Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

Matios Maury González

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2024

Resumen

Este informe técnico aborda las estrategias de ciberseguridad necesarias para proteger la información sensible de organizaciones frente a las crecientes amenazas cibernéticas. En el marco normativo colombiano, se analizan leyes clave como la Ley 1273 de 2009 y su importancia en la protección de los sistemas informáticos. Asimismo, se examina un caso práctico de Red Team, enfocado en identificar y explotar vulnerabilidades críticas mediante herramientas como Metasploit y Nmap, demostrando el impacto potencial de ataques exitosos y proponiendo mejoras de seguridad.

El análisis también incluye estrategias de contención y defensa empleadas por el Blue Team, destacando el uso de tecnologías como SIEM y medidas de endurecimiento de sistemas para mitigar amenazas en tiempo real. Se refuerza la necesidad de una gestión ética y responsable de los datos en empresas de ciberseguridad, como se ejemplifica en el caso de CyberFort Technologies. Este documento propone un enfoque integral que combina aspectos técnicos, legales y operativos, con el objetivo de fortalecer la resiliencia cibernética y proteger los activos críticos de las organizaciones.

Palabras Clave. Ciberseguridad, Equipo Rojo, Equipo Azul, Medidas de Seguridad, Amenazas Cibernéticas.

Abstract

This white paper addresses the cybersecurity strategies needed to protect organizations' sensitive information from growing cyber threats. Within the Colombian regulatory framework, key laws such as Law 1273 of 2009 and their importance in protecting computer systems are analyzed. A Red Team case study is also examined, focusing on identifying and exploiting critical vulnerabilities using tools such as Metasploit and Nmap, demonstrating the potential impact of successful attacks and proposing security improvements.

The analysis also includes containment and defense strategies employed by the Blue Team, highlighting the use of technologies such as SIEM and system hardening measures to mitigate threats in real time. The need for ethical and responsible data management in cybersecurity companies is reinforced, as exemplified in the case of CyberFort Technologies. This document proposes a comprehensive approach that combines technical, legal, and operational aspects, with the aim of strengthening cyber resilience and protecting organizations' critical assets.

***Keywords*.** Cybersecurity, Red Team, Blue Teams, Cyber Defense, Digital Threats.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

La evolución tecnológica ha generado un aumento exponencial en las amenazas cibernéticas, exigiendo a las organizaciones y gobiernos fortalecer su ciberseguridad. En el contexto colombiano, el marco legal —representado por normativas como las Leyes 1266, 1273 y 527— ha buscado regular la protección de datos personales, combatir delitos informáticos y fomentar prácticas seguras en el entorno digital. Estas leyes, complementadas con herramientas avanzadas como Metasploit, Nmap y OpenVAS, y repositorios como CVE y ExploitDB, proveen a los profesionales de recursos esenciales para identificar y mitigar vulnerabilidades.

El papel de los equipos de Red Team y Blue Team es clave en este escenario. Mientras el Red Team simula ataques para identificar puntos débiles, el Blue Team fortalece la defensa contra amenazas reales. Este análisis combina ambos enfoques para evaluar la seguridad de sistemas, como un equipo Windows con la aplicación vulnerable Rejetto v. 2.3, validando riesgos mediante pruebas prácticas.

Asimismo, el caso de ciberespionaje en CyberFort Technologies resalta la relevancia de la ética en el sector, subrayando la necesidad de controles y sanciones eficaces para prevenir incidentes similares. Este informe técnico sintetiza las actividades realizadas en los enfoques Red Team, Blue Team y legales, con el objetivo de demostrar capacidades estratégicas y técnicas que contribuyan a la seguridad organizacional.

Justificación

La ciberseguridad se ha convertido en una prioridad estratégica para las organizaciones, debido al crecimiento de las amenazas informáticas y su impacto en la confidencialidad, integridad y disponibilidad de los datos. Este informe responde a la necesidad de evaluar, mitigar y prevenir riesgos mediante enfoques integrales de seguridad que combinen estrategias ofensivas y defensivas, representadas por los equipos de Red Team y Blue Team.

En un contexto como el colombiano, donde el marco legal ha avanzado para regular la protección de datos y sancionar delitos cibernéticos, es imprescindible contar con herramientas técnicas, metodologías probadas y profesionales éticos que garanticen la eficacia de estas normativas en la práctica. Casos como el ciberespionaje en CyberFort Technologies evidencian la importancia de implementar controles estrictos y promover una cultura de responsabilidad en el manejo de información sensible.

Este documento no solo busca demostrar competencias técnicas mediante la identificación y explotación de vulnerabilidades, sino también proponer estrategias de defensa y endurecimiento que alineen las prácticas operativas con estándares internacionales de seguridad. Su objetivo es respaldar la capacidad de garantizar la resiliencia cibernética, reduciendo riesgos para las organizaciones y fomentando la confianza en sus operaciones tecnológicas.

Objetivos

Objetivo General

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Objetivos Específicos

Aspectos que aporten al desarrollo de estrategias de Red Team & Blue Team.

Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

Marco Legal Colombiano: Delitos Informáticos y Protección de Datos

En el marco del Estado de Derecho colombiano, diversas leyes y normativas han sido promulgadas para enfrentar las crecientes amenazas cibernéticas y garantizar la protección de la información y los datos personales en la era digital:

Ley 1266 de 2008. Regula el hábeas data y el manejo de información personal, estableciendo directrices para la protección y el acceso a los datos (Congreso de la República de Colombia, 2008, 31 de Diciembre).

Ley 527 de 1999. Define y reglamenta el uso de mensajes de datos, comercio electrónico y firmas digitales, asegurando la validez jurídica de las transacciones electrónicas (Congreso de la República de Colombia, 1999, 18 de agosto).

Ley 1273 de 2009. Introduce medidas específicas contra delitos informáticos, penalizando actividades ilícitas relacionadas con el uso no autorizado de información. Reconoce los datos como un bien jurídico valioso y busca concientizar sobre su manejo ético, destacando la necesidad de actualizar continuamente la legislación para enfrentar nuevas amenazas (Congreso de la República de Colombia, 1999, 18 de agosto).

Decreto 1078 de 2015. Establece requisitos para el registro e incorporación de tecnologías de información y comunicación (TIC) en el país (Presidencia de la República de Colombia, 2015, 6 de mayo).

Ley 1581 de 2012. Considerada pilar de la protección de datos personales, garantiza el derecho de los ciudadanos a conocer, actualizar y rectificar información en bases de datos públicas y privadas. Establece estándares para el manejo ético y seguro de los datos, promoviendo la privacidad y la integridad en su tratamiento (Congreso de la República de Colombia, 2012, 17 de octubre).

Pruebas de Penetración o Pentesting

Escaneo de Puertos

El escaneo de puertos es una técnica clave en ciberseguridad que permite identificar los puntos de acceso en una red, asociados a servicios o aplicaciones específicas. (Naqvi & Sultan, 2022) Proporciona información esencial sobre la infraestructura digital y ayuda a fortalecer su protección.

Importancia del Escaneo de Puertos

Identificación de Servicios Activos. Detecta qué servicios y aplicaciones están operativos.

Cartografía de la Red. Ofrece una visión clara de la topología y las conexiones entre dispositivos.

Detección de Barreras de Seguridad. Permite identificar firewalls y filtros en puertos restringidos.

Preparación para Ataques Dirigidos. Identifica vulnerabilidades para prevenir posibles ataques sofisticados. Esta práctica proactiva está alineada con leyes colombianas como:

Ley 1273 de 2009. Penaliza el acceso indebido y la explotación de vulnerabilidades.

Ley 1581 de 2012. Protege los datos personales, cuya seguridad puede verse comprometida por sistemas vulnerables.

Método de Escaneo de Puertos.

El escaneo de puertos es una técnica crucial en ciberseguridad que identifica los puntos de acceso, servicios activos y vulnerabilidades en una red (Romero, y otros, 2023), proporcionando una visión clara de la superficie de ataque y permitiendo medidas preventivas. Su uso es esencial para reforzar defensas y tomar decisiones informadas (Sahu & Achraya, 2020).

Tipos de Escaneo de Puertos

TCP. El más común, analiza detalladamente el estado de los puertos.

UDP. Más complejo, evalúa la naturaleza sin conexión de este protocolo.

Sigiloso (Stealth). Evita la detección mediante métodos como escaneo SYN o FIN.

Exhaustivo (All Ports). Examina todos los puertos, aunque puede ser más lento y detectable.

Importancia y Relación con Normativas

Identifica configuraciones inseguras y vulnerabilidades críticas. Facilita la protección de datos personales y sistemas, alineándose con:

La ley 1273 de 2009. Penaliza accesos no autorizados y delitos informáticos.

Ley 1581 de 2012. Protege los datos personales y fomenta el manejo seguro de información sensible.

La Enumeración

La enumeración es una fase clave en las pruebas de intrusión que sigue al escaneo de puertos y precede a la explotación de vulnerabilidades (Martínez-Sanchez, Nespoli, Garcia-alfaro, & Gómez, 2023). Su objetivo es proporcionar una comprensión profunda del entorno digital de una organización, identificando usuarios, sistemas y configuraciones para anticiparse a amenazas y planificar estrategias defensivas efectivas.

Principales Actividades en la Enumeración

Compilación de Información Exhaustiva. Análisis detallado de usuarios, grupos, recursos compartidos, políticas de seguridad y configuraciones del sistema.

Determinación de Usuarios y Grupos. Ayuda a entender la jerarquía de accesos y planificar posibles escalamientos de privilegios.

Análisis de Recursos Compartidos. Evalúa la exposición de datos sensibles y permisos asociados.

Mapeo de Interacciones. Revela cómo los usuarios interactúan con los recursos, proporcionando una visión integral de la infraestructura.

Evaluación de Políticas de Seguridad. Examina medidas como requisitos de contraseñas, bloqueos de cuentas y otras protecciones clave.

La Importancia de la Enumeración en las Pruebas de Intrusión

La enumeración es una fase crucial en las pruebas de intrusión que permite recopilar información detallada sobre sistemas, usuarios, redes y servicios en una infraestructura digital (Martínez-Sanchez, Nespoli, Garcia-alfaro, & Gómez, 2023). Su propósito es identificar configuraciones internas, puntos débiles y servicios vulnerables para fortalecer la seguridad y mitigar riesgos cibernéticos.

Proporciona conocimiento clave para reforzar defensas y establecer una postura de seguridad robusta.

Contribuye a identificar áreas críticas donde podrían exponerse datos personales o información sensible.

Relación Legal en Colombia

Ley 1273 de 2009. Penaliza actividades ilícitas en sistemas informáticos y fomenta la implementación de medidas de protección.

Ley 1581 de 2012. Refuerza la necesidad de proteger los datos personales, siendo la enumeración una herramienta para identificar vulnerabilidades y cumplir con los estándares legales.

Preparación para la Fase de Explotación

La información recopilada durante la enumeración sirve como base para la fase de explotación (Couretas, 2022). Identificar usuarios, servicios y configuraciones específicas prepara al equipo de seguridad para ataques más dirigidos y efectivos.

Análisis de Vulnerabilidades Específicas. Facilita la identificación de vulnerabilidades específicas en usuarios o servicios, lo que contribuye a una evaluación más precisa de las amenazas potenciales.

Evaluación de la Superficie de Ataque. Ayuda a determinar la exposición total de la red, incluyendo recursos compartidos, servicios y usuarios, lo que es crucial para la comprensión completa de la superficie de ataque.

Identificación de Objetivos de Interés. Permite a los profesionales de seguridad identificar objetivos específicos de interés, como cuentas de administrador o sistemas críticos, para evaluar su nivel de protección y mitigar posibles riesgos.

La explotación de Vulnerabilidades

La explotación es la etapa en pruebas de intrusión donde se simulan ataques controlados para evaluar el impacto real de las vulnerabilidades identificadas (Abdelrazek, Mammi, & Din, 2021). Su propósito principal es demostrar cómo un atacante podría comprometer un sistema y ayudar a fortalecer las defensas de la infraestructura (Alonso, 2023).

Identificación de Vulnerabilidades. Utiliza información obtenida en fases previas, como el escaneo de puertos y la enumeración.

Uso de Exploits. Emplea herramientas o códigos diseñados para aprovechar vulnerabilidades específicas.

Objetivos. Ganar acceso no autorizado, escalar privilegios y, en algunos casos, establecer un acceso persistente al sistema.

Simulación Controlada. Evalúa la eficacia de las defensas y permite entender el impacto potencial de un ataque exitoso.

Informe y Recomendaciones. Documenta hallazgos y sugiere medidas para mitigar riesgos.

Consideraciones Éticas y Legales.

