecer las capacidades tanto ofensivas como defensivas de los analistas.

Finalmente, se presentan conclusiones orientadas a aportar elementos de reflexión para la práctica profesional y a promover una cultura de seguridad que responda a los desafíos actuales y futuros de la ciberseguridad.

Justificación

La elección de este tema se fundamenta en la necesidad de comprender de manera profunda y estructurada los riesgos, mecanismos y respuestas que intervienen en un ataque informático real, especialmente en un contexto donde la digitalización avanza con rapidez y la exposición de vulnerabilidades se convierte en una amenaza constante para las organizaciones. (Panda Security, 2018). La simulación de un ejercicio Red Team – Blue Team ofrece una oportunidad invaluable para analizar, desde una perspectiva práctica y teórica, cómo se lleva a cabo una intrusión, qué herramientas técnicas permiten su ejecución y cuáles son las acciones necesarias para detectarla y contenerla oportunamente. Este enfoque permite no solo estudiar el fenómeno del ciberataque, sino también entender sus implicaciones en la seguridad institucional, la continuidad operativa y la protección de la información.

Asimismo, existe una necesidad creciente de fortalecer las competencias de los futuros profesionales de la ciberseguridad, quienes deben afrontar escenarios complejos donde convergen factores técnicos, humanos, éticos y jurídicos. Aunque la literatura internacional ofrece diversos estudios sobre pentesting y respuesta a incidentes, a nivel local aún persisten vacíos relacionados con el análisis integrado de las dimensiones ofensivas y defensivas, y con la reflexión ética vinculada a la práctica profesional (Incibe, 2019).Este proyecto contribuye a suplir estos vacíos mediante la aplicación directa de metodologías reconocidas, la identificación de vulnerabilidades, la reconstrucción del ataque y la evaluación de la respuesta defensiva, todo ello bajo un marco legal que regula la actuación del analista.

Finalmente, la relevancia de este trabajo radica en su impacto potencial tanto en el ámbito académico como en el profesional. Los resultados aquí obtenidos pueden servir como base para futuras investigaciones sobre seguridad ofensiva y defensiva, para el diseño de políticas internas de seguridad, para la formulación de protocolos de respuesta ante incidentes y para la formación

de profesionales capaces de actuar con responsabilidad, rigor metodológico y alto sentido ético. En conjunto, esta investigación representa un aporte significativo para el fortalecimiento de la cultura de ciberseguridad en entornos educativos, institucionales y organizacionales.

Objetivos

Objetivo General

Analizar de manera integral el desarrollo, impacto y alcance técnico, ético y legal de un ejercicio de ciberseguridad basado en las estrategias Red Team y Blue Team, con el fin de comprender los mecanismos de ataque, los procedimientos de defensa y las implicaciones que estos tienen en la protección de la infraestructura tecnológica de una organización.

Objetivos Específicos

Identificar las vulnerabilidades explotadas durante la simulación Red Team, examinando los vectores de intrusión, las técnicas de acceso inicial y los métodos de movimiento lateral empleados para comprometer los sistemas internos.

Evaluar la efectividad de las acciones ejecutadas por el Blue Team mediante el análisis de los procesos de detección, triage, contención, erradicación y recuperación, con el propósito de determinar la capacidad de respuesta frente a incidentes de seguridad.

Relacionar las actividades desarrolladas en cada fase del ejercicio con los principios éticos y el marco legal vigente en Colombia, destacando la importancia de la autorización, la responsabilidad profesional y el manejo adecuado de la evidencia digital.

Proponer recomendaciones orientadas al fortalecimiento de la postura de seguridad institucional, considerando los hallazgos del ejercicio, las debilidades detectadas en la infraestructura y las mejores prácticas de hardening y monitoreo continuo.

Estrategias Red Team

SecureNova Labs es una compañía especializada en ejecutar pruebas ofensivas de alta complejidad para evaluar la resiliencia de redes corporativas. Como parte de sus auditorías internas, la empresa realiza simulaciones donde el Red Team debe reproducir la cadena completa de un ataque real: explotación inicial, consolidación del acceso, movimiento lateral, y validación del impacto en sistemas críticos.

En uno de sus procesos de monitoreo, SecureNova Labs detectó actividad irregular en una estación Windows corporativa (Host-A), donde se evidenciaba la ejecución de un servicio vulnerable, posibles intentos de acceso remoto y la creación no autorizada de cuentas administrativas. Además, los registros señalaban comunicaciones hacia un segundo sistema interno (Host-B), lo que sugería un movimiento lateral desde el equipo inicialmente comprometido.

Para determinar el alcance de la intrusión, el Red Team recibió la misión de reconstruir el ataque en un entorno controlado, identificar el vector inicial, evaluar la posibilidad de explotación real, y comprobar si Host-A podía servir como pivote hacia la red interna donde se encontraba Host-B. El laboratorio se diseñó replicando la arquitectura observada en el incidente: un atacante externo, un host vulnerable con doble interfaz de red y un servidor interno aislado.

Arquitectura de red

El entorno de laboratorio simula una organización donde:

- Host-A presta un servicio HTTP vulnerable accesible desde la red corporativa/LAN.
- Host-A dispone de una segunda interfaz conectada a una red interna aislada (intnet / 10.10.10.0/24) que aloja a Host-B.

- El atacante solo ve inicialmente la red 192.168.0.x; no tiene visibilidad directa de 10.10.10.x.

Esta configuración permite evaluar estrategias de Red Team para:

- Obtener acceso inicial a un host expuesto.
- Utilizar dicho host como pivote hacia una red interna no enrutable desde el exterior.
- Realizar movimiento lateral y ejecutar acciones de alto impacto (creación de cuentas administrativas).
-

Herramientas y Estrategias Utilizadas Según Fases del Pentesting

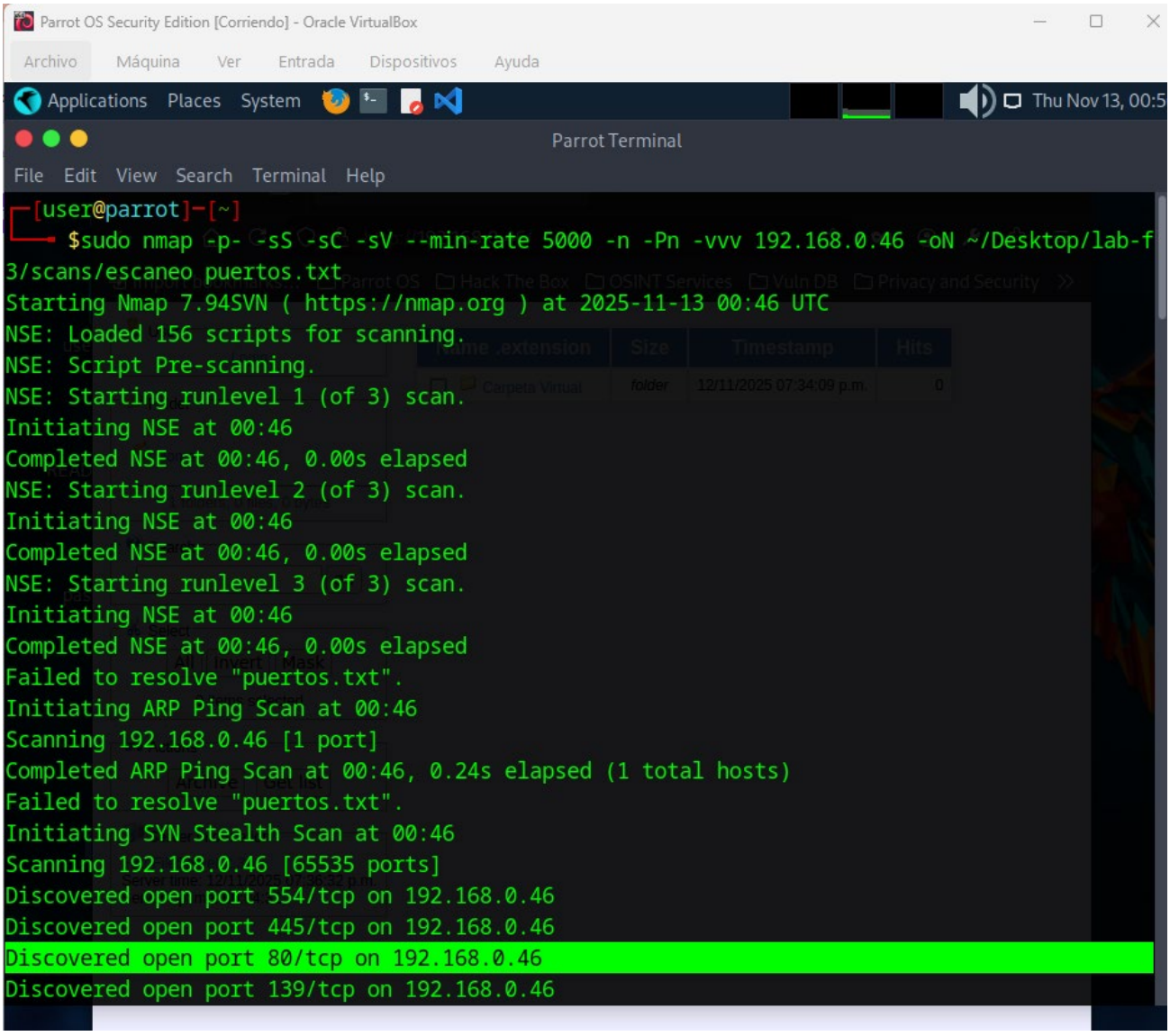
Reconocimiento y Enumeración

La primera etapa del ataque consistió en identificar qué servicios exponía Host-A a la red externa. Para ello se utilizó Nmap, que no solo permitió identificar puertos abiertos sino también características adicionales del sistema como versión del servicio, scripts NSE relevantes y comportamiento del host ante los paquetes enviados.

El escaneo reveló que Host-A tenía abierto el puerto 80, donde se ejecutaba Rejetto HFS, un servidor HTTP ligero conocido por presentar vulnerabilidades críticas en versiones antiguas que permiten ejecución remota de código. Esta observación resultó fundamental porque proporcionó un vector de ataque claro que podía ser explotado sin credenciales. Además, Nmap indicó que el sistema operativo era Windows 7, lo que representa un riesgo significativo debido a la falta de actualizaciones y soporte oficial, incrementando la superficie de ataque. Las figuras 1 y 2 muestran esta fase.

Figura 1

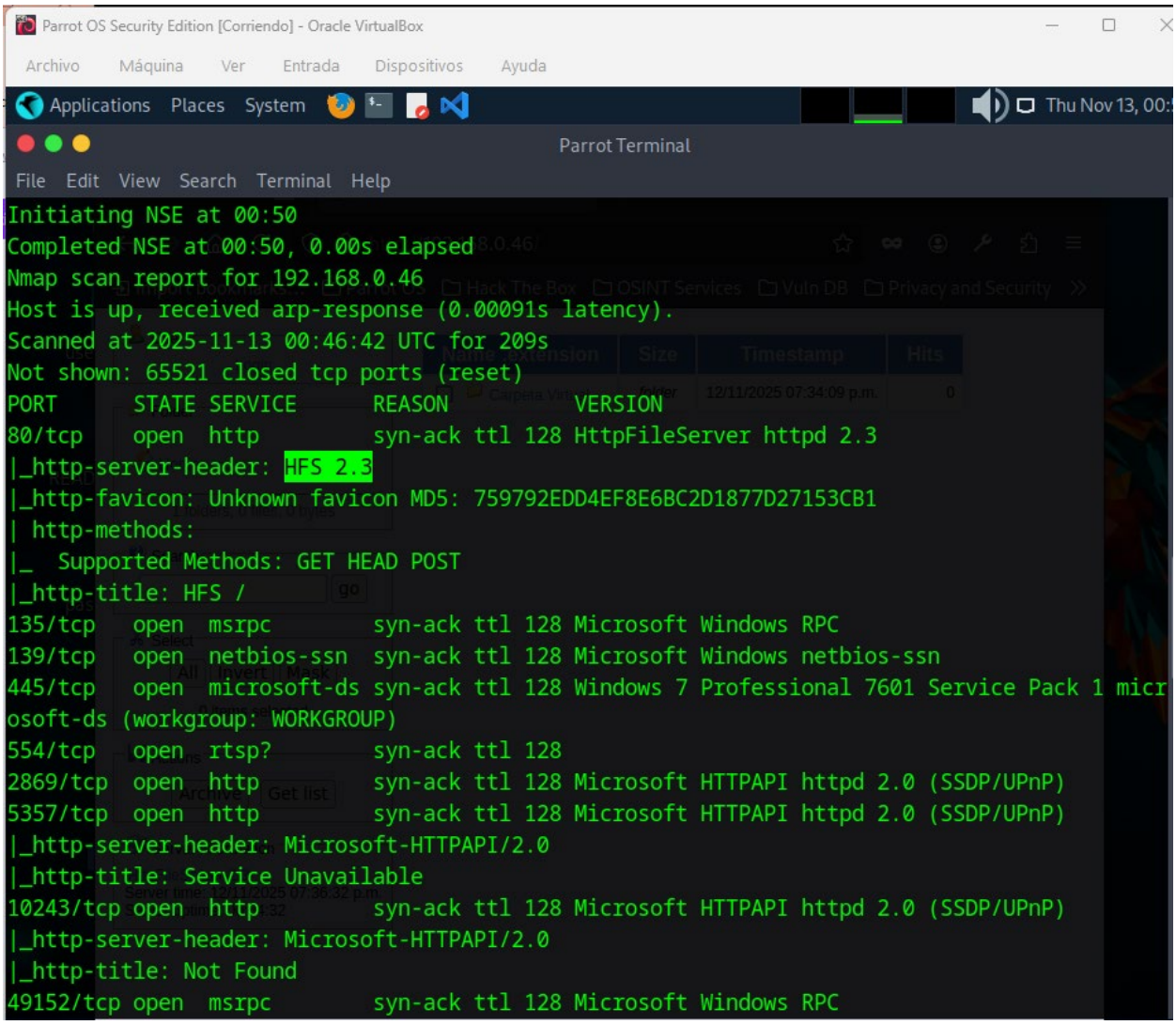
Escaneos de servicios con NMAP



Nota: Salida del comando nmap ejecutado desde Parrot OS, identificando el puerto 80 abierto.

Figura 2

Puerto 80 abierto



Nota: Salida del comando nmap mostrando el puerto 80 abierto y la presencia del servicio vulnerable Rejetto HFS

La tabla siguiente resume los hallazgos clave del reconocimiento:

Tabla 1

Síntesis de Hallazgos Clave en la Fase de Reconocimiento (Host-A)

Elemento identificado	Resultado
Servicio expuesto	Rejetto HFS en puerto 80
OS detectado	Windows 7
Acceso a red interna	No visible desde atacante

Nota. Esta tabla resume los elementos críticos identificados en el Host-A (192.168.0.46) tras el escaneo inicial de puertos y servicios, confirmando la exposición del servicio vulnerable Rejetto HFS y la alta superficie de ataque.

