Capacidades técnicas, legales y de gestión para equipos blue Team y red Team

Estudiante:

Oruel Exneyder Jaramillo Vargas

Director del Curso:

MSc. Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

Mayo 2025

Resumen

El presente informe técnico expone los resultados de una investigación aplicada sobre las capacidades técnicas, legales y de gestión requeridas por los equipos Red Team y Blue Team en un entorno simulado de ciberseguridad. A través del análisis de un caso práctico desarrollado por etapas, se evaluaron procesos ofensivos y defensivos orientados a la identificación, explotación, contención y mitigación de la vulnerabilidad crítica (MS17-010) “Eternal Blue” en el sistema operativo de Windows. El trabajo incluyó la aplicación de pruebas de penetración (pentesting), el uso de herramientas como Nmap y Metasploit, y la implementación de estrategias de defensa basadas en normas internacionales como los CIS Benchmarks y principios de respuesta a incidentes. Asimismo, se examinó el marco normativo colombiano aplicable a la seguridad informática, identificando transgresiones legales y éticas simuladas en el ejercicio. El informe articula teoría y práctica mediante un enfoque metodológico riguroso, proporcionando recomendaciones para el fortalecimiento de las capacidades institucionales en ciberseguridad.

Palabras clave: Seguridad Red Team Blue Team Vulnerabilidad

Abstract

This white paper presents the results of applied research on the technical, legal and managerial capabilities required by Red Team and Blue Team in a simulated cybersecurity environment. Through the analysis of a practical case developed in stages, offensive and defensive processes aimed at the identification, exploitation, containment and mitigation of the critical vulnerability (MS17-010) "Eternal Blue" in the Windows operating system were evaluated. The work included the application of penetration testing (pentesting), the use of tools such as Nmap and Metasploit, and the implementation of defense strategies based on international standards such as CIS Benchmarks and incident response principles. Likewise, the Colombian regulatory framework applicable to computer security was examined, identifying simulated legal and ethical transgressions in the exercise. The report articulates theory and practice through a rigorous methodological approach, providing recommendations for strengthening institutional capacities in cybersecurity.

Keywords: Security Red Team Blue Team Vulnerability

Índice

Glosario

Red Team	Equipo ofensivo que simula ataques reales para evaluar la seguridad de una organización.
Blue Team:	Equipo defensivo que protege los sistemas y responde ante incidentes de seguridad.
MS17-010	Vulnerabilidad crítica en SMBv1 explotada por el exploit EternalBlue
Hardenización:	Proceso de asegurar un sistema mediante la eliminación de vulnerabilidades y la configuración segura.
SIEM:	Sistema de Gestión de Información y Eventos de Seguridad.
Pentesting:	Prueba de penetración que simula un ataque controlado para evaluar las debilidades de los sistemas informáticos.
CVE:	(Common Vulnerabilities and Exposures): Catálogo público de vulnerabilidades de seguridad conocidas.
SMB:	(Server Message Block): Protocolo de red usado por Windows para compartir archivos e impresoras.
Nmap:	Herramienta de escaneo de redes para detectar hosts, puertos abiertos y servicios activos.
Metasploit:	Framework para pruebas de penetración que permite desarrollar y ejecutar exploits.
OpenVAS:	Escáner de vulnerabilidades de código abierto.
Wireshark:	Analizador de tráfico de red que permite visualizar paquetes en tiempo real.

CIS Benchmarks:	Conjuntos de buenas prácticas para la configuración segura de sistemas, desarrollados por el Center for Internet Security.
COPNIA:	Consejo Profesional Nacional de Ingeniería en Colombia, que regula el ejercicio ético de los ingenieros
Escalada de privilegios:	Técnica mediante la cual un atacante obtiene mayores permisos dentro de un sistema después de un acceso inicial, pasando de usuario básico a administrador.
Exploit:	Código o software que aprovecha una vulnerabilidad específica para realizar un ataque.
Firewall:	Dispositivo o software que regula el tráfico de red entrante y saliente según reglas de seguridad preestablecidas.
Análisis Forense:	Técnica que permite recolectar, preservar y analizar evidencia electrónica tras un incidente de seguridad.

