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

Jessica Fernanda Corredor Cuesta

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

Dedico este trabajo a mi familia, especialmente a mis padres, quienes han sido mi principal fuente de apoyo, motivación y fortaleza durante todo mi proceso de formación académica. Gracias a su esfuerzo, confianza y acompañamiento constante he podido superar los desafíos que se han presentado a lo largo de este camino. También dedico este logro a todas las personas que, de una u otra manera, me brindaron palabras de ánimo, comprensión y apoyo en los momentos de mayor exigencia. Cada enseñanza, consejo y muestra de confianza contribuyó significativamente al cumplimiento de esta meta académica y profesional.

Agradecimientos

Expreso mi más sincero agradecimiento a Dios por brindarme la fortaleza, la perseverancia y la sabiduría necesarias para culminar esta importante etapa de mi formación profesional. Agradezco especialmente a mi familia por su amor incondicional, comprensión y apoyo permanente, los cuales fueron fundamentales para mantener la motivación y el compromiso durante el desarrollo de este proceso académico. De igual manera, agradezco al tutor del seminario por su orientación, acompañamiento y valiosos aportes académicos, que permitieron fortalecer los conocimientos adquiridos y enriquecer el desarrollo de este trabajo. Finalmente, agradezco a la Universidad Nacional Abierta y a Distancia – UNAD por brindarme los espacios de aprendizaje y crecimiento profesional que hicieron posible alcanzar este importante logro.

Resumen

El presente documento evidencia y consolida los resultados obtenidos durante el desarrollo del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, en el cual se abordaron aspectos relacionados con la seguridad ofensiva, la seguridad defensiva, la gestión de incidentes y el cumplimiento normativo dentro de entornos organizacionales. A lo largo del seminario se analizaron los fundamentos conceptuales de las operaciones Red Team y Blue Team, las implicaciones éticas y legales asociadas al ejercicio profesional de la ciberseguridad y la aplicación práctica de metodologías de pentesting para la identificación y explotación controlada de vulnerabilidades. Durante el desarrollo de los escenarios propuestos se identificaron debilidades de seguridad presentes en sistemas Windows vulnerables, empleando herramientas especializadas como Nmap y Metasploit para la ejecución de actividades de reconocimiento, análisis y validación de vulnerabilidades. Asimismo, se evaluó el impacto de vulnerabilidades críticas como MS17-010 (EternalBlue) y fallos asociados a servicios HTTP vulnerables, evidenciando los riesgos que representan los sistemas desactualizados dentro de una infraestructura tecnológica. Desde la perspectiva defensiva, se analizaron estrategias de hardenización, gestión de vulnerabilidades, monitoreo continuo, respuesta a incidentes y aplicación de controles de seguridad basados en marcos de referencia como NIST, CIS Controls e ISO 27001. Igualmente, se estudiaron herramientas de contención y protección tales como Cisco ASA, Microsoft Defender for Endpoint y Palo Alto Networks, destacando su importancia dentro de las operaciones Blue Team para reducir la superficie de ataque y fortalecer la postura de seguridad organizacional. Los resultados obtenidos permitieron comprender la importancia de integrar capacidades ofensivas y defensivas dentro de una estrategia integral de ciberseguridad, promoviendo la identificación temprana de vulnerabilidades, la implementación de controles preventivos y la adopción de mecanismos de respuesta orientados a proteger la confidencialidad, integridad y disponibilidad de la información.

***Palabras clave*:** Ciberseguridad, hardening, pentesting, red team, vulnerabilidad.

Abstract

This document presents and consolidates the results obtained during the Specialized Seminar: Strategic Cybersecurity Teams: Red Team & Blue Team, which addressed topics related to offensive security, defensive security, incident management, and regulatory compliance within organizational environments. Throughout the seminar, the conceptual foundations of Red Team and Blue Team operations were analyzed, along with the ethical and legal implications associated with cybersecurity practice and the practical application of penetration testing methodologies for the identification and controlled exploitation of vulnerabilities. During the proposed scenarios, security weaknesses were identified in vulnerable Windows systems using specialized tools such as Nmap and Metasploit to perform reconnaissance, analysis, and vulnerability validation activities. In addition, the impact of critical vulnerabilities such as MS17-010 (EternalBlue) and flaws associated with vulnerable HTTP services was evaluated, highlighting the risks posed by outdated systems within technological infrastructures. From a defensive perspective, strategies related to system hardening, vulnerability management, continuous monitoring, incident response, and the implementation of security controls based on frameworks such as NIST, CIS Controls, and ISO 27001 were examined. Likewise, containment and protection tools such as Cisco ASA, Microsoft Defender for Endpoint, and Palo Alto Networks were studied, emphasizing their relevance within Blue Team operations to reduce the attack surface and strengthen organizational security posture. The results obtained demonstrated the importance of integrating offensive and defensive capabilities within a comprehensive cybersecurity strategy, promoting the early identification of vulnerabilities, the implementation of preventive controls, and the adoption of response mechanisms aimed at protecting the confidentiality, integrity, and availability of information.

Keywords**:** Cybersecurity, hardening, penetration testing, red team, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Grupo de trabajo encargado de proteger los sistemas de información de una organización mediante actividades de monitoreo, análisis, detección y respuesta frente a posibles incidentes de seguridad.

Ciberseguridad:

Conjunto de acciones, herramientas y buenas prácticas orientadas a proteger la información, los sistemas y las redes frente a accesos no autorizados, ataques o cualquier situación que pueda afectar su funcionamiento.

CSIRT:

Equipo especializado que coordina la atención de incidentes de seguridad informática, apoyando las actividades de análisis, contención, recuperación y seguimiento de los eventos ocurridos.

EDR (Endpoint Detection and Response):

Tecnología que permite supervisar continuamente los equipos finales de una organización para detectar actividades sospechosas y responder rápidamente ante posibles amenazas.

EternalBlue:

Vulnerabilidad conocida que afecta versiones de Windows que utilizan SMBv1 y que permite a un atacante ejecutar acciones remotas sobre sistemas que no cuentan con las actualizaciones de seguridad correspondientes.

Exploit:

Método o código utilizado para aprovechar una vulnerabilidad existente con el fin de obtener acceso o ejecutar acciones sobre un sistema de manera no autorizada.

Incidente de seguridad:

Situación que afecta o pone en riesgo la protección de la información, los servicios tecnológicos o los recursos informáticos de una organización.

MS17-010:

Actualización de seguridad publicada por Microsoft para corregir vulnerabilidades críticas presentes en el protocolo SMB de Windows.

Nmap:

Herramienta utilizada para analizar redes y descubrir información sobre equipos, puertos abiertos y servicios disponibles dentro de una infraestructura tecnológica.

Pentesting:

Evaluación controlada de seguridad que busca identificar vulnerabilidades mediante la simulación de técnicas empleadas por posibles atacantes.

Pivoting:

Técnica que permite utilizar un equipo previamente comprometido como punto de acceso para alcanzar otros sistemas dentro de la misma red.

Post-explotación:

Fase que se desarrolla después de obtener acceso a un sistema vulnerable, en la cual se recopila información adicional y se valida el alcance del compromiso logrado.

Red Team:

Equipo que realiza pruebas ofensivas simulando escenarios reales de ataque para evaluar la capacidad de defensa y los controles de seguridad de una organización.

Rejetto HFS:

Aplicación utilizada para compartir archivos mediante un servidor web ligero, la cual ha

presentado vulnerabilidades que pueden ser aprovechadas si no se encuentra adecuadamente protegida.

Vulnerabilidad:

Debilidad presente en un sistema, aplicación o configuración que puede ser aprovechada para comprometer la seguridad de la información o afectar el funcionamiento normal de los servicios.

Introducción

La ciberseguridad se ha convertido en un componente fundamental para las organizaciones modernas debido al incremento constante de amenazas, vulnerabilidades y ataques dirigidos contra infraestructuras tecnológicas, sistemas de información y activos digitales. La transformación digital, la adopción de servicios en línea y la creciente interconectividad de los sistemas han ampliado la superficie de ataque de las organizaciones, generando nuevos desafíos para la protección de la información y la continuidad de las operaciones. En este contexto, resulta indispensable implementar estrategias que permitan identificar, evaluar y mitigar los riesgos asociados a incidentes de seguridad informática.

Los equipos Red Team y Blue Team desempeñan un papel fundamental dentro de los programas de ciberseguridad organizacional. Mientras el Red Team se encarga de simular técnicas y procedimientos utilizados por atacantes reales para identificar vulnerabilidades y evaluar la efectividad de los controles de seguridad existentes, el Blue Team tiene la responsabilidad de monitorear, detectar, contener y responder a las amenazas que puedan afectar la infraestructura tecnológica. La integración de ambos enfoques permite fortalecer la postura de seguridad de las organizaciones mediante una visión complementaria entre ataque y defensa.

La integración de capacidades ofensivas y defensivas permite fortalecer la postura de seguridad organizacional mediante la identificación temprana de vulnerabilidades y la mejora continua de los controles de protección (Arroyo, 2025) además de Kotwani et al. (2023).

El presente informe técnico consolida los resultados obtenidos durante el desarrollo del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, tomando como referencia el escenario propuesto de SecureNova Labs. A lo largo de las diferentes etapas se abordaron aspectos relacionados con el marco legal y ético de la ciberseguridad, las metodologías de pruebas de penetración, la identificación y explotación

controlada de vulnerabilidades, la gestión de incidentes y la implementación de controles defensivos orientados a reducir los riesgos asociados a amenazas cibernéticas.

Dentro del componente práctico se desarrollaron ejercicios de reconocimiento, enumeración de servicios, análisis de vulnerabilidades y explotación controlada de sistemas Windows vulnerables mediante herramientas especializadas como Nmap y Metasploit. Asimismo, se analizaron vulnerabilidades críticas como MS17-010 (EternalBlue) y servicios vulnerables asociados a Rejetto HFS, permitiendo comprender el impacto que pueden generar los sistemas desactualizados dentro de un entorno organizacional. Posteriormente, desde la perspectiva Blue Team, basados en marcos de referencia como NIST (NIST, 2022), CIS Controls (Center for Internet Security, 2024) e ISO 27001 (International Organization for Standardization, 2022)."

Justificación

La realización del presente seminario responde a la necesidad de comprender y aplicar estrategias integrales de ciberseguridad que permitan identificar, evaluar y mitigar los riesgos asociados a vulnerabilidades presentes en infraestructuras tecnológicas. En un entorno donde las organizaciones dependen cada vez más de los sistemas de información para el desarrollo de sus actividades, resulta fundamental contar con profesionales capaces de reconocer amenazas, validar debilidades de seguridad y proponer mecanismos efectivos de protección y respuesta ante incidentes informáticos.

A través del escenario SecureNova Labs fue posible analizar situaciones reales relacionadas con la gestión de vulnerabilidades, las pruebas de penetración, la respuesta a incidentes y el cumplimiento de principios éticos y normativos en materia de ciberseguridad. La ejecución de actividades propias de los equipos Red Team permitió identificar vulnerabilidades críticas presentes en sistemas Windows, evidenciando los riesgos derivados de configuraciones inseguras, servicios expuestos y sistemas desactualizados. De igual manera, las actividades desarrolladas desde la perspectiva Blue Team permitieron comprender la importancia de implementar medidas de hardenización, monitoreo continuo, gestión de eventos de seguridad y controles orientados a reducir la superficie de ataque.

El análisis de marcos de referencia y estándares reconocidos internacionalmente, como NIST, CIS Controls e ISO 27001, permitió establecer buenas prácticas para la gestión de riesgos y la protección de los activos de información. En consecuencia, este trabajo no solo consolida los conocimientos adquiridos durante el seminario, sino que también aporta elementos técnicos y metodológicos que pueden ser aplicados en entornos organizacionales reales para fortalecer la capacidad de prevención, detección, contención y respuesta frente a amenazas cibernéticas.

Objetivos

Objetivo General

Analizar las estrategias ofensivas y defensivas implementadas durante el seminario, mediante la evaluación de vulnerabilidades, la aplicación de técnicas de pentesting y la implementación de mecanismos de protección y contención, con el fin de fortalecer la seguridad de infraestructuras tecnológicas organizacionales.

Objetivos Específicos

Identificar las vulnerabilidades presentes en los sistemas analizados mediante técnicas de reconocimiento, enumeración y explotación controlada.

Evaluar la efectividad de las estrategias de defensa implementadas por el Blue Team para reducir los riesgos identificados durante el ejercicio práctico.

Proponer medidas de fortalecimiento basadas en buenas prácticas, estándares y herramientas de ciberseguridad orientadas a mejorar la postura de seguridad organizacional.

Fundamentos de Ciberseguridad y Operaciones Red Team – Blue Team

Marco normativo colombiano en ciberseguridad y protección de datos

Ley 1581 de 2012 (Congreso de Colombia, 2012): En Colombia regula el derecho fundamental al hábeas data, el cual está relacionado con la facultad que tienen las personas para conocer, actualizar y controlar la información personal que se encuentra en bases de datos. Este derecho tiene sustento en la Constitución Política, específicamente en los artículos 15 y 20, donde se protege la intimidad, el buen nombre y la libertad individual.

Esta ley establece que cada persona es dueña de su información personal y, por tanto, tiene la capacidad de decidir cómo, cuándo y para qué se utilizan sus datos. El hábeas data permite a los ciudadanos ejercer control sobre la información que ha sido recolectada por entidades públicas o privadas, evitando que se generen afectaciones en su vida personal, reputación o derechos fundamentales. la Ley 1581 fue reglamentada parcialmente por el Decreto 1377 de 2013 (Presidencia de la República de Colombia, 2013), el cual define aspectos importantes sobre el tratamiento de datos, como la autorización previa del titular, las políticas de privacidad y las responsabilidades de quienes administran bases de datos.

Uno de los aspectos más relevantes de esta normativa es que reconoce tres derechos fundamentales del titular de la información: el acceso a sus datos, la posibilidad de modificarlos cuando sean incorrectos o incompletos, y la opción de eliminarlos cuando ya no sean necesarios o se estén utilizando de manera indebida. Estas garantías buscan proteger la esfera personal del individuo frente al uso inadecuado de su información.

