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

Ing. Linda Mayerly Enciso Ortiz

Asesor

Ing. Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI)

Especialización en Seguridad Informática

2025

Dedicatoria

Quiero dedicar con mucho cariño el desarrollo de este trabajo a mis padres, hermana, gatitos e hijo, ya que son mi mayor motivación para crecer día a día personal y profesionalmente, y muy especialmente a mi hijo por darme ese impulso y motivación para ser un gran mujer y excelente profesional; y a mis bellos gatitos quienes se han acercado a mi lado cada día y noche en los cuales me sentaba en mi escritorio a desarrollar mis actividades y labores académicas hasta finalizarlas con éxito.

Agradecimientos

Agradezco muy cordialmente la gestión y acompañamiento que te he tenido por parte mi querida UNAD y por parte de mi tutor el Ing. Eduvin ya que estos acompañamientos fueron valiosos, fructíferos e indispensables, para el conocimiento que he logrado adquirir y me han convertido en la profesional que soy hoy día. Estoy orgullosa de ser egresada, estudiante y ser parte de esta honorable y prestigiosa universidad, la cual construyó en mi todas las cualidades y conocimientos que me permitirán seguir siendo una gran profesional para este país, y llevar el buen nombre de esta prestigiosa universidad a todos, y por supuesto que seguiré formándome y cultivando en mí una excelente profesional, muchas gracias querida UNAD somos parte de una gran familia.

Resumen

Para el desarrollo de este informe técnico general que se ha logrado consolidar con el desempeño, desarrollo del proceso formativo y práctico que se ha empleado a lo largo de las cinco guías del Seminario Especializado Equipos Estratégicos en Ciberseguridad Red Team & Blue Team, manejando todos los procesos de análisis legales, éticos, técnicos y operativos aplicados en escenarios simulados de evaluación de seguridad y con ello se obtuvieron los resultados alcanzados en las anteriores guías con lo cual se realiza una síntesis estructurada del ciclo completo de un ejercicio ofensivo y defensivo, relacionando las acciones de reconocimiento, explotación y pivoting propias del equipo de Red Team y las actividades de detección, contención, análisis de vectores y hardenización ejecutadas desde la perspectiva del Blue Team además, se referencian los elementos normativos relacionados con la Ley 1273 de 2009, la Ley 1581 de 2012 y el Código de Ética del COPNIA con lo cual se considera el impacto en el ejercicio profesional que realizamos como Especialistas en Seguridad Informática.

Palabras clave: Ataques, defensa, hardening, pentesting, respuesta.

Abstract

The development of this general technical report was consolidated through the performance and practical training process employed across the five modules of the Specialized Seminar: Strategic Cybersecurity Teams Red Team & Blue Team. This process encompassed the management of legal, ethical, technical, and operational analysis applied within simulated security assessment scenarios. Building upon the results achieved in previous stages, this report provides a structured synthesis of the complete offensive and defensive exercise cycle. It establishes the relationship between reconnaissance, exploitation, and pivoting actions inherent to the Red Team, alongside the detection, containment, vector analysis, and hardening activities executed from the Blue Team's perspective. Furthermore, it references the regulatory frameworks of Law 1273 of 2009, Law 1581 of 2012, and the COPNIA Code of Ethics, considering their impact on our professional practice as Information Security Specialists.

Keywords: Attacks, defense, hardening, pentesting, response.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Análisis Forense Digital:

Es considerada como la disciplina especializada que aplica métodos científicos para la identificación, preservación, extracción, análisis y presentación de evidencia digital lo cual garantiza la cadena de custodia y validez jurídica ante incidentes de seguridad.

Autenticación Multifactor MFA:

Es el mecanismo de verificación que combina dos o más factores independientes como lo son el conocimiento, posesión o inherencia para así fortalecer la fiabilidad del proceso de autenticación y reducir el riesgo de acceso no autorizado.

Blue Team:

Es el conjunto de especialistas que les compete la defensa activa y pasiva de la infraestructura tecnológica con el manejo del monitoreo, detección de amenazas, análisis de incidentes, contención y aplicación de estrategias de hardenización.

Cadena de Custodia:

Es el procedimiento documentado que asegura integridad, trazabilidad y confiabilidad de los elementos probatorios digitales los cuales son recolectados durante una investigación o incidente de seguridad.

Ciberataque:

Es la acción deliberada y es orientada para afectar la confidencialidad, integridad o disponibilidad de un activo digital mediante técnicas de explotación, intrusión, ingeniería social o la manipulación de sistemas.

Ciberinteligencia:

Es el proceso sistemático en el cual se hace la recolección, análisis y correlación de información técnica para así responder ante los riesgos que acarrean las amenazas, para evaluar riesgos y apoyar la toma de decisiones estratégicas en seguridad informática.

CVE Common Vulnerabilities and Exposures:

Es el sistema que cataloga las vulnerabilidades públicas que ayudan a la identificación unificada y las cuales permiten facilitar el análisis de riesgos y la correlación entre herramientas de seguridad.

Defensa en Profundidad:

Es la estrategia de seguridad que se usa en múltiples capas de controles técnicos, administrativos y físicos para mitigar la probabilidad de compromiso y demorar el avance de un atacante.

Hardening:

Es el conjunto de técnicas avanzadas que permiten el endurecimiento destinadas a minimizar la superficie de exposición de un sistema, eliminando así las configuraciones inseguras, cerrando servicios innecesarios y aplicando controles de restricción.

Indicadores de Compromiso IoC:

Son los artefactos técnicos que evidencian actividad maliciosa, tales como direcciones IP, hashes, modificaciones en el registro o patrones extraños en el tráfico de red.

Lateral Movement:

Es una técnica utilizada por adversarios para desplazarse entre sistemas internos después de comprometer un host inicial con la intención de escalar privilegios o acceder a servicios críticos.

Pentesting:

Es el ejercicio autorizado que simula ataques reales para evaluar vulnerabilidades técnicas, operativas de una infraestructura, para que pueda ser empleadas las metodologías estandarizadas como OSSTMM o PTES.

Pivoting:

Es una técnica avanzada que permite utilizar un sistema comprometido como el punto de salto para así tener ingreso a las redes internas que no son expuestas mediante túneles dinámicos, proxies o rutas redirigidas.

Red Team:

Es el equipo ofensivo especializado y que se encarga de simular ataques controlados y muy realistas para así evaluar la resiliencia de la organización, explotando vulnerabilidades, realizando reconocimiento profundo y generando la ejecución de acciones encadenadas.

Riesgo Cibernético:

Es la probabilidad de que se genere un evento adverso que llegue a afectar los activos digitales, combinado con el impacto potencial sobre la operación, continuidad de las funciones del negocio y reputación organizacional.

SIEM Security Information and Event Management:

Es el sistema que centraliza, correlaciona y analiza cada eventualidad de seguridad provenientes de múltiples fuentes para detectar anomalías para así alertar incidentes y generar inteligencia operacional.

SOC Security Operations Center:

Es la unidad operativa que se encarga del monitoreo continuo como lo son la gestión de alertas, la atención de incidentes y la coordinación de la defensa integral de la infraestructura tecnológica de la empresa.

Threat Hunting:

Es la actividad proactiva de permite generar la búsqueda avanzada y en la más utilizada para generar las hipótesis basadas en inteligencia de amenazas para identificar presencia de adversarios que evaden controles tradicionales de seguridad.

Vulnerabilidad:

Es la debilidad técnica, procedimental o de diseño que puede ser explotada por un atacante para lograr comprometer la seguridad de un activo, y que debe ser gestionada mediante el análisis de riesgos y procesos de remediación.

Zero Day:

Es la vulnerabilidad desconocida por el fabricante y sin parche disponible con la cual se busca la explotación representa un riesgo crítico debido a la ausencia de mecanismos de defensa específicos.

Introducción

Con la finalización de quinta etapa del Seminario Especializado se presenta este informe técnico que reúne y aplica la relación del conocimiento y aprendizaje en ciberseguridad Red Team y Blue Team comprendiéndolo como un proceso en el que se integró un análisis normativo, la evaluación técnica, las prácticas ofensivas y defensivas, así como reflexiones éticas aplicadas a los escenarios de seguridad informática es por ello que, a lo largo de las cuatro etapas anteriores se trabajaron los elementos primordiales para la comprensión de lo que ocurre con las amenazas, teniendo el conocimiento y regulación los marcos que rigen la actuación profesional y las metodologías que orientan el ataque controlado y la defensa estructurada de infraestructuras tecnológicas, es ahora en esta etapa 5 que se procede a reunir y plasmar estos aprendizajes con la intención de consolidar la visión integral adquirida del ciclo de ciberseguridad, llevándolo hacia el fortalecimiento de competencias técnicas y estratégicas adquiridas en este seminario. (NIST, 2020; MITRE Corporation, 2024)

Por esa razón con este informe se elabora bajo la guía solicitado por la empresa SecureNova Labs cuya organización propone un escenario de evaluación donde se requieren habilidades de análisis, documentación y comunicación de resultados relacionados con operaciones Red Team y Blue Team es por ello, que bajo este escenario se integran los avances obtenidos en ejercicios como lo son la identificación y explotación de vulnerabilidades críticas, el movimiento lateral controlado, la aplicación de técnicas de mitigación desde el rol defensivo y la comprensión del marco legal que se debe aplicar a incidentes de seguridad pues esta articulación permite presentar una visión completa sobre la gestión de riesgos, la respuesta a incidentes y la importancia del comportamiento ético en el momento de desarrollar una práctica profesional.

De igual forma se realiza una revisión de cada uno de los procesos que fueron realizados en las anteriores etapas con el desarrollo de cada guía en donde se ha podido detallar cada una de las estrategias ofensivas y defensivas aplicadas, los resultados obtenidos y las implicaciones técnicas derivadas de cada fase y con ello se presenta un análisis de los aspectos normativos que llevan la regulación de la actuación que debemos asumir como profesionales en ciberseguridad. (Consejo Profesional Nacional de Ingeniería [COPNIA], 2018)

Justificación

Para el desarrollo que se ha tenido para este informe técnico se ha buscado consolidar el conocimiento obtenido en cada fase, el análisis y comunicación de los resultados obtenidos en en desarrollo de las actividades del Seminario especializado, ya que con ello se está demostrando la capacidad profesional que tendremos para enfrentar escenarios complicados de seguridad informática desde una perspectiva ofensiva, defensiva, ética y normativa puesto que, en un contexto donde las empresas se encuentran expuestas a vulnerabilidades o afectaciones muy críticas, amenazas persistentes y ataques que se vuelven novedosos, es bastante importante y necesario fortalecer las competencias que ayudarían a ejecutar evaluaciones de penetración controladas, identificar brechas técnicas, aplicar medidas de mitigación rápidas. (NIST, 2018; Center for Internet Security, 2022)

Para así documentar hallazgos con severidad y por supuesto con este informe también se busca plasmar e integrar los elementos trabajados en cada una de las etapas ya realizadas manteniendo ese enfoque de análisis legal y ético, la explotación y movimiento lateral observados en el escenario técnico, la respuesta y contención orientada a la recuperación operativa, teniendo presentes dichos resultados con los requerimientos del escenario 5 propuestos por la empresa SecureNova Labs y un enfoque donde se reflejé el desarrollo de habilidades prácticas en Red Team y Blue Team y la evidencia de la comprensión del marco regulatorio colombiano, la importancia de seguir la buena conducta de la ética profesional y la necesidad de adoptar una perspectiva sistémica basándonos en el riesgo y defensa en profundidad así mismo, esta entrega que es de índole académica permite reforzar el conocimiento especializado en ciberseguridad. (Symantec Corporation, 2023)

Objetivos

Objetivo General

Analizar los resultados técnicos, normativos y estratégicos obtenidos en el seminario de Red Team & Blue Team de forma integral, con el estudio que se tuvo en las etapas 1 a 4 y del escenario 5 propuesto por la empresa SecureNova Labs, para así poder consolidar un informe técnico desde una perspectiva profesional que permita identificar vulnerabilidades, aplicar tácticas ofensivas y defensivas, y generar las respectivas recomendaciones de seguridad informática avanzadas. (NIST, 2020; SANS Institute, 2022)

Objetivos Específicos

1. Evaluar las estrategias del equipo Red Team que pudieron ser aplicadas en el transcurso del desarrollo del seminario, entre ellas las actividades de reconocimiento, explotación, escalamiento de privilegios y movimiento lateral, para que sea posible identificar brechas críticas y analizar su impacto en la infraestructura evaluada. (MITRE Corporation, 2024)

2. Examinar las acciones del equipo de Blue Team desarrolladas en las etapas anteriores, que tengan que ver con la detección, la contención, el análisis de vectores, la respuesta a incidentes y medidas de hardenización, lo cual es necesario para lograr detección rápida en la mitigación de riesgos.

