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

María Fernanda Rios Corredor

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

Este documento detalla la ejecución técnica de ciberseguridad ofensiva y defensiva en el entorno controlado de SecureNova Labs. Basándose en el marco del Escenario 5, se integran las competencias de Red Team y Blue Team desarrolladas a lo largo del curso. El informe abarca desde el análisis del marco legal colombiano (Ley 1273 de 2009) hasta la explotación de vulnerabilidades (como EternalBlue) y la implementación de medidas de contención. La conclusión principal destaca que la seguridad organizacional robusta nace de la alineación entre la ética profesional y la colaboración técnica entre equipos de ataque y defensa.

***Palabras clave*:** Ciberseguridad, NIST, Resiliencia, Vulnerabilidades.

Abstract

This document details the technical execution of offensive and defensive cybersecurity in the controlled environment of SecureNova Labs. Based on the Scenario 5 framework, it integrates the Red Team and Blue Team competencies developed throughout the course. The report covers everything from the analysis of the Colombian legal framework (Law 1273 of 2009) to the exploitation of vulnerabilities (such as EternalBlue) and the implementation of containment measures. The main conclusion highlights that robust organizational security stems from the alignment between professional ethics and technical collaboration between attack and defense teams.

***Keywords*:** Cybersecurity, NIST, Resilience, Vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Apéndices

Glosario

Blue Team:

Especialistas en protección dedicados al monitoreo, contención y resolución de incidentes de seguridad.

Ciberseguridad:

Disciplinas y herramientas enfocadas en resguardar la integridad y confidencialidad de la infraestructura digital y los datos.

EDR:

Herramienta enfocada en la detección proactiva y respuesta automatizada ante amenazas directamente en los dispositivos finales.

Exploit:

Fragmento de software o método específico diseñado para aprovechar un fallo y comprometer un sistema.

Hardening:

Proceso de robustecimiento de un sistema operativo o aplicación para minimizar su superficie de ataque.

Kill Chain:

Diagrama que describe la secuencia lógica de pasos que sigue un adversario desde el acecho hasta el objetivo final.

Meterpreter:

Herramienta de post-explotación que permite el control interactivo y la administración remota de un equipo vulnerado.

MITRE ATT&CK:

Base de conocimiento global que cataloga y clasifica las tácticas criminales observadas en el mundo real.

Pentesting:

Evaluación sistemática de un entorno para descubrir y documentar fallos de seguridad explotables.

Pivoting:

Estrategia de salto que utiliza un equipo ya infectado para infiltrarse en otros segmentos de red que no son accesibles directamente.

Red Team:

Grupo táctico que ejecuta intrusiones controladas para evaluar la efectividad de los controles de seguridad.

SIEM:

Solución tecnológica que centraliza y analiza registros para identificar comportamientos sospechosos en la red.

Vulnerabilidad:

Falta de seguridad o error de configuración en un activo que permite el acceso no autorizado.

Zero Trust:

Filosofía de seguridad que exige la verificación continua de cada usuario y dispositivo, sin conceder privilegios automáticos.

Introducción

Según el National Institute of Standards and Technology (NIST, 2020), la vertiginosa aceleración de la transformación digital ha forzado a las empresas a adoptar infraestructuras híbridas, lo que a su vez ha fragmentado el perímetro de seguridad tradicional. En este panorama de alta interconectividad, la probabilidad de sufrir un ciberataque no es una posibilidad, sino una certeza estadística. Por ello, el presente informe no solo describe una serie de ejercicios técnicos, sino que fundamenta la necesidad de adoptar un enfoque de seguridad proactiva. Al integrar metodologías de Red Team para la explotación y Blue Team para la contención, se logra una visión de 360 grados sobre el estado real de la resiliencia en SecureNova Labs, permitiendo identificar brechas que las auditorías pasivas suelen ignorar.

El núcleo de la actividad se centró en la simulación de un ataque de alta criticidad dirigido a la vulnerabilidad MS17-010 (EternalBlue) sobre un sistema Windows. Este proceso de auditoría permitió documentar cómo un atacante puede escalar privilegios y realizar desplazamientos laterales dentro de una red si no existen parches de seguridad actualizados. Sin embargo, el valor agregado de este laboratorio reside en la respuesta inmediata: el diseño de protocolos para detectar el tráfico anómalo, mitigar la amenaza y restaurar la integridad del sistema. Este ciclo de ataque y respuesta directa es lo que permite validar la efectividad de los controles implementados durante las etapas previas del curso.

Más allá de la destreza técnica, este informe destaca el compromiso irrestricto con la legalidad vigente en el territorio colombiano. Las operaciones se ejecutaron bajo la lupa de la Ley 1273 de 2009, asegurando que cada intrusión simulada se mantuviera dentro de los límites del consentimiento y la protección de datos. Asimismo, se integran los principios éticos dictados por el COPNIA, subrayando que el ejercicio del profesional en ciberseguridad debe estar siempre

al servicio de la protección de la sociedad y el respeto a la propiedad intelectual. La seguridad no se entiende aquí solo como un reto de código, sino como un ejercicio de responsabilidad civil y profesional.

Para finalizar, el documento presenta una hoja de ruta estratégica orientada al robustecimiento de la seguridad organizacional. No se trata simplemente de recomendaciones aisladas, sino de una propuesta integral que abarca desde el endurecimiento (hardening) de sistemas hasta la formación de una cultura de ciberseguridad. Los resultados obtenidos en este laboratorio sirven como evidencia para demostrar que una postura de seguridad madura requiere de la sinergia constante entre la detección de fallos y la capacidad de respuesta, garantizando así la continuidad del negocio frente a las tácticas cada vez más sofisticadas del cibercrimen moderno.

Justificación

Las metodologías modernas de pruebas de penetración recomiendan un enfoque integral que combine explotación técnica y análisis estratégico del adversario (Alhamed & Rahman, 2023; Herrera, 2022). La evolución constante de los vectores de ataque, en particular aquellos orquestados por actores de Amenazas Persistentes Avanzadas (APT), ha demostrado que la seguridad puramente reactiva es insuficiente. Este informe se fundamenta en la premisa de que la resiliencia no es un estado estático, sino un proceso dinámico de mejora continua. Al integrar los ejercicios de Red Team y Blue Team, se trasciende la teoría para comprender cómo la visibilidad de red y la correlación de eventos impactan directamente en el tiempo de detección (MTTD) y el tiempo de respuesta (MTTR). Esta sinergia práctica es la que permite a SecureNova Labs transformar vulnerabilidades potenciales en fortalezas defensivas antes de que se produzca una brecha real.

Diversos estudios académicos confirman que la aplicación de modelos estructurados como la Cyber Kill Chain mejora la detección de Amenazas Persistentes Avanzadas, permitiendo correlacionar fases del ataque con controles defensivos específicos (Ahmed, 2021; Kazimierczak, 2024).

La utilidad de este estudio reside en la aplicación rigurosa de metodologías de estándar industrial como MITRE ATT&CK y el marco de NIST. No se trata simplemente de ejecutar herramientas de intrusión, sino de mapear cada fase del ataque (desde el acceso inicial hasta el pivoting) dentro de la Cyber Kill Chain. Este enfoque estructurado permite a la organización no solo identificar que existe una debilidad, sino comprender el contexto táctico del adversario. Al analizar vulnerabilidades reales como MS17-010, se evidencia el impacto devastador que una

configuración inadecuada puede tener en la continuidad del negocio, justificando así la inversión en auditorías técnicas recurrentes. (Lockheed, 2015)

Un aspecto crítico de esta labor es la demostración de que la robustez defensiva no depende exclusivamente de presupuestos ilimitados. El uso estratégico de herramientas bajo licencia GPL (General Public License) permite establecer centros de monitoreo y detección de intrusos de grado profesional sin los costos prohibitivos de las soluciones propietarias. Esta democratización de la tecnología de seguridad es vital para organizaciones que, como SecureNova Labs, buscan optimizar sus recursos financieros sin sacrificar la integridad de sus sistemas. La contención efectiva de incidentes mediante software de código abierto valida que el talento humano y el conocimiento metodológico son, en última instancia, los activos más valiosos de cualquier estrategia de ciberseguridad. (MITRE, 2023)

Finalmente, la dimensión jurídica de este informe aborda la prevención de riesgos legales que a menudo se pasan por alto. La seguridad informática en Colombia no solo es un reto técnico, sino un cumplimiento irrestricto de la Ley 1273 de 2009. Este estudio garantiza que todos los procesos de auditoría interna y acuerdos de confidencialidad estén alineados con la ética profesional. De este modo, se protege a la institución de posibles delitos de encubrimiento y se deslinda la responsabilidad penal de los colaboradores, asegurando que el fortalecimiento de la infraestructura digital se realice siempre bajo un paraguas de transparencia, honestidad y responsabilidad institucional.

Objetivos

Objetivo General

Evaluar la postura de ciberseguridad de SecureNova Labs mediante la simulación de amenazas y la implementación de mecanismos de defensa. Esta integración permite diagnosticar brechas de seguridad y proponer recomendaciones estratégicas que mejoren la capacidad de respuesta operativa, garantizando en todo momento que las actividades se desarrollen dentro de un entorno lícito y ético.

Objetivos Específicos

Implementar un entorno de simulación aislado y controlado, diseñado específicamente para la ejecución coordinada de maniobras de ataque y defensa sin comprometer infraestructuras reales.

Evaluar las implicaciones legales y los principios deontológicos que rigen las actividades de seguridad informática, garantizando la licitud de cada procedimiento técnico realizado.

Desarrollar un ciclo de intrusión profesional, abarcando desde el rastreo de activos hasta la persistencia y control de sistemas, siguiendo protocolos estandarizados de Red Teaming.

Desplegar un ecosistema de respuesta proactiva que integre la vigilancia continua, la identificación de amenazas y la restauración de servicios para minimizar el impacto operacional.

Auditar los protocolos operativos y contractuales para detectar posibles brechas de cumplimiento frente a la Ley 1273 de 2009, mitigando riesgos de responsabilidad penal y civil.

Realizar un ejercicio de explotación avanzada, con el fin de testear la capacidad del adversario para elevar permisos y transitar lateralmente hacia activos de información sensibles.

Ciberseguridad en la Actualidad

En el panorama actual, la ciberseguridad ha dejado de ser un componente técnico opcional para transformarse en un pilar estratégico vital. Hoy en día, la viabilidad y el éxito competitivo de cualquier entidad dependen de su capacidad para proteger sus activos digitales. Con la integración masiva de infraestructuras en la nube, la proliferación de dispositivos iot y la interconexión constante de redes, la "superficie de ataque" ha crecido exponencialmente. Este escenario obliga a las organizaciones a abandonar enfoques reactivos en favor de estrategias defensivas multidimensionales y proactivas. (National Institute of Standards and Technology [NIST], 2020)

Evolución y Aumento de Amenazas Avanzadas

El ecosistema de amenazas ha mutado de simples virus informáticos a operaciones de alta complejidad. Entre las amenazas más críticas que enfrentan las empresas modernas se encuentran:

- Grupos apt (advanced persistent threats): actores estatales o criminales que ejecutan ataques sigilosos y prolongados en el tiempo.
- Ransomware como servicio (raas): un modelo de negocio criminal que democratiza el acceso a software extorsivo.
- Ingeniería social dirigida: técnicas de spear-phishing (pesca dirigida) y whaling (ataques a altos ejecutivos) que explotan la psicología humana.
- Vulnerabilidades en la cadena de suministro: ataques dirigidos a proveedores externos para comprometer a los clientes finales.

- Amenazas automatizadas con ia: el uso de inteligencia artificial para descubrir vulnerabilidades a una velocidad sobrehumana.

Un entorno de Hiperconectividad

La infraestructura corporativa ya no tiene perímetros definidos. La adopción de tecnologías diversas ha abierto nuevos vectores de entrada que requieren controles rigurosos:

- Internet de las cosas (iot): dispositivos que a menudo carecen de seguridad nativa.
- Cloud computing: servicios de nube que exigen un modelo de responsabilidad compartida.
- Sistemas industriales (ot): infraestructuras críticas que ahora están conectadas a la red it, incrementando el riesgo operativo.

La centralidad de la Protección del Dato

La información es el activo más crítico de la era moderna. Para protegerla, la planificación estratégica se rige por la tríada cia, un modelo fundamental en seguridad:

- Confidencialidad: garantizar que solo el personal autorizado acceda a la información.
- Integridad: mantener los datos exactos y libres de alteraciones no autorizadas.
- Disponibilidad: asegurar que los sistemas y datos sean accesibles cuando se necesiten.

El rol del Red Team

El red team actúa como un grupo de "atacantes éticos" dedicados a desafiar las defensas de la organización. Su propósito trasciende el simple hallazgo de fallos técnicos; buscan evaluar la respuesta operativa global, identificando puntos ciegos en los procesos y la capacidad de resistencia del personal ante ataques de alta fidelidad.(Rojas & Osorio, 2016).

Objetivos y Capacidades del Red Team

El equipo rojo no solo explota sistemas, sino que:

- Adopta la mentalidad y tácticas de un adversario real.
- Detecta brechas procedimentales y humanas, no solo tecnológicas.
- Utiliza habilidades avanzadas en ingeniería social, desarrollo de payloads personalizados, movimiento lateral dentro de la red y técnicas de persistencia para evitar ser detectados por los sistemas de monitoreo.

Metodologías de Trabajo

Para estructurar sus ataques de forma profesional, se apoyan en marcos reconocidos como:

- Cyber kill chain: modelo de lockheed martin que desglosa las etapas de un ataque.
- Mitre att&ck: una base de conocimiento global sobre tácticas y técnicas de atacantes.

El rol del Blue Team

El blue team es la unidad responsable de la protección diaria. Su misión es detectar, contener y neutralizar cualquier intento de intrusión antes de que cause daños significativos. (NIST, 2012)

Capacidades y Respuesta a Incidentes

Este equipo gestiona herramientas avanzadas como siem (gestión de eventos), edr (detección en endpoints) y realiza análisis forenses tras una brecha. Suelen seguir el marco del nist 800-61, que divide la respuesta a incidentes en fases críticas: desde la preparación y detección, hasta la erradicación de la amenaza y la recuperación de servicios.(Ahmed, 2021).

Purple Team: Sinergia y Colaboración

El enfoque purple team nace para romper el aislamiento entre el red y el blue team. No es necesariamente un equipo nuevo, sino una metodología donde ambos grupos colaboran estrechamente. El objetivo es que los ataques simulados se conviertan de inmediato en mejoras para los sistemas de detección, optimizando así la madurez de seguridad de la empresa.(Velásquez, 2023).

