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

Edison Leonardo Sequera Garcia

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 principalmente a Dios, por permitirme llegar hasta este momento de mi formación académica, por darme la fortaleza necesaria para superar las dificultades que se presentaron durante el proceso y por brindarme la oportunidad de seguir creciendo tanto personal como profesionalmente.

A mi familia, que ha sido el pilar fundamental en cada una de las etapas de mi vida. Gracias por su apoyo incondicional, por sus palabras de aliento en los momentos de cansancio y por acompañarme en este camino lleno de retos, aprendizajes y experiencias que han contribuido a mi formación como profesional. Cada logro alcanzado también les pertenece, porque han sido parte importante de este proceso.

A mis padres, por enseñarme desde temprana edad el valor del esfuerzo, la responsabilidad y la perseverancia. Gracias por los sacrificios realizados y por brindarme siempre su confianza y apoyo para continuar avanzando hacia mis metas.

A mis seres queridos y amigos, quienes de una u otra manera estuvieron presentes durante esta etapa académica, brindándome motivación, comprensión y ánimo para continuar cuando las circunstancias parecían difíciles.

Dedico también este trabajo a todas aquellas personas que creen en el poder de la educación como herramienta de transformación social y crecimiento personal. Cada página de este informe representa el resultado del compromiso, la dedicación y el deseo constante de adquirir nuevos conocimientos para enfrentar los desafíos del mundo profesional.

Finalmente, dedico este logro a mí mismo, por la disciplina, el esfuerzo y la constancia demostrados a lo largo de este proceso. Por no rendirme ante las dificultades y por mantener siempre la convicción de que cada meta alcanzada es el resultado del trabajo realizado día tras día.

Agradecimientos

Al culminar este proceso académico, deseo expresar mi más sincero agradecimiento a todas las personas e instituciones que contribuyeron de manera directa e indirecta al desarrollo de este trabajo y al fortalecimiento de mi formación profesional.

En primer lugar, agradezco a la Universidad Nacional Abierta y a Distancia (UNAD) por brindarme la oportunidad de acceder a una formación de calidad, basada en el aprendizaje autónomo, la investigación y el desarrollo de competencias que fortalecen el desempeño profesional en diferentes áreas del conocimiento.

Agradezco especialmente al Ingeniero Eduvin Trigos Sánchez, tutor del seminario especializado "Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team", por su acompañamiento académico, orientación y disposición para resolver las inquietudes presentadas durante el desarrollo de las diferentes actividades. Sus aportes fueron fundamentales para comprender la importancia de la ciberseguridad desde una perspectiva técnica, estratégica y ética.

De igual manera, agradezco a mis compañeros de estudio, quienes a través del intercambio de ideas, experiencias y conocimientos contribuyeron al fortalecimiento del aprendizaje colaborativo y al enriquecimiento de las actividades desarrolladas durante el seminario.

Expreso un agradecimiento especial a mi familia por su paciencia, comprensión y apoyo permanente. Gracias por motivarme a continuar avanzando incluso en los momentos de mayor exigencia académica. Su confianza y respaldo fueron una fuente constante de inspiración para alcanzar esta meta.

También agradezco a todas las personas que, de alguna manera, aportaron a mi proceso de formación mediante consejos, enseñanzas y experiencias que contribuyeron a fortalecer mis capacidades personales y profesionales.

Finalmente, agradezco la oportunidad de haber participado en este seminario especializado, ya que permitió consolidar conocimientos relacionados con ciberseguridad ofensiva y defensiva, análisis de vulnerabilidades, gestión de riesgos y protección de infraestructuras tecnológicas, fortaleciendo competencias que serán de gran utilidad en mi desarrollo profesional futuro.

Resumen

La ciberseguridad se ha convertido en uno de los principales retos para las organizaciones debido al incremento constante de amenazas informáticas que afectan la confidencialidad, integridad y disponibilidad de la información. El crecimiento de ataques cibernéticos, vulnerabilidades en infraestructuras tecnológicas y riesgos asociados a la transformación digital ha generado la necesidad de implementar estrategias ofensivas y defensivas que permitan fortalecer la protección de los sistemas informáticos.El presente informe técnico consolida los resultados obtenidos durante el desarrollo del seminario especializado “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, integrando las actividades realizadas en las diferentes etapas del curso relacionadas con análisis de vulnerabilidades, pruebas de penetración, monitoreo de eventos de seguridad y estrategias de contención de incidentes.Durante el desarrollo del ejercicio se aplicaron metodologías de pentesting orientadas a la identificación y explotación controlada de vulnerabilidades presentes en entornos tecnológicos simulados. Asimismo, se implementaron mecanismos defensivos enfocados en el monitoreo, análisis de registros y fortalecimiento de la infraestructura mediante herramientas de seguridad y técnicas de hardening. De igual manera, se realizó un análisis relacionado con aspectos éticos y legales asociados a las actividades de ciberseguridad, destacando la importancia del cumplimiento normativo y la aplicación responsable de pruebas de seguridad dentro de entornos organizacionales. Finalmente, se presentan conclusiones y recomendaciones orientadas al fortalecimiento de la seguridad informática mediante la implementación de controles preventivos, monitoreo continuo, gestión de riesgos y capacitación permanente en ciberseguridad.

***Palabras clave*:** Blue team, ciberseguridad, pentesting, red team, vulnerabilidades.

Abstract

Cybersecurity has become one of the main challenges for organizations due to the constant increase in cyber threats affecting the confidentiality, integrity, and availability of information. The growth of cyberattacks, vulnerabilities in technological infrastructures, and risks associated with digital transformation has generated the need to implement offensive and defensive strategies aimed at strengthening the protection of information systems. This technical report consolidates the results obtained during the development of the specialized seminar “Strategic Cybersecurity Teams: Red Team & Blue Team”, integrating the activities carried out throughout the different stages of the course related to vulnerability analysis, penetration testing, security event monitoring, and incident containment strategies. During the development of the exercise, penetration testing methodologies were applied for the identification and controlled exploitation of vulnerabilities present in simulated technological environments. Likewise, defensive mechanisms focused on monitoring, log analysis, and infrastructure hardening were implemented through the use of security tools and hardening techniques. Additionally, an analysis related to ethical and legal aspects associated with cybersecurity activities was conducted, highlighting the importance of regulatory compliance and the responsible application of security testing within organizational environments. Finally, conclusions and recommendations are presented, aimed at strengthening cybersecurity through the implementation of preventive controls, continuous monitoring, risk management, and permanent cybersecurity training.

Keywords**:** blue team, cybersecurity, pentesting, red team, vulnerabilities.

Tabla de contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Activo digital:

Elemento tecnológico o información que posee valor para una organización y requiere mecanismos de protección frente a amenazas informáticas.

Blue Team:

Equipo responsable de la defensa, monitoreo, análisis y contención de incidentes de seguridad informática dentro de una organización.

Ciberseguridad:

Conjunto de prácticas, procesos y tecnologías orientadas a proteger sistemas, redes y datos frente a ataques cibernéticos o accesos no autorizados.

Exploit:

Código o técnica utilizada para aprovechar una vulnerabilidad presente en un sistema o aplicación informática.

Fail2Ban:

Herramienta de seguridad utilizada para detectar y bloquear intentos de acceso no autorizados mediante el análisis de registros del sistema.

Firewall:

Mecanismo de seguridad encargado de controlar y filtrar el tráfico de red según reglas previamente establecidas.

Hardening:

Proceso de fortalecimiento de sistemas mediante configuraciones de seguridad orientadas a reducir vulnerabilidades.

IDS:

Sistema de detección de intrusiones utilizado para identificar actividades sospechosas dentro de una red o infraestructura tecnológica.

Metasploit:

Framework especializado en pruebas de penetración utilizado para validar vulnerabilidades mediante explotación controlada.

Nmap:

Herramienta de escaneo de redes utilizada para identificar dispositivos, servicios activos y puertos abiertos.

Pentesting:

Proceso de pruebas de penetración orientado a identificar vulnerabilidades explotables dentro de una infraestructura tecnológica.

pfSense:

Firewall de software libre utilizado para el filtrado y control del tráfico de red en entornos organizacionales.

Pivoting:

Técnica utilizada por atacantes para desplazarse dentro de una red utilizando un sistema previamente comprometido.

Red Team:

Equipo encargado de simular ataques controlados con el objetivo de evaluar la seguridad de una organización.

SIEM:

Sistema de gestión de eventos e información de seguridad encargado de centralizar y analizar registros relacionados con incidentes de seguridad.

SMB:

Protocolo utilizado para compartir archivos e impresoras dentro de redes Windows.

Vulnerabilidad:

Debilidad presente en un sistema, red o aplicación que puede ser aprovechada por un atacante.

Wazuh:

Plataforma de monitoreo y análisis de seguridad utilizada para detección de amenazas y correlación de eventos.

Introducción

En la actualidad, las organizaciones enfrentan un panorama de amenazas cibernéticas cada vez más complejo debido al crecimiento de la transformación digital y al incremento de ataques dirigidos contra infraestructuras tecnológicas. La dependencia de sistemas informáticos para el desarrollo de procesos administrativos, operativos y financieros ha generado la necesidad de fortalecer los mecanismos de protección orientados a garantizar la seguridad de la información y la continuidad de los servicios tecnológicos.

Los ataques cibernéticos pueden generar afectaciones significativas relacionadas con pérdida de información, interrupción de operaciones, accesos no autorizados y daños económicos o reputacionales para las organizaciones. Por esta razón, la implementación de estrategias ofensivas y defensivas en ciberseguridad se ha convertido en un componente fundamental dentro de los procesos de gestión tecnológica. La ciberseguridad se ha convertido en un componente fundamental para las organizaciones modernas debido al crecimiento constante de las amenazas informáticas y al aumento de la dependencia de los sistemas digitales. De acuerdo con el National Institute of Standards and Technology (NIST, 2018), la implementación de estrategias de protección y gestión de riesgos resulta indispensable para garantizar la seguridad de la información.

Dentro de este contexto, los equipos Red Team y Blue Team desempeñan funciones esenciales para evaluar y fortalecer la postura de seguridad de las organizaciones. El Red Team se encarga de simular ataques controlados mediante metodologías ofensivas que permiten identificar vulnerabilidades presentes en sistemas y redes. Por otra parte, el Blue Team desarrolla actividades orientadas al monitoreo, análisis, detección y contención de amenazas informáticas mediante la implementación de controles defensivos.

El presente informe técnico final consolida las actividades desarrolladas durante el seminario especializado “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, integrando los conocimientos adquiridos en las diferentes etapas relacionadas con análisis de vulnerabilidades, pruebas de penetración, monitoreo de eventos de seguridad y fortalecimiento de infraestructuras tecnológicas.

El documento presenta un análisis técnico de las metodologías utilizadas, las herramientas implementadas y las estrategias aplicadas tanto desde la perspectiva ofensiva como defensiva. Finalmente, se establecen conclusiones y recomendaciones orientadas al fortalecimiento de la seguridad informática dentro de entornos organizacionales.

Asimismo, las pruebas de penetración permiten identificar vulnerabilidades antes de que estas sean aprovechadas por actores maliciosos, contribuyendo al fortalecimiento de los controles de seguridad existentes (Offensive Security, 2024).

Justificación

El crecimiento de amenazas informáticas y el incremento de ataques cibernéticos han generado la necesidad de fortalecer las estrategias de protección dentro de las organizaciones, especialmente en aquellos entornos donde la información representa un activo crítico para el desarrollo de las operaciones institucionales.

Actualmente, las organizaciones dependen de infraestructuras tecnológicas para la gestión de información, prestación de servicios y ejecución de procesos administrativos y operativos. Sin embargo, esta dependencia tecnológica también incrementa la exposición a vulnerabilidades y riesgos relacionados con accesos no autorizados, robo de información, malware y afectaciones a la disponibilidad de los sistemas.

La realización de ejercicios de análisis de vulnerabilidades y pruebas de penetración constituye una práctica ampliamente utilizada para evaluar el nivel de exposición de los sistemas frente a amenazas cibernéticas. Según OWASP Foundation (2024), la identificación temprana de vulnerabilidades permite implementar controles preventivos que reducen significativamente los riesgos de seguridad.

El desarrollo del presente informe técnico permite integrar los conocimientos adquiridos durante el seminario especializado “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, fortaleciendo competencias relacionadas con pruebas de penetración, análisis de vulnerabilidades, monitoreo de eventos de seguridad y estrategias de contención frente a incidentes informáticos.

Asimismo, este ejercicio académico facilita la comprensión de metodologías ofensivas y defensivas utilizadas dentro de procesos de evaluación de seguridad informática, permitiendo reconocer la importancia de implementar controles preventivos, mecanismos de monitoreo y políticas de protección orientadas al fortalecimiento de la seguridad organizacional.

De igual manera, la integración de estrategias ofensivas y defensivas contribuye al fortalecimiento de las capacidades organizacionales para la detección y respuesta frente a incidentes de seguridad informática (MITRE, 2025).

Finalmente, la elaboración de este informe contribuye al desarrollo de habilidades relacionadas con documentación técnica, análisis de riesgos y formulación de recomendaciones orientadas a la mejora continua de la seguridad informática en entornos empresariales y organizacionales.

Objetivos

Objetivo General

Analizar las estrategias ofensivas y defensivas aplicadas en entornos organizacionales mediante ejercicios Red Team y Blue Team, con el propósito de identificar vulnerabilidades, evaluar riesgos y fortalecer la seguridad informática mediante la implementación de mecanismos de protección y contención.

Objetivos Específicos

Identificar vulnerabilidades presentes en sistemas y redes mediante metodologías de análisis y pruebas de penetración.

Aplicar estrategias ofensivas orientadas a la simulación controlada de ataques informáticos dentro de entornos de laboratorio.

Implementar mecanismos defensivos para la detección, monitoreo y contención de incidentes de seguridad informática.

Analizar los riesgos asociados a las vulnerabilidades identificadas dentro de la infraestructura tecnológica evaluada.

Reconocer la importancia de los aspectos éticos y legales relacionados con las actividades de ciberseguridad y pruebas de penetración.

Formular recomendaciones orientadas al fortalecimiento de la seguridad informática y la protección de los activos digitales organizacionales.

Fundamentos de Red Team y Blue Team

Introducción a la ciberseguridad

La ciberseguridad se ha convertido en uno de los componentes más importantes dentro de las organizaciones modernas debido al incremento constante de amenazas informáticas que afectan la confidencialidad, integridad y disponibilidad de la información. El crecimiento del uso de plataformas digitales, servicios en la nube, dispositivos conectados y redes empresariales ha generado nuevos riesgos relacionados con accesos no autorizados, malware, robo de información y explotación de vulnerabilidades.

Actualmente, las organizaciones dependen de infraestructuras tecnológicas para la gestión de procesos administrativos, financieros y operativos. Sin embargo, esta dependencia también incrementa la exposición frente a ataques cibernéticos capaces de generar pérdidas económicas, daños reputacionales e interrupciones en la continuidad de los servicios tecnológicos.

Frente a este panorama, la ciberseguridad surge como una disciplina encargada de implementar mecanismos de prevención, detección y respuesta orientados a proteger los activos digitales de una organización. Estas estrategias incluyen monitoreo de eventos, gestión de vulnerabilidades, análisis de riesgos y aplicación de controles defensivos que permitan fortalecer la infraestructura tecnológica.

Asimismo, dentro de la ciberseguridad moderna se destacan los equipos Red Team y Blue Team, encargados de ejecutar actividades ofensivas y defensivas para evaluar el nivel de protección de los sistemas informáticos y fortalecer la capacidad de respuesta frente a amenazas cibernéticas.