3. Integrar los aspectos legales, éticos y normatividades asociadas a nuestra profesión en ciberseguridad, para que se puedan tomar decisiones técnicas, garantizar la responsabilidad institucional y soportar las conclusiones y recomendaciones que buscan las mejoras y estrategias de protección las empresas como en SecureNova Labs.

Desarrollo del Informe Técnico

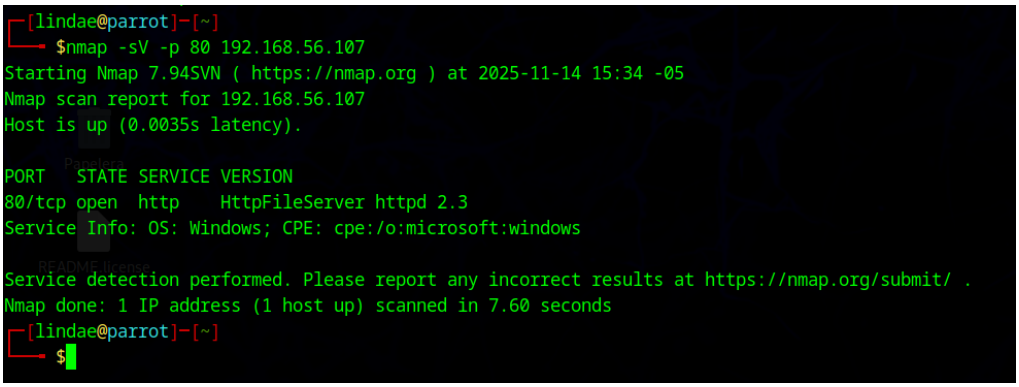
Estrategias Red Team aplicadas en el seminario

Las estrategias del equipo de Red Team que fueron empleadas durante el seminario han permitido replicar un ciclo ofensivo en totalidad basado en metodologías profesionales de pruebas de penetración, en el siguiendo fases de reconocimiento, enumeración, explotación, persistencia y movimiento lateral es por ello que con este proceso se completó el análisis técnico realizado en la etapa 3 en donde se trabajó sobre un entorno controlado compuesto por un Host A maquina Windows 7 y un Host B también de sistema operativo Windows 7, representando un escenario corporativo con servicios vulnerables en donde la operatividad del equipo Red Team se ha propuesto identificar debilidades explotables mediante técnicas realistas que representa una emulación del comportamiento de un adversario avanzado APT para así poder evaluar la resiliencia de la infraestructura y obtener acceso no autorizado con privilegios escalados. (NIST, 2018)

En el desarrollo de la primera fase se pudo identificar y reconocer el entorno activo mediante herramientas de escaneo, lo que permitió hallar los puertos expuestos y servicios que podían ser vulnerables y entre los hallazgos más relevantes se detectó el servicio Rejetto HFS versión 2.3 el cual es conocido por su vulnerabilidad crítica CVE-2014-6287 que conlleva a la ejecución remota de comandos a partir de esta identificación, y seguido a ello se hizo la explotación controlada utilizando módulos específicos que sirvieron para abrir una sesión remota sobre el Host A y así validar que el sistema no tenía mecanismos de protección adecuados y robustos para prevenir ataques externos. (MITRE Corporation, 2024)

Figura 1

Detección del servicio HttpFileServer (HFS) 2.3 vulnerable en el Host-A mediante escaneo de puertos.



Fuente. Autoría Propia

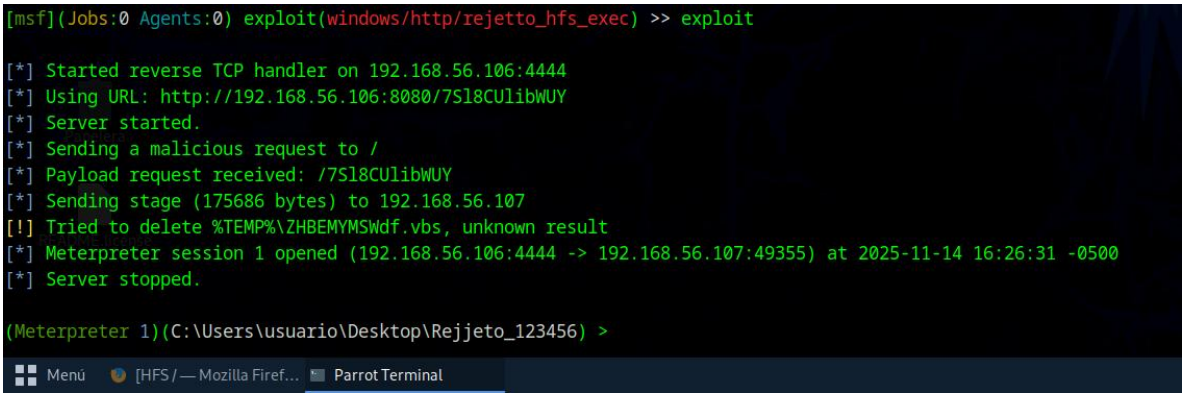
Nota. En esta captura se evidencia que el puerto 80 está abierto, que el servicio es HttpFileServer (HFS), que la versión es 2.3 es VULNERABLE al exploit CVE-2014-6287, y que en la maquina Windows está perfecta para este exploit, es decir que esta captura evidencia el reconocimiento, detección del servicio HFS y confirmación de vulnerabilidad.

Después de esto se orientaron los esfuerzos para a manejo de técnicas de post explotación en donde se estableció una sesión Meterpreter que sirvió para facilitar el reconocimiento interno del sistema, la obtención de información sensible y la manipulación del entorno comprometido además esta sesión sirvió como punto de ayuda para ejecutar técnicas de pivoting, generando un túnel hacia la red interna para acceder al Host B con lo que se pudo acceder a una simulación de un ataque real en donde el atacante se desplaza lateralmente dentro de la infraestructura y con las técnicas empleadas se evidenció que no había segmentación, falta de monitoreo y la exposición

directa de servicios sensibles evidenciando así vulnerabilidades estructurales de alto impacto y gravedad. (SANS Institute, 2022)

Figura 2

Ejecución del exploit contra HFS y apertura de sesión Meterpreter en el Host A

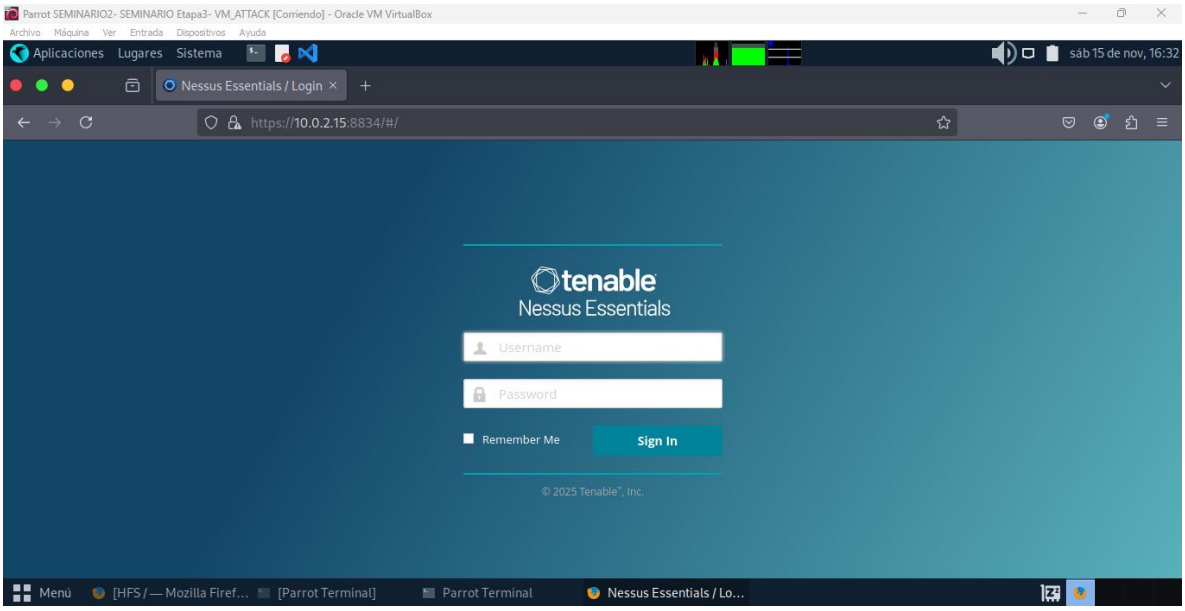


Fuente. Autoría Propia

Nota. En esta captura se evidencia que ya hay acceso a la maquina Windows – Sesión METERPRETER ABIERTA, con esto se evidencia que el exploit funcionó, el payload reverse_tcp se ejecutó, la conexión volvió a la atacante Parrot y ahora hay control remoto total, es decir se evidencia la sesión Meterpreter activa tras la explotación exitosa del servicio HFS 2.3 en el Host A.

Figura 3

Acceso a Nessus en el Host B a través de túnel SOCKS y pivoting desde el Host A comprometido



Fuente. Autoría Propia

Nota. En esta captura se evidencia un Pivoting real, donde se evidencia Parrot (Host A comprometido) → túnel SOCKS4 → Host B (10.0.2.15) → Nessus Essentials abierto y con ello ya se evidencia el Pivoting avanzado, navegación desde Parrot hacia Host B, acceso profundo a un servicio crítico en la red interna, SOCKS4 funcionando, Proxychains ejecutándose bien, puertos descubiertos (1080, 8834) y Firefox en Host A atravesando la red interna como si estuviera en Host B.

Fase de reconocimiento y enumeración inicial

En el desarrollo del proceso ofensivo se inició con un reconocimiento activo dado a la identificación de los servicios expuestos, la topología básica de la red y los puertos accesibles desde el entorno del atacante y para ello se emplearon técnicas de escaneo de puertos utilizando herramientas como el manejo de los comandos Nmap, lo cual sirvió para obtener una visión

preliminar de la superficie de ataque del Host A, es importante mencionar que esta fase es muy importante dentro de la metodología Red Team ya que brinda los elementos necesarios para establecer los vectores potenciales de explotación y evaluar la robustez inicial del sistema objetivo y con los resultados obtenidos se evidenció la disponibilidad del puerto 80 y la ejecución del servicio HttpFileServer HFS de la versión 2.3, lo cual es evidenciado como una versión ampliamente documentada, vulnerable y con un historial de explotación asociado al CVE-2014-6287.

Después de esto se procedió a generar la enumeración del servicio identificado para así confirmar la versión exacta del software y determinar si existían configuraciones inseguras o exposiciones adicionales asociadas al servidor web y con la información recolectada se pudo verificar que la versión en ejecución se encontraba sin parches y era de un servicio de ejecución remota de comandos es por ello que, con esa información validada se estableció el punto de entrada más crítico para el ataque y se definió que este vector establecería el acceso inicial al sistema durante la fase de explotación es por ello que, se comprende que con los principios del Red Team de debe dar prioridad a la explotación de vulnerabilidades de alto impacto que permitan tener visibilidad de la primera sesión remota estable y con capacidad de una post explotación.