Arquitectura Zero Trust (Confianza Cero)

El modelo Zero Trust surge como respuesta a la pérdida del perímetro tradicional de seguridad, proponiendo la verificación continua de identidades, dispositivos y contextos de acceso. Estudios recientes destacan que este enfoque reduce significativamente el movimiento lateral y los accesos no autorizados en entornos híbridos y distribuidos (He. 2022; Ghasemshirazi. 2023). Asimismo, el principio de que ‘la confianza es una vulnerabilidad’

refuerza la necesidad de eliminar cualquier confianza implícita dentro de la red (Beyond Zero Trust, 2015). Bajo el paradigma zero trust, la premisa es radical: "nunca confiar, siempre verificar". Este modelo asume que las amenazas pueden estar tanto fuera como dentro del perímetro. Se basa en:

- Microsegmentación: dividir la red en zonas pequeñas para evitar que un atacante se mueva libremente.
- Mfa (autenticación de múltiples factores): obligatoria para cada intento de acceso.
- Mínimo privilegio: otorgar a los usuarios solo los permisos estrictamente necesarios.

Ética, Normatividad y Marco Legal

La práctica de la ciberseguridad debe estar sujeta a un código ético inquebrantable. Cualquier prueba ofensiva requiere de reglas de compromiso (roe) y autorización explícita para evitar consecuencias legales.

Contexto Legal en Colombia

En el ámbito nacional, los profesionales deben operar bajo el estricto cumplimiento de:

- Ley 1273 de 2009: el régimen penal que castiga el acceso abusivo, el daño informático y la interceptación de datos. (Congreso de la República de Colombia, 2009)
- Ley 1581 de 2012: que regula la protección de datos personales y la privacidad de los ciudadanos. (Congreso de la República de Colombia, 2012)

Actuar sin la debida diligencia legal no solo es poco ético, sino que puede derivar en responsabilidades penales graves para el consultor o la organización.

Análisis técnico de las Etapas 1 a 4

El presente capítulo desarrolla exhaustivamente el análisis técnico de cada una de las cuatro etapas realizadas durante el curso, las cuales conforman el ciclo completo de ciberseguridad propuesto por securenova labs. Cada etapa aborda un componente esencial: el laboratorio y fundamentos técnicos (etapa 1), el marco ético y legal (etapa 2), las prácticas ofensivas (etapa 3) y las prácticas defensivas (etapa 4). La combinación de estos elementos proporciona una visión integral del funcionamiento de los equipos red team y blue team dentro de una organización.

Etapa 1 Fundamentos de Operaciones Red Team y Blue Team

La etapa 1 representó el punto de partida para la construcción de un entorno de pruebas controlado y funcional que permitiera ejecutar ataques y defensas sin poner en riesgo infraestructuras reales. Esta etapa se centró en:

- La configuración del laboratorio
- La instalación de máquinas virtuales
- La preparación del entorno ofensivo y defensivo
- La exploración inicial de herramientas
- La comprensión teórica del ciclo de ataque y defensa

Construcción del Laboratorio

El laboratorio se construyó empleando oracle vm virtualbox, con el objetivo de simular un entorno corporativo mínimo compuesto por:

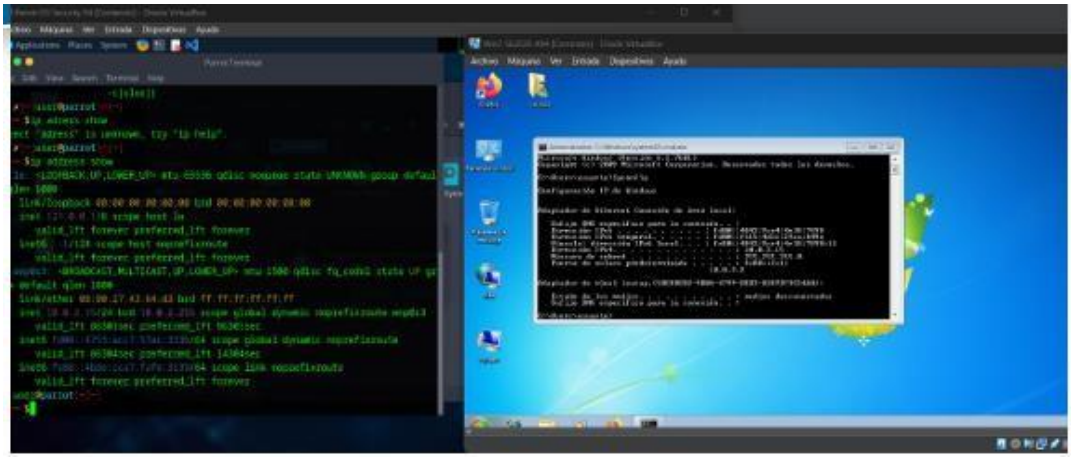
El sistema atacante estuvo conformado por una máquina basada en Parrot Security OS o Kali Linux, plataformas especializadas en pruebas de penetración que incorporan de forma nativa un amplio conjunto de herramientas ofensivas. Este entorno permitió ejecutar actividades de reconocimiento, escaneo de servicios, explotación de vulnerabilidades, análisis de tráfico de red y procesos de automatización, reproduciendo de manera realista las capacidades de un adversario técnico en un escenario corporativo controlado.

El sistema víctima correspondió a equipos con sistemas operativos Windows 10 y Windows Server configurados de forma deliberadamente vulnerable. Estos sistemas presentaban puertos expuestos y versiones antiguas del protocolo SMB, condición necesaria para permitir la explotación de la vulnerabilidad MS17-010 (EternalBlue), facilitando así la ejecución controlada de técnicas de intrusión y post-explotación propias de un ejercicio de Red Team.

Finalmente, se implementó una red interna simulada con características similares a las de una red empresarial típica. En este entorno, el sistema atacante operó con una dirección IP del rango 10.10.10.x, mientras que el servidor víctima fue asignado a una dirección 10.10.10.y, ambos conectados mediante un gateway simulado. La red fue configurada de forma completamente aislada, sin acceso a Internet, con el propósito de evitar riesgos reales y garantizar que todas las pruebas se desarrollaran en un entorno seguro y controlado.

Figura 1

Instalación de Máquinas Virtuales



Nota. Autoría Propia

Etapa 2 – Ética Profesional y Marco Normativo

Esta fase se centró en el análisis ético y legal de las operaciones de seguridad ofensiva. Se revisó un caso de estudio donde un acuerdo de confidencialidad contenía cláusulas ilegales que obligaban a ocultar incidentes o accesos indebidos. Se identificaron violaciones a la ley 1273 de 2009, la ley 1581 de 2012 y los principios éticos profesionales. Las pruebas de penetración se fundamentan en metodologías estructuradas que permiten identificar, explotar y documentar vulnerabilidades de forma controlada (Penetration Testing, s. f.).

El análisis resaltó la obligación de los profesionales de ciberseguridad de actuar dentro de un marco regulatorio, reportar actividades ilícitas y garantizar la protección de datos. Se aclaró que ningún equipo red team puede operar sin consentimiento explícito y dentro de los límites legales establecidos.

Revisión del Marco Legal Colombiano

Marco Criminalístico Digital: Ley 1273 de 2009

Esta normativa constituye el eje penal de la seguridad informática en Colombia, tipificando conductas que atentan contra la confidencialidad, integridad y disponibilidad de los datos.

Representa el blindaje jurídico contra el cibercrimen. En el contexto de este informe, su análisis asegura que las tácticas de Red Team (como el acceso a sistemas o la interceptación de datos) se ejecuten bajo una autorización expresa y documentada, evitando que la simulación de vulnerabilidades se clasifique como un "acceso abusivo" o "daño informático" bajo los artículos 269A y 269D.

Régimen de Privacidad y Habeas Data: Ley 1581 de 2012

Es la norma general que regula el tratamiento de datos personales, imponiendo a las organizaciones la obligación de implementar medidas de seguridad técnicas y administrativas.

Define las responsabilidades de SecureNova Labs frente al manejo de información sensible. Durante el ejercicio de Blue Team, esta ley obliga a que la recolección de logs y el monitoreo de tráfico respeten el derecho de los titulares de la información, garantizando que el fortalecimiento de la seguridad no derive en un tratamiento ilícito de datos personales recolectados durante la fase de auditoría.

Garantía Constitucional de la Intimidad: Art. 15 de la Constitución Política

Este precepto eleva la protección de la información personal a un derecho fundamental, estableciendo que la correspondencia y demás formas de comunicación privada son inviolables.

Actúa como el límite ético y superior de toda operación de ciberseguridad. Establece que cualquier intervención en redes o sistemas debe equilibrar la necesidad de protección institucional con el derecho a la autodeterminación informática, asegurando que los procedimientos de detección de incidentes no vulneren la privacidad fundamental de los individuos vinculados a la organización.

Evaluación Ética del Acuerdo de Confidencialidad

En esta actividad se identificaron cláusulas problemáticas tales como:

- Obligación de encubrir actividades ilegales
- Permiso para interceptar comunicaciones
- Uso indebido de información sin autorización
- Comunicación poco clara del alcance de pruebas

Estas cláusulas representan:

- Violación a la normativa
- Riesgo legal y reputacional
- Conflicto ético para el profesional

Principios Éticos Fundamentales

Un analista red/blue team debe cumplir con:

- Integridad profesional
- Respeto por la privacidad
- Confidencialidad de datos
- Transparencia en procedimientos
- Consentimiento informado
- Autorización formal

Impacto moral y legal

La etapa 2 permitió comprender que:

- Un red team sin autorización es un cibercriminal.
- Un blue team que manipule evidencia puede cometer delitos.
- Un contrato mal redactado puede invalidar una prueba.
- La ética guía la actuación técnica.

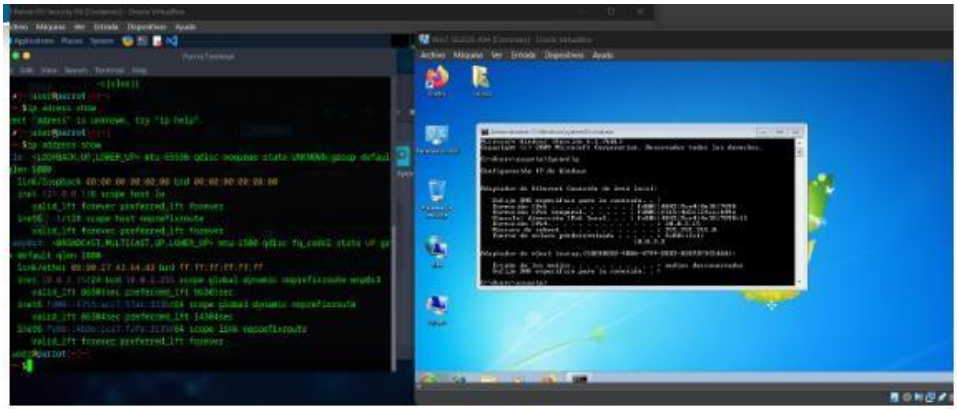
Etapa 3 – Práctica Simulada Red Team

Esta etapa fue esencial, pues permitió ejecutar un ataque realista, siguiendo metodologías ofensivas profesionales. Representa el trabajo típico de un analista red team en un entorno corporativo.

Esta imagen muestra dos máquinas virtuales ejecutándose simultáneamente. En el lado izquierdo se observa la terminal de kali linux ejecutando el comando 'ip address', donde se identifica la interfaz eth0 con la ip 10.10.10.6 y el gateway 10.10.10.2.

Figura 2

Configuración IP Máquinas Virtuales

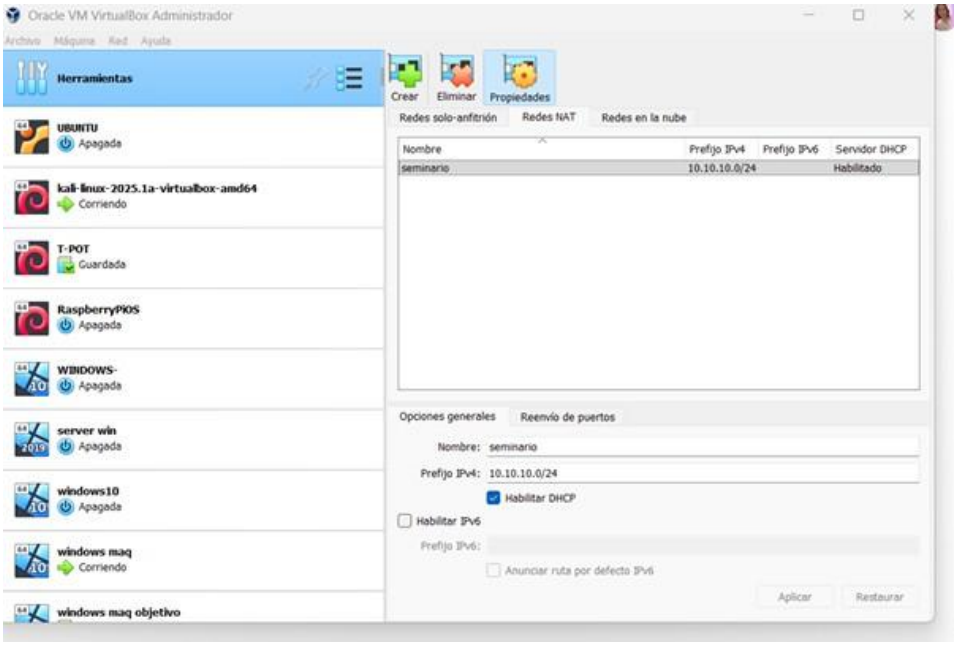


Nota. Autoría Propia

En el lado derecho se muestra el cmd de windows 7 con el comando 'ipconfig', donde la máquina posee la ip 10.10.10.5 en la misma red nat. Esta evidencia confirma la comunicación correcta entre ambas máquinas, necesaria para el reconocimiento y explotación posterior.