Debe realizarse con consentimiento explícito del propietario del sistema. Regida por la Ley 1273 de 2009, que sanciona ataques malintencionados y promueve prácticas éticas en ciberseguridad.

La Escalada de Privilegios

La escalada de privilegios busca demostrar cómo un atacante con acceso limitado puede explotar vulnerabilidades para obtener permisos más altos y mayor control sobre un sistema (Safla, 2023). Este proceso revela riesgos críticos que podrían comprometer datos sensibles y operaciones esenciales. Aquí se exploran los aspectos clave de la escalada de privilegios (Laprovittera, 2023):

Identificación de Vulnerabilidades. Detectar errores o configuraciones que permitan elevar el nivel de acceso.

Técnicas de Escalada. Incluyen explotación de errores de diseño, manipulación de configuraciones, ejecución de comandos maliciosos y uso de vulnerabilidades específicas.

Impacto Potencial. Ilustra cómo una falla menor puede otorgar control completo del sistema, acceso a datos sensibles o comprometer otros sistemas conectados.

Evaluación de Políticas. Analiza las políticas de seguridad vigentes para detectar y corregir deficiencias.

Uso de Exploits Específicos. Herramientas diseñadas para aprovechar vulnerabilidades concretas.

Consideraciones Éticas y Legales

Regida por la Ley 1581 de 2012, que protege los datos personales y fomenta prácticas que prevengan accesos no autorizados.

Resultado

Informe y Mitigación. Documentación de los hallazgos y recomendaciones para eliminar riesgos y reforzar la seguridad del sistema.

La Obtención de Acceso Remoto

Esta fase simula cómo un atacante podría establecer y mantener acceso remoto no autorizado a un sistema, evaluando la capacidad para sortear defensas y lograr control persistente (Costantino & Mattucci, 2019).

Objetivo. Identificar vulnerabilidades y simular técnicas avanzadas para lograr acceso remoto y persistente.

Importancia. Expone fallas críticas en el entorno digital, subrayando la necesidad de reforzar las defensas.

Relevancia Legal. La Ley 1273 de 2009 penaliza el acceso indebido y destaca la importancia de proteger sistemas contra intrusiones.

Capacidad del Sistema. Evalúa la habilidad del entorno para detectar, mitigar intrusiones y limitar el impacto de accesos no autorizados.

Identificación de Vulnerabilidades de Acceso Remoto

Esta fase evalúa cómo un atacante podría ingresar a un sistema de manera remota, destacando vulnerabilidades y simulando ataques externos para obtener control continuo (Díaz-Cacho, Chaves, & Pereira, 2023).

Identificación de Vulnerabilidades. Se detectan puntos de entrada remotos que puedan ser explotados.

Explotación de Puntos de Entrada. Simulación de ataques para aprovechar vulnerabilidades específicas.

Conexiones Persistentes. Creación de backdoors, cuentas de usuario o manipulación de servicios para mantener acceso continuo.

Uso de Herramientas Especializadas. Se emplean herramientas diseñadas para facilitar el acceso remoto.

Obtención de Datos y Control. Simulación del acceso a información y el dominio del sistema comprometido.

Informe y Recomendaciones. Se documentan las vulnerabilidades halladas y se proponen medidas para fortalecer la seguridad.

La Ingeniería Social

La ingeniería social explota la psicología humana, manipulando emociones y confianza, para acceder a información sensible o comprometer sistemas (Prado, 2021).. Este enfoque resalta la necesidad de combinar infraestructura técnica sólida con una cultura organizacional de seguridad y concienciación.

Phishing. Correos fraudulentos para obtener credenciales o información financiera.

Vishing. Uso de llamadas o mensajes de voz falsos para engañar y obtener datos.

Smishing. Mensajes de texto fraudulentos que inducen a acciones inseguras.

Ataques en Redes Sociales. Uso de perfiles falsos o manipulados para recolectar información personal y corporativa.

Ingeniería Social Presencial. Interacciones cara a cara para obtener acceso no autorizado o información sensible.

La Ley 1581 de 2012 destaca la importancia de proteger los datos personales frente a estas tácticas, reforzando la necesidad de sensibilizar y capacitar a las personas como parte integral de la seguridad organizacional.

Pruebas de Intrusión

Las pruebas de intrusión simulan ataques cibernéticos para identificar vulnerabilidades y fortalecer la seguridad de las organizaciones. Estas evaluaciones no solo detectan debilidades puntuales, sino que permiten anticipar vectores de ataque y aplicar medidas proactivas a largo plazo. Más allá de detectar debilidades puntuales, estas evaluaciones ofrecen un enfoque estratégico para anticipar posibles vectores de ataque (Fajardo, Montaño, Donado, & Villalba, 2019).

Al analizar exhaustivamente cada fase de las pruebas, se pueden identificar no solo los puntos vulnerables, sino también las oportunidades para implementar medidas proactivas que fortalezcan la seguridad a largo plazo (Coronel & Quirumbay, 2022).

Este proceso es fundamental para asegurar que las organizaciones estén preparadas de manera efectiva ante las amenazas cibernéticas, que evolucionan constantemente. Siendo en este caso las fases éticas de las pruebas de intrusión (Coronel & Quirumbay, 2022) de las Fases Principales:

Reconocimiento. Recolección inicial de información sobre el objetivo (red, dominios, IPs) para identificar posibles puntos de entrada.

Escaneo. Uso de herramientas como NMAP para mapear la red y detectar servicios activos.

Enumeración. Obtención de detalles específicos como usuarios, grupos y recursos compartidos, preparando ataques específicos.

Explotación. Uso de exploits para demostrar cómo un atacante podría comprometer el sistema.

Post-Explotación. Evaluación de actividades como escalada de privilegios y acceso remoto para mantener el control.

Informe y Recomendaciones. Documentación detallada de hallazgos y medidas de mejora.

Contexto Legal

Ley 1273 de 2009. Protege la información y los datos frente a vulneraciones.

Ley 1581 de 2012. Refuerza la importancia de resguardar tanto los sistemas como los datos personales.

Las Herramientas Principales para el Desarrollo del Pentesting

Herramientas de Ciberseguridad

Metasploit. Metasploit es un marco de trabajo (framework) de código abierto utilizado para desarrollar, probar y ejecutar exploits en sistemas informáticos. (Suntaxi, Nasimba, Pallango, & Yaguarshungo, 2023). Metasploit permite lanzar ataques simulados para comprobar cómo responderían los sistemas ante vulnerabilidades conocidas.

Nmap. Nmap (Network Mapper) es una herramienta de código abierto para explorar redes y realizar auditorías de seguridad (Díaz, 2019). Se utiliza para descubrir hosts activos y servicios disponibles en una red. Esto permite a los administradores de red y los auditores de seguridad detectar configuraciones incorrectas o vulnerabilidades en sus redes.

OpenVAS. OpenVAS (Open Vulnerability Assessment System) es una herramienta de análisis de vulnerabilidades que se utiliza para detectar fallas de seguridad en sistemas y redes (Chiluiza & & Enciso, 2023). OpenVAS ofrece una plataforma para realizar escaneos de vulnerabilidad detallados y automáticos.

Servicios en Línea

ExploitDB. ExploitDB es una base de datos en línea de exploits y vulnerabilidades de código abierto (Kekül, Ergen, & Arslan, 2022). Proporciona un repositorio público donde se almacenan exploits y pruebas de concepto. Esto permite a los profesionales de la seguridad estudiar y comprender cómo funcionan las vulnerabilidades en diversas aplicaciones y sistemas operativos. Es una fuente clave para quienes buscan detalles sobre exploits disponibles para vulnerabilidades conocidas.

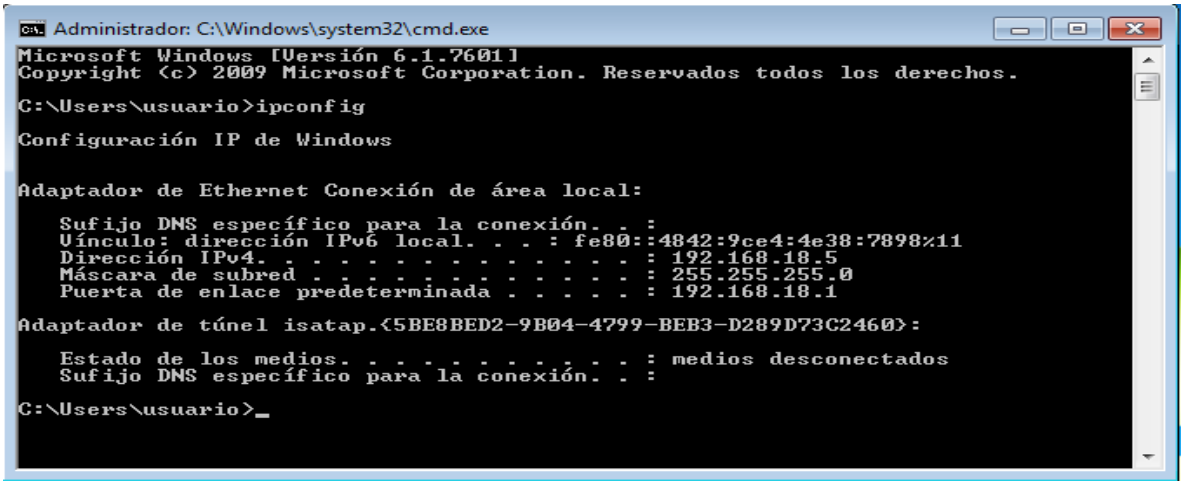
CVE (Common Vulnerabilities and Exposures). CVE es un sistema de identificación y estandarización de vulnerabilidades de seguridad (Walkowski, Oko, & Sujecki, 2021).

Proporciona un método estándar para identificar y nombrar vulnerabilidades y exposiciones de software, lo que permite a los equipos de seguridad compartir información de manera más eficiente.

Evidencia de la Implementación del "Banco de Trabajo" en su Entorno Local

Figura 1

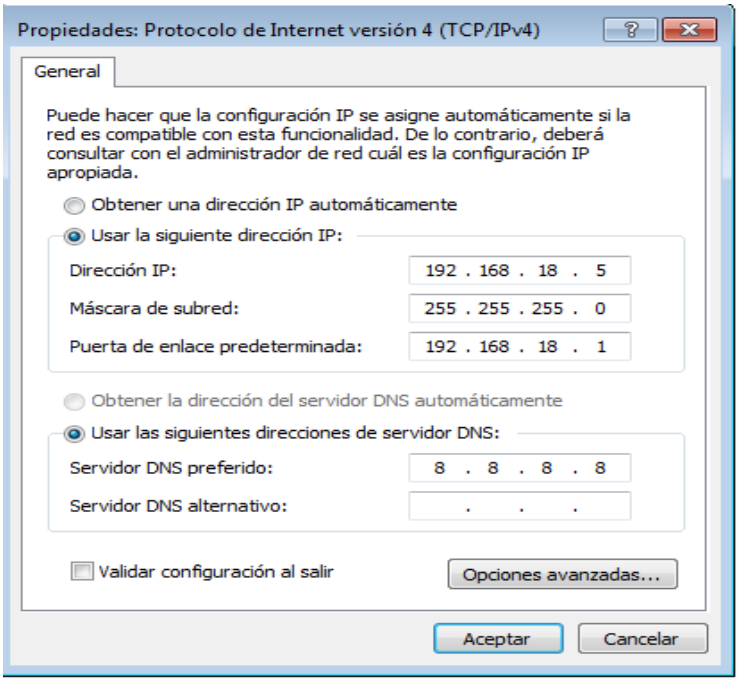
Conexión a Windows



Nota. Elaboración propia.

Figura 2

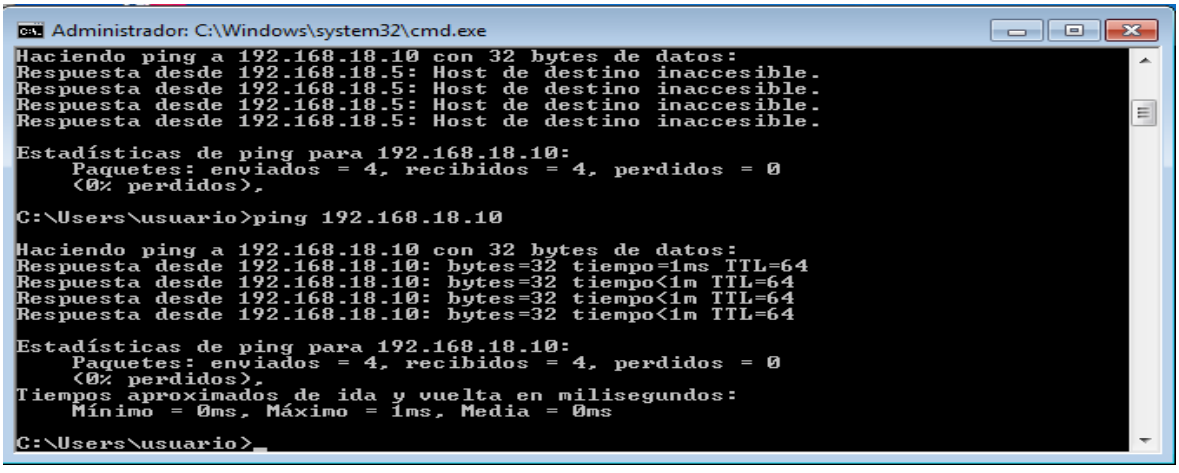
Protocolo IPv4



Nota. Elaboración propia.

