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

John Cesar Prieto Duran

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

Quiero expresar mi más sincero agradecimiento a Universidad Nacional Abierta y a Distancia UNAD por brindarme la oportunidad de cursar esta especialización en Seguridad Informática.

Agradezco especialmente a los profesores por su orientación y apoyo en la dirección de mi proyecto de grado, por compartir sus conocimientos y experiencias conmigo mediante la metodología de nuestra Universidad.

Dedicatoria

A mi esposa, por su amor, apoyo y comprensión durante todo este tiempo. Gracias por ser mi compañera y motivarme a seguir adelante.

A mis queridos hijos, quienes son mi mayor inspiración y motivo de orgullo. Gracias por enseñarme la importancia de ser perseverante y luchar por nuestros sueños.

A mis padres, por su amor incondicional, consejos y valores que me han guiado en todo momento. Gracias por ser mi ejemplo para seguir y por enseñarme a ser una persona íntegra y comprometida.

Resumen

El presente informe técnico reúne las actividades y aprendizajes desarrollados en el seminario especializado "Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team". Este curso abordó la simulación de ataques cibernéticos y las estrategias de defensa para fortalecer la seguridad organizacional, con un enfoque práctico y alineado a estándares internacionales. A través de ejercicios orientados, se evaluaron vulnerabilidades, se implementaron medidas de contención y se propusieron mejoras estratégicas en ciberseguridad.

El seminario se estructuró en dos perspectivas complementarias: el Red Team, encargado de simular ataques ofensivos, y el Blue Team, responsable de defender las infraestructuras críticas y contener incidentes en tiempo real. Durante la etapa inicial, se exploraron las fases del pentesting, desde el reconocimiento hasta la cobertura de huellas, empleando herramientas como Nmap, Metasploit y OpenVAS. Estas actividades permitieron identificar vulnerabilidades clave en entornos simulados y documentar técnicas avanzadas de ataque, como la explotación de vulnerabilidades y la escalación de privilegios. El informe destaca la importancia del cumplimiento normativo y las mejores prácticas internacionales en ciberseguridad. Se revisaron marcos legales relevantes, como la Ley 1273 de 2009 y la Ley 1581 de 2012 en Colombia, así como guías técnicas como los CIS Benchmarks y estándares como ISO 27001. Estas referencias fortalecieron la alineación entre las estrategias técnicas y los requisitos legales, asegurando la protección de datos y la privacidad en un contexto organizacional.

***Palabras clave*:** Blue Team, Ciberseguridad, Red Team, Seguridad informática, Vulnerabilidades

Abstract

This technical report compiles the activities and learnings developed during the specialized seminar "Strategic Teams in Cybersecurity: Red Team & Blue Team." This course addressed the simulation of cyberattacks and defense strategies to strengthen organizational security, with a practical approach aligned with international standards. Through guided exercises, vulnerabilities were evaluated, containment measures were implemented, and strategic cybersecurity improvements were proposed.

The seminar was structured into two complementary perspectives: the Red Team, responsible for simulating offensive attacks, and the Blue Team, tasked with defending critical infrastructures and containing incidents in real time. During the initial stage, the phases of penetration testing were explored, from reconnaissance to covering tracks, using tools such as Nmap, Metasploit, and OpenVAS. These activities enabled the identification of key vulnerabilities in simulated environments and the documentation of advanced attack techniques, including vulnerability exploitation and privilege escalation. The report highlights the importance of regulatory compliance and international best practices in cybersecurity. Relevant legal frameworks, such as Colombia's Law 1273 of 2009 and Law 1581 of 2012, were reviewed, along with technical guides like CIS Benchmarks and standards such as ISO 27001. These references strengthened the alignment between technical strategies and legal requirements, ensuring data protection and privacy within an organizational context.

Keywords: Blue Team, Cybersecurity, Red Team, Information Security, Vulnerabilities

Tabla de Contenido

pág.

Lista de Tablas

Lista de Figuras

Glosario

Amenazas: posibles daños que pueden ocurrir y perjudicar sustancialmente el sistema de información de la empresa en caso de suceder. Algunas amenazas son exposición de información confidencial, robo de contraseñas, phishing, spam, malware, redes zombie, exploit, ataques día cero, virus informáticos, denegación de servicios, caballos de troya, interceptación, entre otros.

Antivirus: software desarrollado para contrarrestar las infecciones maliciosas en los equipos. Tiene características para la protección de archivos, navegación segura en internet, almacenamiento de contraseñas, protección de la red, filtros anti-spam, defensa ante sitios web maliciosos y firewall.

Atacantes: usuarios que poseen conocimientos en informática y aprovechan internet para realizar estafas, daños, propagar virus, robar dinero, espiar personas o provocar daños en los computadores con la distribución de malware.

Autenticación: proceso mediante el cual el usuario que desee ingresar a los programas de la empresa debe suministrar un usuario y contraseña habilitados para confirmar que efectivamente es la persona indicada y poder acceder a los recursos informáticos.

Blue Team [1]: El grupo responsable de defender el uso de los sistemas de información de una empresa manteniendo su postura de seguridad contra un grupo de atacantes simulados (es decir, el Equipo Rojo). Por lo general, el Equipo Azul y sus seguidores deben defenderse contra ataques reales o simulados 1) durante un período de tiempo significativo, 2) en un contexto operativo representativo (por ejemplo, como parte de un ejercicio operativo), y 3) de acuerdo con

[1] NIST. (2015 *Equipo azul - Glosario | CSRC*. National Institute of Standards and Technology (NIST). https://csrc.nist.gov/glossary/term/blue_team

las reglas establecidas y monitoreadas con la ayuda de un grupo neutral que arbitra la simulación o ejercicio (es decir, el Equipo Blanco).

Firewall: software o dispositivo informático que previene el ingreso no autorizado de usuarios y/o programas a la red interna de la empresa. Se debe implementar una configuración para instaurar unas restricciones y autorizaciones para que los equipos se comuniquen de forma segura.

IDS: Sistema de detección de intrusos, programa que permite a las organizaciones identificar accesos no autorizados a la red o a una determinada computadora.

Ingeniería social: es una de las formas en las que los cibercriminales usan las interacciones entre personas para que el usuario comparta información confidencial. Ya que la ingeniería social se basa en la naturaleza y las reacciones humanas, hay muchas formas en que los atacantes pueden engañar, en línea o sin conexión.[2]

Malware: software malintencionado, como virus, troyanos o gusanos, creado con el fin de introducirse en la computadora y provocar daños en el sistema de múltiples formas.

Phishing: suplantación o falsificación ingeniosa en la que se presenta una página web como oficial, haciendo creer al usuario que puede ingresar sus credenciales de autenticación para ser recolectados y utilizados en fraudes.

Políticas de seguridad: son las directrices y medidas establecidas por una empresa para proteger su sistema de información y sus activos. Incluyen políticas para la autenticación de usuarios, la protección de contraseñas, la gestión de accesos, el uso de dispositivos móviles y la respuesta a incidentes de seguridad.

---

[2] Norton. (2018). *¿Qué es la ingeniería social?*. Norton. https://co.norton.com/blog/emerging-threats/what-is-social-engineering

Ransomware: es un tipo de malware que cifra los archivos en la computadora del usuario y exige un rescate para desbloquearlos. A menudo se distribuye a través de correos electrónicos con archivos adjuntos infectados o mediante descargas de software malicioso desde sitios web comprometidos.

Red Team[3]: Un grupo de personas autorizadas y organizadas para emular las capacidades de ataque o explotación de un adversario potencial contra la postura de seguridad de una empresa. El objetivo del Equipo Rojo es mejorar la ciberseguridad empresarial demostrando los impactos de los ataques exitosos y demostrando lo que funciona para los defensores (es decir, el Equipo Azul) en un entorno operativo.

Rootkit: es un tipo de malware diseñado para ocultar su presencia en la computadora y evitar la detección por parte de los antivirus y otros programas de seguridad. Los rootkits suelen instalarse de forma oculta en el sistema y pueden ser utilizados para robar información, realizar ataques de denegación de servicio o controlar la computadora de forma remota.

Spam: son correos electrónicos no deseados que suelen incluir publicidad engañosa, ofertas falsas, malware o phishing. Es importante tener medidas de seguridad adecuadas para filtrar el spam y evitar que los usuarios interactúen con estos correos electrónicos.

Troyano: es un tipo de malware que se disfraza de programa legítimo y se instala en la computadora del usuario sin su conocimiento. Los troyanos pueden ser utilizados para robar información, tomar el control de la computadora de forma remota o realizar otras actividades maliciosas.

---

[3] National Institute of Standards and Technology (NIST). (2015). *Red Team - Glossary term.* CSRC. https://csrc.nist.gov/glossary/term/red_team

VPN: es una red privada virtual que permite a los usuarios conectarse a internet de forma segura y proteger su privacidad. Los usuarios pueden acceder a recursos de la red de la empresa desde cualquier lugar del mundo sin comprometer la seguridad de la información. Es importante utilizar una VPN segura para proteger la información confidencial y evitar el acceso no autorizado.

Zero day[4]: se refiere a una vulnerabilidad de seguridad en un sistema que aún no ha sido descubierta por los fabricantes de software o por la comunidad de seguridad. Los ataques zero-day son especialmente peligrosos ya que no hay parches o soluciones disponibles para protegerse contra ellos. Es importante tener medidas de seguridad adecuadas para detectar y protegerse contra estos ataques.

[4] Kaspersky . (2025). *Zero-day exploit: Definición y funcionamiento*. Kaspersky Resource Center. https://latam.kaspersky.com/resource-center/definitions/zero-day-exploit

Introducción

En el entorno actual de ciberseguridad, las organizaciones se enfrentan a un panorama de amenazas en constante evolución, lo que hace indispensable el desarrollo de estrategias eficaces para proteger sus activos y sistemas críticos. En este contexto, el seminario especializado "Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team" ha proporcionado una plataforma para adquirir y aplicar conocimientos clave en la evaluación y mejora de las defensas cibernéticas de las organizaciones. A través de un enfoque práctico, los participantes han tenido la oportunidad de experimentar con las tácticas y herramientas utilizadas por los equipos Red Team y Blue Team para simular y defenderse de ataques cibernéticos, respectivamente.

El Red Team se encarga de realizar simulaciones de ataques, con el objetivo de identificar vulnerabilidades en los sistemas de una organización, mientras que el Blue Team tiene la responsabilidad de proteger esos sistemas, contener incidentes y mitigar las amenazas identificadas. Ambas facetas del seminario han sido esenciales para fortalecer la comprensión de las técnicas ofensivas y defensivas, proporcionando un marco completo para mejorar la postura de seguridad de las organizaciones.

Este informe presenta un análisis detallado de las actividades realizadas durante el seminario, con un enfoque en las estrategias implementadas por el Red Team y el Blue Team, así como las herramientas y metodologías utilizadas. A través de este informe, se busca evaluar las lecciones aprendidas, proponer recomendaciones para mejorar las estrategias de ciberseguridad y ofrecer conclusiones sobre el impacto de estas prácticas en la protección de los sistemas informáticos. También, se discuten las implicaciones legales y normativas que deben tenerse en cuenta al implementar estas estrategias, asegurando el cumplimiento de las leyes de protección de datos y privacidad.

Objetivos

Objetivo Principal

Analizar las estrategias implementadas por los equipos Red Team y Blue Team durante el seminario especializado en ciberseguridad, evaluando su efectividad en la identificación y mitigación de amenazas.

Objetivos Específicos

Evaluar las implicaciones legales y normativas relacionadas con el manejo de la información, la privacidad y la protección de datos, proporcionando recomendaciones que garanticen el cumplimiento normativo y la transparencia en las prácticas de seguridad informática dentro de la organización.

Identificar las técnicas utilizadas por el equipo ofensivo (Red Team) para la simulación de ataques, la explotación de vulnerabilidades y el acceso no autorizado, evaluando los resultados obtenidos y su impacto en la postura de seguridad organizacional.

Examinar las medidas implementadas por el Blue Team para la mitigación de los ataques identificados por el Red Team, enfocándose en la contención de incidentes, la mejora de la postura de seguridad y la implementación de acciones correctivas basadas en las lecciones aprendidas

Desarrollo del Trabajo

En un entorno donde las amenazas cibernéticas son cada vez más sofisticadas, las organizaciones deben adoptar un enfoque integral que combine la aplicación de estrategias técnicas con el cumplimiento de principios legales y éticos. La gestión efectiva de la seguridad informática no solo implica detectar y mitigar vulnerabilidades, sino también garantizar que todas las acciones se realicen en un marco que respalde la protección de la información, la transparencia y la responsabilidad profesional.