El CONPES 3995 de 2020 constituye la política nacional de confianza y seguridad digital en Colombia y representa un avance significativo en la gestión de los riesgos asociados al entorno digital. Este documento define la ciberseguridad como la capacidad del Estado para identificar, gestionar y reducir los riesgos derivados del uso de las tecnologías de la información,

garantizando la confidencialidad, integridad, disponibilidad y autenticidad de la información (Consejo Nacional de Política Económica y Social [CONPES], 2020). Asimismo, reconoce que la ciberseguridad no se limita a la protección de sistemas tecnológicos, sino que involucra la protección de las personas, los procesos y los activos estratégicos dentro del ciberespacio mediante la implementación de políticas, controles, tecnologías y estrategias de gestión del riesgo.

Uno de los aspectos más importantes de este CONPES es que proporciona una base conceptual clara, lo que permite que todas las entidades trabajen bajo un mismo enfoque. Esto facilita la coordinación entre instituciones y fortalece la implementación de estrategias de seguridad digital a nivel nacional. El objetivo principal de esta política es fortalecer la confianza digital en el país, mediante el desarrollo de capacidades, la mejora del marco de gobernanza y la adopción de nuevas tecnologías. Para lograrlo, el CONPES se estructura en tres ejes principales: el fortalecimiento de capacidades, la actualización del marco institucional y el análisis de modelos de seguridad digital.

En cuanto al fortalecimiento de capacidades, se plantea la articulación de diferentes entidades del Estado, como el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa y el sector educativo, con el fin de diseñar estrategias de formación en seguridad digital tanto para el sector público como privado. Esto permite que los esfuerzos sean coordinados y que cada entidad contribuya desde su rol al desarrollo de una cultura de ciberseguridad en la ciudadanía.

Ley 1273 de 2009: Fue creada en Colombia con el propósito de proteger la información y los datos frente a las nuevas amenazas derivadas del uso de las tecnologías. Esta ley modificó el Código Penal e incorporó una serie de delitos relacionados con el uso indebido de sistemas informáticos, convirtiéndose en uno de los principales instrumentos jurídicos para combatir la

ciberdelincuencia en Colombia (Congreso de Colombia, 2009), convirtiéndose en una de las principales herramientas legales para combatir la ciberdelincuencia en el país. El objetivo principal de esta normativa es sancionar a aquellas personas que realicen conductas ilícitas a través de medios tecnológicos, como el acceso no autorizado a sistemas, la manipulación de información o el uso fraudulento de datos. De esta manera, se busca no solo castigar estos comportamientos, sino también prevenir los riesgos asociados al crecimiento de las tecnologías de la información.

Dentro de esta ley se establecen varios tipos de delitos informáticos. Por ejemplo, se contempla el hurto por medios informáticos, el cual ocurre cuando una persona logra vulnerar sistemas de seguridad para obtener información o recursos de manera ilegal, incluso suplantando la identidad de un usuario. Asimismo, se incluye la transferencia no consentida de activos, que se presenta cuando, mediante manipulaciones informáticas, se realizan movimientos de dinero u otros recursos sin autorización, afectando a terceros.

Estas conductas se encuentran asociadas a los delitos informáticos incorporados al ordenamiento jurídico colombiano para proteger la información y los sistemas informáticos frente a accesos no autorizados (Maya, 2013).

Esta ley representa un avance importante en la adaptación del marco jurídico colombiano frente a los cambios tecnológicos, ya que reconoce que los delitos también evolucionan junto con la digitalización. Sin embargo, su efectividad depende en gran medida del conocimiento que tengan los ciudadanos sobre estas normas y de la capacidad de las autoridades para aplicarlas correctamente.

Decreto 1377 de 2013 (Presidencia de la República de Colombia, 2013): Reglamenta parcialmente la Ley 1581 de 2012 (Congreso de Colombia, 2012) y establece las condiciones bajo las cuales se deben tratar los datos personales en Colombia. Su principal objetivo es facilitar

la aplicación de la ley, definiendo de manera más específica las responsabilidades de las organizaciones y los derechos de los titulares de la información.

Este decreto desarrolla aspectos clave como la autorización del titular para el uso de sus datos personales, indicando que dicha autorización debe ser previa, informada y verificable. Además, establece que las organizaciones deben informar claramente la finalidad para la cual se recolectan los datos y no pueden utilizar medios engañosos o fraudulentos para obtenerlos. El decreto también establece que las empresas deben contar con políticas de tratamiento de la información, las cuales deben ser claras, accesibles y conocidas por los titulares de los datos. Estas políticas deben incluir información sobre los derechos de los usuarios, los procedimientos para ejercerlos y los responsables del manejo de la información.

Fases y metodología del pentesting

Una prueba de penetración, también conocida como pentest, es un proceso de evaluación de seguridad en el que se simula un ataque controlado sobre un sistema con el fin de identificar vulnerabilidades antes de que puedan ser explotadas por actores maliciosos (Zuluaga Mateus, 2017) y (Álvarez, 2018). Durante esta prueba, el especialista en seguridad actúa como un atacante real, intentando descubrir fallas en redes, aplicaciones o sistemas que puedan ser aprovechadas de manera maliciosa.

El objetivo principal del pentesting es detectar debilidades antes de que un atacante real las explote, permitiendo a las organizaciones tomar medidas preventivas. A partir de los resultados obtenidos, se puede realizar un análisis de riesgos que ayude a entender el impacto que estas vulnerabilidades podrían tener sobre la operación del negocio.

El proceso de pentesting se desarrolla a través de varias fases estructuradas que permiten evaluar de manera organizada la seguridad de un sistema. Las pruebas de penetración

constituyen una herramienta fundamental para evaluar el nivel de exposición de las organizaciones frente a amenazas reales (Vanegas Romero, 2019; INCIBE, 2019).

Interacciones previas al compromiso (Planificación): En esta fase inicial se establecen las condiciones bajo las cuales se realizará la prueba. Se define el alcance del pentest, los objetivos, los sistemas que serán evaluados y las reglas del ejercicio. También se acuerdan aspectos legales, permisos y formas de comunicación con el cliente.

Recolección de información (Reconocimiento): En esta fase el pentester recopila toda la información posible sobre el objetivo, como direcciones IP, dominios, correos electrónicos, tecnologías utilizadas y estructura de la red. Esta información puede obtenerse de forma pasiva (sin interactuar directamente con el sistema) o activa.

Modelado de amenazas: En esta etapa se analizan los posibles escenarios de ataque, identificando qué activos son más importantes para la organización y qué tipo de amenazas podrían afectarlos. Se evalúan los posibles atacantes, sus capacidades y sus motivaciones.

Análisis de vulnerabilidades: Aquí se identifican las debilidades presentes en los sistemas, aplicaciones o redes. Se utilizan herramientas automatizadas y pruebas manuales para detectar errores de configuración, fallas de seguridad o software vulnerable.

Explotación: En esta fase se intenta aprovechar las vulnerabilidades encontradas para demostrar qué tan grave puede ser el impacto. El objetivo no es dañar el sistema, sino evidenciar hasta qué punto un atacante podría comprometer la seguridad. Las pruebas de penetración permiten a las organizaciones conocer de manera anticipada las debilidades presentes en sus infraestructuras tecnológicas y establecer acciones correctivas antes de que estas sean aprovechadas por atacantes reales (Panda Security, 2018).

Post-explotación: Después de explotar una vulnerabilidad, se analiza hasta dónde puede llegar el atacante dentro del sistema comprometido. Por ejemplo, si puede acceder a información sensible, moverse dentro de la red o escalar privilegios.

Reporte (Informe final): Finalmente, se documentan todos los hallazgos del pentest, incluyendo las vulnerabilidades encontradas, su nivel de riesgo y las recomendaciones para mitigarlas. Este informe es clave para que la organización pueda tomar acciones correctivas.

Herramientas utilizadas en pruebas de penetración

Metasploit: es uno de los marcos de explotación más utilizados en auditorías de seguridad, ya que permite validar vulnerabilidades mediante el uso controlado de exploits y módulos especializados (Palomo et al., 2024).

Es una herramienta de software libre ampliamente utilizada en el campo de la ciberseguridad para realizar pruebas de penetración. Su principal función es facilitar la explotación de vulnerabilidades en sistemas informáticos, permitiendo a los profesionales de seguridad evaluar qué tan expuesto se encuentra un sistema frente a posibles ataques.

Esta herramienta cuenta con una amplia base de datos de exploits, los cuales son programas diseñados para aprovechar fallas específicas en sistemas o aplicaciones. Gracias a esto, el usuario puede ejecutar pruebas de manera más eficiente, simulando ataques reales sobre las vulnerabilidades previamente identificadas.

Nmap: Es una herramienta de código abierto ampliamente utilizada para el descubrimiento de hosts, identificación de puertos abiertos y detección de servicios en redes de datos (National Institute of Standards and Technology [NIST], 2008). Su funcionamiento se basa en el envío de paquetes a diferentes dispositivos dentro de una red y el análisis de las respuestas obtenidas, lo que permite identificar hosts activos, puertos abiertos y servicios en ejecución.

Esta herramienta es utilizada tanto por administradores de sistemas para gestionar redes, como por profesionales de ciberseguridad durante la fase de reconocimiento en pruebas de penetración. Gracias a su flexibilidad, también puede ser empleada por atacantes para recolectar información sobre posibles objetivos.En cuanto a los resultados, Nmap clasifica los puertos en diferentes estados, como abiertos, cerrados o filtrados, lo cual permite al analista comprender mejor la superficie de ataque del sistema evaluado. Esta información es fundamental para las siguientes fases del pentesting, especialmente el análisis de vulnerabilidades.

OpenVas**:** Permite realizar análisis automatizados para identificar vulnerabilidades y apoyar la gestión de riesgos de seguridad en infraestructuras tecnológicas (Ávila Pardo & Ramírez Restrepo, s. f.). Forma parte de un conjunto de servicios orientados al análisis de seguridad, permitiendo a los profesionales detectar fallas en redes, servidores y aplicaciones de manera automatizada.

Funciona mediante el escaneo de los sistemas objetivo, analizando configuraciones, servicios y posibles debilidades. Posteriormente, genera reportes detallados donde se clasifican las vulnerabilidades encontradas según su nivel de riesgo, facilitando así la priorización de acciones correctivas.

Una de sus principales ventajas es que es un software libre bajo licencia GNU GPL, lo que permite su uso sin costo y su adaptación según las necesidades de cada organización. Además, su constante actualización garantiza que pueda detectar nuevas amenazas y vulnerabilidades emergentes.

ExploitDB**:** Es una plataforma en línea que funciona como una base de datos pública de exploits asociados a vulnerabilidades conocidas. Esta herramienta es ampliamente utilizada en el ámbito de la ciberseguridad, ya que permite a los profesionales consultar, descargar y analizar código que ha sido desarrollado para explotar fallas específicas en sistemas informáticos.

Una de sus principales características es que se alimenta de aportes de la comunidad, lo que permite mantener una base de datos actualizada y en constante crecimiento. Constituye una de las bases de datos públicas más utilizadas para la consulta de vulnerabilidades y código de explotación asociado (Palomo et al., 2024).

CVE**:** Es un sistema de identificación estándar utilizado a nivel mundial para clasificar y registrar vulnerabilidades de seguridad conocidas. Cada vulnerabilidad recibe un código único, lo que permite la identificación estandarizada de vulnerabilidades conocidas a nivel internacional (NIST, 2008).

Las vulnerabilidades asociadas a códigos CVE suelen estar relacionadas con fallas en software, hardware o configuraciones de sistemas, las cuales pueden afectar aspectos críticos como la confidencialidad, integridad y disponibilidad de la información. Estas vulnerabilidades son documentadas y publicadas, permitiendo que sean conocidas y analizadas a nivel global.

Configuración del entorno de laboratorio

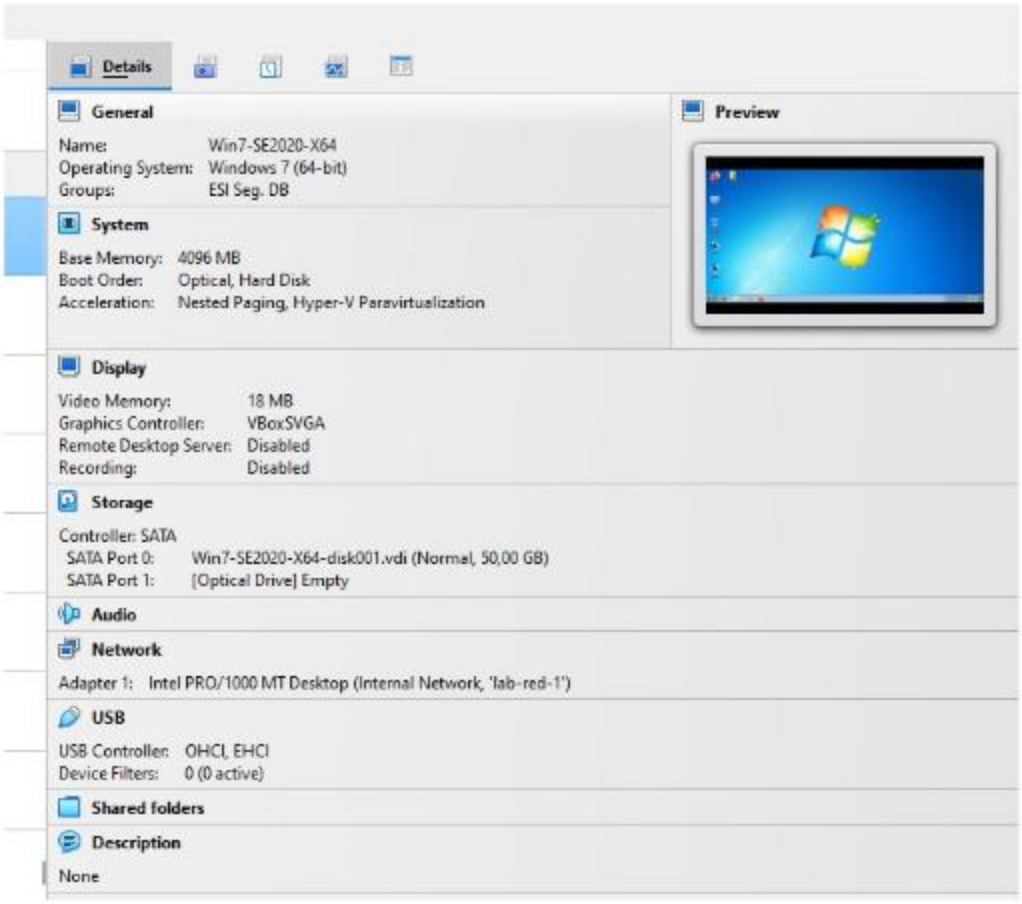
Para el desarrollo del laboratorio se emplearon sistemas diseñados específicamente para la práctica de pruebas de penetración en entornos controlados. Este tipo de plataformas contienen vulnerabilidades conocidas que permiten reproducir escenarios reales de explotación y análisis de seguridad de forma segura (Rapid7, 2012).

