Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Brayan Andrés Gómez Lizarazo

Asesor

Luis Fernando Zambrano Hernandez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Sociales Artes y Humanidades ECSAH

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team -

(202337164A_2042)

2025

Resumen

Este informe ofrece una visión integral del desarrollo de las fases 1 a 5, abordando las capacidades técnicas, legales y de gestión requeridas para la operación eficiente de los equipos Red Team y Blue Team en entornos organizacionales. A partir del análisis de escenarios prácticos realizados durante el seminario especializado, se examinan tácticas ofensivas y defensivas, así como medidas de respuesta ante amenazas reales en infraestructuras tecnológicas. Asimismo, se contemplan los marcos normativos y éticos que sustentan la actuación profesional de los equipos de ciberseguridad. El documento concluye con recomendaciones estratégicas orientadas a fortalecer las políticas de seguridad, la capacidad de respuesta y la coordinación entre los equipos operativos.

***Palabras clave*:** Ciberseguridad, Red Team, Blue Team, Gestión de incidentes, Estrategias ofensivas y defensivas.

Abstract

This report provides a comprehensive overview of the development from phases 1 to 5, addressing the technical, legal, and management capabilities required for the effective operation of Red Team and Blue Team units in organizational environments. Based on the analysis of practical scenarios carried out during the specialized seminar, offensive and defensive tactics are examined, along with response measures to real threats in IT infrastructures. The report also considers legal and ethical frameworks that support the professional conduct of cybersecurity teams. It concludes with strategic recommendations aimed at strengthening security policies, response capabilities, and effective coordination between operational teams.

Keywords**:** Cybersecurity, Red Team, Blue Team, Incident Management, Offensive and defensive strategies.

Glosario

Red Team: Grupo de especialistas que simula ataques reales para evaluar la seguridad de una organización.

Blue Team: Grupo encargado de defender la infraestructura de TI frente a amenazas y ataques.

Pentesting: Prueba de penetración que evalúa vulnerabilidades mediante ataques simulados.

MITRE ATT&CK: Base de conocimientos sobre tácticas y técnicas usadas por adversarios en ciberataques.

SIEM: Sistema de gestión de eventos e información de seguridad (Security Information and Event Management).

Hardening: Proceso de reforzamiento de sistemas para reducir vulnerabilidades.

RAT (Remote Access Trojan): Malware que permite el control remoto de sistemas sin autorización.

Forense digital: Disciplina que analiza evidencias digitales para investigar incidentes de seguridad.

CVE (Common Vulnerabilities and Exposures): Base de datos pública de vulnerabilidades conocidas.

TTPs: Tácticas, Técnicas y Procedimientos usados por atacantes.

Regulación 1581 de 2012: Ley colombiana sobre protección de datos personales.

SOC (Security Operations Center): Centro de operaciones encargado de monitorear y responder a incidentes.

Table de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En el contexto actual de amenazas cibernéticas cada vez más sofisticadas, las organizaciones requieren fortalecer sus capacidades de defensa y respuesta ante incidentes. Los equipos Red Team y Blue Team desempeñan un papel fundamental en esta tarea, permitiendo simular ataques reales y diseñar estrategias de protección que robustezcan la infraestructura tecnológica. La articulación entre ambos equipos es importante para anticipar vulnerabilidades, probar la resiliencia organizacional y establecer mecanismos de mejora continua.

El presente informe técnico tiene como propósito analizar las capacidades técnicas, legales y de gestión desarrolladas durante el seminario especializado, mediante la simulación de escenarios aplicados en el entorno de evaluación de CyberFort Technologies. En dichos escenarios, se identificaron vulnerabilidades, se desplegaron tácticas ofensivas y defensivas, y se abordaron aspectos normativos que regulan la actuación profesional en ciberseguridad, tanto en el ámbito nacional como internacional.

Este documento resume los principales aprendizajes obtenidos, presenta un análisis de las estrategias aplicadas por los equipos Red Team y Blue Team, y formula recomendaciones para fortalecer la postura de seguridad de las organizaciones.

Justificación

La creciente sofisticación de las amenazas cibernéticas obliga a las organizaciones a adoptar enfoques estructurados y especializados para la protección de sus activos digitales. En este contexto, la integración de equipos Red Team y Blue Team se ha consolidado como una práctica fundamental para evaluar y fortalecer la seguridad informática, al permitir la identificación de vulnerabilidades desde una perspectiva ofensiva y la implementación de mecanismos defensivos efectivos.

El presente informe se justifica en la necesidad de analizar, desde un enfoque técnico, legal y de gestión, las estrategias utilizadas por ambos equipos durante escenarios prácticos simulados. Esta revisión permite establecer lineamientos que contribuyan a la mejora continua de las capacidades de respuesta y contención frente a incidentes de seguridad, aspectos que resultan esenciales para garantizar la integridad, disponibilidad y confidencialidad de la información.

Objetivos

Objetivo General

Analizar las capacidades técnicas, legales y de gestión implementadas por los equipos Red Team y Blue Team en entornos simulados, con el fin de proponer estrategias que fortalezcan la ciberseguridad organizacional.

Objetivos Específicos

Identificar las principales tácticas ofensivas y defensivas empleadas por los equipos Red Team y Blue Team durante los escenarios de simulación.

Evaluar el marco legal y normativo que regula la actuación de los profesionales de ciberseguridad en contextos organizacionales.

Formular recomendaciones que integren elementos técnicos, legales y de gestión para optimizar la respuesta ante incidentes cibernéticos.

Contenido del Trabajo

Etapa 1 Conceptos equipos de Seguridad

La primera fase del proyecto tuvo como objetivo establecer el entorno técnico de pruebas mediante la instalación y configuración de un banco de trabajo virtual, así como el fortalecimiento de conceptos esenciales sobre ciberseguridad, legislación aplicable en Colombia, pruebas de penetración (pentesting) y herramientas especializadas. Esta base es fundamental para desarrollar, de forma estructurada y ética, las actividades de simulación de ataque (Red Team) y defensa (Blue Team) en las siguientes fases del proyecto.