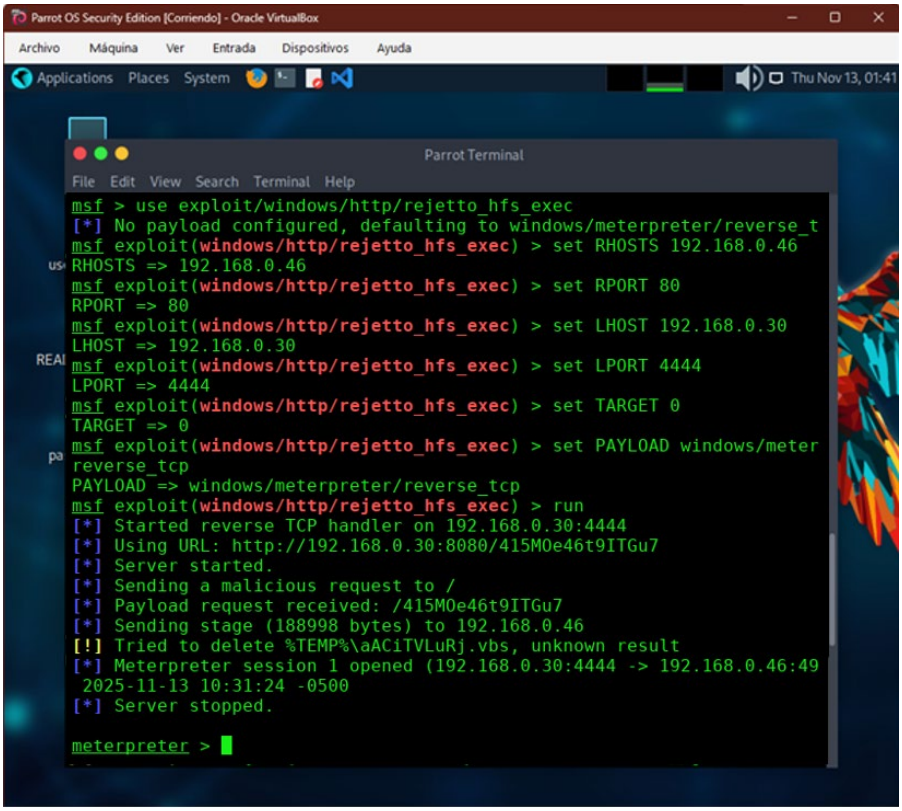
Explotación de la Vulnerabilidad en Host-A

La explotación del servicio vulnerable se efectuó mediante el módulo rejetto_hfs_exec de Metasploit. Este módulo aprovecha una vulnerabilidad que permite ejecutar código arbitrario enviando una cadena especialmente diseñada a través del servicio HTTP. Tras configurar los parámetros correspondientes al host objetivo y al equipo atacante, el exploit fue lanzado con éxito.

El uso de entornos deliberadamente vulnerables como Metasploitable 2 resulta común en escenarios de entrenamiento y simulación, ya que permite reproducir ataques reales de forma segura y controlada, facilitando el aprendizaje práctico de técnicas de explotación y post-explotación (Rapid7, 2012).

Figura 3

Configuración y Ejecución de metasploit



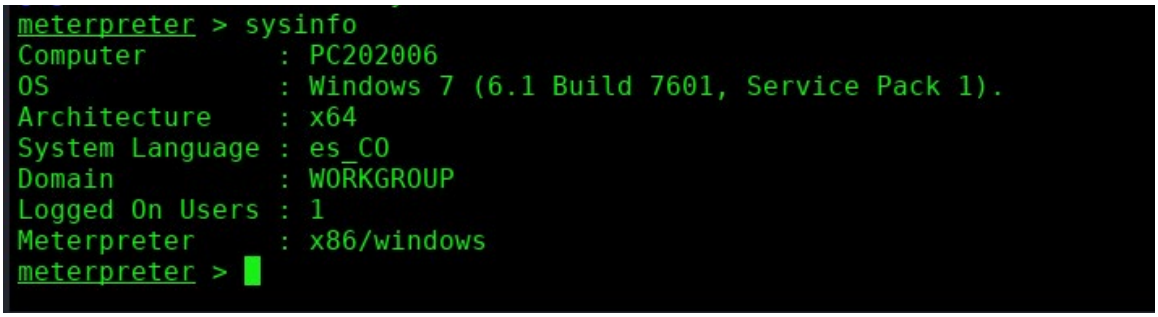
Nota: Muestra la configuración final de las opciones (RHOST, LHOST, LPORT) y la ejecución del comando run dentro de Metasploit, culminando con el mensaje de éxito que indica la apertura de la sesión Meterpreter.

Una vez establecida la sesión Meterpreter, se ejecutaron verificaciones para identificar el contexto del sistema. El comando sysinfo confirmó la versión del sistema operativo (figura 4)., mientras que getuid reveló el usuario bajo el cual corría el proceso vulnerable. El comando

ipconfig mostró la presencia de dos interfaces de red, una conectada a la red externa y otra a la red interna 10.10.10.0/24. Esta observación confirmó que Host-A funcionaba como puente entre la red del atacante y la red interna, lo que lo convertía en un objetivo estratégico

Figura 4

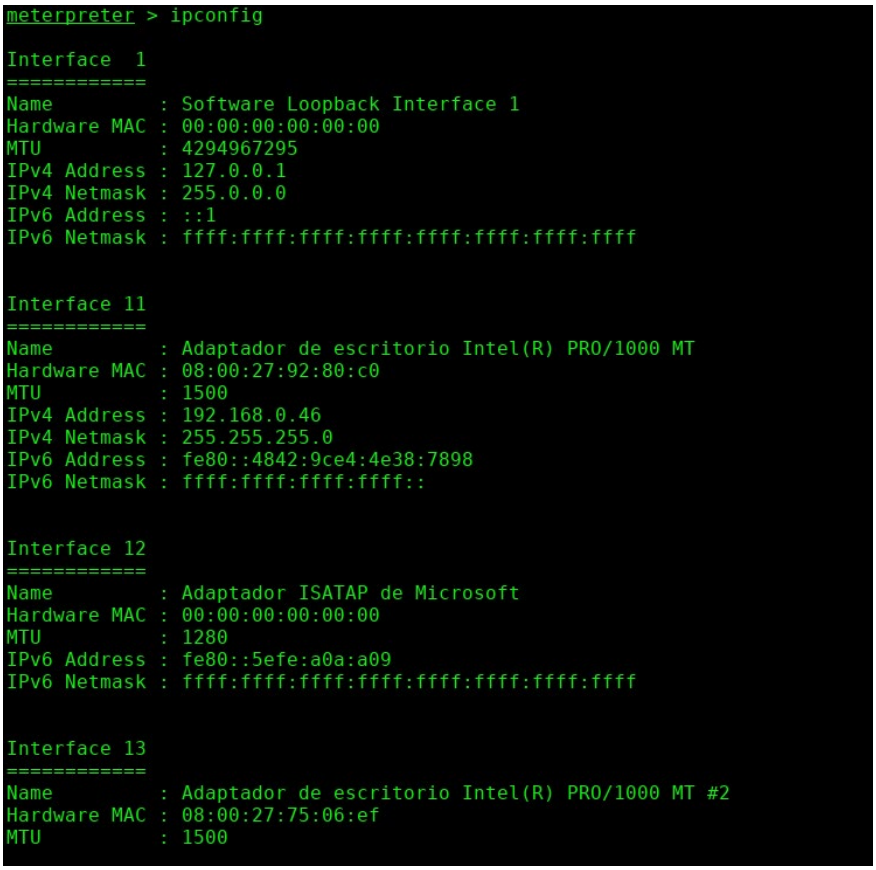
Verificación del Sistema Operativo del Host-A mediante sysinfo



Nota: Salida del comando sysinfo ejecutado en la sesión Meterpreter, confirmando la versión del sistema operativo del Host-A (Windows 7), esencial para posteriores acciones de post-explotación.

Figura 5

Descubrimiento de Interfaces de Red con ipconfig



Nota: Salida del comando ipconfig, mostrando las interfaces de red del Host-A, incluyendo la dirección IP expuesta al atacante.

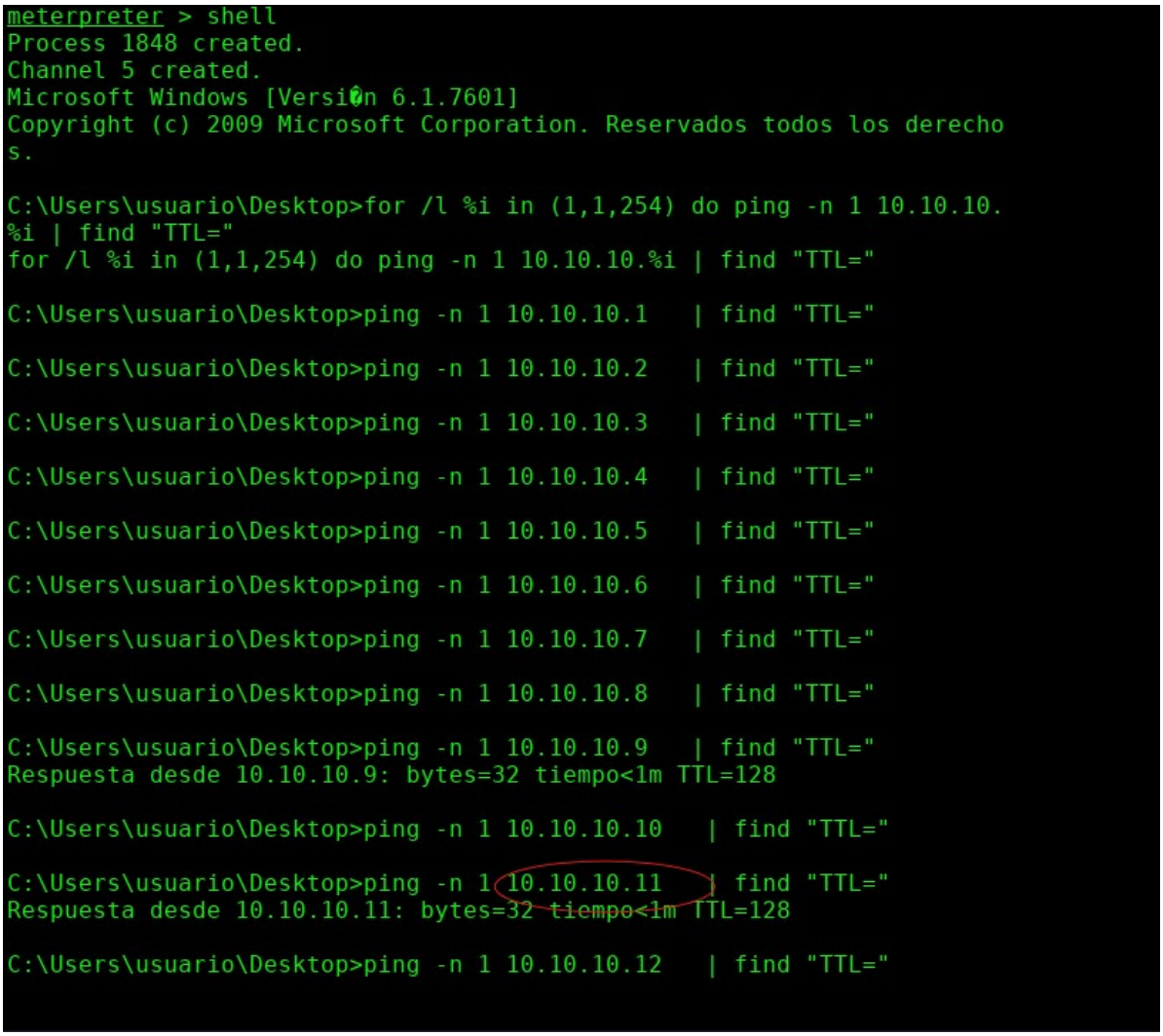
Post-Explotación y Descubrimiento de Host-B

Durante la post-explotación, se procedió a mapear la red interna. Para minimizar el ruido y evitar el uso de herramientas avanzadas, se empleó un barrido ICMP básico desde CMD. El comando utilizado iteraba sobre todas las direcciones posibles del segmento interno, mostrando únicamente aquellas que respondían.

Este barrido permitió identificar dos direcciones activas: la IP local del Host-A y la IP 10.10.10.11, correspondiente al Host-B. Este hallazgo confirmó la existencia de un servidor interno accesible únicamente desde Host-A, consistente con los registros observados en la fase de análisis de incidentes (figura 6).

Figura 6

Descubrimiento de Hosts Activos en la Red Interna (10.10.10.0/24)



Nota: Captura de la ejecución del barrido ICMP (*ping sweep*) desde la shell de Host-A, mostrando la respuesta válida (TTL=128) del objetivo secundario (Host-B) identificado en la dirección 10.10.10.11.

Pivoting: Redirección de Puertos a través de Host-A

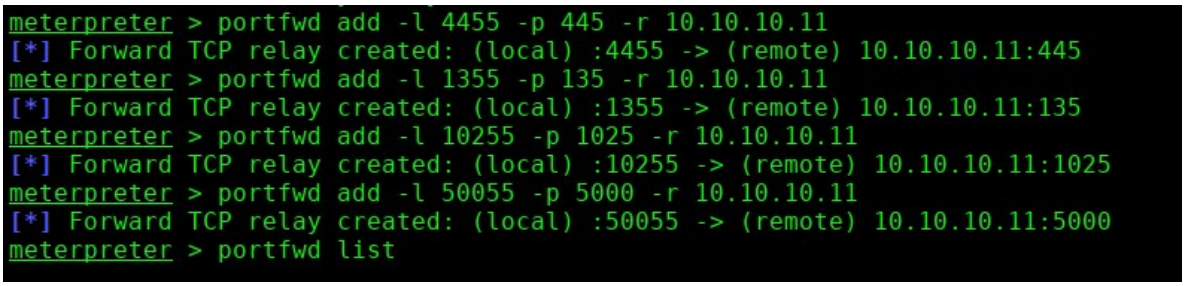
El descubrimiento de Host-B permitió iniciar el proceso de pivoting. Utilizando la sesión Meterpreter activa en Host-A, se generaron túneles mediante portfwd que permitieron al atacante acceder a puertos internos de Host-B como si se encontraran en su propia máquina. Este procedimiento transformó a Host-A en un puente silencioso y eficiente entre la red externa y la red interna.

Los túneles configurados cubrieron SMB, RPC y puertos dinámicos requeridos por PSExec. Sin estos túneles la comunicación sería imposible debido a la segmentación de la red.

Con estos túneles se garantizó la estabilidad del acceso remoto hacia Host-B.

Figura 7

Configuración de Túneles portfwd en Meterpreter para Pivoting hacia Host-B



Nota: Muestra la ejecución secuencial del comando portfwd add dentro de la sesión Meterpreter, estableciendo la redirección de puertos clave (445, 135, 1025 y 5000) de Host-B ($10.10.10.11$) a puertos locales específicos en la máquina atacante (Parrot OS), lo cual permite el acceso a servicios internos como SMB para el posterior movimiento lateral.