1. Banco de Trabajo

se realizó la instalación de la herramienta de virtualización VirtualBox en su versión más reciente

Figura 1

Configuración de la máquina virtual Windows 7



Fuente. Autoría propia

Nota. La figura muestra las características de hardware asignadas a la máquina virtual Windows 7 utilizada como objetivo de las pruebas de penetración.

Una vez importadas las máquinas virtuales, se procedió a revisar y ajustar sus características técnicas con el fin de garantizar un entorno adecuado para la ejecución del laboratorio.

En este sentido, la máquina correspondiente a Windows 7 cuenta con un sistema operativo de 64 bits, 4096 MB de memoria RAM, 1 CPU, almacenamiento en disco VDI de 50 GB, controlador gráfico VBoxSVGA, memoria de video de 18 MB y controlador de audio Intel HD Audio, mientras que la máquina de pruebas basada en Parrot OS Security Edition (Debian

12) dispone de 8192 MB de memoria RAM, 8 CPU, disco VDI de 64 GB, controlador gráfico VMSVGA y 128 MB de memoria de video, además de contar con aceleración mediante tecnologías como Nested VT-x/AMD-V y paravirtualización KVM.

se realizó la verificación de la conectividad de red. En primer lugar, se identificaron las direcciones IP asignadas automáticamente mediante el uso del comando ipconfig en el sistema Windows.

Ética Profesional y Cumplimiento Normativo en Ciberseguridad

Análisis ético y legal del caso SecureNova Labs

Desde el enfoque de la ética informática, el manejo de la información debe regirse por principios fundamentales como la privacidad, la seguridad, la transparencia y la responsabilidad, los cuales establecen que los datos deben ser utilizados únicamente con fines legítimos y autorizados, garantizando siempre la protección de los derechos de los individuos. El ejercicio profesional de la ingeniería debe estar sustentado en principios de responsabilidad, honestidad y compromiso social, garantizando que las decisiones técnicas no generen afectaciones a terceros (Bilbao et al., 2006).

Durante el análisis realizado se identificaron cláusulas contractuales que pueden afectar principios relacionados con la transparencia, la responsabilidad profesional y el cumplimiento normativo. En particular, se observó una disposición que prohíbe la divulgación de información confidencial o relacionada con actividades ilegales dentro de la organización. Aunque la protección de la información sensible constituye una práctica legítima, esta restricción podría interpretarse como una limitación al deber de informar o denunciar hechos ilícitos, generando posibles implicaciones éticas y legales para los profesionales involucrados.

En la definición de información confidencial, se incluyen prácticas como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”, lo cual evidencia que dentro del acuerdo se contemplan actividades que pueden constituir delitos informáticos.

De igual forma, en las obligaciones de la parte receptora se indica explícitamente que se debe “no denunciar ante las autoridades actividades sospechosas de espionaje” y “abstenerse de denunciar y publicar la información confidencial e ilegal”, lo cual constituye una grave vulneración del principio de responsabilidad profesional.

Estas disposiciones son contrarias a la ética, ya que un profesional en ciberseguridad tiene el deber de actuar con integridad y reportar cualquier conducta que pueda generar daño o que implique actividades ilícitas. Además, se vulnera el principio de seguridad de la información, dado que se promueve el uso indebido de datos y el acceso no autorizado a sistemas, afectando la confidencialidad, integridad y disponibilidad de la información.

Se puede concluir que el acuerdo presenta múltiples irregularidades, tanto desde el punto de vista legal como ético, ya que no solo permite, sino que también encubre prácticas ilegales como el espionaje y el acceso indebido a sistemas, además de limitar la posibilidad de denuncia, lo cual es incompatible con el ejercicio responsable y ético de la ciberseguridad.

Vulneración de la Ley 1273 de 2009

Artículo 269A Acceso abusivo a un sistema informático: lo cual implica el ingreso sin autorización a plataformas o sistemas. Esta conducta vulnera el principio de confidencialidad, ya que permite que personas no autorizadas accedan a información sensible. En el acuerdo se hace referencia explícita a “accesos abusivos a sistemas informáticos”, lo cual evidencia la posible realización de este tipo de prácticas, constituyéndose en una conducta sancionada por la Ley 1273 de 2009 (Congreso de Colombia, 2009).

Artículo 269C Interceptación de datos informáticos: lo cual constituye una conducta ilegal cuando se realiza sin autorización. Esta práctica afecta tanto la confidencialidad como la integridad, ya que los datos pueden ser capturados o alterados durante su transmisión. En el acuerdo se mencionan actividades como la “interceptación de información”, lo cual representa una vulneración directa a este artículo, al tratarse de una acción que compromete la seguridad de los datos.

Artículo 269F Violación de datos personales: el uso y manejo de información sensible sin el consentimiento del titular, como se sugiere en el acuerdo, puede constituir una violación de datos personales. Esto afecta directamente los derechos fundamentales de los individuos y el principio de protección de la información.

La protección de los datos personales constituye un derecho fundamental que exige mecanismos adecuados para garantizar el control de la información por parte de los titulares (Hernández et al., 2021). Además, al tratarse de información confidencial obtenida en contextos no autorizados, se evidencia un riesgo claro de uso indebido de datos personales.

Evaluación profesional de la propuesta laboral

Desde una perspectiva profesional, ética y legal, no aplicaría a la oferta laboral planteada por SecureNova Labs, a pesar de las condiciones económicas atractivas, como el salario ofrecido y la estabilidad laboral.

Esta decisión se fundamenta en que se evidencia la posible ejecución de actividades ilegales, tales como el acceso no autorizado a sistemas, la interceptación de información y la restricción para denunciar dichas conductas. Estas prácticas no solo vulneran la Ley 1273 de 2009, sino que también contravienen los principios fundamentales del ejercicio ético de la ingeniería.

De acuerdo con el Código de Ética Profesional establecido, los profesionales tienen el deber de actuar con responsabilidad, integridad y respeto por la ley. En particular, se establece como deber general “denunciar los delitos, contravenciones y faltas de que tenga conocimiento en el ejercicio de su profesión”, lo cual entra en contradicción directa con las cláusulas del acuerdo que prohíben reportar actividades ilegales.

El código establece la obligación de custodiar y proteger la información a la que se tenga acceso, evitando su uso indebido, lo cual se ve vulnerado en el acuerdo al promover prácticas como la interceptación de datos y el acceso no autorizado a sistemas, dentro de las prohibiciones establecidas, se indica que los profesionales no deben aceptar trabajos que vayan en contra de las disposiciones legales vigentes, lo cual refuerza la idea de que participar en una organización con este tipo de prácticas constituye una falta ética grave. Desde el enfoque de la ética profesional, se reconoce que la ingeniería es una disciplina orientada al servicio de la sociedad, cuyo ejercicio debe estar guiado por valores como la honestidad, la responsabilidad y el compromiso con el bien común. En este sentido, la conducta del profesional no debe estar determinada únicamente por beneficios económicos, sino por principios morales que garanticen un ejercicio digno y responsable de la profesión.

Aceptar una oferta laboral en estas condiciones implicaría participar directa o indirectamente en actividades que pueden generar daño a terceros, afectar derechos fundamentales y comprometer la integridad profesional. Además, podría acarrear sanciones disciplinarias, como la suspensión o incluso la cancelación de la matrícula profesional, de acuerdo con lo establecido en el Código de Ética.

Gestión de información sensible durante auditorías de seguridad

El acceso a información sensible por parte de empresas de ciberseguridad durante una auditoría debe estar estrictamente limitado a lo necesario para cumplir con los objetivos del

servicio contratado. El acceso debe regirse por el principio de mínimo privilegio, garantizando que solo se consulte la información indispensable para identificar vulnerabilidades y fortalecer la seguridad del sistema.

Desde el punto de vista legal y ético, el acceso a datos sensibles debe estar respaldado por el consentimiento explícito del cliente, acuerdos de confidencialidad claros y el cumplimiento de normativas de protección de datos. Esto se debe a que la información tratada durante una auditoría puede incluir datos personales, financieros o estratégicos, cuya exposición o uso indebido puede generar graves consecuencias para las organizaciones y los individuos. La protección de los datos personales se ha convertido en un desafío crítico en la era digital, debido al incremento del uso de tecnologías y la creciente exposición a ciberamenazas, lo que exige mayores controles en el manejo de la información.

El derecho a la privacidad implica que los individuos deben tener control sobre su información personal, lo cual obliga a las empresas de ciberseguridad a actuar con responsabilidad, garantizando que los datos no sean utilizados para fines distintos a los autorizados.

Para evitar el uso indebido de la información, es fundamental implementar controles como:

- Políticas estrictas de acceso y manejo de la información
- Acuerdos de confidencialidad (NDA)
- Registro y monitoreo de actividades realizadas durante la auditoría
- Segmentación de la información sensible
- Auditorías internas y controles de cumplimiento

Controles para el uso adecuado de herramientas forenses

En empresas de ciberseguridad, donde se manejan herramientas altamente especializadas y con gran capacidad de acceso a sistemas e información sensible, resulta imprescindible establecer mecanismos de control que no solo sean técnicos, sino también organizacionales y éticos. Esto se debe a que el riesgo no proviene únicamente de amenazas externas, sino también del uso indebido por parte de personal interno con acceso legítimo.

Tabla 1

Controles de herramientas forenses en organizaciones de ciberseguridad

Control	Descripción
Gestión de accesos basada en roles	Consiste en asignar permisos de acuerdo con las funciones y responsabilidades de cada usuario, limitando el acceso únicamente a los recursos necesarios para el desarrollo de sus actividades y reduciendo el riesgo de uso indebido de herramientas especializadas.
Autenticación y control de acceso	Comprende la implementación de mecanismos de autenticación robustos que permitan validar la identidad de los usuarios y restringir el acceso a sistemas y herramientas sensibles únicamente a personal autorizado.

Monitoreo continuo de actividades	Permite registrar y supervisar las acciones realizadas por los usuarios dentro de los sistemas, facilitando la detección de comportamientos inusuales, accesos no autorizados o posibles usos indebidos de herramientas forenses.
Sistema de control interno	Corresponde al conjunto de políticas, procedimientos y mecanismos de supervisión establecidos por la organización para regular el uso adecuado de los recursos tecnológicos y gestionar los riesgos asociados a la seguridad de la información.
Auditorías periódicas	Consisten en evaluaciones internas o externas orientadas a verificar el cumplimiento de las políticas de seguridad, identificar debilidades en los controles implementados y promover acciones de mejora continua.
Indicadores y seguimiento	Incluyen métricas y mecanismos de evaluación que permiten medir la efectividad de los controles de seguridad implementados y realizar seguimiento a su desempeño dentro de la organización.

Capacitación y concientización	Comprende actividades de formación orientadas a fortalecer las competencias del personal en materia de seguridad informática, uso responsable de herramientas especializadas y cumplimiento de las políticas organizacionales.

Nota. La tabla describe los mecanismos de control recomendados para garantizar el uso seguro y supervisado de herramientas forenses, reduciendo los riesgos asociados al acceso y manejo de información sensible.

Gestión organizacional frente a incidentes de ciberespionaje

Cuando una organización o un gobierno identifica que una empresa de ciberseguridad ha incurrido en prácticas de ciberespionaje, la respuesta debe orientarse no solo a la sanción del hecho, sino también a la contención del riesgo, la protección de la información y la reconstrucción de la confianza institucional.

La gestión efectiva de incidentes requiere la existencia de procedimientos formales de detección, análisis, contención, erradicación y recuperación, coordinados por equipos especializados de respuesta a incidentes (CSIRT). Estos equipos permiten reducir el impacto operativo y facilitar la toma de decisiones durante eventos de seguridad que comprometen la información o la infraestructura tecnológica (Chuquiguanca Vicente, 2020).

- Investigación forense digital y recolección de evidencias: se debe iniciar un proceso de investigación apoyado en la ciencia forense digital, con el fin de recopilar, preservar y analizar evidencia que permita esclarecer los hechos. Este proceso garantiza la integridad

y validez de la información recolectada, lo cual es fundamental para su uso en procesos legales.