Este informe técnico analiza, en primer lugar, el marco legal y ético que guía las operaciones de ciberseguridad, proporcionando una base sólida para la toma de decisiones. A continuación, se presentan las acciones realizadas por los equipos Red Team y Blue Team, destacando cómo cada uno contribuye a fortalecer la seguridad organizacional mediante la identificación y mitigación de riesgos, con el objetivo final de proponer mejoras que refuercen la postura de seguridad integral de la organización.

Legislación Colombiana en Delitos Informáticos y Protección de Datos Personales

La legislación colombiana en materia de delitos informáticos y protección de datos personales continúa evolucionando para hacer frente a las crecientes amenazas cibernéticas y al constante avance tecnológico. Colombia ha fortalecido su marco normativo para garantizar la seguridad de la información y la privacidad de los ciudadanos, estableciendo sanciones específicas para quienes vulneren los sistemas informáticos o traten indebidamente datos personales.

En el marco legal colombiano, se destacan las siguientes leyes y decretos:

Ley 1273 de 2009: Esta ley modificó el Código Penal colombiano, creando el bien jurídico de la "protección de la información y los datos", y sanciona delitos como el acceso

abusivo a sistemas informáticos, la interceptación de datos, el daño informático, y el uso de software malicioso. Sigue siendo uno de los pilares fundamentales para la protección de los activos informáticos en el país. Esta legislación ha sido complementada con lineamientos adicionales emitidos por organismos de control, que refuerzan la capacidad de las autoridades para perseguir y castigar a los ciberdelincuentes. [5]

Ley 1581 de 2012: Conocida como la Ley de Protección de Datos Personales, esta legislación establece los principios fundamentales para el tratamiento de los datos personales en Colombia. Garantiza a los ciudadanos derechos como el acceso, la rectificación, cancelación y oposición (ARCO) respecto de sus datos personales. Esta ley ha sido la base para regular el manejo de datos por parte de empresas y entidades públicas, obligándolas a implementar medidas de seguridad adecuadas para proteger la información personal. En los últimos años, la Superintendencia de Industria y Comercio (SIC) ha intensificado la vigilancia y el cumplimiento de esta norma, imponiendo sanciones más severas por incumplimientos.

Decreto 1377 de 2013: Este decreto reglamenta la Ley 1581 de 2012, estableciendo mecanismos para que las empresas informen a los titulares sobre el tratamiento de sus datos personales y obtengan su consentimiento informado. Desde 2024, las empresas han tenido que adaptar sus políticas de privacidad de acuerdo con las directrices más recientes del Ministerio de tecnologías de la Información y las Comunicaciones (MinTIC), que exigen una mayor transparencia en el tratamiento de los datos personales.

CONPES 3995 de 2020: La Política Nacional de Confianza y Seguridad Digital, implementada mediante el CONPES 3995, establece un marco estratégico para fomentar la

---

[5] Congreso de la República de Colombia. (2011, 23 de diciembre). Ley 1273 de 2009 - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

confianza en el uso del entorno digital en Colombia. Esta política busca fortalecer las capacidades del país en ciberseguridad, promoviendo la colaboración entre el sector público y privado para responder a las crecientes amenazas digitales.6

Convenio sobre la Ciberdelincuencia de la OEA (2018): Colombia también se ha alineado con marcos internacionales, como el Convenio sobre la ciberdelincuencia de la Organización de los Estados Americanos, que proporciona una estructura de cooperación internacional en la lucha contra los delitos cibernéticos y refuerza el compromiso de Colombia con la protección de la información en el ámbito global.

[6] Departamento Nacional de Planeación. (2019). CONPES 3995 de 2019 - Política nacional para la formalización empresarial en Colombia. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Etapas del Pentesting y Herramientas Utilizadas

El pentesting es una actividad crítica en ciberseguridad que consiste en evaluar la seguridad de un sistema mediante simulaciones de ataques controlados. Este proceso permite identificar y corregir vulnerabilidades antes de que sean explotadas por actores malintencionados. Las pruebas de penetración siguen un conjunto de etapas definidas que permiten estructurar el análisis de seguridad[7].

Fase 1: Reconocimiento (Information Gathering)

Esta primera fase consiste en recopilar toda la información posible sobre el objetivo, como direcciones IP, nombres de dominio, puertos abiertos, servicios expuestos, entre otros. El objetivo es crear un perfil del sistema para identificar puntos potenciales de ataque.

Herramienta recomendada: Nmap es un escáner de red esencial en esta fase, ya que permite mapear la red y descubrir los puertos y servicios disponibles. Además, puede ser complementado con whois y dig para obtener información de dominios y DNS.

Fase 2: Escaneo y Enumeración (Scanning & Enumeration)

En esta etapa, se exploran los puertos y servicios descubiertos durante el reconocimiento, buscando vulnerabilidades asociadas. Es crucial comprender las versiones de software utilizadas y cualquier vulnerabilidad pública conocida.

Herramienta recomendada: OpenVas es un escáner de vulnerabilidades que permite automatizar el análisis de servicios, identificando posibles puntos débiles con base en una extensa base de datos de vulnerabilidades conocidas (CVE).

---

[7] IBM. (2024). Penetration testing. IBM. https://www.ibm.com/es-es/topics/penetration-testing

Fase 3: Explotación (Exploitation)

Una vez identificadas las vulnerabilidades, el pentester intenta explotarlas para obtener acceso no autorizado al sistema. Esta es la fase más crítica, ya que implica ejecutar exploits reales en un entorno controlado para comprobar si el sistema es susceptible a ataques.

Herramienta recomendada: Metasploit Framework es una de las herramientas más potentes en esta fase, facilitando la explotación de vulnerabilidades con una amplia colección de exploits automatizados. Además, herramientas específicas como SQLmap pueden ser usadas para explotar vulnerabilidades en bases de datos.

Fase 4: Mantenimiento del Acceso (Maintaining Access)

Después de explotar con éxito una vulnerabilidad, el objetivo es mantener el acceso al sistema sin ser detectado. Para esto, se utilizan técnicas que permiten al atacante establecer puertas traseras o persistencia, asegurando que puedan volver al sistema incluso si el vector inicial de ataque es corregido.

Herramienta recomendada: Netcat, conocido como la "navaja suiza" de las redes, permite establecer conexiones ocultas y crear túneles de comunicación entre el atacante y el sistema comprometido.

Fase 5: Cobertura de Huellas (Covering Tracks)

La última fase implica eliminar cualquier rastro del ataque, asegurándose de que las actividades realizadas durante la prueba no puedan ser detectadas ni rastreadas. Esto es crucial en un entorno real para que los atacantes no dejen pistas de sus acciones.

Herramienta recomendada: Ccleaner, aunque generalmente se asocia con la limpieza de archivos temporales, también puede utilizarse para eliminar logs y rastros de actividad en el sistema comprometido.

Herramientas y Servicios en Ciberseguridad

Las herramientas y servicios en ciberseguridad son primordiales para proteger los activos tecnológicos y responder a las amenazas en un entorno cada vez más complejo. En la actualidad, las organizaciones no solo deben defenderse contra ciberataques, sino también anticiparse a ellos mediante el uso de tecnologías avanzadas que permitan identificar vulnerabilidades, simular ataques controlados y fortalecer sus defensas.

A continuación, se describen algunas de las herramientas más utilizadas en la industria, tanto en el ámbito ofensivo (Red Team) como defensivo (Blue Team), destacando su aplicabilidad en entornos de simulación como en producción:

Metasploit Framework

Metasploit es una de las plataformas más robustas para realizar pruebas de penetración. Permite a los profesionales de ciberseguridad ejecutar exploits y evaluar la seguridad de sus sistemas mediante un amplio catálogo de vulnerabilidades conocidas. Su flexibilidad para desarrollar y automatizar ataques hace de Metasploit una herramienta indispensable en la fase de Explotación de un pentesting.

Aplicación: Además de su uso ofensivo, también es valiosa para el Blue Team, ya que puede utilizarse para simular ataques y evaluar las defensas actuales de los sistemas.

Nmap (Network Mapper)

Nmap es una herramienta esencial para el reconocimiento y mapeo de redes. 0Permite identificar puertos abiertos, servicios en ejecución y sistemas operativos activos en una red, proporcionando información crítica para entender el estado de seguridad del sistema. En la fase de Reconocimiento del pentesting, Nmap es la primera herramienta en ser utilizada.

Aplicación: Los equipos defensivos también pueden utilizar Nmap para monitorear sus

redes y detectar actividad inusual, como la apertura de puertos inesperados.

Openvas

Este es un escáner de vulnerabilidades de código abierto que permite realizar análisis profundos en sistemas, identificando posibles vulnerabilidades de acuerdo con bases de datos de CVE (Common Vulnerabilities and Exposures). OpenVAS es crucial en la fase de Escaneo y Enumeración, donde se busca obtener un diagnóstico completo de los puntos débiles del sistema.

Aplicación: Tanto en entornos ofensivos como defensivos, OpenVAS ayuda a identificar vulnerabilidades que deben ser priorizadas para mitigación.

Wireshark

Wireshark es un analizador de protocolos de red que permite la captura y análisis de tráfico en tiempo real. Su capacidad para inspeccionar paquetes de red lo convierte en una herramienta clave para la detección de intrusiones y el análisis forense post-ataque.

Aplicación: El Blue Team la utiliza para monitorear tráfico sospechoso y detectar posibles exfiltraciones de datos o actividades maliciosas.

Exploitdb y CVE[8]

ExploitDB es un repositorio en línea de exploits y vulnerabilidades, mientras que CVE (Common Vulnerabilities and Exposures) es una referencia estandarizada para identificar vulnerabilidades conocidas. Estas bases de datos son herramientas cruciales para profesionales de seguridad que necesitan acceder rápidamente a información actualizada sobre vulnerabilidades críticas.

---

[8] Fortinet. (2024). **CVE (Common Vulnerabilities and Exposures)**. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/cve

Aplicación: El Red Team usa ExploitDB para desarrollar nuevos vectores de ataque basados en vulnerabilidades conocidas, mientras que el Blue Team monitorea continuamente las CVE para parchear sus sistemas de manera proactiva.

Burp Suite

Burp Suite es una plataforma integrada para realizar pruebas de seguridad en aplicaciones web. Permite descubrir vulnerabilidades en aplicaciones web, como inyecciones de SQL, ataques XSS y problemas de autenticación. Burp Suite es fundamental en la fase de Explotación para atacar aplicacionesnweb.

Aplicación: También es útil para el equipo de defensa, ya que permite detectar vulnerabilidades en las aplicaciones antes de que sean explotadas por atacantes externos.

Servicios de Monitoreo de Amenazas

Servicios en la nube como AlienVault o ThreatConnect proporcionan inteligencia sobre amenazas, alertando a las organizaciones sobre posibles ataques vulnerabilidades activas en sus infraestructuras. Estos servicios ayudan a los equipos de ciberseguridad a estar actualizados sobre las últimas tácticas, técnicas y procedimientos (TTPs) utilizados por los atacantes.

Aplicación: Estos servicios son usados predominantemente por el Blue Team para la detección y respuesta ante incidentes, permitiéndoles actuar de manera rápida y proactiva.

Implementación del Banco de Trabajo

Para llevar a cabo pruebas de seguridad y simulaciones realistas, es esencial crear un entorno controlado. Este "banco de trabajo" permite ejecutar pruebas de ciberseguridad en un ambiente seguro, garantizando la replicabilidad de los resultados sin comprometer la máquina desde donde se realice el laboratorio.

Se procedió a descargar la última versión de VirtualBox desde su sitio oficial, asegurando su compatibilidad con el sistema operativo anfitrión. VirtualBox es una plataforma de virtualización de código abierto ampliamente utilizada, que proporciona la flexibilidad necesaria para crear y gestionar múltiples máquinas virtuales en un solo equipo físico.

Descarga e Instalación de VirtualBox

Se descargó la última versión de VirtualBox desde su sitio oficial, asegurando la compatibilidad con el sistema operativo host.

Figura 1

Máquinas virtuales instaladas

Nota. elaboración propia

Configuración de Máquinas Virtuales

Se importaron las imágenes en formato OVA de Windows y Kali Linux. Estas máquinas se configuraron con la siguiente especificación de hardware: Windows: 4 GB de RAM, 2 núcleos de CPU.