Concepto y funciones del Red Team

El Red Team corresponde al equipo especializado en la simulación de ataques informáticos controlados con el propósito de identificar vulnerabilidades y evaluar el nivel de exposición de una infraestructura tecnológica frente a posibles amenazas.

Este equipo adopta técnicas similares a las utilizadas por atacantes reales, lo que permite identificar diferentes debilidades dentro de los sistemas evaluados, como configuraciones inseguras, servicios vulnerables, errores en los mecanismos de autenticación, aplicaciones desactualizadas y malas prácticas de seguridad que podrían ser aprovechadas para comprometer la infraestructura tecnológica.

Las actividades desarrolladas por el Red Team se enfocan en simular escenarios de ataque controlados con el objetivo de identificar posibles debilidades dentro de una infraestructura tecnológica. Estas actividades incluyen el reconocimiento de objetivos, la recolección de información, el escaneo de puertos, la enumeración de servicios y la validación de vulnerabilidades encontradas durante el análisis. De igual forma, pueden involucrar pruebas relacionadas con el impacto que tendría un acceso comprometido, como el escalamiento de privilegios o posibles movimientos laterales dentro de la red.

El desarrollo de estas pruebas permite obtener una visión más cercana de los riesgos existentes y proporciona información útil para que el equipo defensivo implemente controles orientados a mejorar la seguridad del entorno evaluado.

Estas acciones permiten identificar riesgos antes de que sean aprovechados por atacantes externos y facilitan la implementación de medidas correctivas orientadas al fortalecimiento de la seguridad organizacional.

Dentro de las herramientas más utilizadas por los equipos Red Team se encuentran:

- Kali Linux.

- Metasploit Framework.
- Nmap.
- Burp Suite.
- Wireshark.
- OpenVAS

Cada una de estas herramientas permite desarrollar actividades específicas relacionadas con análisis de vulnerabilidades y pruebas de penetración en entornos controlados.

Concepto y funciones del Blue Team

El Blue Team es el equipo encargado de la defensa y protección de la infraestructura tecnológica dentro de una organización. Su función principal consiste en prevenir, detectar y responder ante incidentes de seguridad informática que puedan afectar la operación normal de los sistemas.

A diferencia del Red Team, el Blue Team trabaja desde una perspectiva defensiva, implementando mecanismos de protección orientados al monitoreo continuo de eventos, análisis de registros y detección de actividades sospechosas dentro de la red organizacional.

Entre las funciones más importantes desarrolladas por el Blue Team se encuentran:

- Monitoreo de tráfico de red.
- Análisis de logs
- Gestión de vulnerabilidades.
- Administración de firewalls.
- Respuesta a incidentes.

- Aplicación de parches de seguridad.
- Fortalecimiento de sistemas mediante hardening.

Asimismo, este equipo utiliza herramientas especializadas como Wazuh, PfSense, Fail2Ban, sistemas SIEM, IDS/IPS y plataformas de monitoreo de seguridad, las cuales permiten recopilar eventos, analizar comportamientos anómalos y fortalecer la capacidad de detección y respuesta ante posibles incidentes de seguridad (Wazuh Inc., s.f.).

El uso de estas herramientas facilita la supervisión continua del entorno, ayuda a generar alertas tempranas y permite responder de manera más eficiente ante posibles amenazas o intentos de intrusión. Estas herramientas permiten detectar amenazas en tiempo real y aplicar mecanismos de contención orientados a minimizar el impacto de posibles incidentes informáticos.

Diferencias entre Red Team y Blue Team

Aunque ambos equipos forman parte de las estrategias de ciberseguridad organizacional, sus funciones presentan enfoques diferentes. El Red Team trabaja desde una perspectiva ofensiva, simulando ataques controlados con el objetivo de identificar vulnerabilidades presentes en la infraestructura tecnológica.

Por otro lado, el Blue Team desarrolla actividades defensivas enfocadas en la detección y mitigación de amenazas informáticas mediante monitoreo continuo y aplicación de controles de seguridad.

Mientras el Red Team busca explotar vulnerabilidades para evaluar el nivel de exposición de los sistemas, el Blue Team implementa mecanismos de protección orientados a corregir las debilidades identificadas y fortalecer la seguridad organizacional.

La interacción entre ambos equipos permite generar procesos de mejora continua dentro de las organizaciones, incrementando la capacidad de respuesta frente a amenazas cibernéticas.

Importancia del pentesting

Las pruebas de penetración o pentesting constituyen una metodología utilizada para identificar vulnerabilidades presentes en sistemas, aplicaciones y redes mediante simulaciones controladas de ataques reales.

El objetivo principal del pentesting consiste en detectar fallos de seguridad antes de que puedan ser aprovechados por atacantes externos, permitiendo implementar medidas correctivas de manera preventiva.

El proceso de pentesting generalmente se desarrolla en varias fases que permiten evaluar la seguridad de un sistema de manera estructurada. Estas etapas incluyen el reconocimiento inicial, donde se recopila información del objetivo; el escaneo y la enumeración de servicios, con el fin de identificar posibles puntos vulnerables; la explotación controlada de las debilidades encontradas; la fase de post explotación, en la que se analiza el alcance del acceso obtenido; y finalmente la elaboración de informes técnicos donde se documentan los hallazgos, riesgos identificados y recomendaciones de mejora.

Durante la etapa de reconocimiento se recopila información sobre los sistemas objetivo, incluyendo direcciones IP, dominios y servicios activos. Posteriormente, mediante técnicas de escaneo y enumeración se identifican puertos abiertos y configuraciones inseguras que podrían representar riesgos para la organización.

La explotación permite validar si las vulnerabilidades identificadas pueden ser aprovechadas para obtener acceso no autorizado a los sistemas. Finalmente, los resultados

obtenidos son documentados en informes técnicos orientados a la implementación de controles de seguridad y estrategias de mitigación.

Herramientas utilizadas en pruebas de penetración

Nmap

Nmap es una herramienta utilizada para el escaneo y análisis de redes. Su principal función consiste en identificar dispositivos conectados, puertos abiertos y servicios activos dentro de una infraestructura tecnológica.

Esta herramienta resulta fundamental durante la fase de reconocimiento debido a que permite obtener información detallada sobre los sistemas evaluados y detectar posibles puntos de entrada.

Metasploit Framework

Metasploit es una plataforma especializada en pruebas de penetración utilizada para validar vulnerabilidades mediante explotación controlada. Esta herramienta facilita la simulación de ataques reales y permite evaluar el impacto que podría generar una vulnerabilidad explotada exitosamente.

OpenVAS

OpenVAS es un escáner de vulnerabilidades orientado a identificar fallos de seguridad presentes en sistemas y aplicaciones. Su funcionamiento se basa en el análisis de configuraciones inseguras y vulnerabilidades conocidas dentro de la infraestructura tecnológica.

Wireshark

Wireshark es una herramienta de análisis de tráfico de red utilizada para capturar y examinar paquetes de información transmitidos dentro de una red. Su implementación permite

identificar comportamientos anómalos y analizar eventos relacionados con incidentes de seguridad informática.

Burp Suite

Burp Suite es una plataforma especializada en pruebas de seguridad para aplicaciones web. Esta herramienta permite analizar solicitudes HTTP, detectar vulnerabilidades web y realizar pruebas relacionadas con autenticación, sesiones y manipulación de parámetros.

Importancia de la ciberseguridad en las organizaciones

La ciberseguridad representa un componente estratégico para las organizaciones debido a la necesidad de proteger la información y garantizar la continuidad operativa de los servicios tecnológicos.

Los incidentes de seguridad informática pueden generar afectaciones económicas, interrupciones operativas y daños reputacionales significativos. Por esta razón, resulta indispensable implementar políticas de seguridad, estrategias de monitoreo continuo y mecanismos de gestión de riesgos que permitan fortalecer la infraestructura tecnológica.

Asimismo, la capacitación constante del personal y la actualización de sistemas constituyen medidas fundamentales para reducir la exposición frente a amenazas cibernéticas cada vez más sofisticadas.

La combinación de estrategias ofensivas y defensivas mediante la participación de equipos Red Team y Blue Team permite a las organizaciones evaluar continuamente su nivel de seguridad y mejorar su capacidad de respuesta frente a posibles ataques informáticos.

La ciberseguridad requiere la aplicación de controles orientados a proteger la confidencialidad, integridad y disponibilidad de la información, principios fundamentales para garantizar una adecuada gestión de los activos tecnológicos (Whitman & Mattord, 2022).

Marco legal y ético en ciberseguridad

Importancia del marco legal en ciberseguridad

El crecimiento de amenazas informáticas y el incremento de ataques cibernéticos han generado la necesidad de establecer normas y regulaciones orientadas a proteger la información y garantizar el uso adecuado de los recursos tecnológicos.

Dentro del ámbito de la ciberseguridad, el marco legal cumple una función fundamental debido a que permite definir responsabilidades, establecer sanciones y regular las actividades relacionadas con el manejo de información digital y pruebas de seguridad informática.

La implementación de normas jurídicas orientadas a la protección de datos y prevención de delitos informáticos contribuye al fortalecimiento de la confianza digital y al desarrollo seguro de las operaciones organizacionales.

Los marcos de referencia de seguridad permiten establecer procesos organizados para identificar, proteger, detectar, responder y recuperar recursos tecnológicos frente a amenazas cibernéticas (National Institute of Standards and Technology [NIST], 2018).

Asimismo, las regulaciones relacionadas con seguridad informática permiten delimitar el alcance de actividades ofensivas como las pruebas de penetración y análisis de vulnerabilidades, garantizando que estas acciones se desarrollen únicamente bajo autorización y dentro de entornos controlados.

Ley 1273 de 2009

La Ley 1273 de 2009 constituye uno de los principales referentes normativos relacionados con delitos informáticos en Colombia. Esta ley modificó el Código Penal

Colombiano incorporando medidas orientadas a la protección de la información y los datos frente a actividades ilícitas realizadas mediante medios tecnológicos.

Dentro de esta normativa se establecen delitos relacionados con:

- Acceso abusivo a sistemas informáticos.
- Interceptación de datos.
- Daño informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar información.

La implementación de esta legislación busca proteger la confidencialidad, integridad y disponibilidad de la información frente a amenazas informáticas que puedan afectar personas, organizaciones o entidades gubernamentales.

Asimismo, la Ley 1273 establece sanciones económicas y penales para quienes desarrollen actividades ilícitas relacionadas con acceso no autorizado a sistemas informáticos.

Protección de datos personales

La protección de datos personales representa uno de los aspectos más importantes dentro de la seguridad informática debido al gran volumen de información sensible almacenada por las organizaciones en plataformas digitales.

En Colombia, la Ley 1581 de 2012 establece disposiciones relacionadas con el tratamiento y protección de datos personales. Esta normativa reconoce el derecho que tienen las personas a conocer, actualizar y rectificar la información almacenada en bases de datos públicas o privadas.

Entre los principios fundamentales relacionados con la protección de datos se encuentran la legalidad, finalidad, libertad, transparencia, seguridad, confidencialidad y control de acceso. Estos principios buscan garantizar que la información sea tratada de manera adecuada, evitando usos no autorizados y asegurando que los datos permanezcan protegidos durante todo su ciclo de vida. Su aplicación dentro de una infraestructura tecnológica permite fortalecer las medidas de seguridad, establecer controles sobre la información y reducir riesgos asociados a accesos indebidos o pérdida de confidencialidad.

Las organizaciones deben implementar mecanismos de protección orientados a prevenir accesos no autorizados, filtraciones de información y pérdida de datos sensibles mediante controles de autenticación, monitoreo y cifrado de información.

Ética profesional en ciberseguridad

La ética profesional constituye un componente esencial dentro del ejercicio de la ciberseguridad debido a que muchas herramientas utilizadas en pruebas de penetración pueden generar impactos significativos sobre los sistemas si son utilizadas de manera indebida.

Los profesionales especializados en seguridad informática deben actuar bajo principios de responsabilidad, integridad y confidencialidad, garantizando que las actividades realizadas tengan fines exclusivamente académicos, preventivos o autorizados por las organizaciones involucradas.

El hacking ético se diferencia de las actividades maliciosas porque se desarrolla dentro de entornos controlados y con autorización previa. Su propósito principal consiste en identificar vulnerabilidades antes de que sean aprovechadas por atacantes reales.

Asimismo, el profesional en ciberseguridad debe evitar realizar acciones que puedan comprometer la seguridad de la información, incluyendo accesos indebidos, divulgación de datos

sensibles, alteraciones no autorizadas en los sistemas o cualquier actividad que afecte la disponibilidad y correcto funcionamiento de los servicios tecnológicos.

Principios de confidencialidad, integridad y disponibilidad

La confidencialidad, integridad y disponibilidad constituyen pilares fundamentales dentro de cualquier estrategia de seguridad informática (Whitman & Mattord, 2022).

La confidencialidad busca garantizar que la información únicamente sea accesible para personas autorizadas, evitando accesos indebidos o filtraciones de datos sensibles.

La integridad permite asegurar que la información no sea modificada de manera no autorizada durante su almacenamiento o transmisión.

Finalmente, la disponibilidad garantiza que los sistemas y servicios tecnológicos permanezcan accesibles para los usuarios autorizados cuando sean requeridos.

La afectación de cualquiera de estos principios puede generar incidentes de seguridad con impactos operativos, económicos y reputacionales significativos para las organizaciones.

Metodologías de pentesting y análisis de vulnerabilidades

Introducción al pentesting

Las pruebas de penetración o pentesting constituyen una metodología utilizada para evaluar la seguridad de sistemas, redes y aplicaciones mediante la simulación controlada de ataques informáticos. Estas pruebas permiten identificar vulnerabilidades presentes dentro de una infraestructura tecnológica antes de que puedan ser aprovechadas por atacantes reales.

El objetivo principal del pentesting consiste en analizar el nivel de exposición de los sistemas y determinar el impacto que podrían generar posibles vulnerabilidades sobre la confidencialidad, integridad y disponibilidad de la información.

Actualmente, las organizaciones implementan pruebas de penetración como parte de sus estrategias de gestión de riesgos y fortalecimiento de la seguridad informática. Estas evaluaciones permiten identificar configuraciones inseguras, servicios vulnerables y debilidades presentes en la infraestructura tecnológica, facilitando la aplicación de medidas correctivas y mecanismos de mitigación.

Las pruebas de penetración permiten evaluar la postura de seguridad de una organización mediante la identificación de vulnerabilidades y la simulación controlada de posibles ataques (Wilkins, 2022).

Asimismo, las pruebas de penetración permiten validar la efectividad de los controles de seguridad implementados por los equipos Blue Team y contribuyen al fortalecimiento de la capacidad de respuesta frente a amenazas cibernéticas.

Fases del pentesting

Las pruebas de penetración generalmente se desarrollan mediante varias fases orientadas a recopilar información, identificar vulnerabilidades y validar posibles escenarios de explotación dentro de un entorno tecnológico.

Reconocimiento

La fase de reconocimiento corresponde al proceso inicial de recopilación de información relacionada con la infraestructura objetivo. Durante esta etapa se identifican direcciones IP, dominios, servicios activos, tecnologías implementadas y posibles puntos de entrada que puedan representar un riesgo para la organización.

El reconocimiento puede desarrollarse mediante técnicas pasivas y activas. Las técnicas pasivas permiten obtener información pública sin interactuar directamente con los sistemas objetivo, mientras que las técnicas activas implican comunicación directa con la infraestructura evaluada.

Esta etapa resulta fundamental debido a que la información recopilada permite planificar las siguientes fases del proceso de pentesting y facilita la identificación de posibles vulnerabilidades.

Escaneo

La fase de escaneo tiene como objetivo identificar puertos abiertos, servicios activos y configuraciones presentes dentro de la infraestructura tecnológica evaluada.