- Aplicación de estándares en manejo de evidencia: es importante seguir lineamientos internacionales como los establecidos en normas ISO, que orientan procesos como la identificación, recolección, adquisición y preservación de evidencia digital, asegurando la confiabilidad y trazabilidad de la información.
- Activación de un plan de respuesta a incidentes: las organizaciones deben aplicar un enfoque estructurado para la gestión del incidente, contemplando fases como: preparación, detección, contención, erradicación y recuperación. Este proceso permite mitigar el impacto del ataque y restablecer el funcionamiento normal de los sistemas.
- Notificación a autoridades y acciones legales: dado que el ciberespionaje puede constituir un delito, es obligatorio informar a las autoridades competentes, iniciar procesos legales contra los responsables y aplicar las sanciones correspondientes.
- Evaluación del impacto y protección de infraestructuras: Se debe analizar el alcance del incidente, especialmente si afecta infraestructuras críticas, ya que estas son fundamentales para el funcionamiento de los Estados y pueden comprometer la seguridad nacional y la economía
- Fortalecimiento de controles y prevención: posterior al incidente, es necesario reforzar los mecanismos de seguridad, incluyendo controles de acceso, monitoreo, auditorías y gestión de proveedores, con el fin de evitar que situaciones similares se repitan.
- Transparencia y comunicación: las organizaciones deben informar de manera clara y oportuna a las partes interesadas sobre lo ocurrido, las medidas adoptadas y las acciones correctivas, lo cual es clave para recuperar la confianza.

Ejercicio Práctico de Red Team

Reconocimiento y enumeración de servicios

Las actividades de reconocimiento constituyen una de las fases más importantes dentro del proceso de pentesting, ya que permiten identificar servicios expuestos, versiones de software y posibles vectores de ataque que posteriormente pueden ser analizados y validados mediante técnicas de explotación controlada (García Montes, 2025).

Se realizó un proceso de reconocimiento utilizando la herramienta Nmap, con el objetivo de identificar los puertos abiertos y los servicios activos en la máquina objetivo (Host-A), correspondiente a un sistema Windows.

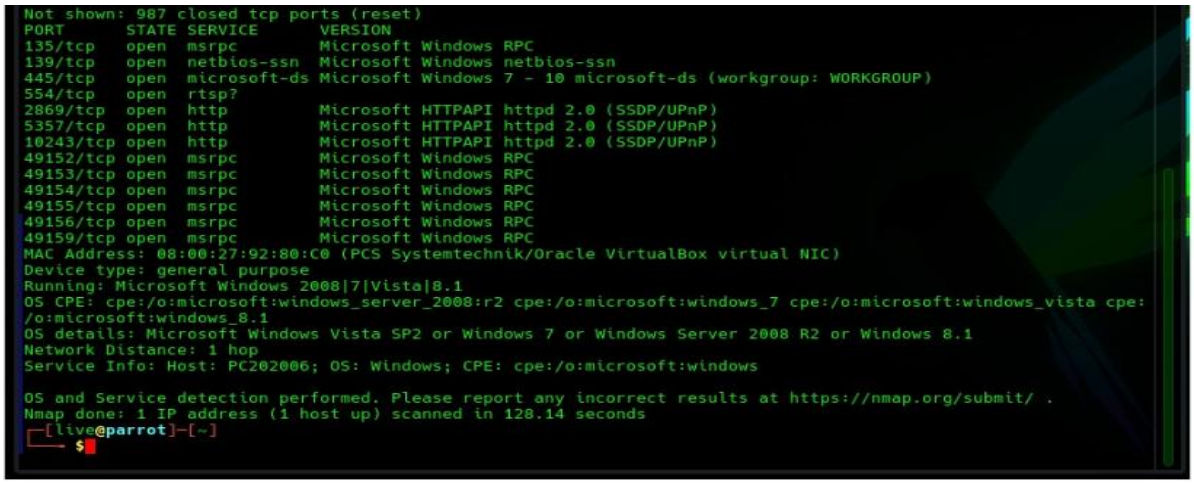
Para ello, se ejecutó el siguiente comando:

sudo nmap -sS -sV -O 192.168.56.10

Este comando permitió realizar un escaneo de puertos, identificar versiones de servicios y detectar el sistema operativo del host analizado.

Figura 2

Resultado del escaneo de puertos mediante Nmap



Fuente. Autoría propia

Nota. La figura presenta los resultados obtenidos durante la fase de reconocimiento, identificando puertos abiertos, servicios activos y características del sistema operativo de la máquina objetivo.

Del análisis del escaneo se identificaron varios puertos abiertos, entre los que destacan:

- Puerto 445 (SMB)
- Puerto 139 (NetBIOS)
- Servicios MSRPC activos

Estos servicios están asociados a sistemas Windows y pueden representar vulnerabilidades críticas si no se encuentran debidamente actualizados.

En particular, el puerto 445 indica la presencia del protocolo SMB, el cual ha sido históricamente vulnerable a ataques como **MS17-010 (EternalBlue)**, lo que podría permitir la ejecución remota de código y el acceso no autorizado al sistema.

Identificación de vulnerabilidades

Con base en los resultados obtenidos en el escaneo, se identificó que la máquina objetivo presenta el puerto 445 abierto, asociado al protocolo SMB (Barrios González, 2024).

Este servicio es conocido por presentar vulnerabilidades críticas en sistemas Windows desactualizados, especialmente la vulnerabilidad MS17-010, también conocida como EternalBlue, la cual permite la ejecución remota de código sin autenticación previa.

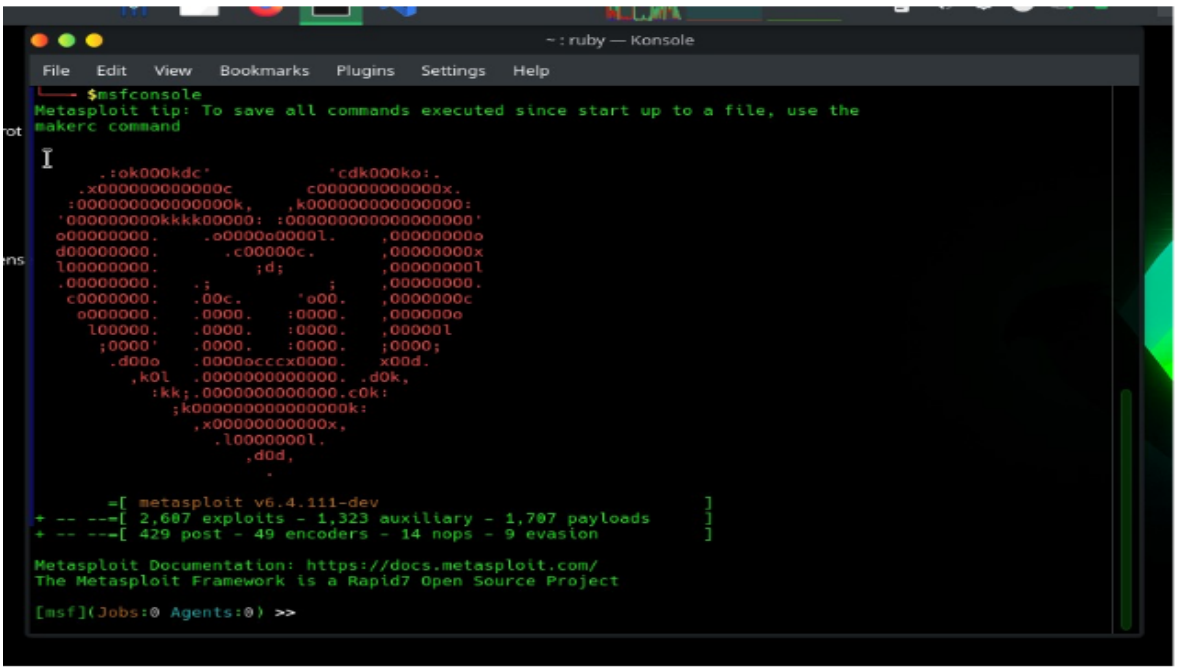
Explotación de vulnerabilidades

En esta fase se intentó explotar la vulnerabilidad del servicio SMB utilizando el exploit MS17-010 (EternalBlue) mediante la herramienta Metasploit.

Aunque se logró establecer comunicación con el sistema objetivo, no fue posible obtener una sesión activa, presentándose el mensaje “Exploit completed, but no session was created”, lo cual evidencia la inestabilidad del exploit en este entorno.

Figura 3

Reinicio de Metasploit Framework

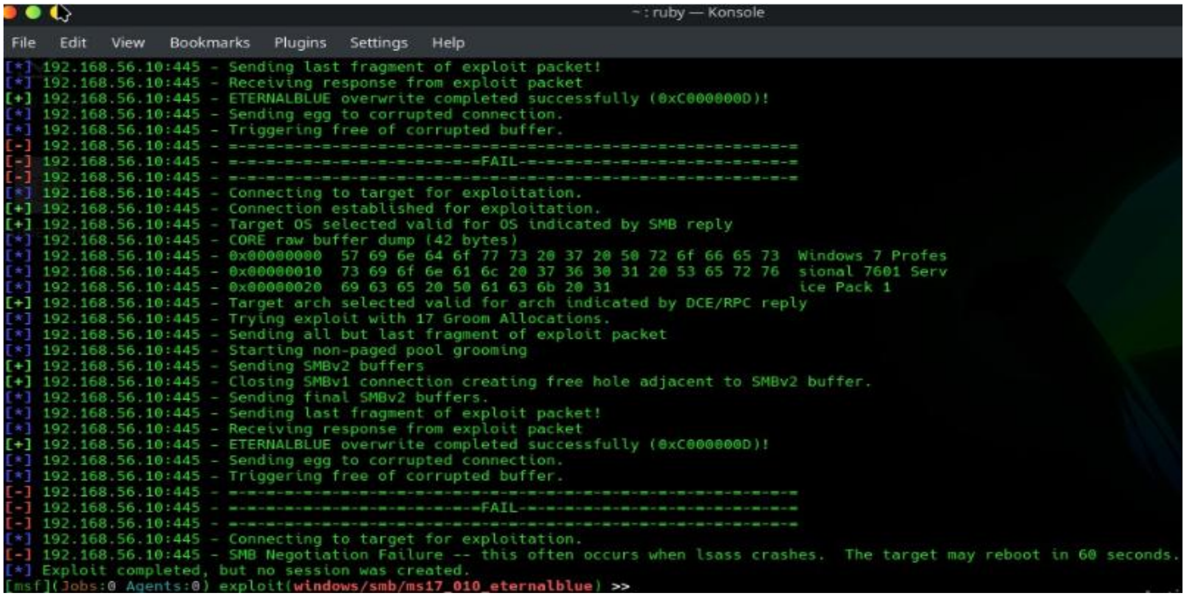


Fuente. Autoría propia

Nota. La figura muestra la ejecución de Metasploit Framework, herramienta utilizada para validar y explotar vulnerabilidades identificadas durante el ejercicio Red Team.

Figura 4

Carga del exploit MS17-010 EternalBlue



Fuente. Autoría propia

Nota. La figura presenta la selección del módulo exploit/windows/smb/ms17_010_eternalblue para la validación de la vulnerabilidad SMB en la máquina objetivo

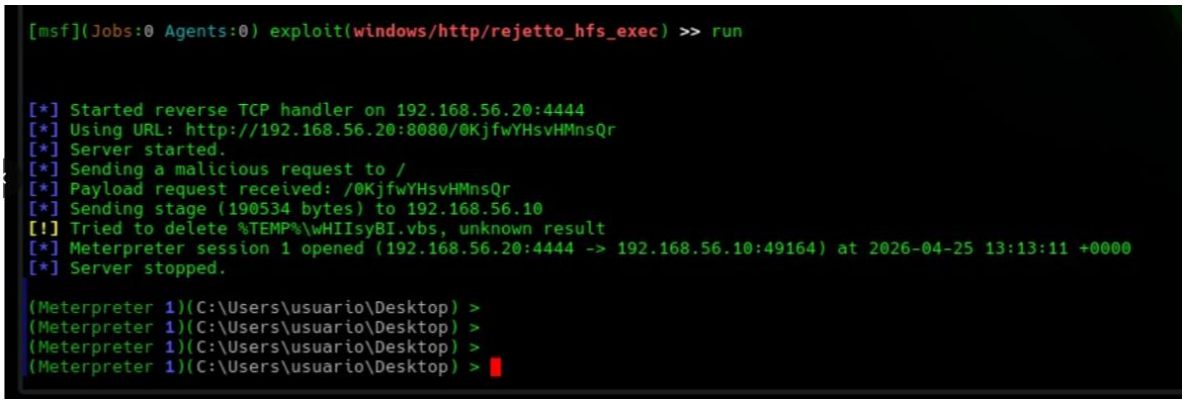
Explotación exitosa mediante Rejetto HFS

Posteriormente, se procedió a utilizar el exploit asociado al servicio HTTP (Rejetto HFS), el cual presenta una vulnerabilidad de ejecución remota de comandos.

Se configuraron los parámetros necesarios en Metasploit, logrando ejecutar el ataque y establecer una sesión Meterpreter.

Figura 5

Obtención de sesión Meterpreter mediante la explotación de Rejetto HFS



Fuente. Autoría propia

Nota. La figura muestra la ejecución exitosa del módulo exploit/windows/http/rejetto_hfs_exec en Metasploit Framework. Como resultado de la explotación del servicio vulnerable Rejetto HFS, se obtuvo una sesión Meterpreter sobre la máquina objetivo Windows 7, permitiendo la interacción remota con el sistema comprometido y la ejecución de actividades de post-explotación.