La siguiente tabla resume los túneles configurados:

Tabla 2

Resumen de la Configuración de Túneles portfwd para Acceso a Host-B

Puerto local (Parrot)	Puerto remoto (Host-B)	Función
4455	445	Canal SMB para PSExec
1355	135	Protocolo RPC
10255	1025	Puertos dinámicos
50055	5000	Puertos dinámicos

Nota: Se detallan los puertos locales configurados en la máquina atacante (Parrot OS) y su correspondiente puerto remoto en Host-B (10.10.10.11) mediante el comando portfwd add de Meterpreter. Estos túneles permiten la comunicación a través del host intermedio (Host-A) para ejecutar herramientas de movimiento lateral como psexec.py

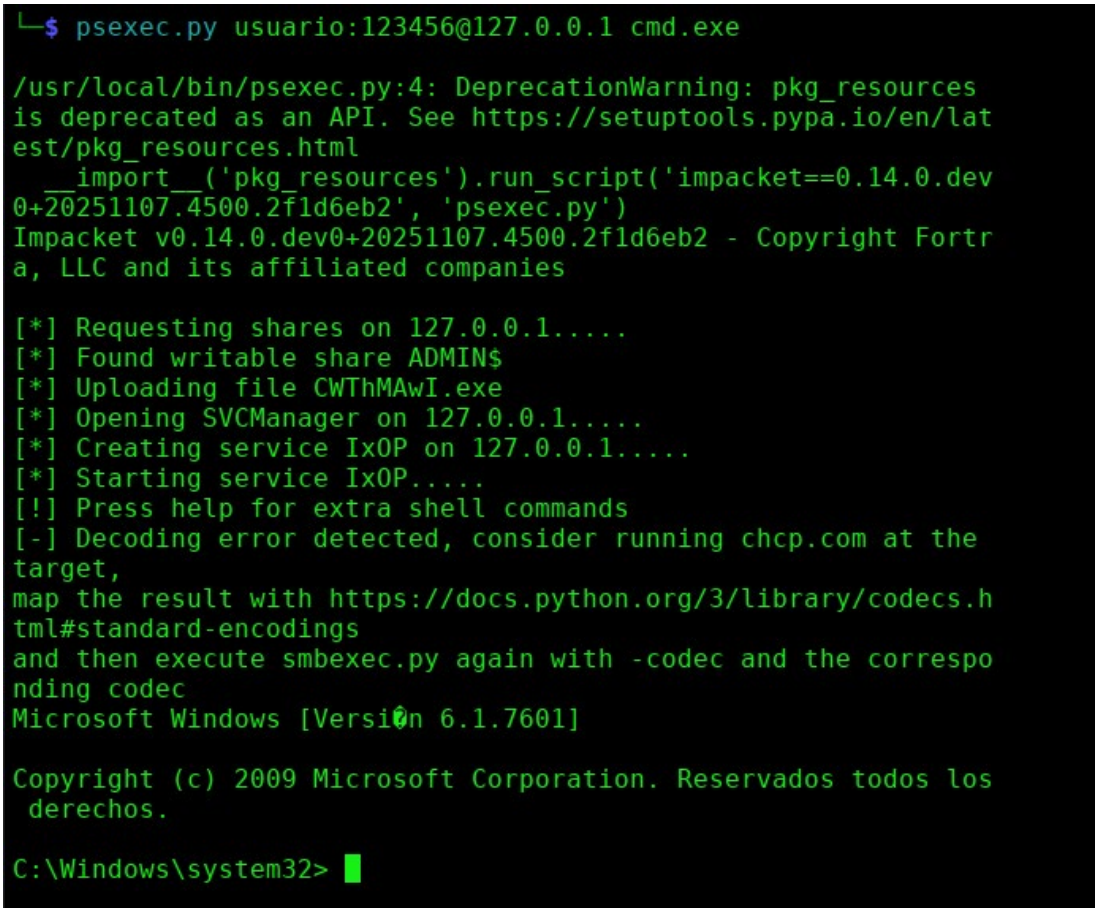
Movimiento Lateral: Compromiso de Host-B

Una vez establecidos los túneles, el atacante utilizó PSExec para conectarse a Host-B a través del puerto local redirigido. La autenticación fue exitosa y se desplegó una consola CMD con privilegios suficientes para realizar operaciones administrativas.

Este acceso confirmó que el pivoting había sido exitoso y que el atacante podía controlar Host-B sin necesidad de acceso directo a la red interna.

Figura 8

Movimiento Lateral Exitoso y Obtención de Consola CMD en Host-B Mediante psexec.py



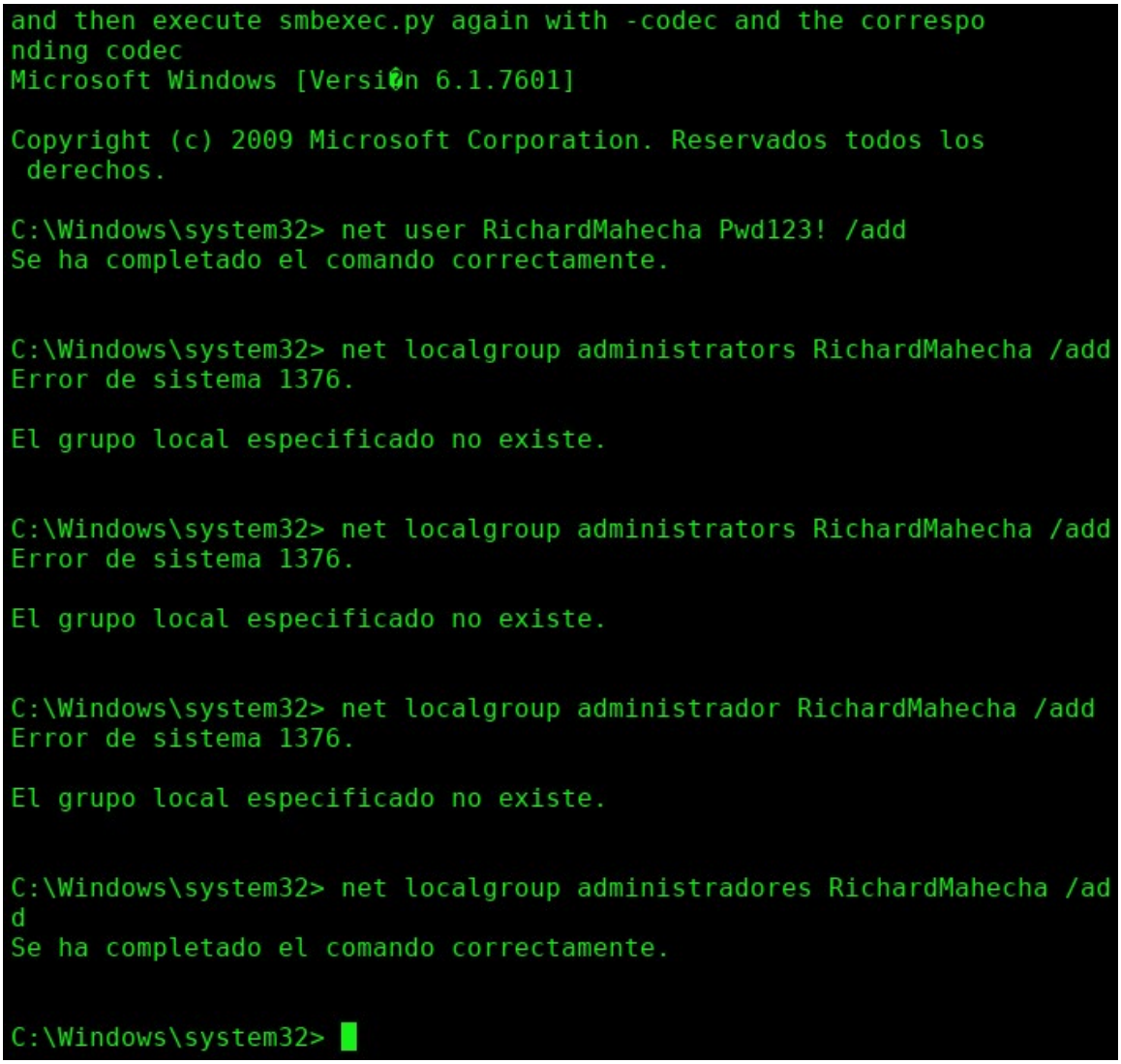
Nota: Captura de la ejecución del comando psexec.py dirigido al puerto local 4455 a través del túnel portfwd. La figura muestra la consola CMD interactiva obtenida en Host-B ($10.10.10.11$), confirmando que el pivoting y la inyección remota de servicios fueron exitosos, y que el atacante tiene la capacidad de ejecutar comandos arbitrarios en el objetivo final.

Prueba de Concepto: Creación de la Cuenta Efímera

La prueba de concepto consistió en demostrar que el atacante tenía capacidad para ejecutar acciones administrativas en Host-B. Para ello se creó una cuenta llamada “RichardMahecha”, se añadió al grupo Administradores y posteriormente se eliminó.

Figura 9

Creación y Elevación de Privilegios de Cuenta Administrativa Efímera

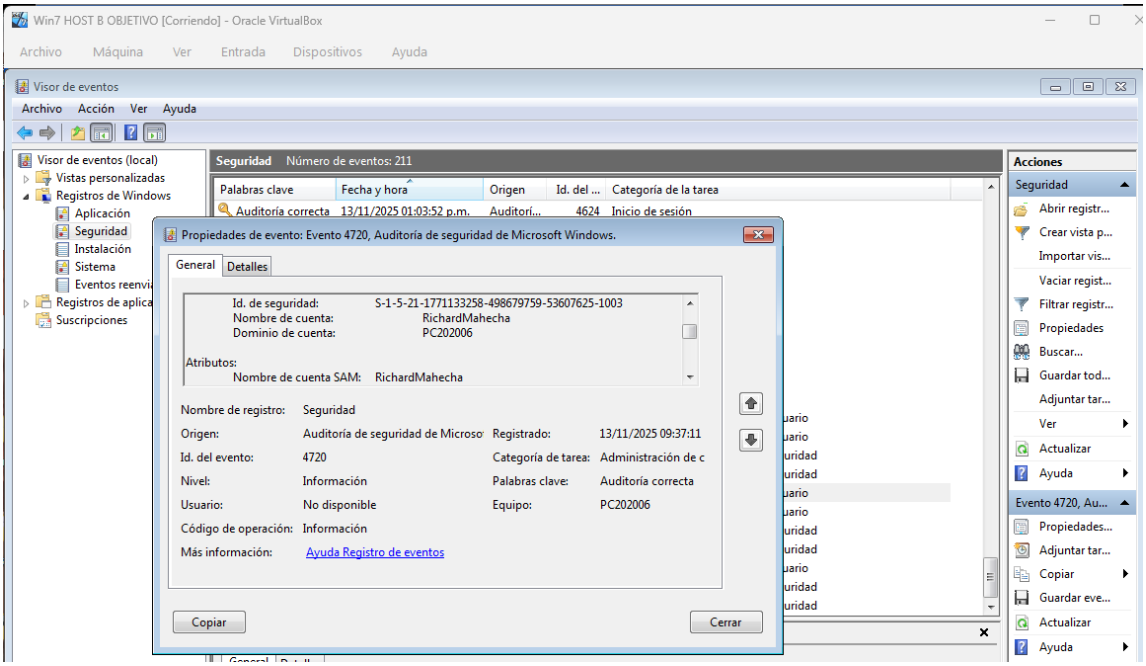


Nota: Muestra la ejecución de los comandos net user y net localgroup administradores desde la consola CMD de Host-B. Estos comandos confirman la creación exitosa de la cuenta de usuario temporal (RichardMahecha) y su adición al grupo de Administradores locales, demostrando el impacto y el control total obtenido en el sistema comprometido.

Todo el proceso quedó registrado en el visor de eventos, lo cual es esencial para auditorías posteriores.

Figura 10

Registro de la Creación de la Cuenta (Evento 4720)



Nota: Muestra la entrada en el Log de Seguridad del Visor de Eventos correspondiente al ID 4720 ("A user account was created"), que constituye la evidencia forense de la creación de la cuenta efímera (RichardMahecha), indicando la cuenta de servicio que originó el cambio.

La siguiente tabla presenta los eventos generados:

Tabla 3

Eventos de auditoría registrados en el log de seguridad de windows

ID Evento	Descripción
4720	Creación de cuenta
4728	Inclusión en Administradores
4729	Retiro del grupo

ID Evento	Descripción
4726	Eliminación de cuenta

Nota: Se listan los Identificadores de Evento de Auditoría ($ID \space Evento$) capturados en el Log de Seguridad de Host-B, que documentan cronológicamente las acciones realizadas sobre la cuenta administrativa efímera (creación, elevación de privilegios y limpieza/eliminación), cumpliendo con la fase de prueba de impacto y trazabilidad forense.

Impacto sobre la infraestructura Windows

El ejercicio demostró que una aplicación vulnerable con acceso externo puede comprometer por completo un sistema Windows, especialmente cuando este funciona como puente hacia redes internas. Host-A permitió al atacante no solo ejecutar código remoto sino también utilizarlo como plataforma de salto hacia Host-B. Este último quedó expuesto pese a encontrarse en un segmento aislado.

Diversos estudios han demostrado que los ejercicios Red Team permiten evaluar de forma realista la capacidad de una organización para resistir ataques avanzados, al simular tácticas, técnicas y procedimientos similares a los empleados por atacantes reales (Rajendran et al., 2011; Sanne, 2024).

Estrategias Blueteam

SecureNova Labs detectó en tiempo real indicios de un ataque informático que afectaba a uno de sus equipos Windows, identificado como Host-A, el cual formaba parte de un entorno segmentado conectado a otros activos internos críticos. Frente a esta situación, el equipo Blue Team activó un flujo estructurado de respuesta a incidentes, orientado a confirmar la intrusión, analizar el alcance del compromiso, contener la actividad maliciosa, erradicar los artefactos utilizados por el atacante y recuperar la estabilidad del sistema, aplicando buenas prácticas de ciberdefensa.

La respuesta se organizó siguiendo un ciclo de seis fases: detección del incidente, análisis inicial (triage), contención rápida, erradicación del ataque, recuperación del sistema y validación post-incidente. Sobre esta base, se combinó el análisis del sistema operativo, la revisión detallada de procesos y conexiones de red, la inspección del visor de eventos y la aplicación de acciones técnicas directas en el sistema comprometido, con el objetivo de impedir que Host-A siguiera siendo utilizado como punto de pivotaje hacia otros equipos, en particular hacia Host-B.

Detección del incidente

Análisis de procesos sospechosos (tasklist /v)

El primer paso consistió en determinar si el comportamiento del sistema operativo era coherente con un uso legítimo o si existían señales claras de actividad maliciosa. Para ello, en Host-A se ejecutó el comando tasklist /v, obteniéndose un listado detallado de procesos en ejecución, con información de PID, nombre de ejecutable, usuario asociado y estado.

El análisis de esta salida permitió identificar varios elementos que, considerados en conjunto, constituyeron indicadores de compromiso evidentes. En primer lugar, se observó el proceso hfs.exe (por ejemplo, con PID 2128), correspondiente a un servidor HTTP liviano que

no forma parte del conjunto estándar de servicios nativos de Windows. El hecho de que este binario estuviera en ejecución, escuchando conexiones, lo señaló como posible vector de entrada o canal de transferencia de archivos maliciosos.