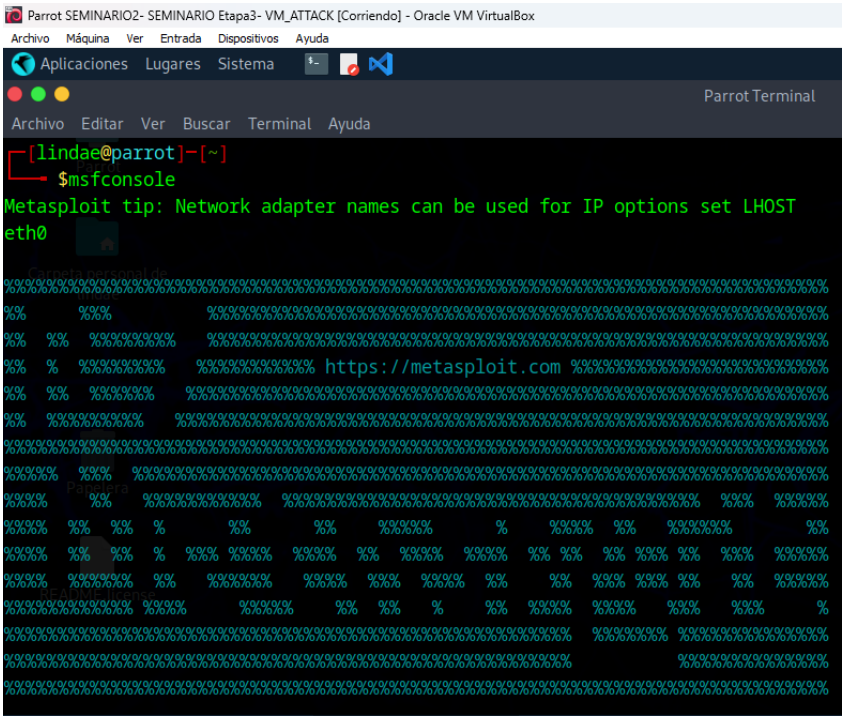
Fase de explotación del servicio vulnerable HFS

Cuando ya fue identificada la vulnerabilidad crítica asociada al servicio HttpFileServer (HFS) versión 2.3 se procedió a la fase de explotación el cual tuvo como propósito comprometer el Host A mediante la ejecución remota de código y para dicha acción se empleó Metasploit Framework, la cual es una herramienta ampliamente utilizada en las actividades desarrolladas por

el equipo de Red Team ya que tiene la capacidad de automatizar procesos de explotación y generar sesiones remotas estables para la post explotación y por esta razón en esta etapa se inició la consola de Metasploit desde la máquina atacante lo cual permitió acceder a la base de datos de módulos disponibles y tener una preparación del entorno para la búsqueda del exploit adecuado. (MITRE Corporation, 2024)

Figura 4

Inicio de Metasploit Framework para la explotación del servicio vulnerado



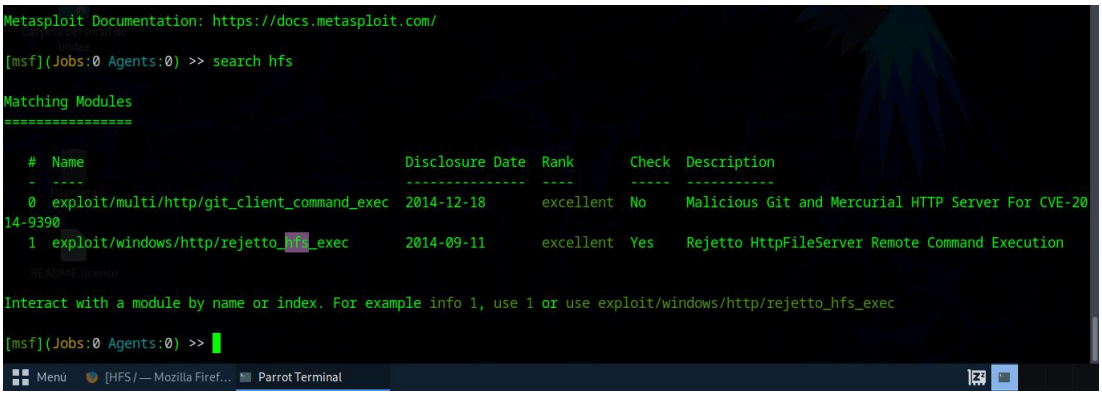
Fuente. Autoría Propia

Nota. Esta captura evidencia que Metasploit está iniciado correctamente y que el servicio funciona lo cual permite que el entorno esté listo para comenzar el exploit es decir que, se evidencia la apertura de Metasploit desde el equipo atacante.

Después de esto se realizó la búsqueda dirigida del exploit específico para la vulnerabilidad CVE-2014-6287 y por esta razón se utilizó el comando search hfs y con el resultado del mismo se identificó la consulta que confirmó la disponibilidad del módulo exploit/windows/http/rejetto_hfs_exec, el cual corresponde a un exploit de ejecución remota especialmente efectivo contra hosts Windows que ejecutan versiones vulnerables de HFS sin parches de seguridad con este hallazgo se pudo validar que el vector de ataque era totalmente viable y que el sistema objetivo no tenía medidas de mitigación que lograra bloquear este tipo de explotación.

Figura 5

Resultado de la búsqueda del exploit CVE-2014-6287 mediante el comando search hfs



Fuente. Autoría Propia

Nota. En esta captura se evidencia que se ha identificado el módulo exploitable rejetto_hfs_exec.

Es por esto que al ser hallado el módulo apropiado se procedió a cargarlo en Metasploit mediante el comando use exploit/windows/http/rejetto_hfs_exec, después de esto se revisaron cada uno de los parámetros requeridos para su correcta ejecución y entre las configuraciones principales se establecieron las direcciones RHOSTS y LHOST las cuales son importantes y necesarias para detallar el objetivo remoto y la interfaz local que recibiría la conexión inversa del payload y ya con estos valores correctamente configurados se entendió que el entorno quedó preparado para iniciar el ataque y proceder a la explotación del servicio vulnerable.

Figura 6

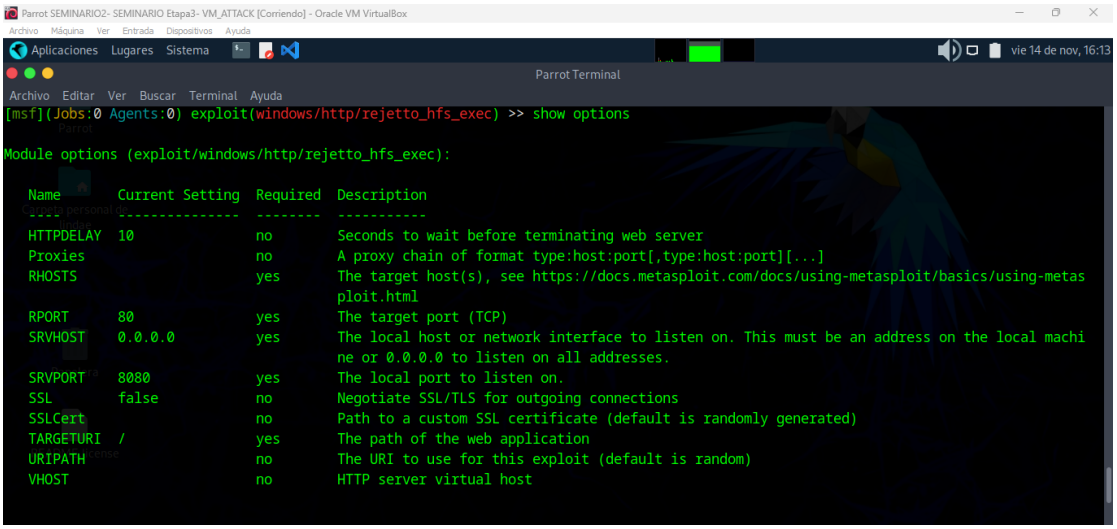
Carga del módulo rejetto_hfs_exec en Metasploit

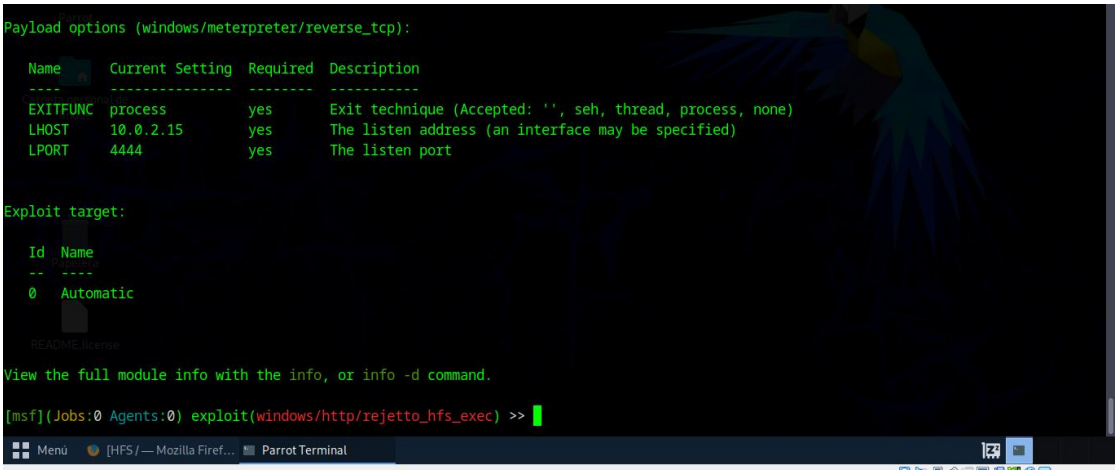
Fuente. Autoría Propia

Nota. En esta captura se evidencia cargado el módulo rejjetto_hfs_exec y Metasploit ya asignó el payload por defecto: “windows/meterpreter/reverse_tcp”, es decir que muestra la selección del módulo de explotación adecuado

Figura 7

Configuración de los parámetros del exploit rejetto_hfs_exec en Metasploit

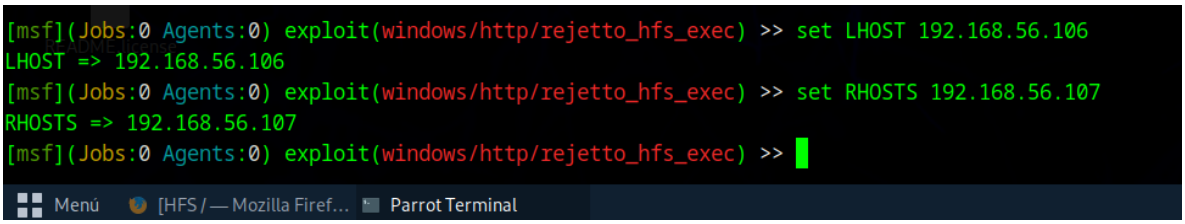




Fuente. Autoría Propia

Figura 8

Configurar LHOST - RHOSTS correctamente



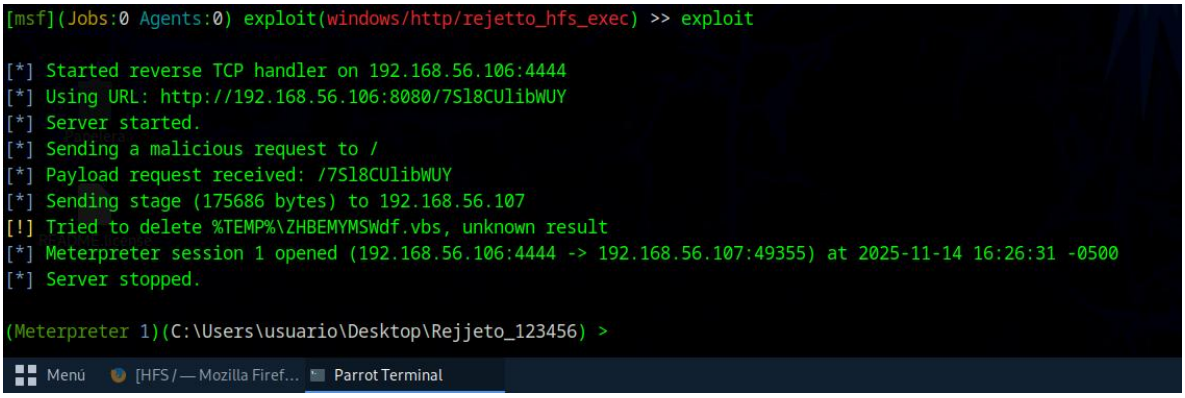
Fuente. Autoría Propia

Nota. Con esta captura se evidencia que **LHOST = 192.168.56.106** en Parrot ATTACK VM y **RHOSTS = 192.168.56.107** la Host-A con HFS, esto significa que ya está configurados los parámetros críticos del módulo, es decir que se evidencia donde se ajustan las direcciones RHOSTS y LHOST para la explotación remota.