Actividades de post-explotación

Una vez obtenida la sesión Meterpreter, se realizaron acciones de post-explotación con el fin de validar el acceso y recopilar información del sistema comprometido

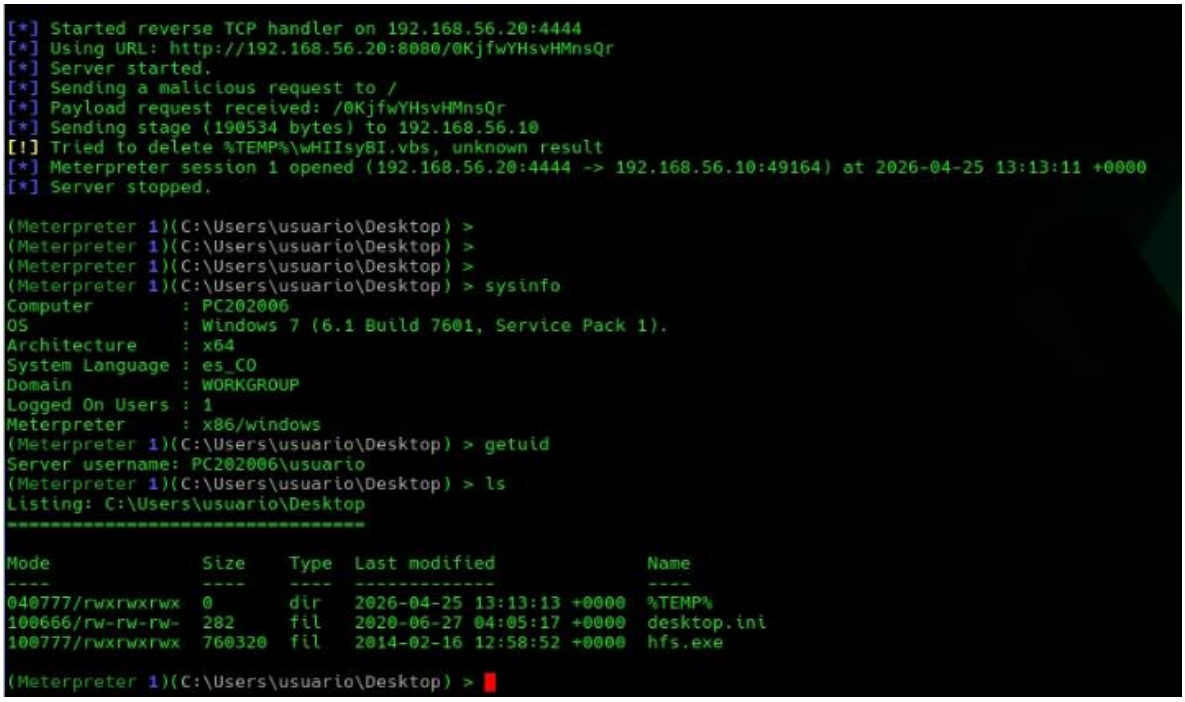
Se ejecutó el comando “sysinfo” para obtener información del sistema operativo, arquitectura y características del equipo comprometido.

Mediante el comando “getuid” se identificó el usuario bajo el cual se encuentra ejecutándose la sesión comprometida.

Se utilizó el comando “ls” para listar los archivos y directorios del sistema, evidenciando acceso a la estructura del sistema de archivos.

Figura 6

Ejecución de actividades de post-explotación mediante Meterpreter

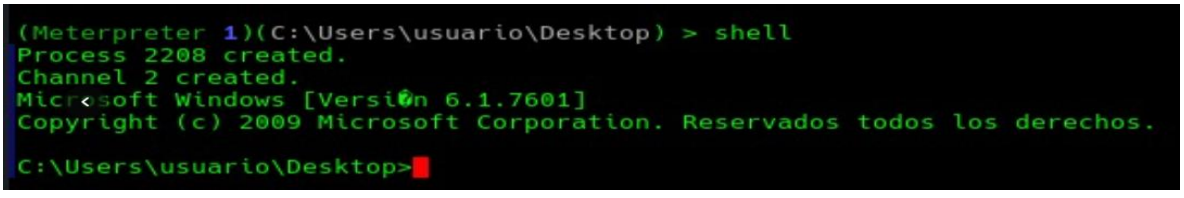


Fuente. Autoría propia

Nota. La figura muestra la ejecución de comandos de post-explotación sobre la máquina comprometida utilizando una sesión Meterpreter. Mediante los comandos sysinfo, getuid y ls fue posible obtener información del sistema operativo, identificar el usuario comprometido y visualizar el contenido del directorio de trabajo, validando el acceso remoto al equipo objetivo y la capacidad de interacción con sus recursos

Figura 7

Obtención de una consola interactiva del sistema operativo Windows



Fuente. Autoría propia

Nota. La figura muestra la ejecución del comando shell desde una sesión Meterpreter, permitiendo acceder a una consola interactiva del sistema operativo Windows comprometido.

Estas acciones evidencian que el atacante logró no solo acceder al sistema, sino también interactuar con él, obteniendo información sensible y ejecutando comandos de manera remota.

Movimiento lateral (Pivoting)

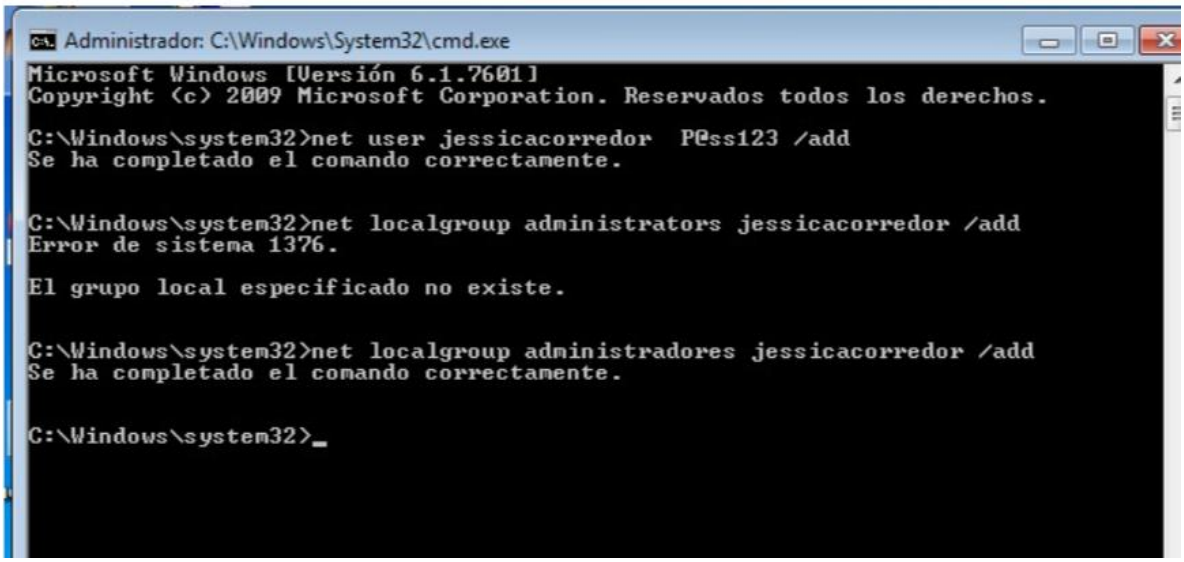
Como parte de las actividades de validación posteriores a la explotación, se desarrolló un escenario controlado de movimiento lateral (pivoting) hacia una segunda máquina del entorno de laboratorio (Host-B). Para ello, se creó una cuenta de usuario con privilegios administrativos siguiendo el esquema de nomenclatura establecido de primerNombre+primerApellido.

Esta actividad permitió demostrar el impacto que puede generar el compromiso inicial de un sistema vulnerable, evidenciando cómo un atacante podría aprovechar el acceso obtenido para expandir su alcance dentro de la red y comprometer otros activos tecnológicos de la organización.

Una vez finalizada la prueba y documentados los resultados obtenidos, se procedió a eliminar la cuenta creada con el propósito de restablecer el estado original del entorno de laboratorio, garantizando el carácter temporal de la actividad y evitando modificaciones permanentes sobre los sistemas evaluados.

Figura 8

Creación de un usuario con privilegios administrativos en el sistema comprometido

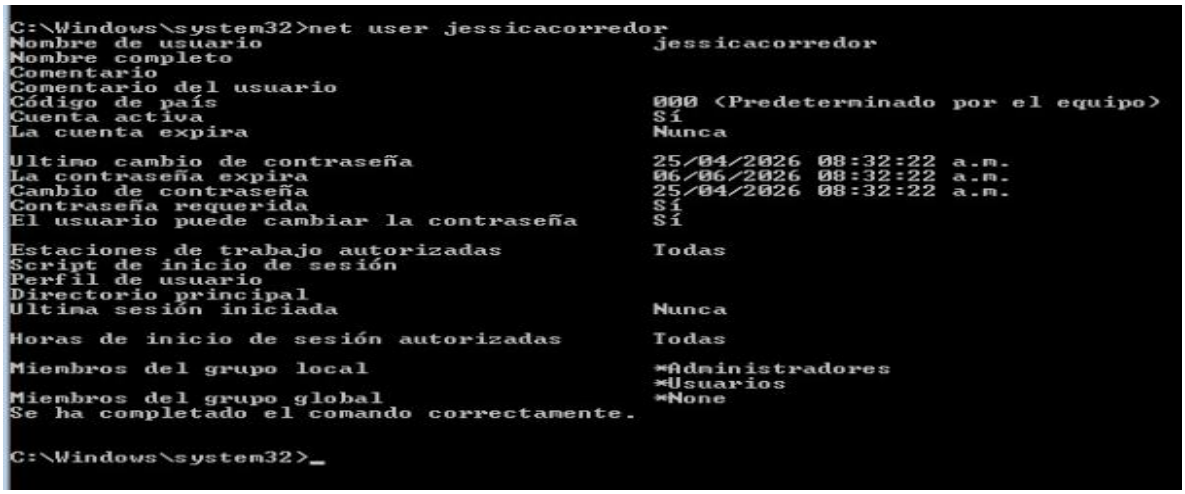


Fuente. Autoría propia

Nota. La figura muestra la creación de un nuevo usuario local mediante el comando net user y su posterior incorporación al grupo de administradores utilizando net localgroup administradores.

Figura 9

Verificación de privilegios del usuario creado durante la post-explotación



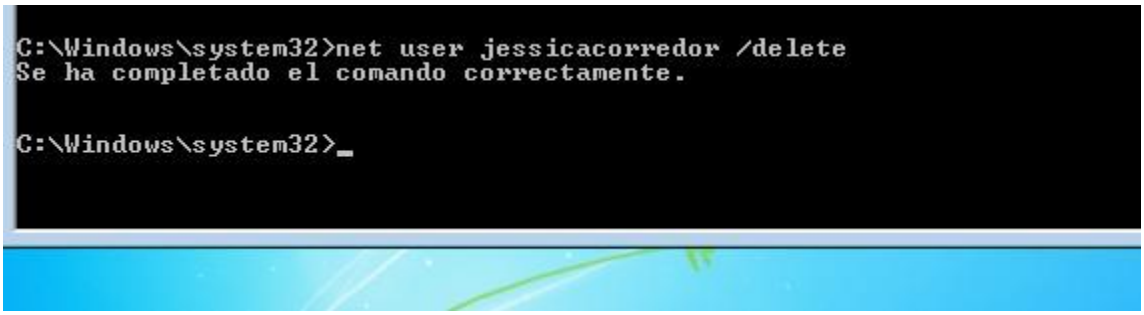
Fuente. Autoría propia

Nota. La figura presenta la validación de la cuenta de usuario creada durante la fase de post-explotación mediante el comando net user. Los resultados evidencian que el usuario fue creado

correctamente y que pertenece al grupo local de administradores, confirmando la asignación exitosa de privilegios elevados sobre el sistema comprometido.

Figura 10

Eliminación del usuario creado durante la fase de post-explotación



Fuente. Autoría propia

Nota. La figura muestra la eliminación del usuario local creado durante las actividades de post-explotación mediante el comando net user [usuario] /delete. Esta acción fue realizada con el fin de restaurar el estado original del sistema y garantizar que no permanecieran cuentas adicionales o configuraciones modificadas después de finalizar las pruebas de seguridad en el entorno controlado de laboratorio.

Análisis de resultados del ejercicio Red Team

En el contexto actual, caracterizado por una creciente digitalización de los procesos organizacionales, la seguridad informática se consolida como un componente esencial para la protección de los activos de información. Los sistemas, redes y aplicaciones se encuentran expuestos de manera permanente a múltiples amenazas, lo que exige la implementación de estrategias orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información.

A partir del análisis del escenario planteado, se logró identificar una vulnerabilidad crítica en la máquina objetivo (Host-A), asociada a un servicio web expuesto mediante la herramienta Rejetto HFS. Este tipo de servicios, cuando no cuentan con configuraciones seguras o actualizaciones adecuadas, pueden presentar fallos que permiten la ejecución remota de comandos, facilitando el acceso no autorizado al sistema.

Desde el enfoque de la gestión de riesgos, una vulnerabilidad corresponde a una debilidad presente en un sistema que puede ser aprovechada por una amenaza para comprometer un activo de información. En este caso, la exposición del servicio HTTP vulnerable permitió que, mediante el uso de herramientas especializadas como Metasploit Framework, se validara la existencia de dicha debilidad, logrando su explotación y el acceso al sistema objetivo.

La obtención de una sesión Meterpreter evidenció el nivel de compromiso alcanzado, permitiendo la ejecución de comandos, la exploración de la estructura del sistema y el control remoto del equipo. Este resultado pone de manifiesto el impacto que puede generar la ausencia de controles de seguridad adecuados, tales como la actualización de servicios, la restricción de accesos y la correcta configuración de los sistemas.

El ejercicio permitió analizar la relevancia del movimiento lateral o pivoting dentro de un ataque de tipo Red Team. Una vez comprometido el sistema inicial, el atacante puede extender su alcance hacia otros dispositivos dentro de la red, incrementando el impacto del incidente. Esto se evidenció mediante la creación de una cuenta con privilegios administrativos en una segunda máquina (Host-B), demostrando la posibilidad de escalar privilegios y ampliar el control dentro del entorno.

Desde una perspectiva integral, la seguridad de la información requiere la adopción de un enfoque continuo que contemple la planificación, el análisis, la implementación y el monitoreo

de controles de seguridad, con el fin de adaptarse a las amenazas emergentes y reducir los riesgos asociados.

Análisis del ataque presentado a cada una de las maquinas identificadas

El análisis del ataque desarrollado en el escenario propuesto permite comprender cómo la explotación de vulnerabilidades puede afectar de manera significativa la seguridad de los sistemas dentro de una red. En este contexto, se identificaron dos máquinas principales: Host-A, como punto inicial de compromiso, y Host-B, como sistema secundario dentro del entorno.