Durante esta etapa se utilizan herramientas especializadas capaces de detectar dispositivos conectados, sistemas operativos y versiones de servicios ejecutándose dentro de la red.

El escaneo permite identificar posibles vulnerabilidades dentro de la infraestructura tecnológica, relacionadas con servicios desactualizados, puertos expuestos, protocolos inseguros y configuraciones incorrectas que podrían representar riesgos para la seguridad del sistema.

Asimismo, esta fase facilita la identificación de vectores de ataque que posteriormente podrían ser utilizados durante la etapa de explotación.

Enumeración

La enumeración corresponde al proceso mediante el cual se obtiene información detallada sobre los servicios identificados durante la fase de escaneo.

En esta etapa se recopilan datos relacionados con los usuarios, recursos compartidos, políticas de autenticación, servicios SMB, configuraciones DNS y versiones específicas de software, con el objetivo de obtener una visión más detallada de la infraestructura evaluada e identificar posibles puntos de riesgo.

La información obtenida durante la enumeración permite identificar vulnerabilidades explotables y facilita el análisis del nivel de exposición de la infraestructura tecnológica.

Explotación

La explotación corresponde a la fase donde se valida si las vulnerabilidades identificadas pueden ser aprovechadas para obtener acceso no autorizado a los sistemas evaluados.

Durante esta etapa se utilizan herramientas y exploits especializados orientados a simular ataques controlados dentro de entornos autorizados.

La explotación de vulnerabilidades permite evaluar el impacto real que una falla de seguridad podría generar sobre una infraestructura tecnológica dentro de un entorno controlado. Esta fase facilita la identificación de riesgos relacionados con accesos remotos, posibles

escalamientos de privilegios, movimientos laterales dentro de la red y exposición de información sensible.

Estas fases permiten analizar progresivamente una infraestructura tecnológica, desde la recopilación inicial de información hasta la validación del impacto de las vulnerabilidades identificadas (Young & Aitel, 2018).

Asimismo, estas actividades deben realizarse bajo criterios éticos y con autorización previa, teniendo como objetivo identificar debilidades y fortalecer los mecanismos de protección sin afectar la disponibilidad ni el funcionamiento de los servicios evaluados.

Post explotación

La post explotación corresponde al conjunto de actividades realizadas después de obtener acceso a un sistema comprometido.

Durante esta etapa se evalúan aspectos relacionados con:

- Persistencia.
- Privilegios obtenidos.
- Acceso a recursos internos.
- Posibles movimientos laterales dentro de la red.

El objetivo principal de esta fase consiste en determinar el impacto que podría generar un atacante real una vez comprometido el sistema objetivo.

Asimismo, la información obtenida durante esta etapa permite formular recomendaciones orientadas al fortalecimiento de la seguridad organizacional.

Elaboración del informe técnico

La elaboración del informe técnico constituye una de las etapas más importantes del proceso de pentesting debido a que consolida todos los hallazgos identificados durante la evaluación de seguridad.

El informe debe contener los elementos necesarios para presentar de manera organizada los resultados obtenidos durante el análisis de seguridad. Para esto, se incluyen las vulnerabilidades identificadas, el nivel de criticidad asociado, los posibles impactos que podrían generarse, las evidencias técnicas recopiladas durante las pruebas, las herramientas utilizadas y las recomendaciones propuestas para disminuir los riesgos encontrados.

Asimismo, el documento debe mantener una estructura clara que facilite la comprensión de los hallazgos identificados y permita establecer acciones correctivas enfocadas en mejorar la seguridad de la infraestructura tecnológica evaluada.

Herramientas utilizadas durante el proceso de análisis

Durante el desarrollo de las pruebas de penetración se implementaron diferentes herramientas especializadas orientadas al análisis de vulnerabilidades, reconocimiento de servicios y validación de fallos de seguridad dentro de la infraestructura tecnológica evaluada.

Kali Linux

Kali Linux proporciona un entorno especializado para pruebas de seguridad, incorporando herramientas orientadas al análisis de vulnerabilidades, pruebas de penetración y auditorías de seguridad (Offensive Security, 2024).

Es una distribución orientada a pruebas de penetración y análisis de seguridad informática. Esta plataforma incluye múltiples herramientas utilizadas para:

- Escaneo de redes.
- Análisis forense.
- Explotación de vulnerabilidades.
- Evaluación de seguridad.

Su implementación permitió desarrollar actividades relacionadas con reconocimiento, enumeración y validación de vulnerabilidades dentro del entorno de laboratorio.

Nmap

Nmap fue utilizado como herramienta principal para el escaneo y análisis de puertos abiertos dentro de la infraestructura tecnológica.

Mediante esta herramienta fue posible obtener información relevante sobre el entorno evaluado, identificando los dispositivos conectados, los servicios activos, las características de los sistemas operativos y las versiones de las aplicaciones presentes en los equipos analizados. Estos resultados permitieron tener una visión más clara de la infraestructura y reconocer posibles puntos de exposición que podrían requerir una revisión desde el enfoque de seguridad defensiva.

La información obtenida durante el escaneo permitió identificar posibles vectores de ataque relacionados con servicios vulnerables expuestos dentro de la red.

Nmap es una de las herramientas más utilizadas para el reconocimiento de redes debido a su capacidad para identificar puertos abiertos, servicios y sistemas operativos presentes en los equipos analizados (Nmap Project, s.f.).

Metasploit Framework

Metasploit Framework fue utilizado para validar vulnerabilidades identificadas durante las fases de reconocimiento y escaneo.

Esta herramienta permitió desarrollar pruebas relacionadas con:

- Explotación controlada.
- Ejecución de payloads.
- Validación de acceso remoto.
- Análisis del impacto asociado a vulnerabilidades críticas.

Asimismo, Metasploit facilitó la simulación de escenarios reales de ataque dentro del entorno controlado de laboratorio.

Wireshark

Wireshark fue utilizado para el análisis y monitoreo del tráfico de red generado durante las pruebas de penetración.

La implementación de esta herramienta permitió realizar la captura y análisis de paquetes de información dentro del entorno evaluado, facilitando la revisión de diferentes comunicaciones de red, protocolos utilizados, procesos de autenticación, transferencia de datos y posibles eventos inusuales. Este análisis contribuyó a identificar comportamientos que podrían estar relacionados con actividades sospechosas o intentos de explotación, permitiendo obtener información útil para fortalecer las medidas de monitoreo y respuesta ante posibles incidentes de seguridad.

Importancia del análisis de vulnerabilidades

El análisis de vulnerabilidades constituye un componente fundamental dentro de cualquier estrategia de ciberseguridad debido a que permite identificar debilidades presentes en

sistemas y aplicaciones antes de que sean explotadas por atacantes externos (Serrano & Muñoz, 2021).

Las vulnerabilidades pueden originarse por diferentes factores, como errores de configuración, servicios desactualizados, malas prácticas de seguridad, aplicaciones con fallas conocidas y deficiencias en los controles de protección implementados, lo que puede aumentar el riesgo de afectación sobre los sistemas y la información.

La identificación temprana de estas debilidades permite implementar medidas correctivas orientadas a reducir la superficie de ataque y fortalecer la seguridad organizacional.

Asimismo, el análisis de vulnerabilidades facilita la priorización de riesgos y contribuye a mejorar los procesos de gestión de seguridad dentro de las organizaciones.

Riesgos asociados a vulnerabilidades críticas

Las vulnerabilidades críticas representan uno de los principales riesgos para las organizaciones debido al impacto que pueden generar sobre la infraestructura tecnológica y la información institucional.

Una vulnerabilidad explotada exitosamente puede generar diferentes afectaciones dentro de una infraestructura tecnológica, dependiendo del nivel de exposición del sistema comprometido. Entre los posibles impactos se encuentran accesos no autorizados, robo o alteración de información, ejecución remota de código malicioso, propagación de malware, interrupción de servicios y afectación de la continuidad operativa de la organización. Estos escenarios resaltan la importancia de identificar y corregir las vulnerabilidades de manera oportuna para reducir los riesgos asociados a posibles ataques.

Por esta razón, resulta indispensable implementar procesos continuos de monitoreo, actualización y fortalecimiento de sistemas que permitan reducir la exposición frente a amenazas cibernéticas.

De igual manera, las organizaciones deben desarrollar estrategias de respuesta a incidentes y planes de contingencia orientados a minimizar el impacto asociado a posibles ataques informáticos.

Análisis técnico del escenario

Descripción del entorno de laboratorio

El entorno de laboratorio implementado para el desarrollo de las actividades del seminario especializado permitió simular escenarios relacionados con análisis ofensivo y defensivo dentro de una infraestructura tecnológica controlada. Este entorno fue diseñado con el propósito de identificar vulnerabilidades, ejecutar pruebas de penetración y aplicar mecanismos de monitoreo y contención frente a posibles amenazas informáticas.

La infraestructura utilizada estuvo compuesta por diferentes máquinas virtuales y herramientas especializadas orientadas a la simulación de ataques y análisis de eventos de seguridad. Entre las plataformas utilizadas se destacan sistemas operativos Linux y Windows configurados dentro de una red de laboratorio destinada al desarrollo de pruebas controladas de ciberseguridad.

Asimismo, el escenario desarrollado permitió llevar a cabo diferentes actividades relacionadas con la evaluación de seguridad de una infraestructura tecnológica, incluyendo el reconocimiento de red, el escaneo de puertos, la identificación de servicios, la validación de vulnerabilidades y el análisis de eventos de seguridad. Estas actividades permitieron aplicar conocimientos asociados a los enfoques Red Team y Blue Team, comprendiendo tanto la identificación de posibles puntos de ataque como la implementación de medidas orientadas a fortalecer la protección del entorno evaluado.

La implementación de este entorno facilitó la integración de estrategias Red Team y Blue Team mediante ejercicios prácticos orientados al fortalecimiento de competencias técnicas relacionadas con seguridad informática ofensiva y defensiva.

Reconocimiento y análisis inicial de la red

La primera fase del análisis técnico correspondió al proceso de reconocimiento de la infraestructura tecnológica con el objetivo de identificar dispositivos activos, servicios expuestos y posibles puntos de acceso dentro de la red evaluada.

Durante esta etapa se utilizaron herramientas de escaneo y reconocimiento orientadas a recopilar información relacionada con:

- Direcciones IP activas.
- Puertos abiertos.
- Servicios disponibles.
- Sistemas operativos identificados dentro del entorno de laboratorio.

El reconocimiento inicial permitió establecer una visión general de la infraestructura tecnológica y facilitó la identificación de posibles vectores de ataque relacionados con servicios vulnerables o configuraciones inseguras.

Asimismo, esta etapa permitió identificar servicios asociados al protocolo SMB, los cuales posteriormente fueron analizados debido a la presencia de vulnerabilidades críticas relacionadas con ejecución remota de código.

Escaneo de puertos mediante Nmap

Para el análisis de la infraestructura tecnológica se utilizó la herramienta Nmap con el propósito de identificar puertos abiertos y servicios activos presentes en los equipos evaluados.

El escaneo realizado permitió detectar diferentes servicios ejecutándose dentro del sistema objetivo, incluyendo servicios relacionados con compartición de archivos y comunicación remota.

Entre los principales puertos identificados se encontraron:

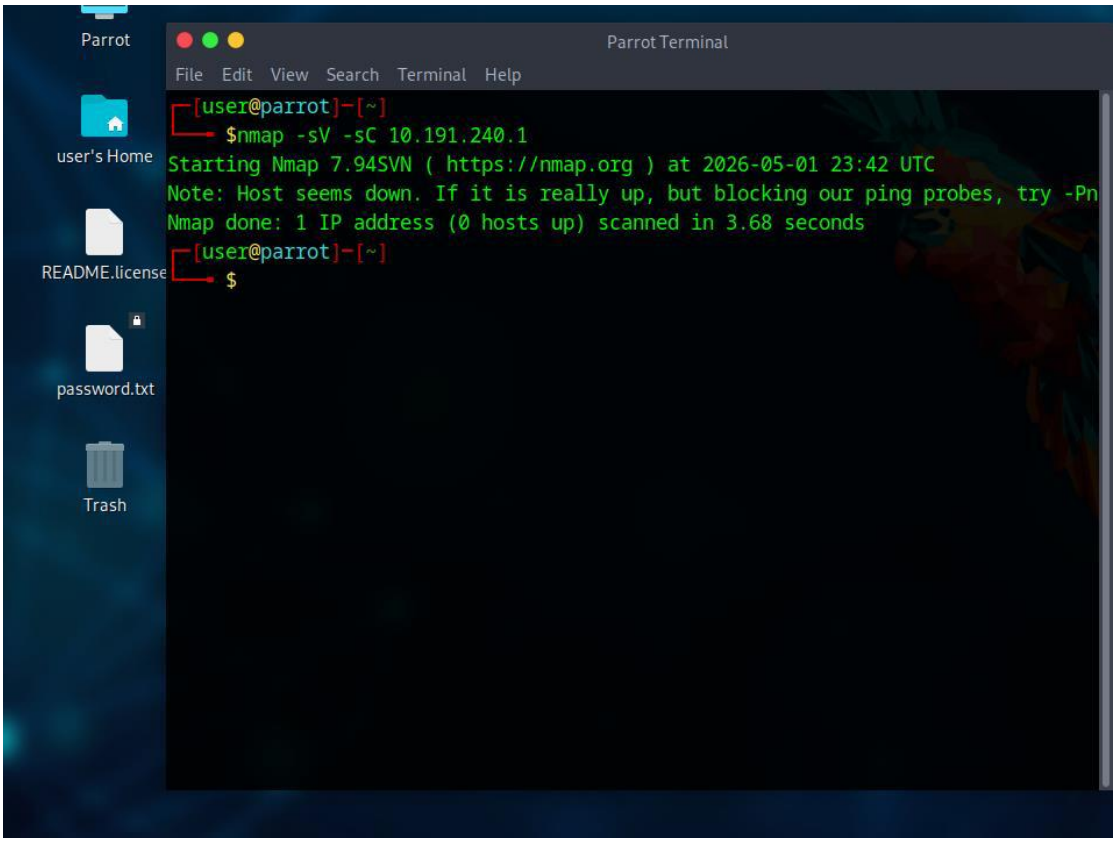
- Puerto 135/TCP
- Puerto 139/TCP
- Puerto 445/TCP

La presencia del puerto 445 asociado al protocolo SMB representó un elemento de interés debido a que este servicio ha sido históricamente relacionado con múltiples vulnerabilidades críticas explotadas por atacantes para obtener acceso remoto no autorizado.

El análisis realizado mediante Nmap permitió obtener información relevante sobre la infraestructura evaluada, incluyendo las versiones de los servicios disponibles, el estado de los puertos identificados, características del sistema operativo y posibles configuraciones que podrían representar riesgos de seguridad dentro del entorno de laboratorio. Estos resultados fueron utilizados como base para orientar las siguientes etapas del análisis, permitiendo identificar puntos de exposición y enfocar la búsqueda de vulnerabilidades presentes en los servicios encontrados.

Figura 1

Resultado del escaneo de puertos realizado mediante Nmap.



Nota. La figura presenta los resultados obtenidos durante la fase inicial de reconocimiento utilizando la herramienta Nmap. En el análisis se identificaron diferentes puertos abiertos y servicios activos dentro del sistema evaluado, destacando el puerto 445 asociado al protocolo SMB. Este hallazgo permitió establecer posibles puntos de exposición en la red y orientar las siguientes pruebas hacia la búsqueda de vulnerabilidades relacionadas con dicho servicio. Elaboración propia.