Legislación Colombiana en Delitos Informáticos

Colombia cuenta con un marco legal que regula los delitos informáticos y la protección de datos personales. Entre las normas más relevantes se encuentran:

Ley 1273 de 2009: Modifica el Código Penal e introduce el delito de "protección de la información y de los datos", incluyendo figuras como acceso abusivo a sistemas informáticos, interceptación de datos informáticos, y daño informático. Esta ley es la piedra angular de la ciberlegislación en Colombia. (Función Pública, 2009)

Ley 1581 de 2012: Regula la protección de datos personales y establece principios como legalidad, finalidad, libertad, veracidad, acceso y circulación restringida, seguridad y confidencialidad. (Función Pública, 2012)

Etapas del Pentesting

El pentesting o prueba de penetración se compone de varias fases estructuradas, cuyo objetivo es identificar y explotar vulnerabilidades en un sistema de forma controlada. (Nuclio Digital School, s.f.). Las etapas son:

Reconocimiento (Reconnaissance)

Recolección pasiva y activa de información sobre el objetivo.

Herramienta asociada: Nmap – escaneo de puertos y servicios.

Análisis de Vulnerabilidades

Identificación de posibles puntos débiles en el sistema.

Herramienta asociada: OpenVAS – análisis automático de vulnerabilidades.

Explotación (Exploitation)

Uso de vulnerabilidades para obtener acceso no autorizado.

Herramienta asociada: Metasploit – desarrollo y ejecución de exploits.

Escalada de Privilegios

Obtención de permisos elevados dentro del sistema comprometido.

Herramienta asociada: Scripts personalizados o módulos específicos de Metasploit.

Post-explotación

Análisis del impacto del ataque, mantenimiento del acceso y extracción de información.

Herramienta asociada: Meterpreter (de Metasploit).

Reporte

Documentación detallada de hallazgos y recomendaciones.

Herramientas auxiliares: Plantillas de informes técnicos + referencias normativas.

Herramientas de Ciberseguridad Estudiadas

Las herramientas abordadas en esta fase constituyen una base sólida para las tareas técnicas posteriores. A continuación, se describen brevemente:

Metasploit: Framework utilizado para desarrollar, probar y ejecutar exploits en sistemas vulnerables. Permite simular ataques reales y es esencial en la fase de explotación. (Metasploit, s.f.)

Nmap: Utilidad de código abierto para escaneo de redes. Permite detectar hosts, puertos abiertos, servicios activos y sistemas operativos en un entorno objetivo. (Nmap.org, s.f.)

OpenVAS: Sistema de escaneo de vulnerabilidades altamente completo. Su base de datos se actualiza con regularidad para incluir los últimos CVEs. (Greenbone OpenVAS, s.f.)

ExploitDB: Base de datos pública de exploits y vulnerabilidades, útil para investigación y actualización constante en seguridad ofensiva. (KeepCoding, 2024)

CVE (Common Vulnerabilities and Exposures): Sistema de referencia estandarizada para la identificación y seguimiento de vulnerabilidades de seguridad. (CVE.org, s.f.)

Implementación del Banco de Trabajo

Como parte fundamental de esta fase, se implementó un entorno de laboratorio compuesto por máquinas virtuales, siguiendo los lineamientos de CyberFort Technologies:

Herramienta de virtualización: VMware WorkStation .

Sistemas utilizados: Kali Linux (ofensivo) y Windows (objetivo).

Características técnicas básicas:

Kali Linux: 2 CPU, 4 GB RAM, 20 GB HDD.

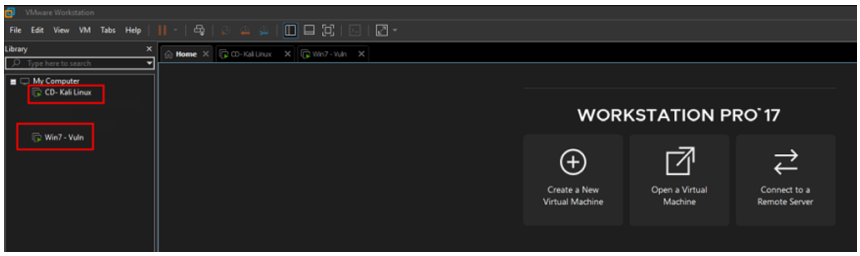
Windows 7/10: 2 CPU, 3 GB RAM, 30 GB HDD.

Configuración de red: Red interna o adaptador puente para permitir comunicación entre máquinas.

Pruebas realizadas:

- Encendido secuencial de máquinas.

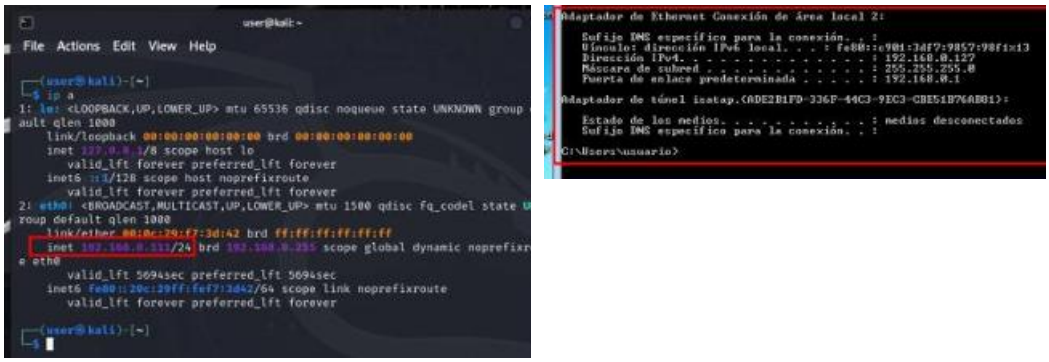
***Figura** 1 Configuración y encendido secuencial de máquinas*



Fuente: Autoría propia.

- Prueba de conectividad entre Kali y Windows.

***Figura 2** Prueba de conectividad entre Kali y Windows*



Fuente: Autoría propia.

Etapa 2 Actuación ética y legal

La segunda fase del proyecto se centró en el análisis ético y legal relacionado con la contratación de profesionales en ciberseguridad, tomando como base el estudio de un contrato de confidencialidad (Anexo 3) y un escenario problemático (Anexo 2) propuesto por CyberFort Technologies. Asimismo, se examinó un caso realista de ciberespionaje (Anexo 7), lo que permitió una reflexión profunda sobre los límites éticos del ejercicio profesional y la aplicación de normas legales como la Ley 1273 de 2009 y el Código de Ética del COPNIA.