Desde una perspectiva de ciberseguridad, la protección de los sistemas de información se orienta a prevenir accesos no autorizados, daños o usos indebidos de los recursos tecnológicos, considerando tanto factores técnicos como humanos. Sin embargo, cuando existen debilidades en la configuración o en la actualización de los servicios, estos pueden ser aprovechados por un atacante para comprometer el sistema.

En el caso de la máquina Host-A, el ataque inició con la identificación de servicios expuestos mediante técnicas de escaneo, evidenciando la presencia de múltiples puertos abiertos asociados a servicios de Windows. Este tipo de exposición incrementa la superficie de ataque, ya que cada servicio activo representa un posible punto de entrada para un atacante. A través del uso de herramientas de pentesting, se logró identificar una vulnerabilidad en el servicio HTTP, la cual permitía la ejecución remota de comandos.

La explotación de esta vulnerabilidad permitió establecer una sesión remota sobre el sistema, evidenciando la pérdida de control sobre el equipo comprometido. Este tipo de ataques afecta directamente los principios fundamentales de la seguridad de la información, particularmente la confidencialidad, al permitir el acceso no autorizado a los datos; la integridad, al posibilitar la modificación de la información; y la disponibilidad, al poner en riesgo el funcionamiento normal del sistema.

Posteriormente, el análisis del ataque permitió evidenciar una fase de movimiento lateral o pivoting hacia la máquina Host-B. Este proceso representa una etapa avanzada dentro de un ataque, en la cual el atacante, una vez comprometido un sistema, busca expandir su alcance dentro de la red. En este caso, la creación de una cuenta con privilegios administrativos en la segunda máquina demuestra la capacidad de escalar privilegios y mantener persistencia en el entorno.

Este tipo de comportamiento es característico de ataques dirigidos, en los cuales el objetivo no es únicamente comprometer un sistema, sino extender el control a múltiples dispositivos dentro de la infraestructura. La ausencia de controles de seguridad adecuados, como la segmentación de red, el monitoreo continuo o la gestión de accesos, facilita este tipo de escenarios.

De acuerdo con las prácticas de pruebas de penetración, este tipo de ejercicios permite simular ataques reales de manera controlada, con el fin de identificar vulnerabilidades antes de que sean explotadas por actores maliciosos. En este sentido, el caso analizado evidencia la importancia de implementar mecanismos de defensa robustos que permitan detectar, prevenir y responder ante posibles incidentes de seguridad.

Validación de vulnerabilidades identificadas

El proceso de validación de vulnerabilidades sobre la máquina Windows inició con la ejecución de un escaneo de red mediante la herramienta Nmap, cuyo propósito fue identificar los puertos abiertos y los servicios expuestos en el sistema objetivo. Como resultado de esta actividad se detectaron diversos servicios asociados a los protocolos SMB y HTTP, los cuales fueron considerados como posibles vectores de ataque debido a su exposición dentro de la infraestructura analizada. Esta información constituyó el punto de partida para las actividades posteriores de evaluación y explotación.

Una vez identificados los servicios disponibles, se procedió a analizar las posibles vulnerabilidades asociadas a cada uno de ellos mediante el uso de Metasploit Framework. Inicialmente, la evaluación se centró en el servicio SMB, considerando la existencia de vulnerabilidades ampliamente documentadas para este protocolo en sistemas Windows. Para ello, se realizó la búsqueda de módulos de explotación relacionados, seguida de la configuración y ejecución de los exploits correspondientes con el fin de verificar la exposición real del sistema frente a este tipo de amenazas.

Aunque las pruebas realizadas sobre el servicio SMB permitieron validar información relevante sobre el objetivo, los intentos de explotación no produjeron resultados satisfactorios. En consecuencia, el análisis se redireccionó hacia el servicio HTTP identificado previamente durante la fase de reconocimiento. Esta decisión permitió ampliar la superficie de evaluación y explorar otros posibles puntos de compromiso presentes en la máquina analizada.

Como resultado de esta nueva línea de análisis, se identificó la presencia de la aplicación Rejetto HTTP File Server (HFS), la cual presentaba una vulnerabilidad susceptible de explotación. A partir de este hallazgo se localizó el módulo correspondiente dentro de Metasploit Framework y se configuraron los parámetros requeridos para su ejecución, incluyendo las direcciones IP del atacante y del sistema objetivo. Posteriormente, se ejecutó el exploit, logrando establecer exitosamente una sesión Meterpreter que confirmó el compromiso del sistema y la obtención de acceso remoto.

Una vez alcanzado el acceso inicial, se desarrollaron actividades de post-explotación orientadas a determinar el nivel de control obtenido sobre el equipo comprometido. En esta etapa se utilizaron comandos como *sysinfo*, *getuid* y *ls*, los cuales permitieron recopilar información sobre el sistema operativo, identificar el contexto de ejecución de la sesión y examinar la estructura de directorios disponible. De igual forma, mediante el comando *shell* se

accedió a la consola nativa de Windows, validando la capacidad de interacción directa con el sistema y ampliando las posibilidades de ejecución de acciones posteriores.

El acceso obtenido durante la fase de post-explotación permitió evaluar escenarios adicionales asociados al impacto de un compromiso exitoso. Por esta razón, se llevó a cabo una prueba controlada de movimiento lateral (*pivoting*) hacia una segunda máquina del entorno de laboratorio, con el propósito de evidenciar cómo un atacante podría extender su alcance dentro de una red corporativa una vez comprometido un activo inicial.

Para materializar esta prueba, se creó una cuenta de usuario con privilegios administrativos en el sistema objetivo secundario, verificando posteriormente su correcta asignación dentro de los grupos de administración del equipo. Una vez documentados los resultados obtenidos, la cuenta fue eliminada con el fin de restablecer el estado original del entorno y garantizar el carácter controlado y temporal de la actividad. Este ejercicio permitió demostrar de manera práctica cómo un atacante podría utilizar el acceso obtenido para escalar privilegios, desplazarse lateralmente y comprometer otros activos críticos dentro de una infraestructura tecnológica.

Estrategias de Defensa y Respuesta Blue Team

Acciones de contención ante incidentes de seguridad

Para ello, es necesario realizar un proceso inicial de análisis y contextualización que permita establecer qué sistemas, servicios, aplicaciones o usuarios podrían estar involucrados dentro del evento de seguridad. Esta etapa resulta fundamental, ya que permite definir las prioridades de atención, orientar la toma de decisiones y determinar el nivel de criticidad del incidente dentro de la infraestructura tecnológica.

Como parte de este análisis inicial, se deben revisar registros de eventos, conexiones activas, tráfico de red, procesos sospechosos, accesos no autorizados y cualquier comportamiento anómalo que permita identificar indicadores de compromiso (IOC). Los indicadores de compromiso permiten identificar actividades maliciosas mediante el análisis de eventos y comportamientos anómalos en los sistemas (Suárez Restrepo, 2021). Del mismo modo, resulta importante verificar si existen servicios vulnerables expuestos, movimientos laterales dentro de la red o intentos de escalamiento de privilegios que puedan comprometer otros sistemas de información. La identificación temprana de estos elementos permite determinar si el ataque continúa activo y facilita la implementación de acciones de contención oportunas. Se deben establecer claramente los roles y responsabilidades de los equipos encargados de la atención del incidente.

Una vez identificado el comportamiento del ataque, se deben aplicar medidas inmediatas de contención orientadas a limitar la propagación de la amenaza dentro de la organización. Entre las principales acciones se encuentra el aislamiento de los equipos comprometidos, la restricción de accesos sospechosos, el bloqueo de puertos o direcciones IP maliciosas y la deshabilitación temporal de servicios vulnerables que puedan estar siendo utilizados por el atacante. Asimismo, la segmentación de red representa una medida importante para evitar movimientos laterales y proteger otros activos críticos de información.

Durante la atención del incidente es indispensable preservar la integridad de las evidencias digitales, garantizando que logs, registros y archivos relacionados con el ataque no sean alterados. Esta información será fundamental para posteriores procesos de análisis forense, identificación de la causa raíz y fortalecimiento de controles de seguridad. En este sentido, las herramientas de monitoreo y correlación de eventos, como los sistemas SIEM, permiten detectar

patrones anómalos, centralizar registros y generar alertas tempranas frente a actividades sospechosas, mejorando la capacidad de respuesta del equipo Blue Team.

Desde el punto de vista operativo, también es importante analizar el alcance del incidente considerando los activos involucrados, los procesos afectados y las posibles repercusiones sobre la continuidad del negocio. Esto permite priorizar las acciones de recuperación y establecer estrategias de mitigación acordes con el impacto generado por el ataque.

Estrategias de hardening para reducción de riesgos

Considerando las vulnerabilidades explotadas durante el ejercicio, particularmente las asociadas al protocolo SMBv1 y al servicio HTTP vulnerable de Rejetto HFS, una de las principales medidas de hardenización consiste en realizar una gestión adecuada de parches y actualizaciones de seguridad sobre los sistemas operativos y aplicaciones instaladas. La explotación de vulnerabilidades como EternalBlue evidencia el riesgo de mantener sistemas Windows obsoletos o sin actualizaciones críticas, por lo que resulta indispensable implementar políticas de actualización automática y validación periódica de parches de seguridad.

Es fundamental reducir la superficie de exposición del sistema mediante la deshabilitación de protocolos inseguros y servicios innecesarios. En este caso, se recomienda desactivar SMBv1 debido a las vulnerabilidades históricas asociadas a este protocolo, restringir el acceso a recursos compartidos y limitar la exposición de puertos críticos mediante reglas de firewall y segmentación de red. Del mismo modo, los servicios HTTP deben configurarse bajo criterios de seguridad, eliminando módulos innecesarios, restringiendo permisos de ejecución y evitando configuraciones por defecto que puedan facilitar la ejecución remota de comandos o la explotación de aplicaciones vulnerables.

Desde la perspectiva del sistema operativo, es necesario aplicar políticas de endurecimiento orientadas al control de acceso y gestión de privilegios. Entre estas medidas se

incluyen la implementación de contraseñas robustas, bloqueo automático de cuentas por múltiples intentos fallidos, deshabilitación de cuentas predeterminadas, restricción de privilegios administrativos y aplicación del principio de mínimo privilegio. Estas configuraciones permiten limitar la capacidad de escalamiento de privilegios y reducir el impacto de un posible compromiso del sistema.

Resulta importante fortalecer los mecanismos de monitoreo y detección temprana mediante la implementación de herramientas SIEM, análisis de logs y sistemas IDS/IPS que permitan identificar comportamientos anómalos, intentos de explotación y movimientos laterales dentro de la red. El monitoreo continuo de eventos de seguridad facilita la generación de alertas tempranas y mejora la capacidad de respuesta frente a incidentes relacionados con accesos no autorizados, ejecución de payloads o conexiones sospechosas.

Realizar evaluaciones periódicas de vulnerabilidades utilizando herramientas especializadas como Nessus, OpenVAS y OpenSCAP, las cuales permiten identificar configuraciones inseguras, servicios vulnerables y fallos de seguridad presentes en los sistemas. Estas herramientas, apoyadas en estándares como SCAP, facilitan la automatización de auditorías de seguridad y permiten validar el cumplimiento de controles técnicos orientados al hardening de servidores y servicios críticos.

En cuanto a la protección de servicios web, es recomendable implementar mecanismos adicionales de defensa como firewalls de aplicaciones web (WAF), cifrado mediante HTTPS y revisión periódica de archivos de configuración del servidor. La correcta configuración de servidores constituye una de las medidas más efectivas para reducir la superficie de ataque y prevenir compromisos de seguridad (Illa Gay, 2019). Una configuración segura del entorno web permite limitar la exposición de información sensible, restringir accesos no autorizados y reducir el riesgo de explotación asociado a vulnerabilidades en aplicaciones HTTP.

Diferencias entre Blue Team y equipos de respuesta a incidentes

Ambos cumplen funciones defensivas dentro de la estrategia de ciberseguridad de una organización; sin embargo, su enfoque operativo, alcance técnico y momento de actuación son diferentes. El Blue Team se orienta principalmente a la defensa proactiva y al fortalecimiento continuo de la postura de seguridad, enfocándose en actividades de monitoreo permanente, detección temprana de amenazas, gestión de vulnerabilidades y hardenización de sistemas. Su objetivo principal es reducir la superficie de ataque y prevenir que un actor malicioso logre comprometer la infraestructura tecnológica. Para ello, implementa controles de seguridad como firewalls, IDS/IPS, EDR, SIEM, segmentación de red, análisis de vulnerabilidades y políticas de control de acceso.

Desde una perspectiva técnica, el Blue Team trabaja continuamente sobre la infraestructura realizando correlación de eventos, monitoreo de logs, análisis de tráfico de red, revisión de configuraciones inseguras y validación de controles de seguridad. Asimismo, participa en actividades de hardenización mediante la aplicación de estándares como CIS Benchmarks, NIST SP 800-53 e ISO 27001, buscando minimizar vulnerabilidades explotables dentro de los sistemas operativos, servicios y aplicaciones. Además, este equipo suele colaborar con áreas de DevSecOps, SOC y pruebas de seguridad ofensiva para fortalecer los mecanismos de defensa antes de que ocurra un incidente real.

El CSIRT (Computer Security Incident Response Team) posee un enfoque reactivo y especializado en la gestión técnica de incidentes de seguridad informática. Su intervención ocurre cuando un incidente ya ha sido detectado, reportado o confirmado dentro de la organización. En este contexto, el equipo CSIRT se encarga de ejecutar procedimientos de contención, análisis forense, erradicación y recuperación, buscando minimizar el impacto operativo y restablecer los servicios comprometidos en el menor tiempo posible.

Entre las funciones técnicas del CSIRT se encuentran la identificación de indicadores de compromiso (IOC), aislamiento de sistemas comprometidos, adquisición y preservación de evidencias digitales, análisis de malware, revisión de artefactos forenses y reconstrucción del incidente mediante trazabilidad de eventos. Este equipo debe coordinar actividades con áreas legales, administrativas y de continuidad del negocio, garantizando una adecuada gestión del incidente y el cumplimiento de procedimientos organizacionales.