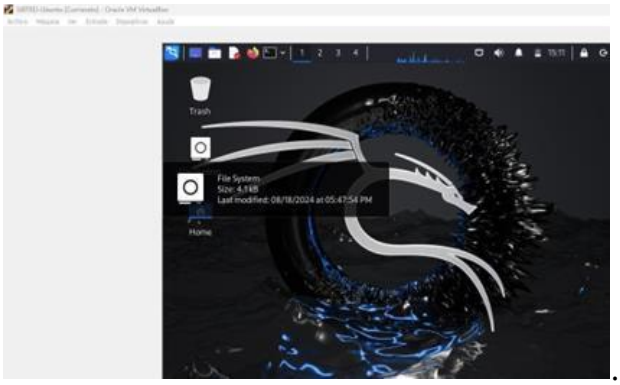
Figura 2

Maquina Virtual Windows 7

Nota. elaboración propia

Figura 3

Kali Linux: 4 GB de RAM, 2 núcleos de CPU



Nota. Maquina Kali Linux

Validación de la Comunicación

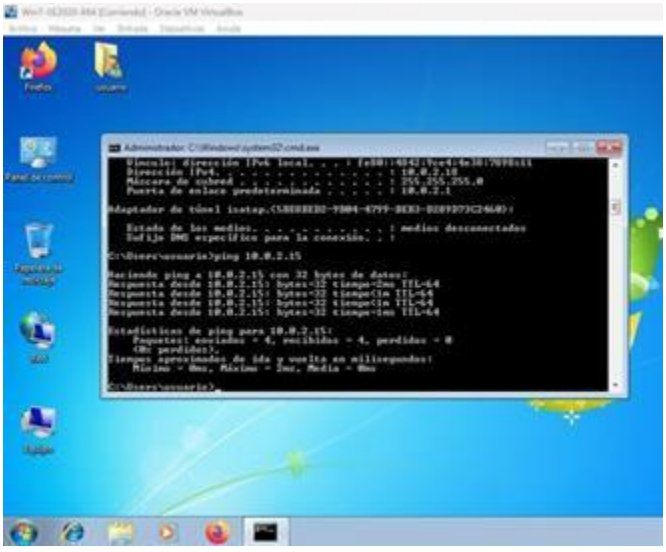
Para garantizar la efectividad del entorno virtual, se verificó la conectividad entre las máquinas utilizando el protocolo ICMP (ping). Las pruebas fueron exitosas, asegurando que ambas máquinas pudieran comunicarse entre sí para llevar a cabo ejercicios de pentesting, lo cual es crucial para simular escenarios de ataque y defensa.

Evidencias gráficas del proceso de instalación y la conectividad fueron documentadas mediante capturas de pantalla. Estas evidencias no solo respaldan la correcta configuración del entorno de trabajo, sino que también sirven como referencia para futuros ejercicios.

Evidencias: Capturas de pantalla del proceso de instalación y comunicación fueron tomadas para documentar la correcta configuración del entorno de trabajo.

Figura 4

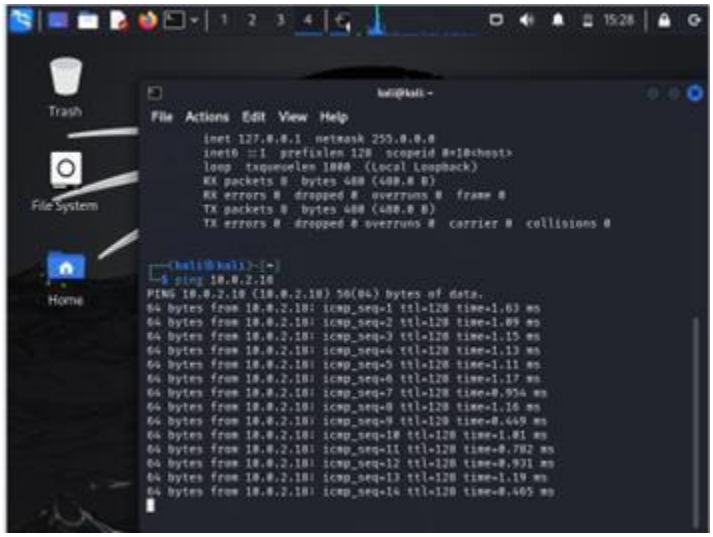
Prueba de conexión de Windows a Kali Linux. IP 10.0.2.15.



Nota. Elaboración propia

Figura 5

Prueba de conexión de Linux a Windows7 IP 10.0.2.18.



Nota. Elaboración propia

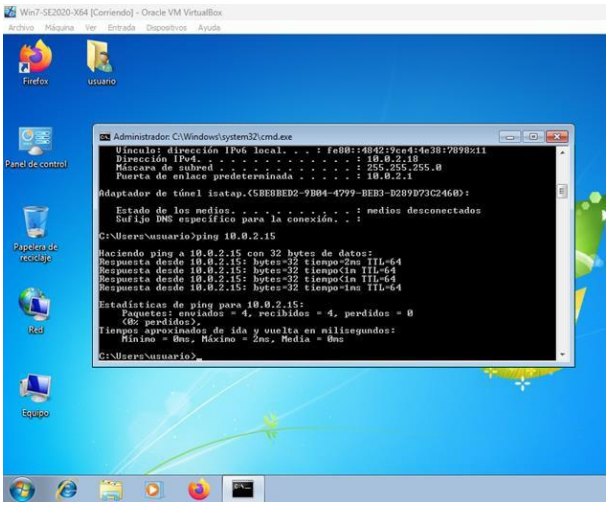
Para poder realizar la comunicación entre Kali Linux y Windows fue necesario habilitar el protocolo ICMP, como se mencionó en la conferencia web. Lo cual hizo posible poder realizar ping entre las dos máquinas como se muestra en las imágenes.

Etapas del Pentesting y Herramientas Utilizadas

El pentesting sigue cinco fases esenciales para evaluar la seguridad de un sistema mediante simulaciones de ataques controlados. La primera es reconocimiento, donde se recopila información del objetivo, como direcciones IP y puertos abiertos; aquí, Nmap resulta crucial para realizar escaneos de red y detectar servicios expuestos. La segunda fase, escaneo y enumeración, explora los puertos y servicios identificados para obtener detalles adicionales sobre posibles puntos de entrada. En la fase de explotación, se busca aprovechar las vulnerabilidades halladas para obtener acceso no autorizado, usando herramientas como Metasploit, que permite desarrollar y ejecutar exploits sobre vulnerabilidades conocidas. Una vez dentro, el pentester pasa a mantener el acceso, con el fin de garantizar la permanencia en el sistema sin ser detectado. Por último, la fase de cobertura de huellas se centra en eliminar cualquier evidencia del ataque para evitar su detección. Estos pasos estructurados permiten al equipo de seguridad identificar y corregir debilidades antes de que sean aprovechadas por actores maliciosos.

Figura 6

Prueba de conexión de Windows a Kali Linux. IP 10.0.2.15.



Nota. Elaboración propia

Red Team:

El Red Team es un equipo especializado en realizar simulaciones de ataques cibernéticos diseñados para evaluar la seguridad de una organización desde la perspectiva de un atacante. Su objetivo es identificar vulnerabilidades en los sistemas, redes y aplicaciones mediante técnicas avanzadas como la explotación de fallos, la ingeniería social y la escalación de privilegios. A diferencia de un atacante malintencionado, el Red Team trabaja en un entorno controlado y bajo autorización, buscando mejorar la postura de seguridad organizacional a través de sus hallazgos.

Situación Problema: Análisis Red Team

De acuerdo con el problema planteado en el desarrollo del seminario se nos expone la siguiente situación: “La primera misión del equipo Red Team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación vulnerable bajo un Windows; esta aplicación al parecer tiene asociado un exploit que puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque. Dentro de la indagación, también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos”.

Solución Interrogante Uno:

Escaneo y Reconocimiento.

Para iniciar el análisis de seguridad, se llevó a cabo un escaneo de red utilizando Nmap, una herramienta esencial en esta fase del pentesting. Este escaneo permitió identificar los puertos abiertos y los servicios activos en la máquina objetivo, revelando posibles puntos de entrada para el ataque en proceso. La información recopilada incluyó direcciones IP activas, puertos en escucha y versiones de los servicios, lo cual proporciona un mapa detallado de la infraestructura de red del sistema comprometido. Este paso es importante para comprender la superficie de ataque y definir el enfoque de las siguientes fases del pentesting.

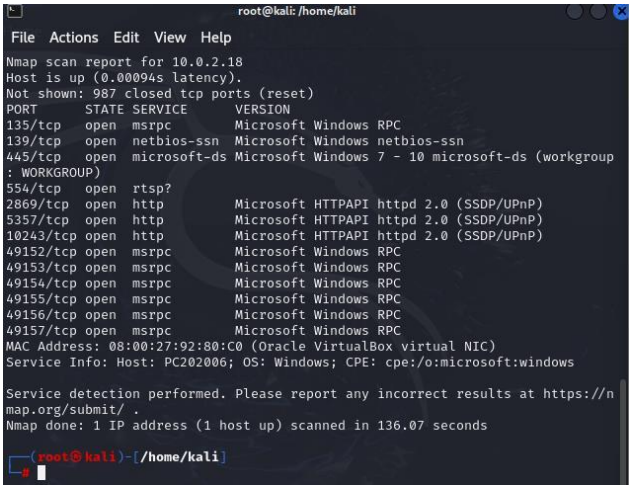
Nmap:

Se usa para escanear puertos y servicios abiertos en la máquina Windows 7. Comenzamos con un escaneo básico y luego avanzar a un escaneo de versiones detallado:

Ejecutando el comando: nmap -sS -sV 10.0.2.18.

Figura 7

Nmap -sS -sV 10.0.2.18

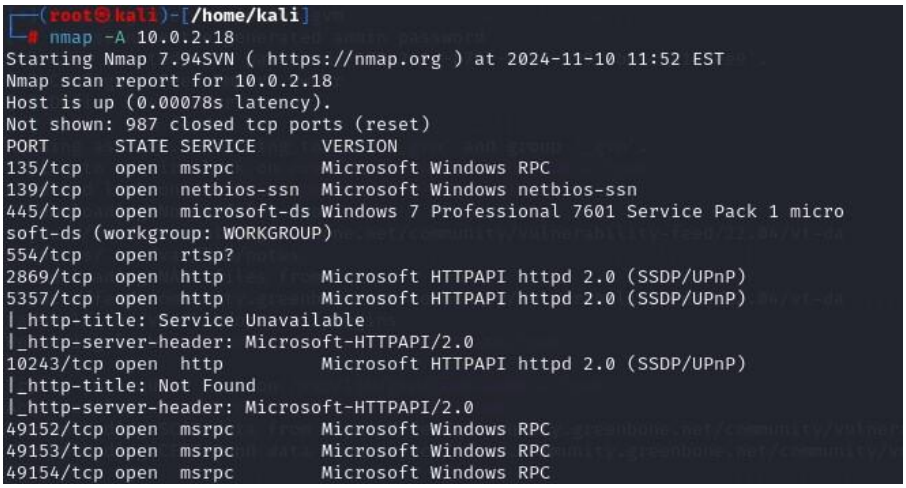


Nota. Elaboración propia

Nmap -A: para realizar un escaneo avanzado que proporciona un análisis detallado de la máquina objetivo. Con -A, Nmap ejecuta varias técnicas de detección de manera combinada para obtener la mayor cantidad de información posible.

Figura 8

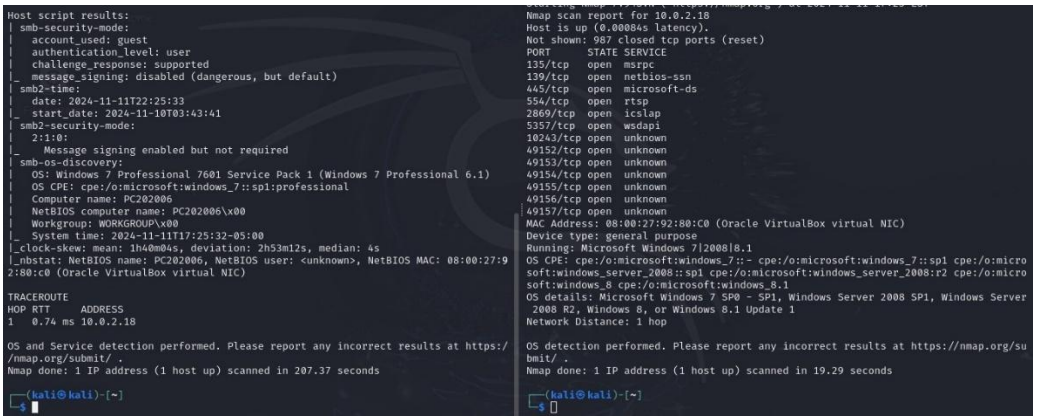
Nmap - A para escaneo avanzado



Nota. Elaboración propia

Figura 9

Identificación de sistema operativo y puertos abiertos.