Análisis del Acuerdo de Confidencialidad

El contrato de confidencialidad entregado a los aspirantes contenía diversas cláusulas que contravienen principios legales y éticos. Algunas de las irregularidades más evidentes incluyen:

El contrato prohíbe explícitamente a los aspirantes denunciar actividades ilegales, lo cual va en contra del deber ciudadano y del ejercicio ético profesional (Cláusula Cuarta, ítems 3 y 4).

Se establece que, ante cualquier procedimiento legal, el empleado debe asumir la responsabilidad de actos ilícitos, exonerando a la empresa, lo que contraviene los principios de equidad legal.

Esto vulnera derechos constitucionales y legales establecidos en la Ley 1273 de 2009 y contradice el deber ético de todo profesional de informar sobre hechos delictivos.

Estas cláusulas son incompatibles con una práctica profesional honesta y responsable, y configuran posibles delitos como encubrimiento y omisión de denuncia.

Aplicación de la Ley 1273 de 2009

De acuerdo con la Ley 1273 de 2009, se identifican vulneraciones específicas en el acuerdo de confidencialidad:

Artículo 269A (Acceso abusivo a un sistema informático): Al omitir controles éticos sobre la manipulación de datos, se propicia un entorno favorable a este delito. (Función Pública, 2009)

Artículo 269F (Violación de datos personales): La no denuncia de accesos indebidos a datos de terceros puede constituir complicidad en este delito. (Función Pública, 2009)

Artículo 269H (Uso de software malicioso): El contrato no prohíbe el uso de herramientas potencialmente ilegales, dejando una zona gris que podría facilitar conductas delictivas. (Función Pública, 2009)

Estas omisiones en el acuerdo pueden facilitar o encubrir comportamientos que contravienen la ley penal colombiana.

Reflexión Ética sobre la Propuesta Laboral

La propuesta de un salario de $15.000.000 COP mensuales y contrato vitalicio en una empresa con cláusulas abiertamente ilegales y poco éticas plantea un dilema ético serio. Desde el punto de vista del Código de Ética Profesional del COPNIA, se identifican varias incompatibilidades:

Artículo 9: El profesional debe actuar conforme a los intereses de la sociedad, aún por encima de intereses económicos personales. (COPNIA, s.f.)

Artículo 12: Prohíbe aceptar encargos que puedan implicar conflictos éticos o legales. (COPNIA, s.f.)

En consecuencia, aceptar esta oferta laboral sería contraria a los principios de la ética profesional. La integridad debe prevalecer sobre los beneficios económicos, más aún en una profesión tan sensible como la ciberseguridad.

Caso de Estudio: Ciberespionaje en CyberFort Technologies

El caso simulado de ciberespionaje revela múltiples implicaciones legales y éticas:

La empresa utilizó el acceso obtenido para robar información gubernamental, rompiendo los límites del acuerdo con el cliente.

Este acto configura delitos graves como espionaje, tráfico de información y daño a la soberanía nacional.

El hecho de que empleados pudieran realizar estas acciones sin supervisión refleja una falla estructural en la gestión de riesgos.

Preguntas orientadoras:

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible?

El acceso debe estar delimitado por contrato y principios de necesidad, proporcionalidad y consentimiento explícito.

¿Qué mecanismos de control implementar?

Auditorías internas periódicas, políticas de doble supervisión, registro de accesos y análisis post auditoría son fundamentales.

¿Cómo deben responder los gobiernos ante incidentes de espionaje?

Aplicar sanciones penales, romper contratos, exigir reparación del daño e implementar mejores controles de selección de proveedores.

Etapa 3 Ejecución pruebas de intrusión

En esta fase se simula un escenario práctico de Red Team donde se analiza una posible fuga de información en un equipo Windows, causada por la presencia de una aplicación vulnerable. El objetivo es identificar, explotar y documentar la vulnerabilidad, aplicando técnicas reales de intrusión bajo un entorno controlado y legal. Esta fase se desarrolla a partir del Anexo 4 – Escenario 3, haciendo uso del banco de trabajo configurado previamente.

CyberFort Technologies enfrenta un incidente de seguridad, una de sus máquinas presenta una fuga de información. Se sospecha que una aplicación vulnerable instalada en un sistema Windows está permitiendo acceso remoto a través de un exploit. El equipo Red Team debe identificar el vector de ataque, explotarlo y presentar una prueba de concepto (PoC) que demuestre el control del sistema mediante la creación de un nuevo usuario administrador.

Identificación del Fallo de Seguridad

Durante la fase de análisis, se detectaron los siguientes elementos clave:

Sistema vulnerable: Máquina con sistema operativo Windows 7 con software de gestión obsoleto expuesto en el puerto TCP 445.