Introducción

En el contexto actual de transformación digital, la ciberseguridad se ha convertido en un componente estratégico esencial para las organizaciones públicas y privadas. La creciente sofisticación de los ataques informáticos exige no solo conocimientos técnicos, sino también la articulación de competencias legales, éticas y de gestión, que permitan anticipar, detectar y responder eficazmente ante incidentes de seguridad. En este sentido, el presente informe técnico tiene como propósito consolidar los aprendizajes obtenidos durante el desarrollo del seminario especializado en equipos estratégicos Red Team y Blue Team, mediante la ejecución de un caso práctico simulado que reproduce condiciones reales de vulnerabilidad en una infraestructura TI.

El trabajo está estructurado por etapas, abarcando desde el reconocimiento legal y técnico de los marcos normativos colombianos, hasta la ejecución de pruebas de Red Team y Blue Team en un sistema operativo Windows vulnerable a la falla MS17-010 “Eternal Blue”. Se simula una situación crítica en la que el Red Team compromete el sistema mediante el exploit EternalBlue, mientras que el Blue Team despliega acciones de contención, análisis forense y hardenización, aplicando principios como el mínimo privilegio, monitoreo continuo (SIEM) y gestión proactiva de amenazas.

Objetivos

Objetivo General

Analizar integralmente las capacidades técnicas, legales y operativas requeridas por los equipos Red Team y Blue Team en escenarios simulados de ciberseguridad, con el fin de evaluar la eficacia de las estrategias ofensivas y defensivas aplicadas, enmarcadas en estándares internacionales y normativas legales vigentes.

Objetivos Específicos

1. Identificar el marco normativo y ético que regula la actuación profesional relacionada con la seguridad de la información en Colombia, especialmente en relación con los roles Red Team y Blue Team.
2. Ejecutar procedimientos ofensivos mediante pruebas de penetración (pentesting) sobre la vulnerabilidad crítica (MS17-010) “Eternal Blue”, evaluando su impacto en un entorno de sistema operativo Windows simulado.
3. Implementar acciones defensivas desde el enfoque Blue Team, orientadas a la contención del incidente, el análisis forense básico y la hardenización del sistema comprometido.
4. Proponer mejoras y recomendaciones alineadas con estándares internacionales (como NIST y CIS) que fortalezcan la seguridad informática en entornos organizacionales.

1. Desarrollo del Informe

En el contexto planteado por CyberFort Technologies, se simuló una situación crítica de ciberseguridad en la que una infraestructura tecnológica presentaba vulnerabilidades activas, específicamente en una máquina Windows susceptible al exploit MS17-010. Esta condición generó un entorno ideal para evaluar tanto las capacidades ofensivas como defensivas de los equipos Red Team y Blue Team, enmarcadas en un proceso riguroso de análisis técnico, ético y legal. De acuerdo con (Wash & Rader, 2021) “el enfoque dual Red Team y Blue Team permite evaluar las capacidades de defensa y ataque de una organización, integrando análisis técnico con procedimientos de respuesta a incidentes”

La necesidad inmediata de la organización radicaba en identificar brechas de seguridad, demostrar la viabilidad de explotación por parte de un actor malicioso, y posteriormente diseñar e implementar estrategias efectivas de contención y mitigación de riesgos. Así, el presente informe recoge las acciones ejecutadas desde ambas perspectivas, evidenciando la importancia de un enfoque integral y colaborativo en la protección de los activos digitales.

1.1.Reconocimiento Legal y Técnico en Seguridad Informática

Durante la primera etapa, se desarrolló una comprensión fundamental de los pilares legales y técnicos que sustentan la práctica profesional en ciberseguridad. "En Colombia, la protección de datos personales y la ciberseguridad están reguladas por leyes como la Ley 1581 de 2012 y la Ley 1266 de 2008, que establecen los principios para el tratamiento de información y las obligaciones de los responsables del manejo de datos" (Villegas Carrasquilla, 2021)

En el marco colombiano, se identificaron y analizaron leyes clave como: la Ley 1273 de 2009, la Ley 1581 de 2012, la Ley 1266 de 2008 y el Decreto 886 de 2014, que definen los delitos informáticos, los derechos de los titulares de datos personales, las obligaciones de las centrales de riesgo y los lineamientos para el registro nacional de bases de datos, respecto a las medidas de ciberdefensa, de acuerdo con (Parraguez Kobek & Caldera, 2016) "Colombia ha adoptado una estrategia integral de ciberdefensa, estableciendo entidades como el colCERT y el Comando Conjunto Cibernético (CCOC) para enfrentar amenazas cibernéticas y proteger la infraestructura crítica del país".