Figura 3

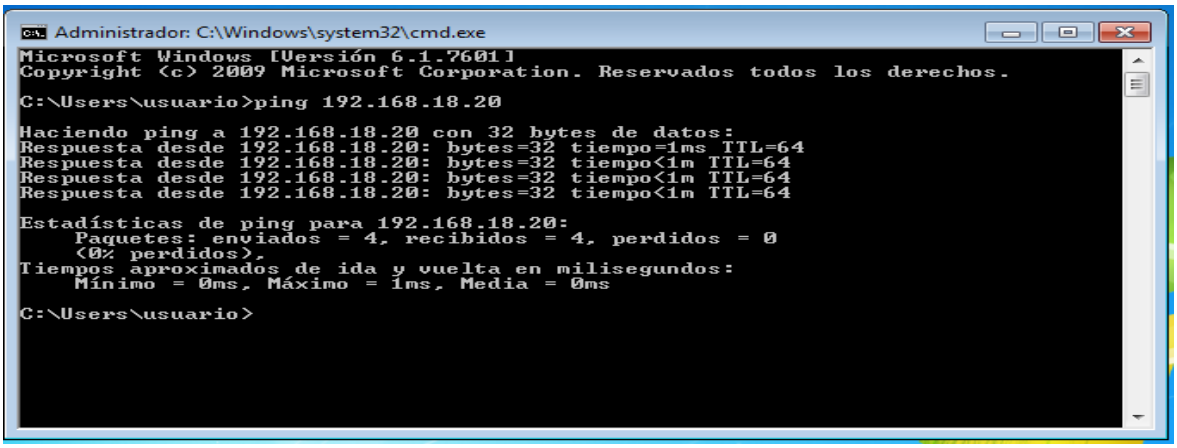
Ping al Equipo Kali Linux 01



Nota. Elaboración propia.

Figura 4

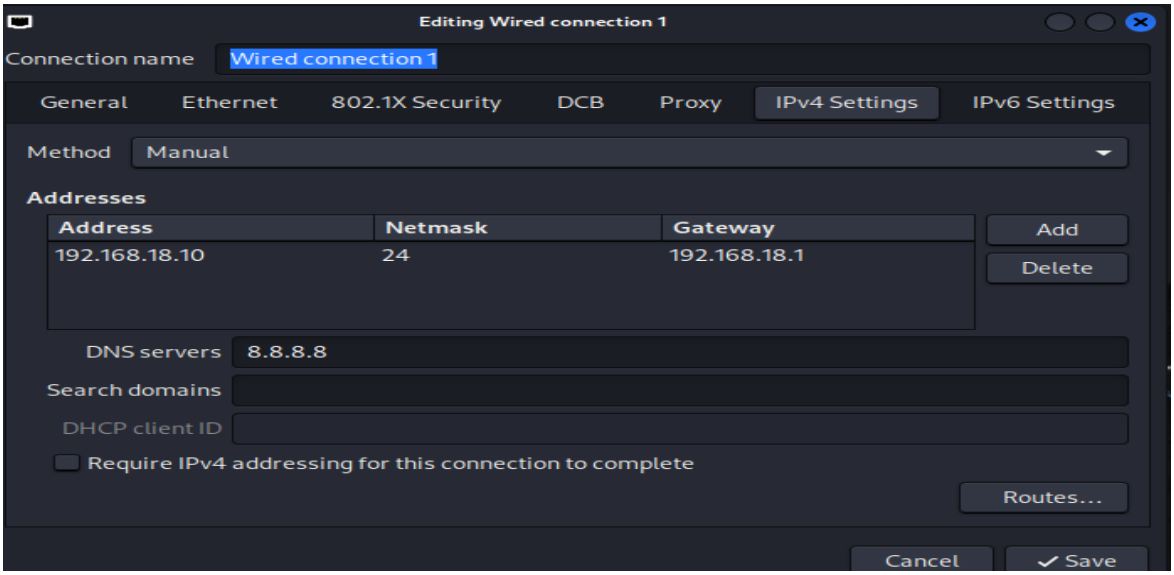
Ping desde Windows al Equipo Kali Linux 02



Nota. Elaboración propia.

Figura 5

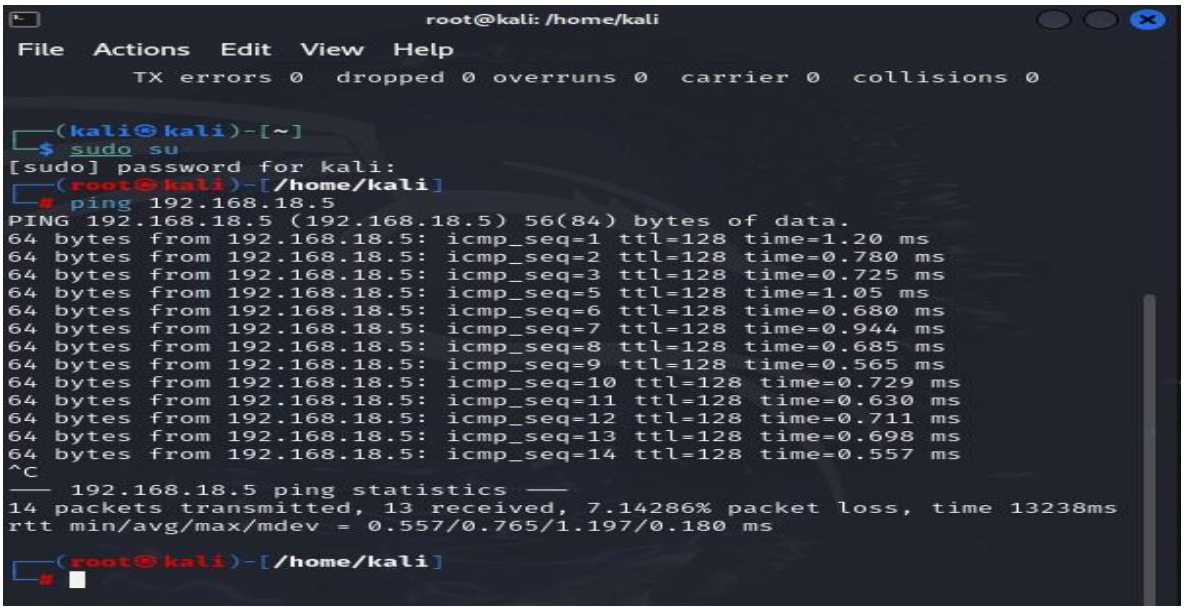
Nueva #IP - Kali Linux 01



Nota. Elaboración propia.

Figura *6*

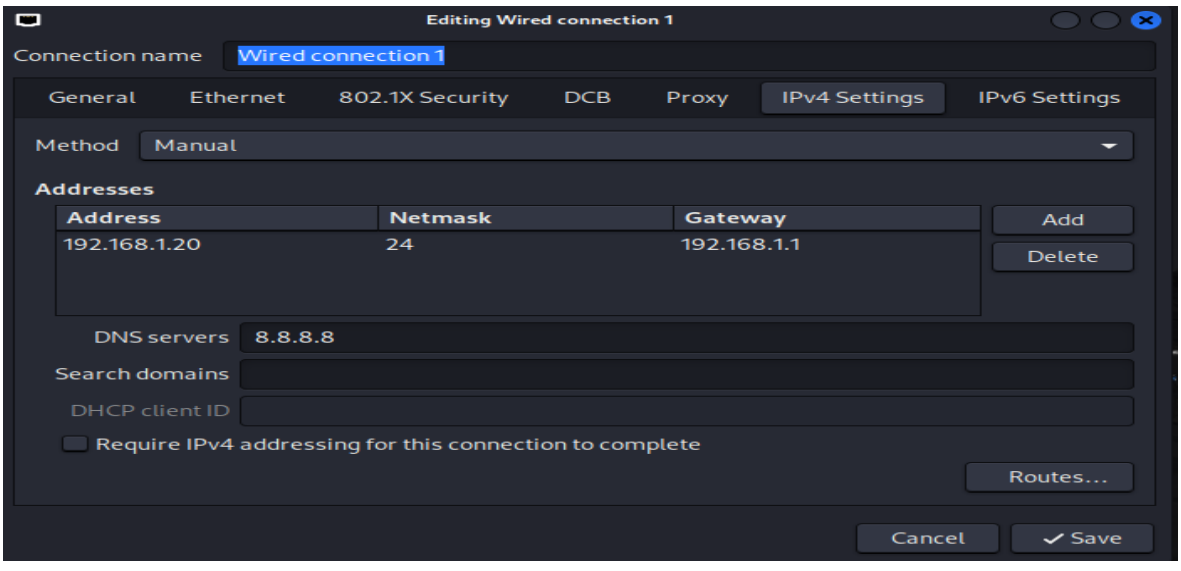
Ping de Kali Linux 01 a Windows



Nota. Elaboración propia.

Figura 7

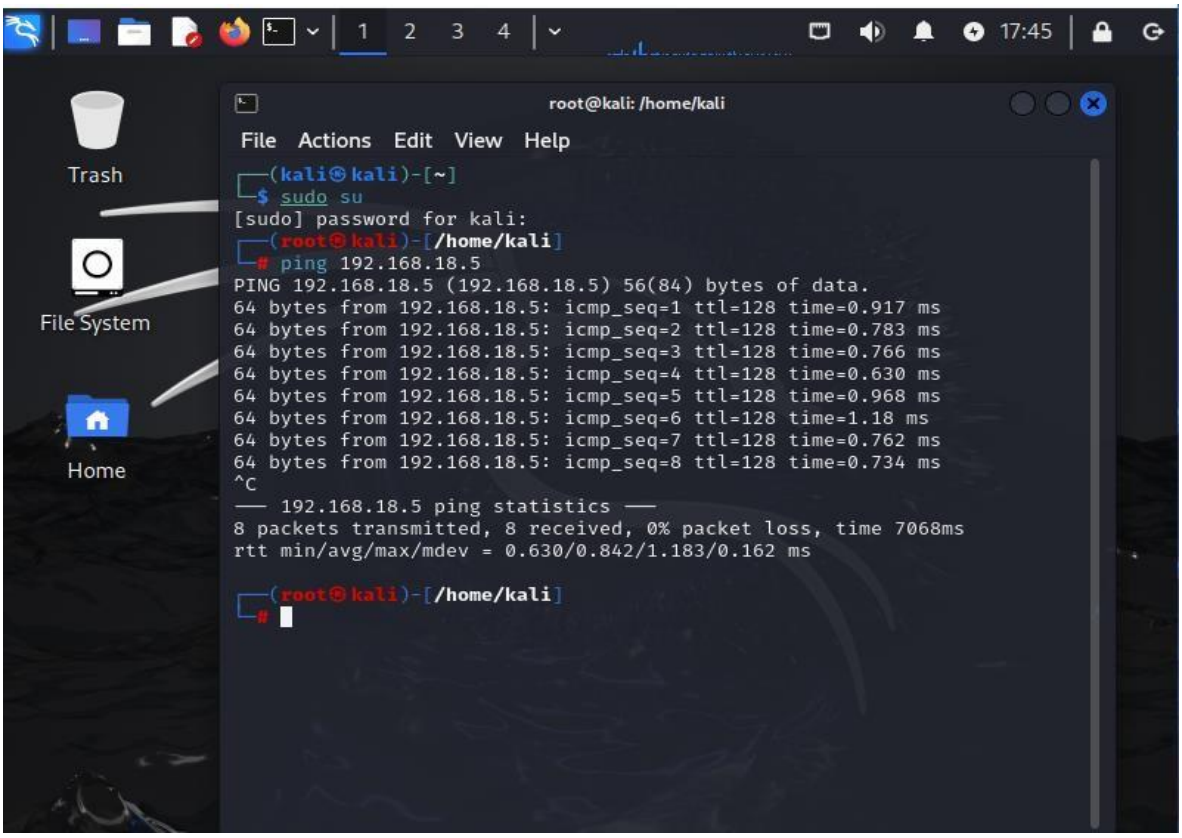
Nueva #IP - Kali Linux 02



Nota. Elaboración propia.