Identificación de vulnerabilidad MS17-010

Durante el proceso de análisis se identificó la presencia de la vulnerabilidad MS17-010 relacionada con el protocolo SMBv1 implementado en sistemas Windows.

Esta vulnerabilidad permite la ejecución remota de código debido a fallos presentes en el manejo de solicitudes SMB, lo que posibilita que un atacante ejecute comandos maliciosos sobre el sistema objetivo sin necesidad de autenticación previa.

La vulnerabilidad MS17-010 fue ampliamente conocida debido a su utilización en ataques masivos como WannaCry y NotPetya, los cuales generaron afectaciones significativas a nivel mundial.

El análisis técnico permitió identificar que el sistema objetivo presentaba configuraciones vulnerables relacionadas con versiones desactualizadas del servicio SMB, incrementando el riesgo de explotación remota.

Asimismo, la detección de esta vulnerabilidad evidenció la importancia de implementar políticas de actualización y gestión de parches orientadas a reducir la exposición frente a amenazas cibernéticas.

Tabla 1

Vulnerabilidades

Vulnerabilidad	Descripción	Servicio afectado	Nivel de riesgo	Impacto potencial	Recomendación
MS17-010 (EternalBlue)	Vulnerabilidad crítica presente en SMBv1 que permite ejecución remota de	SMBv1 – Puerto 445/TCP	Crítico	Compromiso total del sistema, propagación de malware y	Aplicar parches de seguridad y deshabilitar SMBv1.

	código sin autenticación previa.			acceso remoto no autorizado.	
Protocolo SMBv1 habilitado	Uso de un protocolo obsoleto con múltiples vulnerabilidades conocidas.	SMB	Alto	Exposición frente a ataques de ejecución remota y propagación lateral.	Deshabilitar SMBv1 y utilizar versiones seguras del protocolo.
Puertos críticos expuestos	Existencia de puertos accesibles desde la red sin restricciones adecuadas.	135, 139 y 445/TCP	Alto	Facilita reconocimiento y explotación de servicios vulnerables.	Implementar reglas de firewall y segmentación de red.
Falta de actualización del sistema	Sistema operativo sin parches recientes de seguridad.	Sistema Windows	Crítico	Incrementa la exposición frente a exploits conocidos.	Implementar gestión continua de actualizaciones y parches.

Configuración insegura de servicios	Servicios ejecutándose con configuraciones por defecto o sin endurecimiento.	Servicios de red	Medio	Posibles accesos no autorizados y aumento de superficie de ataque.	Aplicar hardening y configuraciones seguras.
Ausencia de segmentación de red	Infraestructura sin separación adecuada entre servicios y equipos.	Red interna	Alto	Facilita movimiento lateral de atacantes dentro de la red.	Implementar segmentación y control de tráfico interno.

Nota. La tabla muestra los resultados obtenidos durante la identificación de vulnerabilidades dentro del escenario evaluado. En esta se organizan los hallazgos encontrados, indicando el servicio relacionado, el nivel de riesgo que representa, las posibles consecuencias y las acciones recomendadas para disminuir la probabilidad de afectación. Elaboración propia.

Durante el análisis se identificó que la vulnerabilidad MS17-010 asociada al servicio SMBv1 representa uno de los riesgos más relevantes, debido a que puede comprometer un sistema que no tenga las actualizaciones de seguridad aplicadas. También se encontraron otros factores que aumentan la exposición de la infraestructura, como el uso de protocolos antiguos, puertos disponibles y configuraciones que requieren fortalecimiento.

Las medidas propuestas buscan reducir los riesgos encontrados mediante la actualización de los sistemas, la eliminación de servicios innecesarios, el control del tráfico de red y la aplicación de configuraciones más seguras. Estas acciones ayudan a mejorar la protección de la infraestructura y facilitan la labor de monitoreo y respuesta desde el enfoque del Blue Team.

Explotación de vulnerabilidad mediante Metasploit

Con el propósito de validar el impacto asociado a la vulnerabilidad identificada, se implementó Metasploit Framework como herramienta de explotación controlada dentro del entorno de laboratorio.

La utilización de Metasploit permitió ejecutar pruebas orientadas a verificar si la vulnerabilidad MS17-010 podía ser aprovechada para obtener acceso remoto al sistema objetivo.

Durante el proceso de explotación se configuraron módulos especializados relacionados con EternalBlue, exploit ampliamente conocido por aprovechar fallos presentes en SMBv1.

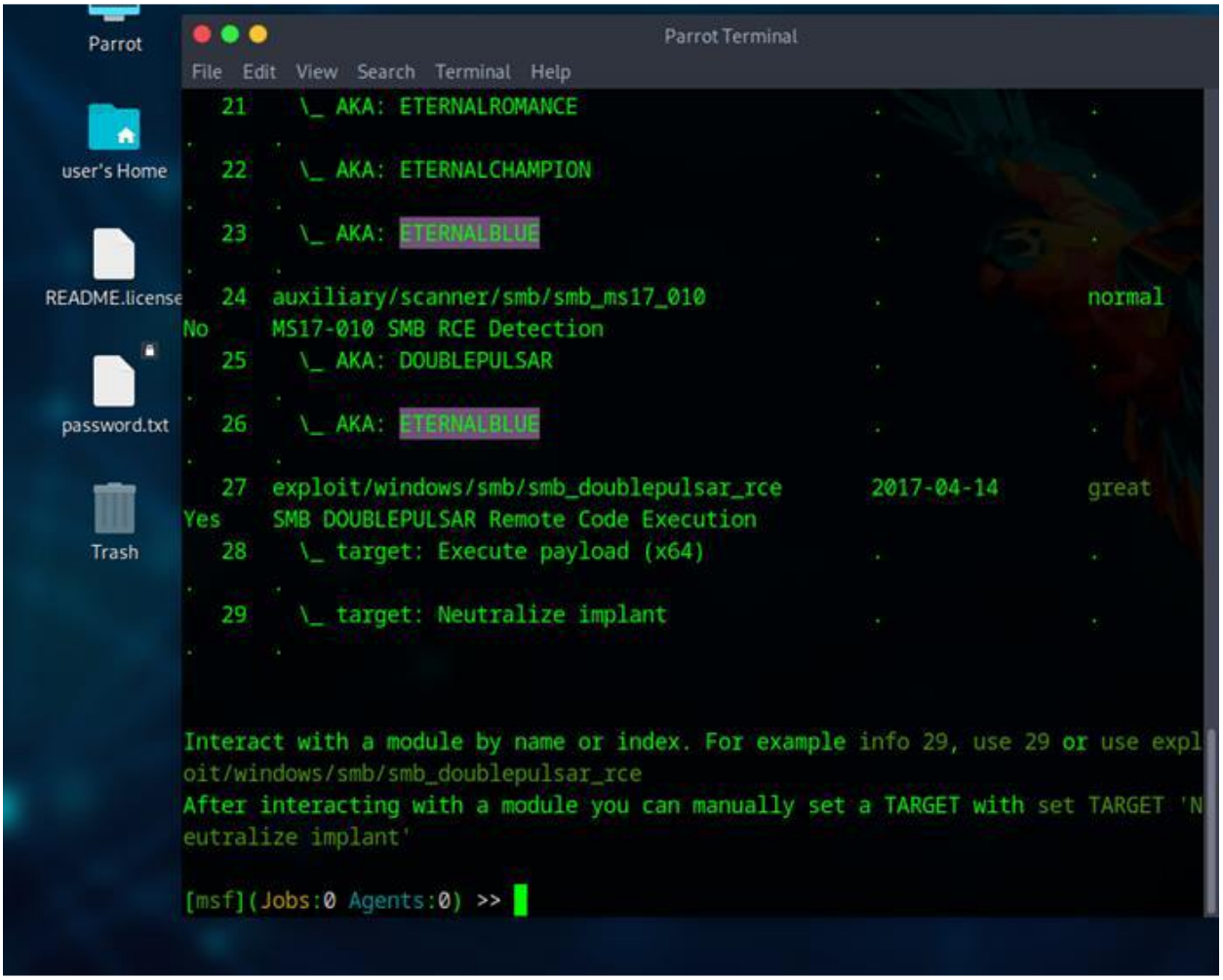
La ejecución controlada del exploit permitió obtener acceso al sistema vulnerable, evidenciando el impacto crítico asociado a la falta de actualización y endurecimiento de servicios expuestos dentro de la red.

Asimismo, este análisis permitió comprender la importancia de implementar controles de seguridad orientados a:

- Segmentación de red.
- Gestión de parches.
- Monitoreo continuo.
- Deshabilitación de protocolos inseguros.

Figura 2

Proceso de explotación realizado mediante Metasploit Framework.



Nota. En la figura se observa el proceso realizado mediante Metasploit Framework para validar la vulnerabilidad identificada previamente. La ejecución de esta prueba permitió comprobar en un ambiente controlado si el servicio detectado podía ser comprometido. Este procedimiento fue

importante para analizar el impacto que podría generar una configuración insegura dentro de una infraestructura tecnológica. Elaboración propia.

Análisis del impacto de la explotación

La explotación controlada de la vulnerabilidad MS17-010 permitió evidenciar el alto nivel de riesgo asociado a servicios desactualizados y protocolos inseguros presentes dentro de la infraestructura tecnológica evaluada.

Una vez obtenido acceso al sistema vulnerable mediante Metasploit Framework, fue posible validar el impacto que puede generar la explotación de una vulnerabilidad dentro de un entorno controlado. Durante esta etapa se identificaron escenarios asociados a la ejecución remota de comandos, accesos no autorizados, posible compromiso del sistema objetivo y riesgos relacionados con movimientos laterales dentro de la red. Estos resultados permitieron comprender la importancia de aplicar controles preventivos y medidas de seguridad que reduzcan la posibilidad de que un atacante pueda ampliar su alcance dentro de la infraestructura.

El análisis realizado permitió identificar que un atacante con acceso exitoso podría comprometer la confidencialidad, integridad y disponibilidad de la información almacenada en el sistema afectado.

Asimismo, la explotación evidenció riesgos asociados con:

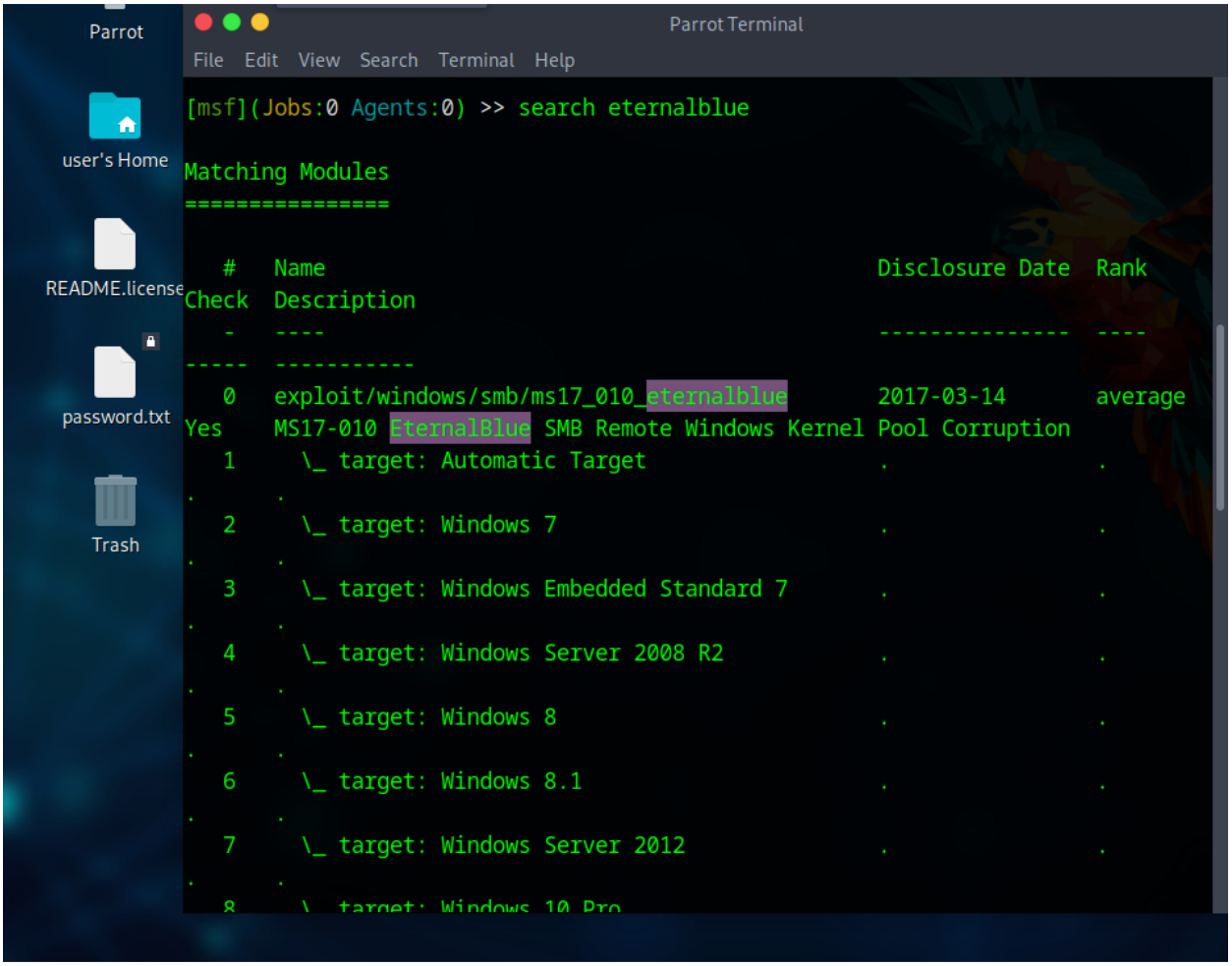
- Propagación de malware.
- Robo de información sensible.
- Interrupción de servicios.
- Escalamiento de privilegios.

La presencia de servicios vulnerables expuestos dentro de la red representa una amenaza significativa para las organizaciones debido a que facilita la ejecución de ataques automatizados

capaces de propagarse rápidamente entre diferentes dispositivos conectados a la infraestructura tecnológica.

Figura 3

Acceso obtenido mediante explotación de vulnerabilidad MS17-010.



Nota. La figura evidencia el resultado obtenido después de realizar la explotación controlada de la vulnerabilidad MS17-010. La prueba permitió demostrar que un sistema sin las actualizaciones de seguridad necesarias puede quedar expuesto a accesos no autorizados. Este resultado permitió analizar el riesgo asociado al uso de servicios vulnerables y la importancia de aplicar medidas preventivas. Elaboración propia.

Riesgos asociados a EternalBlue

EternalBlue es uno de los exploits más conocidos dentro del ámbito de la ciberseguridad debido al impacto generado por su utilización en ataques cibernéticos a nivel mundial.

Este exploit aprovecha vulnerabilidades presentes en SMBv1 para ejecutar código malicioso de manera remota sobre sistemas Windows vulnerables. Su utilización permitió la propagación de amenazas como WannaCry y NotPetya, afectando organizaciones gubernamentales, entidades financieras y empresas privadas (Palo Alto Networks, 2024).

Entre los principales riesgos asociados a EternalBlue se encuentran:

- Ejecución remota de código.
- Propagación automática dentro de redes corporativas.
- Compromiso masivo de equipos.
- Cifrado de información.
- Afectación de la continuidad operativa.

Asimismo, la explotación de este tipo de vulnerabilidades evidencia la importancia de implementar mecanismos de actualización y monitoreo continúo orientados a reducir la exposición frente a amenazas cibernéticas avanzadas.

La vulnerabilidad MS17-010 fue catalogada como crítica por Microsoft debido a la posibilidad de ejecución remota de código a través del protocolo SMB, afectando principalmente sistemas Windows sin las actualizaciones de seguridad correspondientes (Microsoft, 2017).