Referente al apartado técnico, se abordaron los conceptos fundamentales de las pruebas de penetración (pentesting), definiendo cada una de sus fases: reconocimiento, escaneo, enumeración de vulnerabilidades, explotación, escalada de privilegios y reporte, etapas las cuales permiten evaluar de forma estructurada y metódica la seguridad de un sistema informático, replicando el comportamiento de un atacante con el fin de identificar y mitigar posibles fallas antes de que sean explotadas de forma maliciosa. Se estudiaron herramientas clave para cada fase del pentesting, incluyendo:

- **Maltego** para el reconocimiento pasivo.
- **Nmap** para escaneo de puertos y servicios.
- **OpenVAS** para detección de vulnerabilidades.
- **Metasploit** para explotación de fallos.
- **LinPEAS** para escalada de privilegios.
- **Dradis** para documentación de hallazgos.

El desarrollo de esta etapa permitió sentar las bases técnicas y legales que fundamentaron el trabajo práctico posterior. A través de la creación de un entorno virtual de pruebas, se integró

la teoría con la práctica, fortaleciendo la preparación profesional en el ámbito de la seguridad informática con una visión ética y legalmente alineada.

1.2. Reconocimiento de Normas y Leyes vulneradas

Durante la segunda etapa se profundizó en el análisis ético y legal de un escenario problemático presentado por CyberFort Technologies. A partir del estudio del acuerdo de confidencialidad propuesto por la organización, se identificaron cláusulas que contravenían directamente la legislación colombiana sobre delitos informáticos y protección de datos, así como los principios éticos que rigen la práctica profesional de la ingeniería.

El documento contenía disposiciones que prohibían denunciar actividades ilícitas, calificaban actos delictivos como información confidencial y trasladaban la responsabilidad legal al firmante, exonerando a la empresa de cualquier consecuencia. Estos elementos vulneraban varios artículos de la Ley 1273 de 2009 así:

Artículo 269A. “El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena” (Congreso de Colombia, 2009)

El acuerdo contempla como información confidencial actividades como el acceso abusivo a sistemas informáticos, lo que constituye delito según este artículo. Al prohibir denunciarlo, el acuerdo encubre dicha conducta.

Artículo 269C. “El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas

provenientes de un sistema informático que los transporte incurrirá en pena" (Congreso de Colombia, 2009)

El acuerdo menciona expresamente como parte de la información confidencial los "datos de chuzadas", es decir, interceptaciones ilegales de información. Esta cláusula normaliza una práctica penalizada por este artículo, y a su vez no permite denunciarla

Además, se identificaron transgresiones a los deberes contemplados en el Código de Ética Profesional del COPNIA. Entre ellos, el deber de denunciar actos contrarios a la ley (art. 31, literal f), el respeto a las disposiciones legales (art. 35, literal b), y la obligación de mantener la confidencialidad sin encubrir delitos (art. 39, literal a) (COPNIA, 2015).

La aceptación del acuerdo propuesto podría interpretarse como complicidad u omisión ética grave, con posibles sanciones disciplinarias, incluida la pérdida de la matrícula profesional.

Esta etapa permitió reforzar el criterio profesional frente a situaciones que, aunque estén formalizadas contractualmente, contravienen principios fundamentales del ejercicio ético y legal de la ciberseguridad.

1.3. Ejecución Enfoque Red Team

Durante la Etapa 3 se ejecutaron pruebas de intrusión ofensiva en el marco de un entorno controlado. El objetivo fue explotar una vulnerabilidad crítica en una máquina Windows 7 SP1 que simulaba una infraestructura vulnerable en una organización.

La actividad comenzó con la fase de recolección de información. A través de los comandos ipconfig en la máquina Windows e ip a en Kali Linux, mediante los cuales se identificaron las direcciones IP internas de ambos equipos, confirmando que pertenecían a la

misma red (192.168.1.9 y 192.168.1.8). Se verificó la conectividad entre ellos mediante el uso de ping, validando la viabilidad de realizar el ataque.