Ejecución del exploit y apertura de sesión Meterpreter

Figura 9

Ejecutar el exploit



Fuente. Autoría Propia

Nota. En esta captura se evidencia que ya hay acceso a la maquina Windows – Sesión **METERPRETER ABIERTA**, con esto se evidencia que el exploit funcionó, el payload reverse_tcp se ejecutó, la conexión volvió a la atacante Parrot y ahora hay control remoto total, es decir que contiene la evidencia del comando exploit ejecutado, sesión Meterpreter abierta y conexión exitosa del payload

Una vez que han sido configurados correctamente los parámetros del módulo rejetto_hfs_exec se procedió a la ejecución del exploit con la intención de tener acceso remoto al Host A mediante un payload de conexión inversa, es por ello que en esta etapa Metasploit estableció comunicación con el servicio HttpFileServer vulnerado y logró ejecutar la instrucción maliciosa que permitió abrir una sesión remota en la máquina objetivo y con este proceso se concluyó con la creación satisfactoria de una sesión Meterpreter la cual forma parte de una interfaz

avanzada para realizar acciones posteriores dentro del sistema comprometido y con esta sesión confirma se llevará a cabo la explotación exitosa del servicio vulnerable y la ausencia de mecanismos de protección efectivos en el Host A, como la acción del monitoreo de tráfico, filtros de firmas o soluciones antiexploit que hubiesen bloqueado la actividad ofensiva. (National Institute of Standards and Technology [NIST], 2018)

Con la apertura de la sesión Meterpreter se pudo validar que el atacante había obtenido control total sobre la máquina comprometida y por supuesto a partir de este punto fue posible interactuar con el sistema operativo, teniendo así verificación a los privilegios de la cuenta comprometida, acceso a la lista de información del sistema y examinar estructuras básicas del entorno Windows, de igual forma la estabilidad de la sesión fue un indicador muy importante de que la explotación había sido completamente exitosa, ya que fue lo que proporcionó el punto de apoyo necesario para ejecutar fases posteriores, como lo fue la post explotación, el reconocimiento interno y el movimiento lateral hacia el Host B por esta razón esta etapa constituye uno de los momentos más críticos dentro del ciclo ofensivo puesto que está demostrando la capacidad del adversario para comprometer un host, mantenerse dentro del mismo y continuar expandiendo su alcance dentro de la infraestructura evaluada.

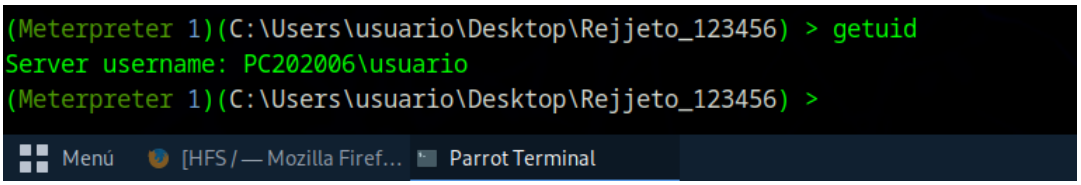
Fase de post explotación - Validación del control y obtención de información interna

Una vez que se inició la sesión Meterpreter sobre el Host A se procedió a la fase de post explotación la cual tiene el propósito que sea validado el nivel de control adquirido y compilar información sensible que permitiera entender la arquitectura interna del sistema comprometido y a través de esta interfaz se pudieron ejecutar comandos orientados a identificar el contexto de

ejecución, confirmar los privilegios obtenidos y examinar elementos clave del sistema operativo, tales como lo son los usuarios, procesos activos y estructura de archivos y la verificación del usuario comprometido por medio del comando getuid lo cual confirmó que la sesión operaba con privilegios suficientes para realizar actividades avanzadas de reconocimiento y manipulación del sistema.

Figura 10

Identificación del usuario comprometido mediante el comando getuid en Meterpreter.



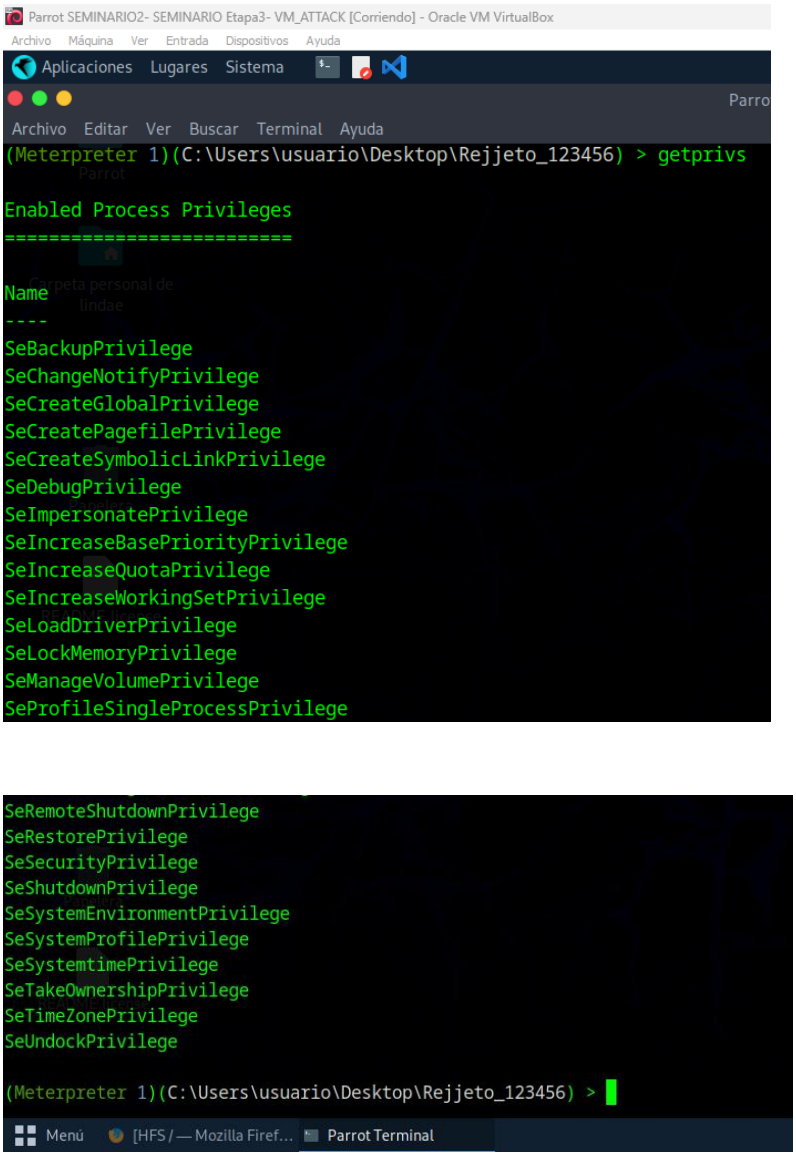
Fuente. Autoría Propia

Nota. En esta captura se evidencia el contexto de ejecución de la sesión remota.

Después de ello se evaluaron los privilegios que estaban disponibles en la sesión con el uso del comando getprivs, lo que permitió establecer la capacidad real del atacante para ejecutar funciones críticas como lo es la lectura de archivos del sistema, modificación de configuraciones, acceso a directorios restringidos y potenciales técnicas de escalamiento por supuesto, esta información fui muy importante para comprender el nivel de exposición del Host A y reconocer la ausencia de controles restrictivos que limitarían las actividades del atacante dentro del entorno comprometido.

Figura 11

Verificación de privilegios disponibles mediante el comando getprivs.



Fuente. Autoría Propia

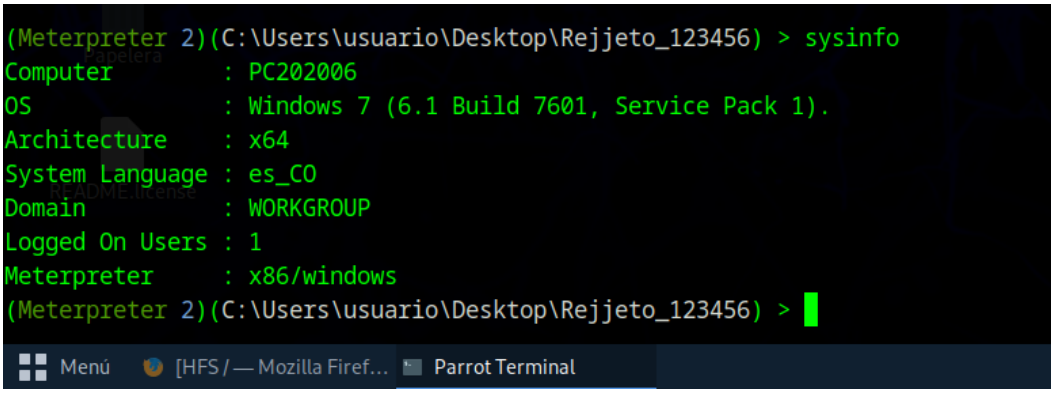
Nota. En esta captura se muestran los privilegios activos obtenidos tras la explotación.

De igual forma se realizaron actividades de recolección de información interna con el uso de comandos como sysinfo y navegación del sistema de archivos y con estos pasos se ha podido

identificar la versión del sistema operativo, arquitectura, nombre del equipo y directorios relevantes, la cual fue información muy necesaria para planificar las fases posteriores del ataque y como fue el movimiento lateral hacia otros hosts, la disponibilidad de esta información ha permitido evidenciar que el Host A no tenía mecanismos de protección apropiados lo cual ha facilitado la permanencia, también se ha generado el reconocimiento interno y la preparación del entorno que se ha planteado para el desarrollo de la siguiente fase del ejercicio ofensivo.

Figura 12

Información detallada del sistema comprometido mediante el comando sysinfo.



Fuente. Autoría Propia

Nota. En esta captura se evidencian los datos del sistema operativo del Host A.

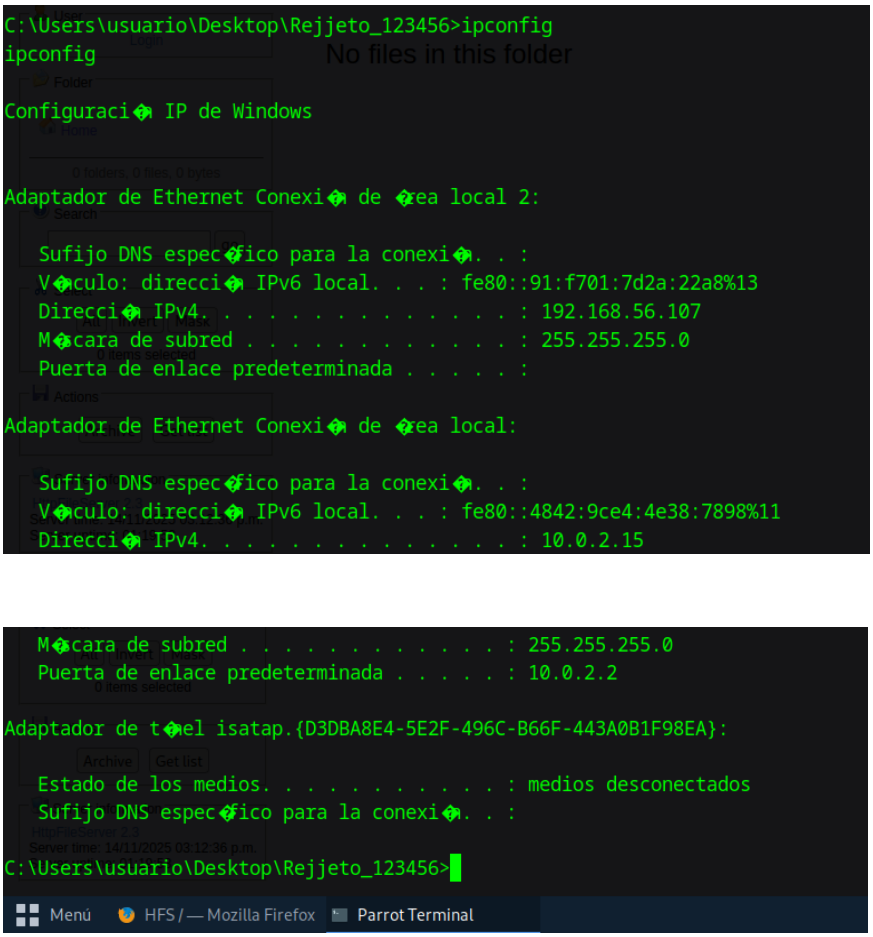
Movimiento lateral y pivoting hacia Host B

Después de realizar la post explotación inicial sobre el HostA se procedió a una de las fases más avanzadas del ejercicio ofensivo el cual es el movimiento lateral y el establecimiento de pivoting hacia otros elementos de la red interna es importante mencionar que esta etapa es fundamental en un escenario Red Team, ya que permite evaluar la capacidad del atacante para

expandir su alcance más allá del primer sistema comprometido y establecer si la infraestructura presenta segmentación adecuada o controles que limiten la propagación del ataque es por ello que el proceso se inició verificando la conectividad interna desde la sesión Meterpreter, con lo cual permitió hayar que en el Host A había una comunicación directa con el Host B lo que permitía confirmar la posibilidad de realizar un desplazamiento lateral dentro del entorno.

Figura 13

Verificación de conectividad interna entre Host A y Host B desde la sesión comprometida.



Fuente. Autoría Propia

Nota. En esta captura se evidencia la comunicación interna previa al movimiento lateral.