Figura 3

Configuración red NAT



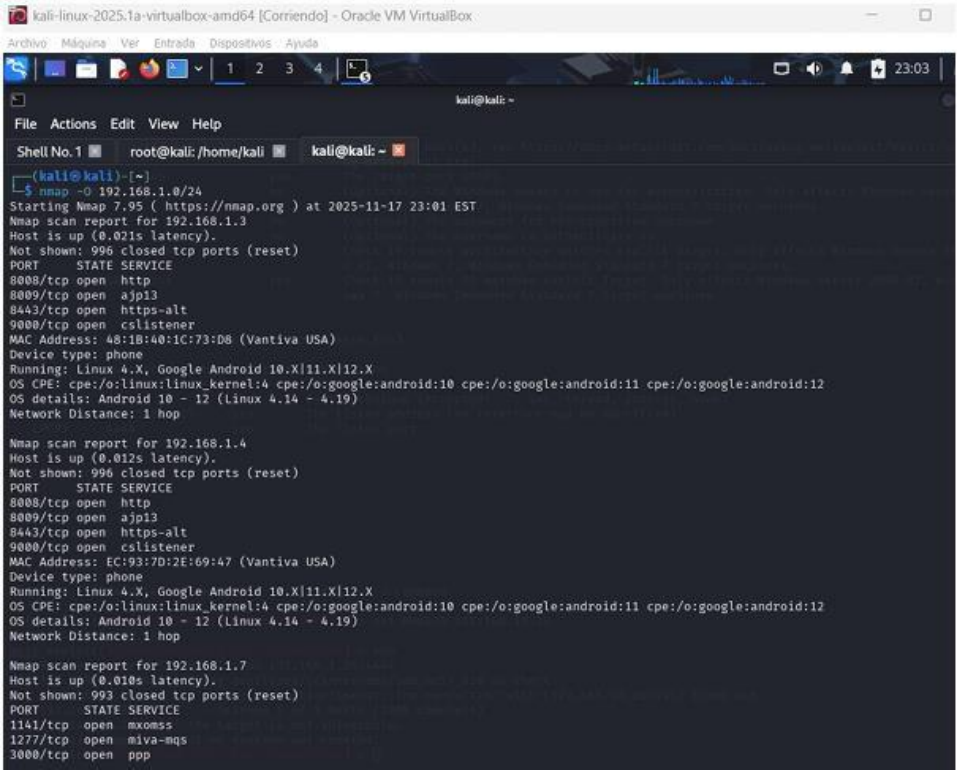
Nota. Autoría Propia

En esta captura se visualiza la configuración de la red nat llamada 'seminario' en virtualbox.

Se muestra el prefijo 10.10.10.0/24 y el dhcp habilitado. Esta configuración crea un entorno seguro y aislado donde las máquinas virtuales pueden comunicarse entre sí, permitiendo escenarios de ataque controlado sin afectar el sistema real del usuario.

Figura 4

Escaneo NMAP



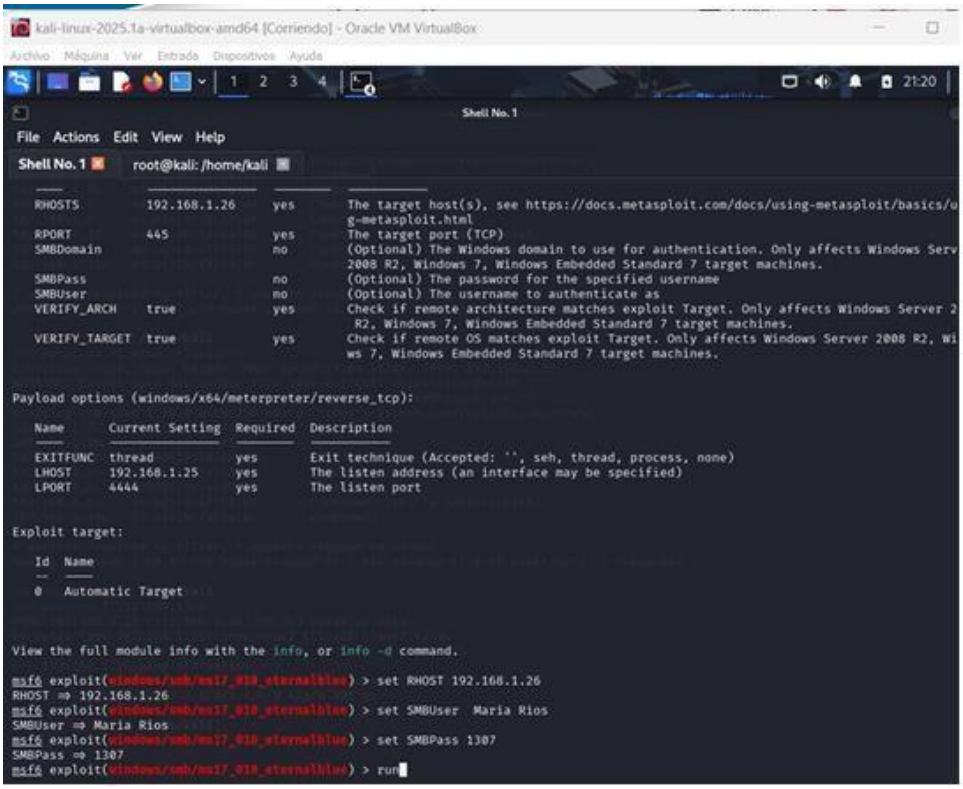
Nota. Autoría Propia

La imagen representa un escaneo nmap realizado con el comando 'nmap -st 192.168.1.0/24'.

Los resultados identifican múltiples hosts activos, servicios expuestos como http (80), https (443), y otros puertos relevantes. Esta fase corresponde al reconocimiento activo previo a la explotación, permitiendo mapear la superficie de ataque en la red.

Figura 5

Ejecución del exploit ms17-010 (eternalblue) en metasploit



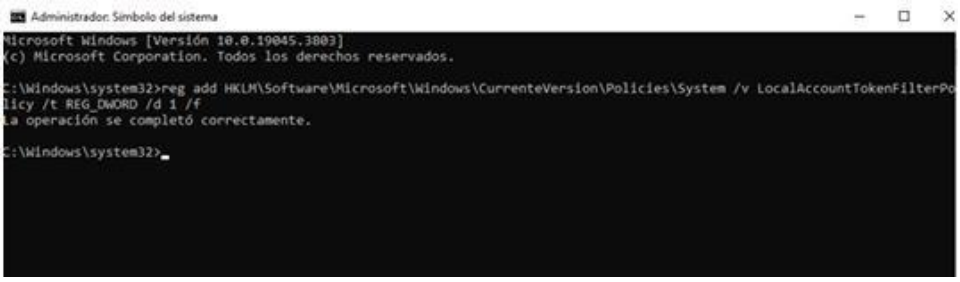
Nota. Autoría Propia

Aquí se observa metasploit configurando el módulo exploit/windows/smb/ms17_010_eternalblue.

Se detallan parámetros esenciales como rhost 192.168.1.26, rport 445, lhost 192.168.1.25 y el payload meterpreter reverse_tcp. Esta evidencia corresponde a la etapa de explotación directa del sistema vulnerable mediante eternalblue.

Figura 6

Modificación del Registro en Windows (post-explotación)



Nota. Autoría Propia

La imagen muestra la ejecución del comando 'reg add ... Localaccounttokenfilterpolicy', el cual modifica el registro de windows para permitir privilegios administrativos remotos completos. Este cambio confirma la fase de post-explotación y escalamiento de privilegios tras comprometer exitosamente la máquina víctima.

Reconocimiento Activo y Pasivo

El ejercicio de Red Team se inició con una fase de reconocimiento pasivo, cuyo objetivo principal fue recopilar información relevante sin interactuar directamente con los sistemas objetivo, minimizando así la probabilidad de detección. Durante esta etapa se llevó a cabo el análisis de banners y la identificación preliminar de sistemas potencialmente vulnerables mediante la revisión de información pública disponible. Este enfoque permitió construir un perfil inicial del entorno tecnológico, identificar tecnologías utilizadas y estimar posibles vectores de ataque sin generar registros o alertas en la infraestructura analizada.(Gomez, 2022)

Una vez consolidada la información obtenida de manera pasiva, se procedió con la fase de reconocimiento activo, en la cual se emplearon herramientas especializadas para interactuar directamente con el sistema objetivo. En particular, se utilizó la herramienta Nmap para realizar un escaneo dirigido al puerto 445, asociado al servicio SMB. Los resultados obtenidos confirmaron que dicho puerto se encontraba abierto y que el servicio en ejecución correspondía a una versión vulnerable, lo cual permitió inferir la exposición del sistema a la vulnerabilidad MS17-010, conocida como EternalBlue. Este hallazgo evidenció deficiencias en la gestión de parches y en la configuración del sistema.

Posteriormente, se llevó a cabo un análisis detallado de vulnerabilidades con el fin de validar técnicamente la exposición identificada durante el reconocimiento activo. Mediante el uso de scripts específicos para SMB, se confirmó de forma explícita que el host objetivo era vulnerable a MS17-010, reduciendo el margen de error y asegurando que la explotación se realizara sobre una debilidad real del sistema. Esta validación previa resulta fundamental para evitar intentos de explotación innecesarios y minimizar el impacto operativo durante las pruebas.

En la fase de explotación, se utilizó el framework Metasploit para ejecutar el exploit correspondiente a EternalBlue contra el sistema objetivo. Como resultado, se logró establecer una sesión Meterpreter con el host comprometido, obteniendo acceso remoto de manera exitosa. Este acceso inicial permitió al equipo ofensivo interactuar con el sistema, confirmar el nivel de compromiso alcanzado y evaluar los controles de seguridad presentes en el entorno.

A continuación, se ejecutaron técnicas de escalamiento de privilegios con el objetivo de obtener control total del sistema comprometido. A través de comandos específicos, fue posible elevar los permisos hasta nivel administrativo y extraer credenciales almacenadas en el sistema.

Estas acciones evidenciaron la ausencia de mecanismos efectivos de control de privilegios y la falta de monitoreo de actividades anómalas, lo que facilitó la consolidación del ataque.

Una vez alcanzado el control completo del host, se implementaron mecanismos de persistencia diseñados para garantizar el acceso continuo al sistema en el tiempo, incluso ante reinicios o interrupciones del servicio. Esta fase simuló el comportamiento típico de amenazas avanzadas persistentes, cuyo objetivo es mantener presencia prolongada dentro de la infraestructura comprometida sin ser detectadas.

Finalmente, se llevaron a cabo técnicas de movimiento lateral y *pivoting*, configurando rutas hacia una segunda subred interna previamente no accesible. Esta acción permitió ampliar el alcance del ataque, enumerar nuevos equipos y explorar recursos adicionales dentro de la red, demostrando debilidades significativas en la segmentación de red y en los controles de tráfico interno. El impacto global del ataque evidenció la posibilidad de comprometer un equipo crítico, obtener control total del sistema, acceder a redes adicionales, extraer credenciales sensibles y superar controles de seguridad deficientes, subrayando la importancia de una estrategia defensiva integral basada en hardening, segmentación y monitoreo continuo.

Etapa 4 – respuesta y Contención Blue Team Introducción A

La Respuesta Ante Incidentes

La fase 4 aborda uno de los procesos más críticos en la ciberseguridad organizacional: la respuesta, contención y manejo de incidentes de seguridad. A diferencia de las primeras fases (orientadas al reconocimiento, ataque ético o análisis normativo), esta etapa se centra en los

procedimientos defensivos que se activan cuando un evento de seguridad afecta o puede afectar la infraestructura tecnológica de una organización.

El objetivo principal de esta fase es desarrollar la capacidad para:

- Detectar incidentes oportunamente.
- Determinar su impacto real y potencial.
- Contener la amenaza de forma efectiva.
- Realizar análisis forense inicial.
- Restaurar la operatividad sin comprometer evidencia.
- Evitar que el ataque se repita.

Esta fase integra conocimientos del blue team, del manejo de evidencias digitales y del ciclo estándar de respuesta a incidentes reconocido por organismos como nist, first y sans.

Identificación del Incidente

La detección temprana es la base de una adecuada contención. Durante la fase se estudiaron diferentes métodos que permiten identificar señales de compromiso (indicators of compromise – iocs) como:

- Conexiones sospechosas a puertos no autorizados.
- Aumento inusual en el consumo de cpu, ram o red.
- Aparición de procesos desconocidos o persistentes.
- Creación inesperada de usuarios administradores.

- Cambios no autorizados en el registro o políticas de seguridad.
- Alertas generadas por el siem (security information event management).

En ambientes corporativos, los incidentes suelen ser detectados a través de herramientas automatizadas como firewalls de nueva generación, sistemas ids/ips o sistemas edr/xdr.
Sin embargo, también pueden ser reportados por usuarios cuando encuentran comportamientos extraños.

Dentro del estudio se realizó énfasis en la importancia de que cada organización cuente con un plan de monitoreo continuo, ya que la detección tardía aumenta el impacto del ataque y dificulta la recuperación.

Análisis del Incidente y Priorización

Una vez detectado un incidente de seguridad, resulta indispensable realizar un proceso de clasificación que permita determinar su nivel de severidad y definir la respuesta más adecuada. Para ello, se analizan diversos factores críticos, entre los que se incluyen el tipo de ataque identificado como malware, ransomware, explotación de vulnerabilidades, fuga de información o ataques internos, así como el alcance del incidente, determinado por la cantidad de máquinas, sistemas o servicios comprometidos. Adicionalmente, se evalúa el impacto operativo sobre los procesos de negocio afectados y el posible impacto reputacional y legal, especialmente en los casos que involucran la exposición de datos personales o información corporativa sensible. Otro elemento clave en esta fase es el tiempo de exposición, que permite establecer durante cuánto tiempo el atacante ha permanecido activo dentro de la red. (MITRE, 2023)

En esta etapa también se realiza la revisión de información altamente volátil, cuya pérdida puede comprometer el análisis posterior del incidente. Dicha información incluye los

procesos activos en ejecución, las conexiones de red vigentes, las entradas recientes en el registro del sistema, los archivos temporales y las sesiones cargadas en memoria. Dado que estos datos pueden desaparecer si el equipo es apagado o reiniciado, su recolección debe efectuarse mediante técnicas de análisis forense en vivo (live analysis), garantizando la preservación de la evidencia digital y la trazabilidad del incidente.

Contención Inicial

La contención se divide en dos fases: contención inmediata y contención a largo plazo.

Contención INMEDiata

Su objetivo es evitar que el incidente siga propagándose. Puede incluir:

- Aislar la máquina afectada de la red.
- Bloquear direcciones ip, dominios o puertos sospechosos.
- Deshabilitar cuentas de usuario comprometidas.
- Detener procesos maliciosos.
- Cortar sesiones activas del atacante.

Es fundamental realizar estas acciones sin borrar evidencia, ya que la información será necesaria para investigaciones posteriores.

Contención a Largo Plazo

Implica aplicar medidas que permitan seguir operando mientras se investiga:

- Implementar reglas temporales de firewall.

- Reconfigurar políticas de acceso.
- Aplicar parches urgentes.
- Activar monitoreo avanzado.

Esta fase debe realizarse cuidadosamente para no alertar al atacante si aún está dentro del sistema.

Erradicación de la Amenaza

Una vez contenida la amenaza, se procede a la erradicación. Esta etapa busca remover completamente los artefactos maliciosos que el atacante pudo haber dejado:

- Eliminación de malware o backdoors.
- Revisión de tareas programadas sospechosas.
- Eliminación de llaves de registro maliciosas.
- Auditoría de usuarios y permisos.
- Reversiones de cambios en políticas de seguridad.
- Revisión de credenciales filtradas o comprometidas.