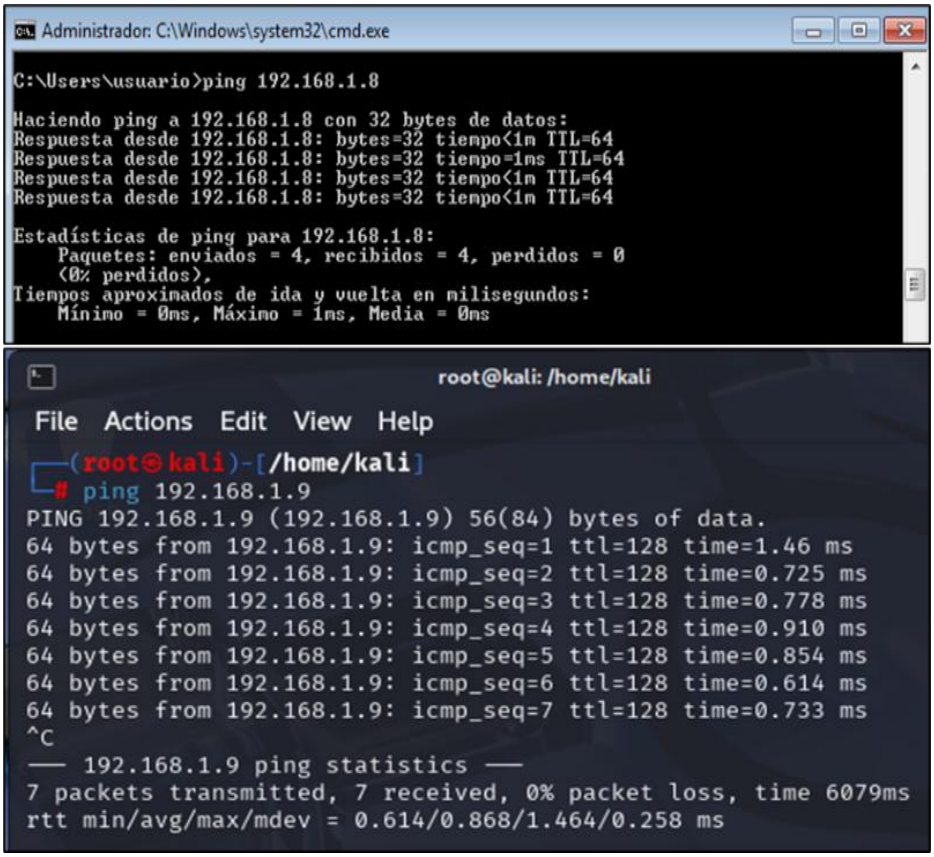

Figura 1 Verificación de conectividad mediante ping

En la fase de escaneo y análisis de vulnerabilidades, se utilizó la herramienta Nmap con los parámetros -sS -sV -O -p- detectando el puerto 445/TCP abierto y el sistema operativo Windows 7, potencialmente vulnerable al exploit EternalBlue (MS17-010). De acuerdo con (Le, Dang, Do, Hoang, & Nguyen, 2024) "El exploit EternalBlue, identificado como CVE-2017-0144, permite a actores maliciosos ejecutar código remoto en sistemas Windows vulnerables, facilitando ataques como WannaCry y NotPetya".