Tabla 1

Comunicación interna previa al movimiento lateral

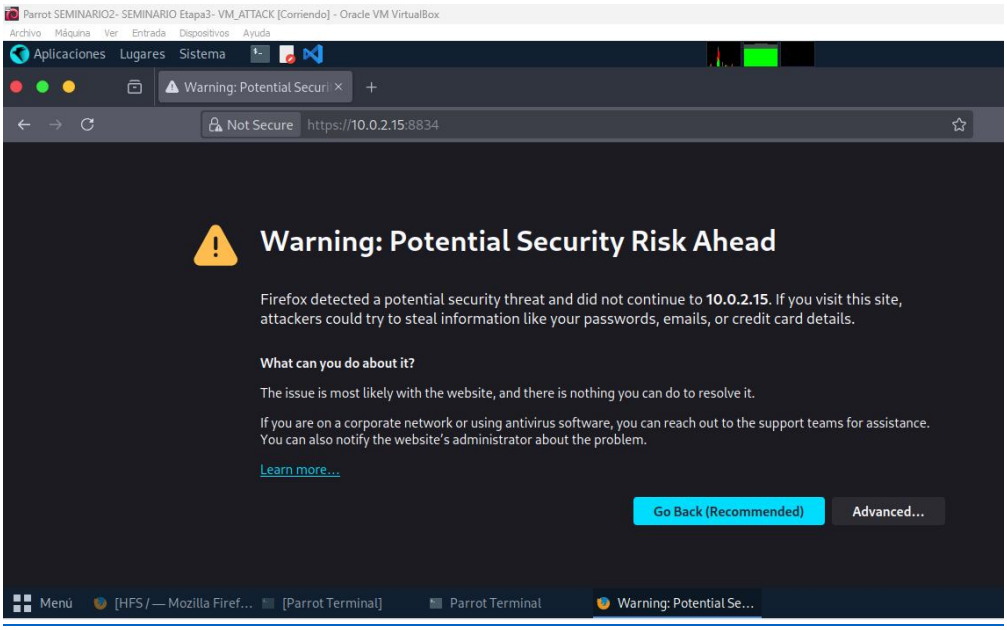
Interfaz	IP	Detalle
Conexión de área local 2	192.168.56.107	Red Parrot ↔ Host-A la cual fue usada para explotar Rejetto
Conexión del área local	10.0.2.15	Red interna Host-A ↔ Host-B aquí esta HOST-B

Nota. La segunda 10.0.2.15 es la clave del pivoting, ya que es la red privada que el atacante normalmente NO puede ver desde Parrot y como Especialista de Seguridad Informática ya podemos observar dentro de Host-A y ahora SÍ puede ser usada.

Luego para habilitar el movimiento lateral se configuró un túnel SOCKS a través del módulo socks_proxy de Metasploit, el cual permitió redirigir el tráfico del atacante a través del Host A, actuando este como un puente hacia la red interna y una vez activado el túnel se utilizaron herramientas como lo son proxychains en la máquina atacante para generar que el tráfico sea redirigido hacia recursos internos del Host B y mediante esta configuración se logró acceder de manera indirecta a servicios del Host B a través del Host A con lo cual se evidencia la efectividad del pivoting y se está evidenciando la falta de controles de segmentación o firewalls internos que detectaran o bloquearan de inmediato este tipo de conexiones.

Figura 14

Ejecución de tráfico redirigido mediante ProxyChains a través del túnel SOCKS configurado



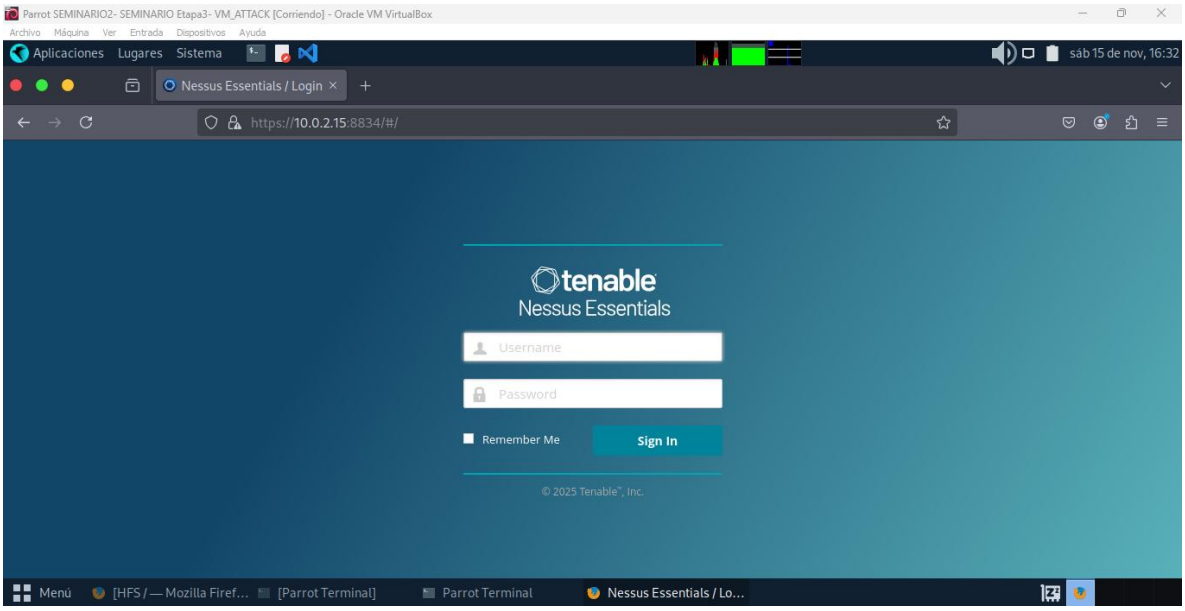
Fuente. Autoría Propia

Nota. En esta captura se muestra el uso de ProxyChains para el movimiento lateral hacia el Host-B.

Después se confirmó el movimiento lateral exitoso con el acceso a la interfaz web de Nessus en el Host B con lo cual se evidenció que el túnel estaba funcionando de manera correcta y que el atacante había logrado atravesar la red interna sin ser detectado es por eso que con este resultado se puede ver reflejada una debilidad crítica en la arquitectura de la organización simulada, ya que se evidencia que permite al atacante acceder a servicios internos sensibles sin autenticación adicional y con la capacidad de efectuar pivoting desde un host comprometido establece uno de los indicadores más representativos de un fallo estructural en la defensa en profundidad, y también se ve resaltada la necesidad de implementar controles como lo son los IDS internos, segmentación de VLAN, listas de acceso y monitoreo avanzado del tráfico lateral.

Figura 15

Acceso al servicio Nessus del Host B a través de pivoting desde el Host A comprometido.



Fuente. Autoría Propia

Nota. En esta captura se demuestra la efectividad del movimiento lateral mediante túneles SOCKS.

Hallazgos ofensivos - Resumen de vulnerabilidades - impacto

En el desarrollo del ejercicio ofensivo que se ha podido identificar un conjunto de vulnerabilidades críticas y fallas estructurales que fueron las que permitieron el compromiso completo del Host A y el movimiento lateral hacia el Host B por esa razón como primera medida se evidenció la presencia del servicio HttpFileServer HFS versión 2.3 en estado vulnerable, el cual estaba configurado sin parches de seguridad y expuesto directamente a la red, lo cual habilitó la explotación remota asociada al CVE-2014-6287 por esta razón esta falta de actualización y endurecimiento del servicio generó el vector inicial de compromiso y permitió evidenciar que no hay un proceso adecuado para la gestión de vulnerabilidades por parte de la organización simulada,

y durante la fase de post explotación se determinó que el Host A operaba sin controles de restricción de privilegios, permitiendo así que el atacante pudiera ejecutar comandos avanzados mediante la sesión Meterpreter y en cuanto a la capacidad para enumerar información del sistema, listar archivos, revisar privilegios y obtener detalles internos sin ninguna alerta o bloqueo lo cual evidencia que no existían mecanismos de seguridad básicos como lo son las auditorías del sistema, políticas de privilegios mínimos o generar soluciones antimalware con protección contra payloads de conexión inversa. (MinTIC, 2021)

Por tanto, el ejercicio de movimiento lateral nos ha mostrado una debilidad crítica en la segmentación de la red, ya que el Host A comprometido tenía una comunicación directa con el Host B sin filtros, firewalls internos ni controles de inspección a fondo además con la generación de un túnel SOCKS y el acceso exitoso al servicio Nessus, se pudo confirmar que no hay políticas de separación de dominios de seguridad y que no existe un monitoreo del tráfico lateral por esa razón todos estos hallazgos nos ha mostrado un escenario muy vulnerable donde la explotación inicial deriva rápidamente en un compromiso total de la infraestructura, lo cual representa la necesidad de implementar controles de defensa en profundidad, segmentación de red y monitoreo continuo como medidas prioritarias para evitar riesgos a futuro.

Tabla 2

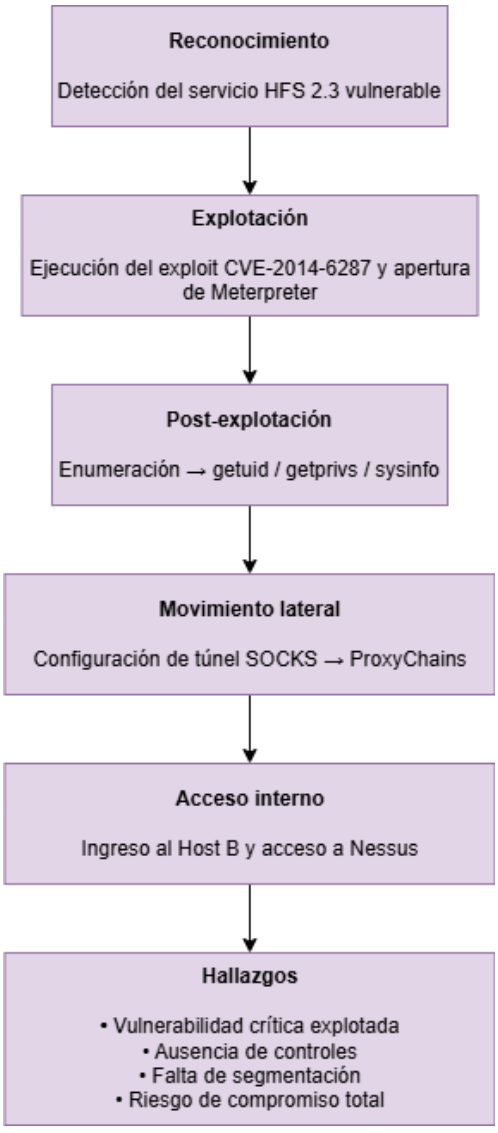
Resumen de hallazgos ofensivos identificados durante el ejercicio Red Team

Categoría del hallazgo	Descripción	Evidencia de la practica	Impacto potencial	Recomendación
Vulnerabilidad del servicio HFS 2.3	Servicio HttpFileServer expuesto, versión 2.3 vulnerable al CVE-2014-6287	Detección mediante escaneo de puertos como se ve en la figura 1	Ejecución remota de comandos y compromiso inicial del Host-A	Se debe aplicar parches, retirar versiones obsoletas y fortalecer configuración del servicio
Ausencia de controles de privilegios	La sesión Meterpreter permite enumeración y ejecución sin restricciones	Comandos getuid y getprivs como se ve en las figuras 4 y 5	Manipulación de archivos, acceso sensible, y riesgo de escalamiento	Se deben implementar política de privilegios mínimos y auditoría constante de cuentas
Falta de monitoreo y alertas	No hubo mecanismos para detectar la explotación ni el payload	Ejecución exitosa del exploit como se ve en la figura 2	Compromiso silencioso del host y permanencia prolongada	Se deben implementar SIEM - IDS que alerten actividad anómala en tiempo real
Conectividad interna abierta	Comunicación directa Host A → Host B sin filtrado	Prueba de conectividad interna como se ve en la figura 6	Facilita pivoting y movimiento lateral no autorizado	Se debe segmentar red mediante VLAN y listas de control de acceso
Acceso a servicios internos	Acceso al servicio Nessus desde Host-B vía túnel SOCKS	Pivoting exitoso como se ve en la figura 7	Exposición de activos críticos y riesgo de infiltración profunda	Se debe implementar firewalls internos e inspección de tráfico lateral

Nota. Esta tabla representa los resultados obtenidos en la Etapa 3 del seminario dentro del ejercicio ofensivo Red Team.

Figura 16

Flujo ofensivo del ataque ejecutado durante el ejercicio Red Team.



Fuente. Autoría Propia

Nota. Diagrama elaborado para representar el flujo ofensivo completo desde el vector inicial hasta el movimiento lateral hacia el Host-B.