En los casos en que el adversario haya mantenido persistencia mediante técnicas avanzadas, como rootkits o reescritura de bios/uefi, puede ser necesario reconstruir el sistema desde cero.

Recuperación del Sistema

Esta fase se enfoca en restaurar los servicios afectados a su estado funcional normal sin comprometer la seguridad.

Incluye:

- Restablecimiento de servicios esenciales.
- Verificación de logs para confirmar ausencia de actividad sospechosa.
- Aplicación de parches de seguridad faltantes.
- Restauración de copias de seguridad (solo si están libres de infección).
- Monitoreo reforzado post-incidente para validar estabilidad.

El tiempo de recuperación depende del tipo de ataque. Por ejemplo:

- Ransomware: recuperación lenta por análisis de daños.
- Explotación sin borrado de datos: recuperación más rápida.

Uso del Siem Y Herramientas de Monitoreo

Diversos estudios destacan que las plataformas SIEM continúan siendo componentes críticos e irremplazables para la correlación de eventos, detección temprana y respuesta ante incidentes de seguridad (Why SIEM is Irreplaceable, s. f.). Una parte sustancial de esta fase se centró en comprender el rol del siem en la respuesta ante incidentes. Estas herramientas permiten:

- Correlación de eventos de diferentes fuentes.
- Normalización de logs.

- Generación de alertas basadas en reglas o comportamientos.
- Identificación de patrones repetitivos.
- Construcción de líneas de tiempo del ataque.

El siem se convierte en la pieza central del blue team, permitiendo detectar ataques activos incluso antes de que generen daño significativo.

Cis Control Y Medidas de Hardenización

Como parte de la prevención de futuros incidentes, se estudiaron las recomendaciones del center for internet security (cis). (Center for Internet Security [CIS], 2021)

Los controles más relevantes aplicados en esta fase fueron:

- Cis 4: control de dispositivos administrados.
- Cis 7: configuración segura de sistemas.
- Cis 8: gestión de vulnerabilidades.
- Cis 13: monitoreo continuo.
- Cis 16: gestión de cuentas privilegiadas (pam).

Medidas específicas revisadas:

- Eliminación de smbv1 (evita vulnerabilidades como eternalblue).
- Segmentación estricta entre redes internas.
- Restricciones de ejecución mediante applocker.

- Políticas de contraseñas fuertes.
- Activación de autenticación multifactor (mfa).
- Lista blanca de aplicaciones en estaciones de trabajo críticas.

Lecciones Aprendidas Y Comunicación

La fase de lecciones aprendidas constituye un componente esencial del ciclo de respuesta a incidentes, ya que permite convertir un evento de seguridad en una oportunidad de mejora continua para la organización. Esta etapa culmina con la elaboración de un informe post-incidente estructurado, cuyo objetivo principal es documentar de manera clara y verificable qué ocurrió, cómo ocurrió, qué impacto tuvo, cómo se resolvió y qué acciones deben adoptarse para evitar que el incidente se repita.

En primer lugar, el informe debe describir qué ocurrió, identificando el tipo de incidente, los sistemas afectados y el momento en que fue detectado. Posteriormente, se debe detallar cómo ocurrió, explicando el vector de ataque, las vulnerabilidades explotadas, las técnicas utilizadas por el atacante y las fallas de control que permitieron la materialización del evento. Este análisis técnico resulta clave para comprender la cadena de ataque y evaluar la efectividad de los mecanismos de detección existentes.

Asimismo, el documento debe analizar qué impacto tuvo el incidente, considerando no solo las afectaciones técnicas, sino también las consecuencias operativas, financieras, legales y reputacionales para la organización. Esta evaluación permite dimensionar la gravedad real del evento y priorizar las acciones de mitigación de acuerdo con el nivel de riesgo asumido. A

continuación, se debe documentar cómo se resolvió el incidente, detallando las acciones de contención, erradicación y recuperación implementadas, así como los tiempos de respuesta y los recursos involucrados durante la gestión del evento.

Finalmente, el informe post-incidente debe establecer qué acciones deben tomarse para evitar que suceda nuevamente, proponiendo medidas correctivas y preventivas tanto a nivel técnico como organizacional. Estas acciones pueden incluir ajustes en la arquitectura de seguridad, fortalecimiento de controles, actualización de políticas, mejoras en los procesos de monitoreo y respuesta, y programas de capacitación dirigidos al personal. La correcta formulación de estas recomendaciones garantiza que las lecciones aprendidas se traduzcan en mejoras concretas y sostenibles.

De manera complementaria, se resalta la importancia de una comunicación efectiva y coordinada durante esta fase, en la cual el equipo de respuesta a incidentes debe trabajar conjuntamente con las áreas legal, de recursos humanos, comunicaciones y la alta dirección. Esta coordinación asegura una respuesta ética, controlada y alineada con los requerimientos legales, evitando impactos negativos en la imagen corporativa y fortaleciendo la confianza de las partes interesadas. (Buitrago, 2018)

Estrategias Red Team

El red team tiene como objetivo principal simular adversarios reales con el fin de evaluar la resistencia de la infraestructura tecnológica, la efectividad de los controles de seguridad y la capacidad de respuesta del blue team. Para ello, debe emplear estrategias ofensivas avanzadas que permitan reproducir escenarios que un atacante real podría ejecutar dentro de una

organización. Este capítulo detalla las estrategias fundamentales, técnicas, tácticas y procedimientos (ttps) que conforman la operación de un red team profesional.

Enfoque Estratégico Del Red Team

El enfoque del Red Team debe ser eminentemente realista, orientado a simular amenazas que efectivamente existen y que representan un riesgo tangible para la industria. Esto implica modelar escenarios basados en ataques de ransomware, operaciones de grupos APT de carácter estatal o militar, ciberdelincuencia organizada, acciones de hacktivismo y amenazas internas (insider threats). La simulación de este tipo de adversarios permite evaluar de manera precisa la capacidad de la organización para enfrentar ataques con distintos niveles de sofisticación, motivación e impacto potencial. La diferenciación funcional entre Red Team y Blue Team, así como su articulación estratégica, responde a modelos formativos y operativos consolidados en entornos académicos y profesionales (Barón, 2024).

Adicionalmente, el Red Team debe operar de forma sigilosa, procurando evitar la detección por parte de los controles defensivos. Cada acción ejecutada durante el ejercicio debe orientarse a evadir soluciones de antivirus, EDR y SIEM, así como a minimizar la generación de registros que puedan delatar la presencia del atacante. Este enfoque permite evaluar no solo la eficacia de los controles técnicos, sino también la capacidad del Blue Team para identificar comportamientos anómalos de bajo ruido, característicos de amenazas avanzadas persistentes.

El trabajo del Red Team debe estar claramente orientado a objetivos definidos, los cuales pueden incluir el compromiso de un dominio, la exfiltración de información sensible, la obtención de acceso persistente, el control de servidores críticos o la simulación de un ataque de ransomware. La definición de objetivos concretos permite medir el éxito del ejercicio en función

del impacto real que un atacante podría generar sobre la organización, en lugar de limitarse a la identificación aislada de vulnerabilidades técnicas. La integración de equipos ofensivos y defensivos debe realizarse bajo lineamientos éticos claramente definidos y supervisados institucionalmente (Fernando, 2024).

Asimismo, el enfoque estratégico del Red Team debe basarse en el uso sistemático de inteligencia de amenazas (Threat Intelligence), con el fin de construir escenarios de ataque alineados con tácticas, técnicas y procedimientos reales. Para ello, se deben tomar como referencia grupos ampliamente documentados como FIN7, Lazarus Group, APT29, APT41 y TA505, cuyas operaciones han demostrado un alto nivel de sofisticación y efectividad. Este enfoque garantiza que los ejercicios de Red Team reflejen el panorama actual de amenazas y contribuyan al desarrollo de una defensa más madura.

Metodologías profesionales del Red Team

Las actividades del Red Team no deben improvisarse, sino que deben apoyarse en metodologías estructuradas y reconocidas a nivel internacional, las cuales aportan orden, trazabilidad y consistencia a los ejercicios ofensivos. Entre estas metodologías se destaca el Penetration Testing Execution Standard (PTES), que define un conjunto de fases claramente delimitadas, incluyendo el reconocimiento, el modelado de amenazas, el análisis de vulnerabilidades, la explotación, la post-explotación y la elaboración de reportes. Este marco metodológico permite ejecutar pruebas sistemáticas y comparables en el tiempo.

El modelo Cyber Kill Chain permite estructurar las fases de un ataque avanzado, desde el reconocimiento hasta la exfiltración de información, facilitando la identificación de controles defensivos en cada etapa (Lockheed, 2015).

De igual forma, el modelo de la Cyber Kill Chain proporciona una estructura secuencial para replicar ataques utilizados por grupos APT, permitiendo analizar cada etapa del ciclo de ataque y evaluar la capacidad de detección y respuesta de la organización en cada una de ellas. Complementariamente, el marco MITRE ATT&CK ofrece un lenguaje común para mapear técnicas específicas empleadas durante los ejercicios, tales como la explotación de aplicaciones públicas (T1190), la ejecución de comandos (T1059), la recolección de cuentas (T1087), la comunicación de comando y control sobre HTTP/HTTPS (T1071) y la exfiltración de datos (T1041). El uso de estas metodologías fortalece la trazabilidad de los hallazgos y facilita la alineación entre los equipos Red Team, Blue Team y Purple Team.

Estrategias Avanzadas de Reconocimiento

El reconocimiento es la base de cualquier operación ofensiva. Entre las estrategias más efectivas se encuentran:

Reconocimiento Pasivo

El reconocimiento pasivo se llevó a cabo sin interactuar directamente con los sistemas objetivo, con el fin de minimizar la generación de alertas y evitar la detección temprana. En esta fase se realizaron actividades como el análisis de registros DNS, la revisión de metadatos presentes en documentos públicos, la enumeración de subdominios y la recopilación de inteligencia de fuentes abiertas (Open Source Intelligence – OSINT). Adicionalmente, se examinó la posible exposición de información en bases de datos públicas producto de filtraciones previas, utilizando servicios especializados como Have I Been Pwned y LeakCheck. Estas acciones permitieron construir un perfil inicial del objetivo y orientar las fases posteriores del ataque de manera más precisa y efectiva.

Reconocimiento Activo

El reconocimiento activo implicó la interacción directa con los sistemas objetivo, permitiendo identificar de forma detallada los servicios y configuraciones expuestas en la red. En esta fase se ejecutaron escaneos avanzados mediante la herramienta Nmap, con el propósito de detectar servicios accesibles, identificar versiones vulnerables y realizar fingerprinting del sistema operativo. Como parte del laboratorio, se utilizó el comando nmap -sV -O 10.10.10.5, cuyo resultado evidenció la presencia de un sistema operativo Windows 7 vulnerable, así como la exposición del puerto 445 con el protocolo SMBv1 activo. Estos hallazgos confirmaron la existencia de condiciones propicias para la explotación de la vulnerabilidad MS17-010, justificando la transición hacia la fase de explotación controlada.

Estrategias de Explotación

Las estrategias de explotación constituyen una fase crítica dentro de las operaciones del Red Team, ya que en esta etapa se seleccionan y aprovechan vulnerabilidades de alto impacto con el objetivo de obtener acceso inicial a los sistemas objetivo. La elección de las vulnerabilidades no se realiza de manera arbitraria, sino que responde a criterios de criticidad, nivel de exposición, facilidad de explotación y valor estratégico del activo comprometido, simulando el comportamiento de adversarios reales.

La explotación de Vulnerabilidades de Red

Se consideran ataques ampliamente documentados y utilizados en escenarios reales, como EternalBlue (MS17-010), BlueKeep sobre servicios RDP, PrintNightmare y la explotación de servicios expuestos tales como FTP, SSH y SMB. Durante el laboratorio desarrollado, se llevó a cabo la explotación de la vulnerabilidad MS17-010 mediante el módulo

exploit/windows/smb/ms17_010_eternalblue de Metasploit, lo cual permitió comprometer de forma controlada el sistema objetivo y avanzar hacia las fases de post-explotación.

La Explotación de Aplicaciones Web

Se orienta a identificar y aprovechar fallas en la lógica o en la validación de entradas de las aplicaciones, empleando técnicas como inyección SQL (SQL Injection), Cross-Site Scripting (XSS), Command Injection y cargas inseguras de archivos (insecure file upload). Para la ejecución de estas pruebas se utilizan herramientas especializadas como Burp Suite, SQLMap y Wfuzz, las cuales facilitan la automatización de ataques, el análisis de respuestas del servidor y la identificación de vulnerabilidades explotables en entornos web.

Explotación de Debilidades Humanas

La explotación de debilidades humanas constituye uno de los vectores de ataque más efectivos dentro de las operaciones del Red Team, dado que se basa en la manipulación psicológica de los usuarios más que en fallas técnicas del sistema. Esta fase se desarrolla mediante técnicas de ingeniería social orientadas a inducir a las personas a realizar acciones que comprometan la seguridad de la organización, tales como la entrega involuntaria de credenciales, la ejecución de archivos maliciosos o la habilitación de accesos no autorizados.

Entre las técnicas más utilizadas se encuentran el phishing, el spear phishing, el smishing, el vishing y el USB baiting, las cuales explotan factores como la confianza, la urgencia y el desconocimiento del usuario. Diversos estudios y experiencias prácticas han demostrado que este tipo de ataques presenta tasas de éxito superiores al 70 %, lo que confirma que el componente humano sigue siendo uno de los eslabones más vulnerables en la cadena de seguridad y refuerza la necesidad de programas continuos de concientización y capacitación en ciberseguridad.

Estrategias de post-explotación

Una vez obtenida una sesión activa en el sistema víctima, se da inicio a la fase de post-explotación, considerada una de las etapas más críticas dentro de un ejercicio de Red Team, ya que permite evaluar el impacto real de la intrusión y el nivel de control que un atacante puede alcanzar sobre la infraestructura comprometida.

En primer lugar, se realiza la enumeración interna, cuyo objetivo es recopilar información detallada del entorno comprometido. En esta etapa se identifican los usuarios locales y de dominio, los recursos compartidos en la red, las credenciales almacenadas en el sistema y los servicios que presentan configuraciones vulnerables. Para ello se emplean comandos nativos del sistema operativo, como net user, net group e ipconfig /all, los cuales permiten obtener información clave para planificar movimientos posteriores dentro de la red.