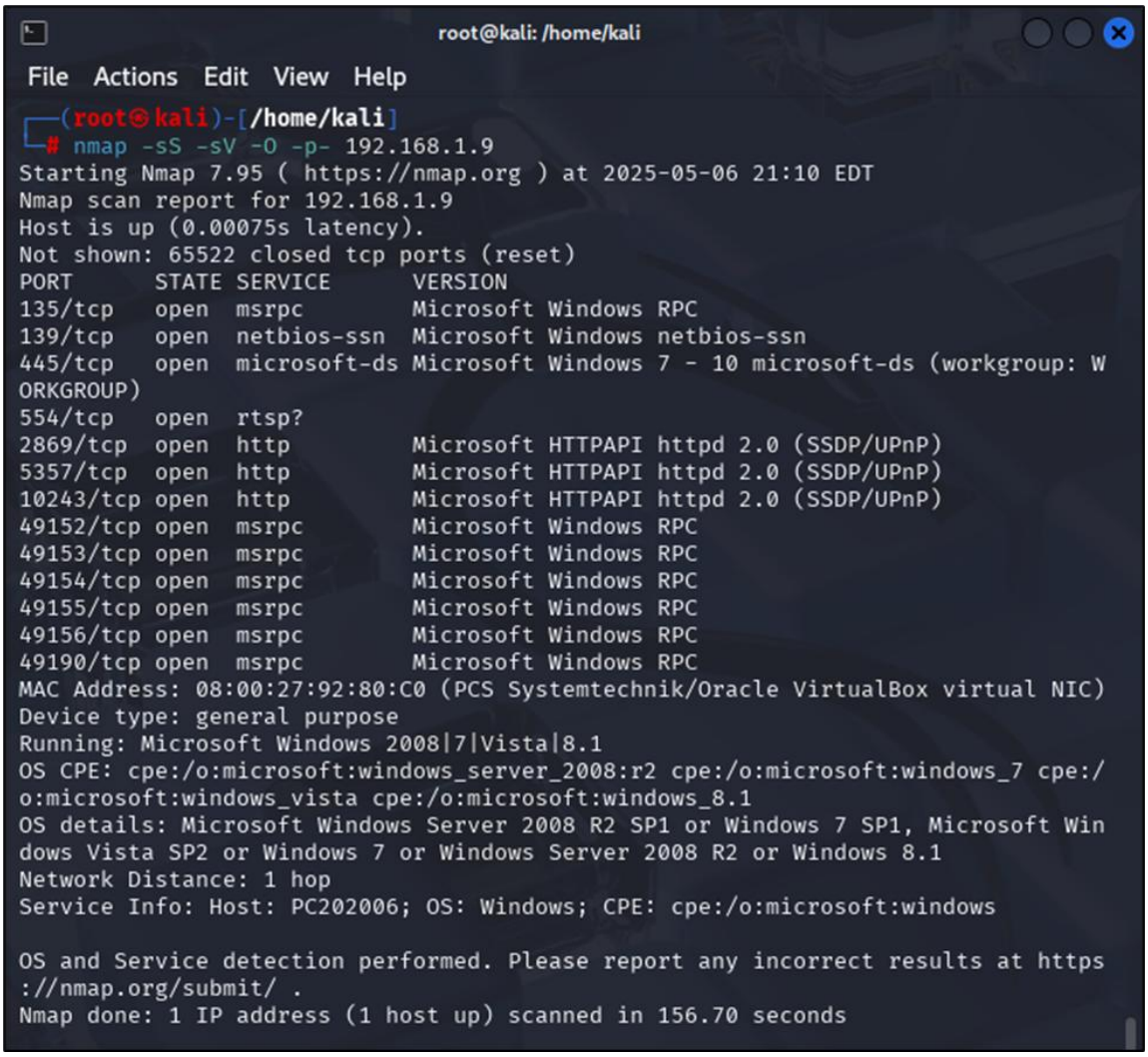

Figura 2 Identificación de vulnerabilidades

Una vez identificada la presencia del puerto 445/TCP abierto y la ejecución de un sistema operativo Windows 7 / Server 2008 R2 —ambos susceptibles al exploit MS17-010 (EternalBlue)— se procedió a utilizar el framework Metasploit para explotar la vulnerabilidad de manera remota. “El uso de Metasploit para explotar MS17-010 en entornos de prueba permite validar la criticidad de esta vulnerabilidad bajo condiciones controladas” (Novokhrestov, Kalyakin, Kovalenko, & Repkin, 2024)

Se definieron las variables RHOSTS (IP de la víctima) y LHOST (IP del atacante) y se ejecutó el ataque, logrando establecer una sesión remota con privilegios del sistema.