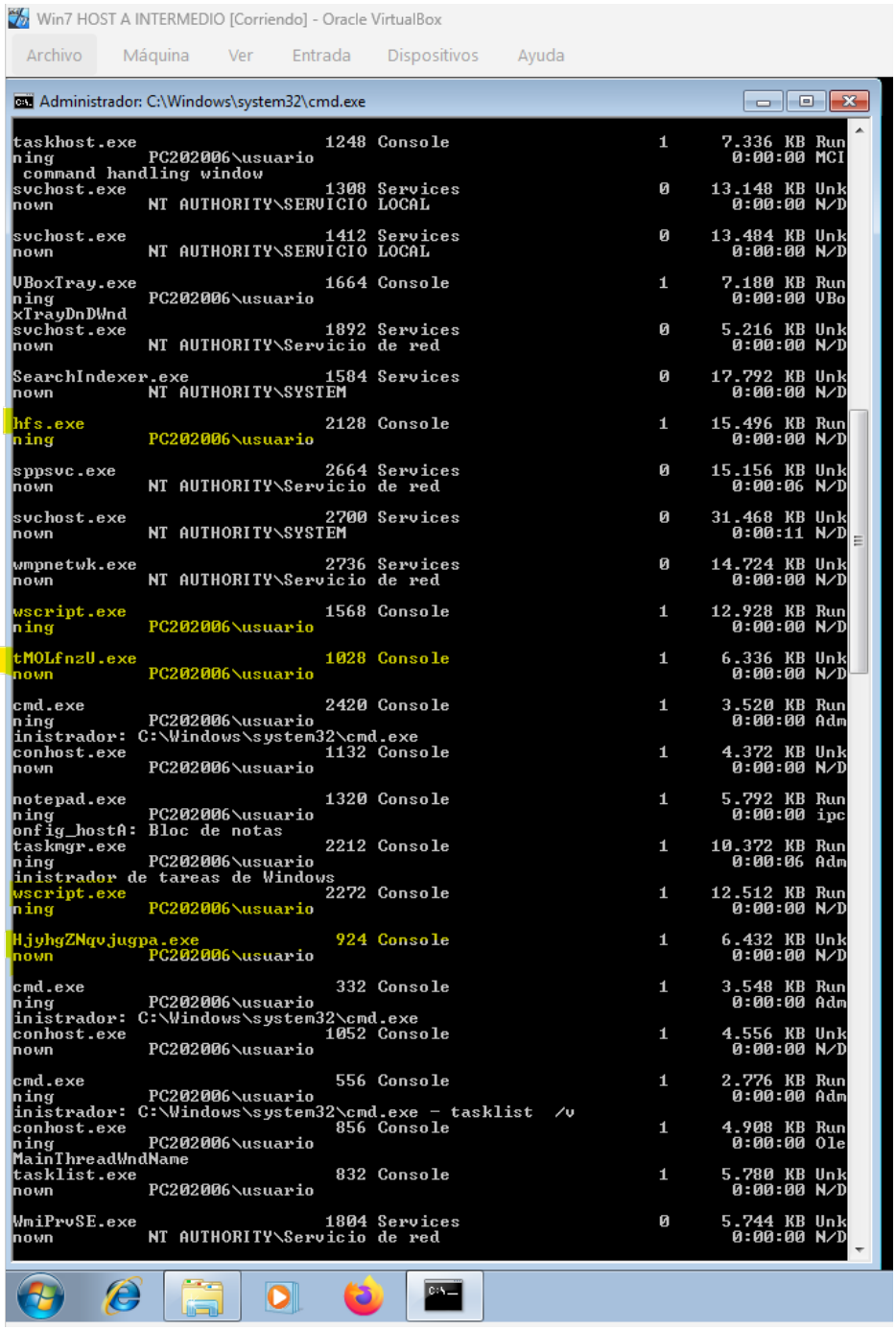
Adicionalmente, se detectaron ejecutables con nombres aleatorios, como tMOLfnzU.exe y HjyhgZNqvjugpa.exe, asociados a procesos en ejecución bajo PIDs concretos (por ejemplo 1028 y 924). Estos nombres no se corresponden con aplicaciones legítimas conocidas, ni con software corporativo desplegado en la organización, y son característicos de payloads generados de forma dinámica por herramientas de explotación o kits de malware. Su sola presencia es indicio de intrusión, pero su ejecución simultánea refuerza la conclusión de que el atacante logró introducir código arbitrario en el sistema.

Asimismo, se observaron múltiples instancias de wscript.exe, lo que indica la ejecución de scripts de Windows Script Host. En un entorno estándar, la ejecución repetida y paralela de wscript es anómala y suele asociarse a automatizaciones maliciosas, descarga de nuevos componentes, establecimiento de persistencia o ejecución silenciosa de comandos. A ello se suman varias consolas cmd.exe activas sin justificación por parte del usuario legítimo, lo cual es típico cuando un adversario interactúa de forma remota con la máquina comprometida o encadena comandos a través de un payload.

En conjunto, la presencia del servidor HFS activo, ejecutables con nombres aleatorios, múltiples instancias de wscript y consolas de comandos abiertas sin causa aparente constituyó una base sólida para afirmar que Host-A se encontraba comprometido.

Figura 11

Resultados del Comando tasklist e Indicadores de Compromiso (IOCs) en Host-A



Nota: Captura de la salida del comando tasklist /v ejecutado en el Host-A comprometido. Los procesos resaltados (incluyendo hfs.exe, ejecutables con nombres aleatorios como

tMOLfnzU.exe, y múltiples instancias de wscript.exe y cmd.exe) confirman la existencia de actividad maliciosa y el compromiso del sistema por parte de un atacante.

Análisis de conexiones de red activas (netstat -ano)

En paralelo con el análisis de procesos, se revisaron las conexiones de red mediante el comando netstat -ano, con el fin de identificar comunicaciones inusuales, puertos abiertos no autorizados y posibles canales de mando y control.

El análisis de esta salida mostró, en primer lugar, el puerto 80/TCP en estado LISTENING bajo el mismo PID asociado a hfs.exe. Esto confirmó que el servidor HTTP vulnerable estaba publicado y aceptando conexiones, por lo que podía haber servido tanto como vector inicial de explotación como canal de transferencia de payloads. Además, se identificaron múltiples conexiones en estado ESTABLISHED entre la IP interna de Host-A (10.10.10.9) y la dirección 10.10.10.11, por el puerto 445/TCP. Este puerto es utilizado por SMB y se asoció al PID 924, coincidiendo con uno de los ejecutables de nombre aleatorio previamente detectados. Este patrón sugiere que Host-A estaba siendo utilizado como plataforma de movimiento lateral hacia otro equipo interno (Host-B).

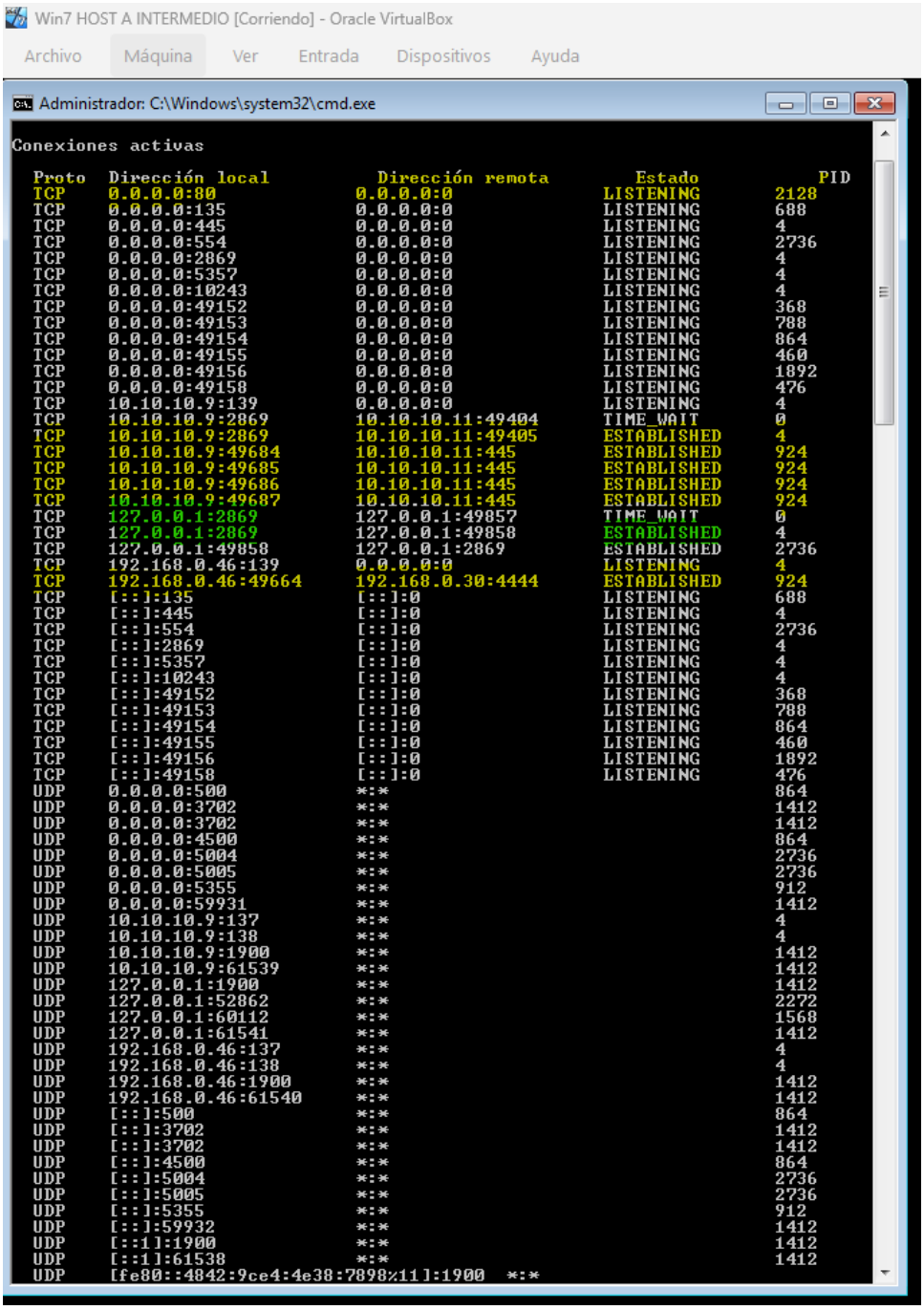
Adicionalmente, se observó una conexión establecida hacia la dirección 192.168.0.30:4444, también vinculada al PID 924. El puerto 4444 es comúnmente utilizado por múltiples frameworks de explotación como puerto por defecto para shells reversas, lo que refuerza la hipótesis de que el atacante mantenía control remoto sobre Host-A a través de una reverse shell activa. Finalmente, se detectaron conexiones en puertos como 2869, lo cual puede asociarse a actividad de descubrimiento o enumeración dentro de la red interna.

En suma, la combinación de un puerto 80/TCP asociado a un servicio no autorizado, conexiones SMB persistentes hacia un host interno y una conexión externa en un puerto típico de

reverse shell confirmó que el sistema no solo había sido comprometido, sino que además funcionaba como punto de pivotaje dentro del entorno de SecureNova Labs.

Figura 12

Salida del Comando netstat -ano y conexiones de red maliciosas en Host-A



Nota: Muestra el listado de conexiones de red activas en el Host-A comprometido. La figura destaca el servicio LISTENING en el puerto 80/TCP (PID 2128), la conexión de control remoto a 192.168.0.30:4444, y las conexiones ESTABLISHED a 10.10.10.11:445 (SMB), lo que confirma el control externo y el uso del Host-A como pivote para movimiento lateral.

Revisión del visor de eventos (event ID 4624)

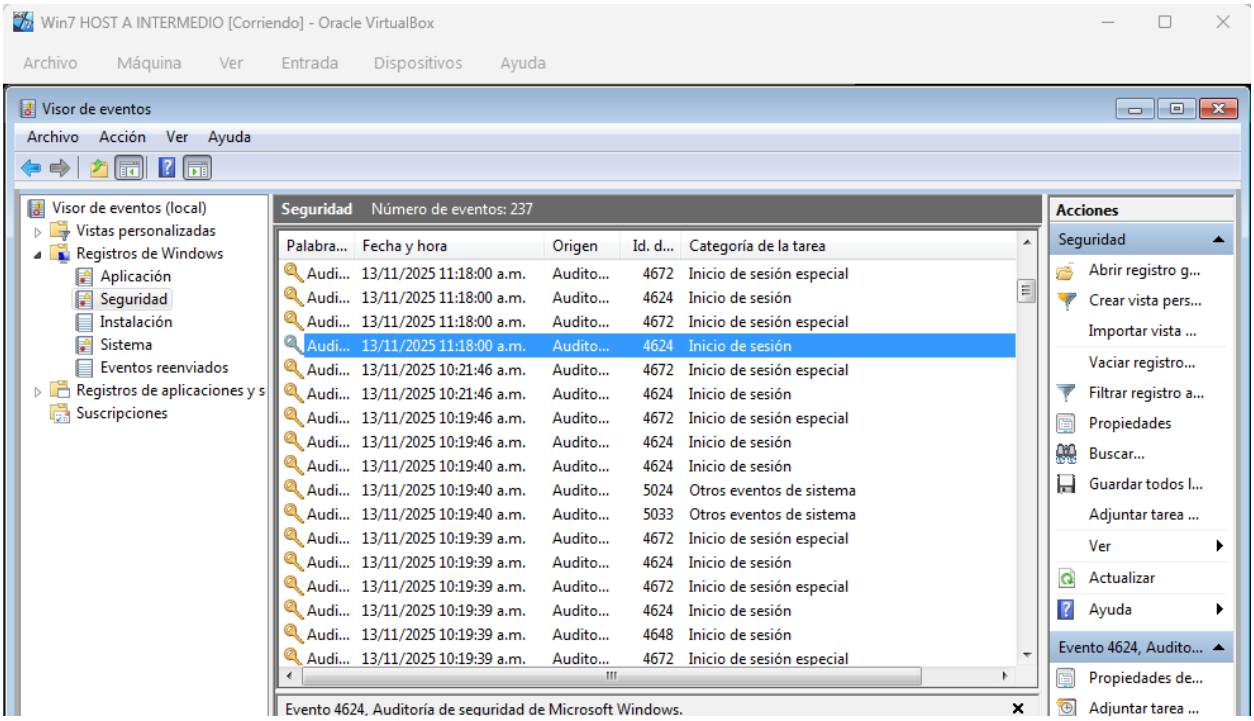
Complementando el análisis de procesos y conexiones, se procedió a revisar el Visor de eventos, enfocándose en el log de Seguridad y específicamente en los eventos con ID 4624, que corresponden a inicios de sesión exitosos. En un entorno normal, la frecuencia y el tipo de inicios de sesión suelen seguir patrones previsibles; sin embargo, en Host-A se identificó un número elevado de eventos 4624 en intervalos de tiempo muy cortos.

Este comportamiento es típico de sesiones remotas establecidas de forma repetitiva, ya sea mediante SMB, servicios de ejecución remota o herramientas de administración abusadas por el atacante. El análisis detallado de algunos de estos eventos (tipo de inicio de sesión, cuenta utilizada, equipo de origen) permitió inferir que el host había sido accedido desde ubicaciones no habituales, con una frecuencia y un horario que no correspondían a la operación normal del usuario legítimo.

Aunque el evento 4624 por sí solo solo indica un inicio de sesión exitoso, el patrón observado —múltiples logons en poco tiempo, combinados con la presencia de procesos sospechosos y conexiones de red anómalas— reforzó la conclusión de que existía actividad maliciosa y que el atacante se encontraba, o se había encontrado recientemente, interactuando con el sistema.

Figura 13

Análisis forense: Múltiples inicios de sesión exitosos (Evento ID 4624)



Nota. Muestra el Log de Seguridad en el Visor de Eventos del Host-A, destacando la presencia atípica y recurrente del Evento ID 4624 ("An account was successfully logged on"). La concentración de estos eventos en un corto período de tiempo constituye un Indicador de Compromiso (IOC) que sugiere el uso de herramientas de ejecución remota o el establecimiento repetitivo de sesiones por parte del atacante.

Análisis inicial (Triage)

Una vez confirmados los indicadores de compromiso, el Blue Team realizó el triage del incidente con el fin de determinar su criticidad, alcance y prioridad de respuesta. El triage combinó la información procedente de processes, red y eventos, y permitió construir una primera valoración técnica.

Se determinó que el proceso asociado al PID 924, identificado como uno de los binarios con nombre aleatorio, mantenía conexiones simultáneas hacia la IP del atacante (a través del puerto 4444/TCP) y hacia la IP interna 10.10.10.11 mediante SMB. Esto indica la existencia de una reverse shell activa hacia el exterior y actividad de movimiento lateral hacia el interior de la red. La presencia de múltiples instancias de wscript y cmd reforzó la idea de que, además de la ejecución remota interactiva, el atacante había desplegado scripts para automatizar ciertas tareas, como la ejecución de payloads o la persistencia de ciertas funcionalidades.