Estrategias Blue Team aplicadas en el seminario

Las estrategias Blue Team que fueron aplicadas en el marco del seminario fueron orientadas a comprender el conjunto de medidas defensivas que permitirían la mitigación, detección y respuesta de manera efectiva ante los incidentes simulados durante el ejercicio Red Team, por esta razón se analizó el ciclo de respuesta a incidentes siguiendo las etapas propuestas por marcos de referencia como NIST SP 800-61 por tanto, se incorporaron procesos de preparación, identificación, contención, erradicación y recuperación es por ello que, este enfoque permitió evidenciar cuales eran los controles que habrían sido necesarios para evitar la explotación inicial del servicio HttpFileServer HFS versión 2.3 y qué mecanismos de defensa hubieran limitado el acceso no autorizado y la ejecución remota de código además entre los controles más relevantes se identifican la gestión de parches, el hardening del servicio, la deshabilitación de versiones obsoletas y la aplicación de configuraciones seguras, acciones que habrían evitado que el vector CVE-2014-6287 fuera explotado con éxito. (National Institute of Standards and Technology [NIST], 2020)

Respecto al desarrollo de la fase de detección se pudo evaluar la importancia de contar con un sistema de monitoreo que sea continuo mediante soluciones con herramientas como SIEM - Security Information and Event Management o IDS - IPS, las cuales podrían correlacionar eventos inusuales, hallar rapidamente comportamientos extraños y alertar sobre actividades sospechosas como los son los intentos de exploit, conexiones inversas o movimientos laterales y por supuesto al no tener estos mecanismos permitió que el atacante obtuviera una sesión Meterpreter sin generar alertas, lo que confirma la prioridad que se requiere para implementar reglas de detección basadas

en firmas, umbrales de comportamiento, análisis de tráfico interno y monitoreo del uso de comandos potencialmente maliciosos.

También se implementaron estrategias orientadas a contener y mitigar el avance del ataque una vez comprometido el Host A y por ello también la segmentación de red, el uso de firewalls internos, las listas de control de acceso, la separación de VLAN y la inspección del tráfico lateral son mostradas como medidas esenciales para evitar el movimiento lateral hacia el Host B y la implementación de políticas de privilegios mínimos, auditoría de cuentas de usuario, restringir accesos administrativos y aplicar controles de integridad son un buen complemento a las acciones necesarias para asegurar la infraestructura puesto que, estas medidas combinadas con la adopción de herramientas de análisis forense post incidente, sirven preservar evidencia, comprender el alcance real del ataque y restaurar la operación con por esa razón, las estrategias Blue Team nos muestra la importancia de una defensa en profundidad robusta, totalmente competente para que se pueda prevenir, detectar y mitigar amenazas en todo entorno empresarial. (Kaspersky Lab, 2023)

Controles preventivos recomendados

Los controles preventivos son los que representan la primera línea de defensa dentro de un modelo de seguridad integral y son los que forman las medidas esenciales que una organización debe emplear para minimizar la probabilidad de que un ataque se llegue a materializar y a partir de los hallazgos obtenidos en el ejercicio ofensivo y se pudo identificar que cada uno de los aspectos críticos fue que no hubo una gestión de vulnerabilidades efectiva, lo cual permitió que el servicio HttpFileServer HFS versión 2.3 operara con una falla grave sin parchear es por esto que, para mitigar este tipo de riesgos resulta indispensable establecer un programa formal de actualización y gestión de parches, donde se puedan integrar los inventarios actualizados de

activos, priorización con base en la criticidad y la aplicación rápida de las actualizaciones de seguridad asimismo, el uso de herramientas automatizadas de escaneo periódico permitiría identificar debilidades antes de que sean explotadas por un atacante y por supuesto, otro control preventivo muy importante es el que corresponde a la aplicación de técnicas de hardening tanto a nivel de sistema operativo como de servicios. (AEPD, 2021)

Estas medidas tienen que ver con la desactivación de servicios innecesarios, la restricción de interfaces de administración, la aplicación de configuraciones seguras y la eliminación de versiones antiguas o vulnerables de software y con el uso de plantillas de endurecimiento la cuales con basadas en estándares como CIS Benchmarks o NIST SP 800-70 se podrían llegar a establecer configuraciones seguras mínimas para entornos Windows y Linux y así mismo se implementarían las políticas de privilegios mínimos lo cual reduciría de manera amplia el impacto de una eventual explotación, al limitar las capacidades de ejecución de un usuario comprometido. (Centro Criptológico Nacional [CCN-CERT], 2022)

Se recomienda igualmente establecer segmentación de red mediante VLAN y listas de control de acceso para que sea impedida la comunicación directa entre zonas internas con diferentes niveles de sensibilidad puesto que, esta separación lógica reduce la superficie de exposición, evita que un atacante pueda desplazarse fácilmente entre hosts y limita el alcance de un compromiso inicial y con la combinación de gestión de vulnerabilidades, endurecimiento de sistemas, políticas restrictivas de acceso y segmentación esto representaría una configuración robusta de controles preventivos que fortalecen la postura de seguridad y disminuyen el riesgo de explotación dentro de la infraestructura corporativa.

Tabla 3

Controles preventivos recomendados para la infraestructura evaluada

Control preventivo	Descripción técnica	Objetivo
Gestión de vulnerabilidades y parches	Es el inventario actualizado de activos, priorización por criticidad, aplicación oportuna de parches y actualizaciones.	Se busca reducir la probabilidad de explotación de fallas conocidas y mantener los sistemas protegidos.
Hardening del sistema y servicios	Es la configuración segura basada en CIS-NIST, desactivación de servicios innecesarios y eliminación de software obsoleto.	Se busca minimizar la superficie de ataque y eliminar vectores de explotación.
Políticas de privilegios mínimos	Es la restricción de permisos, control de cuentas administrativas y auditoría periódica de accesos.	Se busca limitar el alcance de una posible intrusión y reducir impacto del compromiso.
Segmentación de red	Es la separación lógica mediante VLAN, listas de acceso y firewalls internos.	Se busca evitar desplazamientos laterales no autorizados y aislar zonas críticas.
Control de accesos a servicios expuestos	Es el filtrado de puertos, autenticación obligatoria, y restricción de interfaces administrativas.	Se busca prevenir accesos no autorizados y proteger servicios sensibles.

Nota. Esta tabla representa el análisis defensivo de los hallazgos ofensivos del ejercicio Red Team.

Tabla 4

Relación entre riesgos identificados y controles preventivos aplicables

Riesgo hallado	Control preventivo que se ha aplicado	Resultado que se espera
Explotación del servicio HFS vulnerado	La gestión de parches y hardening	El vector inicial corregido y eliminación de falla crítica
Escalamiento y abuso de privilegios	Implementacion de la política de privilegios mínimos	La restricción de capacidades del atacante tras compromiso
Movimiento lateral interno	Gestionar la implementación de la segmentación de red	Se procede a impedir desplazamiento hacia otros hosts Host B
Acceso no autorizado a servicios sensibles	Generar el control de accesos a servicios expuestos	Se genera el bloqueo de intentos externos e internos no autorizados

Nota. Tabla que representa la relación entre riesgos y medidas preventivas.

Controles detectivos recomendados

Los controles detectivos son los que representan el componente principal dentro de una arquitectura de defensa en profundidad, ya que se puede identificar de manera oportuna y rapida las actividades sospechosas, patrones extraños o comportamientos maliciosos antes de que puedan llegar a comprometer la infraestructura de forma irreversible es por ello que, a partir del análisis del escenario ofensivo ejecutado en el Host A y en el Host B se evidenció que no hay mecanismos de monitoreo y correlación de eventos, razón por la cual permitió que la explotación del servicio HttpFileServer HFS versión 2.3 y la apertura de la sesión Meterpreter se llevaron a cabo sin generar alertas por ello para corregir esta brecha, es necesario implementar soluciones con la herramienta SIEM - Security Information and Event Management las cuales son capaces de recolectar, analizar y correlacionar logs provenientes de servidores, firewalls, sistemas operativos y servicios expuestos.

Estas plataformas permiten generar alertas basadas en reglas, correlaciones temporales, firmas de ataques conocidos y modelos de comportamiento del usuario UEBA y asimismo se recomienda la implementación de sistemas IDS-IPS Intrusion Detection/Prevention Systems la cuales permitan investigar el tráfico de red en busca de patrones asociados a exploits, cargas maliciosas o conexiones inversas no autorizadas es por ello que con la practica hecha se entiende que un IDS correctamente configurado podría detectar la explotación del CVE-2014-6287, la ejecución de un payload de conexión inversa y el establecimiento del túnel SOCKS utilizado para el movimiento lateral y a que este tipo de sistemas complementados con listas de firmas actualizadas y análisis heurístico aumentan la probabilidad de descubrir un ataque en sus primeras fases. (Scarfone & Mell, 2022)

Es importante también activar auditorías de seguridad en los sistemas operativos de Windows y Linux involucrados y muy especialmente aquellas asociadas con acceso a archivos sensibles, creación de procesos, uso de comandos administrativos y cambios en configuraciones críticas puesto que la activación de logs detallados permite que se pueda llegar a identificar acciones asociadas al abuso de privilegios, manipulación de archivos o exploración interna del sistema después de la explotación inicial además se comprende que la correlación de estos logs dentro del SIEM permite tener una mejora la visibilidad del entorno y permite responder con rapidez ante comportamientos que pudieran pasar desapercibidos es por ello que todos estos controles detectivos fortalecen la capacidad de una organización que permitiría identificar ataques en curso y activar mecanismos de respuesta antes de que el atacante pueda completar o llevar a cabo su presencia en la infraestructura.

Tabla 5

Controles detectivos y su función dentro del monitoreo de seguridad

Control detectivo	Descripción	Evento que puede detectar	Beneficio
SIEM	Genera la correlación de logs, alertas en tiempo real y análisis UEBA	Explotación, conexiones inversas y escalamiento	Se podría detectar ataques en sus primeras fases
IDS/IPS	Genera la inspección profunda de paquetes, firmas y heurística	Exploits, payloads y túneles anómalos	Se podrían bloquear o alertar actividades maliciosas en red
Auditoría de sistemas	Genera el registro detallado de eventos del SO	Comandos sospechosos, acceso a archivos y creación de procesos	Este permite análisis forense y detección de abuso
Monitoreo interno de tráfico lateral	Gestiona las reglas específicas para conexiones inusuales entre hosts	Pivoting, túneles SOCKS y proxificación	Permite detectar movimientos laterales no autorizados

Nota. Esta tabla representa los requerimientos defensivos derivados del ejercicio Red Team.

Controles correctivos y de respuesta a incidentes

Los controles correctivos y los procedimientos de respuesta a incidentes componen la fase en la que la empresa actúa después de que un ataque ha sido detectado o confirmado con la intención de contener los daños, eliminar la amenaza y restaurar las funciones operativas de la empresa con normalidad de manera segura y a partir de los hallazgos del ejercicio Red Team se pudo identificar la explotación exitosa del servicio HttpFileServer HFS versión 2.3, el inicio de una sesión Meterpreter después el movimiento lateral hacia el Host B permitiendo evidenciar que no hay procedimientos formales de respuesta que permitan reaccionar ante incidentes de seguridad. (Instituto Nacional de Ciberseguridad de España [INCIBE], 2023)

Por supuesto para corregir esta brecha es necesario implementar un plan de respuesta a dichos incidentes alineándolo con estándares como NIST SP 800-61 incluyendo las fases de identificación, contención, erradicación, recuperación y retroalimentación, es importante mencionar que durante la fase de contención, la empresa debe actuar rápidamente para detener la actividad del atacante, aislando los equipos comprometidos y así poder evitar la propagación del incidente hacia otros sistemas internos por ello debe desconectar temporalmente los hosts afectados, bloquear conexiones sospechosas, deshabilitar cuentas comprometidas y aplicar filtros en los dispositivos perimetrales y a continuación en la fase de erradicación, es necesario eliminar cualquier rastro de permanencia o configuración maliciosa introducida por el atacante, con lo que se puede incluir la limpieza de payloads, la restauración de archivos modificados, la desinstalación de software no autorizado y la aplicación de parches de seguridad que permiten cerrar la vulnerabilidad explotada.

Ahora en la fase de recuperación se requiere restaurar los sistemas afectados a un estado seguro y funcional, lo cual permite garantizar que se hayan eliminado los vectores de ataque que fueron empleados durante el incidente es por esto que con este proceso puede involucrar la restauración desde respaldos confiables, la reconfiguración de servicios, el fortalecimiento de los hosts comprometidos y la validación de la integridad general del sistema.