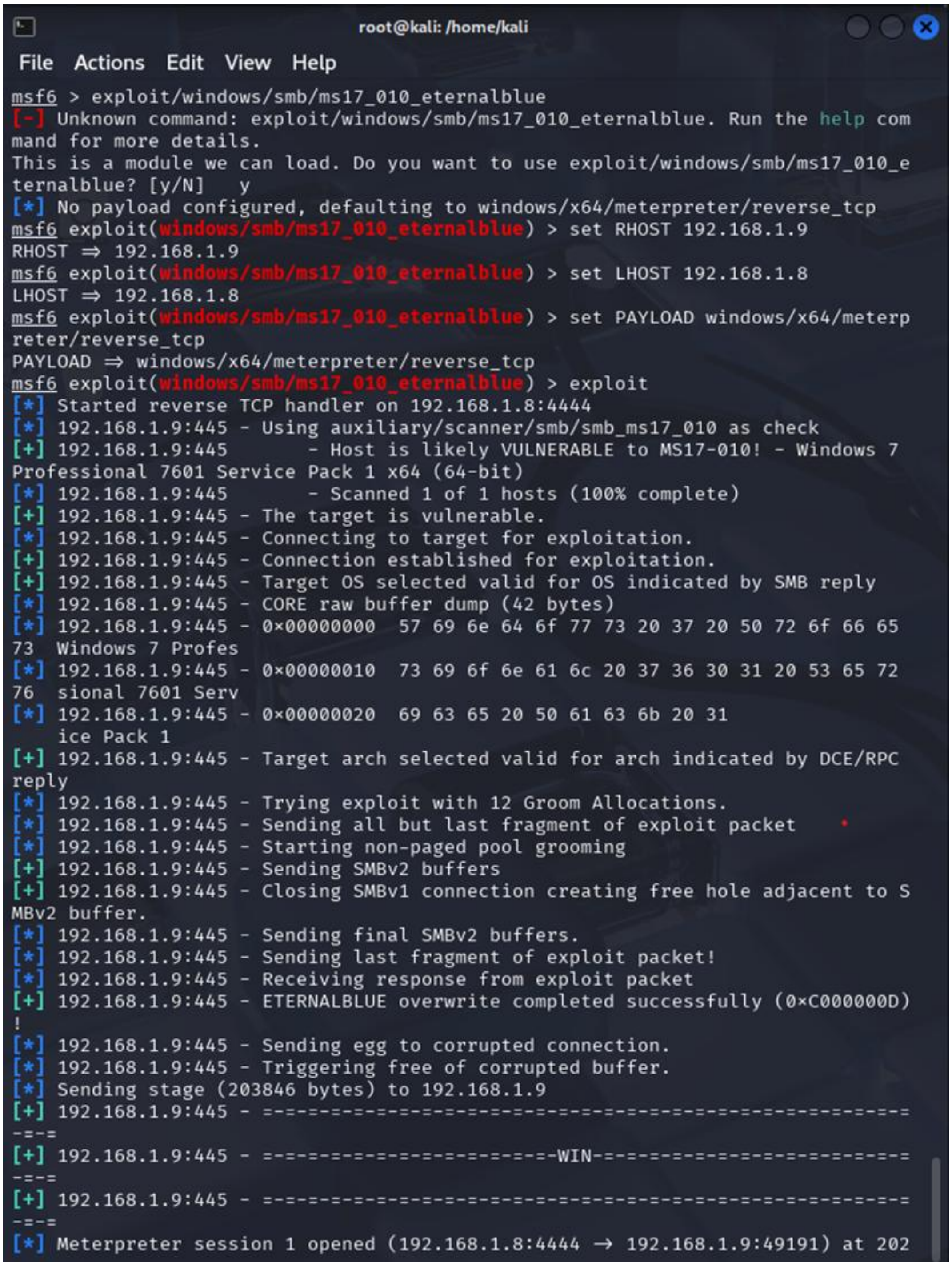

Figura 3 Ejecución del exploit

Como prueba de concepto solicitada por el escenario, se accedió al shell de Windows mediante Meterpreter y se creó un nuevo usuario administrador.