Este cuadro situó el incidente en un nivel de severidad crítico: el host comprometido no solo estaba bajo control del adversario, sino que además estaba siendo utilizado como trampolín para atacar otros sistemas internos. Por tanto, el triage concluyó que la contención debía ser inmediata, priorizando el corte de comunicaciones y la eliminación de los procesos maliciosos activos, para impedir que la intrusión se propagara y afectara la integridad de la infraestructura.

Contención rápida del ataque

Aislamiento de la interfaz de red comprometida

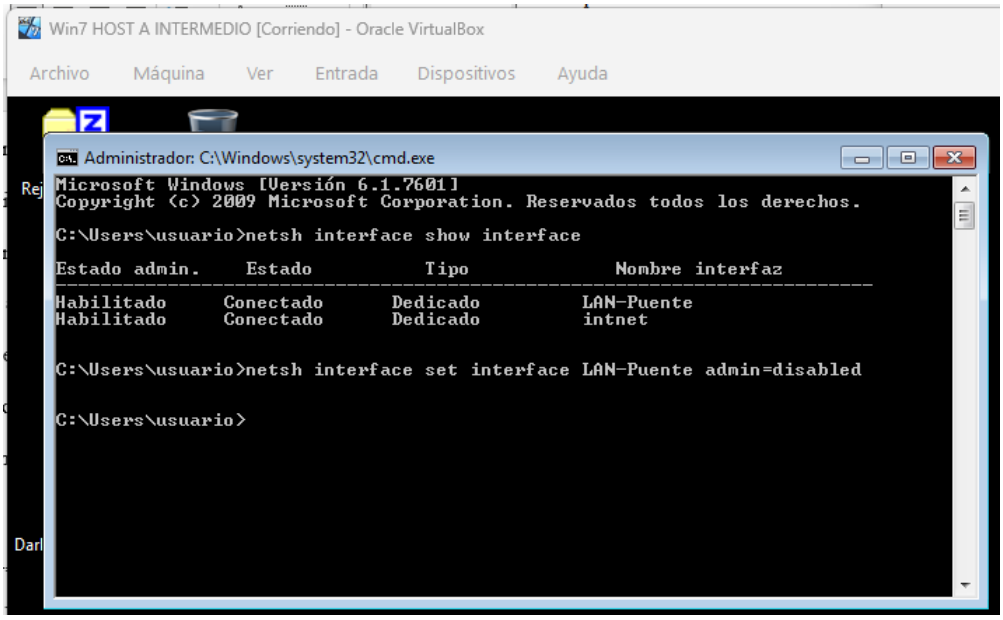
Como primera medida de contención, se decidió aislar Host-A de la red para cortar de inmediato las comunicaciones tanto con el atacante como con otros sistemas internos. Para ello se identificaron las interfaces de red mediante netsh interface show interface y posteriormente se deshabilitó la interfaz principal, asociada al modo puente de VirtualBox, con el comando:

```
netsh interface set interface "LAN-Puente" admin=disabled
```

Esta acción interrumpió las conexiones activas, incluyendo la reverse shell hacia 192.168.0.30:4444 y las conexiones SMB hacia 10.10.10.11, evitando que el atacante siguiera ejecutando comandos o propagando el ataque a otros equipos.

Figura 14

Deshabilitación de la interfaz de red comprometida para aislamiento



Nota. Muestra la ejecución de los comandos netsh interface set interface en el Host-A, deshabilitando la interfaz "LAN-Puente". Esta acción constituye el primer paso de contención al cortar inmediatamente la comunicación de la reverse shell del atacante y las conexiones SMB utilizadas para el movimiento lateral.

Terminación de procesos maliciosos

Tras el aislamiento de la red, el siguiente paso consistió en finalizar los procesos directamente ligados a la intrusión. Con base en la información obtenida en la fase de detección, se ejecutaron comandos taskkill dirigidos a los PIDs identificados como maliciosos:

taskkill /PID 924 /F

taskkill /PID 1028 /F

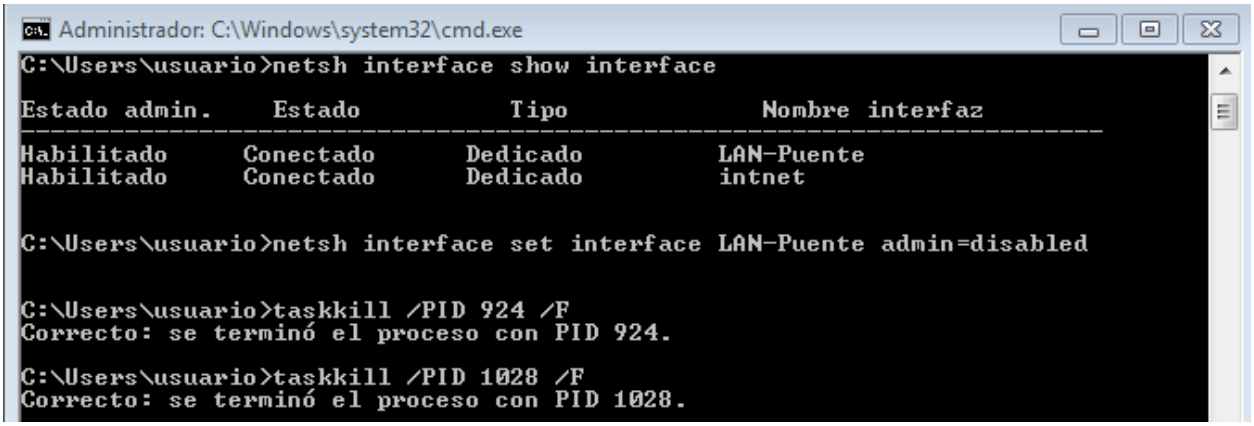
taskkill /IM wscript.exe /F

taskkill /IM cmd.exe /F

La terminación de estos procesos eliminó tanto la ejecución de los binarios sospechosos como la de los scripts y consolas que el atacante podría estar utilizando para mantener el control. Esta acción contribuyó a romper cualquier sesión activa en el host, incluso aunque existieran mecanismos de reconexión una vez restaurada la red.

Figura 15

Terminación forzosa de procesos maliciosos mediante taskkill



Nota. Muestra la ejecución de los comandos taskkill /PID para finalizar forzosamente los procesos maliciosos identificados (PIDs 924 y 1028) y los comandos taskkill IM para cerrar todas las instancias de wscript.exe y cmd.exe. Esto neutraliza el código malicioso activo y garantiza que el atacante pierde la capacidad de ejecución local.

Bloqueo de puertos utilizados durante la intrusión

Como complemento a la deshabilitación de la interfaz y eliminación de procesos, se configuró el firewall local de Windows para bloquear los puertos específicos utilizados durante el ataque: el puerto 80, asociado a HFS; el 445, asociado a SMB y movimiento lateral; y el 135, asociado a RPC. Los comandos utilizados fueron:

netsh advfirewall firewall add rule name="Bloqueo_HTTP_HFS" dir=in action=block protocol=TCP localport=80

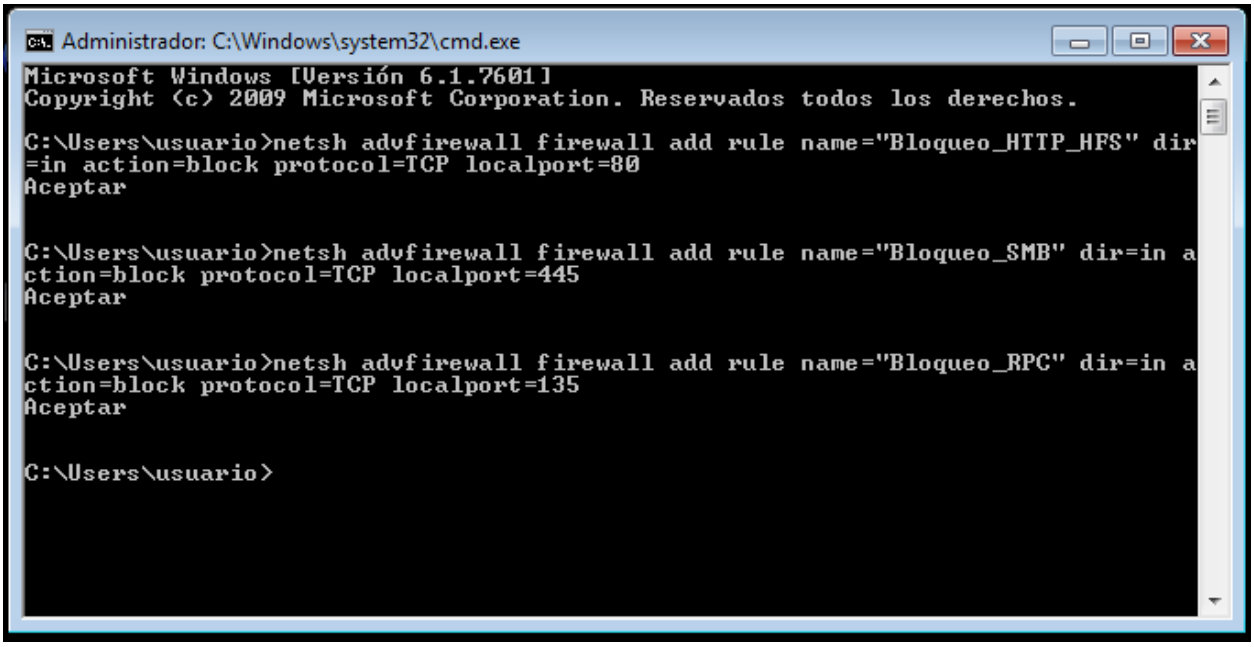
netsh advfirewall firewall add rule name="Bloqueo_SMB" dir=in action=block protocol=TCP localport=445

netsh advfirewall firewall add rule name="Bloqueo_RPC" dir=in action=block protocol=TCP localport=135

Aunque la interfaz principal se encontraba deshabilitada, la creación de estas reglas garantiza que, al momento de restaurar la conectividad, los puertos clave empleados por el atacante permanezcan restringidos, reduciendo la probabilidad de reuso inmediato del vector o de ejecución de técnicas similares.

Figura 16

Bloqueo de puertos de ataque mediante reglas del firewall avanzado de Windows



Nota. Muestra la ejecución de los comandos netsh add firewall add rule, creando reglas entrantes con acción de bloqueo para los puertos clave de la intrusión: 80/TCP (vector de HFS), 445/TCP (movimiento lateral SMB) y 135/TCP (RPC). Esta acción limita la superficie de ataque y previene la re-explotación mientras continúa la respuesta al incidente.

Resultado de la contención

Al finalizar la fase de contención, se consiguió detener la reverse shell activa, interrumpir las conexiones SMB utilizadas para movimiento lateral, cerrar los procesos que mantenían la ejecución de payloads maliciosos y desactivar el servicio HFS que sirvió como vector inicial. Gracias a ello, el sistema pasó de un estado de compromiso activo a un estado controlado, apto para iniciar las tareas de erradicación con menor riesgo de que el atacante siguiera operando en paralelo.

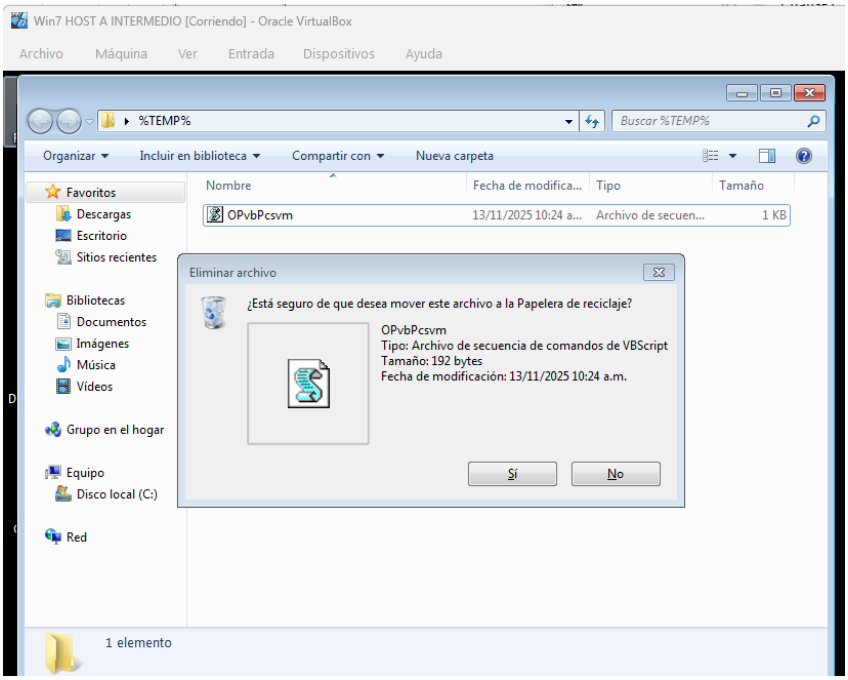
Erradicación del ataque

Eliminación de ejecutables maliciosos

La erradicación se centró en eliminar los artefactos que el atacante había introducido en el sistema. Basándose en la información de procesos, se localizaron los ejecutables con nombres aleatorios asociados a los PIDs previamente terminados, almacenados principalmente en directorios temporales del usuario o de Windows. Estos archivos fueron eliminados de forma manual y mediante comandos, asegurándose de que no quedaran copias residuales que pudieran volver a ejecutarse.

Figura 17

Eliminación de archivos ejecutables maliciosos remanentes



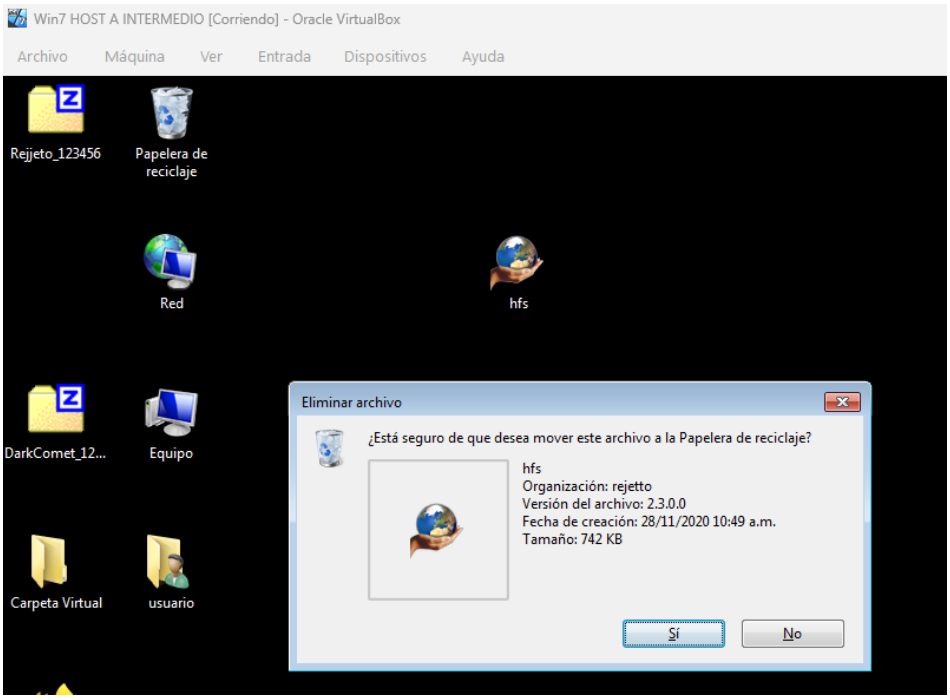
Nota. Muestra la eliminación de los archivos ejecutables con nombres aleatorios previamente identificados (asociados a PIDs 924 y 1028). Este paso es crucial en la fase de Erradicación para suprimir los artefactos de malware y prevenir la persistencia o reactivación de las cargas del atacante.