Figura 8

Ping de Kali Linux 02 a Windows



Nota. Elaboración propia.

Metodología, Herramientas y Softwares Utilizadas en el Caso de Red Team

Para abordar el anexo 4 – escenario 3 y responder a la pregunta sobre las herramientas utilizadas en el proceso de Red Team, te propongo dividir el análisis en las fases de un pentesting clásico (Reconocimiento, Escaneo, Explotación y Post-explotación) y especificar las herramientas de cada etapa con evidencias de comandos y resultados.

Rejetto HFS

Es un servidor de archivos HTTP gratuito y ligero (HTTP File Server) que permite compartir archivos a través de una red utilizando un navegador web. La versión 2.3 de esta aplicación es conocida por contener una vulnerabilidad que puede ser explotada para obtener acceso remoto al sistema (Jaswal, 2020).

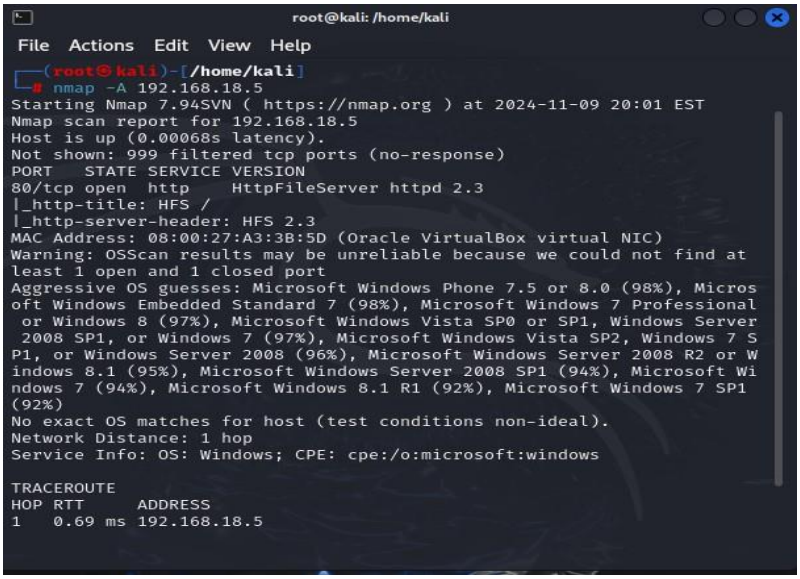
Fase 1: Reconocimiento

Herramientas Usadas. Para realizar un escaneo de puertos y detectar servicios en ejecución.

NMAP. Es una herramienta de escaneo de redes que se utiliza para descubrir dispositivos en una red y evaluar sus puertos abiertos y servicios. Nmap es muy utilizado en pruebas de seguridad para identificar posibles puntos de entrada en un sistema o red (Raj & Walia, 2020).

Figura 9

Rastreo de Puertos



Nota. Elaboración propia.

Resultado. Información sobre los servicios y puertos abiertos en la máquina objetivo, además del sistema operativo y versión de la aplicación vulnerable.

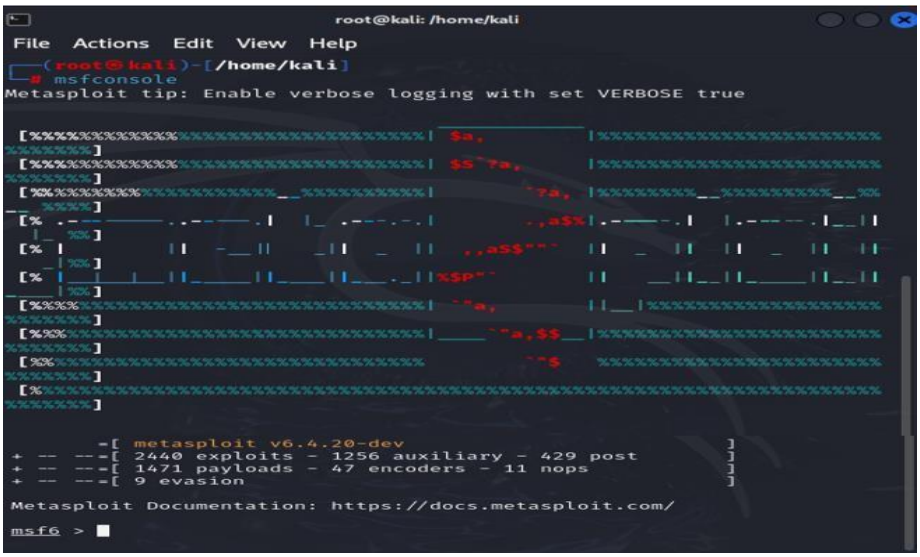
Fase 2: Escaneo

Herramientas Usadas. Para verificar exploits específicos de la versión de la aplicación vulnerable en la máquina objetivo.

Metasploit: Es una plataforma de explotación de seguridad que permite a los profesionales de la ciberseguridad probar y demostrar vulnerabilidades en sistemas. Contiene una colección de exploits y herramientas, y permite establecer conexiones remotas (como Meterpreter) en sistemas comprometidos (Tabassum, Mohanan, & Tripti, 2021).

Figura 10

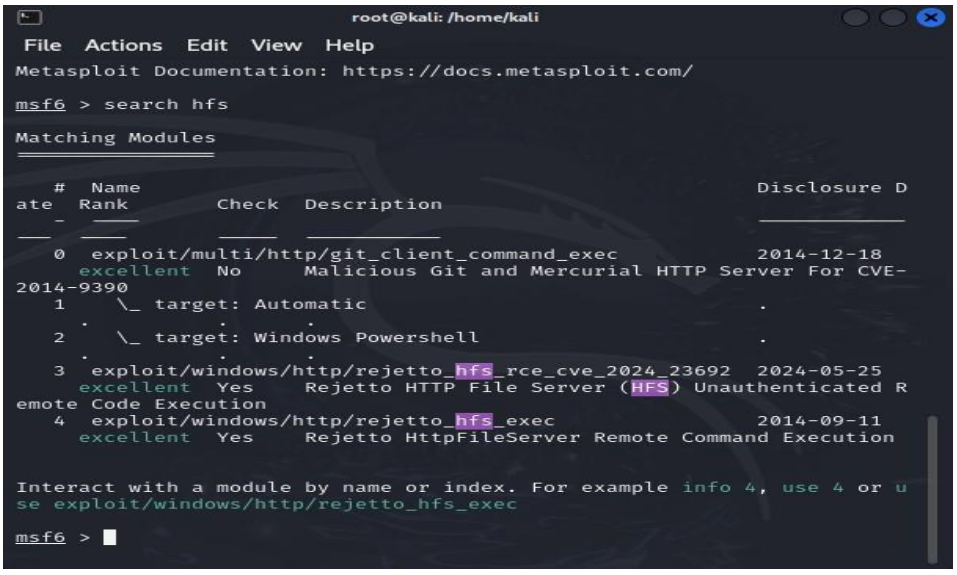
Instalación de Metasploit Msfconsole



Nota. Elaboración propia.

Figura 11

Búsqueda de Archivos HFS



Nota. Elaboración propia.

Resultado. Lista de exploits disponibles para la aplicación, indicando si alguno permite una ejecución remota de comandos (RCE) o acceso a shell.

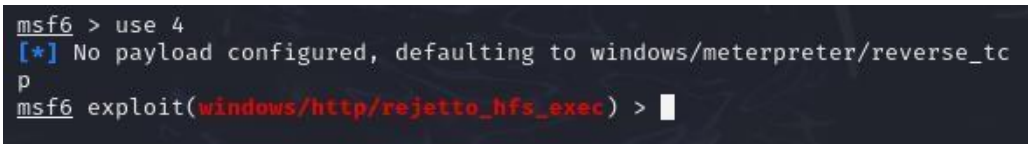
Fase 3: Explotación

Herramientas Usadas. Se utiliza para ejecutar el exploit correspondiente a la aplicación vulnerable y acceder al sistema mediante shell.

Metasploit (con Exploit Específico). Metasploit es una herramienta avanzada de pruebas de penetración que permite a los profesionales de ciberseguridad identificar, probar, y explotar vulnerabilidades en sistemas de manera controlada. (Valea & Ciprian, 2020). Utiliza exploits específicos (código o instrucciones diseñadas para aprovechar fallos de seguridad en software) que, una vez ejecutados, pueden conceder acceso o control sobre un sistema vulnerable. Por ejemplo, en un entorno de prueba con Rejetto HFS v. 2.3, se puede usar un exploit específico que aproveche una vulnerabilidad en esta versión del software para obtener acceso no autorizado.

Figura 12

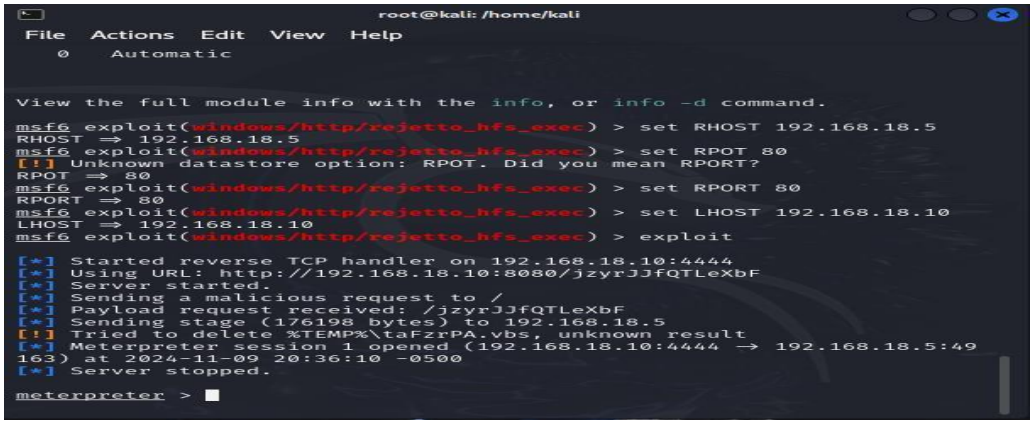
Búsqueda en el Shell



Nota. Elaboración propia.

Figura 13

Búsqueda en el Shell



Nota. Elaboración propia.

Resultado. Acceso a un shell de sistema con permisos de usuario básico o administrador, dependiendo del éxito del exploit.

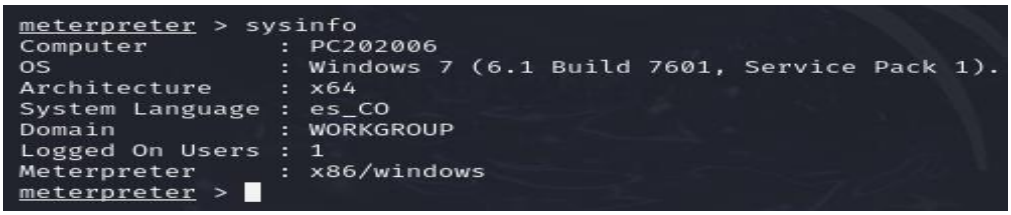
Fase 4: Post-Explotación

Herramientas Usadas. Para crear un usuario administrador y demostrar la PoC.

PowerShell. Es un marco de automatización y administración de tareas de Windows que incluye una interfaz de línea de comandos (CLI) y un lenguaje de scripting basado en .NET. PowerShell permite a los administradores y usuarios realizar una amplia variedad de tareas en Windows, desde la gestión de configuraciones hasta la ejecución de scripts complejos (Mimura & Tajiri, 2021).

Figura 14

Información del PC



Nota. Elaboración propia.

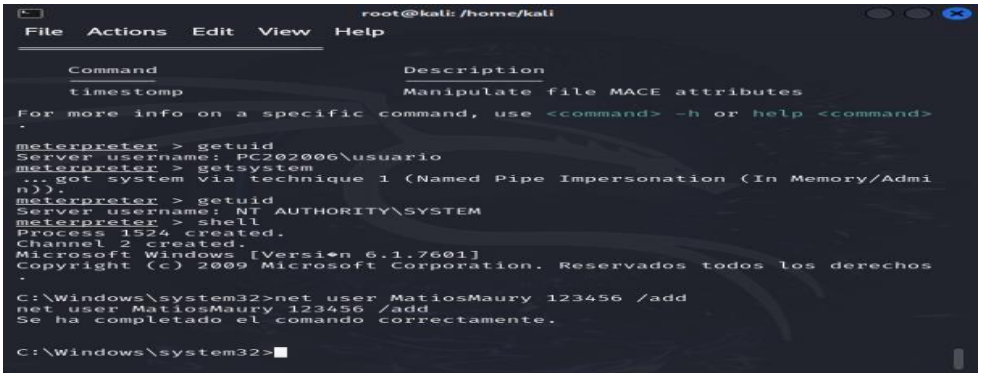
Figura 15

Creación del Usuario

Nota. Elaboración propia.