Posteriormente, se procede con la escalación de privilegios, fase orientada a obtener permisos de mayor nivel que permitan un control más amplio del sistema. Las vías más comunes incluyen la explotación de servicios mal configurados, la suplantación de tokens (*token impersonation*), el aprovechamiento de vulnerabilidades locales y el uso de credenciales filtradas o reutilizadas. En el laboratorio, este proceso se ejemplificó mediante el comando getsystem, el cual permite elevar privilegios hasta niveles administrativos o de sistema, evidenciando el riesgo que representan configuraciones inseguras.

Finalmente, se implementan mecanismos de persistencia, cuyo propósito es asegurar el acceso continuo al sistema comprometido incluso después de reinicios o cierres de sesión. Entre las técnicas empleadas se encuentran la creación de usuarios ocultos, la instalación de *backdoors* mediante servicios SSH, la modificación del registro del sistema, la inclusión de scripts de inicio

automático y la creación de servicios maliciosos. Estas acciones reflejan cómo un atacante avanzado puede mantener el control a largo plazo si no se aplican medidas adecuadas de detección y respuesta.

Movimiento lateral

El movimiento lateral corresponde a la fase en la que el atacante, una vez comprometido un sistema inicial, busca expandir su presencia dentro de la red interna con el objetivo de acceder a otros equipos, servicios o recursos críticos. Esta etapa se apoya en la información obtenida durante la enumeración interna y en el uso de credenciales válidas, permitiendo simular el comportamiento de amenazas avanzadas persistentes (Advanced Persistent Threats – APT). Entre las técnicas más comunes se encuentran el uso de Pass-the-Hash, Pass-the-Ticket, la reutilización de credenciales y el acceso remoto a través de protocolos como SMB, RDP y WinRM. Estas acciones evidencian cómo una segmentación deficiente y la falta de controles de acceso adecuados pueden facilitar la propagación del atacante dentro de la infraestructura.

Exfiltración de Información

La exfiltración de información tiene como finalidad la extracción de datos sensibles desde los sistemas comprometidos hacia un entorno controlado por el atacante. En esta fase se identifican y recopilan archivos críticos, bases de datos, credenciales y otra información de alto valor, los cuales pueden ser comprimidos, cifrados u ocultados para evadir mecanismos de detección. La exfiltración puede realizarse mediante distintos canales, como conexiones HTTP/HTTPS, túneles cifrados, servicios de almacenamiento en la nube o protocolos legítimos utilizados de forma abusiva. Este proceso permite dimensionar el impacto real de un incidente, especialmente en términos de confidencialidad y cumplimiento normativo.

Evasión de Controles Defensivos

La evasión de controles defensivos consiste en la aplicación de técnicas destinadas a evitar la detección por parte de soluciones de seguridad como antivirus, sistemas de detección y prevención de intrusos (IDS/IPS), EDR y SIEM. En esta etapa, el atacante puede emplear ofuscación de payloads, modificación de firmas, desactivación de servicios de seguridad, uso de procesos legítimos (living off the land) y ejecución de código en memoria para reducir la huella forense. Estas técnicas ponen de manifiesto la necesidad de contar con capacidades avanzadas de monitoreo, correlación de eventos y respuesta temprana, así como con una adecuada integración entre los equipos Blue Team y Purple Team.

Durante la fase de movimiento lateral, el atacante hace uso de diversas herramientas y protocolos legítimos del entorno Windows para desplazarse entre sistemas comprometidos sin levantar alertas inmediatas. Entre las herramientas más empleadas se encuentran PsExec, WMI, WinRM y RDP, las cuales permiten la ejecución remota de comandos, la administración de sistemas y el acceso interactivo a equipos internos utilizando credenciales válidas o tokens comprometidos. Adicionalmente, se aplican técnicas como Pass-the-Hash, que posibilitan la autenticación sin necesidad de conocer la contraseña en texto claro, incrementando la probabilidad de propagación dentro de la red cuando no existen controles adecuados de autenticación y segmentación.

De manera complementaria, se implementa el pivoting, una técnica que permite utilizar un sistema previamente comprometido como punto de acceso intermedio para alcanzar redes internas que no se encuentran expuestas directamente al atacante. Esta estrategia resulta especialmente relevante en entornos corporativos segmentados, donde ciertos segmentos de red solo son accesibles desde sistemas internos. En el laboratorio desarrollado, se aplicó esta técnica

mediante el uso del comando autoroute -s 10.10.20.0/24, lo que permitió enrutar el tráfico hacia una subred adicional y extender el alcance del ataque de forma controlada. Este escenario evidencia cómo la ausencia de controles de segmentación estrictos y de monitoreo interno puede facilitar la expansión de un atacante dentro de la infraestructura organizacional.

Estrategias de Evasión Frente a los Controles del Blue Team

Durante un ejercicio de Red Team, resulta fundamental aplicar estrategias orientadas a evitar la detección por parte de los mecanismos defensivos implementados por el Blue Team, con el fin de evaluar de manera realista la eficacia de los controles de seguridad existentes. Estas técnicas buscan reducir la huella del atacante y simular el comportamiento de amenazas avanzadas capaces de operar de forma sigilosa dentro de la infraestructura comprometida.

En relación con la evasión de soluciones antivirus, se emplean técnicas como la ofuscación de payloads, la modificación de firmas conocidas, el uso de crypters y la generación de payloads polimórficos. Estas prácticas permiten alterar la estructura del código malicioso sin modificar su funcionalidad, dificultando su detección mediante mecanismos basados en firmas estáticas y evidenciando las limitaciones de soluciones tradicionales de protección.

Por otra parte, la evasión de sistemas SIEM se basa en la reducción del ruido operativo y en la ejecución de acciones de manera controlada para evitar correlaciones automáticas de eventos. Entre las estrategias aplicadas se incluye la ejecución de actividades en horarios con menor nivel de monitoreo, la limitación de acciones repetitivas, el encadenamiento de comandos para reducir la generación de eventos y la eliminación de registros únicamente cuando el contexto lo permite. Estas técnicas ponen de manifiesto la importancia de contar con reglas de correlación robustas y monitoreo continuo, independientemente de la franja horaria.

Finalmente, la evasión de soluciones EDR se apoya principalmente en el uso de técnicas conocidas como Living off the Land (LoL), que consisten en aprovechar herramientas y funcionalidades nativas del sistema operativo para ejecutar acciones maliciosas sin introducir software externo. En este contexto, se destaca el uso de PowerShell sin macros, la ejecución de utilidades legítimas del sistema y frameworks ofensivos que operan en memoria, como Invoke-Mimikatz, PowerShell Empire y Cobalt Strike Beacon. Estas técnicas demuestran cómo un atacante puede operar de manera encubierta y refuerzan la necesidad de capacidades avanzadas de detección basadas en comportamiento y análisis contextual.

Simulación de Ataques Avanzados

El red team debe ser capaz de ejecutar simulaciones complejas como:

- Ransomware simulado (sin cifrar archivos reales)
- Compromiso de active directory
- Exfiltración de datos simulada
- Ataques desde el interior (insider threat)
- Persistencia de nivel rootkit (controlado)

Gestión y Documentación del Ataque

Toda acción ofensiva debe documentarse en:

- Registro técnico
- Bitácora de comandos

- Evidencias
- Capturas de pantalla
- Listado de vulnerabilidades
- Mapas att&ck

Relación con el escenario 5

Las estrategias aplicadas en el laboratorio demostraron:

- Deficiencias en smbv1
- Falta de parches
- Falta de monitoreo
- Controles insuficientes
- Alta exposición a exploits críticos

Esto permitió evidenciar la necesidad de un red team continuo.

Estrategias Blue Team

El blue team constituye la primera línea de defensa de una organización, responsable de la protección, monitoreo, detección de amenazas, análisis forense, contención y recuperación ante incidentes de seguridad. Su labor es continua y abarca no solo responder a ataques, sino prevenirlos mediante la implementación de políticas, controles y herramientas que fortalezcan la postura de seguridad.

Este capítulo detalla las estrategias de defensa operativa, técnicas y tácticas empleadas por un blue team profesional, así como su aplicación en el escenario 5 desarrollado en el laboratorio.

Enfoque Estratégico del Blue Team

Mientras el red team actúa como atacante, el blue team adopta un enfoque proactivo y reactivo, basado en:

La proactividad constituye el primer pilar de la estrategia defensiva del Blue Team y se enfoca en la implementación de acciones preventivas antes de la ocurrencia de un incidente de seguridad. Estas acciones incluyen la aplicación oportuna de parches de seguridad, el hardening de los sistemas, la correcta configuración de firewalls y soluciones EDR, así como la gestión continua de vulnerabilidades. De igual forma, se contempla la definición y actualización de políticas de seguridad y la capacitación permanente de los usuarios, reconociendo que el factor humano desempeña un papel crítico en la reducción de la superficie de ataque.

La reactividad agrupa las acciones ejecutadas durante y después de un ataque, orientadas a reducir su impacto y restablecer la operación normal de la organización. En esta fase, el Blue Team prioriza la detección temprana del incidente mediante mecanismos de monitoreo en tiempo real, seguida de la contención para limitar la propagación del ataque. Posteriormente, se realizan procesos de erradicación de la amenaza, recuperación y restauración de los sistemas afectados, complementados con actividades de análisis forense que permiten comprender el alcance del incidente, preservar evidencias y apoyar posibles acciones legales o disciplinarias.

Finalmente, la resiliencia representa el objetivo estratégico de largo plazo de la ciberseguridad organizacional. Este enfoque busca garantizar la continuidad del negocio incluso

frente a incidentes de alto impacto, minimizar las consecuencias operativas, reputacionales y legales, y extraer aprendizajes del ataque para fortalecer la postura de seguridad. A partir de estos aprendizajes, se optimizan los controles técnicos, operativos y humanos, cerrando el ciclo de mejora continua y reforzando la capacidad de la organización para enfrentar futuras amenazas de manera más eficaz.

Monitoreo y Detección

El blue team debe monitorear continuamente el entorno y detectar comportamientos anómalos.

SIEM (Security Information and Event Management)

Constituyen la herramienta central del Blue Team para la supervisión y gestión de la seguridad en entornos corporativos. Estas plataformas permiten la recolección y centralización de registros (logs) provenientes de múltiples fuentes, facilitando la correlación de eventos y la detección de patrones maliciosos que podrían pasar desapercibidos de forma aislada. A través del análisis de estos datos, el SIEM contribuye a la identificación de cuentas sospechosas, el monitoreo del tráfico de red y la generación de alertas tempranas ante comportamientos anómalos. Entre las soluciones SIEM más utilizadas en entornos empresariales se encuentran Splunk, Wazuh, QRadar, ELK Stack (Elastic) y Azure Sentinel, las cuales ofrecen capacidades avanzadas de análisis, visualización y respuesta ante incidentes.

EDR (Endpoint Detection and Response)

Están orientadas a la protección y monitoreo de los endpoints, proporcionando visibilidad detallada sobre la actividad de los equipos finales. Tecnologías como CrowdStrike Falcon, SentinelOne y Microsoft Defender for Endpoint (ATP) permiten la detección de malware

avanzado, el bloqueo de ataques de ransomware y la aplicación de análisis de comportamiento (behavioral analysis) para identificar actividades sospechosas. Adicionalmente, estas plataformas incorporan mecanismos de contención automática del endpoint, lo que permite aislar equipos comprometidos de manera rápida y efectiva para evitar la propagación del ataque.

NDR (Network Detection and Response)

Se enfocan en el monitoreo continuo del tráfico de red, con el objetivo de identificar comportamientos anómalos y actividades maliciosas a nivel de comunicación. Estas tecnologías permiten detectar tráfico lateral no autorizado, identificar canales de comando y control (C2) y reconocer patrones de tráfico inusuales que podrían indicar la presencia de un atacante dentro de la red. Herramientas como Zeek y Suricata desempeñan un papel fundamental en este ámbito, aportando capacidades de inspección profunda del tráfico y generación de alertas basadas en comportamiento, complementando así las funciones del SIEM y el EDR dentro de una estrategia de defensa integral.

Gestión de Vulnerabilidades en el Enfoque del Blue Team

La gestión de vulnerabilidades constituye una función esencial del Blue Team, orientada a la identificación, evaluación y priorización de debilidades en los sistemas antes de que puedan ser explotadas por el Red Team o por atacantes reales. Este proceso permite reducir de manera proactiva la superficie de ataque de la organización y fortalecer su postura de seguridad frente a amenazas internas y externas.

Como parte de este enfoque, se realizan escaneos periódicos de seguridad mediante herramientas especializadas como OpenVAS, Nessus y QualysGuard. Estos escaneos permiten detectar parches faltantes, configuraciones inseguras, servicios expuestos y aplicaciones

vulnerables, proporcionando una visión integral del estado de seguridad de la infraestructura tecnológica. La periodicidad y el alcance de estos escaneos deben ajustarse al nivel de criticidad de los activos y a los cambios constantes del entorno.

Posteriormente, los hallazgos identificados son sometidos a un proceso de evaluación de riesgo, en el cual se priorizan las vulnerabilidades considerando factores como la criticidad asignada por el puntaje CVSS, el nivel de exposición real del activo afectado, el impacto potencial sobre la operación y la probabilidad de explotación. Esta priorización permite enfocar los esfuerzos de mitigación en aquellas debilidades que representan un mayor riesgo para la organización.

Finalmente, la gestión de vulnerabilidades se consolida a través de un ciclo de remediación estructurado, que incluye la identificación y clasificación de las vulnerabilidades, su priorización, la asignación de responsables para su tratamiento, la aplicación de parches o controles compensatorios y la verificación posterior de las correcciones implementadas. Este ciclo continuo garantiza una mejora progresiva de la seguridad y refuerza la capacidad del Blue Team para anticiparse a escenarios de ataque.

Estrategias de Hardening en la Defensa del Blue Team

El hardening consiste en el proceso de fortalecimiento de sistemas, redes y aplicaciones con el objetivo de reducir la superficie de ataque y minimizar las posibilidades de explotación por parte de actores maliciosos. Esta estrategia forma parte fundamental de las acciones preventivas del Blue Team y se basa en la eliminación de configuraciones inseguras, la aplicación de controles restrictivos y la adopción de buenas prácticas de seguridad.

En cuanto al hardening del sistema operativo, se implementan acciones orientadas a reforzar la seguridad de los equipos y servidores. Estas incluyen la deshabilitación de protocolos obsoletos como SMBv1, la correcta configuración del cortafuegos, el establecimiento de políticas de contraseñas robustas, la eliminación de servicios innecesarios y la aplicación oportuna de parches de seguridad. Estas medidas permiten reducir significativamente las oportunidades de explotación de vulnerabilidades conocidas y mejorar la postura de seguridad general del sistema.