Eliminación del servicio HFS vulnerable

Dado que HFS fue uno de los elementos clave del ataque, se procedió a eliminar el ejecutable hfs.exe y cualquier archivo de configuración relacionado. De esta manera se desmontó completamente el servicio, cerrando de raíz el vector que había permitido la explotación remota.

Figura 18

Remoción del ejecutable vulnerable (HFS.exe)



Nota. Muestra la eliminación del ejecutable hfs.exe y sus archivos asociados. Esta acción elimina el vector de explotación original (servidor HTTP vulnerable en el puerto 80), asegurando la erradicación completa de la vulnerabilidad inicial que desencadenó el incidente.

Revisión de mecanismos de persistencia

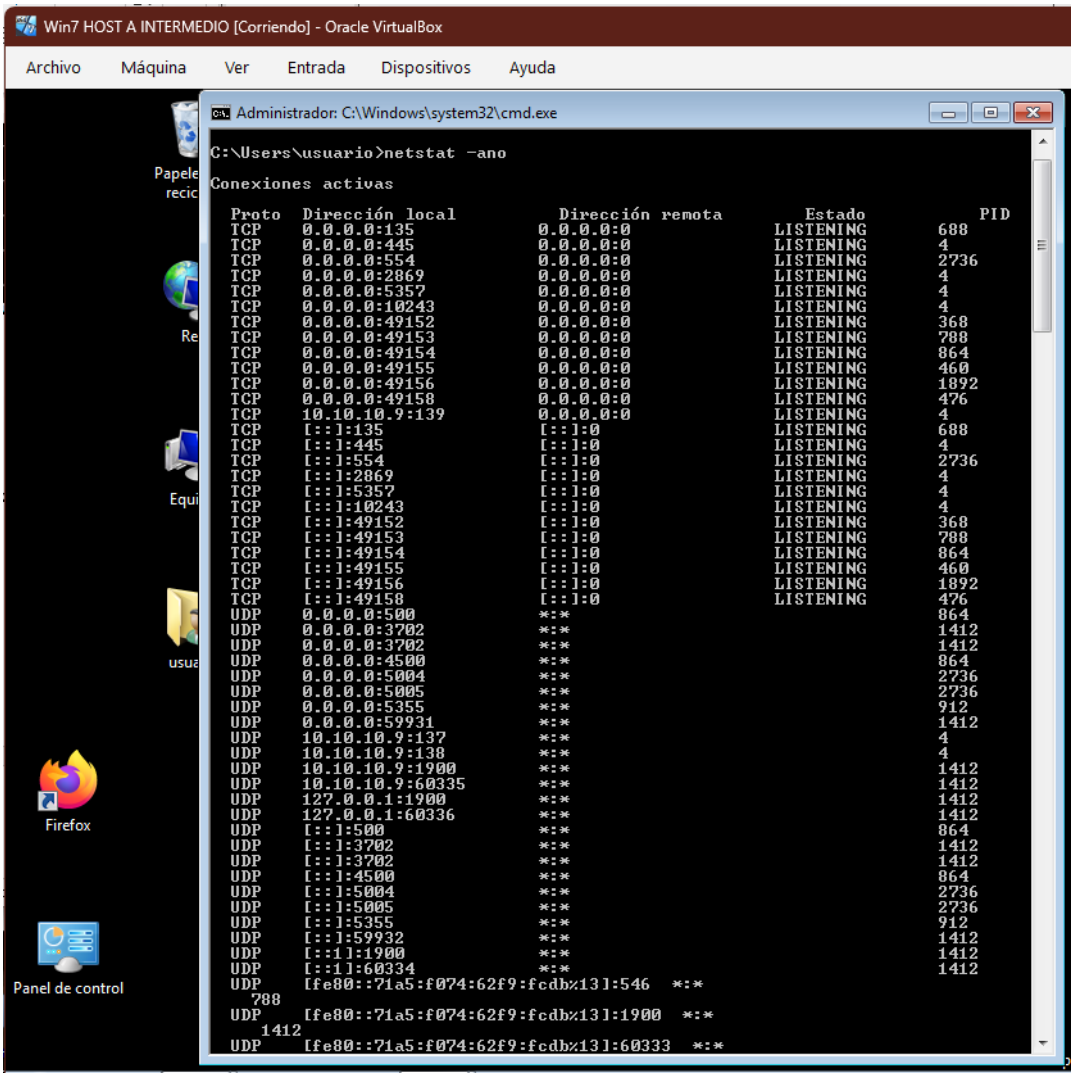
Como parte de la erradicación se revisaron posibles mecanismos de persistencia, incluyendo las claves de ejecución automática en el registro (Run de HKCU y HKLM), tareas programadas, carpetas de inicio y cualquier script asociado a wscript. Aunque no se identificaron servicios persistentes nuevos, se eliminaron scripts sospechosos en formatos como .vbs o .js, que hubieran podido servir como ganchos de reconexión en futuros reinicios.

Validación técnica tras la erradicación

Para verificar que no quedaban procesos activos relacionados con el ataque, se ejecutaron nuevamente comandos como tasklist /v y netstat -ano, constatando la ausencia de los PIDs maliciosos y de conexiones anómalas hacia el exterior o hacia otros sistemas internos. Esta validación confirmó que, al menos a nivel de procesos y conexiones, el sistema había sido limpiado de la actividad más evidente del atacante.

Figura 19

Validación post-erradicación: ausencia de conexiones maliciosas (netstat -ano)



Nota. Muestra la salida del comando netstat - ano ejecutado después de la fase de Erradicación. La ausencia de conexiones remotas inusuales (incluyendo los puertos 4444, 445 y 80) confirma la limpieza exitosa del Host-A, asegurando que el atacante ya no posee canales de control ni pivoting activos en el sistema.

Recuperación del sistema

Restauración controlada de la conectividad

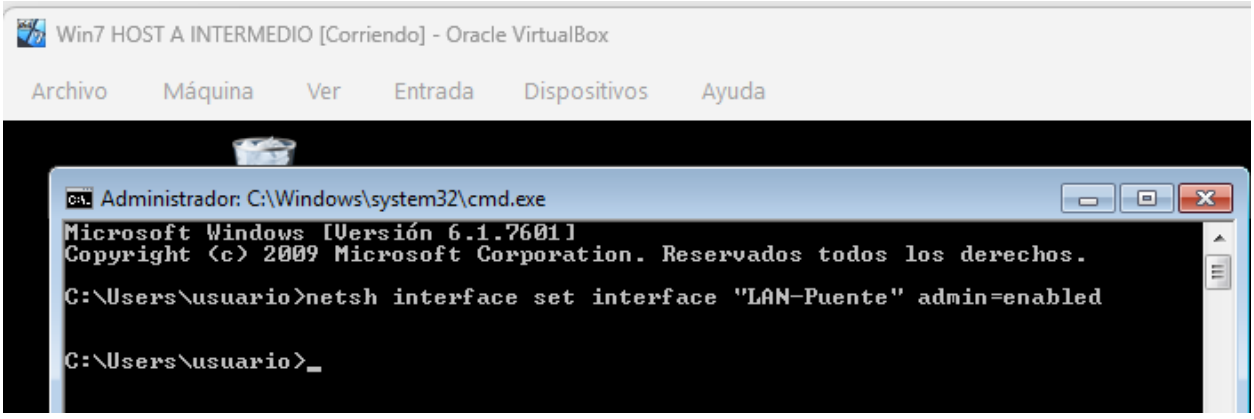
Una vez completada la erradicación, se procedió a reactivar la interfaz de red que había sido deshabilitada durante la contención, mediante:

netsh interface set interface "LAN-Puente" admin=enabled

Esta restauración se realizó manteniendo activas las reglas de firewall que bloqueaban los puertos críticos identificados, de modo que la conectividad del sistema se recuperó de forma controlada, reduciendo el riesgo de que el mismo vector de intrusión pudiera reutilizarse inmediatamente.

Figura 20

Restauración de la conectividad de red del Host-A



Nota. Muestra la ejecución del comando netsh interface set interface con el parámetro admin=enabled. Esta acción habilita nuevamente la interfaz de red ("LAN-Puente") del Host-A,

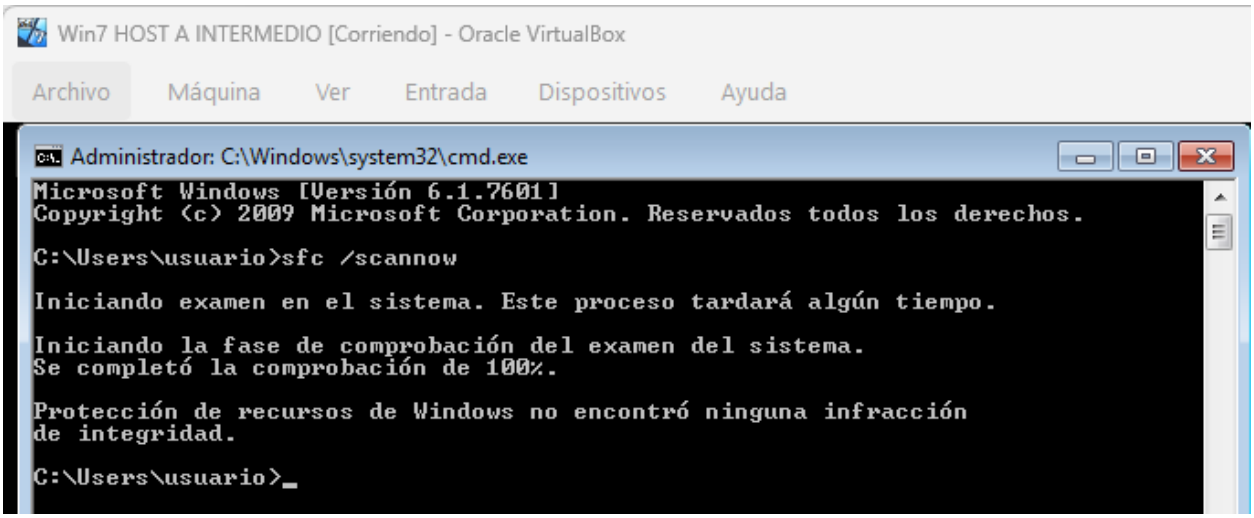
recuperando la conectividad del sistema una vez que se ha verificado la erradicación de todo el malware y artefactos del ataque.

Verificación de integridad del sistema operativo

Como medida adicional, se ejecutó la herramienta de comprobación de archivos del sistema (sfc /scannow), con el objetivo de detectar y reparar posibles modificaciones en archivos críticos de Windows que pudieran haber sido alterados por el atacante. Esta verificación contribuyó a asegurar que los componentes esenciales del sistema estuvieran en un estado consistente y confiable.

Figura 21

Verificación de la integridad del sistema operativo (SFC Scan)



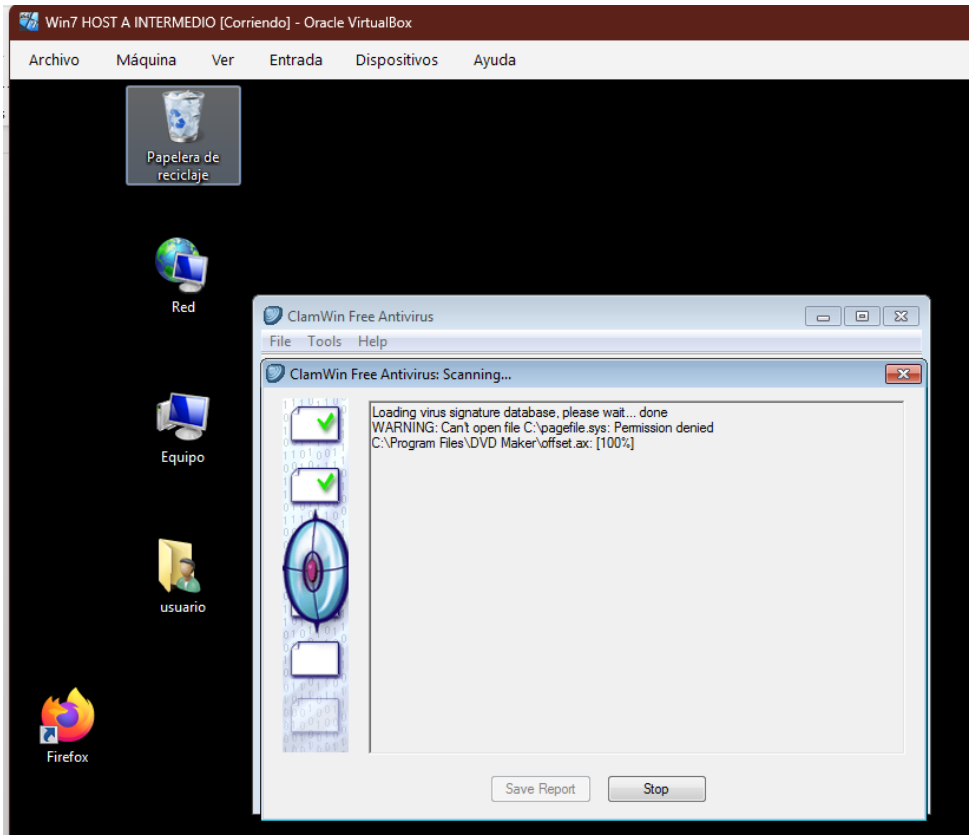
Nota. Muestra la ejecución de la herramienta nativa sfc scannow en la consola CMD. Este comando es ejecutado en la fase de Recuperación para escanear y reparar cualquier archivo esencial del sistema que pudiera haber sido modificado, dañado o corrompido por la actividad maliciosa durante el incidente, asegurando la confiabilidad operativa del Host-A.

Escaneos complementarios con herramientas GPL

Para reforzar la confianza en el estado del sistema, se utilizaron herramientas GPL como ClamWin y utilidades de análisis de procesos para realizar un escaneo profundo en busca de malware residual y comportamientos anómalos. Los resultados de estas herramientas no mostraron nuevas amenazas activas, lo que refuerza la conclusión de que la erradicación había sido efectiva.

Figura 22

Escaneo antivirus del sistema con ClamWin (Herramienta Open Source)



Nota. Muestra el resultado de la ejecución del escáner antivirus de código abierto ClamWin. Este escaneo se realiza como medida de validación complementaria post-erradicación, confirmando la ausencia de malware activo o artefactos residuales ocultos y garantizando una limpieza exhaustiva del sistema.

Monitoreo posterior a la recuperación

Durante un periodo de observación posterior a la reconexión (entre 15 y 30 minutos), se monitorizaron procesos, conexiones y eventos de seguridad (como 4624, 4672) en busca de reaparición de patrones sospechosos. No se registraron nuevas conexiones hacia la IP del atacante ni hacia puertos utilizados durante la intrusión, ni se observaron procesos inesperados, lo que permitió considerar el sistema en condiciones estables para su reintegración al entorno productivo simulado.

Validación post-incidente

La fase final consistió en verificar que no quedaban indicadores de compromiso activos y en evaluar la eficacia de las medidas adoptadas. Se revisaron de nuevo los eventos de seguridad para comprobar que no se producían nuevos intentos de autenticación anómalos, creación de cuentas no autorizadas o modificaciones de servicios relevantes. También se volvió a examinar el listado de procesos y conexiones activas.

Paralelamente, se documentó una línea de tiempo detallada del incidente, incluyendo detección, contención, erradicación y recuperación, así como las evidencias recopiladas. Esta documentación constituye un insumo fundamental para la mejora continua de los procedimientos y la definición de futuras estrategias de hardening.

Medidas de hardenización para evitar la repetición del ataque

A partir del análisis de este incidente, el Blue Team propuso un conjunto de medidas de hardenización orientadas a reducir la probabilidad de que un ataque similar vuelva a tener éxito:

- Eliminación del uso de HFS u otros servidores HTTP improvisados y sustitución por soluciones seguras con autenticación y cifrado.