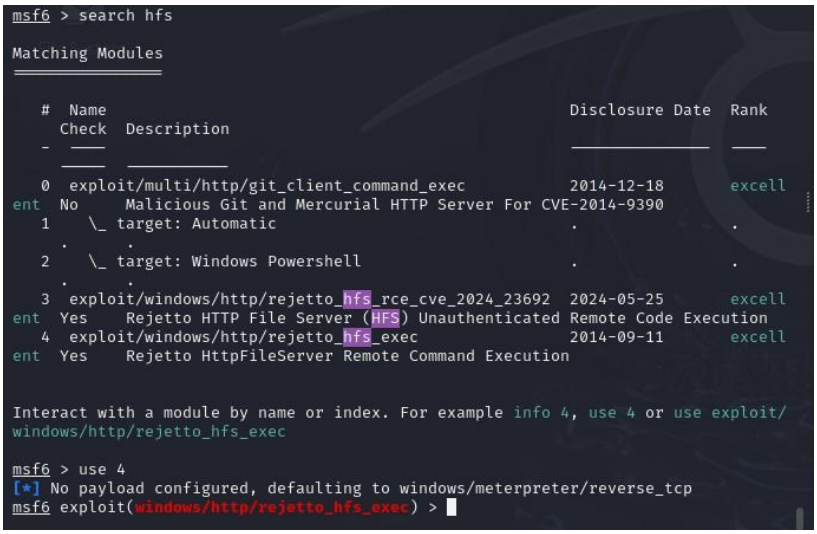
Nota. Elaboración propia

Identificación de Vulnerabilidad

Tras el escaneo inicial con Nmap, se observó que la máquina objetivo tenía instalado Rejetto HTTP File Server (HFS), un software conocido por tener vulnerabilidades que permiten la ejecución de código remoto en ciertas versiones. Esta aplicación expone un puerto accesible externamente, lo que facilita su identificación y análisis. Identificamos el ítem 3 y 4 vamos a trabajar con el 4 con el comando use 4, como se ve en la imagen:

Figura 10

Identificación de Rejjeto

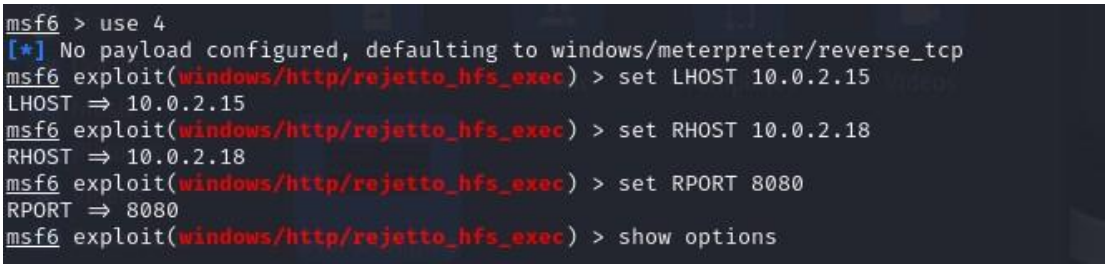


Nota. Elaboración propia

Para explotar la vulnerabilidad en Rejetto HFS y lograr una conexión remota con la máquina objetivo, configuramos el payload, RHOST (Remote Host), y RPORT (Remote Port) en Metasploit

Figura 11

Pasos de configuración de metasploit

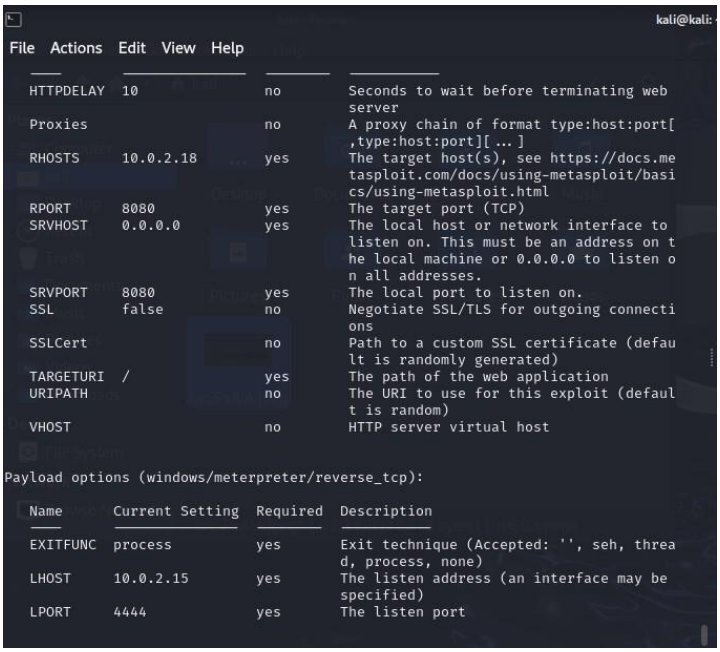


Nota. Elaboración propia

Con el comando show options, verificamos que los parámetros del exploit estaban configurados correctamente. Esto incluyó la revisión del payload, RHOST, y RPORT, asegurando que la configuración fuese precisa antes de ejecutar el exploit.

Figura 12

Exploit



Nota. Elaboración propia

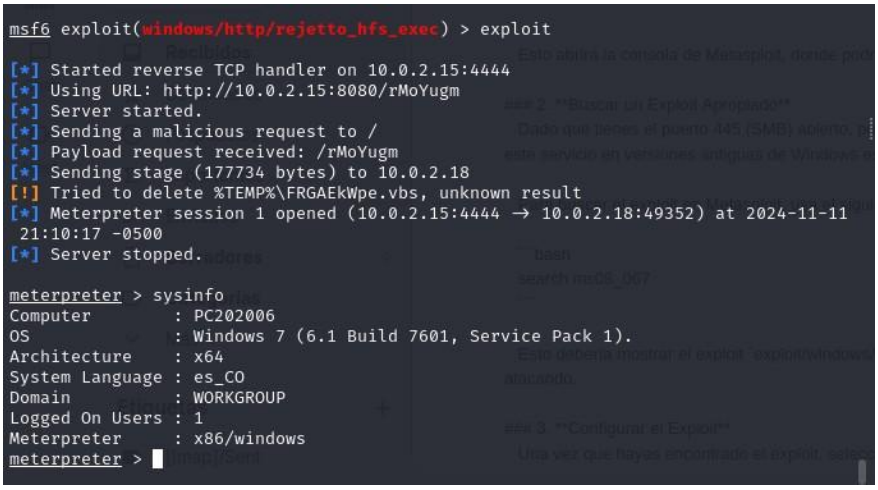
Una vez configurados estos parámetros, se ejecutó el comando exploit, iniciando el ataque y logrando una sesión remota en la máquina objetivo mediante una sesión de Meterpreter.

Acceso logrado.

Con la ejecución exitosa del exploit, se logró establecer una sesión remota en la máquina objetivo mediante Meterpreter. A partir de este acceso, se verificó la presencia y permisos del usuario activo en el sistema comprometido, así como el entorno en el que se encontraba. Esta conexión permitió interactuar directamente con el sistema Windows afectado, proporcionando control sobre sus recursos y permitiendo realizar diversas acciones de recolección de información, como capturas de pantalla del escritorio, y enumeración de procesos activos. Además, este acceso habilitó la posibilidad de ejecutar comandos de sistema para explorar posibles rutas de escalación de privilegios y consolidar la persistencia en el sistema. Esta etapa fue fundamental para demostrar el impacto del exploit en el entorno comprometido y la gravedad de la vulnerabilidad que permitió el acceso inicial.

Figura 13

Acceso a máquina por exploit y sysinfo



Nota. Elaboración propia

En la sesión de Meterpreter después de explotar una vulnerabilidad en una máquina Windows 7 (Build 7601, Service Pack 1). Los siguientes comandos han sido ejecutados:

Sysinfo: Este comando muestra información del sistema comprometido. En este caso:

Nombre del equipo: PC202006

Sistema operativo: Windows 7 (versión 6.1, Service Pack 1) Arquitectura: x64

Idioma del sistema: español (Colombia) Dominio: WORKGROUP getuid: Este comando muestra el usuario con el que se tiene acceso en el sistema comprometido. Aquí, el usuario es NT AUTHORITY\SYSTEM, lo que indica que la sesión se ejecuta con permisos de nivel sistema (máximo privilegio en un entorno Windows).

getprivs: Este comando enumera los privilegios habilitados en el proceso actual. Algunos privilegios importantes habilitados son:

SeAssignPrimaryTokenPrivilege

SeAuditPrivilege

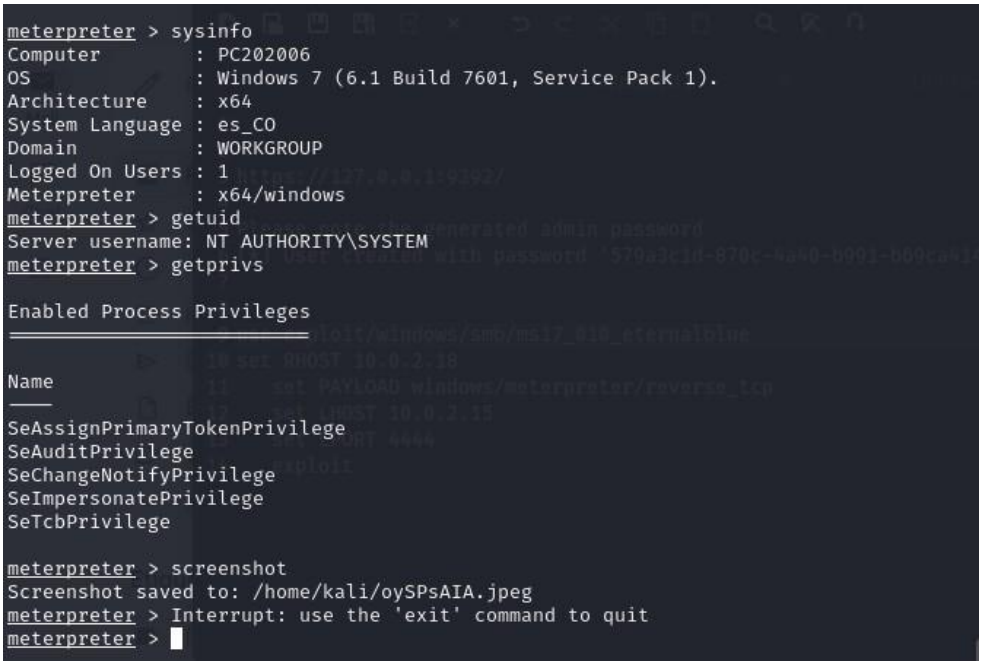
SeChangeNotifyPrivilege

SeImpersonatePrivilege

SeTcbPrivilege

Figura 14

Validando Acceso y Privilegios



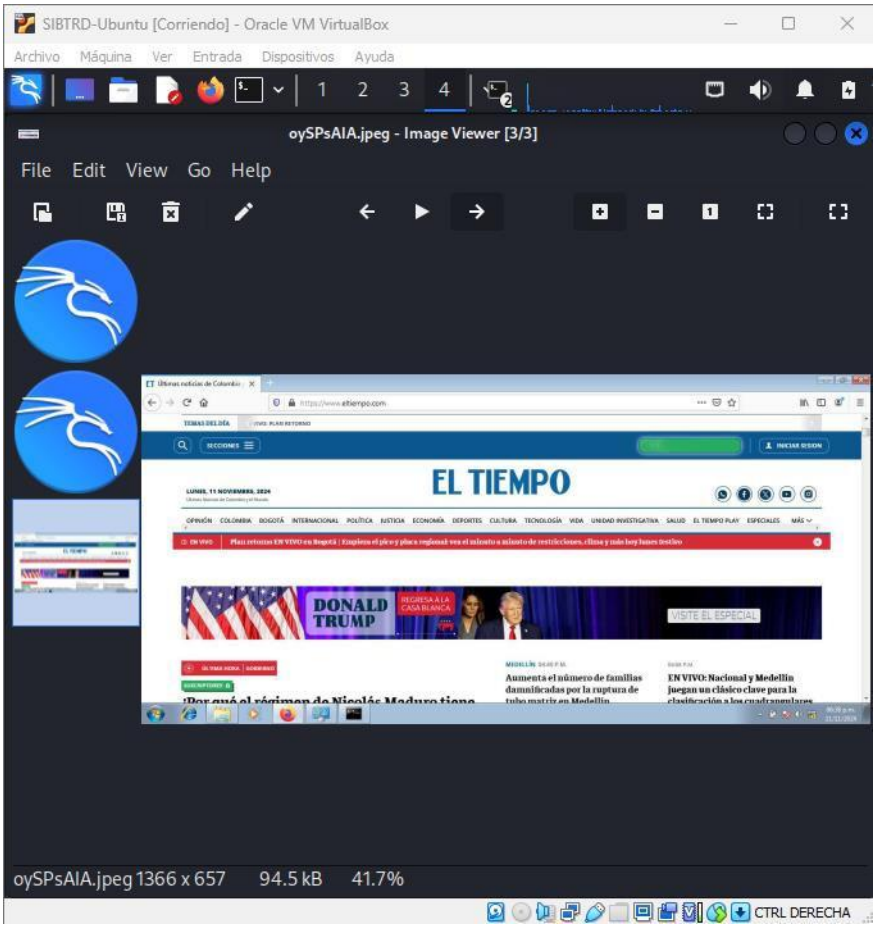
Nota. Elaboración propia

Estos privilegios indican que la sesión tiene permisos avanzados en el sistema, lo cual podría ser aprovechado para realizar acciones críticas.