El hardening de Active Directory resulta especialmente crítico en entornos empresariales, dado que este servicio concentra la gestión de identidades y privilegios. En esta área se aplican controles como la reducción de privilegios excesivos, la implementación de restricciones de inicio de sesión, la protección de cuentas privilegiadas y la monitorización avanzada de las actividades dentro del directorio. Para apoyar estas tareas, se emplean herramientas especializadas como BloodHound, utilizada para auditorías de relaciones y permisos, y PingCastle, que permite evaluar el nivel de madurez y exposición de seguridad de Active Directory.

Por su parte, el hardening de redes se orienta a limitar el movimiento no autorizado dentro de la infraestructura mediante la implementación de VLAN segmentadas, microsegmentación basada en el modelo Zero Trust, la activación de sistemas IDS/IPS, el apagado de puertos no utilizados y la restricción del tráfico lateral. Estas medidas dificultan la propagación de un atacante y fortalecen los controles perimetrales e internos de la red.La adopción del modelo Zero Trust elimina la confianza implícita dentro de la red y refuerza los mecanismos de validación continua (Ghasemshirazi, 2023).

Finalmente, el hardening de aplicaciones se centra en la protección de los sistemas desarrollados o utilizados por la organización, aplicando mecanismos como la validación adecuada de entradas, la implementación de Web Application Firewalls (WAF), la revisión y restricción de permisos y la protección de interfaces de programación de aplicaciones (API). Estas acciones contribuyen a mitigar vulnerabilidades comunes en aplicaciones web y servicios expuestos, reforzando la seguridad desde la capa de software. El mapeo de vulnerabilidades CVE hacia técnicas MITRE ATT&CK permite mejorar la trazabilidad del ataque y la priorización defensiva (Grigorescu, 2022).

Respuesta a Incidentes

El blue team ejecuta una metodología estructurada conforme al nist sp 800-61 rev. 2.

Fase 1: Preparación

Incluye:

- Políticas de seguridad
- Procedimientos documentados
- Herramientas listas
- Accesos controlados
- Roles de respuesta definidos

Fase 2: Detección y Análisis

El blue team confirmó la intrusión durante el escenario 5 examinando:

- Eventos en el visor de sucesos
- Conexiones smb sospechosas
- Creación de usuarios inusuales
- Uso de herramientas no autorizadas

Indicadores en este caso:

- Tráfico sobre el puerto 445es dec
- Sesiones remotas de meterpreter
- Fallos de autenticación

Fase 3: Contención

Acciones tomadas:

- Aislamiento del equipo comprometido
- Bloqueo temporal del puerto smb
- Detención de procesos desconocidos
- Deshabilitar cuentas sospechosas

Fase 4: Erradicación

Incluyó:

- Eliminación de payloads maliciosos

- Limpieza de backdoors
- Desinstalación de servicios manipulados
- Aplicación de parche ms17-010

Fase 5: Recuperación

Acciones:

- Reinstalación segura de componentes
- Validación del funcionamiento
- Restauración desde backups

Fase 6: Lecciones Aprendidas

Se concluyó que:

- La red estaba vulnerable
- El blue team no tenía alertas efectivas
- El hardening era insuficiente
- La segmentación no existía

Implementación del Modelo Zero Trust en Blue Team

Zero trust requiere:

- Autenticación continua

- Validación granular
- No confiar en nadie por defecto

Aplicaciones:

- Mfa obligatorio
- Políticas de mínimo privilegio
- Control de dispositivos
- Revisión constante de accesos

Análisis de logs y forense digital

El blue team debe ser capaz de:

Identificar Evidencia

- Archivos modificados
- Usuarios creados
- Servicios instalado

Realizar Análisis Forense

Herramientas:

- Autopsy
- Ftk imager
- Volatility

Documentar Evidencia

Incluye:

- Hashes
- Cadena de custodia
- Capturas
- Trazabilidad

Comunicación y Coordinación

El blue team interactúa con:

- Equipo directivo
- Departamento legal
- Comunicaciones
- Mesa de ayuda
- Red team

Buena comunicación evita:

- Pánico innecesario
- Mal manejo de incidentes
- Divulgación no autorizada

Aprendizaje Continuo y Simulaciones

El blue team debe practicar regularmente mediante:

- Simulaciones de ataque (purple team)
- Pruebas de penetración internas
- Ejercicios de phishing controlado
- Entrenamiento del personal

El Blue Team representa un pilar fundamental dentro de la estrategia integral de ciberseguridad organizacional, al garantizar la protección continua de los activos de información mediante procesos sistemáticos de detección, contención y prevención de incidentes. Su labor trasciende la respuesta reactiva, ya que promueve una cultura de vigilancia permanente y mejora continua orientada a la reducción del riesgo. La articulación con el Red Team, a través del enfoque Purple Team, fomenta un modelo colaborativo en el que el conocimiento derivado de los ejercicios ofensivos se convierte en insumos estratégicos para el fortalecimiento de los controles defensivos. Esta sinergia contribuye de manera directa al incremento de la madurez de seguridad y a la consolidación de una postura resiliente frente a amenazas cada vez más sofisticadas (MITRE, 2023).

Relación con Aspectos Legales y Éticos

Las actividades de red team y blue team no pueden realizarse sin una comprensión sólida de los aspectos legales y éticos que regulan la ciberseguridad tanto en colombia como a nivel internacional. La legislación, los estándares, las políticas internas y los principios éticos definen

los límites del comportamiento aceptado y protegen a la organización, a sus clientes y a los profesionales involucrados.

Este capítulo analiza detalladamente la relación entre las prácticas de ciberseguridad realizadas en las etapas 1 a 4 y su alineación con la normativa vigente y los marcos éticos aplicables.

Importancia de La Legalidad en la Ciberseguridad

La legalidad constituye un pilar fundamental en el ejercicio profesional de la ciberseguridad, especialmente en el desarrollo de actividades ofensivas y defensivas como las pruebas de penetración, el monitoreo de sistemas y la respuesta a incidentes. Toda acción realizada en este ámbito debe estar respaldada por una autorización formal, contratos claramente definidos, acuerdos de confidencialidad y límites de alcance establecidos de manera precisa, garantizando en todo momento el respeto por la privacidad y la protección de la información. La ausencia de estos elementos puede derivar en consecuencias legales graves, ya que un ejercicio de Red Team sin el debido marco legal puede configurar delitos penales, mientras que actuaciones inadecuadas del Blue Team pueden vulnerar derechos fundamentales de las personas y organizaciones. Las pruebas de penetración siguen un enfoque sistemático orientado a la identificación y explotación controlada de vulnerabilidades.

Desde esta perspectiva, la legalidad en ciberseguridad cumple un rol esencial al delimitar responsabilidades entre las partes involucradas, proteger al profesional frente a posibles reclamaciones y reducir los riesgos jurídicos asociados a la ejecución de actividades técnicas. Asimismo, contribuye a garantizar la transparencia en los procesos de seguridad y a promover la confianza entre las organizaciones, los profesionales y los usuarios, fortaleciendo así la

legitimidad y sostenibilidad de las prácticas de ciberseguridad en entornos corporativos y gubernamentales.

Marco legal Colombiano y Normativo Aplicable a la Ciberseguridad

El marco jurídico colombiano proporciona un sustento normativo sólido para el ejercicio profesional de la ciberseguridad, estableciendo tanto las responsabilidades legales de los actores involucrados como las sanciones aplicables frente a conductas maliciosas o negligentes. Este marco resulta especialmente relevante en escenarios de pruebas ofensivas y defensivas, donde la línea entre una actividad legítima y un delito informático depende del cumplimiento estricto de la ley, la autorización previa y el respeto de los derechos fundamentales.

La Ley 1273 de 2009, que modifica el Código Penal colombiano en materia de protección de la información y los datos, representa el principal referente legal frente a los delitos informáticos. Esta norma tipifica conductas como el acceso abusivo a sistemas informáticos, la interceptación ilícita de datos, el daño informático, la suplantación de sitios web, el uso de software malicioso y la violación de datos personales. En el contexto de las actividades de Red Team y Blue Team, esta ley establece límites claros al indicar que todo acceso a sistemas debe estar debidamente autorizado, que la interceptación de comunicaciones sin consentimiento constituye un delito y que la alteración, destrucción o extracción de información solo es legal cuando se realiza en entornos controlados y con fines previamente definidos. De esta manera, la Ley 1273 actúa como un marco de protección tanto para las organizaciones como para los profesionales de ciberseguridad, siempre que sus actuaciones se encuentren documentadas y avaladas contractualmente.

Ley 1581 de 2012, junto con sus decretos reglamentarios, regula el tratamiento de datos personales y establece principios fundamentales como la legalidad, la finalidad, la libertad, la veracidad, la transparencia, el acceso y la circulación restringida, así como la seguridad y la confidencialidad de la información. Durante ejercicios de seguridad ofensiva y defensiva, es habitual el manejo de credenciales, registros de actividad, datos sensibles y metadatos, lo que obliga a los equipos técnicos a garantizar que la información recolectada sea utilizada únicamente para el propósito autorizado, protegida contra accesos no autorizados y eliminada una vez cumplido el objetivo del ejercicio. El incumplimiento de estas disposiciones puede generar sanciones administrativas y responsabilidades legales para la organización y los profesionales involucrados.

La Constitución Política de Colombia, en su artículo 15, consagra el derecho fundamental a la intimidad personal y familiar, así como al buen nombre y a la protección de los datos personales. En el marco de operaciones de Red Team, este principio constitucional implica restricciones claras sobre la revisión de correos electrónicos, la interceptación de comunicaciones privadas y la recopilación de información personal, las cuales solo pueden realizarse con autorización expresa y dentro de los límites definidos por el empleador o el titular de la información. Este mandato constitucional refuerza la necesidad de que toda actividad de ciberseguridad esté respaldada por políticas internas claras y consentimiento informado.

Estándar ISO/IEC 27001 se posiciona como un referente internacional para la implementación de sistemas de gestión de seguridad de la información (SGSI). Este estándar promueve un enfoque basado en la gestión del riesgo, obligando a las organizaciones a identificar, analizar y tratar los riesgos asociados a la información, así como a documentar políticas, procedimientos y controles de seguridad. ISO/IEC 27001 establece la necesidad de

evaluar continuamente la eficacia de los controles implementados, gestionar incidentes de seguridad y asegurar el cumplimiento de los requisitos legales y contractuales aplicables.

ISO/IEC 27001, se destacan controles especialmente relevantes para los ejercicios de Red Team y Blue Team, como A.12, orientado a la seguridad operacional y al control de los procesos técnicos; A.14, enfocado en la seguridad durante el desarrollo y mantenimiento de sistemas; A.16, relacionado con la gestión de incidentes de seguridad de la información; y A.18, que aborda el cumplimiento de requisitos legales, regulatorios y contractuales. La adopción de estos controles no solo fortalece la postura de seguridad de la organización, sino que también contribuye a garantizar que las actividades de ciberseguridad se desarrollen de manera legal, ética y alineada con estándares internacionales. (International Organization for Standardization [ISO], 2013)

Ética Profesional en Operaciones de Red Team y Blue Team

La ética profesional constituye el fundamento de toda práctica segura, responsable y confiable en el ámbito de la ciberseguridad. En las operaciones de Red Team y Blue Team, donde se tiene acceso privilegiado a sistemas, información sensible y procesos críticos de la organización, el comportamiento ético del profesional resulta tan importante como sus competencias técnicas, ya que de él depende la legitimidad y el impacto real de las actividades desarrolladas.

Principios Éticos Clave

Un profesional de ciberseguridad debe basarse en:

Integridad

El principio de integridad exige que el profesional de ciberseguridad actúe con honestidad y rigor técnico durante las operaciones de Red Team y Blue Team. Esto implica no alterar, ocultar ni manipular información sin autorización expresa, así como preservar la veracidad de los datos obtenidos y de los resultados reportados. La integridad garantiza que los hallazgos reflejen fielmente el estado real de seguridad de la organización y que las decisiones tomadas a partir de ellos sean confiables y objetivas.

Responsabilidad

La responsabilidad se refiere a la obligación del profesional de asumir plenamente las consecuencias de las acciones ejecutadas durante un ejercicio de seguridad. En este sentido, el especialista debe actuar dentro de los límites establecidos, documentar adecuadamente cada actividad realizada y responder ante la organización por cualquier impacto generado. Este principio refuerza la necesidad de una planificación cuidadosa y de una ejecución controlada de las pruebas técnicas.

Transparencia

La transparencia implica informar de manera clara, completa y oportuna a la organización o al cliente sobre los hallazgos, vulnerabilidades identificadas y riesgos asociados. Un profesional ético no minimiza ni exagera los resultados, sino que comunica la información de forma comprensible y basada en evidencia técnica, permitiendo que la organización tome decisiones informadas para fortalecer su postura de seguridad.

Autorización

El principio de autorización establece que toda actividad de ciberseguridad debe contar con aprobación formal y documentada antes de su ejecución. Esto incluye la definición precisa

del alcance, los objetivos, las técnicas permitidas y las restricciones operativas. La autorización protege tanto a la organización como al profesional, al delimitar claramente las responsabilidades y evitar interpretaciones indebidas sobre la legalidad de las acciones realizadas.

Respeto

El respeto se manifiesta en la protección de la privacidad, los recursos y el tiempo de la organización durante las operaciones de seguridad. Este principio implica evitar accesos innecesarios a información sensible, no interferir con procesos críticos y actuar siempre considerando el impacto potencial sobre los usuarios y los sistemas. El respeto fortalece la relación de confianza entre las partes involucradas en el ejercicio.

No maleficencia

El principio de no maleficencia obliga al profesional a evitar causar daño, incluso cuando se simulan escenarios de ataque reales. Esto implica diseñar y ejecutar las pruebas de forma controlada, minimizando riesgos y asegurando que la continuidad del negocio no se vea comprometida. La no maleficencia refuerza el carácter preventivo y formativo de las operaciones de Red Team y Blue Team, priorizando la mejora de la seguridad sobre la generación de impactos negativos.

Ética en las Operaciones del Red Team

Las operaciones de Red Team implican el uso de herramientas y técnicas que, si no se aplican de manera controlada, pueden generar consecuencias graves para la organización. Entre los riesgos asociados se encuentran la pérdida de datos, la interrupción de servicios críticos, la exposición de información sensible y, en escenarios extremos, la destrucción accidental de sistemas. Por esta razón, el ejercicio del Red Team debe regirse estrictamente por principios

éticos, legales y técnicos que garanticen que las pruebas se realicen de forma responsable y segura.