Tabla 1 *Resumen de los servicios y puertos de la maquina objetivo*

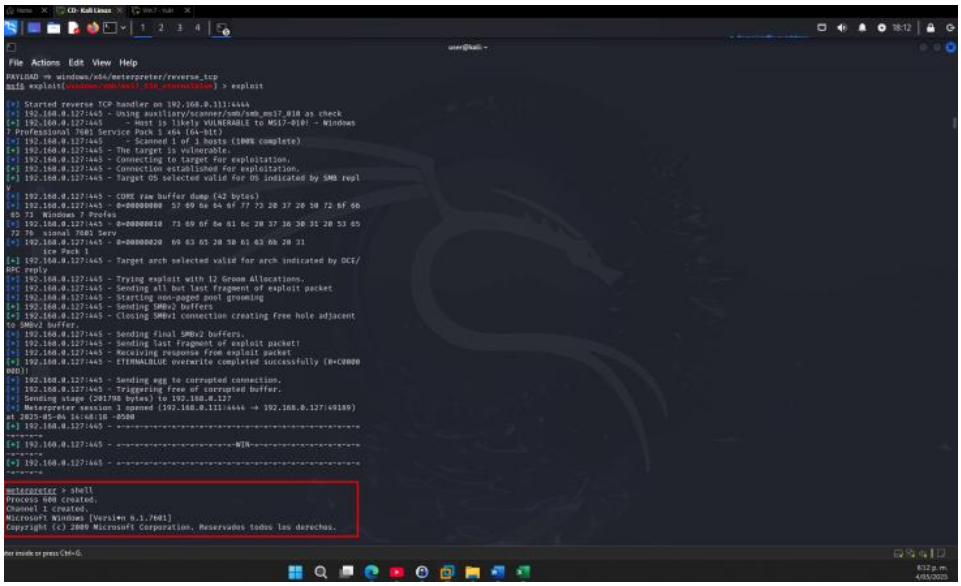
Puerto	Servicio	Comentario
135	MS RPC	Se usa para DCOM; a menudo expuesto a exploits como EternalBlue.
139, 445	SMB	Puede ser vulnerable a **EternalBlue**, **SMBGhost**, o permitir acceso a recursos compartidos.
554	RTSP?	Servicio multimedia; menos común pero a veces vulnerable.
2869, 5357, 10243	HTTPAPI 2.0	UPnP / WS-Discovery; también relacionados con servicios locales expuestos.
49152–49157	MSRPC	Son puertos dinámicos RPC, probablemente relacionados con el servicio DCOM/SMB.

Fuente: Autoría propia.

Exploit asociado: Vulnerabilidad conocida relacionada con SMBv1 (EternalBlue - CVE-2017-0144).

En este punto, se ejecuta el comando de explotación para obtener una Shell de Windows en la máquina víctima, lo que permite al atacante interactuar con el sistema comprometido a través de una interfaz de línea de comandos remota.

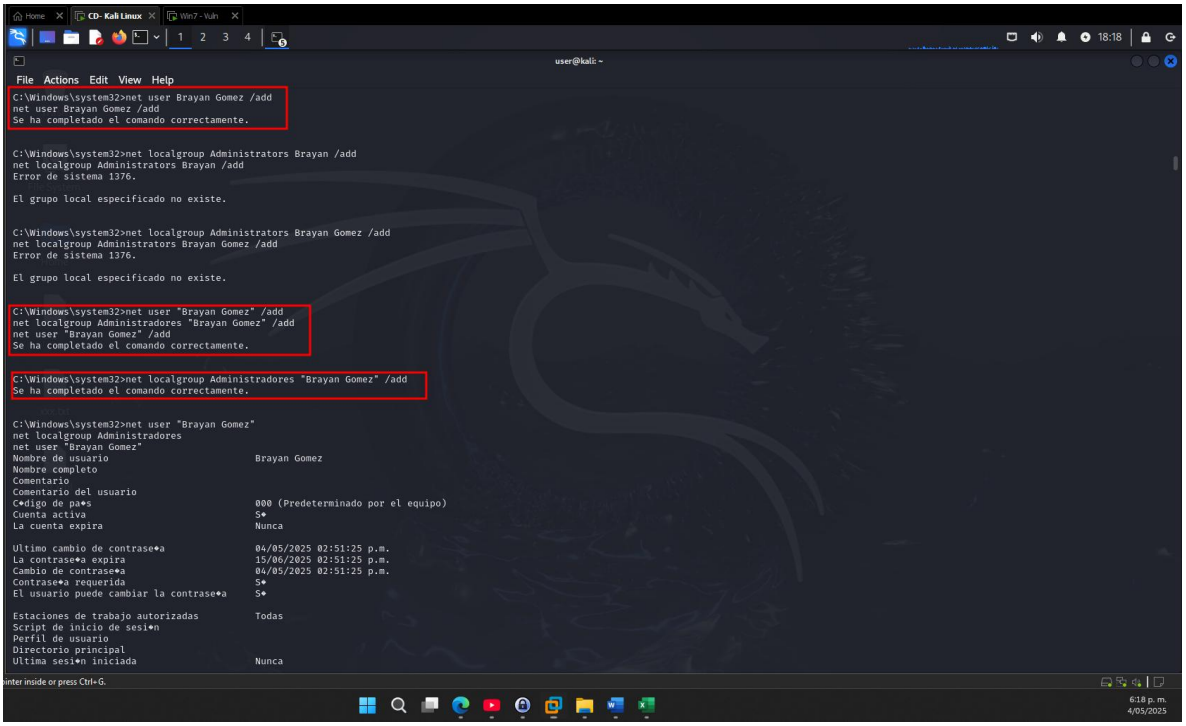
Figura 3 *Shell obtenida en la maquina objetivo*



Fuente: Autoría propia.

Se procede a crear un usuario administrador en el sistema con el primer nombre y apellido, en este caso (Brayan Gomez).

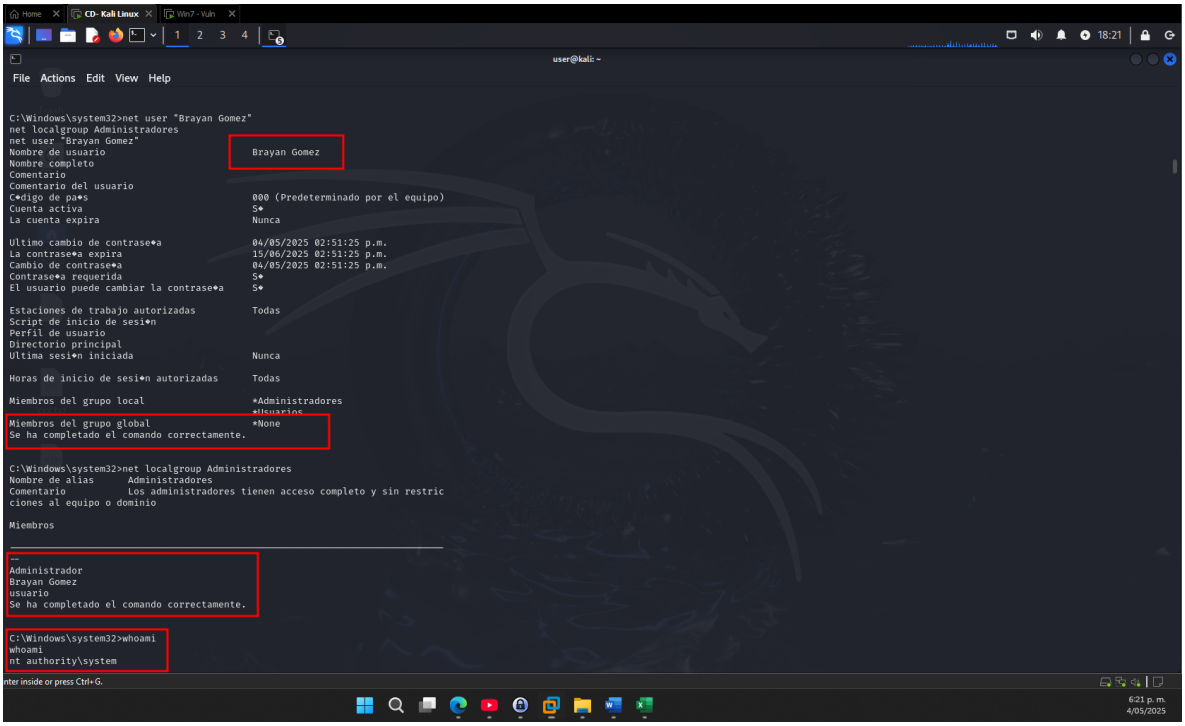
Figura 4 *Creación de usuario en la maquina objetivo.*