La existencia de protocolos obsoletos y sistemas desactualizados incrementa significativamente el riesgo de compromiso de la infraestructura tecnológica, especialmente en entornos donde no existen políticas adecuadas de gestión de parches y segmentación de red.

Análisis de superficie de ataque

La superficie de ataque corresponde al conjunto de puntos de acceso y servicios expuestos que podrían ser utilizados por un atacante para comprometer la infraestructura tecnológica de una organización.

Durante el análisis realizado se identificaron diferentes elementos que incrementaban la exposición del entorno evaluado, incluyendo:

- Puertos abiertos.
- Protocolos inseguros.
- Servicios vulnerables.
- Configuraciones deficientes de seguridad.

La presencia de servicios SMB expuestos dentro de la red representó uno de los principales riesgos detectados durante el proceso de evaluación debido a las vulnerabilidades críticas asociadas a este protocolo.

Asimismo, la falta de segmentación de red y endurecimiento de servicios incrementó la posibilidad de movimiento lateral y propagación de amenazas dentro del entorno tecnológico.

El análisis de la superficie de ataque permitió comprender la importancia de implementar estrategias defensivas orientadas a disminuir los puntos de exposición de la infraestructura tecnológica. Entre las principales medidas identificadas se encuentran la reducción de servicios innecesarios, la aplicación de reglas de firewall, la segmentación adecuada de la red, el monitoreo constante de eventos y la actualización permanente de los sistemas. Estas acciones contribuyen a limitar posibles accesos no autorizados y fortalecen la capacidad de prevención y respuesta ante amenazas de seguridad.

Importancia del monitoreo durante el análisis ofensivo

El monitoreo de eventos de seguridad constituye un componente fundamental durante el desarrollo de pruebas de penetración debido a que permite identificar actividades sospechosas y evaluar el comportamiento de los sistemas frente a posibles escenarios de ataque.

Durante las actividades realizadas fue posible analizar eventos relacionados con:

- conexiones de red,
- intentos de acceso,
- ejecución de procesos,
- tráfico sospechoso,
- y generación de alertas de seguridad.

El monitoreo continuo facilita la detección temprana de incidentes y contribuye al fortalecimiento de las capacidades defensivas de la organización.

Asimismo, la correlación de eventos de seguridad permite identificar patrones asociados a actividades maliciosas y facilita la respuesta frente a posibles amenazas cibernéticas.

La integración entre actividades Red Team y mecanismos de monitoreo Blue Team representa una estrategia fundamental para evaluar el nivel de madurez de seguridad dentro de entornos organizacionales.

Relevancia del análisis técnico en ciberseguridad

El análisis técnico desarrollado durante el ejercicio permitió comprender la importancia de implementar estrategias ofensivas y defensivas orientadas a la identificación temprana de vulnerabilidades y fortalecimiento de la infraestructura tecnológica.

Las pruebas realizadas evidenciaron cómo servicios desactualizados y configuraciones inseguras pueden ser aprovechados por atacantes para comprometer sistemas y acceder de manera no autorizada a información sensible.

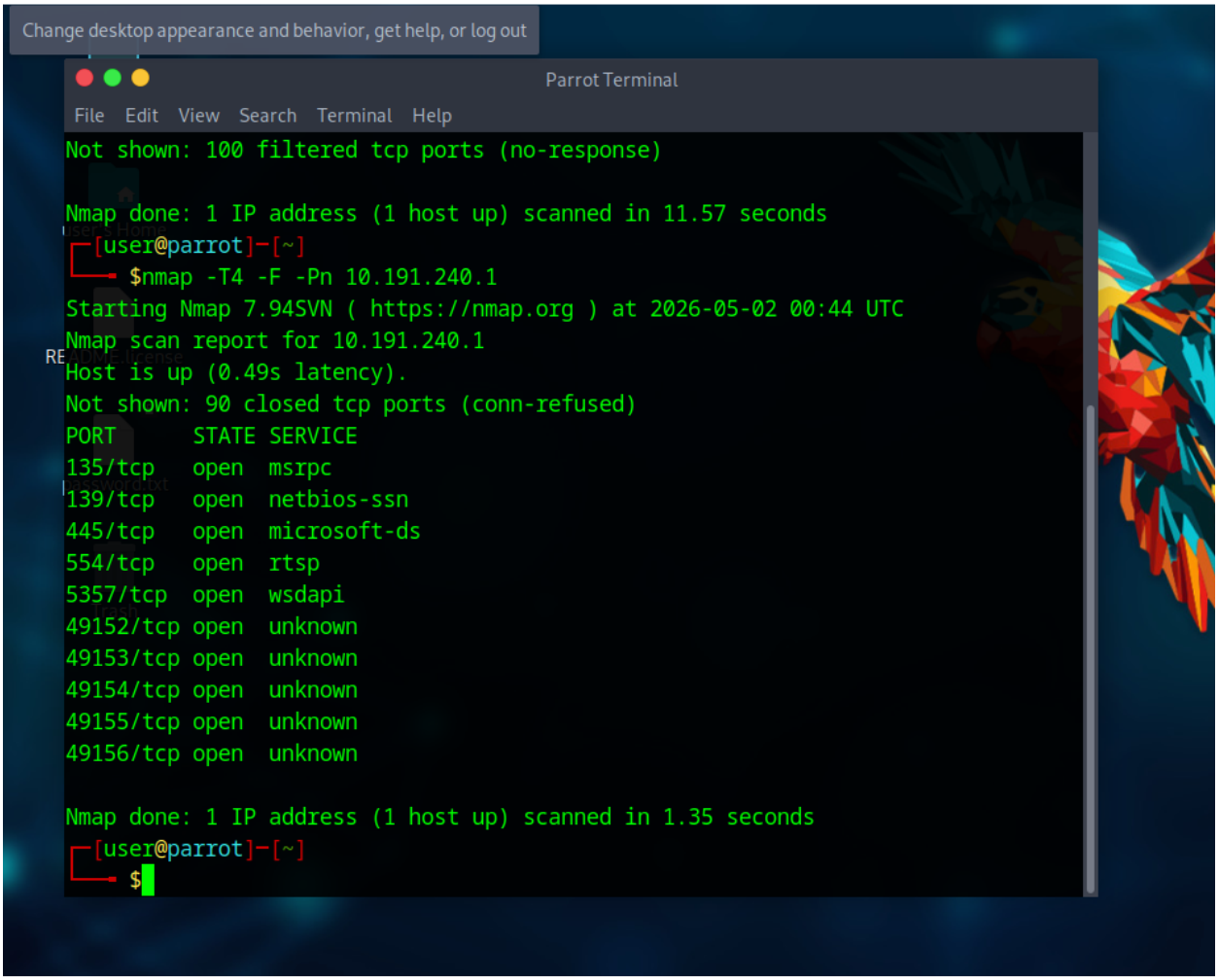
El desarrollo de las actividades relacionadas con las fases de reconocimiento, explotación y monitoreo permitió fortalecer conocimientos técnicos asociados al análisis de vulnerabilidades, la ejecución de pruebas de penetración, la identificación de riesgos y la respuesta ante posibles incidentes de seguridad. Estas actividades ayudaron a comprender la importancia de evaluar continuamente los sistemas para identificar debilidades y establecer medidas preventivas antes de que puedan ser aprovechadas.

Finalmente, el proceso realizado permitió reconocer la importancia de implementar controles de seguridad orientados a reducir la exposición de la infraestructura frente a posibles amenazas. Entre las principales medidas identificadas se encuentran la gestión adecuada de parches, la segmentación de red, el monitoreo constante de eventos, el fortalecimiento de configuraciones mediante hardening y la aplicación de políticas de seguridad que permitan mejorar la protección de los recursos tecnológicos.

Evidencias técnicas del proceso de explotación

Figura 4

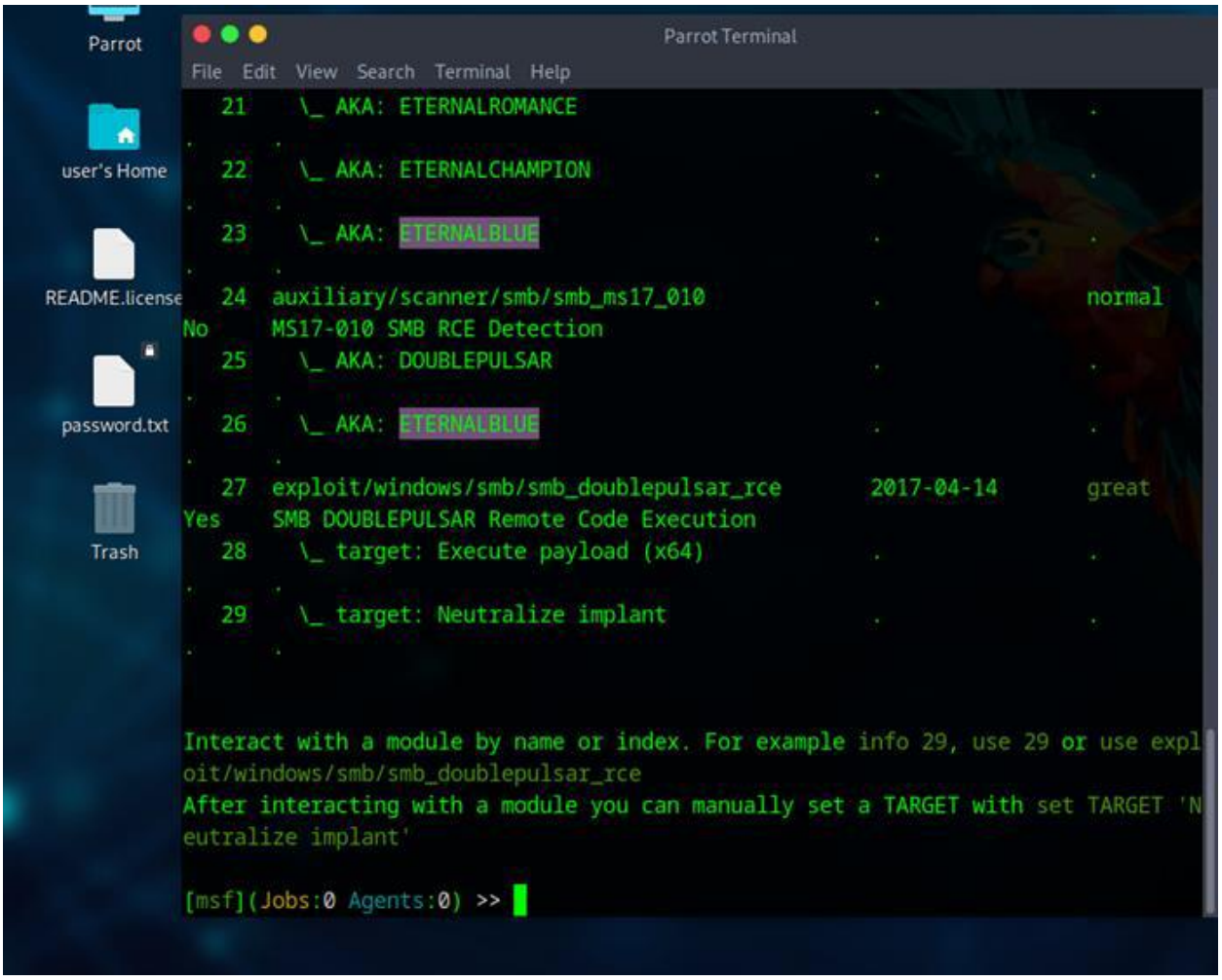
Resultado del escaneo



Nota. Los resultados obtenidos permitieron identificar la presencia del puerto 445 asociado al protocolo SMB. Este hallazgo fue especialmente relevante debido a que dicho servicio ha estado relacionado con vulnerabilidades críticas que han sido aprovechadas en múltiples ataques informáticos. La identificación de este puerto permitió enfocar el análisis en la búsqueda de posibles fallos de seguridad asociados al servicio y evaluar el nivel de exposición del sistema frente a amenazas conocidas. Elaboración propia.

Figura 5

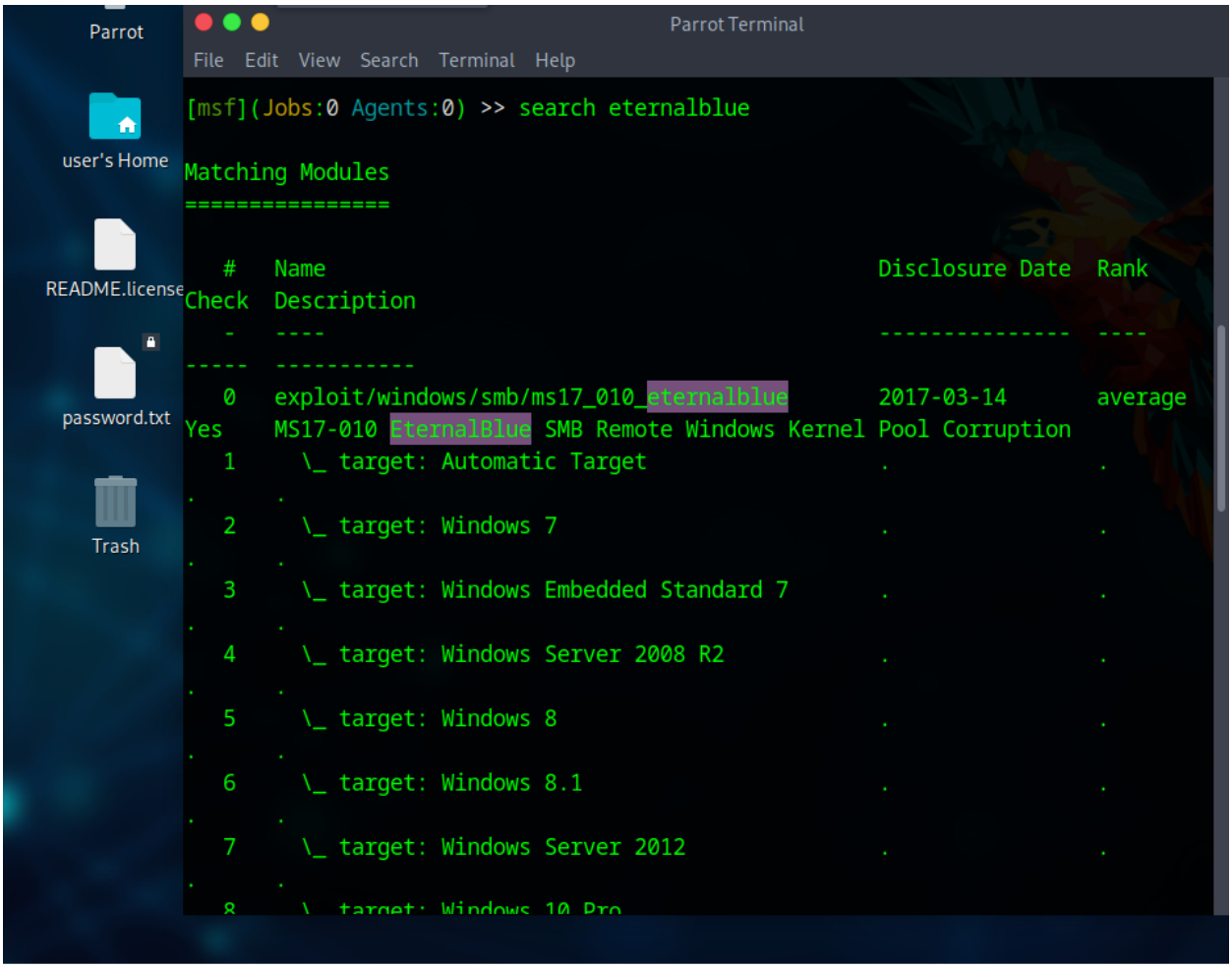
Búsqueda del exploit



Nota. En esta etapa se realizó la consulta de los módulos disponibles dentro de Metasploit Framework con el propósito de identificar exploits compatibles con las características del sistema analizado. Este procedimiento permitió verificar la existencia de herramientas capaces de aprovechar vulnerabilidades relacionadas con SMB. La búsqueda y selección adecuada del exploit representa una fase importante dentro de las pruebas de penetración, ya que de ello depende la efectividad y validez técnica de la explotación posterior. Elaboración propia.