- Restricción estricta de puertos y servicios, limitando el uso de SMB y RPC solo a donde sea indispensable y bajo controles adicionales.
- Implementación de mecanismos de control de ejecución (AppLocker, SRP) para impedir la ejecución de binarios no firmados desde ubicaciones no confiables y restringir el uso de motores de scripting.
- Fortalecimiento de SMB (deshabilitar SMBv1, activar firma de SMB, segmentar accesos) para dificultar el movimiento lateral.
- Aplicación del principio de privilegios mínimos, separando cuentas de usuario y administrativas.
- Activación de auditorías avanzadas (eventos 4624, 4625, 4672, 4688, entre otros) y revisión periódica de logs.
- Uso de herramientas GPL de monitoreo y detección (ClamAV, OSSEC/Wazuh, Sysmon, Yara) para mejorar la visibilidad sobre procesos y cambios en el sistema.
- Actualización del sistema operativo a versiones soportadas y adopción de un esquema de parchado continuo. (Scarfone & Mell, 2022)
- Segmentación de la red mediante VLAN y controles de acceso que limiten el impacto de un host comprometido. (CCN-CERT, 2018).

Diferencias entre Blue Team y Equipo de Respuesta a Incidentes (IR Team)

Aunque en este ejercicio el equipo Blue Team ejecutó fases propias de un IR Team, es importante distinguir sus roles. El Blue Team se centra en la defensa continua, el hardening, el monitoreo y la prevención. El IR Team entra en acción cuando un incidente se ha materializado y gestiona el ciclo específico de respuesta.

En la práctica, muchos de los pasos mostrados —como triage, contención y erradicación— son típicos de un IR Team. Sin embargo, el conocimiento y las herramientas utilizadas (como logs, firewalls, SIEM y normas CIS) son parte del trabajo habitual del Blue Team. En organizaciones maduras, ambos equipos trabajan de forma complementaria: el Blue Team fortalece y vigila; el IR Team actúa cuando el ataque ya está ocurriendo.

Uso del CIS dentro del Blue Team

El Center for Internet Security (CIS) se integra como referencia fundamental para el Blue Team (CIS Security, 2020). Los CIS Benchmarks proporcionan guías detalladas para endurecer sistemas operativos, servidores y dispositivos de red, ayudando a definir parámetros seguros, deshabilitar servicios innecesarios y reforzar controles de autenticación, permisos y auditoría. Por su parte, los CIS Controls ofrecen una hoja de ruta priorizada para gestionar activos, proteger datos, reducir la superficie de ataque y establecer controles mínimos imprescindibles.

En el contexto de este incidente, el uso sistemático de CIS habría permitido, por ejemplo, evitar que un servicio como HFS se ejecutara sin control, limitar el uso de puertos como 445 y 135 en estaciones de trabajo y activar registros suficientes para detectar comportamientos anómalos antes de que el atacante consolidara su posición.

Funciones y características principales de un SIEM en apoyo al Blue Team

Un SIEM se convierte en el núcleo de la capacidad de detección y análisis del Blue Team. Al centralizar los logs de servidores, estaciones de trabajo, dispositivos de red y aplicaciones, permite correlacionar eventos que, vistos por separado, podrían pasar desapercibidos (Zambrano Hernández et al., 2024). Su capacidad para normalizar registros heterogéneos, aplicar reglas de correlación, generar alertas en tiempo real y almacenar

información histórica para análisis forense resulta clave para identificar patrones como los observados en este ejercicio: múltiples eventos 4624 en poco tiempo, creación de procesos no habituales, conexiones externas a puertos de control remoto y actividad inusual en SMB.

Investigaciones previas resaltan que los sistemas SIEM constituyen un componente central en la detección y respuesta a incidentes, al permitir la correlación de eventos, el análisis forense inicial y la generación de alertas tempranas frente a comportamientos anómalos (Moreno, 2015).

Además, los dashboards y reportes del SIEM facilitan la visualización comprensible de la situación de seguridad, mientras que sus capacidades de soporte a auditorías ayudan a demostrar cumplimiento de normativas. Integrado con herramientas de orquestación (SOAR), un SIEM puede incluso automatizar respuestas iniciales como el aislamiento de un host o el bloqueo de una IP sospechosa, lo cual reduce los tiempos de reacción del Blue Team ante incidentes en curso.

Herramientas de contención de ataques informáticos

En escenarios más avanzados, el Blue Team puede apoyarse en herramientas específicas de contención. Wazuh, por ejemplo, permite desplegar agentes en endpoints que no solo monitorizan eventos, sino que también pueden ejecutar acciones remotas como finalizar procesos, eliminar archivos maliciosos o bloquear IPs sospechosas. CrowdStrike Falcon destaca por su capacidad de aislar máquinas de la red de forma inmediata, cortando el movimiento lateral y la exfiltración, mientras que SentinelOne combina análisis conductual con automatización y ofrece funcionalidades como el rollback, que permite revertir cambios realizados por malware o ransomware.

Estas herramientas, utilizadas de forma coherente con las políticas y procedimientos del Blue Team, convierten la detección en acción efectiva, cerrando el ciclo entre visibilidad, análisis y contención.

Análisis técnico

Visión general del proyecto y su importancia técnica

El desarrollo completo de las cuatro etapas constituye un ciclo realista de simulación de ciberataques y defensa corporativa, donde no solo se examina el componente técnico del hacking ético, sino que también se analizan los fundamentos legales, los principios profesionales y la articulación metodológica necesaria para ejecutar un ejercicio Red Team – Blue Team de manera controlada. A diferencia de un laboratorio tradicional, este proyecto integra contexto, teoría, técnica, incidente realista y respuesta operativa, reproduciendo las condiciones reales bajo las cuales opera un equipo de ciberseguridad moderno.

El escenario construido es especialmente relevante porque permite observar cómo un ataque aparentemente simple como la explotación de un servicio vulnerable puede desencadenar un compromiso profundo, afectando sistemas internos, configuraciones críticas y mecanismos de autenticación. Al mismo tiempo, demuestra cómo un equipo defensivo puede reconstruir el ataque a partir de indicadores forenses, contener al adversario y restablecer la integridad del sistema.

En suma, el proyecto no solo evalúa conocimientos, sino que forma una visión profesional integral, alineada con las funciones actuales de analistas de SOC, ingenieros de respuesta a incidentes, especialistas Red Team y arquitectos de seguridad.

Etapa 1: Fundamentos, Construcción del Laboratorio y Metodología

La Etapa 1 desarrolla los cimientos conceptuales y operativos que permiten ejecutar el resto del proyecto. Esta etapa no es meramente introductoria: cumple una función técnica esencial. Define las bases metodológicas que se aplicarán posteriormente en las fases ofensivas y defensivas, y establece las reglas del entorno experimental donde se ejecutará el ataque.

Desde el punto de vista metodológico, la adopción del *Penetration Testing Execution Standard (PTES)* no solo organiza la estructura del ataque, sino que también permite emplear una metodología reconocida en la industria (Álvarez, 2018). PTES garantiza que el ejercicio no sea improvisado, sino replicable, documentado y trazable (Palomo Luna et al., 2024). Esto incluye cumplir el ciclo:

- Reconocimiento (identificar superficies accesibles)
- Modelado de amenazas (definir riesgos y rutas de ataque)
- Análisis de vulnerabilidades (identificar debilidades explotables)
- Explotación (ejecutar el ataque de forma controlada)
- Post-explotación (tomar control y profundizar acceso)
- Reporte (documentar toda la operación)

La construcción del laboratorio virtual cumple con estándares profesionales: aislamiento de la red, segmentación de equipos, control total del entorno y uso de sistemas desarrollados para ofensiva (Parrot OS) y para simulación de víctimas (Windows 7 vulnerable). Este diseño no solo reproduce un entorno real, sino que también introduce la importancia de la arquitectura de red en la seguridad. La doble interfaz de Host A, por ejemplo, es un vector clave que condiciona toda la operación de las etapas 3 y 4, pues permite al Red Team pivotar y al Blue Team comprender por qué el ataque pudo expandirse.

Finalmente, la Etapa 1 sirve como puente conceptual entre el estudio de la vulnerabilidad y la acción ofensiva que se verá más adelante, demostrando que un ataque técnico solo es posible cuando existe un entendimiento profundo del entorno (Zuluaga Mateus, 2017).

Etapa 2: Análisis ético, legal y profesional del escenario

La Etapa 2 complementa la parte técnica con el componente ético–legal, indispensable para que un profesional de ciberseguridad opere dentro de los límites permitidos. Este análisis es extremadamente relevante porque un ejercicio Red Team sin autorización o sin parámetros éticos puede convertirse en una actividad ilegal.

En esta etapa se analiza detalladamente un acuerdo de confidencialidad que, en apariencia, busca formalizar el ejercicio; sin embargo, algunas de sus cláusulas implican prácticas que contravienen la Ley 1273 de 2009, especialmente en temas como acceso no autorizado, interceptación de comunicaciones, alteración de datos y manipulación de sistemas. El estudiante detecta estas inconsistencias y demuestra conocimiento del marco penal aplicable a delitos informáticos.

Esto revela un elemento crítico:
El experto en ciberseguridad no solo debe saber cómo atacar y defender sistemas, sino cuándo, cómo y bajo qué marco puede hacerlo.

Asimismo, la Etapa 2 refuerza principios deontológicos del COPNIA: responsabilidad, integridad, respeto por la ley y obligación de no causar daño. Este análisis permite comprender que las etapas 3 y 4 solo pueden ejecutarse bajo condiciones éticas y con plena claridad de las responsabilidades implicadas.

En síntesis, la Etapa 2 demuestra madurez profesional al reconocer que el conocimiento ofensivo implica también un compromiso moral y legal.

Etapa 3: Estrategia Red Team – Reconstrucción del Ataque Completo

La Etapa 3 constituye la ejecución ofensiva central del proyecto. Su análisis técnico permite comprender de manera profunda no solo cómo se compromete un sistema, sino por qué el ataque tiene éxito y cómo evoluciona dentro de una arquitectura de red.

Reconocimiento y descubrimiento del vector de entrada

Con herramientas como Nmap, el atacante identifica el puerto 80 abierto con el servicio vulnerable Rejetto HFS. Esta fase demuestra la importancia de la exposición de servicios y la falta de parches en sistemas obsoletos como Windows 7.

Explotación y obtención de control remoto

La explotación con Metasploit utilizando rejetto_hfs_exec permite obtener una sesión Meterpreter, que habilita capacidades como:

- ejecución de comandos,
- inspección del sistema,
- enumeración de interfaces,
- reconocimiento de la red interna,
- preparación para pivoting.

El atacante identifica que Host A tiene dos interfaces: una hacia la red del atacante y otra hacia la red interna.

Movimiento lateral mediante pivoting

La clave técnica de esta etapa es el uso de túneles portfwd para reenviar tráfico hacia Host B, haciendo que el atacante pueda comunicarse con el servidor interno aunque no tenga acceso directo.

Esto reproduce fielmente las tácticas MITRE ATT&CK asociadas a:

- T1572 (Protocol Tunneling)
- T1090 (Proxy)
- T1021.002 (SMB/Windows Admin Shares)

Compromiso de Host B

El uso de PSExec a través del túnel permite:

- autenticación remota,
- ejecución de comandos con privilegios,
- demostración de impacto creando y eliminando cuentas administrativas.

Esta etapa refleja el avance de un intruso desde un perímetro externo hacia un sistema crítico interno, demostrando lo devastador que puede ser un sistema puente comprometido.

Etapa 4: Estrategia Blue Team – Respuesta, Contención y Eradicación del Incidente

La Etapa 4 ofrece un análisis defensivo completamente coherente con lo detectado en la Etapa 3, porque las evidencias encontradas (procesos, conexiones, eventos) corresponden exactamente con las actividades ofensivas ejecutadas anteriormente.

Detección del ataque

El uso de herramientas nativas de Windows (tasklist, netstat, Visor de eventos) permite identificar:

- procesos maliciosos con nombres aleatorios,
- scripts automatizados ejecutados por wscript,
- varias consolas cmd asociadas a control remoto,
- un servicio HTTP no autorizado en ejecución,
- conexiones externas persistentes (reverse shell),
- actividad SMB hacia la red interna.

Esto demuestra que un Blue Team bien entrenado puede detectar actividad hostil incluso sin herramientas avanzadas.

Contención rápida

El Blue Team ejecuta una estrategia efectiva:

- aislamiento de la interfaz de red,
- cierre de procesos maliciosos,
- eliminación de payloads,
- bloqueo de puertos utilizados por el atacante (80, 135, 445),
- neutralización del vector de entrada (HFS).

Estas acciones rompen la cadena de ataque, invalidan la reverse shell y evitan que el atacante continúe escalando o moviéndose lateralmente.

Erradicación y limpieza profunda

Mediante análisis de persistencia, eliminación de archivos ejecutables, verificación de claves de registro y limpieza de scripts, el Blue Team asegura que no queden mecanismos de reactivación.

Recuperación y validación

Se restaura conectividad, se valida integridad del sistema con SFC y se ejecutan herramientas GPL como ClamWin. El monitoreo posterior confirma que el sistema opera sin indicadores de compromiso.

Esta etapa demuestra un ciclo completo de respuesta a incidentes, siguiendo prácticas de NIST 800-61.

Integración Profunda de Etapas: Un Ataque–Defensa de Ciclo Completo

Al integrar las etapas, se observa un ejercicio de ciberseguridad completo:

- La Etapa 1 prepara el escenario: Sin el laboratorio correctamente segmentado, el pivoting no podría ocurrir y el análisis Blue no tendría sentido.
- La Etapa 2 establece los límites: Sin comprender la legalidad y ética, la explotación técnica sería inapropiada o incluso delictiva.
- La Etapa 3 demuestra cómo un ataque avanza en un entorno realista: Se observa la cadena completa: exposición, explotación, persistencia, pivote, compromiso interno.
- La Etapa 4 reconstruye el ataque y ejecuta defensa estructurada: El Blue Team identifica exactamente los rastros que deja el Red Team, mostrando un ejercicio completamente trazable.

En conjunto, el proyecto exhibe el ciclo ATAQUE–DETECCIÓN–CONTENCIÓN–ERRADICACIÓN–RECUPERACIÓN, fundamental en la operación real de SOCs y equipos de seguridad corporativos (Arroyo, 2025).

Relación con aspectos legales y éticos

Relación entre el ejercicio Red Team – Blue Team y la Ley 1273 de 2009

La Ley 1273 de 2009 constituye el marco jurídico fundamental que regula los delitos informáticos en Colombia, estableciendo sanciones para actividades como el acceso no autorizado, la interceptación de datos, la alteración de información y la afectación de la disponibilidad o integridad de los sistemas. Este marco legal es esencial para comprender los límites dentro de los cuales un profesional de ciberseguridad debe operar, especialmente cuando se realizan prácticas técnicas que involucran explotación de vulnerabilidades y manipulación de sistemas. La Etapa 2 permite identificar que muchas de las acciones realizadas posteriormente en el ejercicio Red Team, como la explotación del servicio HFS, la obtención de acceso remoto mediante herramientas de post-explotación o el movimiento lateral dentro de la red, serían consideradas delitos graves si se ejecutaran fuera de un entorno autorizado. Esto demuestra que la mera capacidad técnica para comprometer un sistema no implica permiso para hacerlo y que cualquier actividad de pentesting requiere un alcance claramente definido, un contrato formal y la autorización expresa del dueño del sistema.