Fuente: Autoría propia.

Se crea el usuario Brayan Gomez y se agrega al grupo de usuarios administradores. Posteriormente, se verifican los permisos de ejecución, y se observa que el contexto de ejecución corresponde a NT AUTHORITY\SYSTEM, lo que indica que los comandos se están ejecutando con privilegios de administrador en el sistema, **confirmando así el escalamiento exitoso de privilegios.**

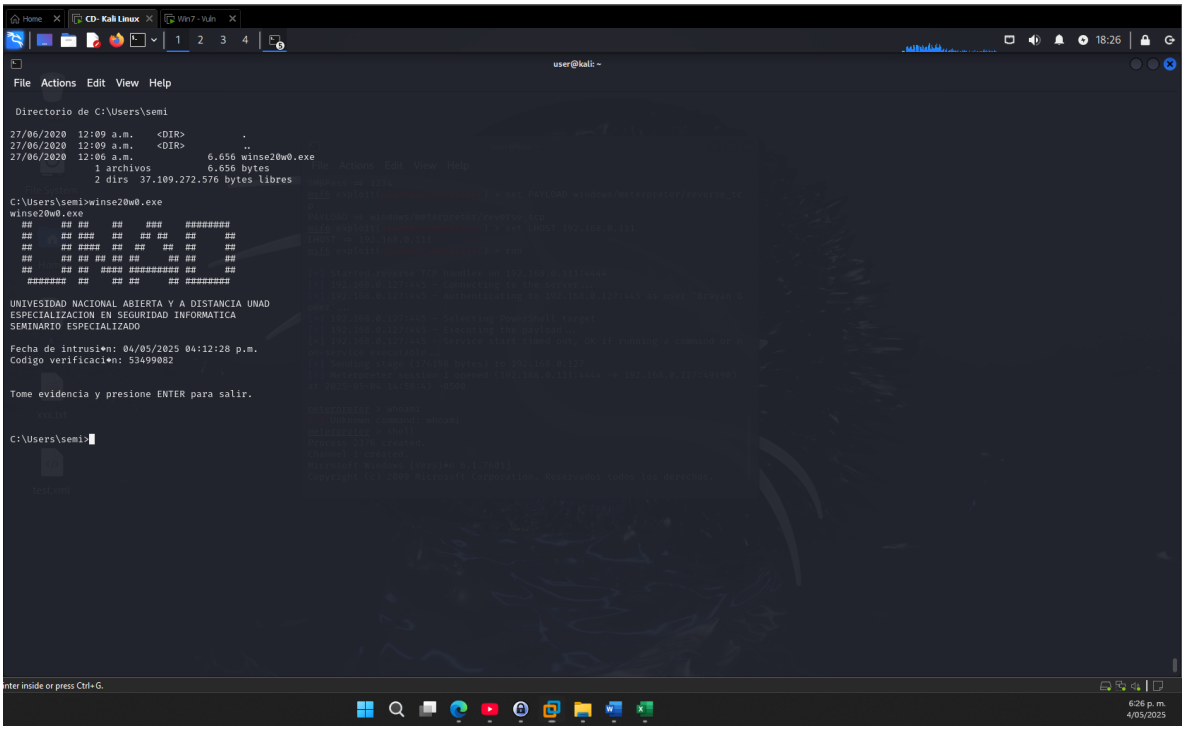
Figura 5 *Elevación de privilegios.*



Fuente: Autoría propia.

Se realiza una búsqueda de información en la máquina objetivo y se encuentra un ejecutable en la ruta C:\Users\semi, denominado winse20w0.exe. Al ejecutar el archivo, el sistema produce el siguiente resultado:

Figura 6 *Archivo de ejecución de la UNAD.*



Fuente: Autoría propia.

Condiciones del entorno: Ausencia de parches de seguridad y acceso directo a la red interna por parte del atacante.

Impacto del Ataque

El ataque simulado permitió:

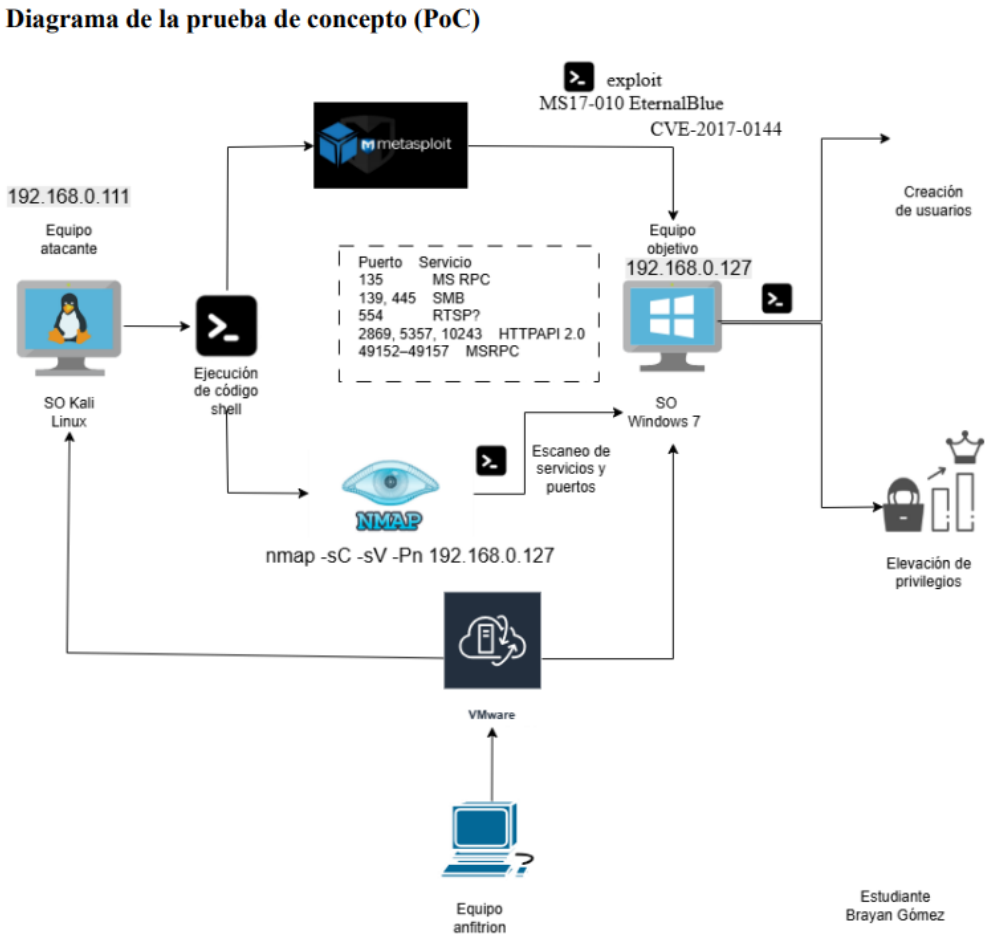
- Acceder remotamente al sistema.
- Escalar privilegios hasta nivel administrador.
- Crear un usuario persistente.
- Demostrar la debilidad del sistema por falta de actualizaciones críticas.

La máquina Windows en cuestión tenía el puerto 445/tcp abierto, lo que expuso el servicio SMB a ataques remotos. Utilizando un exploit que no requiere credenciales, el atacante envía paquetes especialmente diseñados para provocar un desbordamiento de búfer en la

memoria del sistema. Al ser explotada, la vulnerabilidad permite ejecutar código arbitrario en el sistema, obteniendo acceso con privilegios de NT AUTHORITY\SYSTEM, el nivel más alto de permisos.

Una vez comprometida, el atacante tiene control total sobre el sistema, permitiendo crear nuevos usuarios, modificar o eliminar archivos, y ejecutar malware o puertas traseras. Este acceso también permite la fuga de información, manipulación de configuraciones y usuarios, y la posibilidad de que el atacante mantenga persistencia en la red, comprometiendo otros sistemas conectados.

Figura 7 *Diagrama de la prueba de concepto*



Fuente: Autoría propia.

Etapa 4 Contención de ataques informáticos

La cuarta fase del proyecto se centra en la respuesta defensiva ante un ataque informático simulado. Luego de la intrusión exitosa realizada en la Fase 3, el equipo Blue Team asume el reto de analizar el incidente, contener la amenaza y fortalecer la seguridad del entorno afectado. Este ejercicio, basado en el Anexo 5 – Escenario 4, permite aplicar conocimientos en hardening, monitoreo, respuesta a incidentes, y uso de herramientas defensivas bajo licencias libres.

CyberFort Technologies reporta un ataque en tiempo real sobre un sistema Windows previamente vulnerado. La tarea del Blue Team es investigar lo sucedido a nivel del sistema operativo y la red, contener el incidente y proponer medidas que prevengan la repetición del ataque. Dado que no hay presupuesto para software propietario, se deben usar herramientas de código abierto con licencia GPL o equivalente.

Se utilizó un escenario de ataque mediante el protocolo SMB (puerto 445), explotando la vulnerabilidad EternalBlue, lo cual permitió al Red Team evidenciar fallas comunes en sistemas Windows sin hardening.

Respuesta Blue Team:

- Aislamiento inmediato del host comprometido.
- Recolección de evidencia volátil con herramientas como Volatility, Wireshark, netstat, etc.
- Análisis de tráfico y servicios activos.
- Enfoque forense antes de cualquier eliminación de evidencia.

Diferencias de roles:

- El Blue Team actúa de forma proactiva con defensas preventivas y monitoreo.
- El equipo de respuesta a incidentes actúa reactivamente cuando el ataque ya está en curso.

Tabla 2 *Blue Team vs. Equipo de Respuesta a Incidentes*

Blue Team	Equipo de Respuesta a Incidentes (CSIRT)
Se enfoca en la **prevención y detección** de amenazas	Se enfoca en la **gestión y resolución** de incidentes activos
Realiza análisis continuo del entorno	Actúa cuando el ataque ya ha sido detectado
Implementa medidas de hardening y monitoreo	Coordina mitigación, recuperación y análisis post mortem
Es parte estructural del equipo de seguridad	Puede actuar como unidad interna o externa

Fuente: Autoría propia.

Etapa 5 Socialización de informe técnico

Durante esta etapa final del seminario, se elaboró y presentó un informe técnico que consolidó los aprendizajes obtenidos a lo largo del curso. El documento incluyó:

Estrategias aplicadas por los equipos Red Team y Blue Team, basadas en los escenarios de ataque y defensa simulados.

Análisis técnico de vulnerabilidades y medidas de contención, principalmente sobre el protocolo SMB y el exploit EternalBlue.

Recomendaciones específicas orientadas a fortalecer la seguridad organizacional, mediante políticas de hardening, uso de herramientas como SIEM, EDR y marcos como CIS Controls.

Conclusiones orientadas a la construcción del conocimiento, destacando la importancia de la detección temprana, la gestión estructurada de incidentes y la defensa en profundidad.