Otra diferencia importante radica en las herramientas utilizadas por cada equipo. El Blue Team se apoya principalmente en plataformas SIEM, herramientas de monitoreo continuo, scanners de vulnerabilidades y soluciones de detección y prevención, mientras que el CSIRT utiliza herramientas especializadas en análisis forense, captura de memoria, análisis de discos, análisis de malware y recuperación de sistemas afectados. Esto evidencia que el Blue Team se enfoca en la prevención y detección continua, mientras que el CSIRT actúa sobre incidentes materializados con el fin de contenerlos y mitigar sus efectos.

Aplicación de CIS Controls en operaciones Blue Team

Los CIS Controls constituyen un conjunto priorizado de buenas prácticas orientadas a reducir la superficie de ataque y fortalecer la capacidad de detección y respuesta frente a amenazas (Center for Internet Security, 2024).

Sería utilizado para implementar controles de seguridad, procesos de hardenización y mecanismos de monitoreo orientados a reducir la superficie de ataque y fortalecer la capacidad defensiva de la infraestructura tecnológica. Los CIS Controls y CIS Benchmarks permiten establecer configuraciones seguras sobre sistemas operativos, aplicaciones, dispositivos de red y servicios críticos, tomando como bases prácticas de seguridad desarrolladas a partir del análisis de amenazas reales y técnicas comúnmente utilizadas por atacantes.

Desde una perspectiva técnica, CIS sería aplicado principalmente para la implementación de controles relacionados con gestión de vulnerabilidades, configuración segura de sistemas, control de privilegios administrativos, monitoreo de logs, protección de servicios expuestos y defensa perimetral. Esto permitiría al Blue Team fortalecer componentes críticos de la infraestructura, minimizando riesgos asociados a explotación de vulnerabilidades, escalamiento de privilegios, ejecución remota de código y movimientos laterales dentro de la red.

En escenarios como el desarrollado durante el ejercicio de Red Team, donde se explotaron vulnerabilidades asociadas a SMBv1 y servicios HTTP vulnerables, CIS permitiría establecer configuraciones seguras mediante la deshabilitación de protocolos inseguros, restricción de puertos y servicios innecesarios, implementación de reglas de firewall, segmentación de red y aplicación de políticas de autenticación robusta. Asimismo, controles relacionados con inventario de activos, monitoreo de cuentas y gestión continua de vulnerabilidades facilitarían la identificación temprana de configuraciones inseguras y software vulnerable dentro del entorno tecnológico.

CIS puede ser utilizado para realizar procesos de auditoría y validación automática de configuraciones de seguridad mediante herramientas compatibles con estándares SCAP, como OpenSCAP, Nessus SCAP Plugin y SCAP Workbench. Estas herramientas permiten ejecutar escaneos automatizados sobre servidores, estaciones de trabajo y dispositivos de red, detectando desviaciones respecto a configuraciones seguras definidas por CIS Benchmarks y generando reportes técnicos orientados a la mitigación de vulnerabilidades.

Desde el punto de vista del monitoreo y la operación continua del Blue Team, CIS también permite establecer controles orientados al análisis y correlación de eventos de seguridad, protección de datos, monitoreo de logs de auditoría y defensa contra malware. Controles como el mantenimiento de registros centralizados, monitoreo de intentos de acceso no autorizados y

protección de servicios de borde fortalecen las capacidades de detección temprana frente a actividades maliciosas y facilitan la integración con plataformas SIEM, IDS/IPS y soluciones EDR.

Otra función importante de CIS dentro de las operaciones Blue Team consiste en apoyar procesos de cumplimiento y alineación con otros marcos de ciberseguridad como NIST SP 800-53 e ISO 27001. Los controles CIS pueden ser utilizados como línea base de seguridad para evaluar el nivel de madurez de los controles implementados, establecer métricas de seguimiento y priorizar acciones de remediación de acuerdo con el nivel de riesgo identificado.

Funciones y características de una plataforma SIEM

Su propósito principal consiste en centralizar logs y eventos provenientes de múltiples fuentes con el fin de detectar amenazas, identificar anomalías y facilitar la respuesta ante incidentes de seguridad informática en tiempo real. Actualmente, los SIEM constituyen uno de los componentes principales de los SOC (Security Operations Center), debido a su capacidad para procesar grandes volúmenes de información y generar inteligencia de seguridad a partir de eventos distribuidos dentro de la red.

Desde el punto de vista técnico, un SIEM integra funciones de SIM (Security Information Management) y SEM (Security Event Management). El componente SIM se encarga del almacenamiento, administración y análisis histórico de logs, mientras que el componente SEM se enfoca en el monitoreo en tiempo real, correlación de eventos y generación de alertas automáticas frente a actividades sospechosas. Esta integración permite mantener visibilidad continua sobre el comportamiento de la infraestructura y facilita la identificación temprana de amenazas avanzadas.

Una de las principales funciones de un SIEM es la centralización de eventos de seguridad provenientes de múltiples fuentes de datos, tales como firewalls, IDS/IPS, EDR, antivirus,

servidores, sistemas operativos, aplicaciones, bases de datos, dispositivos de red y servicios en la nube. Los eventos recopilados son normalizados y estructurados para permitir su procesamiento y análisis uniforme, independientemente del formato original de los logs. Esta capacidad de agregación y normalización facilita la correlación entre eventos relacionados y mejora significativamente la visibilidad de seguridad dentro de la organización.

La correlación de eventos constituye una de las capacidades más relevantes de un SIEM. Mediante motores de reglas y análisis automatizado, la plataforma es capaz de relacionar eventos provenientes de diferentes dispositivos para identificar patrones asociados a amenazas, ataques o anomalías. Esto permite detectar actividades como fuerza bruta, escalamiento de privilegios, movimientos laterales, explotación de vulnerabilidades, ejecución de malware, exfiltración de datos y conexiones no autorizadas. Los motores de correlación pueden trabajar con reglas booleanas, análisis histórico y correlación contextual basada en comportamiento.

Otra característica fundamental corresponde al procesamiento y monitoreo en tiempo real. Los SIEM modernos poseen capacidades para analizar millones de eventos por segundo, permitiendo identificar incidentes de seguridad de manera inmediata y generar alertas automatizadas frente a comportamientos anómalos. Esto reduce considerablemente el tiempo de detección (MTTD) y mejora la capacidad de respuesta del Blue Team y los equipos SOC frente a amenazas activas.

Los SIEM proporcionan capacidades avanzadas de almacenamiento, indexación y búsqueda de logs, facilitando procesos de auditoría, cumplimiento normativo y análisis forense digital. Los registros almacenados permiten reconstruir líneas de tiempo de incidentes, analizar trazabilidad de eventos y preservar evidencia técnica asociada a actividades maliciosas. Estas capacidades resultan fundamentales para investigaciones forenses y procesos de respuesta ante incidentes.

Dentro de las características técnicas más importantes de un SIEM se destacan:

- Recolección y centralización de logs desde múltiples fuentes heterogéneas.
- Normalización y parsing de eventos de seguridad.
- Correlación avanzada de eventos mediante reglas y motores analíticos.
- Monitoreo continuo y procesamiento en tiempo real.
- Generación automática de alertas e indicadores de compromiso (IOC).
- Dashboards y visualización avanzada de eventos de seguridad.
- Integración con inteligencia de amenazas y feeds externos.
- Capacidades UEBA (User and Entity Behavior Analytics).
- Automatización de respuestas mediante playbooks y acciones automatizadas.
- Soporte para auditoría, cumplimiento y análisis forense.
- Gestión y retención de grandes volúmenes de logs.

De igual manera, los SIEM actuales incorporan capacidades de análisis de comportamiento basadas en machine learning y UEBA, permitiendo detectar desviaciones respecto al comportamiento habitual de usuarios, dispositivos y aplicaciones. Esto mejora la identificación de amenazas internas, ataques persistentes avanzados (APT) y actividades anómalas que tradicionalmente no pueden ser detectadas mediante reglas estáticas.

Otra función importante de estas plataformas es la automatización de tareas de seguridad. Algunos SIEM permiten ejecutar respuestas automáticas frente a incidentes, como bloqueo de direcciones IP, aislamiento de hosts comprometidos, generación de tickets o ejecución de scripts de contención.

Herramientas para la contención de ataques informáticos

Dentro de los procesos de respuesta ante incidentes de seguridad informática, las herramientas de contención cumplen una función fundamental orientada a limitar la propagación

de una amenaza y reducir el impacto generado sobre la infraestructura tecnológica. A diferencia de las herramientas de detección, cuyo objetivo principal consiste en identificar comportamientos anómalos o eventos sospechosos, las herramientas de contención permiten ejecutar acciones correctivas o preventivas sobre los sistemas comprometidos, evitando que el incidente continúe afectando otros activos de información. Estas soluciones forman parte de las estrategias implementadas por equipos Blue Team y CSIRT durante las fases de contención, erradicación y recuperación definidas en marcos de referencia como NIST SP 800-61, ITIL e ISO 27035.

Desde el punto de vista operativo, las herramientas de contención son utilizadas para aislar equipos comprometidos, bloquear conexiones maliciosas, restringir accesos no autorizados, controlar el tráfico de red y evitar movimientos laterales dentro de la infraestructura. Estas capacidades permiten minimizar la afectación sobre la confidencialidad, integridad y disponibilidad de la información, reduciendo el riesgo de propagación del incidente hacia otros sistemas críticos. La gestión de incidentes requiere procedimientos estructurados que permitan la detección, contención, erradicación y recuperación frente a eventos de seguridad (Anchala Sánez, 2024; Turcios, 2025).

Actualmente existen diversas herramientas especializadas que permiten fortalecer los procesos de contención, monitoreo y respuesta ante incidentes de seguridad informática como:

Cisco ASA: es una solución de seguridad perimetral desarrollada por Cisco que integra múltiples funciones de protección en una sola plataforma, incluyendo firewall, VPN, prevención de intrusiones (IPS) y filtrado de tráfico de red. Este tipo de tecnología es utilizada dentro de las estrategias Blue Team como mecanismo de contención y control de amenazas, permitiendo restringir accesos no autorizados, bloquear conexiones maliciosas y proteger la infraestructura frente a ataques externos e internos. Desde una perspectiva técnica, Cisco ASA utiliza un modelo basado en niveles de seguridad para controlar el flujo de tráfico entre diferentes segmentos de

red, como la red interna, internet y la DMZ. De manera predeterminada, el tráfico proveniente de zonas de menor confianza es bloqueado, mientras que las conexiones legítimas originadas desde redes internas pueden ser permitidas y monitoreadas mediante mecanismos de inspección con estado (stateful inspection). Esta funcionalidad permite al firewall mantener información de las sesiones activas, validando que únicamente el tráfico asociado a conexiones autorizadas pueda regresar a la red interna.

Otra de las capacidades importantes de Cisco ASA corresponde al filtrado de paquetes y aplicación de listas de control de acceso (ACL), las cuales permiten definir reglas específicas sobre el tráfico autorizado o restringido dentro de la infraestructura. Gracias a esto, es posible bloquear puertos vulnerables, restringir protocolos inseguros y limitar conexiones sospechosas, reduciendo la posibilidad de explotación de vulnerabilidades o movimientos laterales dentro de la red corporativa.

Cisco ASA incorpora funcionalidades avanzadas como prevención de intrusiones (IPS), protección contra malware, análisis de tráfico, detección de amenazas y capacidades VPN para acceso remoto seguro. Estas características fortalecen la capacidad defensiva de la organización, permitiendo detectar actividades anómalas, bloquear ataques conocidos y proteger la comunicación entre usuarios y servicios críticos. Asimismo, la integración con plataformas SIEM facilita el monitoreo centralizado y la correlación de eventos de seguridad en tiempo real.

Microsoft Defender for Endpoint (MDE): es una plataforma de seguridad de endpoints basada en la nube, diseñada para prevenir, detectar, investigar y responder a amenazas avanzadas sobre dispositivos conectados a la infraestructura tecnológica de una organización. Esta solución forma parte de las estrategias modernas de protección implementadas por equipos Blue Team y SOC, permitiendo fortalecer la seguridad de estaciones de trabajo, servidores, dispositivos móviles y entornos híbridos mediante mecanismos avanzados de monitoreo y contención de

incidentes. Desde una perspectiva técnica, Microsoft Defender for Endpoint incorpora capacidades EDR (Endpoint Detection and Response), protección antivirus de nueva generación, análisis de comportamiento y monitoreo continuo de actividades sospechosas sobre los endpoints. La plataforma utiliza sensores de comportamiento integrados en el sistema operativo para recopilar telemetría relacionada con procesos, conexiones de red, ejecución de aplicaciones y actividad de usuarios, permitiendo identificar anomalías y patrones asociados a ataques informáticos avanzados.

Una de las funciones más relevantes de MDE corresponde a la reducción de la superficie de ataque (ASR - Attack Surface Reduction), la cual permite limitar vectores de explotación mediante políticas de seguridad orientadas al bloqueo de comportamientos peligrosos, ejecución de código malicioso, scripts no autorizados y técnicas comúnmente utilizadas por atacantes. Estas capacidades resultan especialmente útiles para prevenir explotación de vulnerabilidades, movimientos laterales y ejecución remota de comandos dentro de la red corporativa. Incorpora capacidades de investigación y remediación automatizada (AIR - Automated Investigation and Remediation), apoyadas en inteligencia artificial y machine learning. Estas funcionalidades permiten analizar alertas de seguridad, identificar artefactos maliciosos y ejecutar acciones automáticas de contención, como aislamiento de dispositivos comprometidos, bloqueo de archivos maliciosos, finalización de procesos sospechosos y cuarentena de amenazas detectadas. Esto reduce significativamente el tiempo de respuesta frente a incidentes y disminuye la carga operativa de los equipos de seguridad.