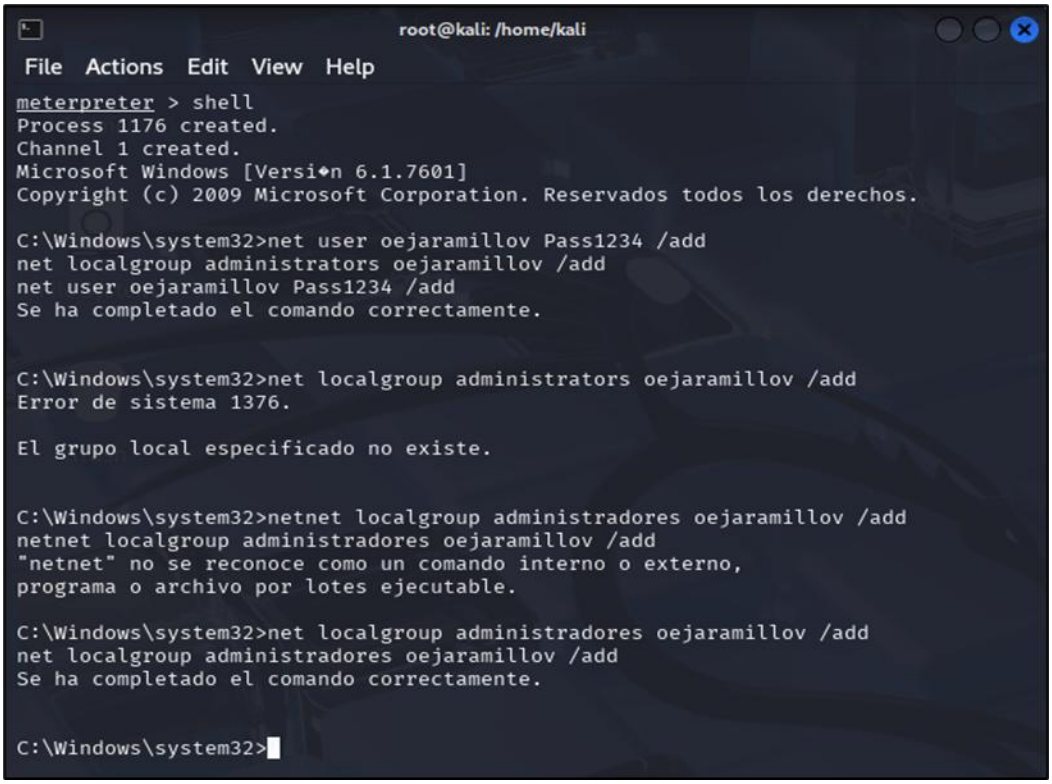

Figura 4 Creación de usuario - Escalamiento Privilegios

Estas acciones demostraron la viabilidad técnica de una escalación de privilegios, cumpliendo con el requerimiento de generar evidencia clara del acceso conseguido.

La actividad fue documentada paso a paso con evidencias gráficas, mostrando tanto los comandos empleados como los resultados obtenidos.

El resultado final evidenció la importancia de contar con equipos Red Team capacitados para identificar y explotar fallas antes de que lo hagan actores maliciosos, reforzando el valor de las pruebas ofensivas como herramienta preventiva en la seguridad de la información.

1.4. Ejecución Enfoque Blue Team

En esta etapa se abordó la respuesta defensiva ante un incidente de seguridad activo, asumiendo el rol del equipo Blue Team dentro de la organización CyberFort Technologies. El escenario planteaba una intrusión en curso en una máquina Windows 7 previamente comprometida por el exploit MS17-010. El objetivo fue implementar acciones inmediatas de contención, análisis forense básico y medidas de hardenización que permitieran mitigar el ataque y prevenir futuras intrusiones,

La primera medida adoptada fue el aislamiento de la máquina comprometida, deshabilitando su interfaz de red para cortar la comunicación con el atacante. Esta acción es fundamental en incidentes en tiempo real, ya que evita el movimiento lateral dentro de la red y la exfiltración de datos.

En paralelo, se utilizó Wireshark para capturar el tráfico de red con el fin de identificar paquetes sospechosos, posibles conexiones remotas activas o comunicaciones con servidores externos. Asimismo, se empleó TCPView para visualizar procesos y conexiones activas dentro del sistema, y el Visor de Eventos de Windows para detectar indicios de escalación de privilegios, creación de nuevos usuarios o ejecución de comandos anómalos. Tras identificar la naturaleza del ataque, se procedió con acciones de hardenización del sistema:

- Instalación del parche de seguridad MS17-010 publicado por Microsoft para cerrar la vulnerabilidad explotada.
- Desactivación del protocolo SMBv1, considerado obsoleto y vulnerable.
- Bloqueo del puerto 445/TCP desde el firewall interno para restringir su uso a comunicaciones justificadas y controladas.

- Eliminación de cuentas sospechosas creadas durante la intrusión, como parte del proceso de restauración de integridad del sistema.
- Revisión y fortalecimiento de la configuración de usuarios y privilegios, aplicando el principio de mínimo privilegio.
- Implementación de políticas de mínimo privilegio. “La escalada de privilegios puede prevenirse aplicando políticas de mínimo privilegio y monitoreo de cuentas privilegiadas” (MITRE ATT&CK, 2025)

Además, se propuso la adopción de los CIS Benchmarks para validar configuraciones seguras del sistema, y la implementación de una solución SIEM gratuita como Wazuh, “Los sistemas SIEM como Wazuh permiten correlacionar eventos y generar alertas ante actividades sospechosas, siendo esenciales para la respuesta temprana*”* (Gonzalez Granadillo, Gonzalez Zarzosa, & Diaz, 2021)

Los resultados de esta etapa reflejan la importancia de combinar acciones técnicas inmediatas con estrategias de mejora continua en la infraestructura. La capacidad del Blue Team para responder de forma estructurada y eficaz frente a amenazas activas es determinante para preservar la seguridad de la información en las organizaciones.