Además, se elaboraron los siguientes componentes del informe:

- Portada, resumen, índice, glosario e introducción.
- Objetivos generales y específicos.
- Desarrollo técnico y argumentativo del caso.
- Conclusiones y recomendaciones.
- Referencias bibliográficas según la norma APA 7.0, cumpliendo con el requisito de incluir al menos 15 fuentes, 5 de ellas en inglés.

Se realizó también una sustentación en video (mínimo de 8 minutos), donde se expuso el contenido del informe, explicando de forma clara y argumentada los puntos clave del trabajo desarrollado.

Estrategias técnicas del Blue Team

El Blue Team, encargado de la defensa de la infraestructura tecnológica, implementó una serie de estrategias orientadas a la detección temprana de amenazas, la respuesta oportuna a incidentes y el fortalecimiento de la postura de seguridad de los sistemas. Entre las principales acciones se destacó la configuración de sistemas de monitoreo continuo mediante herramientas SIEM (Security Information and Event Management), lo que permitió la correlación de eventos y la identificación de comportamientos anómalos. *Chaparro, G. (2020).*

Asi mismo, se aplicaron controles de hardening en servidores y estaciones de trabajo, eliminando servicios innecesarios y reforzando configuraciones de firewall y políticas de contraseñas. Se implementaron técnicas de segmentación de red, control de accesos y autenticación multifactor, con el fin de reducir la superficie de ataque. Adicionalmente, se realizaron análisis forenses post-intrusión para identificar vectores de entrada y ajustar las políticas de seguridad. *Cano, J., & Romero, L. (2021)*

El Blue Team también desplegó campañas de concientización para mitigar riesgos asociados al factor humano, evidenciando que la seguridad no depende exclusivamente de la tecnología, sino también de los usuarios. Estas acciones permitieron establecer mecanismos de mejora continua frente a las tácticas ofensivas del Red Team.

Estrategias ofensivas del Red Team

El Red Team ejecutó actividades de simulación ofensiva con el objetivo de evaluar la efectividad de los controles de seguridad existentes. Entre las principales tácticas empleadas se encuentran la explotación de vulnerabilidades conocidas (CVE), ataques de ingeniería social, y el uso de malware tipo RAT (Remote Access Trojan) para obtener persistencia y control remoto de sistemas críticos. *Instituto Nacional de Ciberseguridad (INCIBE). (2023)*

A través de técnicas basadas en el marco MITRE ATT&CK, el equipo logró comprometer cuentas privilegiadas mediante movimientos laterales, escalada de privilegios y bypass de controles de seguridad. También se realizaron pruebas de intrusión física, identificando debilidades en los procesos de validación de acceso.

Los hallazgos del Red Team fueron documentados en informes de vulnerabilidad que incluyeron evidencia técnica, vectores de ataque utilizados y recomendaciones específicas para mitigar los riesgos encontrados.

Capacidades legales aplicadas en el ejercicio

El ejercicio simuló escenarios realistas en los que fue necesario actuar dentro del marco legal colombiano, específicamente bajo la Ley 1273 de 2009 (delitos informáticos) y la Ley 1581 de 2012 (protección de datos personales). El cumplimiento normativo fue transversal a todas las acciones, tanto ofensivas como defensivas. *Asamblea Nacional de Colombia. (2009).*

Durante las actividades del Red Team, se establecieron límites claros para las pruebas de penetración, incluyendo acuerdos de confidencialidad y autorizaciones internas, alineados con principios de ética profesional. En el caso del Blue Team, se integraron prácticas de recolección y preservación de evidencia digital conforme a los estándares de la cadena de custodia, lo cual es esencial para posibles procesos judiciales.

Conclusiones

La fase 1 sentó las bases teóricas, técnicas y legales para el desarrollo de las simulaciones de Red Team y Blue Team. La comprensión de las leyes colombianas, la estructura del pentesting y el uso de herramientas profesionales permiten abordar las siguientes fases con fundamentos sólidos, fomentando un enfoque ético y responsable en el ejercicio de la ciberseguridad.

La fase 2 permitió identificar riesgos éticos y legales que pueden presentarse en el ejercicio profesional dentro de la ciberseguridad. El análisis crítico de contratos y escenarios realistas refuerza la necesidad de contar con una base ética sólida, conocimiento legal actualizado y estructuras organizacionales que promuevan la transparencia y la legalidad. Este enfoque es esencial para construir confianza en los servicios de ciberseguridad y garantizar prácticas responsables.

Para la fase 3 la prueba de concepto (PoC) demostró la importancia de mantener actualizados todos los sistemas operativos y servicios dentro de una red corporativa. Se recomienda deshabilitar SMBv1 y aplicar parches de seguridad regularmente para prevenir vulnerabilidades conocidas.

La explotación de la vulnerabilidad MS17-010 (EternalBlue) en el servicio SMBv1 de una máquina Windows 7 permitió obtener acceso remoto sin necesidad de autenticación. Esta vulnerabilidad es conocida por ser un vector de ataque, ya que habilita a un atacante para ejecutar código malicioso con privilegios elevados y tomar control total del sistema. La vulnerabilidad afecta a sistemas que no han sido actualizados con los parches de seguridad adecuados, lo que facilita su explotación mediante herramientas como EternalBlue

La simulación del ataque permitió evidenciar la importancia de contar con mecanismos de monitoreo y respuesta activa por parte del equipo Blue Team. Se concluye que una reacción temprana, estructurada y basada en análisis técnico puede mitigar el impacto de un incidente.

Las medidas de hardenización, como la desactivación de SMBv1, segmentación de red y aplicación de parches, resultan esenciales para prevenir la repetición de ataques similares. Además, el uso de marcos como CIS y herramientas como SIEM refuerzan la capacidad de defensa en profundidad

La simulación de escenarios permitió evidenciar la importancia de contar con equipos Red Team y Blue Team coordinados, cuyas capacidades técnicas resultan esenciales para anticipar, detectar y responder a amenazas cibernéticas de forma efectiva.

El análisis de las tácticas ofensivas y defensivas aplicadas demostró que la seguridad de una organización no solo depende de herramientas tecnológicas, sino también de la implementación de buenas prácticas de gestión, monitoreo continuo y entrenamiento del personal.