Una vez superada la recuperación se debe realizar una retroalimentación a totalidad del incidente mediante un informe post mortem que incluya deba incluir partes como lo son la causa raíz, impacto, líneas de tiempo, acciones implementadas y recomendaciones para evitar reincidencias puesto que este análisis representa una parte muy importante para mejorar la madurez

del equipo Blue Team y fortalecer la capacidad institucional frente a ataques futuros y también promoviendo una cultura de mejora continua con respecto a la gestión en ciberseguridad.

Tabla 6

Controles correctivos y acciones de respuesta a incidentes

Fase del incidente	Acción correctiva	Objetivo de dicha acción
Contención	Se gestiona el aislamiento de equipos comprometidos, bloqueo de sesiones activas y tráfico sospechoso	Se pretende detener la actividad del atacante y evitar propagación
Erradicación	Se debe eliminar payloads, cerrar vulnerabilidades y limpiar configuraciones alteradas	Se busca remover cualquier persistencia y preparar el sistema para recuperación
Recuperación	Se debe restaurar servicios desde backups confiables, reconfigurar servicios y aplicar hardening	Se busca devolver el sistema a un estado seguro y funcional
Retroalimentación	Se procede a la elaboración de un informe post incidente, análisis de causa raíz y lecciones aprendidas	Se busca prevenir incidentes similares y fortalecer el proceso de seguridad

Nota. Esta tabla está basada en las fases del estándar NIST SP 800-61.

Medidas de hardening basadas en hallazgos

Las medidas de hardening son las que representan el conjunto de acciones guiada paraa reducir la superficie de un ataque mediante la configuración segura de sistemas, servicios y redes y por ello a partir de los hallazgos del ejercicio ofensivo se pudieron identificar múltiples debilidades asociadas a servicios desactualizados, privilegios excesivos, sin segmentación y sin restricciones en los hosts comprometidos, comprendiendo este escenario el primer componente principal del hardening corresponde a la protección del servicio HttpFileServer HFS versión 2.3, el cual fue el vector inicial de explotación y por supuesto para fortalecer este punto crítico es recomendable desinstalar versiones antiguas del servicio, aplicar parches de seguridad, restringir su acceso únicamente a direcciones autorizadas y para una mayor mejora sustituirlo por alternativas seguras y soportadas. (Center for Internet Security [CIS], 2022)

Por supuesto estas acciones mitigarían vulnerabilidades conocidas y evitarian que un atacante pueda ejecutar código remoto como ocurrió en el escenario visto de igual forma, el hardening del sistema operativo es una medida necesaria para minimizar el impacto de un ataque exitoso por ello, durante el ejercicio aplicado se evidenció que el Host A permitía la ejecución de comandos avanzados sin restricciones y por supuesto esto representa la ausencia de políticas de privilegios mínimos y controles para la ejecución de binarios por esa razón para corregir esta debilidad, es recomendable gestionar configuraciones de seguridad basadas en estándares como lo es CIS Benchmarks, el cual incluye la desactivación de servicios innecesarios, el bloqueo de puertos no requeridos, la implementación de contraseñas más robustas, la habilitación de auditorías de seguridad y la protección de directorios sensibles como también se debe limitar el uso de cuentas administrativas, segmentar los privilegios y deshabilitar el acceso remoto a interfaces que no sean estrictamente necesarias. (Center for Internet Security, 2022)

También las medidas de hardening deben extenderse al entorno de red, en donde el movimiento lateral entre el Host A y Host B ha mostrado una falta de aislamiento adecuado por ende, para mitigar esta vulnerabilidad es recomendable realizar la segmentación mediante VLAN, establecer listas de control de acceso y limitar la comunicación lateral únicamente a flujos autorizados también la adopción de firewalls internos, inspección a detalle de paquetes y filtrado de tráfico SOCKS la cuales son medidas esenciales para impedir el pivoting, como el que le permitió al atacante acceder a los servicios críticos del Host B por ende se entiende que las medidas de hardening propuestas fortalecerán enormemente la postura de seguridad y reducirían la

probabilidad de que un ataque inicial evolucione hacia un compromiso completo de la infraestructura.

Tabla 7

Medidas de hardening propuestas según los hallazgos ofensivos

Área de hardening	Acción correcta	Riesgo que ha sido mitigado
Servicio HFS	Se debe desinstalar versión 2.3, aplicar parches, restringir acceso y reemplazar por versión segura	La explotación remota CVE-2014-6287
Sistema operativo	Se deben desactivar servicios innecesarios, proteger directorios, habilitar auditorías y aplicar CIS Benchmarks	La ejecución de comandos y abuso de privilegios
Cuentas de usuario	Se debe implementar privilegios mínimos, restringir cuentas administrativas y rotar credenciales	La elevación de privilegios y persistencia
Red interna	Se deben aplicar VLAN, ACL y firewalls internos, también bloquear tráfico no autorizado	Movimiento lateral y pivoting
Servicios críticos	Se deben restringir interfaces de administración, habilitar autenticación fuerte y monitoreo constante	El acceso no autorizado a activos internos

Nota. Elaboración propia con base en las debilidades observadas en el ejercicio ofensivo Red Team.

Integración Red Team & Blue Team - Análisis conjunto

Con el desarrollo e integración de los resultados que se han obtenido desde la visión tanto de Red Team como la de Blue Team se ha podido comprender el ejercicio desarrollado en la etapa 3 en el seminario como un proceso completo del ciclo de la ciberseguridad, en las cuales se estudiaron las acciones ofensivas y defensivas en cómo son presentados como esfuerzos aislados y como componentes adicionales de un mismo proceso de mejora continua ya que por supuesto desde el rol ofensivo el Red Team ha logrado identificar y explotar vulnerabilidades críticas

presentes en el servicio HttpFileServer HFS versión 2.3. (National Institute of Standards and Technology [NIST], 2020)

También se ha podido consolidar una sesión remota mediante Meterpreter y así efectuar pivoting hacia el Host B, con lo cual se han evidenciado las fallas relacionadas con la gestión de vulnerabilidades, la falta de segmentación de red, la falta de controles de privilegios mínimos y la inexistencia de monitoreo efectivo es por ello que estos hallazgos han puesto en evidencia las debilidades técnicas de la infraestructura simulada y han ofrecido los insumos concretos para que el equipo de Blue Team pudiera diseñar e realizar controles preventivos, detectivos y correctivos alineados a las necesidades reales del entorno evaluado.

Ahora revisando la perspectiva del equipo de Blue Team se ha analizado cada fase del ataque y se conectó con controles específicos con los que se habrían prevenido o mitigado su impacto, para ello se comprende que se deben integrar las prácticas de gestión de parches, hardening de sistemas, segmentación de red, monitoreo mediante SIEM e IDS - IPS y planes de respuesta a incidentes basados en estándares como NIST SP 800-61 ya que de esta manera, la explotación se exitosa del CVE-2014-6287 se analiza y se gestiona la recomendación de establecer procesos formales de gestión de vulnerabilidades, la obtención de una sesión Meterpreter y el abuso de privilegios se asocian con la necesidad de implementar políticas de privilegios mínimos y auditorías constantes y el movimiento lateral hacia el Host B permite reforzar la importancia de segmentar la red interna, restringir la comunicación entre segmentos y supervisar el tráfico lateral y por supuesto esta correlación directa entre hallazgos ofensivos y controles defensivos

demuestran la utilidad del enfoque en donde se permite transformar la evidencia técnica en decisiones concretas de optimización de la postura de seguridad. (SANS Institute, 2022)

Bajo todo este análisis se entiende que este ejercicio puede interpretarse como una cercanía a la práctica que ejercen el equipo de Purple Team, en el cual los equipos Red Team y Blue Team están trabajando en colaboración de manera coordinada para poder alinear técnicas de ataque con capacidades de defensa y así se genera un aprendizaje bidireccional que permita fortalecer las capacidades profesionales en ciberseguridad.

Por ende se comprende que, las acciones realizadas en el escenario planteado por la empresa SecureNova Labs se puede evidenciar que la efectividad de un trabajo o programa de seguridad depende de la capacidad para detectar y bloquear ataques y también de la disposición para analizar los incidentes, para generar la correcta documentación de las lecciones aprendidas y se pueda ajustar las estrategias de protección con base en la evidencia de igual forma, la integración entre los componentes técnicos y el marco legal como también el ético colombiano fortalece la responsabilidad en nuestra profesión como especialistas en seguridad informática pues debemos garantizar que las actividades de pruebas de penetración, monitoreo y respuesta a incidentes se efectúen dentro de los límites normativos y deontológicos por ello el trabajo en equipo es necesario para obtener los resultados Red Team y Blue Team lo cual demostraría que la seguridad eficaz es el resultado de un proceso continuo de evaluación, fortalecimiento y retroalimentación, y es por ello que en cada ataque simulado se tiene en una oportunidad para elevar el nivel de madurez de la organización frente a futuras amenazas. (Superintendencia de Industria y Comercio, 2020)

Tabla 8

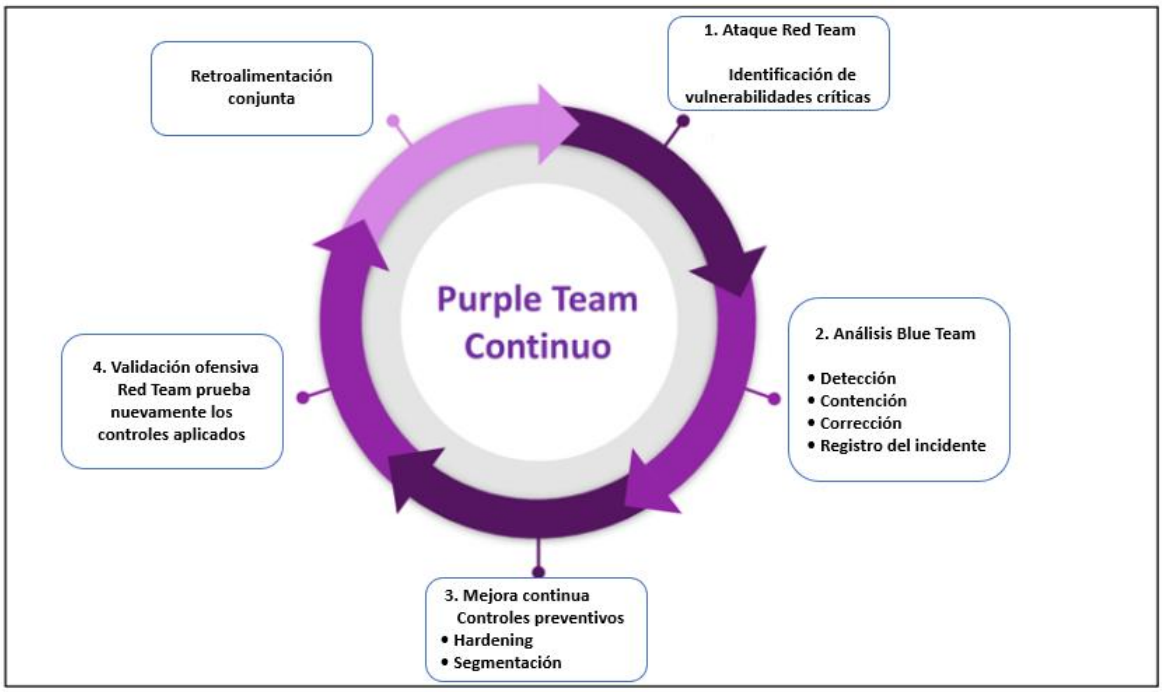
Integración de resultados Red Team y Blue Team en el ejercicio del seminario

Fase de Red Team	Actividad ofensiva ejecutada	Fallo hallado	Respuesta de Blue Team asociada	Control recomendado
Reconocimiento	Se genera la identificación del servicio HFS 2.3 vulnerable	Una exposición de servicios obsoletos	Gestión de vulnerabilidades	Inventario - escaneo periódico - parches
Explotación	Se reconoce el uso del CVE-2014-6287 para obtener acceso remoto	La falta de actualización y hardening	Hardening del servicio	Desinstalar HFS vulnerable - restringir acceso
Post-explotación	Se genera la numeración, privilegios y sysinfo	La ausencia de restricciones y monitoreo	Auditoría del sistema	Privilegios mínimos - logging - SIEM
Movimiento lateral	Se genera el pivoting desde Host A hacia Host B	Se evidencia la red sin segmentación	Firewalls internos y VLAN	Segmentación - ACL
Acceso a activos críticos	Se logra acceder a Nessus por medio del túnel SOCKS	Se evidencia la falta de protección interna	Monitoreo del tráfico lateral	IDS IPS - inspección profunda

Nota. En esta tabla se integran hallazgos ofensivos y controles defensivos para fortalecer la postura de seguridad.