Screenshot: El comando toma una captura de pantalla del escritorio del sistema comprometido. La captura ha sido guardada en el sistema atacante en el archivo */home/Kali/oySPsAlA.jpeg.*

Figura 15

Se Hace un Screenshot



Nota. Elaboración propia

Creando Usuario

Para demostrar el acceso y la posibilidad de escalación de privilegios, se procedea crear un usuario administrador en el sistema comprometido usando la sesión de Meterpreter. Los pasos son los siguientes:

Accede a la Consola de Comandos de Windows desde Meterpreter: Una vez en la sesión meterpreter, abre una consola de comandos de Windows escribiendo: Shell

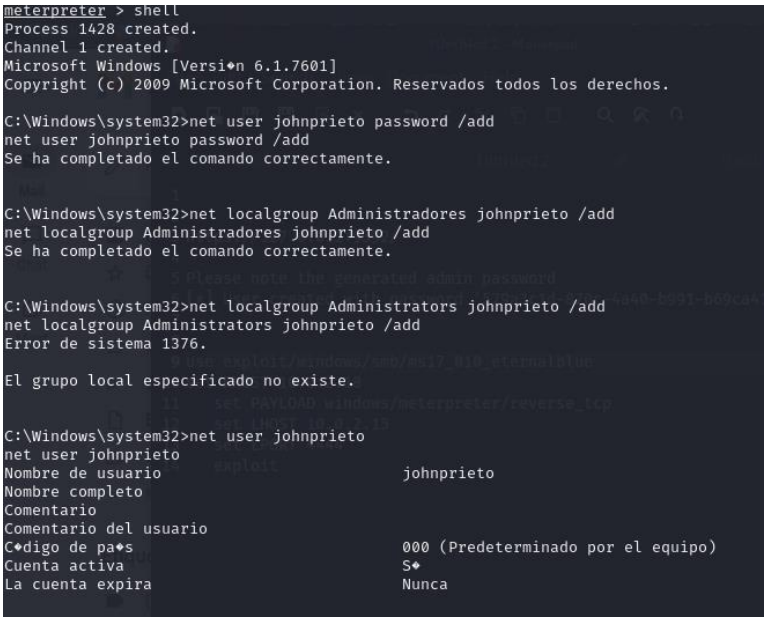
Crear el Usuario con Privilegios Administrativos: Dentro de la consola de comandos de Windows, se ejecutan los siguientes comandos:

Crea un usuario: johnprieto con el comando net user johnprieto password /add

Agrega el usuario al grupo de administradores con el comando :net localgroup Administradores nombre_*usuario /add*

Figura 16

Creación de usuario y permisos de administrador

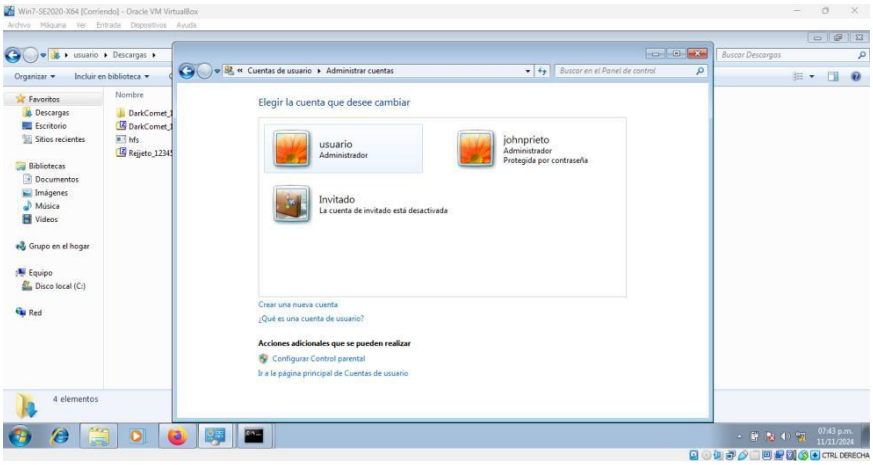


Nota. Elaboración propia

Por último, se deja evidencia de listado de usuarios del equipo Windows 7 que fue objeto del ataque:

Figura 17

Usuarios en Equipo Atacado



Nota. Elaboración propia

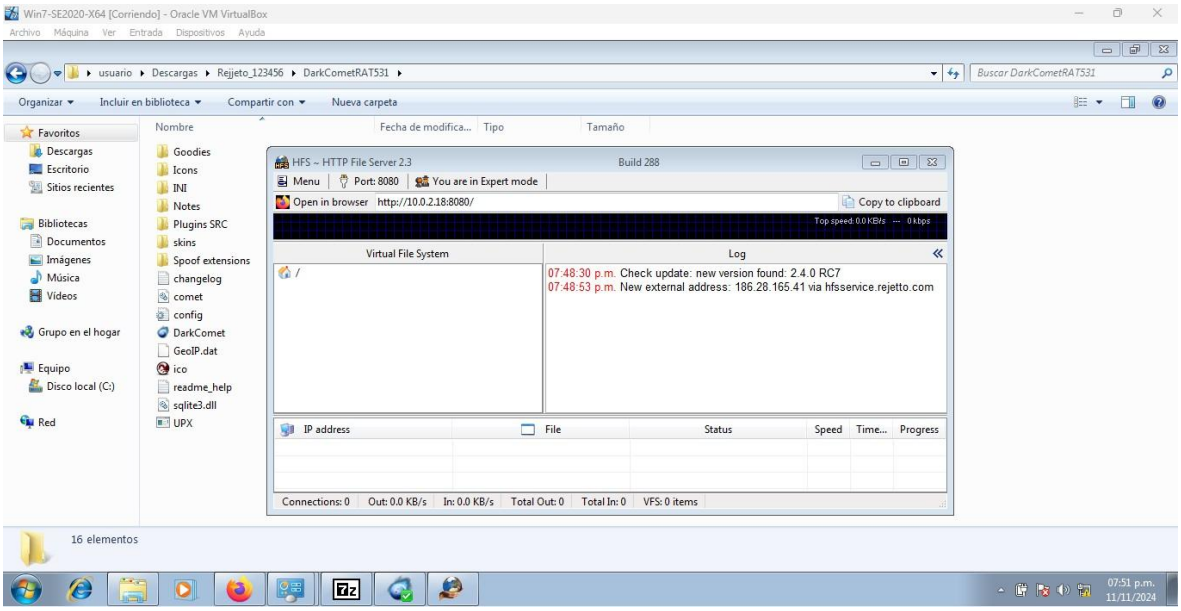
Figura 18

Evidencia de creación de usuario con privilegios de administrador

Nota. Elaboración propia

Figura 19

Evidencia de Software Vulnerable en Máquina



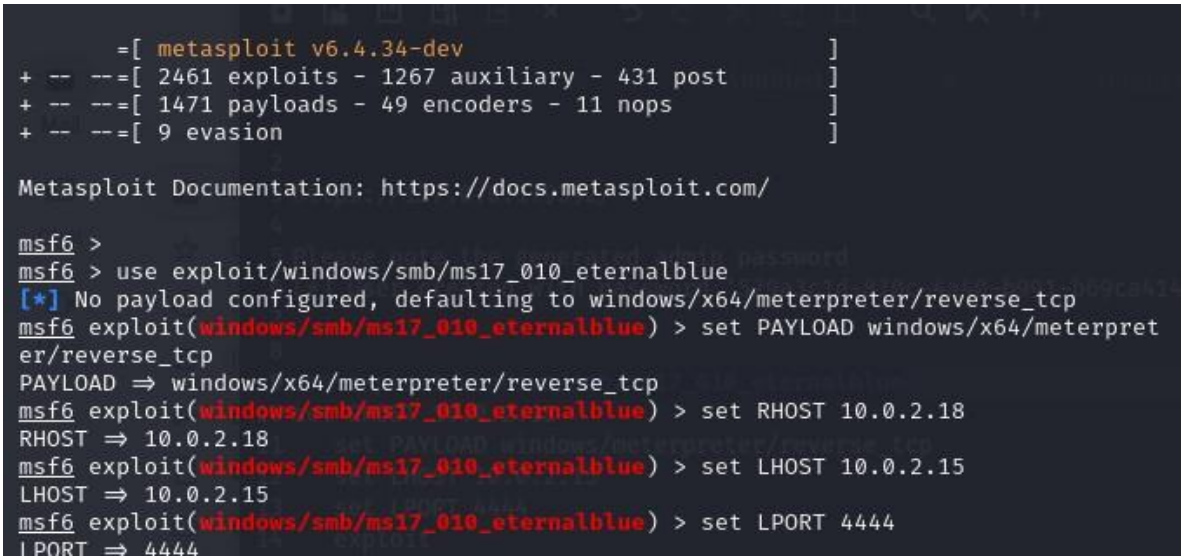
Nota. Elaboración propia

Ejercicio con Eternalblue

Como ejercicio adicional, también se realizó el proceso de explotación utilizando la vulnerabilidad EternalBlue (MS17-010), una vulnerabilidad crítica en el protocolo SMB de Windows que permite la ejecución remota de código. Al ejecutar el exploit eternalblue en Metasploit, se logró obtener acceso mediante una sesión de Meterpreter con privilegios elevados en la máquina objetivo. Este enfoque alternativo permitió validar la presencia de configuraciones inseguras en el sistema y evidenciar cómo distintas vulnerabilidades pueden llevar al mismo resultado de acceso remoto y escalación de privilegios, lo cual resalta la importancia de aplicar parches de seguridad en sistemas vulnerables.

Figura 20

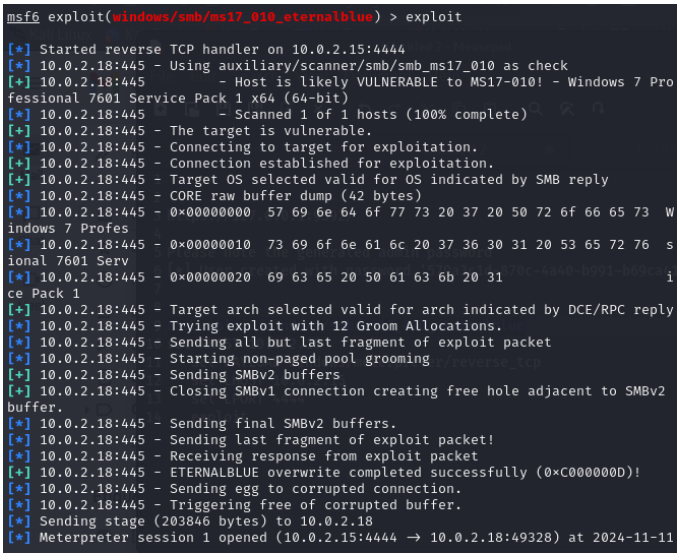
Eternalblue



Nota. Elaboración propia

Figura 21

Ataque Exitoso con Eternalblue



Nota. Elaboración propia

Solución Interrogante Dos

A continuación, se listan y describen los datos e información del Anexo 4 – Escenario 3 que ayudaron a identificar el fallo de seguridad específico en la máquina Windows:[9]

Información sobre una aplicación vulnerable instalada en la máquina objetivo: Se menciona que en el equipo de la organización se encuentra instalada una aplicación vulnerable que corre sobre Windows. Este dato fue clave para orientar el análisis hacia la identificación de vulnerabilidades en aplicaciones conocidas por ser explotables en sistemas Windows, como el Rejetto HTTP File Server o vulnerabilidades de SMB como EternalBlue (MS17-010).

Posible existencia de un exploit asociado: Se indica que esta aplicación vulnerable podría estar asociada a un exploit que permite acceso a través de una shell, escalación de privilegios, u otros tipos de ataques. Esta información orientó el uso de exploits específicos en el entorno de Metasploit, como rejetto_hfs_exec para el Rejetto HTTP File Server y ms17_010_eternalblue para vulnerabilidades en SMB, con el objetivo de acceder a la máquina objetivo y verificar si era posible obtener una sesión remota.