Figura 6

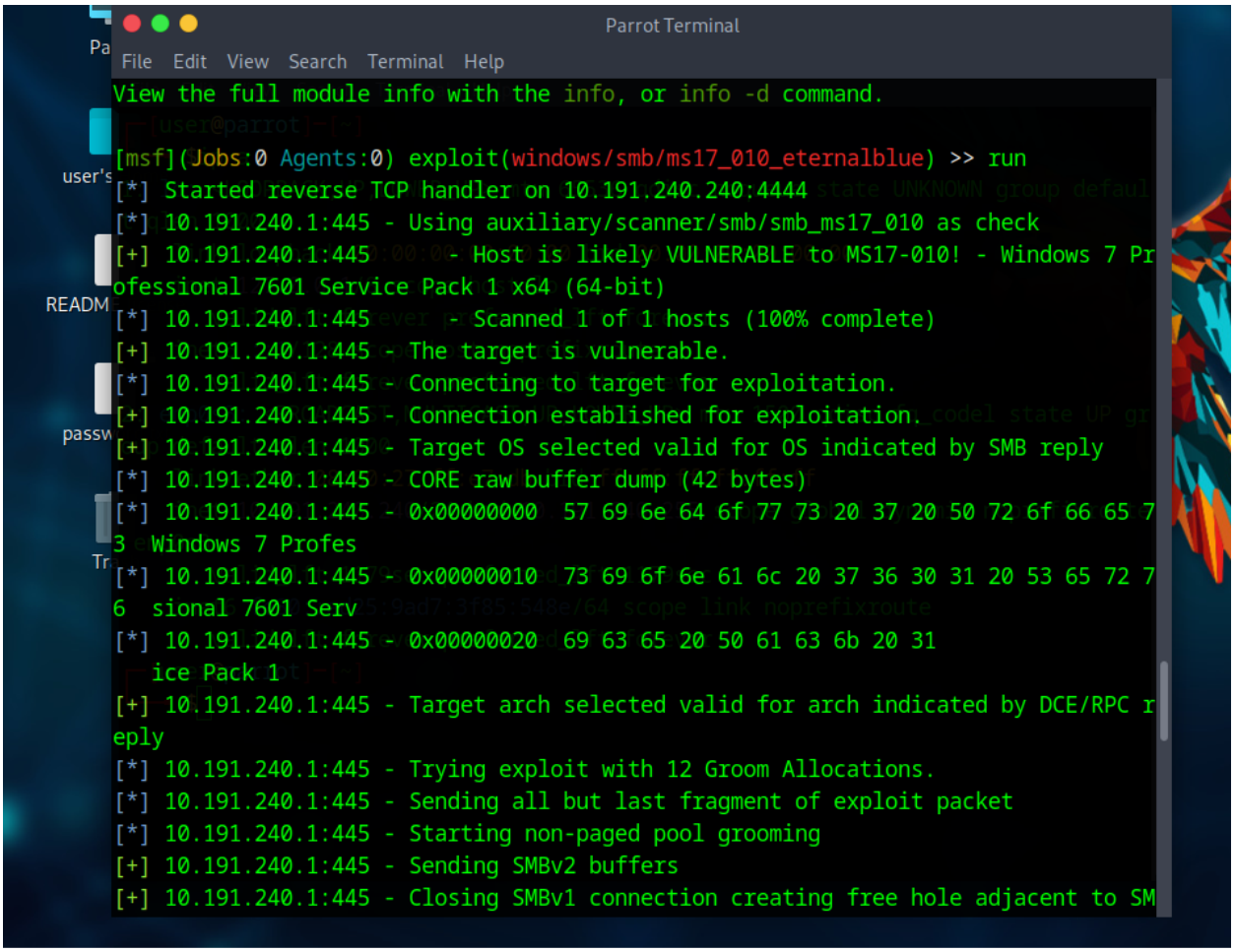
Ejecución del exploit



Nota. La captura evidencia la configuración de los parámetros necesarios para ejecutar el exploit MS17-010 sobre el sistema objetivo. Durante esta fase se definieron aspectos como la dirección IP de la máquina vulnerable y el payload que sería utilizado durante la prueba. Este procedimiento permitió validar de manera controlada la posibilidad de explotación de la vulnerabilidad identificada previamente y medir el nivel de riesgo asociado a la misma. Elaboración propia.

Figura 7

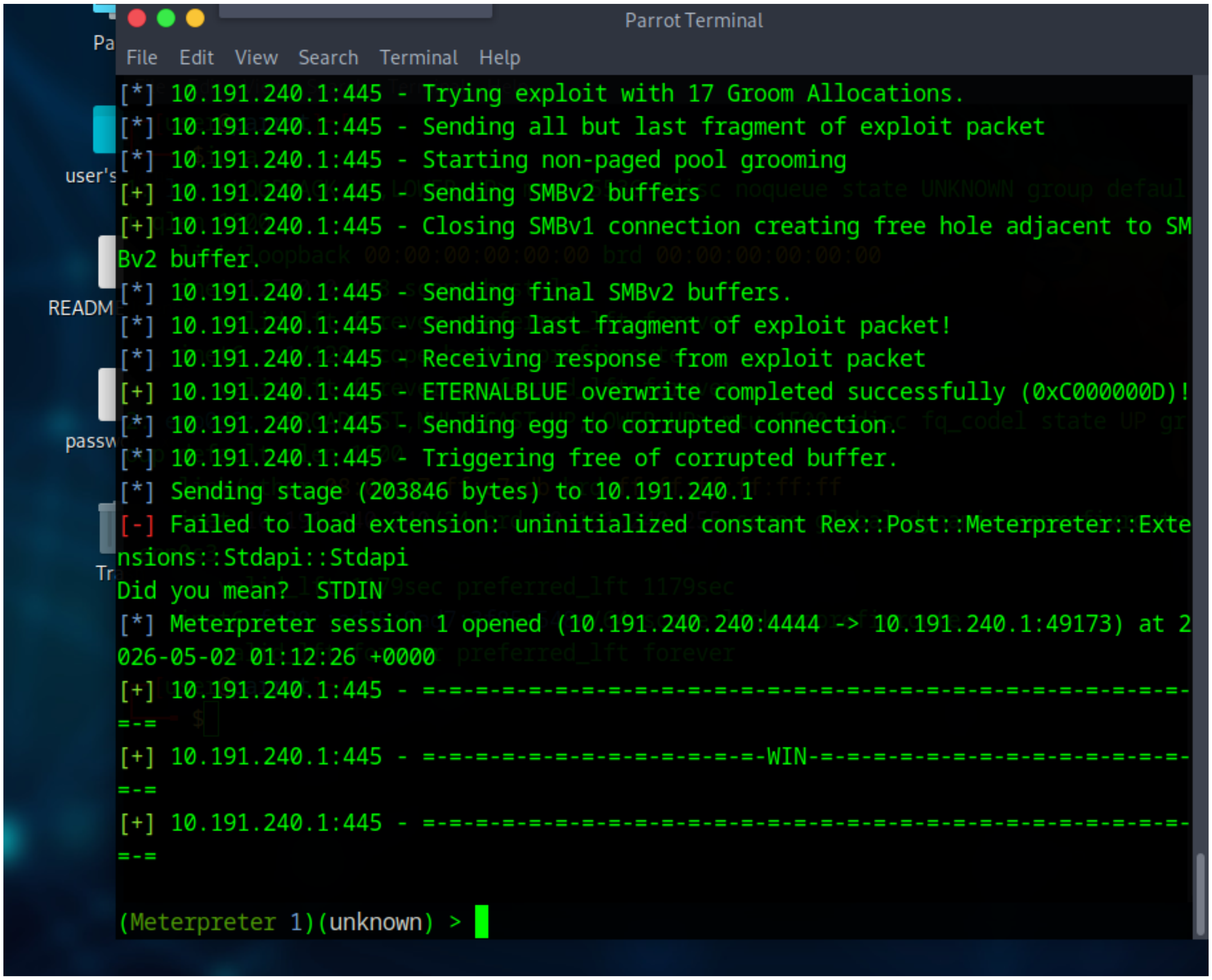
Explotación contra Windows 7



Nota. La evidencia demuestra la ejecución del exploit sobre un sistema Windows 7 vulnerable. El resultado obtenido permitió confirmar la existencia de la vulnerabilidad y evidenciar cómo un sistema sin las actualizaciones de seguridad correspondientes puede ser comprometido mediante técnicas ampliamente conocidas dentro del ámbito de la ciberseguridad. Este escenario permitió comprender la importancia de la gestión de parches y la actualización permanente de los sistemas operativos. Elaboración propia.

Figura 8

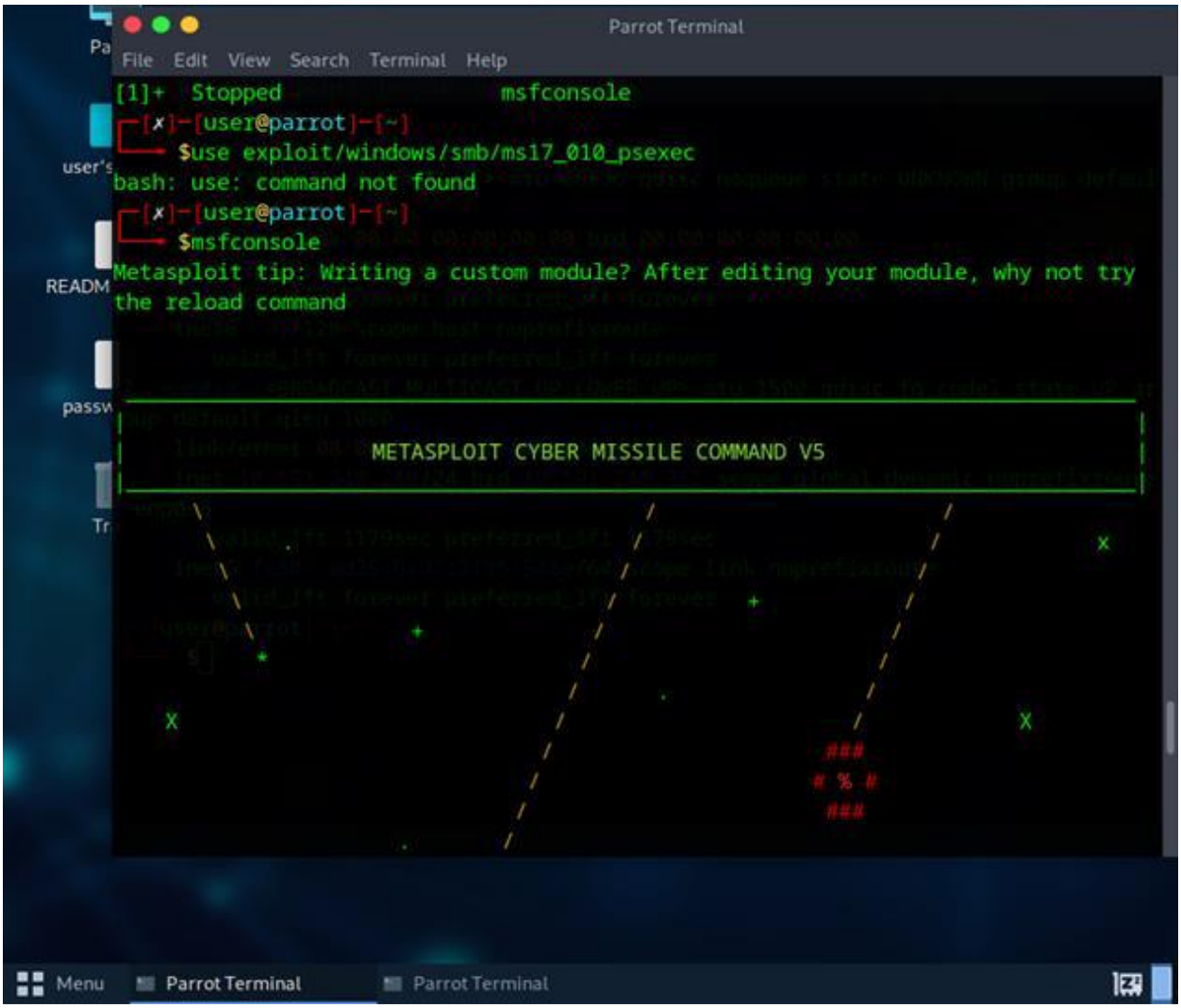
Éxito en la explotación del puerto 445



Nota. La apertura de una sesión Meterpreter confirmó el éxito de la explotación realizada sobre el sistema objetivo. Este resultado evidencia el impacto que puede generar una vulnerabilidad crítica cuando no se implementan mecanismos adecuados de protección. Asimismo, permitió analizar las capacidades que podría obtener un atacante una vez comprometido el equipo, incluyendo la ejecución de comandos, acceso a información y posible desplazamiento hacia otros sistemas dentro de la red. Elaboración propia.

Figura 9

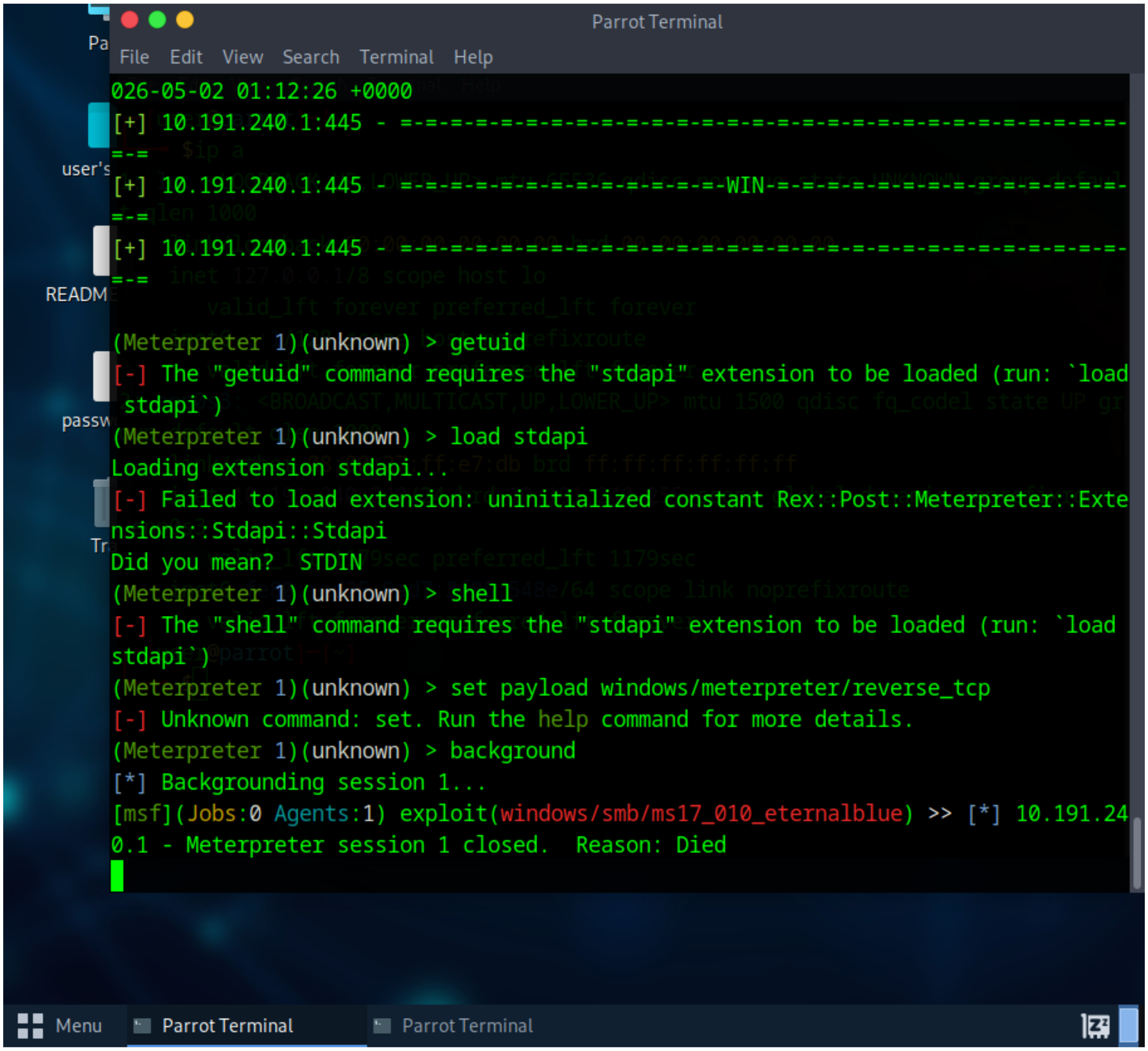
Dificultades durante la explotación



Nota. Durante el desarrollo de las pruebas se presentaron inconvenientes relacionados con la estabilidad de la conexión y la ejecución de algunos comandos dentro del entorno de Metasploit. Estas situaciones son comunes en ejercicios prácticos de ciberseguridad y forman parte del proceso de aprendizaje. La necesidad de reiniciar servicios y ajustar configuraciones permitió comprender la importancia de la resolución de problemas y la correcta interpretación de los mensajes generados por las herramientas utilizadas. Elaboración propia.