Figura 17

Ciclo de integración Red Team & Blue Team - Enfoque Purple Team



Fuente. Autoría Propia

Nota. Diagrama elaborado para representar el ciclo colaborativo Purple Team derivado del ejercicio realizado en el seminario.

Tabla 9

Matriz de correlación entre hallazgos ofensivos y acciones defensivas

Hallazgo ofensivo	Riesgo generado	Acción defensiva que se aplicó	Resultado esperado
HFS 2.3 vulnerable	Acceso remoto no autorizado	Se realiza la gestión de parches y eliminación de versiones obsoletas	Se genera la eliminación del vector inicial
Sesión Meterpreter sin alertas	Ejecución de comandos maliciosos	SIEM - auditorías	Se accede a la detección temprana del ataque
Privilegios excesivos	Escalamiento y abuso	Privilegios mínimos	Se genera la reducción del impacto
Pivoting exitoso	Compromiso lateral	Segmentación de red	Se genera la contención del movimiento lateral
Acceso a Nessus	Exposición de activos críticos	Firewalls internos - monitoreo	Se aplica mayor protección de los servicios sensibles

Nota. Esta tabla representa la matriz que integra el análisis Red Team - Blue Team para fortalecer la defensa en profundidad.

Tabla 10

Mapa de alineación entre táctica ofensiva y control defensivo

Táctica del Red Team	Subtécnica usada	Fallo	Control del Blue Team asociado	Efecto sobre la postura de seguridad
Reconocimiento externo	Escaneo de puertos	Exposición del HFS vulnerable	Gestión de vulnerabilidades	Eliminación del vector inicial
Explotación	CVE-2014-6287 (HFS)	Falta de parches	Hardening - Parches	Reducción del riesgo crítico
Post-explotación	Meterpreter activo	Privilegios excesivos	Privilegios mínimos - Auditoría	Limita el impacto del atacante
Movimiento lateral	Pivoting SOCKS4	Sin segmentación	VLAN - ACL - Firewall interno	Detección del movimiento lateral
Acceso a servicios críticos	Navegación a Nessus	Sin monitoreo interno	SIEM - IDS - Tráfico lateral	Detecta actividades anómalas

Nota. Esta tabla representa la alineación entre táctica ofensiva y control defensivo

Conclusiones

Con el desarrollo del ejercicio presentado en este seminario se pudo evidenciar cómo la combinación de técnicas ofensivas y defensivas fortalecen la comprensión de la seguridad informática en escenarios reales ya que, con la explotación del servicio HttpFileServer HFS versión 2.3, la obtención de una sesión remota mediante Meterpreter y el posterior movimiento lateral hacia el Host B han permitido demostrar que las vulnerabilidades técnicas que no son abordadas a tiempo pueden llegar a escalar rápidamente hacia compromisos mayores en donde se puede ver afectada la disponibilidad, confidencialidad e integridad de los sistemas.

En el desempeño de la funciones y ejercicio del equipo Blue Team se pudo revelar y comprender la importancia de implementar controles preventivos, detectivos y correctivos como parte de una arquitectura de defensa en profundidad y comprender que la falta de monitoreo continuo, la ausencia de alertas frente a conexiones internas sospechosas y el manejo inadecuado de privilegios pueden convertirse en los factores determinantes para que el ataque progresara sin restricciones es por ello que con la implementación de soluciones como SIEM, IDS - IPS, auditorías avanzadas y políticas de privilegios mínimos habrá un fortalecimiento de la capacidad organizacional de detectar incidentes en tiempo real.

Con la integración de los procesos que emplean y ejecutan el equipo del Red Team y las respuestas planteadas por el Blue Team permitió comprender que la asociación de estos dos equipos da como origen al enfoque Purple Team, el cual representa una potencia efectividad de la ciberseguridad organizacional puesto que, cada hallazgo ofensivo aportó un insumo directo para diseñar o reforzar un control defensivo específico y con esto se ha evidenciado que el aprendizaje colaborativo entre equipos es un mecanismo que resulta muy poderoso para optimizar recursos.

Recomendaciones

Implementar un programa formal de gestión de vulnerabilidades

La empresa debe iniciar con un proceso continuo de identificación, clasificación, priorización y remediación de vulnerabilidades, empleando herramientas de escaneo y estandarizando ciclos de actualización basados en criticidad además, este programa debe incluir inventarios actualizados, análisis de riesgo y aplicación oportuna de parches.

Sustituir o actualizar servicios obsoletos y vulnerables

Es importante que cualquier software en estado descontinuado debe eliminarse o actualizarse a versiones seguras especialmente, se recomienda retirar el servicio HttpFileServer HFS versión 2.3 e implementar alternativas soportadas que cuenten con parches vigentes y configuraciones fortalecidas.

Aplicar hardening de sistemas operativos y servicios críticos

Se deben adoptar guías de endurecimiento como CIS Benchmarks o NIST SP 800-70 para que se puedan establecer configuraciones seguras, incluyendo desactivación de servicios innecesarios, bloqueo de puertos no utilizados, protección de directorios sensibles, autenticación robusta y auditoría interna.

Implementar políticas estrictas de privilegios mínimos

Es preciso que de inmediato se restrinjan los permisos administrativos, también separar funciones, deshabilitar cuentas innecesarias y realizar auditorías periódicas del uso de privilegios

ya que con esto se evitará que un atacante con acceso inicial pueda escalar privilegios o manipular procesos críticos.

Establecer mecanismos de segmentación y control del tráfico interno

Es importante que la red sea dividida en segmentos lógicos mediante VLAN, ACL y firewalls internos, permitiendo así que únicamente los flujos estrictamente necesarios entre hosts por supuesto, esto reducirá el riesgo de pivoting, evita el movimiento lateral y mejora la contención de incidentes.

Incorporar soluciones SIEM para monitoreo centralizado

Se recomienda implementar una plataforma de SIEM que la cual permitirá recolectar, correlacionar y analizar eventos de seguridad en tiempo real lo cual facilitará la detección temprana de amenazas, conexiones sospechosas, patrones inusuales y posibles actividades de explotación.

Configurar IDS - IPS para detectar actividad maliciosa en la red

La empresa debe tener presente iniciar con el despliegue de sistemas de detección y prevención de intrusiones que identifiquen exploits, túneles no autorizados, tráfico anómalo y payloads maliciosos ya que con un IDS - IPS correctamente configurado se habría detectado la explotación del CVE-2014-6287.

Establecer un plan formal de respuesta a incidentes

Es importante, prioritario y necesario diseñar, documentar y aplicar un plan de respuesta basado en NIST SP 800-61 en el cual se incluyan procedimientos para identificación, contención,

erradicación, recuperación y análisis post incidente y también es importante comprender que este plan debe actualizarse regularmente y probarse mediante simulaciones.

Realizar copias de seguridad periódicas y verificadas

Es importante generar los respaldos los cuales deben ejecutarse de forma programada, almacenarse en ubicaciones seguras y verificarse periódicamente para que se pueda asegurar su integridad y generar la restauración desde backups confiables lo cual reduce el tiempo de recuperación ante incidentes de seguridad.

Implementar monitoreo del tráfico lateral y conexiones internas

Se deben aplicar reglas y sensores que detecten conexiones inusuales entre hosts, túneles SOCKS, proxificación o intercambios atípicos que indiquen movimiento lateral por supuesto este proceso es fundamental para evitar accesos no autorizados a servicios críticos.

Fortalecer la cultura de seguridad y la capacitación interna

La empresa debe realizar entrenamientos constantes a sus empleados sobre higiene digital, manejo de incidentes, identificación de amenazas y uso responsable de sistemas ya que es entendible que el factor humano continúa siendo un componente esencial de la protección integral.

Cumplir a cabalidad con las normas legales y éticas aplicables en Colombia

Es indispensable y siempre por encima de todo garantizar el cumplimiento de la Ley 1273 de 2009, Ley 1581 de 2012, Decreto 1377, y las directrices de COPNIA para estar totalmente

seguros que todas las actividades de prueba, monitoreo y análisis se realicen dentro de los límites legales y profesionales correspondientes.

Referencias Bibliográficas

Agencia Española de Protección de Datos. (2021). *Guía para la gestión y notificación de brechas de datos personales*. AEPD.

Center for Internet Security. (2022). *CIS controls v8: Implementation guide for enterprises*. CIS.

Centro Criptológico Nacional. (2022). *Guía de seguridad CCN-STIC 817: Hardening de sistemas Windows y Linux*. CCN-CERT.

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por la cual se modifica el Código Penal en materia de delitos informáticos*. Diario Oficial No. 47.223.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.

Consejo Profesional Nacional de Ingeniería. (2018). *Código de ética profesional del COPNIA*. COPNIA.

Instituto Nacional de Ciberseguridad de España. (2023). *Guía de respuesta ante incidentes de ciberseguridad*. INCIBE.

Kaspersky Lab. (2023). *Advanced persistent threats: 2023 predictions report*. Kaspersky Security Bulletin.

MITRE Corporation. (2024). *MITRE ATT&CK framework: Techniques and mitigations for enterprise environments*. MITRE.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Guía de gestión de vulnerabilidades en entidades públicas colombianas*. MinTIC.

National Institute of Standards and Technology. (2018). *NIST SP 800-61 revision 2: Computer security incident handling guide*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2020). *NIST SP 800-53 revision 5: Security and privacy controls for information systems and organizations*. U.S. Department of Commerce.

SANS Institute. (2022). *Red team operations and adversary emulation manual*. SANS.

Scarfone, K., & Mell, P. (2022). *Guide to intrusion detection and prevention systems (IDPS)*. NIST Special Publication.

Superintendencia de Industria y Comercio. (2020). *Guía para la implementación del programa de protección de datos personales*. SIC.

Symantec Corporation. (2023). *Threat intelligence report: Network lateral movement and exploitation techniques*. Broadcom Inc.

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://www.youtube.com/watch?v=D2c_0leFXLQ*

Figura 18

Evidencia del video de sustentación del informe final

Fuente. Autoría Propia

Nota. Evidencia del video publicado

Apéndices

Apéndice A

Resultado de Turnitin - Prueba Antiplagio: Doc Final Biblioteca_Linda Enciso_Esp.pdf

Figura 19

Resultado de Turnitin - Prueba Antiplagio

Doc Final Biblioteca_Linda Enciso_Esp

INFORME DE ORIGINALIDAD

3%	2%	1%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repository.unad.edu.co Fuente de Internet	1%
2	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	1%
3	www.coursehero.com Fuente de Internet	<1%
4	Jimenez Leon, William Humberto. "Modelo de integración de la arquitectura de seguridad empresarial O-ESA con Implementación de controles CIS", Universidad Distrital Francisco JosÃ© de Caldas (Colombia), 2025 Publicación	<1%
5	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	<1%
6	www.colibri.udelar.edu.uy Fuente de Internet	<1%
7	www.youtube.com Fuente de Internet	<1%

8	coleweb.dc.fi.udc.es Fuente de Internet	<1 %
9	kleinnerfarias.github.io Fuente de Internet	<1 %
10	vigilantedeseguridadvs.com Fuente de Internet	<1 %
11	www.mlsjournals.com Fuente de Internet	<1 %
12	www.tecnotendencias.com Fuente de Internet	<1 %
13	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 18 (2002)", Brill, 2006 Publicación	<1 %
14	openaccess.uoc.edu Fuente de Internet	<1 %
15	risti.xyz Fuente de Internet	<1 %
16	www.jca.gobierno.pr Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	Apagado
Excluir bibliografía	Activo		

Recibo Digital de Turnitin - Prueba Antiplagio: recibo_Doc Final Biblioteca_Linda Enciso_Esp.pdf

Figura 20

Recibo Digital de Turnitin - Prueba Antiplagio

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	LINDA MAYERLY ENCISO ORTIZ
Título del ejercicio:	ECBTI - Draftbank 1 Sección 2 (Moodle TT)
Título de la entrega:	Doc Final Biblioteca_Linda Enciso_Esp
Nombre del archivo:	871552_LINDA_MAYERLY_ENCISO_ORTIZ_Doc_Final_Biblioteca...
Tamaño del archivo:	2.75M
Total páginas:	69
Total de palabras:	11,374
Total de caracteres:	64,938
Fecha de entrega:	26-dic-2025 11:42p. m. (UTC-0500)
Identificador de la entrega:	2825327912