El componente legal se consolida como una dimensión crítica en la actuación de los profesionales en ciberseguridad. La aplicación de la Ley 1273 de 2009 y la Ley 1581 de 2012 durante los ejercicios garantiza que las acciones técnicas estén enmarcadas en la legalidad, reduciendo riesgos éticos y judiciales.

La gestión integrada de la seguridad, que articula lo técnico, lo legal y lo organizacional, permite construir una postura de defensa sólida, resiliente y adaptable ante un entorno de amenazas en constante evolución.

Recomendaciones

Implementar planes de formación continua para los equipos de ciberseguridad, que incluyan no solo entrenamiento técnico, sino también actualizaciones en legislación vigente y normativas internacionales.

Establecer procedimientos formales de coordinación entre los equipos Red Team y Blue Team, permitiendo ciclos constantes de retroalimentación que fortalezcan la capacidad organizacional frente a amenazas emergentes.

Incluir dentro de las políticas internas de seguridad un protocolo de actuación legal, que contemple aspectos como la preservación de evidencia digital, la gestión de incidentes y la protección de datos personales.

Priorizar el uso de marcos de referencia reconocidos como MITRE ATT&CK y NIST para estructurar las defensas y ofensivas, lo cual estandariza prácticas y mejora la interoperabilidad entre equipos técnicos.

Promover la creación o fortalecimiento de un Centro de Operaciones de Seguridad (SOC) que centralice la detección y respuesta ante incidentes, y facilite la integración de los componentes técnicos, legales y administrativos de la seguridad de la información.

Referencias Bibliografía

Agudelo, A. (2022). Guía práctica para la respuesta a incidentes de seguridad informática. Universidad Nacional Abierta y a Distancia - UNAD.

Álvarez, F. (2020). Análisis de vulnerabilidades en entornos corporativos: herramientas y técnicas. Revista Colombiana de Tecnologías de Información, 12(1), 45-59.

Asamblea Nacional de Colombia. (2009). Ley 1273 de 2009. Por la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado – la protección de la información y de los datos. Recuperado el 26 de mayo de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=37815

Asamblea Nacional de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Recuperado el 26 de mayo de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Cano, J., & Romero, L. (2021). Ciberseguridad: estrategia integral para organizaciones modernas. Editorial Ecoe.

Cárdenas, M. (2021). Forense digital: principios y aplicación en investigaciones informáticas. Bogotá: RedBooks.

Centro Nacional de Respuesta a Incidentes Cibernéticos (colCERT). (2023). Boletín de alertas y buenas prácticas en ciberseguridad. Recuperado el 26 de mayo de 2025, de https://www.colcert.gov.co

CERT Colombia. (2023). Guía de actuación ante incidentes cibernéticos. Recuperado el 26 de mayo de 2025, de https://www.cert.gov.co

Chaparro, G. (2020). Implementación de estrategias defensivas tipo Blue Team en medianas empresas. Revista de Ingeniería y Desarrollo, 18(2), 33-47.

COPNIA. (s.f.). COPNIA. Recuperado el 26 de mayo de 2025, de COPNIA: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

CVE.org. (s.f.). CVE.org. Recuperado el 26 de mayo de 2025, de https://www.cve.org/

Fernández, C. (2022). Hardening de sistemas operativos y control de accesos. Editorial Alfaomega.

Función Pública. (05 de enero de 2009). Función Pública. Recuperado el 26 de mayo de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34492

Función Pública. (18 de octubre de 2012). Función Pública. Recuperado el 26 de mayo de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

González, D. (2021). Buenas prácticas de gestión en centros de operaciones de seguridad (SOC). Revista Latinoamericana de Seguridad Informática, 7(3), 22-35.

Greenbone OpenVAS. (s.f.). Greenbone OpenVAS. Recuperado el 26 de mayo de 2025, de https://openvas.org/

Gutiérrez, L. (2022). Análisis legal de los delitos informáticos en Colombia. Universidad del Rosario.

Instituto Nacional de Ciberseguridad (INCIBE). (2023). Guía Red Team: ataques simulados en entornos corporativos. Recuperado el 26 de mayo de 2025, de https://www.incibe.es

KeepCoding. (31 de julio de 2024). KeepCoding. Recuperado el 26 de mayo de 2025, de https://keepcoding.io/blog/que-es-exploitdb/

Martínez, P. (2021). Ética profesional y ciberseguridad: desafíos del siglo XXI. Editorial UOC.

Mendoza, S., & Ruiz, T. (2023). Estrategias integradas para la gestión de riesgos tecnológicos. Universidad EAFIT.

Metasploit. (s.f.). Metasploit. Recuperado el 26 de mayo de 2025, de https://docs.metasploit.com/

Mitre Corporation. (2024). MITRE ATT&CK Framework. Recuperado el 26 de mayo de 2025, de https://attack.mitre.org

National Institute of Standards and Technology (NIST). (2020). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Recuperado el 26 de mayo de 2025, de https://www.nist.gov/cyberframework

Nmap.org. (s.f.). Nmap.org. Recuperado el 26 de mayo de 2025, de https://nmap.org/docs.html

Nuclio Digital School. (s.f.). Nuclio Digital School. Recuperado el 26 de mayo de 2025, de https://nuclio.school/blog/que-es-el-pentesting/

O'Reilly, T. (2021). Offensive Security: Red Team Tactics and Techniques. CyberWar Publishing.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications.

Skoudis, E., & Liston, T. (2018). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall.

Apéndices

Apéndice A

Video de socialización

URL: **Brayan Gomez - Video - 2025-05-29 21-51-57.mkv**

Texto claro de la URL: **https://unadvirtualedu-my.sharepoint.com/:v:/g/personal/bagomezl_unadvirtual_edu_co/Ef4gRkOlo8JGueKAGOpLQCEBNy6Bgt6VNVEgtIueqbXAOQ?e=2xjhCJ**

Apéndice B

Presentación - Fase 5

URL: **Brayan Gomez - Presentación - Fase 5.pptx**

Texto claro de la URL: **https://unadvirtualedu-my.sharepoint.com/:p:/g/personal/bagomezl_unadvirtual_edu_co/EWCM-YGPlVdJnzhjfX80_4UB5o7oFUA6JSACjR_g9O5AyA?e=hQODQC**