Figura 16

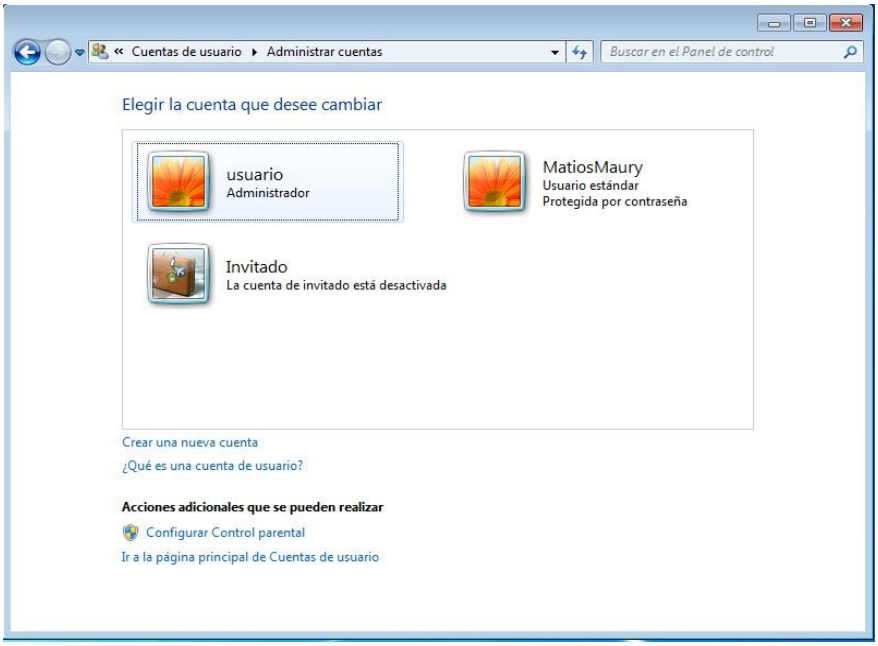
Data de Creación del Usuario



Nota. Elaboración propia.

Figura 17

Nuevo Usuario Administrativo



Nota. Elaboración propia.

Resultado. Confirmación de creación del usuario administrador en el sistema objetivo.

Herramientas para Identificar Fallos de Seguridad en Windows

Para identificar el fallo de seguridad específico en la máquina Windows, se analizaron y describieron los siguientes datos e información detallados en el Anexo 4 – Escenario 3:

Detección de Fuga de Información Interna. Se identificó un incidente de fuga de información en uno de los equipos de la organización, sugiriendo un potencial compromiso de seguridad en su infraestructura.

Aplicación Vulnerable (Rejetto HFS v. 2.3). La máquina Windows 7 con arquitectura x64 utiliza la aplicación HTTP File Server (HFS) en su versión 2.3, conocida por presentar vulnerabilidades de ejecución remota de código, que facilitaron la identificación del fallo.

Disponibilidad de un Exploit para Sesión Remota. Se verificó la existencia de un exploit específico para Rejetto HFS 2.3 que permite la ejecución de una shell reversa. Esta vulnerabilidad abre la posibilidad de establecer una sesión de Meterpreter en la máquina comprometida, permitiendo el control remoto del sistema.

Identificación de una Falla de Seguridad en la Configuración. El análisis del entorno reveló configuraciones que no seguían las mejores prácticas de seguridad, lo que permitió el acceso remoto y la ejecución del exploit.

Posibilidad de Escalación de Privilegios. Además, se encontró una debilidad que facilita el escalamiento de privilegios en el sistema, permitiendo a un atacante con acceso inicial elevar sus permisos y obtener control administrativo en la máquina comprometida.

Herramientas para Detectar Fallos de Seguridad en Windows

Para identificar los fallos de seguridad en la máquina Windows, empleé Nmap y Metasploit como herramientas principales. Estas herramientas me permitieron detectar los servicios y puertos abiertos, así como vulnerabilidades específicas de la aplicación en cuestión.

Herramientas y Uso

Nmap (Network Mapper)

Función. Identificación de puertos abiertos y servicios en ejecución.

Comando. nmap -A 192.168.18.5

Resultado. Este escaneo permitió descubrir puertos abiertos asociados con servicios de la máquina y detectar las configuraciones de la aplicación específica mencionada en el anexo, como el puerto de escucha de la aplicación vulnerable.

Metasploit.

Función. Explorar vulnerabilidades específicas de la aplicación y verificar exploits para la versión identificada.

Comando. Tras identificar el puerto y servicio, ejecuté msfconsole, seguido de una búsqueda en la base de datos de Metasploit con search <nombre de la aplicación o versión> para buscar exploits.

Resultado. Encontré posibles exploits relacionados con la aplicación, confirmando si uno de ellos permite la ejecución remota o escalamiento de privilegios.

Puerto Abierto por la Aplicación

Según el escenario del anexo, la aplicación vulnerable específica abre el puerto 80 y 8080 para comunicaciones. Este puerto suele estar asociado con servicios HTTP, lo cual sugiere que la

aplicación podría ser un servidor web o interfaz de aplicación expuesta, facilitando ataques a través de exploits relacionados con protocolos web o de aplicaciones que corren sobre HTTP.

Cómo Afecta el Ataque a la Máquina Windows

El ataque a la máquina Windows 7 con arquitectura X64 que ejecuta la aplicación Rejetto v. 2.3 puede explotar vulnerabilidades específicas en la aplicación, lo que permite a un atacante obtener acceso no autorizado al sistema. A continuación, te explico cómo funciona el ataque y el impacto que tiene en la máquina víctima.

Contexto: Aplicación Rejetto V. 2.3

Rejetto es una aplicación que permite compartir archivos a través de HTTP (servidor HTTP basado en la aplicación) (Jaswal, 2020). Las versiones antiguas de Rejetto, como la v.2.3, son vulnerables a desbordamientos de búfer y errores en la validación de entradas, lo que permite a un atacante ejecutar código arbitrario en la máquina víctima.

Descripción del Ataque

Paso 1: Escaneo de Vulnerabilidades. El atacante, utilizando Kali Linux, identifica la versión de la aplicación Rejetto en la máquina víctima. Esto puede hacerse utilizando herramientas como nmap y Metasploit para determinar que la versión de la aplicación es vulnerable.

Paso 2: Exploit de la Vulnerabilidad. La vulnerabilidad en Rejetto v.2.3 permite a un atacante enviar una solicitud maliciosa que sobrescribe la memoria del programa (Jaswal, 2020). Esto suele ser un desbordamiento de búfer, donde la entrada proporcionada por el atacante sobrescribe las variables de control en la memoria, permitiendo que el atacante ejecute comandos arbitrarios**.**

Paso 3: Compromiso de la Máquina. El atacante, al aprovechar esta vulnerabilidad, puede ejecutar comandos maliciosos en el sistema, como obtener una shell o incluso escalar

privilegios si es posible. Sí el atacante no tiene privilegios elevados, puede intentar ejecutar un exploit adicional para obtener acceso como administrador o SYSTEM.

Paso 4: Creación de un Usuario con Privilegios Administrativos. Después de obtener acceso a la máquina, el atacante puede crear un usuario con privilegios administrativos, como "Matios Maury", usando comandos de sistema como net user para añadir el nuevo usuario al grupo de administradores.

Paso 5: Control Total Sobre la Máquina. Con el nuevo usuario administrador, el atacante puede realizar cualquier acción en la máquina víctima, como instalar software, robar datos.

3. Impacto en la Máquina Víctima. Una vez que el atacante obtiene acceso, la máquina víctima se ve afectada de varias formas:

***Pérdida de Control del Sistema*.** El atacante tiene acceso completo al sistema, lo que puede permitir la ejecución de comandos, el robo de archivos sensibles, y la manipulación de datos.

***Escalación de Privilegios*.** Si el atacante no tiene privilegios elevados, puede utilizar el sistema para elevar sus privilegios, obteniendo control total.

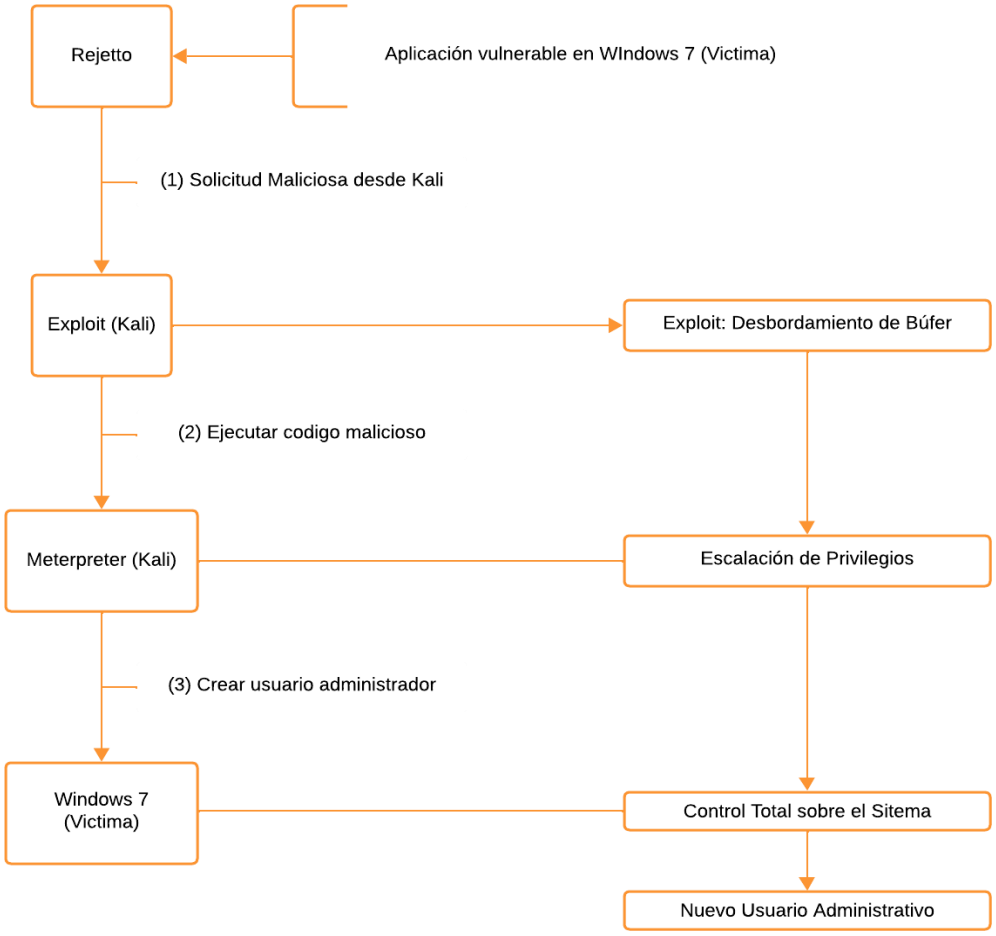
***Instalación de Malware*.** El atacante puede instalar malware para mantener el acceso o para propagarse dentro de la red.

***Exfiltración de Datos Sensibles*.** Si la máquina contiene información sensible, el atacante puede robarla o enviarla a servidores de comando y control (C&C).

Acceso a Recursos de Red. Al obtener privilegios elevados, el atacante puede utilizar la máquina para atacar otros sistemas dentro de la red local.