Otra característica importante corresponde a la integración de inteligencia global de amenazas proporcionada por Microsoft, la cual utiliza información recopilada desde millones de dispositivos y servicios en la nube para identificar amenazas emergentes, vulnerabilidades de día cero y campañas avanzadas de ataque. Gracias a esto, MDE puede detectar actividades

maliciosas en tiempo real y aplicar mecanismos de protección preventiva frente a amenazas conocidas y desconocidas.

Desde el punto de vista de contención de incidentes, Microsoft Defender for Endpoint permite ejecutar acciones inmediatas sobre los endpoints comprometidos, tales como aislamiento del host de la red, bloqueo de conexiones maliciosas, restricción de ejecución de aplicaciones, control de dispositivos externos y protección frente a manipulación de controles de seguridad. Estas capacidades ayudan a limitar la propagación de malware, ransomware o ataques laterales dentro de la infraestructura tecnológica.

Palo Alto Networks: Esta tecnología es utilizada por equipos Blue Team y SOC para fortalecer la postura defensiva de las organizaciones, proporcionando mecanismos de prevención, detección, análisis y contención frente a amenazas informáticas modernas. La plataforma integra capacidades de seguridad para redes, nube, aplicaciones y endpoints, permitiendo administrar la protección de manera centralizada y automatizada.

Desde una perspectiva técnica, Palo Alto Networks implementa arquitecturas de Next Generation Firewall (NGFW), capaces de inspeccionar y analizar el tráfico de red a nivel de aplicaciones, usuarios y contenido, independientemente del puerto o protocolo utilizado. A diferencia de los firewalls tradicionales, esta solución permite identificar aplicaciones de manera nativa y analizar tráfico malicioso en tiempo real mediante motores avanzados de inspección, reduciendo significativamente la posibilidad de evasión de controles de seguridad.

Una de las principales fortalezas de la plataforma corresponde a la integración de múltiples módulos de protección en un entorno unificado, incluyendo antivirus, antispyware, IPS, protección contra ataques DoS, filtrado web, filtrado de contenido y mecanismos DLP (Data Loss Prevention). Esta integración permite que todos los módulos de seguridad trabajen de

manera coordinada sobre el tráfico de red, facilitando la detección y contención de amenazas avanzadas sin afectar significativamente el rendimiento de la infraestructura tecnológica.

Palo Alto Networks incorpora tecnologías avanzadas de inteligencia de amenazas como WildFire y Cortex™, las cuales utilizan análisis de comportamiento, automatización, machine learning e inteligencia en la nube para detectar malware, amenazas avanzadas y ataques de tipo zero-day. Estas herramientas permiten identificar archivos sospechosos, analizar comportamientos maliciosos y compartir información de amenazas en tiempo real entre diferentes componentes de seguridad, fortaleciendo la capacidad de respuesta frente a incidentes informáticos.

Desde el enfoque de contención de ataques, Palo Alto Networks permite aplicar segmentación de red, control granular de aplicaciones, filtrado de tráfico y bloqueo automático de conexiones maliciosas, reduciendo la propagación de amenazas y limitando movimientos laterales dentro de la infraestructura. Estas capacidades son especialmente importantes frente a ataques avanzados, ransomware y explotación de vulnerabilidades sobre servicios expuestos.

Otra característica relevante corresponde a la visibilidad centralizada sobre usuarios, dispositivos, aplicaciones y servicios distribuidos en entornos locales, híbridos y en la nube.

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/PZCFjtTEePY

Conclusiones

El desarrollo del seminario permitió comprender la importancia de integrar capacidades ofensivas y defensivas dentro de una estrategia de ciberseguridad, evidenciando cómo las actividades desarrolladas por los equipos Red Team y Blue Team contribuyen a la identificación, mitigación y gestión de riesgos asociados a los sistemas de información.

Los ejercicios prácticos realizados demostraron que los sistemas desactualizados, los servicios vulnerables y las configuraciones inseguras representan un riesgo significativo para las organizaciones, ya que pueden facilitar la explotación de vulnerabilidades críticas como las identificadas durante el laboratorio, comprometiendo la confidencialidad, integridad y disponibilidad de la información.

La aplicación de herramientas especializadas como Nmap y Metasploit permitió validar la efectividad de las metodologías de pentesting para la identificación y explotación controlada de vulnerabilidades, proporcionando una visión práctica sobre las técnicas utilizadas por actores maliciosos para comprometer infraestructuras tecnológicas.

Desde la perspectiva defensiva, se evidenció que la implementación de medidas de hardenización, monitoreo continuo, gestión de vulnerabilidades y respuesta a incidentes constituye un elemento fundamental para reducir la superficie de ataque y fortalecer la postura de seguridad de las organizaciones frente a amenazas cibernéticas.

Finalmente, el análisis de los aspectos éticos, legales y normativos asociados al ejercicio profesional de la ciberseguridad permitió reconocer la importancia de actuar bajo principios de responsabilidad, cumplimiento normativo y buenas prácticas, garantizando que las actividades de evaluación y protección de la seguridad informática se desarrollen dentro de marcos legales y técnicos apropiados.

Recomendaciones

Implementar un programa permanente de gestión de vulnerabilidades que contemple actividades periódicas de identificación, evaluación y remediación de debilidades de seguridad, priorizando la actualización de sistemas operativos, aplicaciones y servicios expuestos a la red.

Fortalecer los mecanismos de protección de la infraestructura tecnológica mediante la aplicación de controles de hardenización basados en estándares reconocidos como CIS Controls, eliminando servicios innecesarios, restringiendo privilegios y aplicando configuraciones seguras en servidores, estaciones de trabajo y dispositivos de red.

Incorporar soluciones de monitoreo y detección de amenazas, como plataformas SIEM, tecnologías EDR y firewalls de nueva generación, que permitan identificar comportamientos anómalos, correlacionar eventos de seguridad y responder oportunamente ante posibles incidentes.

Realizar ejercicios periódicos de evaluación de seguridad, incluyendo pruebas de penetración, análisis de vulnerabilidades y simulaciones controladas de ataque, con el fin de validar la efectividad de los controles implementados y detectar oportunidades de mejora en la estrategia de ciberseguridad organizacional.

Promover programas continuos de capacitación y concientización en seguridad informática dirigidos a usuarios, administradores y personal técnico, fortaleciendo las capacidades de prevención, detección y respuesta frente a amenazas que puedan afectar los activos de información de la organización.

Referencias Bibliográficas

Álvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos.* Semantic Scholar. https://www.semanticscholar.org/paper/PROPUESTA-DE-UNA-METODOLOG%C3%8DA-DE-PRUEBAS-DE-A-Intriago-Karina/f3be44039e5f4c1bfced6ad23455291b2a304c77#citing-papers

Anchala Sánez, M. R. (2024). *Propuesta de gestión de incidentes de seguridad mediante la integración de inteligencia de amenazas para la contención de ataques informáticos* [Trabajo de grado]. Universidad Israel. http://repositorio.uisrael.edu.ec/handle/47000/4184

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

Ávila Pardo, W., & Ramírez Restrepo, J. L. (s. f.). *Escaneo de vulnerabilidades al servidor principal de la empresa. Caso de estudio.* Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/57335

Barrios González, A. G. (2024). *Análisis e implementación de las fases del pentesting detectando vulnerabilidades en un sistema informático remoto* [Trabajo de grado]. Benemérita Universidad Autónoma de Puebla.

Bilbao, G., Fuertes, J., & Guibert, J. M. (2006). *Ética para ingenieros. Desclée De Brouwer.*

Center for Internet Security. (2024). CIS Critical Security Controls Version 8. Center for Internet Security.

Chuquiguanca Vicente, L. R. (2020). *Implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) en la Fiscalía General del Estado* [Trabajo de grado]. Universidad Internacional SEK. https://repositorio.uisek.edu.ec/handle/123456789/3959

Congreso 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 preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.* Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso 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. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Consejo Nacional de Política Económica y Social (CONPES). (2020). CONPES 3995: *Política Nacional de Confianza y Seguridad Digital.* Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

García, P. A. S., & González, L. D. B. (2024). *Entre la seguridad y la privacidad: dilemas éticos en la recolección de datos digitales.* Intellectual Network Revista Internacional, 2(3), 1–15. https://revinde.org/index.php/intellectual_network/article/view/51

García Montes, J. P. (2025). *Implementación de un módulo de seguridad ofensiva para reconocimiento pasivo y activo de vulnerabilidades de puertos y servicios* [Trabajo de grado]. Universidad Tecnológica de Pereira. https://repositorio.utp.edu.co

Hernández, E. F. T., Canizales, R. R., & Páez, A. V. (2021). *La importancia de la ciberseguridad y los derechos humanos en el entorno virtual.* Misión Jurídica: Revista de Derecho y Ciencias Sociales, 14(20), 142–158.

Illa Gay, R. (2019). *Seguridad en servidores empresariales: Control y análisis de configuraciones de seguridad y vulnerabilidades* [Trabajo de fin de grado]. Universitat Oberta de Catalunya. https://openaccess.uoc.edu

Instituto Nacional de Ciberseguridad. (2019*). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE.* https://www.incibe.es

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems* — Requirements. ISO. https://doi.org/10.37511/apuntesci.v4n2a5

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

Maya, R. P. (2013*). El delito de acceso abusivo a sistema informático: a propósito del artículo 269A del Código Penal de 2000*. Revista de Derecho, Comunicaciones y Nuevas Tecnologías. https://doi.org/10.17230/nfp.13.88.3

Moreno, M. (2022). *Gestión de incidentes de ciberseguridad. Ediciones de la U.* https://books.google.com.co/books?id=ZnugEAAAQBAJ&lpg=PA7&ots=7bRaseLyOq&dq=Moreno%2C%20M.%20(2022).%20Gesti%C3%B3n%20de%20incidentes%20de%20ciberseguridad.%20Ediciones%20de%20la%20U.

National Institute of Standards and Technology. (2008). *Technical guide to information security testing and assessment (NIST Special Publication 800-115).* U.S. Department of Commerce.

National Institute of Standards and Technology. (2012). *Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). U.S. Department of Commerce.*

National Institute of Standards and Technology. (2022). Guide to enterprise patch management technologies (NIST Special Publication 800-40 Revision 4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-40r4

Orellana Jaramillo, P. J., & Morán Velasco, J. M. (2025). *Auditoría de ciberseguridad y detección de vulnerabilidades en plataformas de edutainment: Un enfoque para la protección de datos sensibles y el fortalecimiento de la privacidad* [Trabajo de maestría]. Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/handle/123456789/31411

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

Panda Security. (2018). *Pentesting: Una herramienta muy valiosa para tu empresa.* Panda Security Media Center. https://www.pandasecurity.com

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Diario Oficial No. 48.834. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

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

Suárez Restrepo, S. (2021). *Indicadores de compromiso basados en ataques a servicios web* [Trabajo de grado]. Instituto Tecnológico Metropolitano. https://repositorio.itm.edu.co

Turcios, C. L. R. (2025). *Desarrollo de una metodología para la gestión de incidentes en seguridad informática con aplicación de la ISO 27001 y protocolos NIST para el Hospital María* [Trabajo de grado]. Universidad Tecnológica Centroamericana. https://repositorio.unitec.edu

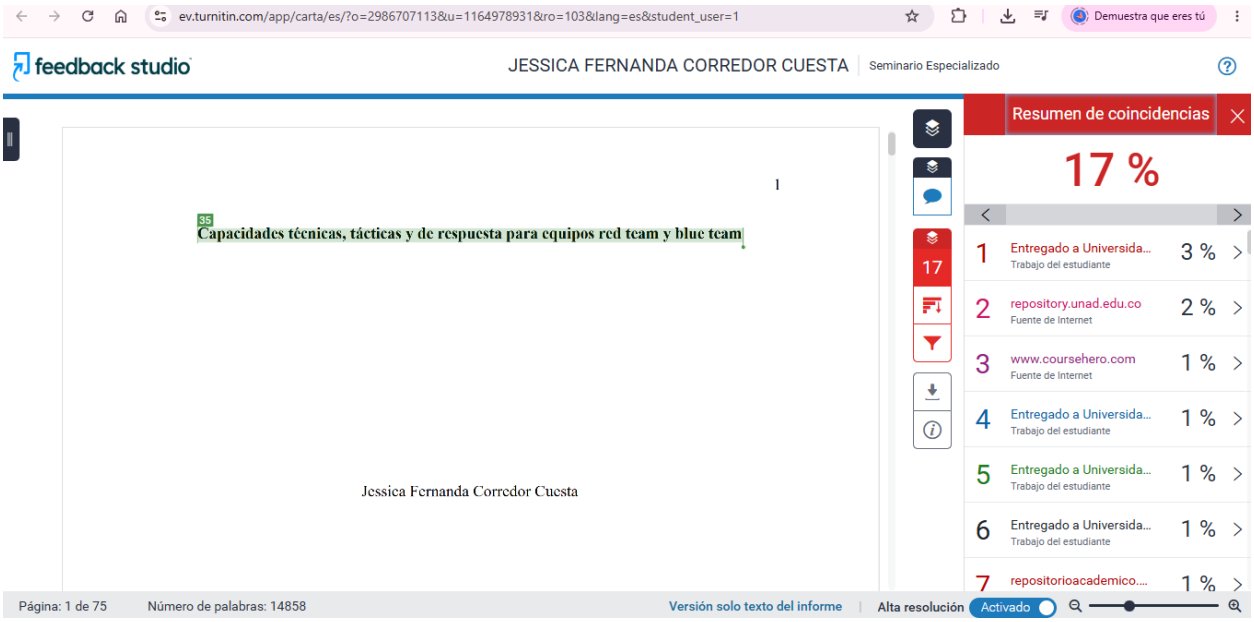
Vanegas Romero, A. Y. (2019). *Pentesting: ¿Por qué es importante para las empresas?* Universidad Piloto de Colombia. https://repository.unipiloto.edu.co/handle/20.500.12277/6286

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

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Muestra el resultado generado por la plataforma Turnitin para el presente trabajo, evidenciando el porcentaje de similitud identificado y los elementos considerados durante el análisis de coincidencias del documento.