Escalación de privilegios mediante la creación de un usuario administrador: El escenario describe un posible escalamiento de privilegios mediante la creación de un usuario con permisos de administrador. Esto dio la pauta para realizar pruebas de escalación de privilegios una vez obtenida la sesión en el sistema comprometido, validando la posibilidad de crear un usuario con privilegios administrativos y demostrando así la explotación efectiva del sistema.

Entregable del equipo de forense: copia del servidor: Se indica que el equipo de forense entregó una copia del servidor comprometido. Esto fue básico para analizar el sistema en un

---

[9] **Universidad Nacional Abierta y a Distancia (UNAD). (s.f.).** *Anexo 4 - Escenario 3*. UNAD. https://campus118.unad.edu.co/ecbti144/pluginfile.php/6398/mod_folder/content/0/Anexo%204%20-%20Escenario%203.pdf?forcedownload=1

entorno controlado y realizar pruebas de explotación y post-explotación sin afectar directamente el sistema en producción, permitiendo explorar el alcance de la vulnerabilidad de manera segura y completa.

Solución Interrogante Tres

La herramienta utilizada para identificar fallos de seguridad en la máquina Windows como ya lo hemos evidenciado a lo largo del trabajo fue Nmap en la fase de reconocimiento. Nmap se utilizó para realizar escaneos de red, detectando puertos abiertos y servicios en ejecución, y Metasploit fue empleado en la fase de explotación para ejecutar exploits específicos. El puerto abierto que expone la vulnerabilidad está asociado a la aplicación Rejetto HTTP File Server (HFS), en el puerto comúnmente configurado (8080), lo cual permitió identificar el fallo de seguridad mediante exploits conocidos

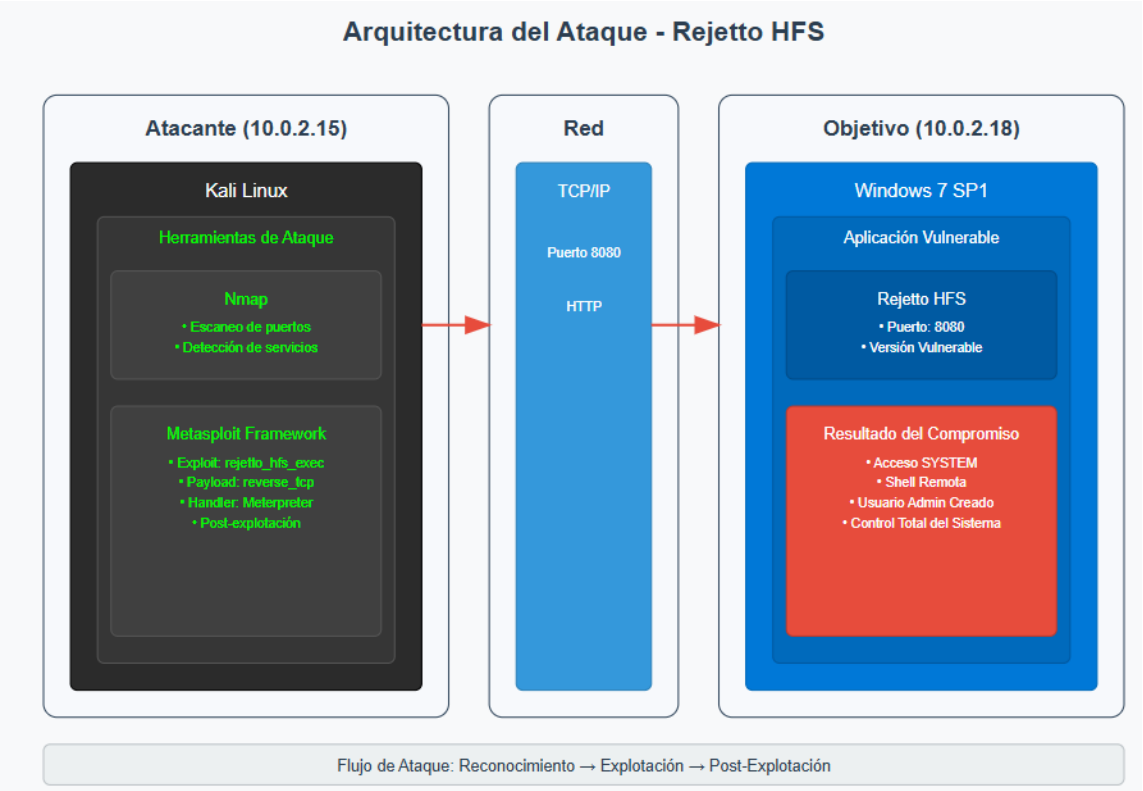
Solución Interrogante Cuatro

Explicación del Ataque y su Impacto en la Máquina Windows

El ataque afecta la máquina Windows permitiendo acceso remoto y escalación de privilegios. Una vez identificado el servicio vulnerable (Rejetto HFS), Metasploit ejecuta un exploit que inicia una sesión remota con Meterpreter, proporcionando control total sobre el sistema. El impacto del ataque incluye la creación de usuarios con privilegios administrativos y manipulación del sistema. Esto es se muestra a continuación en el flujo gráfico del ataque, donde se destacan las fases de escaneo, explotación, y post-explotación mediante la escalación de privilegios y creación de usuarios, entre otras acciones.

Figura 22

Flujo Gráfico del Ataque.



Nota. Elaboración propia

Blue Team

El Blue Team es el equipo encargado de defender la infraestructura de una organización contra ataques cibernéticos. Su enfoque principal es prevenir, detectar y mitigar las amenazas mediante la implementación de medidas de seguridad proactivas y reactivas. El Blue Team utiliza herramientas como firewalls, sistemas de detección de intrusos (IDS), sistemas de gestión de información y eventos de seguridad (SIEM), y realiza auditorías constantes para identificar posibles brechas de seguridad. Además, este equipo es responsable de desarrollar estrategias de respuesta ante incidentes para contener y remediar ataques en tiempo real.

Solución Item 1

"¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos."

Lo primero que el Blue Team indagaría al detectar un ataque en tiempo real sería identificar la naturaleza del ataque y su alcance, evaluando tanto el sistema operativo comprometido como la red afectada. Esto permitiría priorizar las acciones necesarias para contener la amenaza. A continuación, detallo los pasos clave con argumentos técnicos:

Identificación del Tipo de Ataque

Análisis del tráfico de red: Utilizar una herramienta como Wireshark para capturar y analizar paquetes en tiempo real, buscando patrones sospechosos como conexiones a servidores remotos no autorizados, tráfico inusual en puertos específicos o intentos de escaneo de red. Esta acción permite identificar posibles vectores de ataque, como exfiltración de datos o intentos de conexión por parte de un comando y control (C2).

Revisión de Logs del Sistema

Acceder al Visor de Eventos de Windows para revisar los registros relacionados con

inicios de sesión fallidos, cambios de configuración del sistema o servicios que hayan sido iniciados sin autorización. Los logs de eventos pueden revelar intentos de escalación de privilegios o actividad anómala que indique la explotación de vulnerabilidades.

Contención Inmediata del Ataque

Aislamiento del sistema afectado: Desconectar la máquina de la red para evitar la propagación del ataque o la pérdida de más datos. Esto se puede realizar físicamente (desconexión del cable de red) o mediante una política de aislamiento en el firewall. Limitar la conectividad reduce significativamente el impacto del ataque y permite analizar el sistema de forma controlada.

Detección de Procesos Maliciosos

Usar Task Manager, PowerShell (Get-Process) o herramientas como Process Explorer para identificar procesos anómalos ejecutándose en la máquina comprometida. Una vez detectados, detenerlos (Stop- Process) para interrumpir la actividad maliciosa. Los procesos no autorizados suelen ser el resultado de exploits o malware ejecutándose en el sistema. Detenerlos corta la ejecución del ataque.

Evaluación del Alcance y Recuperación

Escaneo del sistema: Emplear herramientas antivirus o antimalware open-source como ClamAV para detectar archivos maliciosos y eliminarlos. Esto permite identificar componentes persistentes del ataque y ayuda en la remediación del sistema afectado.

Recolección de evidencias: Documentar toda la actividad detectada, incluyendo capturas de paquetes, logs de eventos y listas de procesos. Esto es fundamental para realizar un análisis forense posterior y entender cómo se produjo el ataque. Esta información es muy importante para mejorar las defensas del sistema y mitigar futuros ataques.

Solución Item 2

"¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team, qué medidas de hardenización propondría para que el ataque no se repita?"

A continuación, se presentan medidas de hardenización que buscan reducir la superficie de ataque y mejorar la seguridad del sistema. Implementarlas no solo previene ataques similares al del laboratorio práctico, sino que también fortalece el sistema frente a otras amenazas conocidas, minimizando riesgos futuros10.

Medidas de hardenización para prevenir ataques similares: Basándonos en el ataque ejecutado en el laboratorio práctico del ejercicio de Red Team, donde se explotaron vulnerabilidades en la máquina Windows mediante el uso de herramientas como Metasploit y el servicio vulnerable Rejetto HTTP File Server (HFS), se pueden proponer las siguientes medidas de hardenización para mitigar riesgos futuros y evitar que se repitan incidentes similares:

Eliminación de Software Vulnerable

Acción: Inicialmente se debe desinstalar el software Rejetto HTTP File Server (HFS) u otros servicios innecesarios en el sistema.

Ejemplo:

Identificar servicios activos mediante Get-Service en PowerShell.

Desinstalar el software desde el Panel de Control o mediante un comando en PowerShell:

Get-WmiObject Win32_Product | Where-Object {$_.Name - match "HFS"} | ForEach-Object { $_.Uninstall() }

[10] Tarlogic. (s.f.). *¿Qué metodologías se emplean habitualmente en ejercicios de Red Team?*. Tarlogic. https://www.tarlogic.com/es/blog/metodologias-red-team/

Impacto: Esto elimina el principal vector de ataque utilizado en el escenario, dificultando la explotación de vulnerabilidades conocidas.

Configuración del Firewall de Windows

Acción: Bloquear puertos innecesarios, como el puerto 8080 usado por Rejetto HFS, y permitir solo los estrictamente necesarios para las operaciones.

Ejemplo:

Configurar reglas en el Firewall de Windows para bloquear el puerto 8080: *New-NetFirewallRule -DisplayName "Block HFS Port" -Direction Inbound -LocalPort 8080 -Protocol TCP -Action Block*

Impacto: Esto previene el acceso no autorizado desde redes externas a servicios que podrían ser explotados.

Aplicación de actualizaciones y parches.

Acción: Actualizar el sistema operativo y todas las aplicaciones instaladas para asegurar que no existan vulnerabilidades conocidas.

Habilitar las actualizaciones automáticas en Windows o aplicar manualmente parches de seguridad críticos mediante Windows Update.

Para aplicaciones específicas, monitorear bases de datos como CVE para identificar vulnerabilidades y su respectivo parche.

Impacto: Las actualizaciones reducen la superficie de ataque al mitigar exploits disponibles públicamente.

Configuración de Políticas de Seguridad

Acción: Implementar políticas de contraseñas seguras y restringir los permisos de usuarios.

Ejemplo:

Configurar políticas de contraseñas en el Editor de Políticas de Grupo:

Longitud mínima: 12 caracteres.

Complejidad habilitada: incluir letras mayúsculas, minúsculas, números y símbolos.

Crear roles específicos para los usuarios y evitar el uso innecesario de cuentas con privilegios administrativos: net localgroup Administradores

/delete [usuario_innecesario]

Impacto: Esto dificulta los intentos de escalación de privilegios.

Auditoría y monitoreo continuo.

Acción: Activar auditorías para detectar cambios sospechosos en el sistema y monitorear los eventos de seguridad.

Ejemplo:

Habilitar auditorías en el Editor de Políticas de Grupo:

Configurar "Auditar inicio de sesión exitoso/fallido".

Supervisar accesos no autorizados al sistema mediante el Visor de Eventos de Windows.

Complementar con herramientas como OSSEC9 para monitoreo de integridad de archivos y alertas en tiempo real.

Impacto: La auditoría constante permite detectar y responder rápidamente a actividades anómalas.

Aplicación de CIS Benchmarks

Acción: Implementar las configuraciones recomendadas por el Center for Internet

Security (CIS) [11]para fortalecer la seguridad del sistema operativo.

Ejemplo:

Habilitar configuraciones avanzadas como la desactivación de SMBv1 para prevenir vulnerabilidades como EternalBlue: Set-SmbServerConfiguration -

EnableSMB1Protocol $false

Deshabilitar servicios innecesarios usando la guía de CIS como referencia:

Servicios relacionados con la red:

Telnet - Protocolo inseguro para conexiones remotas.[12]

Remote Registry - Permite modificaciones remotas del registro de Windows.