Figura 18

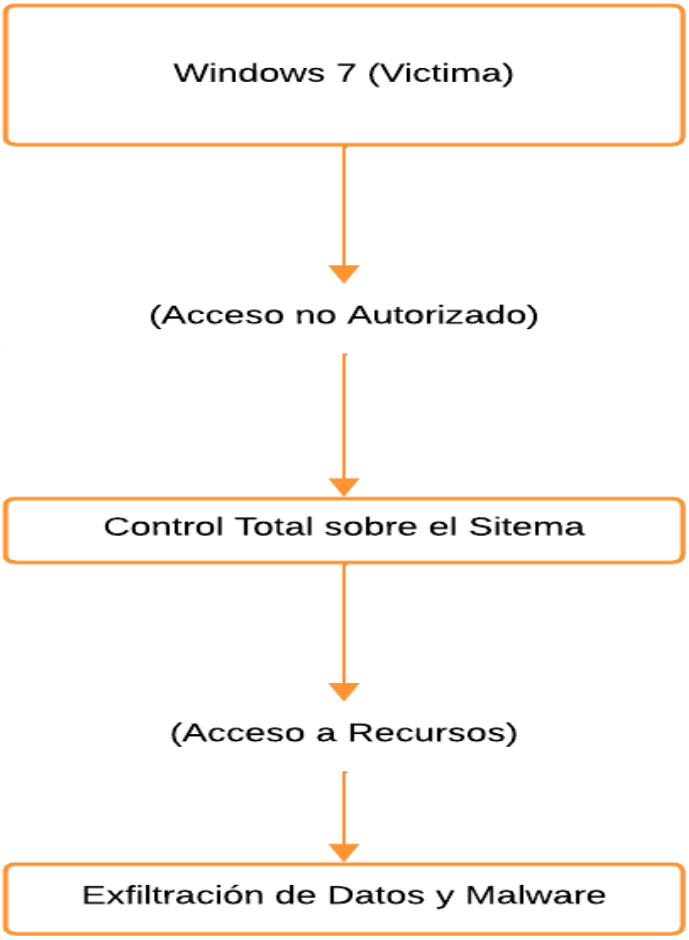
Diagrama 01: Flujo del Ataque



Nota. Elaboración propia.

Figura 19

Diagrama 02: Impacto en la Maquina (Windows)



Nota. Elaboración propia.

Primaeras Acciones en un Ataque en Tiempo Real

Si me encontrara ante un ataque en tiempo real, lo primero que indagaría y haría sería:

Identificación del Tipo de Ataque y Contención Inicial

Razón Técnica. Es crucial identificar rápidamente el tipo de ataque (ransomware, DoS, malware, etc.) para determinar las acciones inmediatas (Danquah, 2020). Esta información se puede obtener observando patrones de tráfico anómalo, comportamientos inusuales en el sistema, o analizando alertas del sistema de detección de intrusos (IDS) o firewall.

Acción. Revisar los logs del sistema operativo y del firewall en busca de anomalías, como conexiones inusuales, procesos desconocidos o picos de actividad.

Aislar el Sistema Comprometido

Razón Técnica. Si el sistema comprometido sigue conectado a la red, el ataque podría propagarse a otros sistemas (Connor, McDaniel, Smith, & Schuchard, 2020). Por lo tanto, se debe desconectar la máquina afectada para mitigar el impacto inicial.

Acción. Usar comandos básicos como ipconfig /release (Windows) o deshabilitar la tarjeta de red para cortar la conexión de manera segura (Choi, 2024).

Inspección de Procesos Activos

Razón Técnica. Un ataque puede involucrar procesos maliciosos en ejecución. Identificarlos puede proporcionar pistas críticas sobre el vector de ataque (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin, 2023).

Acción. Ejecutar el comando tasklist o herramientas como Process Hacker (licencia GPL) para revisar procesos sospechosos.

Análisis de Logs del Sistema Operativo

Razón Técnica. Los eventos registrados en los logs pueden indicar cómo comenzó el ataque y qué recursos están siendo explotados (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin, 2023).

Acción. Revisar los eventos en el Visor de Eventos de Windows, centrándose en:

Seguridad. Intentos de inicio de sesión fallidos o exitosos.

Sistema. Errores críticos o comportamientos anormales.

Aplicaciones. Fallos o ejecuciones no autorizadas.

Revisión de la Red y Conexiones Activas

Razón Técnica. Un ataque en tiempo real puede implicar comunicación con servidores externos (C2). Analizar el tráfico ayuda a identificar IPs sospechosas y bloquearlas (Kim, Park, & Lee, 2020).

Acción. Usar herramientas como Wireshark para capturar paquetes y netstat para identificar conexiones activas sospechosas.

Establecimiento de un Plan de Contención

Razón Técnica. Una vez entendido el ataque, se deben implementar medidas inmediatas para contenerlo (como deshabilitar servicios, bloquear IPs, cerrar puertos específicos).

Acción. Aplicar políticas en el firewall y configurar reglas adicionales en la red para detener el ataque.

El enfoque inicial debe priorizar contener el ataque para evitar más daño. Herramientas GPL como Wireshark, Sysinternals Suite (gratis, aunque no GPL), y Process Hacker son críticas para diagnosticar y mitigar rápidamente los efectos.

Medidas de Hardenización Propuestas

Para mitigar y prevenir futuros ataques como el ejecutado con Rejetto HTTP File Server (HFS), es crucial implementar medidas de hardening tanto a nivel del sistema operativo como de la aplicación vulnerable. De acuerdo a la descripción de CVE:

CVE-2014-6287. La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (aks HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda (CVE Mitre, 2024). Teniendo en cuenta lo anterior, las propuestas incluyen:

Actualización y Parcheo del Software

Medida. Actualizar HFS a su versión más reciente (si aplica) o reemplazarlo por un servidor de archivos más seguro y actualizado.

Razón. La versión explotada probablemente contenía vulnerabilidades conocidas que se solucionan en actualizaciones posteriores.

Uso de un Firewall y Restricciones de Acceso

Medida. Configurar un firewall para limitar el acceso al puerto utilizado por HFS (por defecto, el puerto 80). Permitir conexiones solo desde direcciones IP específicas o rangos confiables.

Razón. Restringir el acceso al servidor minimiza la exposición a actores no autorizados.

Implementación de Autenticación Robusta

Medida. Activar autenticación mediante contraseñas seguras para acceder al servidor y deshabilitar el acceso anónimo.

Razón. El uso de credenciales débiles facilita el acceso no autorizado.

Uso de certificados SSL/TLS

Medida. Configurar HFS para aceptar solo conexiones HTTPS en lugar de HTTP.

Razón. El cifrado HTTPS previene ataques de intercepción y asegura que las comunicaciones entre clientes y el servidor sean seguras.

Deshabilitar Funciones Innecesarias

Medida. Revisar la configuración de HFS para deshabilitar funciones no necesarias (por ejemplo, ejecución de scripts). Eliminar scripts o configuraciones predeterminadas que puedan ser explotadas.

Razón. Las funcionalidades no utilizadas pueden ser vectores de ataque.

Implementación de Políticas de Acceso al Sistema

Medida. Ejecución del HFS bajo una cuenta con privilegios mínimos. Deshabilitar cuentas de administrador innecesarias en el sistema operativo.

Razón. Limitar privilegios evita que los atacantes tomen control total del sistema en caso de explotación.

Monitoreo y Detección de Anomalías

Medida. Implementar un sistema de detección de intrusos (IDS) o monitoreo del tráfico con herramientas como Suricata o Snort.

Razón. Detectar actividades sospechosas (como intentos de explotación o tráfico anómalo) en tiempo real.

Deshabilitar el Uso de HFS sí no es Necesario

Medida. Sustituir HFS por un software más moderno y con soporte activo.

Razón. Si no es absolutamente necesario, eliminar aplicaciones heredadas y vulnerables elimina riesgos innecesarios.

Capacitación del Personal

Medida. Capacitar a los administradores sobre los riesgos asociados con el uso de software vulnerable y cómo configurar aplicaciones de forma segura.

Razón. Un personal capacitado es más consciente de las amenazas y puede prevenir configuraciones inseguras.

Auditorías de Seguridad Periódicas

Medida. Realizar análisis regulares de vulnerabilidades con herramientas como OpenVAS o Nessus (versión gratuita).

Razón. Esto asegura que no existan vulnerabilidades conocidas sin mitigar.

Diferencias Entre un Blue Team y CSIRT

Un equipo Blue Team y un equipo de respuesta a incidentes informáticos tienen roles complementarios dentro de la ciberseguridad, pero difieren en su enfoque, responsabilidades y momentos de acción (Chindrus & Constantin-Florin, 2023).

Blue Team: Proactivo y Defensivo

La tenacidad de Blue Teams se demuestra a través de la detección proactiva de amenazas, la contención rápida de incidentes y la fortificación de perímetros digitales (Chindrus & Constantin-Florin, 2023).

Rol. Se encarga de proteger y reforzar la seguridad de los sistemas y redes de una organización.

Enfoque. Implementar medidas de seguridad preventivas. Monitorear sistemas y redes para detectar actividades sospechosas o anomalías. Evaluar vulnerabilidades y aplicar configuraciones seguras (hardening). Diseñar estrategias para minimizar riesgos. El Blue Team opera de manera constante, asegurando que las defensas estén actualizadas y sean efectivas.

Ejemplo. Configurar firewalls, implementar políticas de acceso, y realizar auditorías periódicas.

Equipo de Respuesta a Incidentes: Reactivo y Estratégico

La respuesta a incidentes tiene lugar bajo una presión de tiempo considerable en un entorno organizacional dinámico y rápidamente cambiante con altos niveles de carga de información, diversidad de información e incertidumbre de tareas. La respuesta a incidentes requiere el comando, control y coordinación de diversas personas, procesos y tecnologías para desarrollar la conciencia de la situación del entorno de amenazas e incidentes dentro de un contexto organizacional en rápida evolución (Atif, y otros, 2021).

Rol. Actúa específicamente cuando ocurre un incidente de seguridad, para contenerlo, investigarlo y mitigar sus impactos.

Enfoque. Contener el ataque en tiempo real para limitar el daño. Investigar la causa raíz del incidente para entender cómo ocurrió. Proveer recomendaciones para prevenir futuros incidentes similares. Coordinar con equipos internos y externos (como reguladores o fuerzas del orden) si es necesario. Su actividad se centra en manejar un incidente particular y se activa cuando ocurre una brecha de seguridad.

Ejemplo. Contener un ataque de ransomware, investigar una intrusión, o recuperar datos comprometidos.

Tabla 1

Blue Team vs Equipo de Respuesta a Incidentes (CSRIT)

Aspecto	Blue Team	CSIRT
Momento de acción	Antes y durante un posible incidente.	Durante y después de un incidente.
Enfoque principal	Prevención, monitoreo, y defensa.	Contención, análisis, y recuperación.
Rol reactivo o proactivo	Proactivo: Minimizar riesgos futuros.	Reactivo: Resolver y mitigar daños.
Duración del trabajo	Continuo y estratégico.	Temporal y basado en incidentes.

Nota. Tabla de creación propia.

Ambos equipos son esenciales para una estrategia de ciberseguridad sólida. El Blue Team actúa como una barrera defensiva, mientras que el equipo de respuesta a incidentes interviene cuando esa barrera es superada, restaurando la normalidad y aprendiendo del ataque para mejorar la defensa futura.

Uso e Importancia de Trabajar con CIS (Center for Internet Security)

El Center for Internet Security (CIS) proporciona recursos y guías ampliamente reconocidas en la industria de la ciberseguridad, que son esenciales para un equipo Blue Team (Ramezan, 2023). Si se me indicara trabajar con CIS, lo utilizaría para los siguientes fines:

Implementación de Benchmarking de Seguridad

Permite a las organizaciones comparar sus prácticas, políticas y configuraciones de seguridad con estándares reconocidos o con otras organizaciones líderes en el sector (Anastasova, Azarderakhsh, & Kermani, 2021).

Uso. Aplicar los CIS Benchmarks, que son guías detalladas de configuración segura para sistemas operativos, aplicaciones y dispositivos de red.

Propósito. Asegurar que los sistemas cumplan con configuraciones seguras recomendadas por expertos, reduciendo vulnerabilidades comunes.

Ejemplo. Configurar políticas de grupo (GPO) en Windows siguiendo los Benchmarks de CIS para endurecer contraseñas, accesos y permisos.

Auditorías de Seguridad

Estas auditorías permiten detectar y corregir deficiencias antes de que sean explotadas por atacantes, fortaleciendo así la postura de seguridad. En escenarios como los ataques en tiempo real, las auditorías también son fundamentales para prevenir futuras intrusiones y minimizar riesgos (Antunes, Maximiano, & Gomes, 2022).

Uso. Evaluar la conformidad de los sistemas con las mejores prácticas de seguridad mediante herramientas como CIS-CAT (CIS Configuration Assessment Tool).

Propósito. Identificar configuraciones deficientes o incumplimientos que puedan ser explotados por atacantes.

Ejemplo. Analizar servidores Windows o Linux para verificar que no tengan puertos o servicios innecesarios habilitados.

Priorización de Controles Esenciales

En el contexto de la ciberseguridad es vital para enfocarse en medidas clave que ofrezcan la mayor protección contra amenazas comunes y avanzadas (Alghassab, 2021).

Uso. Implementar los CIS Controls (anteriormente conocidos como CSC, Critical Security Controls).

Propósito. Aplicar un enfoque sistemático y priorizado para mejorar la seguridad en la organización.