1.5. Sustentación

https://youtu.be/iG34-bj5wXk

Conclusiones

El desarrollo del seminario permitió experimentar de manera integral las capacidades que requiere un profesional en ciberseguridad, combinando habilidades técnicas, legales y éticas. Las fases prácticas demostraron que las vulnerabilidades en sistemas desactualizados como MS17-010 siguen siendo una amenaza real si no se aplican medidas correctivas y preventivas. La ejecución del enfoque Red Team evidenció cómo un atacante puede comprometer fácilmente un entorno no protegido, mientras que la respuesta del Blue Team demostró que una estrategia bien estructurada puede contener eficazmente incidentes y mitigar daños.

Además, el análisis del marco normativo colombiano y del acuerdo simulado de confidencialidad de CyberFort Technologies permitió evidenciar que no basta con tener competencia técnica: el profesional en ciberseguridad debe actuar bajo principios éticos sólidos y conocimiento legal claro, evitando prácticas que puedan derivar en complicidad con actos delictivos. En suma, se consolidó una visión holística de la ciberseguridad, entendida como una práctica interdisciplinar que requiere preparación continua, responsabilidad profesional y compromiso con la protección de la información.

Recomendaciones

Fortalecer la cultura de seguridad: Impulsar la capacitación continua de los equipos técnicos en ciberseguridad ofensiva y defensiva, con énfasis en estándares internacionales como NIST y CIS.

Aplicar parches críticos sin dilación: Priorizar la actualización inmediata de sistemas, especialmente en entornos que manejan datos sensibles o tienen conectividad externa constante.

Eliminar protocolos obsoletos: Desactivar servicios como SMBv1 y restringir el acceso a puertos inseguros (ej. 445/TCP), aplicando controles por segmentación y listas blancas.

Auditar acuerdos legales y cláusulas de confidencialidad: Garantizar que los contratos de prestación de servicios de ciberseguridad no vulneren derechos legales ni éticos.

Implementar soluciones SIEM efectivas: Utilizar herramientas como Wazuh para una vigilancia continua, automatización de alertas y respaldo a investigaciones forenses.

Desarrollar ejercicios de Red vs Blue: Realizar simulaciones periódicas entre equipos ofensivos y defensivos para identificar mejoras en los procedimientos de detección, contención y recuperación. “La capacitación continua en simulacros Red Team vs Blue Team mejora la preparación ante ataques reales y optimiza la colaboración entre roles”

Documentar cada intervención técnica: Consolidar informes estructurados que detallen hallazgos, acciones ejecutadas y recomendaciones específicas para futuras intervenciones.

Bibliografía

Congreso de Colombia. (31 de Diciembre de 2008). *Ley 1266 de 2008*. Obtenido de Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de Colombia. (5 de Enero de 2009). *Ley 1273 de 2009*. Obtenido de Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (05 de Enero de 2009). *Ley 1273 de 2009*. Obtenido de Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (17 de Octubre de 2012). *Ley 1581 de 2012*. Obtenido de Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

COPNIA. (2015). *Consejo Profesional Nacional de Ingenieria.* Obtenido de Codigo de Etica: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Gonzalez Granadillo, G., Gonzalez Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*.

Le, P.-H., Dang, L., Do, Q., Hoang, C., & Nguyen, L. (28 de Mayo de 2024). *Springer Nature Link.* Obtenido de EternalBlue Exploit: Definitions and Working Mechanism: https://doi.org/10.1007/978-981-96-1452-3_1

MITRE ATT&CK. (25 de Abril de 2025). *Privilege Escalation*. Obtenido de MITRE ATT&CK: https://attack.mitre.org/tactics/TA0004/

Mora, E. (2020). *Ciberseguridad y sistemas SIEM: Fundamentos y aplicación práctica.* Editorial RA-MA.

Novokhrestov, A., Kalyakin, A., Kovalenko, A., & Repkin, V. (26 de Junio de 2024). *arxiv*. Obtenido de Creating a vulnerable node based on the vulnerability MS17-010: https://arxiv.org/abs/2401.14979

Parraguez Kobek, L., & Caldera, E. (01 de Junio de 2016). *Redalyc.* Obtenido de Ciberseguridad y Habeas Data: la respuesta latinoamericana a la seguridad informática y la protección de datos: https://www.redalyc.org/journal/531/53163716007/html/?utm_source=chatgpt.com

Presidencia de la Republica. (13 de Mayo de 2014). *Decreto 886 de 2014*. Obtenido de Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Villegas Carrasquilla, L. (18 de Febrero de 2021). *Data protection and cybersecurity laws in Colombia*. Obtenido de CMS law tax future: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/colombia

Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity*, 45-60.