Uno de los elementos fundamentales en este contexto son las reglas de compromiso (Rules of Engagement – ROE), las cuales establecen el marco operativo dentro del cual se desarrollan las actividades ofensivas. Las ROE definen con claridad los sistemas permitidos, las técnicas autorizadas, los horarios de ejecución de las pruebas, los límites técnicos, las acciones explícitamente prohibidas y el manejo adecuado de la evidencia obtenida. Estas reglas permiten controlar el impacto de las pruebas y aseguran que las actividades del Red Team se mantengan dentro de un entorno ético y legalmente aceptable.

De manera complementaria, el alcance de la prueba (scope) constituye un componente crítico de la ética en el Red Team. El scope debe especificar de forma precisa las direcciones IP autorizadas, los servicios que pueden ser evaluados, los tipos de ataques permitidos y el uso autorizado de técnicas de ingeniería social. La ausencia de un alcance claramente definido convierte cualquier acción ofensiva en una actividad potencialmente ilegal, ya que elimina la base de autorización que legitima las pruebas de seguridad.

Asimismo, existen prohibiciones éticas explícitas que el Red Team debe respetar en todo momento. Entre ellas se incluyen la eliminación de evidencias sin autorización, la modificación de archivos sensibles, la exfiltración de datos reales, la explotación de sistemas no incluidos en el alcance definido, la divulgación de vulnerabilidades a terceros y el uso de herramientas no aprobadas. El incumplimiento de estas prohibiciones no solo compromete la ética profesional, sino que también puede acarrear consecuencias legales y disciplinarias.

Evaluación Ética del Acuerdo de Confidencialidad Analizado

En la etapa 2 se revisó un acuerdo de confidencialidad con serias deficiencias éticas:

- Permitía interceptar comunicaciones sin consentimiento
- Exigía al profesional encubrir actividades ilegales
- Autorizaba manipular información sensible sin supervisión
- No delimitaba alcance
- Violaba principios de privacidad

Este acuerdo:

- Va en contra de la ética profesional
- Podría implicar delitos penales
- Invalida cualquier prueba ofensiva
- Pone al profesional en riesgo jurídico

Relación Entre Aspectos Legales y el Escenario 5

El escenario 5 integra lo aprendido:

- En la etapa 3 (red team), se explotó ms17-010 de manera controlada, algo que sin autorización sería ilegal.
- En la etapa 4 (blue team), se analizaron logs, lo que debe hacerse respetando la privacidad de la información.
- La creación de backdoors (persistencia) requiere un alcance aprobado.

- El análisis forense debe respetar cadena de custodia.
- Toda prueba debe incluir un contrato válido y ético.

Recomendaciones Estratégicas

Las recomendaciones estratégicas representan el conjunto de acciones técnicas, administrativas, operativas y legales que una organización debe implementar para fortalecer su postura de ciberseguridad. Estas recomendaciones se basan en el análisis de vulnerabilidades detectadas, los comportamientos del adversario simulados en el escenario 5, la respuesta del blue team, y la evaluación ética y legal desarrollada en capítulos anteriores.

Recomendaciones para Fortalecer las Capacidades del Red Team

El Red Team debe evolucionar de manera constante para simular ataques cada vez más realistas, complejos y alineados con las amenazas actuales. Esta evolución es clave para que las organizaciones puedan identificar debilidades reales en sus controles de seguridad antes de que sean explotadas por atacantes externos. En este sentido, se proponen las siguientes recomendaciones estratégicas.

En primer lugar, se recomienda formalizar un ciclo continuo de ejercicios de Red Team, evitando la realización de pruebas aisladas o esporádicas. Para ello, es conveniente programar simulaciones de forma trimestral, complementar estas actividades con pruebas de penetración continuas y desarrollar ejercicios conjuntos entre Red Team y Blue Team bajo un enfoque de Purple Team. Asimismo, resulta fundamental documentar de manera sistemática los hallazgos obtenidos en cada ejercicio, lo que permite identificar brechas recurrentes y medir la evolución de la postura de seguridad de la organización a lo largo del tiempo.

Adicionalmente, el Red Team debe actualizar permanentemente sus exploits y técnicas de ataque, tomando como referencia el marco MITRE ATT&CK. Esto implica mantenerse al día en tácticas relacionadas con la evasión de soluciones EDR, el uso de técnicas Living off the Land (LoL), métodos de exfiltración sigilosa de información y mecanismos de comando y control (C2) diseñados para evitar la detección. Para facilitar este proceso, se recomienda mantener un repositorio interno de tácticas, técnicas y procedimientos (TTPs) que sea revisado y actualizado de manera semanal.

Otra recomendación clave consiste en integrar inteligencia de amenazas (Threat Intelligence) dentro de la planeación de los ejercicios de Red Team. Las simulaciones deben basarse en amenazas reales, considerando el contexto nacional y regional, las tendencias específicas del sector, la actividad de grupos APT relevantes y las vulnerabilidades recientemente explotadas en escenarios reales. Este enfoque permite replicar ataques modernos y relevantes, evitando el uso de técnicas obsoletas que no reflejan el panorama actual de amenazas.

Asimismo, es importante ampliar y fortalecer las capacidades de ingeniería social, dado que el factor humano continúa siendo uno de los principales vectores de ataque. Las pruebas deben incluir escenarios controlados de phishing, smishing, vishing, campañas de spoofing y técnicas de USB baiting. Para lograrlo, se recomienda crear entornos de phishing simulados, documentar los patrones de engaño que resulten más efectivos y diseñar estrategias específicas enfocadas en cargos críticos dentro de la organización, como personal directivo o áreas con acceso privilegiado.

Finalmente, se debe aplicar buenas prácticas de documentación, asegurando que los informes entregados por el Red Team sean claros, completos y adaptados a diferentes audiencias. Esto implica generar reportes técnicos, ejecutivos y comparativos, acompañados de anexos,

capturas e indicadores relevantes. Los reportes deben incluir de manera estructurada el impacto del hallazgo, la vulnerabilidad identificada, el nivel de riesgo asociado, la recomendación de mitigación, el mapeo correspondiente a MITRE ATT&CK y las evidencias técnicas que respalden cada conclusión. Una documentación de calidad facilita la toma de decisiones y maximiza el valor de los ejercicios de Red Team para la organización.

Recomendaciones para Fortalecer las Capacidades del Blue Team

El Blue Team constituye la columna vertebral de la defensa corporativa, ya que es responsable de la detección, análisis y respuesta frente a amenazas que afectan la confidencialidad, integridad y disponibilidad de los activos de información. Para fortalecer sus capacidades y mejorar la postura de seguridad de la organización, se plantean las siguientes recomendaciones estratégicas.

En primer lugar, se recomienda implementar un Centro de Operaciones de Seguridad (SOC) que permita centralizar las funciones de monitoreo y respuesta ante incidentes. Un SOC proporciona capacidades de monitoreo continuo 24/7, respuesta inmediata a eventos de seguridad, correlación avanzada de eventos, integración de inteligencia de ciberamenazas y control centralizado de la infraestructura de seguridad. Para cumplir con estos objetivos, el SOC debe integrar tecnologías como SIEM, EDR, NDR y firewalls de nueva generación, además de contar con analistas de seguridad organizados por niveles (Nivel 1, 2 y 3), garantizando una atención escalonada y especializada de los incidentes.

Adicionalmente, resulta fundamental fortalecer la capacidad de detección mediante reglas basadas en el marco MITRE ATT&CK. El SIEM debe incorporar reglas personalizadas orientadas a identificar tácticas y técnicas comunes utilizadas por los atacantes, tales como el

movimiento lateral (T1021), el uso de Pass-the-Hash (T1550), el abuso de PowerShell (T1059) y la persistencia mediante servicios del sistema (T1543). El mapeo sistemático de detecciones a MITRE ATT&CK permite mejorar la eficacia de las alertas, reducir falsos positivos y facilitar la comprensión del comportamiento del adversario.

Asimismo, se recomienda implementar un sistema formal de gestión de vulnerabilidades que permita identificar y corregir debilidades de manera proactiva. En este proceso, el Blue Team debe realizar escaneos de vulnerabilidades con una periodicidad semanal, priorizar aquellas con puntajes CVSS iguales o superiores a 7.0, remediar fallos críticos en un plazo no mayor a 48 horas y auditar de forma constante los activos expuestos. Esta práctica contribuye a reducir significativamente la superficie de ataque y a prevenir incidentes antes de que ocurran.

Otra recomendación clave es aplicar un plan estructurado de respuesta a incidentes, alineado con la guía NIST SP 800-61. Dicho plan debe contemplar las fases de preparación, detección, contención, erradicación, recuperación y lecciones aprendidas, además de definir de manera clara los roles y responsabilidades de cada miembro del equipo. Un plan bien definido permite actuar de forma coordinada y eficiente durante un incidente, minimizando su impacto operativo y reputacional.

De igual forma, se aconseja realizar pruebas forenses de manera regular, con el objetivo de fortalecer la capacidad de investigación y análisis posterior a un incidente. Estas pruebas deben incluir la captura de memoria RAM, la verificación de la integridad de los discos, la identificación de mecanismos de persistencia y el análisis de procesos sospechosos. La práctica constante de estas actividades mejora la preparación del equipo y garantiza una respuesta más efectiva ante incidentes reales.

Finalmente, es imprescindible mejorar el monitoreo y la observabilidad de la infraestructura, habilitando registros avanzados, centralizando eventos de seguridad, auditando los comandos ejecutados en los sistemas y activando herramientas como Sysmon para aumentar la visibilidad sobre el comportamiento de los endpoints. Un mayor nivel de observabilidad permite detectar anomalías de manera temprana y fortalece la capacidad del Blue Team para anticiparse a amenazas complejas.

Recomendaciones de Arquitectura y Hardening

El hardening constituye uno de los pilares fundamentales de la ciberseguridad moderna, ya que permite reducir de manera significativa la superficie de ataque y limitar el impacto de posibles incidentes. Una arquitectura bien diseñada, combinada con controles técnicos robustos, fortalece la postura de seguridad de la organización frente a amenazas cada vez más sofisticadas.

En este sentido, se recomienda adoptar una arquitectura Zero Trust, basada en el principio de no confiar en ningún usuario, dispositivo o sistema por defecto. Este enfoque implica la validación constante de identidades y accesos, la segregación extrema de los recursos y la aplicación estricta del principio de privilegios mínimos. Para su correcta implementación, Zero Trust requiere la integración de mecanismos como autenticación multifactor (MFA), soluciones SIEM y EDR, autorización contextual basada en riesgo y microsegmentación de la red, garantizando que cada acceso sea evaluado de forma dinámica.

De manera complementaria, resulta esencial implementar una adecuada segregación de redes, mediante técnicas de segmentación y microsegmentación. Esta estrategia permite evitar el movimiento lateral de los atacantes, reducir el impacto de un compromiso inicial y contener amenazas internas. Se recomienda la creación de VLAN diferenciadas por departamentos, la

segmentación de servidores críticos y el aislamiento de dispositivos IoT, los cuales suelen presentar mayores riesgos de seguridad.

Asimismo, se debe eliminar el uso de protocolos inseguros, deshabilitando tecnologías obsoletas o vulnerables como SMBv1, Telnet y FTP, así como restringiendo el uso de RDP sin MFA y de servicios HTTP sin cifrado TLS. La eliminación de estos protocolos reduce significativamente la exposición a ataques conocidos y vulnerabilidades ampliamente explotadas.

Otra medida clave es el control estricto de privilegios, aplicando de forma consistente el principio de mínimos privilegios, el control de cuentas privilegiadas y el uso de soluciones de Privileged Identity Management (PIM) y Privileged Access Management (PAM). Adicionalmente, se recomienda realizar auditorías periódicas de credenciales para detectar accesos innecesarios, cuentas obsoletas o configuraciones inseguras.

En cuanto a la gestión de actualizaciones, se deben establecer políticas de parcheo estrictas, que contemplen el parcheo automático en sistemas no críticos y la aplicación manual de parches en sistemas críticos, previa validación en entornos de prueba. También se recomienda el seguimiento constante de los boletines mensuales de seguridad de Microsoft (Patch Tuesday) y de otros fabricantes relevantes, con el fin de reducir la ventana de exposición ante vulnerabilidades conocidas.

Recomendaciones Legales y Éticas

Desde una perspectiva legal y ética, se recomienda formalizar acuerdos claros de confidencialidad y alcance antes de ejecutar cualquier actividad de ciberseguridad ofensiva o defensiva. Estos documentos deben especificar de manera explícita los permisos otorgados, los horarios de prueba, las direcciones IP autorizadas, las acciones prohibidas, las políticas de

manejo de datos y los procedimientos para la recolección y custodia de evidencia. Una documentación adecuada protege tanto a la organización como a los profesionales involucrados.

La organización debe cumplir estrictamente con la Ley 1273 de 2009, la Ley 1581 de 2012 y la normativa internacional aplicable, garantizando el respeto por la privacidad, evitando interceptaciones no autorizadas, protegiendo los datos personales y estableciendo mecanismos claros para la notificación y gestión de incidentes de seguridad. El cumplimiento normativo no solo reduce riesgos jurídicos, sino que fortalece la confianza y la transparencia organizacional.

Adicionalmente, se recomienda crear un código ético interno de ciberseguridad, que defina claramente las conductas permitidas y prohibidas, los procedimientos disciplinarios, las técnicas autorizadas y las obligaciones de reporte. Este código debe servir como guía para los equipos Red Team y Blue Team, reforzando una cultura de responsabilidad, legalidad y profesionalismo.

Recomendaciones de Capacitación y Cultura Organizacional

La cultura organizacional desempeña un papel clave en la prevención de incidentes de seguridad, dado que el factor humano continúa siendo uno de los principales vectores de ataque. Por ello, se recomienda implementar programas de capacitación continua para todo el personal, enfocados en temas como phishing, seguridad digital, manejo seguro de contraseñas y buenas prácticas en el uso del correo electrónico y otros canales de comunicación. El factor humano continúa siendo uno de los principales vectores de ataque, especialmente mediante técnicas de ingeniería social que explotan la confianza y el desconocimiento del usuario final (Buitrago, 2018; Gomez, 2022; Ingeniería, 2015).

La organización debe realizar simulaciones periódicas de ataques, incluyendo ejercicios controlados de Red Team, simulaciones de respuesta del Blue Team, ejercicios colaborativos de Purple Team y campañas internas de phishing. Estas actividades permiten evaluar el nivel de preparación del personal y mejorar la capacidad de detección y respuesta ante incidentes reales.

Finalmente, se sugiere crear un programa de concientización continua en ciberseguridad, que sea actualizado de forma periódica según el perfil del personal. Para cargos operativos, se recomienda una actualización trimestral, mientras que para el personal administrativo una actualización semestral resulta adecuada. Este enfoque garantiza que la organización mantenga una cultura de seguridad activa y adaptada a la evolución constante de las amenazas.