Ejemplo. Inventariar activos y software (CIS Control 1 y 2). Monitorear y controlar accesos administrativos (CIS Control 4).

Formación y Capacitación

En escenarios críticos, como ataques en tiempo real, un personal capacitado puede tomar decisiones rápidas y efectivas, minimizando el impacto del incidente y protegiendo los activos organizacionales (Mendivil, Sanz, & Gutierrez, 2022).

Uso. Utilizar los recursos educativos y guías de CIS para capacitar al equipo sobre configuraciones seguras y mejores prácticas.

Propósito. Aumentar el nivel de conocimiento técnico del equipo y alinear sus esfuerzos con estándares reconocidos.

Ejemplo. Formar al equipo sobre cómo implementar políticas de seguridad en servidores basadas en Benchmarks.

Fortalecimiento de la Resiliencia Organizacional

Asegurar la continuidad operativa, la confianza de los clientes y el cumplimiento de normativas (Mendivil, Sanz, & Gutierrez, 2022).

Uso. Adoptar guías de respuesta ante incidentes o medidas de seguridad recomendadas en entornos críticos.

Propósito. Preparar y reforzar la postura defensiva de la organización contra amenazas emergentes.

Ejemplo. Aplicar controles avanzados de monitoreo en endpoints según los Benchmarks y Controls de CIS.

Beneficio Técnico

El uso de los recursos de CIS garantiza un enfoque estructurado, basado en estándares reconocidos, para mejorar la seguridad de la organización, mitigando riesgos comunes y facilitando la conformidad con regulaciones de la industria.

Conclusión

Dentro de un equipo Blue Team, el CIS sería una herramienta esencial para implementar configuraciones seguras, realizar auditorías, y priorizar medidas de defensa que refuercen la ciberseguridad organizacional.

Las Funciones y Características Principales de lo que es un SIEM

Un SIEM (Security Information and Event Management) es una herramienta clave en la ciberseguridad moderna, diseñada para recopilar, correlacionar y analizar eventos de seguridad generados por sistemas y dispositivos en una red. Su objetivo principal es mejorar la visibilidad, detección y respuesta ante amenazas de seguridad (González-Granadillo, González-Zarzosa, & Diaz, 2021).

Funciones principales de un SIEM

Recopilación de Datos. Un SIEM reúne datos en tiempo real o históricos provenientes de múltiples fuentes, como firewalls, sistemas operativos, aplicaciones, servidores, y dispositivos de red.

***Ejemplo*.** Logs de acceso, eventos de sistema y tráfico de red.

Correlación de Eventos. Analiza y relaciona eventos aparentemente independientes para identificar patrones sospechosos o amenazas.

***Ejemplo*.** Si un usuario intenta múltiples inicios de sesión fallidos y poco después accede a datos sensibles, el SIEM lo detecta como actividad anómala.

Monitoreo y Alertas. Supervisa la actividad de la red en tiempo real y genera alertas cuando detecta comportamientos que coinciden con reglas predefinidas o patrones de ataque.

***Ejemplo*.** Alertar sobre intentos de explotación de vulnerabilidades conocidas.

Análisis Forense. Almacena y organiza eventos históricos para permitir investigaciones detalladas sobre incidentes de seguridad.

***Ejemplo*.** Determinar cómo ocurrió una intrusión y qué sistemas se vieron afectados.

Cumplimiento Normativo. Ayuda a las organizaciones a cumplir regulaciones de seguridad (como GDPR, HIPAA, o PCI DSS) al mantener registros detallados de eventos y auditorías.

***Ejemplo*.** Generar reportes automáticos que demuestren la conformidad con normativas.

Gestión Centralizada. Centraliza los datos de seguridad de toda la infraestructura en una sola plataforma, lo que facilita la gestión de incidentes y la colaboración entre equipos.

***Ejemplo*.** Integrar eventos de múltiples servidores y dispositivos en un único panel de control.

Características Principales de un SIEM

Compatibilidad Multiplataforma. Debe ser capaz de recopilar datos de diversos sistemas, como Windows, Linux, firewalls, y dispositivos IoT.

Escalabilidad. Capacidad para manejar grandes volúmenes de datos, adaptándose al crecimiento de la organización.

Análisis Avanzado. Utilización de tecnologías como inteligencia artificial (IA) y aprendizaje automático para detectar amenazas avanzadas o desconocidas.

Automatización. Puede responder automáticamente a ciertos incidentes mediante la ejecución de scripts o el bloqueo de usuarios o direcciones IP sospechosas.

Interfaz Intuitiva. Ofrece dashboards y reportes claros y personalizables que permiten a los equipos tomar decisiones rápidamente.

Beneficios Clave de un SIEM

Visibilidad. Permite obtener una visión integral de la seguridad de la organización.

Detección Proactiva. Identifica amenazas antes de que causen daños significativos.

Eficiencia. Reduce el tiempo necesario para identificar y responder a incidentes.

Colaboración. Mejora la coordinación entre equipos de ciberseguridad.

Ejemplos de SIEM Populares

Open Source. Wazuh, Elastic Stack (ELK), OSSEC.

Comerciales. Splunk, IBM QRadar, ArcSight, LogRhythm.

El SIEM es una herramienta esencial para proteger redes y sistemas al centralizar y analizar datos de seguridad. Su capacidad para detectar amenazas y facilitar el análisis forense lo convierte en una pieza clave en la estrategia de defensa cibernética.

Tres Herramientas para Contener Ataques Informáticos

Las herramientas de contención de ataques informáticos se utilizan para mitigar, limitar o detener un ataque una vez detectado, protegiendo los activos de la organización y evitando daños adicionales. Estas herramientas pueden ser de hardware o software, y están diseñadas para actuar directamente sobre el ataque en tiempo real. A continuación, se describen tres ejemplos:

Firewall

Los firewalls se consideran la primera línea de defensa para proteger las redes inteligentes y abordar los desafíos de la ciberseguridad. Los firewalls se aplican en diferentes niveles en las redes y varían desde los firewalls convencionales basados en servidores hasta los firewalls basados en la nube (Anwar, Abdullah, & Pastore, 2021).

Tipo. Hardware y software.

Función. Controla el tráfico entrante y saliente de la red, permitiendo o bloqueando conexiones según reglas predefinidas.

Modo de Contención. Bloquear direcciones IP o rangos sospechosos. Restringir accesos a puertos vulnerables o específicos. Implementar reglas dinámicas para detener conexiones anómalas o maliciosas.

Ejemplo. Un ataque DDoS puede ser contenido al bloquear el tráfico proveniente de las fuentes identificadas como maliciosas.

Endpoint Detection and Response (EDR) con Capacidades de Contención

Las soluciones de detección y respuesta de puntos finales (EDR) agregan una capa adicional de protección para evitar que una acción de punto final se convierta en una brecha. EDR es la principal herramienta de detección y respuesta de la región que combina datos de

punto final y de red para reconocer y responder a amenazas sofisticadas (Arfeen, Saad, Khan, & Jafri, 2021).

Tipo. Software.

Función. Aunque su principal rol es la detección, un EDR avanzado incluye capacidades de contención para mitigar ataques en dispositivos finales.

Modo de Contención. Aislar automáticamente un endpoint infectado del resto de la red. Terminar procesos maliciosos en ejecución. Bloquear archivos sospechosos antes de que se propaguen.

Ejemplo. En caso de un ransomware, el EDR puede contener el ataque al desconectar la máquina comprometida del resto de la red y detener la encriptación de archivos.

***Network Access Control (NAC)* Tipo:**

Hardware y software.

Función: Regula y restringe el acceso a la red con base en políticas de seguridad, limitando la actividad de dispositivos no autorizados o comprometidos.

Modo de Contención. Denegar acceso a dispositivos no autorizados. Aislar segmentos de red comprometidos para contener el ataque.Aplicar políticas específicas según el nivel de riesgo detectado.

Ejemplo. Si se detecta un dispositivo comprometido, el NAC puede moverlo automáticamente a una red aislada o restringir sus permisos de acceso.

Otras Herramientas de Contención Comunes

IPS (Intrusion Prevention System). Bloquea automáticamente tráfico identificado como malicioso.

Sandboxing. Detiene la ejecución de archivos sospechosos aislándolos en un entorno controlado.

Switch con Capacidades de Contención. Permite deshabilitar o aislar puertos físicos específicos en caso de actividad anómala.

Las herramientas de contención no solo mitigan los impactos inmediatos de un ataque, sino que también ayudan a preservar la integridad de los sistemas mientras se implementan soluciones permanentes. Su función es esencial para proteger activos críticos durante un incidente de seguridad.

Aspectos que Aporten al Desarrollo de Estrategias de Red Team & Blue Team

Estrategias de Red Team

Reconocimiento Avanzado. Realizar análisis OSINT (Open Source Intelligence) para identificar vectores de ataque menos evidentes. Mapear la infraestructura utilizando herramientas como Nmap y Nessus para descubrir activos vulnerables.

Uso de Exploits Personalizados. Desarrollar o adaptar exploits específicos según las vulnerabilidades detectadas en el entorno objetivo. Implementar payloads ofuscados para evitar la detección por sistemas de seguridad.

Simulación de Ataques en Cadena. Ejecutar ataques que combinen phishing, escalación de privilegios y movimientos laterales dentro de la red, emulando actores avanzados.

Persistencia en Sistemas Comprometidos. Desplegar backdoors discretos y aprovechar técnicas como DLL hijacking o registro de tareas programadas.

Evaluación de Respuesta del Blue Team. Registrar y analizar la detección y contención del Blue Team durante ejercicios controlados.

Estrategias de Blue Team

Fortalecimiento del Monitoreo. Implementar herramientas de SIEM como Splunk o ELK para centralizar la detección de incidentes. Configurar alertas en tiempo real para actividades inusuales, como cambios en cuentas privilegiadas.

Gestión de Parches y Configuraciones. Asegurar que todos los sistemas estén actualizados con las últimas correcciones de seguridad. Realizar auditorías regulares para identificar configuraciones inseguras o no autorizadas.

Respuesta a Incidentes en Tiempo Real. Definir y practicar planes de respuesta ante incidentes, asegurando roles claros dentro del equipo. Utilizar técnicas de contención rápida, como aislar dispositivos comprometidos de la red.

Simulaciones Regulares. Organizar ejercicios de ataque simulado (tabletop o live-fire) para evaluar la preparación y mejorar tiempos de respuesta.

Educación y Concienciación. Ofrecer entrenamientos regulares para detectar amenazas comunes como phishing. Involucrar a todos los niveles de la organización en las mejores prácticas de ciberseguridad.

Integración Entre Ambos Equipos

Colaboración en Simulacros. Realizar ejercicios de Red vs. Blue con retroalimentación conjunta.

Intercambio de Inteligencia. Compartir hallazgos sobre tácticas, técnicas y procedimientos (TTPs) de atacantes.

Adopción de Purple Team. Combinar esfuerzos para mejorar defensas y técnicas ofensivas simultáneamente.

Recomendaciones para Endurecer la Seguridad en una Organización

Fortalecimiento de Infraestructura Técnica

Segmentación de Red. Implementar zonas de seguridad (DMZ, red interna y red pública) para minimizar el impacto de posibles ataques.

Gestión de Parches. Establecer un proceso regular de actualización de software y sistemas operativos para corregir vulnerabilidades conocidas.

Control de Acceso. Adoptar el principio de menor privilegio (PoLP) y usar autenticación multifactor (MFA) en todos los accesos críticos.

Endurecimiento de Sistemas. Deshabilitar servicios y puertos no utilizados, además de implementar políticas estrictas de contraseñas.

Monitorización y Respuesta a Incidentes

Implementación de SIEM. Utilizar soluciones como Splunk, Elastic Stack o Wazuh para centralizar la detección y correlación de eventos de seguridad.

Análisis de Comportamiento. Establecer herramientas basadas en machine learning que detecten actividades inusuales en tiempo real.

Resiliencia Ante Ataques. Diseñar un plan de recuperación ante desastres (DRP) y planes de continuidad operativa (BCP) que incluyan respaldos regulares y pruebas periódicas.

Cultura de Seguridad Organizacional

Capacitación Continua. Ofrecer programas regulares de formación en ciberseguridad para empleados, adaptados a las amenazas emergentes.

Simulaciones de Ataques. Realizar simulacros de phishing y ejercicios Red Team para evaluar y mejorar la respuesta organizacional.

Políticas Claras. Crear y mantener políticas de seguridad, como BYOD (Bring Your Own Device), uso aceptable de internet y gestión de datos sensibles.

Pruebas Regulares de Vulnerabilidades

Análisis de Vulnerabilidades. Programar escaneos automáticos y manuales periódicos para identificar puntos débiles en sistemas y aplicaciones.