Routing and Remote Access - Habilita enrutamiento y acceso remoto (VPN). [13]

SSDP Discovery - Permite detectar dispositivos en red que usan UPnP.

Windows Media Player Network Sharing Service - Comparte contenido multimedia en la red.

Servicios relacionados con el sistema:

Windows Error Reporting - Envía informes de errores a Microsoft.

Distributed Link Tracking Client - Rastrea enlaces distribuidos en red.

IP Helper - Proporciona soporte para IPv6.

Tablet PC Input Service - Habilita soporte para dispositivos táctiles o tabletas.

Offline Files - Permite trabajar con archivos fuera de línea en una red.

---

[11] Center for Internet Security (CIS). (2025). *CIS Benchmarks List*. CIS Security. https://www.cisecurity.org/cis-benchmarks
[12] RedesZone. (s.f.). *Protocolo de red Telnet*. RedesZone. https://www.redeszone.net/tutoriales/internet/protocolo-red-telnet/
[13] Microsoft. (s.f.). Disabling terminal services features. Microsoft Learn. https://learn.microsoft.com/es-es/windows/win32/termserv/disabling-terminal-services-features

Impacto: Las configuraciones recomendadas reducen significativamente la probabilidad de explotación de configuraciones inseguras.

Solución Item 3.

"¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?"

Un Blue Team es el grupo especializado en implementar y mantener defensas proactivas dentro de la infraestructura tecnológica de una organización. Este equipo trabaja continuamente en la identificación y mitigación de vulnerabilidades, aplicando controles técnicos como políticas de acceso, configuraciones seguras en sistemas y herramientas de monitoreo avanzado, tales como SIEM (Security Information and Event Management). Su enfoque es proteger los activos críticos y reducir la superficie de ataque, utilizando análisis de logs, auditorías de seguridad y la implementación de medidas de hardenización para prevenir compromisos de seguridad.

Por otro lado, un equipo de respuesta a incidentes informáticos actúa de manera reactiva ante incidentes detectados. Su objetivo es contener y mitigar las amenazas en curso, restaurar la funcionalidad de los sistemas comprometidos y analizar los indicadores de compromiso (IoC) para identificar el alcance del ataque. Este equipo emplea técnicas avanzadas de análisis forense, herramientas de contención (como firewalls y scripts automatizados), y metodologías basadas en estándares como NIST SP 800-61 para la gestión de incidentes. [14]

La siguiente tabla compara las funciones y características de los equipos Blue Team y de respuesta a incidentes, destacando sus diferencias principales:

---

[14] OpenWebinars. (2024). *Ciberseguridad proactiva: La importancia del Blue Team*. OpenWebinars. https://openwebinars.net/blog/ciberseguridad-proactiva-la-importancia-del-blue-team/

Tabla 1

Comparación entre Blue Team y Respuesta a Incidentes

Aspecto	Blue Team	Respuesta a Incidentes
Objetivo	Prevenir ataques y fortalecer la postura de seguridad.	Contener, mitigar y analizar el impacto de un incidente.
Funciones	- Implementación de medidas de hardening. - Análisis de logs para detectar actividades sospechosas.	- Recuperación de sistemas afectados. - Recolección de evidencias para análisis forense.
Herramientas comunes	SIEM, firewalls, IDS/IPS, análisis de logs.	Análisis forense, herramientas de contención y logs específicos.
Perspectiva de tiempo	Proactiva (antes de que ocurra un incidente).	Reactiva (tras detectar un incidente).

Nota. Elaboración propia

El Blue Team y el equipo de respuesta a incidentes son complementarios y esenciales dentro de un enfoque integral de ciberseguridad. Mientras el Blue Team trabaja para fortalecer las defensas y reducir vulnerabilidades, el equipo de respuesta utiliza datos y configuraciones previas del Blue Team para contener amenazas activas y limitar su impacto. Además, los análisis forenses realizados por el equipo de respuesta generan aprendizajes que retroalimentan las estrategias preventivas del Blue Team, fortaleciendo el ciclo de mejora continua en la seguridad organizacional.

Solución Item 4

Para dar solución a la pregunta 4 de la actividad, donde se indaga sí dentro de un equipo Blue Team me indican trabajar con el CIS (Center for Internet Security), lo utilizaría como una guía práctica para fortalecer la seguridad de los sistemas e infraestructuras de TI. Los recursos del CIS son especialmente útiles para implementar configuraciones de seguridad estandarizadas y basadas en mejores prácticas globales. Específicamente, los utilizaría para los siguientes fines:

Aplicación de Benchmarks de Seguridad

Implementar las recomendaciones de los CIS Benchmarks en sistemas operativos, aplicaciones, bases de datos y redes. Estas guías proporcionan configuraciones seguras predeterminadas que ayudan a reducir vulnerabilidades comunes y mejorar la postura de seguridad de los activos críticos.

Monitoreo y Evaluación de Seguridad

Usar herramientas como CIS-CAT (CIS Configuration Assessment Tool) para evaluar si los sistemas cumplen con los estándares de configuración seguros establecidos por el CIS. Esto permite identificar desviaciones y remediarlas rápidamente.

Fortalecimiento de Políticas de Seguridad

Desarrollar e implementar políticas basadas en las recomendaciones del CIS Controls, que incluyen un conjunto de controles fundamentales que priorizan las acciones necesarias para defenderse de amenazas cibernéticas comunes.

Mitigación de Riesgos

Utilizar las guías del CIS para identificar y corregir configuraciones inseguras en puntos finales, servidores y dispositivos de red. Esto ayuda a reducir la superficie de ataque y dificulta la explotación de sistemas vulnerables.

Cumplimiento Normativo

Regulaciones y estándares, como ISO 27001, PCI DSS y NIST, reconocen los recursos del CIS como referencia. Trabajar con el CIS facilita alinear las prácticas de seguridad con estos marcos normativos, mejorando el cumplimiento. Estos son los beneficios del CIS en el cumplimiento normativo.

Estandarización: Facilita la adopción de configuraciones seguras y reconocidas a nivel global.

Ahorro de tiempo y recursos: Ofrece guías prácticas que simplifican la implementación de controles técnicos requeridos por las normativas.

Auditorías más ágiles: La alineación con CIS reduce el esfuerzo en demostrar cumplimiento, ya que sus recomendaciones están ampliamente aceptadas por auditores y reguladores.

Solución Item 5

Un SIEM (Security Information and Event Management) es una herramienta fundamental para proteger la infraestructura de TI de una empresa. Su capacidad para centralizar datos, detectar amenazas en tiempo real y automatizar respuestas permite a las organizaciones garantizar la continuidad del negocio y minimizar el impacto de los ataques cibernéticos. Al combinar análisis avanzado, monitoreo constante y documentación exhaustiva, un SIEM se convierte en un pilar fundamental en cualquier estrategia de ciberseguridad.[15]

Funciones y Características Principales de un SIEM

Un SIEM es una solución tecnológica que combina la gestión de información de

---

[15] **Ambit BST. (2021).** *¿Qué significa SIEM y cómo funciona?*. Ambit BST. https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

seguridad (SIM) y la gestión de eventos de seguridad (SEM) para proporcionar a las empresas una defensa integral contra amenazas cibernéticas. Este sistema permite la detección, monitoreo y respuesta rápida ante incidentes de seguridad, fortaleciendo la postura de ciberseguridad organizacional.

Funciones Principales de un SIEM

Recopilación y centralización de datos:

Reúne y almacena registros (logs) de diferentes fuentes, como dispositivos de red, sistemas operativos, aplicaciones y bases de datos, en una ubicación centralizada.

Permite realizar un análisis profundo para identificar tendencias y patrones de comportamiento anómalos.

Detección de amenazas en tiempo real:

Utiliza reglas predefinidas y algoritmos avanzados para identificar comportamientos sospechosos, como intentos de acceso no autorizados o transferencias de datos inusuales.

Facilita la identificación de amenazas reales frente a falsos positivos, optimizando los recursos de seguridad.

Generación de alertas y automatización de respuestas:

Emite notificaciones inmediatas sobre incidentes detectados para que el personal de seguridad pueda actuar con rapidez.

Automatiza procesos de respuesta, como el bloqueo de IPs sospechosas o la detención de procesos maliciosos.

Monitoreo centralizado:

Supervisa de forma continua todos los activos de la red, proporcionando una vista integral de las actividades en la infraestructura de TI.

Cumplimiento normativo:

Documenta los eventos y proporciona reportes detallados que ayudan a cumplir con regulaciones como ISO 27001, PCI DSS y GDPR, facilitando auditorías y demostrando conformidad.

Creación de una base de conocimiento:

Registra y documenta todos los incidentes y las acciones tomadas, creando un repositorio que permite una resolución más eficiente de problemas futuros y una mejora continua de las defensas.

Para comprender la importancia de los sistemas de monitoreo y respuesta en ciberseguridad, es fundamental analizar las características clave que los hacen eficientes y adaptables a diferentes entornos empresariales. La siguiente tabla resume los principales beneficios y funcionalidades que ofrecen estos sistemas, destacando su capacidad para detectar, correlacionar y responder a amenazas en tiempo real, además de optimizar los recursos mediante la automatización y la escalabilidad.

Tabla 2

Características Principales de un SIEM

Característica	Descripción
Análisis en tiempo real	Permite la detección inmediata de incidentes mediante la supervisión constante de eventos generados en la infraestructura.

Correlación de eventos	Integra datos de múltiples fuentes para identificar patrones complejos de ataque que no serían evidentes al analizar eventos de manera aislada.
Automatización de procesos	Escanea redes, genera alertas y ejecuta respuestas sin intervención manual, optimizando los recursos humanos y reduciendo el tiempo de respuesta.
Visualización interactiva	Ofrece paneles de control (dashboards) intuitivos que permiten monitorear métricas críticas y detectar problemas rápidamente.
Escalabilidad	Diseñado para adaptarse a empresas de cualquier tamaño, desde pequeñas organizaciones hasta grandes corporaciones que manejan millones de eventos diarios.
Reducción de costos	La automatización y centralización minimizan la necesidad de tareas manuales repetitivas, permitiendo a los equipos de seguridad centrarse en actividades estratégicas.

Nota. Elaboración propia

Beneficios de un SIEM

Prevención de ataques: Identifica vulnerabilidades y comportamientos sospechosos antes de que ocurran incidentes graves.

Minimización de daños: Responde rápidamente a incidentes para contenerlos y mitigar su impacto.

Mejora de la eficiencia operativa: Libera recursos humanos al automatizar tareas de monitoreo y respuesta.

Ejemplos de SIEM más utilizados

IBM Security QRadar: Gestión avanzada de eventos con capacidad de soportar grandes volúmenes de datos y proporcionar respuestas inteligentes.[16]

McAfee Enterprise Security Manager: Monitoreo y análisis de registros con una base de datos extensa para detectar amenazas.

LogRhythm: Solución asequible para pequeñas empresas que necesitan capacidades SIEM.[17]

Solución Item 6

Herramientas de contención de ataques informáticos

Basándonos en las recomendaciones realizadas en la web conference, se propone una combinación de herramientas nativas de Windows y soluciones open-source, adecuadas para contener ataques en tiempo real. Estas herramientas permiten bloquear conexiones sospechosas, aislar sistemas comprometidos y frenar comportamientos maliciosos.

Firewall de Windows

Descripción:

El Firewall de Windows es una herramienta nativa que controla el tráfico de red entrante y saliente basado en reglas específicas. Permite bloquear puertos o direcciones IP sospechosas para evitar que el ataque se propague.

Función de contención: Durante un ataque, puede configurarse para aislar la máquina

---

[16] IBM. (s.f.). **QRadar SIEM**. IBM. https://www.ibm.com/es-es/products/qradar-siem

[17] Stellar Cyber. (2025). **Top SIEM solutions**. Stellar Cyber. https://stellarcyber.ai/es/learn/top-siem- solutions/

comprometida o restringir el acceso a servicios vulnerables.

Ejemplo práctico: En caso de un intento de ataque por fuerza bruta en un puerto específico, se puede configurar una regla para bloquear el puerto afectado o las IPs sospechosas.

Powershell

Descripción: PowerShell es una herramienta de automatización nativa de Windows que permite ejecutar comandos y scripts avanzados para responder rápidamente a incidentes.

Función de contención: Se utiliza para bloquear conexiones, deshabilitar servicios comprometidos o incluso apagar interfaces de red afectadas.

Ejemplo práctico: En un ataque detectado en tiempo real, un script de PowerShell puede automatizar el bloqueo de una lista de IPs sospechosas: New- NetFirewallRule -DisplayName "Bloquear IP" -Direction Inbound -Action Block - RemoteAddress <IP> Iptables (Para entornos Linux)

Descripción: Iptables es un firewall para sistemas Linux que filtra paquetes según reglas configuradas manualmente.