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: Seminario

https://youtu.be/b25Kiuf_AXw

Conclusiones

El análisis integral de las actividades realizadas en el marco del anexo 6 – escenario 5, sumado al estudio de las etapas 1 a 4, permite concluir que los equipos red team y blue team desempeñan un papel fundamental en la construcción, evaluación y fortalecimiento de la seguridad de la información dentro de una organización. El desarrollo de este informe demuestra cómo la ciberseguridad moderna requiere un enfoque interdisciplinario donde convergen elementos técnicos, éticos, legales y operativos para garantizar la protección de infraestructuras críticas y datos sensibles.

El desarrollo de este trabajo permitió evidenciar que la ciberseguridad moderna requiere un enfoque integral que combine capacidades técnicas avanzadas, marcos normativos claros y principios éticos sólidos. A través del análisis de las operaciones de Red Team y Blue Team, se demostró que la simulación controlada de ataques constituye una herramienta fundamental para identificar debilidades reales en la infraestructura tecnológica, siempre que estas actividades se realicen dentro de límites legales y con autorización expresa.

Los ejercicios de Red Team desarrollados reflejan cómo vulnerabilidades técnicas, configuraciones inseguras y debilidades humanas pueden ser explotadas de manera encadenada para comprometer sistemas críticos. Este análisis pone de manifiesto que la seguridad no puede depender exclusivamente de controles perimetrales, sino que debe abordarse desde una perspectiva de defensa en profundidad, donde la detección temprana, la segmentación de redes y la gestión adecuada de privilegios desempeñan un papel clave.

Por su parte, el enfoque del Blue Team evidencia la importancia de contar con capacidades robustas de monitoreo, análisis y respuesta ante incidentes. La integración de tecnologías como SIEM, EDR y NDR, junto con procesos estructurados de gestión de

vulnerabilidades, hardening y respuesta a incidentes, permite reducir significativamente el impacto de los ataques y fortalecer la resiliencia organizacional. Asimismo, la adopción de arquitecturas Zero Trust se consolida como una estrategia efectiva para limitar el movimiento lateral y minimizar la superficie de ataque.

Desde el punto de vista legal, el marco normativo colombiano, representado principalmente por las Leyes 1273 de 2009 y 1581 de 2012, junto con los principios constitucionales de protección a la intimidad y los estándares internacionales como ISO/IEC 27001, establece límites claros para el ejercicio profesional de la ciberseguridad. El cumplimiento de estas disposiciones no solo previene riesgos jurídicos, sino que también legitima las prácticas de seguridad y protege tanto a las organizaciones como a los profesionales involucrados.

En el ámbito ético, se concluye que las operaciones de Red Team y Blue Team deben regirse por principios como la integridad, la responsabilidad, la transparencia, la autorización y la no maleficencia. El respeto por estos principios garantiza que las pruebas de seguridad contribuyan efectivamente a la mejora continua de la organización, sin comprometer la privacidad, la confidencialidad de la información ni la continuidad del negocio.

Finalmente, se concluye que la ciberseguridad no es un estado estático, sino un proceso continuo de mejora que involucra tecnología, procesos y personas. La implementación de recomendaciones estratégicas en arquitectura, hardening, capacitación y cultura organizacional resulta esencial para enfrentar un panorama de amenazas en constante evolución. En este sentido, la colaboración entre Red Team, Blue Team y Purple Team se consolida como un enfoque indispensable para fortalecer la postura de seguridad y garantizar una defensa efectiva, legal y ética en los entornos digitales actuales.

Recomendaciones

Las recomendaciones derivadas del análisis realizado evidencian la necesidad de fortalecer de manera integral las capacidades ofensivas, defensivas y organizacionales en materia de ciberseguridad, superando enfoques aislados y adoptando una visión estratégica y continua. En primer lugar, se concluye que las actividades del Red Team deben evolucionar hacia un esquema de auditorías de intrusión cíclicas y progresivas, ya que una evaluación anual resulta insuficiente frente a un ecosistema tecnológico dinámico, caracterizado por cambios constantes en infraestructura, servicios y configuraciones. La combinación de inspecciones trimestrales, evaluaciones semestrales exhaustivas y auditorías no programadas permite construir un inventario dinámico de riesgos, identificar vulnerabilidades emergentes y evaluar de forma realista la capacidad de respuesta de los equipos defensivos.

Asimismo, se recomienda que las operaciones del Red Team se basen en la emulación de adversarios avanzados mediante el uso de inteligencia de amenazas actualizada. La replicación de tácticas empleadas por grupos APT, como el abuso de herramientas legítimas del sistema, técnicas de persistencia sigilosa y métodos de exfiltración encubierta, contribuye a elevar el nivel de madurez de la organización y a preparar al Blue Team frente a amenazas sofisticadas, alejándose de modelos de ataque obsoletos y excesivamente ruidosos. En este contexto, la incorporación controlada de técnicas de ingeniería social resulta fundamental, dado que el factor humano continúa siendo uno de los principales vectores de compromiso. La ejecución de campañas de phishing, vishing o smishing permite identificar patrones de comportamiento de riesgo y diseñar programas de capacitación basados en evidencias reales.

Por otro lado, se destaca la importancia de que los informes generados por el Red Team trasciendan el enfoque puramente técnico y se orienten al impacto operativo, financiero y legal

de los hallazgos. Vincular vulnerabilidades específicas con escenarios de afectación a la continuidad del negocio, pérdidas económicas o sanciones regulatorias facilita la toma de decisiones por parte de la alta dirección y fortalece el rol estratégico de la ciberseguridad dentro de la organización.

Desde la perspectiva defensiva, se concluye que la optimización de la visibilidad mediante la integración de tecnologías SIEM, EDR y NDR resulta crítica para reducir los tiempos de detección y respuesta ante incidentes. La correlación de eventos, el análisis de comportamiento en endpoints y la identificación de anomalías en el tráfico de red permiten transformar procesos reactivos prolongados en respuestas oportunas y efectivas. De igual forma, la adopción del modelo Zero Trust se consolida como una estrategia indispensable para eliminar la confianza implícita dentro de la red, restringir el movimiento lateral y reforzar los controles de acceso mediante validación continua y autenticación multifactor.

El endurecimiento estructural de la infraestructura tecnológica también se identifica como una prioridad, dado que una proporción significativa de los incidentes de seguridad se origina en configuraciones básicas deficientes. La eliminación de protocolos inseguros, la aplicación oportuna de parches críticos y la restricción de la ejecución de software no autorizado elevan sustancialmente la complejidad de los ataques y reducen la superficie de exposición. Complementariamente, la realización periódica de ejercicios de respuesta a incidentes permite fortalecer la coordinación del Blue Team, validar los procedimientos establecidos y mejorar los tiempos de contención y recuperación ante escenarios reales.

A nivel organizacional, se recomienda establecer una gobernanza sólida de la ciberseguridad mediante la conformación de un comité directivo que alinee la estrategia técnica con los objetivos del negocio. Esta gobernanza debe apoyarse en programas continuos de formación y concientización, entendiendo que la capacitación puntual resulta insuficiente frente

a un entorno de amenazas en constante evolución. La adopción de estándares internacionales como ISO/IEC 27001, NIST y CIS Controls contribuye a formalizar los controles de seguridad, reducir la improvisación y fortalecer la credibilidad institucional frente a auditorías y requerimientos regulatorios. La adopción de normas y estándares internacionales proporciona un marco estructurado para la auditoría y gestión de la seguridad informática (Jenny, 2014; Macías, 2023).

Desde una perspectiva técnica avanzada, se resalta la necesidad de implementar microsegmentación de redes, control de accesos basado en roles y esquemas de respaldo inmutable que mitiguen de forma efectiva el impacto de ataques como el ransomware. La integración de inteligencia de amenazas en los procesos defensivos transforma la seguridad en un enfoque preventivo, permitiendo anticiparse a campañas maliciosas mediante el bloqueo proactivo de indicadores de compromiso.

Finalmente, se concluye que todas estas recomendaciones deben ejecutarse dentro de un marco jurídico y ético claramente definido. La formalización de reglas de compromiso, el cumplimiento estricto de la Ley 1273 de 2009 y la Ley 1581 de 2012, así como la protección adecuada de los datos personales, garantizan la legitimidad de las actividades de ciberseguridad. De manera prospectiva, la consolidación de una unidad permanente de Purple Team, la automatización de respuestas mediante SOAR, el aseguramiento de entornos en la nube y la ejecución periódica de auditorías externas permitirán sostener una mejora continua y una postura de seguridad resiliente frente a amenazas cada vez más complejas.

Referencias Bibliográficas

Ahmed, Y., Asyhari, A., Rahman, M. A. (2021). A cyber kill chain approach for detecting advanced persistent threats. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *67*(2), 2497–2513. https://doi.org/10.32604/cmc.2021.014223

Gomez , A. (2022, March 7). *Estudio de los ataques y su defensa en la Ingeniería Social*. https://e-spacio.uned.es/entities/publication/bef19b67-069b-41c3-a7b1-288ee1e52f81

Alhamed, M., Rahman, M. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*, *13*(12), 6986. https://doi.org/10.3390/app13126986

Barón, A. (2024, December 6). *Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team*. https://repository.unad.edu.co/handle/10596/67269

Beyond zero trust: Trust is a vulnerability. (n.d.). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9206246

Buitrago, D. (2018, June 1). *Estudio de metodologías de ingeniería social*. https://openaccess.uoc.edu/items/546286bd-5c70-4efc-8393-1b4948810e98#page=1

Trigos, E. (2025, May 26). *Capacidades técnicas, legales y de gestión para equipos blue team y red team*. https://repository.unad.edu.co/handle/10596/70298

Zambrano , F. (2024, April 10). *Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team*. https://repository.unad.edu.co/handle/10596/60740

Ghasemshirazi, S., Shirvani, G., (2023, September 7). *Zero Trust: applications, challenges, and opportunities*. arXiv.org. https://arxiv.org/abs/2309.03582

Grigorescu, O., Nica, A., Dascalu, M., Rughinis, R. (2022). CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques. *Algorithms*, *15*(9), 314. https://doi.org/10.3390/a15090314

He, Y., Huang, D., Chen, L., Ni, Y., Ma, X. (2022). A survey on Zero Trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*(1). https://doi.org/10.1155/2022/6476274

Ingeniería, E. (2015, December 1). *Ingeniería social : el ataque silencioso*. http://www.redicces.org.sv/jspui/handle/10972/2910

Jenny, L. (2014). *Normas y estándares informáticos*. https://alicia.concytec.gob.pe/vufind/Record/UNAP_755b2fad2f04bd62309736755ab859bb

Kazimierczak, M., Habib, N. Chan, J. H. & Thanapattheerakul, T. (2024). Impact of AI on the Cyber Kill Chain: A Systematic review. *Heliyon*, *10*(24), e40699. https://doi.org/10.1016/j.heliyon.2024.e40699

Medina, L. (2022, September 1). *Revisión sistemática de la literatura relacionada con ciberseguridad apoyada con analisis de Big Data para actividades de red Team*. https://dspace.ups.edu.ec/handle/123456789/23322

Rocha, A. (2019). Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. *RISTI - Revista Ibérica De Sistemas E Tecnologias De Informação*, *32*, VII–IX. https://doi.org/10.17013/risti.32.0

Macias, M. Navarrete, M, Navarrete, J. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *5*(4), 584–599. https://doi.org/10.59169/pentaciencias.v5i4.700

Penetration testing. (n.d.). Google Books. https://books.google.com.co/books?hl=es&lr=&id=T_LlAwAAQBAJ&oi=fnd&pg=PR19&dq=pentesting&ots=NXEW5RCsKU&sig=kf66cUvU7IigbfH_7zWJs2QZVI&redir_esc=y#v=onepage&q=pentesting&f=false

Rojas J. , Medina, Y, y Rico, D. . (2016). Pentesting empleando técnicas de Ethical Hacking en redes IPv6. *Revista Ingenio*, *11*(1), 67–84. https://doi.org/10.22463/2011642X.2096

Velásquez, L., Monterrubio, M., Crespo, S., & Rosado, G. (2023). Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*, *22*(3), 691–711. https://doi.org/10.1007/s10207-022-00657-9

Villacís, C. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situacion actual en el Ecuador. *Revista Tecnológica Ciencia Y Educación Edwards Deming*. https://doi.org/10.37957/rfd.v6i1.88

Why SIEM is Irreplaceable in a Secure IT Environment? (n.d.). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8732173

Yadav, T., Rao, A., Yadav, T., & Rao, M. (2015). Technical aspects of cyber kill chain. In *Communications in computer and information science* (pp. 438–452). https://doi.org/10.1007/978-3-319-22915-7_40

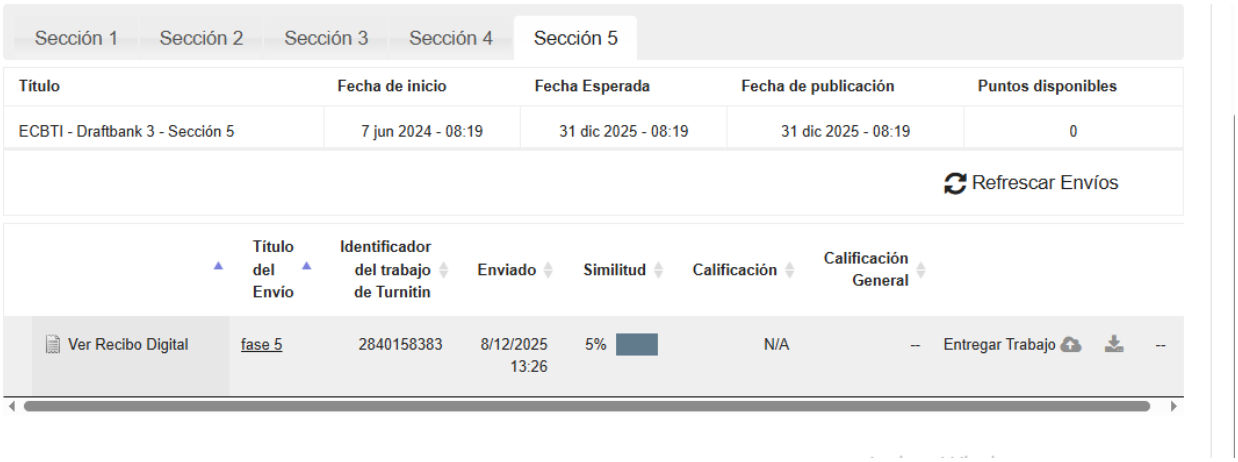
Apéndices

Apéndice A

Resultado de Revisión en Turnitin

Figura 7

Resultado TURNITIN



Fuente: Autoría Propia

Figura 8

Revisión porcentaje TURNITIN

Nota. Autoría Propia