Penetration Testing. Contratar expertos para realizar pruebas de penetración orientadas a simular posibles ataques.

Validación de Parches. Verificar que las actualizaciones implementadas no generen nuevas vulnerabilidades.

Protección Contra Amenazas Internas

Monitoreo de Usuarios Privilegiados. Supervisar la actividad de cuentas con acceso administrativo.

Detección de Insiders. Implementar soluciones de DLP (Data Loss Prevention) para identificar y bloquear intentos de fuga de datos.

Revisión de Accesos. Realizar auditorías periódicas para asegurar que los usuarios tienen los permisos adecuados.

Colaboración y Mejora Continua

Adopción de Frameworks Reconocidos. Seguir estándares como ISO 27001, NIST Cybersecurity Framework o CIS Controls.

Evaluaciones Externas. Participar en auditorías independientes para obtener perspectivas imparciales sobre la postura de seguridad.

Purple Team. Fomentar la colaboración entre equipos Red y Blue para optimizar defensas y técnicas de detección.

Conclusiones

La interconexión aumenta los riesgos de seguridad, debdo a esto la necesidad de las organizaciones de conectarse a internet expone su información sensible a ataques internos y externos, lo que hace imprescindible la implementación de estrategias de ciberseguridad robustas.

Las estrategias del Red Team y Blue Team, tienen un enfoque que permite evaluar y fortalecer la seguridad mediante la simulación de ataques reales y la optimización de respuestas, siendo clave para identificar y mitigar vulnerabilidades.

La cultura de seguridad organizacional, es la capacitación constante, simulaciones de incidentes y concienciación del personal son esenciales para prevenir y responder eficazmente a ciberataques.

La legislación y certificaciones en Colombia, la Ley 1273 de 2009 necesita ajustes para abordar vacíos legales. Las certificaciones en ciberseguridad son fundamentales, pero deben complementarse con enfoques integrales.

El fortalecimiento continuo de la seguridad en las acciones como la segmentación de redes, el monitoreo activo y la gestión de parches fortalecen la protección frente a amenazas. La integración de Red Team y Blue Team asegura mejoras constantes en la postura de seguridad.

Bibliografía

Abdelrazek, S., Mammi, H., & Din, M. (2021). Privilege Escalation Focused Offensive Security Training Platform. *2021 International Conference on Data Science and Its Applications (ICoDSA)* (págs. 169-174). Bandung, Indonesia: IEEE.

Akpinar, M., Fatih, A., & Guvenc, G. (2021). SVM-based anomaly detection in remote working: Intelligent software SmartRadar. *Applied Soft Computing, vol. 109*, 107457.

Alghassab, M. (2021). Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. *Energies, vol. 15, no 1*, 218.

Alonso, J. (30 de Mayo de 2023). *Hacking Ético y prueba de penetración.* Obtenido de Vsistemas: https://www.vsistemas.es/2023/05/30/hacking-etico-en-seguridad-por-vsistemas/

Anastasova, M., Azarderakhsh, R., & Kermani, M. (2021). Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4. *IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no 10*, 4129-4141.

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. *A client-centered information security and cybersecurity auditing framework. Applied Sciences, vol. 12, no 9*, 4102.

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. *Applied Sciences, vol. 11, no 19*, 9183.

Arfeen, A., Saad, A., Khan, M., & Jafri, S. (2021). Arfeen, Asad; Saad, Ahmed; Khan, Muhammad; Jafri, Syed . *2021 International Conference on Cyber Warfare and Security (ICCWS)* (págs. 1-8). Islamabad, Pakistán: IEEE.

Aslan, Ö., Aktuğ, S., Ozkan-Okay, M., Yilmaz, A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics, vol. 12, no 6,* 1333.

Atif, A., Maynard, S., Desouza, K., Kotsias, J., Whitty, M., Baskerville, & Richard. (2021). ow can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security, vol. 101,* 102-122.

Baten, M. A. (2020). Basic Understanding of Fraudulent Activities in Corporate Organisation. *Review of Business, Accounting, & Finance, vol. 1, no 01,* 1-13.

Bodie, M. (2022). The law of employee data: privacy, property, governance. *ndiana Law Journal: Vol. 97: Iss. 2, Article 7.,* 706-754.

Chiluiza, L., & & Enciso, L. (2023). Detección y solución de vulnerabilidades con Greenbone Security Assistant. *Revista Ibérica de Sistemas e Tecnologias de Informação, no E57,* 560-570.

Chindrus, C., & Constantin-Florin, C. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. *Information, vol. 14, no 11,*, 587.

Choi, B. (2024). Linux Fundamentals II–TCP/IP Services. En B. Choi, *Introduction to Python Network Automation Volume I-Laying the Groundwork: The Essential Skills for Growth.* (págs. 475-559). Berkeley, California, E.E.U.U.: Apress.

Código Sustantivo del Trabajo. (2024, 14 de Octubre). *Artículo 62. Terminacion del contrato por justa causa.* (Diario Oficial No. 52.869. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/codigo_sustantivo_trabajo_pr001.html

Congreso de la República de Colombia. (1999, 18 de Agosto). *Ley 527 de 1999.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

Congreso de la República de Colombia. (2008, 31 de Diciembre). *Ley 1266 de 2008.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. (2009, 5 de Enero). *Ley 1273 de 2009.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012, 17 de Octubre). *Ley 1581 de 2012.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Connor, E., McDaniel, T., Smith, J., & Schuchard, M. (2020). PKU Pitfalls: Attacks on PKU-based Memory Isolation Systems. *29th USENIX Security Symposium (USENIX Security 20)* (págs. 1409-1426). Berkeley, California, United States: USENIX Association.

Constitución Política de la República de Colombia 1991. (2024, 4 de Septiembre). *Articulo 30.* Gaceta Constitucional. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

COPNIA. (2015). *Codigo de Ética: Para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.* Bogotá, Cundinamarca, Colombia: COPNIA (Consejo Profesional Nacional de Ingeniería). Obtenido de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Coronel, I., & Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE (RCTU), vol. 9, no 2*, 97-109.

Costantino, G., & Mattucci, I. (2019). CANDY CREAM-hacking infotainment android systems to command instrument cluster via can data frame. *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)* (págs. 476-481). New York: IEEE .

Couretas, J. (2022). Cyber security and defense for analysis and targeting. *An Introduction to Cyber Analysis and Targeting*, 119-150.

CVE Mitre. (21 de 11 de 2024). *CVE*. Obtenido de CVE-2014-6287: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

Danquah, P. (2020). Security operations center: a framework for automated triage, containment and escalation. *Journal of Information Security, vol. 11, no 4*, 225-240.

Díaz, G. (2019). Detección de Intrusos con la Plataforma Open Source Snort. *NEXOS CIENTÍFICOS-ISSN 2773-7489, vol. 3, no 2*, 20-27.

Díaz-Cacho, M., Chaves, A., & Pereira, A. (2023). Control de acceso remoto a redes industriales. . *XLIV Jornadas de Automática.* (págs. 795-800). Zaragoza, España: Universidade da Coruña. Servizo de Publicacións.

El Congreso de la República de Colombia. (2000, 24 de Julio). *LEY 599 DE 2000.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388#:~:text=Prohibici%C3%B3n%20de%20doble%20incriminacion.,establecido%20en%20los%20instrumentos%20internacionales.

El Congreso de la República de Colombia. (2003, 09 de Octube). *LEY 842 DE 2003.* Gaceta Oficial del Congreso. Obtenido de https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

El Congreso de la República de Colombia. (2009, 05 de Enero). *Ley 1273 de 2009.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

El Congreso de la República de Colombia. (2012, 17 de Octubre). *Ley 1581 de 2012.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Fajardo, G., Montaño, D., Donado, S., & Villalba, K. (2019). Pruebas de concepto automatizado sobre aplicaciones web utilizando Raspberry Pi. *Revista Ibérica de Sistemas e Tecnologias de Informação, no E17*, 648-659.

Fenster, M. (2024). How Reputational Nondisclosure Agreements Fail (Or, In Praise of Breach). *Marquette Law Review, Vol. 107, No. 2*, 325-397.

Gautam, A. (2023). The evaluating the impact of artificial intelligence on risk management and fraud detection in the banking sector. *AI, IoT and the Fourth Industrial Revolution Review, vol. 13, no 11*, 9-18.

Giannone, A., Amatriain, H., Rodríguez, D., & Merlino, H. (2018). Método de inclusión de Hacking ético en el proceso de testing de software. *XXIV Congreso Argentino de Ciencias de la Computación - CACIC 2018* (págs. 542-551). Buenos Aires: UNICEN.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors, vol. 21, no 14*, 47-59.

Jaswal, N. (2020). *Mastering Metasploit: Exploit systems, cover your tracks, and bypass security controls with the Metasploit 5.0 framework. .* Birmingham, Reino Unido: Packt Publishing Ltd.

Kekül, H., Ergen, B., & Arslan, H. (2022). Comparison and analysis of software vulnerability databases. *International Journal of Engineering and Manufacturing, vol. 12, no 4,* 1-14.

Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of deep learning to real-time Web intrusion detection. *IEEE Access, vol. 8,* 70245-70261.

Kljajić, M., Kostić, Marija, & Mizdraković, V. (2021). The blacklist of legal entities: The importance of administrative authorities in creating a favourable business environment in the Serbian market. *NBP. Nauka, bezbednost, policija, vol. 26, no 3,* 49-67.

Laprovittera, C. (20 de Diciembre de 2023). *Guía de Hacking y Pentesting – Capítulo 7: Detección y vulnerabilidades y escalada de privilegios.* Obtenido de Álvaro Chirou: https://achirou.com/guia-de-hacking-y-pentesting-capitulo-7-deteccion-y-vulnerabilidades-y-escalada-de-privilegios/

Marquis, Y. A. (2024). From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts. *Journal of Engineering Research and Reports, vol. 26, no 5,* 138-154.

Martínez-Sanchez, P., Nespoli, P., Garcia-alfaro, J., & Gómez, F. (2023). Metodología para automatizar agentes atacantes en plataformas de entrenamiento Cyber Range. *HAL Open Science,* 437-444.

Mendivil, J., Sanz, B., & Gutierrez, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Pixel-Bit: Revista de Medios y Educación, 63,* 197-225.

Mimura, M., & Tajiri, Y. (2021). Static detection of malicious PowerShell based on word embeddings. *Internet of Things, vol. 15*, 100404.

Naqvi, G., & Sultan, H. (2022). Ethical Hacking and its Necessity in the Society. *resmilitaris, vol. 12, no 6*, 1634-1638.

Prado, J. P. (2021). Ingeniería social, un ejemplo práctico. *Revista Odigos, vol. 2, no 3*, 47-76.

Presidencia de la República de Colombia. (2015, 6 de Mayo). *Decreto 1078 de 2015.* Gaceta Oficial del Congreso. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

Raj, S., & Walia, N. K. (2020). A study on metasploit framework: A pen-testing tool. *2020 International Conference on Computational Performance Evaluation (ComPE). IEEE*, 296-302.

Ramezan, C. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. *Journal of Information Systems Education, vol. 34, no 1*, 94-105.

Romero, Y., Santiago, M., Pérez, J., Zenteno, A., Trinidad, G., & Martínez, R. (2023). La Importancia del Cómputo Forense en la Actualidad: The Importance of Computer Forensics in the Topicality. *Tecnología Educativa Revista CONAIC, vol. 10, no 1*, 42-48.

Safla, D. (2023). Vulnerabilidades en aplicaciones web utilizando la metodología de "proyecto abierto de seguridad de aplicaciones web". *Ciencia Ecuador, vol. 5, no 24*, 54-71.

Sahu, P., & Achraya, B. (2020). A Review Paper on Ethical Hacking. *International Journal of Innovative Research in Computer Science & Technology, vol. 11, no 12*, 163-168.

Suntaxi, K., Nasimba, J., Pallango, A., & Yaguarshungo, B. (2023). Mitigación y Previción de Ataques DDOS de tipo Slowloris en Entornos Virtualizados. *Revista de Ciencias de Seguridad y Defensa, vol. 8, no 04*, 89-99.

Syafrizal, M., Selamat, S., & Zakaria, N. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, vol. 12, no 3*, 417-432.

Tabassum, M., Mohanan, S., & Tripti, S. (2021). Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework. *International Journal of Innovation in Computational Science and Engineering, vol. 2, no 1*, 09-22.

Valea, O., & Ciprian, O. (2020). Towards pentesting automation using the metasploit framework. *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)* (págs. 171-178). Cluj-Napoca, Romania: IEEE.

Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability management models using a common vulnerability scoring system. *Applied Sciences, vol. 11, no 18*, 1-25.