Figura 10

Hallazgos de error



Nota. La captura muestra errores identificados durante la interacción con la sesión obtenida. El análisis de estos eventos permitió evidenciar limitaciones relacionadas con la configuración del entorno de pruebas y la compatibilidad de algunos componentes utilizados durante la explotación. Estos hallazgos contribuyeron al fortalecimiento de las competencias técnicas necesarias para diagnosticar incidentes y corregir problemas operativos durante la ejecución de pruebas de seguridad. Elaboración propia.

Estrategias Blue Team y mecanismos de contención

Función del Blue Team dentro de la seguridad informática

Dentro de una organización, el Blue Team cumple un papel esencial en la protección de los sistemas y la información. Su trabajo se enfoca principalmente en prevenir ataques, monitorear actividades sospechosas y responder ante incidentes que puedan afectar la infraestructura tecnológica.

A diferencia de los procesos ofensivos desarrollados por el Red Team, las actividades del Blue Team están orientadas a fortalecer la seguridad de los equipos y reducir el impacto de posibles amenazas. Esto implica realizar monitoreo constante de la red, analizar registros del sistema y aplicar controles que permitan detectar comportamientos anómalos antes de que generen afectaciones mayores.

Durante el desarrollo del seminario fue posible comprender que la seguridad informática no depende únicamente de identificar vulnerabilidades, sino también de la capacidad que tiene una organización para reaccionar de manera rápida frente a eventos sospechosos. Por esta razón, las estrategias defensivas representan un componente fundamental dentro de cualquier entorno tecnológico.

Además, el Blue Team participa en procesos relacionados con actualización de sistemas, fortalecimiento de configuraciones, implementación de reglas de seguridad y análisis continuo de eventos, permitiendo mejorar el nivel de protección de la infraestructura tecnológica.

Monitoreo y análisis de eventos de seguridad

Uno de los aspectos más importantes dentro de la seguridad defensiva es el monitoreo constante de los sistemas y servicios de red. Este proceso permite identificar comportamientos

inusuales que podrían estar relacionados con accesos no autorizados, intentos de explotación o ejecución de actividades maliciosas dentro de la infraestructura tecnológica.

Durante las actividades realizadas en el entorno de laboratorio se analizaron distintos eventos generados por conexiones de red, autenticaciones y tráfico sospechoso. Esto permitió comprender cómo los registros y alertas pueden convertirse en una fuente importante de información para detectar incidentes de seguridad.

El monitoreo continuo ayuda a identificar patrones anormales y facilita la toma de decisiones frente a posibles amenazas. Además, permite reducir los tiempos de respuesta y mejorar la capacidad de contención cuando ocurre un incidente dentro de la red organizacional (National Institute of Standards and Technology [NIST], 2020).

El monitoreo continuo de la infraestructura permite identificar comportamientos anómalos, analizar eventos y mejorar la capacidad de respuesta ante incidentes de seguridad (Bejtlich, 2013).

En muchos casos, los ataques no son detectados inmediatamente por las organizaciones debido a la ausencia de mecanismos adecuados de supervisión. Por esta razón, las herramientas de monitoreo y correlación de eventos se han convertido en componentes fundamentales dentro de las estrategias modernas de ciberseguridad.

Uso de herramientas de monitoreo defensivo

Durante el desarrollo del ejercicio se trabajó con herramientas orientadas al análisis de eventos y supervisión de la infraestructura tecnológica. Estas plataformas permiten centralizar información relacionada con actividad de usuarios, tráfico de red y eventos generados por los sistemas operativos.

El uso de soluciones de monitoreo facilita la identificación de comportamientos sospechosos y permite generar alertas cuando se detectan actividades fuera de lo normal. Asimismo, estas herramientas ayudan a mejorar la visibilidad sobre lo que ocurre dentro de la red y contribuyen al fortalecimiento de las capacidades defensivas de una organización.

Los sistemas de detección y prevención de intrusiones permiten identificar actividades sospechosas y aplicar mecanismos de protección frente a amenazas conocidas (Northcutt & Novak, 2002).

Otro aspecto importante es que las plataformas de monitoreo permiten almacenar registros históricos que posteriormente pueden utilizarse durante procesos de análisis forense o investigaciones relacionadas con incidentes de seguridad.

Fortalecimiento de sistemas mediante hardening

El hardening corresponde al proceso de aplicar configuraciones de seguridad que permitan reducir vulnerabilidades y limitar posibles vectores de ataque dentro de un sistema informático.

Durante el análisis realizado se evidenció la importancia de deshabilitar servicios innecesarios y corregir configuraciones inseguras presentes dentro de la infraestructura tecnológica. Muchas vulnerabilidades pueden ser aprovechadas debido a configuraciones por defecto o servicios expuestos que no cuentan con medidas adecuadas de protección.

La implementación de mecanismos de endurecimiento permite disminuir considerablemente la superficie de ataque y fortalecer la seguridad de los sistemas frente a amenazas externas. Entre las medidas más importantes se encuentran la actualización permanente del software, restricción de accesos innecesarios y deshabilitación de protocolos inseguros como SMBv1.

Asimismo, el hardening contribuye a mejorar la estabilidad y confiabilidad de la infraestructura tecnológica, especialmente en entornos donde existe exposición constante frente a riesgos relacionados con ataques informáticos.

Implementación de firewalls y control del tráfico de red

Los firewalls representan una de las principales barreras de protección dentro de una infraestructura tecnológica. Su función consiste en controlar el tráfico de red y restringir conexiones que puedan representar un riesgo para los sistemas organizacionales.

Durante el desarrollo del análisis se identificó la importancia de establecer reglas de seguridad capaces de limitar accesos no autorizados y reducir la exposición de servicios críticos frente a posibles ataques externos.

La segmentación de red mediante firewalls permite controlar la comunicación entre diferentes áreas de la infraestructura tecnológica, evitando que una amenaza pueda propagarse fácilmente entre equipos conectados a la red.

Además, la implementación de reglas de filtrado ayuda a bloquear conexiones sospechosas y fortalece significativamente las capacidades defensivas de la organización.

Protección frente a intentos de acceso no autorizado

La protección de accesos constituye un aspecto fundamental dentro de las estrategias de seguridad defensiva debido a que muchos ataques buscan comprometer credenciales o aprovechar mecanismos débiles de autenticación.

Durante el análisis realizado se evidenció la importancia de implementar controles orientados a detectar intentos fallidos de acceso y comportamientos sospechosos relacionados con autenticaciones reiteradas.

Las herramientas de bloqueo automático y monitoreo de autenticaciones permiten reducir riesgos asociados a ataques de fuerza bruta y accesos indebidos a servicios críticos.

Asimismo, el uso de políticas seguras de contraseñas y mecanismos adicionales de autenticación contribuye significativamente al fortalecimiento de la seguridad organizacional.

Importancia de la respuesta y contención de incidentes

La capacidad de respuesta frente a incidentes es uno de los elementos más importantes dentro de cualquier estrategia de ciberseguridad. Una organización no solamente debe enfocarse en prevenir ataques, sino también en actuar rápidamente cuando ocurre un evento de seguridad.

La contención busca limitar el impacto de una amenaza y evitar que esta continúe propagándose dentro de la infraestructura tecnológica. Para ello, es necesario identificar los sistemas afectados, bloquear actividades sospechosas y aplicar medidas orientadas a preservar la continuidad operativa.

Durante el desarrollo del escenario se comprendió la importancia de actuar oportunamente frente a vulnerabilidades críticas y servicios inseguros expuestos dentro de la red.

Asimismo, se evidenció que muchas amenazas pueden minimizarse cuando existen procedimientos claros de monitoreo, respuesta y recuperación frente a incidentes de seguridad informática.

Gestión de actualizaciones y reducción de vulnerabilidades

Uno de los principales factores que incrementan la exposición frente a ataques informáticos es la falta de actualización de sistemas y aplicaciones.

La vulnerabilidad MS17-010 utilizada durante el análisis técnico representa un ejemplo claro de cómo un sistema desactualizado puede convertirse en un objetivo fácil para atacantes que buscan obtener acceso remoto no autorizado.

La implementación de políticas de actualización y gestión de parches permite corregir vulnerabilidades conocidas y reducir significativamente el riesgo de explotación.

Además, mantener actualizados los sistemas ayuda a mejorar la estabilidad de la infraestructura tecnológica y fortalece los controles de seguridad implementados dentro de la organización.

Importancia de las estrategias defensivas en las organizaciones

Las estrategias defensivas desarrolladas por el Blue Team permiten fortalecer la protección de la infraestructura tecnológica y mejorar la capacidad de respuesta frente a amenazas cibernéticas.

El monitoreo continuo, la implementación de firewalls, el análisis de eventos y el fortalecimiento de sistemas representan medidas fundamentales para reducir riesgos relacionados con ataques informáticos y vulnerabilidades críticas.

Asimismo, la integración entre actividades ofensivas y defensivas permite que las organizaciones identifiquen debilidades presentes en sus sistemas y desarrollen mecanismos orientados a mejorar continuamente sus procesos de seguridad.

Finalmente, el trabajo realizado durante el seminario permitió comprender que la ciberseguridad requiere procesos constantes de análisis, monitoreo y actualización, especialmente en entornos donde las amenazas evolucionan de manera permanente.

Gestión de riesgos y recomendaciones de seguridad

Importancia de la gestión de riesgos en ciberseguridad

La gestión de riesgos constituye un proceso esencial para identificar, evaluar y mitigar amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información (NIST, 2020).

Actualmente, las organizaciones enfrentan múltiples riesgos relacionados con ataques informáticos, pérdida de información, accesos no autorizados y explotación de vulnerabilidades críticas. Por esta razón, resulta indispensable implementar procesos orientados a identificar debilidades y establecer mecanismos de protección que permitan reducir la exposición frente a amenazas cibernéticas.

La gestión de riesgos no solamente se enfoca en identificar problemas de seguridad, sino también en analizar el nivel de criticidad asociado a cada vulnerabilidad y priorizar acciones correctivas orientadas a minimizar posibles afectaciones operativas.

Durante el desarrollo del seminario fue posible comprender que muchas amenazas pueden prevenirse mediante estrategias adecuadas de monitoreo, actualización y fortalecimiento de sistemas.

Identificación de riesgos presentes en el entorno analizado

El análisis técnico realizado permitió identificar diferentes riesgos relacionados con servicios vulnerables, configuraciones inseguras y exposición de protocolos críticos dentro de la infraestructura tecnológica evaluada.

Uno de los principales riesgos detectados estuvo relacionado con la presencia de SMBv1 habilitado dentro del sistema Windows analizado. Esta vulnerabilidad representaba un alto nivel de criticidad debido a la posibilidad de explotación remota mediante EternalBlue.

Asimismo, durante el análisis realizado se identificaron diferentes condiciones que pueden aumentar el nivel de exposición de la infraestructura evaluada. Entre ellas se encuentran la falta de actualización de los sistemas, la presencia de puertos críticos accesibles, configuraciones inseguras en algunos servicios, ausencia de una adecuada segmentación de red y debilidades en los controles defensivos implementados. Estos factores pueden facilitar la identificación de puntos vulnerables y aumentar la posibilidad de que un atacante aproveche fallas existentes dentro del entorno tecnológico.

Estas condiciones incrementaban significativamente la superficie de ataque y facilitaban posibles escenarios de explotación por parte de atacantes externos.

El análisis desarrollado permitió evidenciar cómo una infraestructura tecnológica sin controles adecuados puede convertirse en un objetivo vulnerable frente a amenazas informáticas avanzadas.

Evaluación del impacto de las vulnerabilidades

Las vulnerabilidades identificadas durante el ejercicio presentaban diferentes niveles de criticidad dependiendo del impacto potencial que podrían generar sobre la infraestructura tecnológica.

La explotación de vulnerabilidades críticas como MS17-010 podría permitir:

- Acceso remoto no autorizado.
- Ejecución de código malicioso.
- Robo de información.

- Propagación de malware.
- Afectación de servicios organizacionales.

Además del impacto técnico, este tipo de incidentes puede generar consecuencias económicas y reputacionales para las organizaciones, especialmente cuando se compromete información sensible o se afecta la continuidad operativa de los servicios tecnológicos.

La evaluación del impacto permitió comprender la importancia de implementar mecanismos preventivos orientados a reducir riesgos asociados a vulnerabilidades conocidas y servicios inseguros expuestos dentro de la red.

Matriz de riesgos

Tabla 2

Matriz de riesgos identificados durante el análisis técnico.

Riesgo identificado	Probabilidad	Impacto	Nivel de riesgo	Medida de mitigación
Explotación de MS17-010	Alta	Crítico	Crítico	Aplicación de parches y des habilitación de SMBv1
Acceso no autorizado mediante puertos expuestos	Alta	Alto	Alto	Implementación de firewall y segmentación
Propagación de malware en red interna	Media	Alto	Alto	Monitoreo continuo y aislamiento de equipos

Configuraciones inseguras de servicios	Media	Medio	Medio	Hardening y revisión de configuraciones
Falta de actualización de sistemas	Alta	Alto	Alto	Gestión permanente de parches
Movimiento lateral dentro de la red	Media	Alto	Alto	Segmentación y control de tráfico interno

Nota. La tabla presenta los principales riesgos identificados durante el análisis de seguridad realizado sobre la infraestructura evaluada. En ella se relacionan los eventos que pueden afectar la disponibilidad, integridad y confidencialidad de los sistemas, teniendo en cuenta la probabilidad de ocurrencia, el impacto que podrían generar y las medidas necesarias para disminuir dichos riesgos. Elaboración propia.