La revisión crítica del acuerdo de confidencialidad presentado en esta etapa evidencia la necesidad de que todo ejercicio de ciberseguridad esté respaldado por documentos legales bien construidos y precisos. Un documento mal redactado o ambiguo podría inducir al profesional a cometer acciones que excedan el alcance permitido o que incluso configuren delitos según los artículos contemplados en la Ley 1273. Por ello, el análisis jurídico realizado no solo sirve como ejercicio académico, sino como una advertencia clara sobre las consecuencias legales de actuar sin permiso o de forma imprudente en sistemas reales.

En el contexto colombiano, el análisis de los delitos informáticos no solo debe abordarse desde la técnica, sino también desde su interpretación jurídica, considerando la eficiencia y aplicación real de la normativa vigente en la persecución de estas conductas (Guarnizo Portela, 2024; Rincón Arteaga et al., 2022).

Responsabilidad ética del analista según los principios del COPNIA

Los principios éticos del COPNIA complementan el marco legal y establecen el comportamiento esperado de un profesional de ingeniería y tecnologías en Colombia (COPNIA, 2015). Estos principios enfatizan la responsabilidad social, la integridad, el respeto por la ley, la transparencia en las acciones, la protección del bienestar público y la obligación de no causar daño. La Etapa 2 demuestra una comprensión profunda de estos principios al cuestionar cláusulas del acuerdo que podrían comprometer la legalidad o la ética del ejercicio. Para un analista de ciberseguridad, ejercer sus habilidades implica asumir un compromiso con la protección del entorno digital y con la garantía de que su trabajo no será utilizado para perjudicar a terceros.

La práctica ofensiva vista en la Etapa 3 solo es ética porque se realiza dentro de un laboratorio controlado, con sistemas diseñados para ser vulnerados y bajo un marco académico formal. La ética profesional exige que, incluso dentro de estos contextos, se actúe con rigurosidad y con un entendimiento claro de que cualquier comportamiento irresponsable podría causar daños reales. La Etapa 2 permite establecer esta base ética al recordar que la confianza depositada en el profesional depende de su integridad y de su respeto por los principios que rigen la práctica de la ingeniería.

Conexión entre ética, legalidad y la ejecución del ataque Red Team

La ejecución del ataque ofensivo en la Etapa 3 adquiere sentido y legitimidad únicamente gracias al análisis ético–legal realizado previamente. Las acciones ofensivas, como el reconocimiento activo, la explotación de vulnerabilidades, la obtención de una reverse shell, el pivoting hacia redes internas o la creación de cuentas administrativas en equipos remotos, constituyen técnicas poderosas que, sin un marco regulado, serían equiparables al actuar de un ciberdelincuente. El hecho de que estas acciones se ejecuten en un entorno controlado no exime al profesional de comprender la responsabilidad que implicaría aplicar estas mismas técnicas en entornos reales sin autorización. La Etapa 2 evidencia esta distinción crucial y refuerza la idea de que el conocimiento ofensivo debe estar sujeto a límites éticos y legales estrictos.

El análisis ético de la Etapa 2 también permite justificar y contextualizar la profundidad del ataque ejecutado. Entender por qué se puede atacar, cómo se puede atacar y bajo qué condiciones se debe atacar es tan importante como dominar las herramientas técnicas. En este sentido, la relación entre ambas etapas demuestra que la práctica de ciberseguridad ofensiva no es un ejercicio puramente técnico, sino una disciplina que exige responsabilidad, criterio y respeto por la ley.

Relación con el rol del Blue Team y responsabilidades legales

El trabajo defensivo realizado en la Etapa 4 también está regulado por consideraciones éticas y legales. Aunque la prioridad del Blue Team es detener el ataque, proteger el sistema comprometido y restablecer la operación normal, estas acciones deben ejecutarse respetando principios como la preservación de la evidencia digital, la protección de datos sensibles, la confidencialidad de la información y la documentación adecuada de cada intervención. La eliminación de archivos, la terminación de procesos sospechosos o el aislamiento de interfaces

de red deben realizarse con precisión y sin alterar elementos críticos que podrían servir para un análisis forense posterior.

El análisis ético de la Etapa 2 refuerza esta perspectiva al recordar que incluso las acciones defensivas pueden generar consecuencias legales si se ejecutan de manera negligente o sin seguir procedimientos que garanticen la integridad y trazabilidad de los datos. Un Blue Team profesional no actúa impulsivamente; actúa bajo protocolos definidos, comprende la responsabilidad de manipular un sistema comprometido y se asegura de que cualquier acción que tome sea justificable técnica y jurídicamente.

Ética profesional: El conocimiento ofensivo no otorga permiso para atacar

Uno de los aportes más importantes de la Etapa 2 es la comprensión de que el dominio de técnicas ofensivas no otorga automáticamente permiso para aplicarlas. Puede existir la tentación de considerar que un analista experto en ciberseguridad tiene derecho a poner a prueba cualquier sistema con el objetivo de identificar errores o demostrar habilidades, pero la legislación y la ética profesional indican lo contrario. Un ejercicio Red Team solo es válido cuando existe autorización explícita, cuando se encuentra delimitado por un alcance formal y cuando se realiza dentro de un entorno debidamente controlado. La Etapa 2 subraya esta realidad y deja claro que el profesional ético actúa únicamente dentro de los límites establecidos y no utiliza sus conocimientos para fines personales o injustificados.

Esta reflexión se conecta de manera directa con las prácticas de la Etapa 3, donde el estudiante ejecuta técnicas reales de explotación, pivoting y movimiento lateral. La comprensión ética de estas acciones permite diferenciarlas de la actividad delictiva, recordando que el propósito de un profesional de ciberseguridad es proteger, no vulnerar sistemas ajenos.

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/8uY1TIp4x-k

Conclusiones

En conclusión, el análisis realizado permitió evidenciar la complejidad inherente al estudio de las estrategias Red Team y Blue Team, así como la profunda interdependencia entre las capacidades ofensivas y defensivas dentro de un entorno de ciberseguridad moderno. El desarrollo del ejercicio demostró que un ataque controlado, correctamente estructurado y éticamente autorizado, no solo revela fallas técnicas, sino que también expone debilidades operativas, procedimentales y humanas que deben ser abordadas integralmente. Los hallazgos obtenidos no solo confirman la relevancia de estudiar la interacción entre ofensiva y defensa, sino que también abren nuevas líneas de reflexión relacionadas con la mejora continua de procesos, la necesidad de actualización permanente y la construcción de infraestructuras resilientes capaces de anticiparse a las amenazas emergentes.

Asimismo, se destaca la importancia de adoptar un enfoque integral que considere tanto el comportamiento del atacante como la capacidad de respuesta del defensor. El ejercicio evidenció que las acciones del Red Team permiten comprender cómo una vulnerabilidad aislada puede convertirse en un punto de entrada crítico, mientras que el trabajo del Blue Team muestra que una respuesta estructurada—basada en detección, contención, erradicación y recuperación—resulta indispensable para garantizar la estabilidad operativa y preservar la integridad del sistema. Esta complementariedad no solo fortalece la defensa, sino que también promueve el aprendizaje organizacional, la optimización de procedimientos internos y la consolidación de una cultura de seguridad proactiva.

Finalmente, es necesario subrayar que la mejora de la postura de ciberseguridad no depende exclusivamente de herramientas o técnicas, sino de la colaboración articulada entre diversos actores: equipos de seguridad ofensiva y defensiva, áreas administrativas, instancias directivas, comunidad académica y organismos reguladores. Solo a través del trabajo conjunto, la

formación continua y la integración de estándares éticos y legales será posible avanzar hacia un entorno digital más seguro, sostenible y preparado para enfrentar los desafíos actuales y futuros.

Recomendaciones

El análisis integral del ejercicio pone de manifiesto la necesidad de consolidar prácticas sistemáticas que fortalezcan simultáneamente las capacidades ofensivas del Red Team y los mecanismos defensivos del Blue Team. Una primera recomendación es establecer ciclos periódicos de simulaciones controladas que permitan evaluar, con regularidad, la madurez de la infraestructura tecnológica. Los ejercicios de Red Team resultan fundamentales para identificar vulnerabilidades que no suelen emerger en auditorías tradicionales, mientras que la participación continua del Blue Team facilita el perfeccionamiento de sus tiempos de reacción, su capacidad analítica y su manejo de incidentes reales. Esta dinámica debe institucionalizarse para garantizar un aprendizaje progresivo y medible.

Es recomendable que las organizaciones incorporen metodologías estandarizadas para ambos equipos, como MITRE ATT&CK para la ofensiva y NIST o CIS Controls para la defensa. Estas guías ofrecen marcos estructurados que permiten organizar las tácticas del Red Team según técnicas reconocidas internacionalmente, al tiempo que facilitan que el Blue Team configure controles de seguridad alineados con mejores prácticas. De igual forma, se sugiere el uso de laboratorios seguros donde los equipos puedan experimentar, replicar ataques y probar mecanismos de respuesta sin comprometer los ambientes productivos.

Otro aspecto clave consiste en fortalecer la comunicación entre Red Team y Blue Team una vez finalizadas las simulaciones. La retroalimentación cruzada, presentada mediante informes técnicos compartidos, contribuye a generar un ciclo de mejora continua. El Red Team debe proporcionar evidencia detallada de sus vectores de intrusión, técnicas de movimiento lateral y mecanismos de evasión empleados, mientras que el Blue Team debe ofrecer información sobre los puntos de detección, alertas generadas, brechas de visibilidad y

oportunidades de optimización. Esta interacción no solo refuerza el aprendizaje, sino que permite redefinir controles, actualizar políticas de seguridad y mejorar la arquitectura defensiva.

Además, se recomienda implementar procesos de hardening preventivo antes de cada ciclo de pruebas, de modo que la infraestructura sea sometida a niveles crecientes de resistencia. Esto puede incluir el endurecimiento de configuraciones del sistema operativo, segmentación de redes, eliminación de servicios innecesarios, actualización de parches y adopción de herramientas de monitoreo avanzado. El objetivo es que los resultados obtenidos en las simulaciones no solo evidencien fallas, sino que también reflejen la evolución de la postura de seguridad.

La formulación de políticas de privacidad y uso responsable de la información se alinea con las directrices establecidas por entidades gubernamentales, las cuales buscan garantizar el uso adecuado de los servicios digitales y la protección de los datos en entornos institucionales (MINTIC, 2022).

Finalmente, resulta indispensable promover la formación continua de ambos equipos. Los miembros del Red Team deben actualizarse en nuevas técnicas ofensivas, vulnerabilidades emergentes y explotación avanzada, mientras que el Blue Team debe fortalecer sus competencias en análisis forense, respuesta a incidentes, uso de SIEM, herramientas EDR y automatización de defensas. Esta formación debe complementarse con capacitaciones interdisciplinares, fomentando la comprensión mutua entre ofensiva y defensa, lo cual incrementa la eficacia global de la organización ante amenazas reales.

Referencias Bibliográficas

Alhamed, M., et al. (2023). *A systematic literature review on penetration testing in network environments*. *Applied Sciences, 13*(12), 6986. https://www.mdpi.com/2076-3417/13/12/6986

Álvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos* (pp. 1–26). Semantic Scholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Arroyo, E. (2025). *Sinergia de equipos Red Team y Blue Team en la protección de entornos corporativos* [Objeto virtual de información – OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/74595

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

Chindrus, C., & Caruntu, C.-F. (2023). *Securing the network: A Red and Blue cybersecurity competition case study*. *Information, 14*(11), 587. https://doi.org/10.2478/bipie-2023-0008

CIS Security. (2020). *CIS Benchmarks*. CIS Center for Internet Security. https://www.cisecurity.org/cis-benchmarks/

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

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

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

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). *Red Teaming vs. Blue Teaming: A comparative analysis of cybersecurity strategies in the digital battlefield*. *International Journal of Scientific Research in Engineering and Management, 07*(12), 1–11. https://doi.org/10.55041/IJSREM27675

MINTIC. (2022). *Políticas de privacidad y condiciones de uso*. https://www.mintic.gov.co/portal/inicio/Secciones

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

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

Panda Security. (2018). *Pentesting: Una herramienta muy valiosa para tu empresa*. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

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

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

Rincón Arteaga, J. A., Castiblanco Hernández, S. A., Quijano Díaz, A., Urquijo Vanegas, J. D., & Pregonero León, Y. K. (2022). *Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos Informáticos? Criminalidad, 64*(3), 95–116. https://doi.org/10.47741/17943108.368

Sanne, S. H. (2024). *Investigaciones sobre técnicas, herramientas y metodologías de pruebas de seguridad para identificar y mitigar vulnerabilidades de seguridad*. URF Journals. https://urfjournals.org/open-access/investigations-into-security-testing-techniques-tools-and-methodologies-for-identifying-and-mitigating-security-vulnerabilities.pdf

Scarfone, K., & Mell, P. (2022). *Guide to enterprise patch management technologies*. NIST. https://doi.org/10.6028/NIST.SP.800-40r4

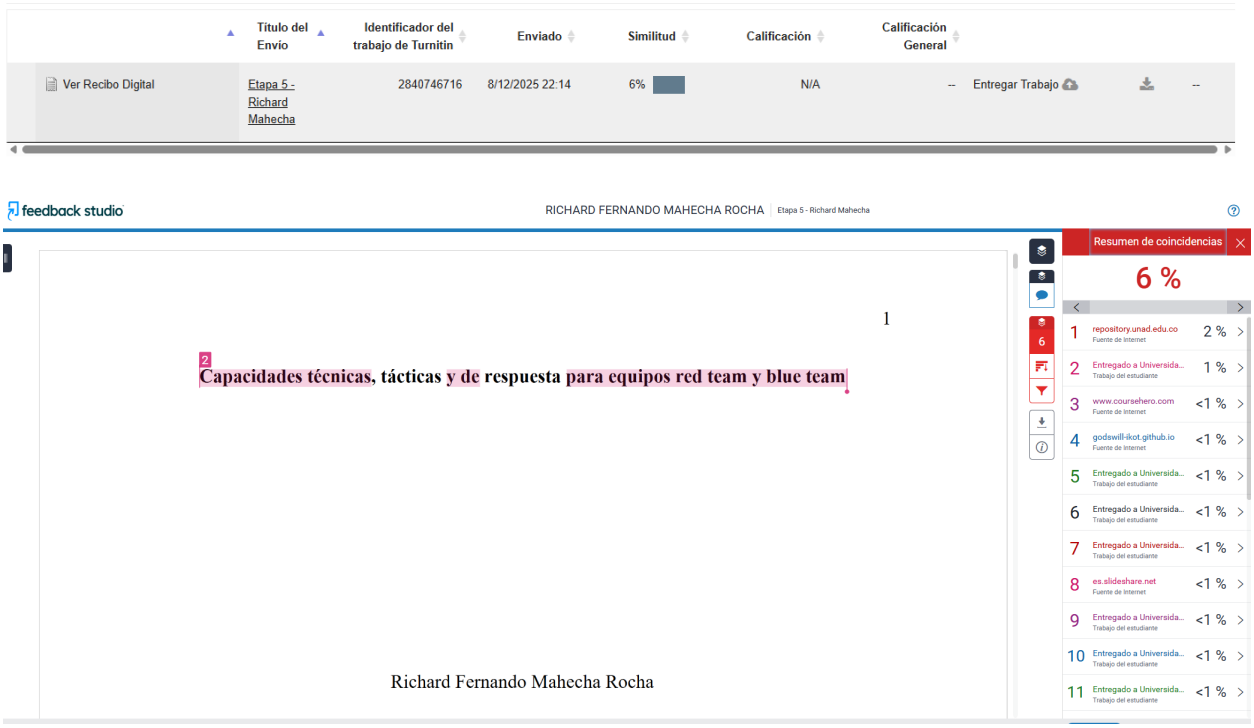
Zambrano Hernández, Peña Hidalgo, H. J., & Cárdenas Corral. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad*. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

e

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Muestra el resultado de la revisión en Turnitin