Función de contención: Bloquea conexiones sospechosas, restringe acceso a servicios vulnerables o aísla máquinas comprometidas en la red.

Ejemplo práctico: Durante un ataque de denegación de servicio (DDoS), Iptables puede bloquear tráfico entrante desde rangos de IPs maliciosas.

Fail2ban (Para Entornos Linux)

Descripción: Fail2Ban monitorea los logs del sistema para detectar comportamientos sospechosos, como intentos fallidos de inicio de sesión, y bloquea automáticamente las IPs ofensivas.

Función de contención: Previene ataques de fuerza bruta al restringir temporalmente el

acceso desde direcciones IP maliciosas.

Ejemplo práctico: Si un atacante intenta acceder repetidamente a un servidor SSH con credenciales incorrectas, Fail2Ban bloquea automáticamente su IP durante un periodo definido.

Aspectos que Aportan al Desarrollo de Estrategias de Red Team y Blue Team

El desarrollo de estrategias efectivas para los equipos Red Team y Blue Team depende de una comprensión profunda de los roles que desempeñan ambos equipos, las herramientas disponibles y la forma en que ambos pueden colaborar para mejorar la postura de seguridad de una organización. Aunque sus enfoques y objetivos son opuestos, la cooperación entre estos equipos es esencial para crear un ciclo de retroalimentación que fortalezca la seguridad organizacional y optimice la respuesta ante incidentes. A continuación, se detallan los aspectos clave que contribuyen al diseño y la implementación de estrategias efectivas para ambos equipos.[18]

Colaboración entre Red Team y Blue Team

La colaboración continua entre el Red Team y el Blue Team es una de las estrategias más efectivas para mejorar la seguridad organizacional. Aunque el Red Team simula ataques para identificar brechas de seguridad y el Blue Team defiende activamente, ambos equipos deben trabajar juntos para crear un ciclo de retroalimentación que fortalezca las medidas de protección.

Red Team: Actúa como el "adversario" simulado, utilizando tácticas de ataque realistas para identificar vulnerabilidades en la infraestructura de la organización.

Blue Team: Evalúa las vulnerabilidades expuestas durante los ataques simulados y ajusta sus defensas para mitigar las futuras amenazas, aprendiendo de cada ejercicio de ataque.

El enfoque colaborativo permite que el Blue Team mejore sus medidas preventivas basándose en los ataques simulados por el Red Team, mientras que el Red Team puede ajustar

[18] S2 Grupo. (2024). Red Team: Definición, funciones y diferencias con Blue Team. S2 Grupo. https://s2grupo.es/red-team-definicion-funciones-y-diferencias-con-blue-team/

sus técnicas y tácticas en función de las defensas implementadas por el Blue Team, logrando un ciclo constante de mejora.

Análisis de Vulnerabilidades y Hardening

El análisis de vulnerabilidades y la posterior implementación de medidas de hardenización son esenciales para ambos equipos. La identificación de brechas de seguridad y la corrección de estas son elementos cruciales en el fortalecimiento de la seguridad organizacional.

Red Team: Utiliza herramientas especializadas, como Metasploit, Nmap y Burp Suite, para identificar vulnerabilidades en sistemas, aplicaciones y redes.

Blue Team: Implementa medidas de hardening, como la configuración de firewalls, la aplicación de CIS Benchmarks y la actualización de parches de seguridad para corregir las vulnerabilidades identificadas.

Un Red Team eficaz identifica vulnerabilidades en fases tempranas del proceso de defensa, lo que permite al Blue Team aplicar medidas de hardening adecuadas. Esto reduce la superficie de ataque y mejora la seguridad de sistemas críticos mediante la configuración de seguridad predeterminada y la eliminación de servicios innecesarios.

Simulaciones de ataques realistas y planificación de respuesta a incidentes

Ambos equipos deben estar preparados para abordar ataques de manera eficiente. Las simulaciones de ataque, ejecutadas por el Red Team, y las estrategias de defensa y contención, implementadas por el Blue Team, son fundamentales en el diseño de una respuesta eficaz ante incidentes.

Red Team: Realiza simulaciones de ataques avanzados, incluyendo técnicas de evasión y explotación, para evaluar la resiliencia de las defensas organizacionales.

Blue Team: Desarrolla planes de respuesta a incidentes, lleva a cabo simulaciones de

contención y utiliza herramientas como SIEM, IDS/IPS y políticas de firewall para mitigar los ataques detectados.

Las simulaciones brindan al Blue Team la oportunidad de evaluar sus capacidades de detección y respuesta. Además, las pruebas realizadas por el Red Team permiten ajustar las estrategias de contención y recuperación, lo que mejora la capacidad del Blue Team para responder eficazmente en situaciones reales.

Monitoreo Continuo y Detección de Anomalías

El monitoreo continuo y la detección de anomalías son elementos clave en las estrategias de ambos equipos, ya que permiten identificar comportamientos sospechosos y posibles ataques en curso.

Red Team: Utiliza herramientas como Cobalt Strike o Empire para realizar movimientos laterales y evadir la detección, imitando los ataques de actores maliciosos reales.

Blue Team: Implementa soluciones avanzadas de monitoreo, como SIEM, Wireshark y Sysmon, para detectar ataques en tiempo real y generar alertas.

Un Red Team proactivo puede evaluar las capacidades de monitoreo del Blue Team mediante pruebas de evasión. Esta interacción ayuda al Blue Team a mejorar sus capacidades de detección, ajustando sus sistemas de monitoreo para identificar patrones anómalos que podrían haberse pasado por alto en simulaciones previas.

Formación y Capacitación Continua

La capacitación continua es fundamental para garantizar que ambos equipos estén actualizados con las últimas amenazas y técnicas de defensa.

Red Team: Se capacita en nuevas técnicas de ataque, vulnerabilidades emergentes y herramientas de explotación para mantenerse al tanto de las tácticas de los atacantes reales.

Blue Team: Se enfoca en la capacitación en herramientas de defensa, análisis de incidentes y gestión de riesgos, así como en la implementación de mejores prácticas de seguridad.

La formación constante asegura que las estrategias y tácticas empleadas por ambos equipos se mantengan efectivas frente a las amenazas emergentes. El Blue Team puede beneficiarse del conocimiento adquirido por el Red Team sobre las técnicas de ataque más recientes, mejorando su capacidad de detección y respuesta ante incidentes.

Evaluación y Retroalimentación Continua

La evaluación constante de las estrategias y la retroalimentación entre los equipos son cruciales para mejorar la ciberseguridad organizacional.

Red Team: Después de cada ejercicio de ataque, el Red Team genera informes detallados sobre las vulnerabilidades encontradas, las herramientas utilizadas y los resultados obtenidos.

Blue Team: Analiza estos informes y ajusta sus medidas de seguridad, basándose en las vulnerabilidades detectadas y las debilidades expuestas durante las simulaciones de ataque.

La retroalimentación proporcionada por el Red Team permite que el Blue Team refine su enfoque de seguridad, mientras que los informes del Blue Team sobre su capacidad de respuesta pueden ayudar al Red Team a ajustar sus tácticas y herramientas para futuros ejercicios.

Conclusiones

Evolución de las Estrategias de Red Team y Blue Team, a lo largo del seminario, se consolidó el entendimiento de las estrategias ofensivas (Red Team) y defensivas (Blue Team). Las actividades realizadas permitieron identificar vulnerabilidades críticas en sistemas informáticos, demostrar técnicas avanzadas de explotación y aplicar medidas de contención para mitigar riesgos. Esto demostró la importancia de un enfoque integral en ciberseguridad que combine ataque y defensa.

La utilización de herramientas como Nmap, Metasploit, Wireshark y OpenVAS fue esencial para simular ataques controlados y evaluar la efectividad de las defensas. Estas herramientas no solo facilitaron la identificación de vulnerabilidades, sino también la implementación de controles proactivos y reactivos para proteger los sistemas.

El seminario destacó la relevancia de alinear las estrategias de seguridad con marcos normativos, como la Ley 1273 de 2009 y la Ley 1581 de 2012 en Colombia, así como con estándares internacionales como ISO 27001. Esto refuerza la necesidad de integrar la ciberseguridad en el cumplimiento legal y organizacional.

Las simulaciones de ataques y defensas evidenciaron que las organizaciones pueden aumentar significativamente su resiliencia mediante el uso de estrategias como la hardenización, la contención inmediata de ataques y la monitorización continua. Estas prácticas reducen la superficie de ataque y garantizan una respuesta oportuna ante incidentes.

Colaboración y Sinergia entre Equipos, la interacción entre los equipos Red Team y Blue Team enfatizó la importancia de un enfoque colaborativo para mejorar la postura de seguridad. Las lecciones aprendidas en las simulaciones de ataque y defensa fortalecieron la cooperación y el entendimiento mutuo, fundamentales para mitigar amenazas cibernéticas.

Necesidad de Mejora Continua, la revisión y análisis de las estrategias empleadas durante el seminario subrayaron la importancia de mantener una mejora continua en la implementación de medidas de seguridad. Esto incluye la actualización constante de herramientas, la capacitación de los equipos y la evaluación periódica de vulnerabilidades.

Referencias Bibliográficas

Álvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos*. Semantic Scholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Ambit BST. (2020). ¿Qué significa SIEM y cómo funciona? *Ambit BST*. https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

Axarnet. (2024). *Fail2Ban: Prevención de ataques de fuerza bruta*. Axarnet. https://axarnet.es/blog/fail2ban

Center for Internet Security (CIS). (2025). *CIS Benchmarks List*. CIS Security. https://www.cisecurity.org/cis-benchmarks

Chindrus, C., & Caruntu, C.-F. (2023). *Securing the network: A red and blue cybersecurity competition case study*. *Information, 14*(11), 587. https://doi.org/10.3390/info14110587

Congreso de Colombia. (2009). *Ley 1273 de 2009 - Protección de la información y los datos personales*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (2012). *Ley 1581 de 2012 - Protección de datos personales*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Copnia. (2015). *Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares*. https://www.copnia.gov.co/tribunal-deetica/codigo-de-etica

Departamento Nacional de Planeación. (2019). *Política nacional para la formalización empresarial en Colombia: CONPES 3995 de 2019*. https://colaboracion.dnp.gov.co/cdt/Conpes/Económicos/3995.pdf

Fortinet. (2023). *CVE (Common Vulnerabilities and Exposures)*. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/cve

IBM. (2024).. *Penetration testing*. IBM. https://www.ibm.com/es-es/topics/penetration-testing

IBM. (2024).. *SIEM (Security Information and Event Management)*. IBM. https://www.ibm.com/mx-es/topics/siem

INCIBE. (2019). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas*. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). *Red Teaming vs. Blue Teaming: A comparative analysis of cybersecurity strategies in the digital battlefield*. *International Journal of Scientific Research in Engineering and Management, 7*(12), 1-11. https://doi.org/10.55041/IJSREM27675

MINTIC. (2022). *Políticas de privacidad y condiciones de uso*. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-dePrivacidad-y-Condiciones-de-Uso

Microsoft. (2023.). *Disabling terminal services features*. Microsoft Learn. https://learn.microsoft.com/es-es/windows/win32/termserv/disabling-terminal-services-features

National Institute of Standards and Technology (NIST). (2015). *Red Team - Glossary term*. CSRC. https://csrc.nist.gov/glossary/term/red_team

Nmap Project. (2024). *Nmap: Network Mapper*. Nmap Project. https://nmap.org/man/es/index.html#man-description

OpenWebinars. (2024). *Ciberseguridad proactiva: La importancia del Blue Team*. OpenWebinars. https://openwebinars.net/blog/ciberseguridad-proactiva-la-importancia-del-blue-team/

Organización de los Estados Americanos. (2001). *Convenio sobre la ciberdelincuencia*. OAS. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Panda Security. (2023). *Pentesting: Una herramienta muy valiosa para tu empresa*. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa

Policía Nacional de Colombia. (2009). *Ley 1273 de 2009*. Policía Nacional.

https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

S2 Grupo. (2024). *Red Team: Definición, funciones y diferencias con Blue Team*. S2 Grupo. https://s2grupo.es/red-team-definicion-funciones-y-diferencias-con-blue-team/

Stellar Cyber. (2024). *Top SIEM solutions*. Stellar Cyber. https://stellarcyber.ai/es/learn/top-siem-solutions

Tarlogic. (2024). ¿Qué metodologías se emplean habitualmente en ejercicios de Red Team? *Blog de Tarlogic*. https://www.tarlogic.com/es/blog/metodologias-red-team

Zuluaga Mateus, C. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad - OSSTMM, aplicado a la rama judicial, seccional Armenia*. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/17410