Dentro de los resultados obtenidos se evidencia que la explotación de la vulnerabilidad MS17-010 representa el riesgo más crítico, debido a que una falla en el servicio SMBv1 puede permitir acciones no autorizadas sobre el sistema afectado. De igual forma, se identificaron otros riesgos asociados a la exposición de puertos, configuraciones inseguras y falta de actualizaciones, los cuales pueden facilitar intentos de acceso indebido o la propagación de amenazas dentro de la red.

Las medidas de mitigación planteadas están enfocadas en reducir la posibilidad de afectación mediante controles como la aplicación de parches de seguridad, deshabilitación de servicios vulnerables, segmentación de red, monitoreo constante y fortalecimiento de las configuraciones del sistema. Estas acciones permiten mejorar la capacidad de prevención y respuesta desde la perspectiva defensiva del equipo Blue Team.

Estrategias de mitigación implementadas

Con el propósito de reducir los riesgos identificados durante el análisis técnico, se propusieron diferentes estrategias orientadas al fortalecimiento de la seguridad organizacional y protección de la infraestructura tecnológica.

Una de las principales medidas recomendadas consistió en deshabilitar SMBv1 y aplicar actualizaciones de seguridad sobre los sistemas vulnerables. Esta acción permite reducir significativamente la exposición frente a exploits relacionados con ejecución remota de código.

Asimismo, se planteó la implementación de mecanismos de monitoreo continuo mediante herramientas SIEM y análisis de registros orientados a detectar actividades sospechosas dentro de la red.

Otra estrategia importante correspondió al fortalecimiento de configuraciones de seguridad mediante hardening, restringiendo servicios innecesarios y reduciendo la superficie de ataque de los sistemas evaluados.

También se recomendó fortalecer las políticas de control de acceso y segmentación de red con el propósito de limitar movimientos laterales y minimizar el impacto asociado a posibles incidentes de seguridad informática.

Importancia de las políticas de seguridad

Las políticas de seguridad representan un componente fundamental dentro de cualquier estrategia organizacional orientada a la protección de la información y reducción de riesgos informáticos.

Las políticas de seguridad representan un componente fundamental dentro de cualquier estrategia organizacional orientada a la protección de la información y reducción de riesgos informáticos (Kim & Solomon, 2016).

Estas políticas permiten establecer lineamientos relacionados con:

- Control de accesos.
- Manejo de información.
- Actualización de sistemas.
- Respuesta a incidentes.
- Uso adecuado de recursos tecnológicos.

La ausencia de políticas claras puede generar debilidades operativas que incrementen significativamente la exposición frente a amenazas cibernéticas.

Por esta razón, las organizaciones deben implementar procesos de capacitación y concientización orientados a fortalecer la cultura de seguridad informática entre los usuarios y administradores de sistemas.

Recomendaciones para fortalecer la infraestructura tecnológica

A partir del análisis realizado durante el seminario, se identificaron diferentes recomendaciones orientadas a mejorar la seguridad de la infraestructura tecnológica y reducir riesgos asociados a vulnerabilidades críticas.

Entre las principales recomendaciones se destacan:

- Mantener actualizados los sistemas operativos y aplicaciones.
- Deshabilitar protocolos inseguros.
- Implementar herramientas de monitoreo continuo.
- Fortalecer configuraciones mediante hardening.
- Restringir accesos innecesarios.
- Segmentar adecuadamente la red organizacional.

Asimismo, se recomienda realizar pruebas periódicas de seguridad y análisis de vulnerabilidades con el propósito de identificar debilidades antes de que puedan ser aprovechadas por atacantes externos.

La implementación de controles de seguridad priorizados permite reducir riesgos conocidos y fortalecer progresivamente la postura de seguridad de una organización (Center for Internet Security, 2024).

La implementación de estrategias preventivas y mecanismos de monitoreo continuo constituye una medida fundamental para fortalecer la capacidad de respuesta frente a amenazas cibernéticas.

Importancia de la integración entre Red Team y Blue Team

La integración entre equipos ofensivos y defensivos permite fortalecer significativamente las capacidades de seguridad dentro de una organización.

Mientras el Red Team se enfoca en identificar vulnerabilidades mediante simulaciones de ataque, el Blue Team trabaja en la detección, monitoreo y contención de amenazas relacionadas con dichos escenarios.

Esta interacción permite mejorar continuamente los procesos de seguridad y facilita la implementación de estrategias orientadas a reducir riesgos asociados a ataques informáticos.

Además, la colaboración entre ambos equipos contribuye al fortalecimiento de políticas de seguridad y mejora la capacidad organizacional frente a incidentes cibernéticos.

Reflexión final sobre el análisis desarrollado

El desarrollo del seminario permitió comprender la importancia de aplicar estrategias ofensivas y defensivas dentro de entornos controlados orientados al fortalecimiento de competencias relacionadas con ciberseguridad.

Las actividades realizadas facilitaron el análisis de vulnerabilidades críticas, identificación de riesgos y aplicación de mecanismos de monitoreo y contención frente a posibles amenazas informáticas.

Asimismo, el ejercicio permitió evidenciar cómo la falta de actualización y configuraciones inseguras pueden comprometer significativamente la seguridad de una infraestructura tecnológica.

Finalmente, el trabajo desarrollado contribuyó al fortalecimiento de conocimientos técnicos relacionados con pruebas de penetración, análisis de vulnerabilidades, gestión de riesgos y estrategias defensivas aplicadas dentro de escenarios reales de ciberseguridad.

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: INFORME FINAL BLUE TEAM READ TEAM

Conclusiones

El desarrollo de este informe permitió comprender la importancia que tienen los equipos Red Team y Blue Team dentro de los procesos actuales de ciberseguridad, evidenciando que ambos enfoques cumplen funciones complementarias. Mientras el Red Team busca identificar debilidades mediante pruebas controladas, el Blue Team se enfoca en la detección, respuesta y fortalecimiento de los controles de seguridad. A partir del análisis realizado se logró observar que una organización puede mejorar significativamente su postura de seguridad cuando integra evaluaciones ofensivas y estrategias defensivas.

En relación con el objetivo de identificar vulnerabilidades presentes en una infraestructura tecnológica, se realizó un proceso de reconocimiento y análisis utilizando diferentes herramientas orientadas a la evaluación de seguridad. Durante este ejercicio se logró identificar riesgos asociados a servicios expuestos y configuraciones inseguras, destacando la importancia de mantener los sistemas actualizados y aplicar buenas prácticas de administración. Estos hallazgos permitieron comprender cómo una vulnerabilidad aparentemente conocida puede representar un riesgo elevado cuando no se aplican las medidas correctivas necesarias.

Respecto al análisis de la vulnerabilidad MS17-010, el ejercicio permitió evidenciar las consecuencias que puede generar una falla de seguridad cuando un sistema no cuenta con los parches correspondientes. La explotación controlada de esta vulnerabilidad permitió comprender, desde una perspectiva práctica, cómo un atacante podría aprovechar una debilidad del sistema y qué acciones deben implementarse desde el equipo defensivo para reducir la posibilidad de compromiso. Esto fortaleció la relación entre las actividades realizadas por un Red Team y las acciones posteriores del Blue Team.

De acuerdo con el objetivo relacionado con la aplicación de metodologías y herramientas de evaluación de seguridad, se pudo evidenciar que herramientas como los escáneres de

vulnerabilidades, utilidades de reconocimiento y plataformas de pruebas permiten obtener información valiosa sobre el estado de una infraestructura. Sin embargo, los resultados obtenidos no deben interpretarse únicamente como hallazgos técnicos, sino como elementos que ayudan a tomar decisiones para mejorar la seguridad, priorizar riesgos y establecer planes de mitigación.

Otro aspecto importante identificado durante el desarrollo del informe fue la necesidad de fortalecer la gestión de riesgos dentro de las organizaciones. Los resultados analizados muestran que medidas como la aplicación de actualizaciones, segmentación de redes, monitoreo constante y control de servicios innecesarios pueden disminuir considerablemente la superficie de ataque. Por esta razón, la seguridad informática no debe enfocarse únicamente en reaccionar ante incidentes, sino en prevenirlos mediante controles adecuados.

Finalmente, el desarrollo de esta actividad permitió cumplir con los objetivos planteados al integrar los conceptos teóricos con un escenario práctico de análisis de seguridad. La experiencia permitió comprender que la ciberseguridad requiere un enfoque continuo, donde la identificación de vulnerabilidades, la respuesta ante incidentes y la mejora permanente de los controles son procesos necesarios para proteger la información y los recursos tecnológicos de una organización.

Recomendaciones

Teniendo en cuenta los hallazgos identificados durante el análisis de seguridad realizado, se recomienda implementar un proceso organizado de gestión de vulnerabilidades que permita identificar, evaluar y corregir las debilidades encontradas en la infraestructura tecnológica. Este proceso debe realizarse de manera periódica con el fin de mantener actualizados los controles de seguridad y reducir la posibilidad de futuros incidentes.

Como medida de prioridad alta, se recomienda aplicar de manera oportuna los parches de seguridad correspondientes a los sistemas identificados con vulnerabilidades. De acuerdo con el análisis realizado sobre la vulnerabilidad MS17-010, mantener equipos sin actualizar puede facilitar la explotación de fallas conocidas y comprometer la seguridad de los servicios internos. Por esta razón, la gestión adecuada de actualizaciones debe ser una actividad permanente dentro de la organización.

De igual forma, como acción prioritaria, se recomienda deshabilitar protocolos y servicios que no sean necesarios para la operación de la infraestructura, especialmente aquellos considerados obsoletos o inseguros. La reducción de servicios expuestos permite disminuir la superficie de ataque y limita las posibilidades de que un atacante aproveche configuraciones débiles.

Como medida de contención, se recomienda implementar una adecuada segmentación de red que permita separar los sistemas críticos, servidores y equipos de usuario. Esta práctica ayudaría a limitar el movimiento lateral de un atacante en caso de que una vulnerabilidad llegue a ser explotada, reduciendo así el impacto sobre otros recursos tecnológicos.

Desde la perspectiva del equipo Blue Team, se recomienda fortalecer los mecanismos de monitoreo, registro y análisis de eventos de seguridad. La implementación de controles de

detección permite identificar comportamientos anormales y generar una respuesta más rápida ante posibles intentos de intrusión.

Asimismo, se recomienda realizar evaluaciones de seguridad periódicas mediante pruebas controladas desde el enfoque del Red Team. Estas actividades permiten verificar si las medidas de protección implementadas son efectivas y ayudan a descubrir nuevas vulnerabilidades antes de que sean aprovechadas por terceros (ENISA, 2023).

Finalmente, se recomienda establecer un proceso de seguimiento y mejora continua donde se evalúe periódicamente la efectividad de los controles aplicados (Center for Internet Security, 2024). La revisión de vulnerabilidades corregidas, el cumplimiento de actualizaciones y el análisis de nuevos riesgos permitirá fortalecer progresivamente la postura de seguridad de la organización.

Referencias Bibliográficas

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

Center for Internet Security. (2024). *CIS Controls Version 8*. https://www.cisecurity.org

European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape Report*. https://www.enisa.europa.eu

Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning.

Microsoft. (2017). *Microsoft Security Bulletin MS17-010: Critical*. Microsoft Security Response Center. https://msrc.microsoft.com

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

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (SP 800-53 Rev. 5). U.S. Department of Commerce. https://csrc.nist.gov

Nmap Project. (s.f.). *Nmap reference guide*. https://nmap.org/book/man.html

Northcutt, S., & Novak, J. (2002). *Network intrusion detection* (3rd ed.). New Riders Publishing.

Offensive Security. (2024). *Kali Linux documentation*. https://www.kali.org/docs

OWASP Foundation. (2024). *OWASP Top 10: The ten most critical web application security risks*. https://owasp.org

Palo Alto Networks. (2024). *Unit 42 threat intelligence report*. https://www.paloaltonetworks.com

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. National Institute of Standards and Technology. https://csrc.nist.gov

Serrano, A., & Muñoz, J. (2021). *Seguridad informática y análisis de vulnerabilidades*. Editorial RA-MA.

The MITRE Corporation. (2025). *MITRE ATT&CK framework*. https://attack.ist.org

Wazuh Inc. (s.f.). *Wazuh documentation*. https://documentation.wazuh.com

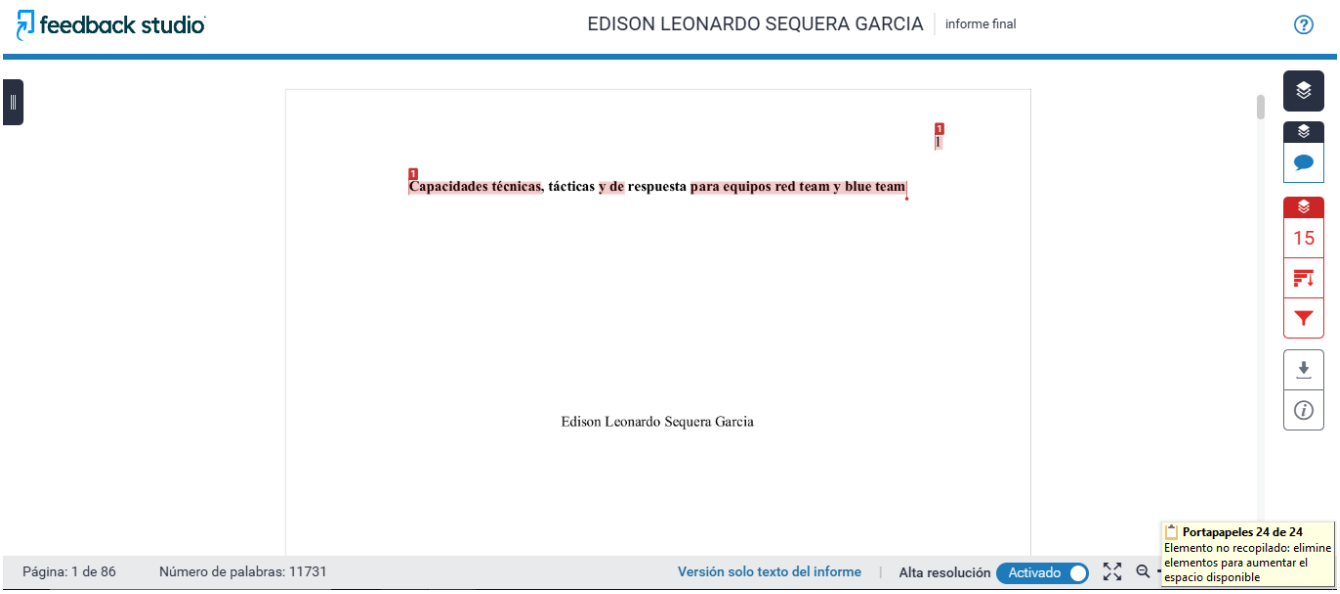
Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Wilkins, S. (2022). *Metasploit: The penetration tester's guide*. No Starch Press.

Young, W., & Aitel, D. (2018). *The hacker's handbook: The strategy behind breaking into and defending networks*. McGraw-Hill Education.

Apéndices

Apéndice A *Resultado de revisión en Turnitin*



La figura muestra el resultado obtenido después de realizar la revisión del documento final mediante la herramienta Turnitin. En el reporte se puede observar el nivel de similitud encontrado en el trabajo y las coincidencias identificadas con otras fuentes de información. Esta revisión permitió verificar la forma en que fueron utilizadas las referencias y citas dentro del documento, además de identificar posibles apartados que requerían ajustes en la redacción.

El análisis del reporte permitió realizar una última validación del contenido antes de la entrega final, buscando mantener una adecuada presentación académica y fortalecer la originalidad del informe.