CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Cristian Camilo Páez Nieto

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Sociales Artes y Humanidades ECSAH

Programa

2025

Tabla de Contenido

Lista de Figuras

Resumen

Este informe explora la sinergia estratégica entre el Red Team y el Blue Team en ciberseguridad, destacando su rol crucial en la protección organizacional. El Red Team simula ciberataques para identificar vulnerabilidades, mientras que el Blue Team defiende los sistemas, detectando y respondiendo a amenazas.

Se subraya que la interacción continua entre ambos equipos es esencial para fortalecer las defensas y mejorar las estrategias de seguridad. El estudio analiza los desafíos de esta colaboración, como las diferencias de enfoque y la necesidad de comunicación fluida.

Finalmente, se abordan los beneficios de una estrategia integrada, que permite una defensa más robusta y adaptada a las crecientes amenazas cibernéticas. Se enfatiza un ciclo de mejora constante, donde las lecciones de los ataques simulados optimizan las defensas del Blue Team, haciendo la ciberseguridad más efectiva y resiliente

Palabras clave: *Ciberseguridad, Red Team, Blue Team, Vulnerabilidades.*

Abstract

This report explores the strategic synergy between the Red Team and the Blue Team in cybersecurity, highlighting their crucial role in organizational protection. The Red Team simulates cyberattacks to identify vulnerabilities, while the Blue Team defends systems by detecting and responding to threats.

It emphasizes that continuous interaction between the two teams is essential to strengthening defenses and improving security strategies. The study analyzes the challenges of this collaboration, such as differences in approach and the need for fluid communication.

Finally, it addresses the benefits of an integrated strategy, which allows for a more robust defense adapted to growing cyber threats. It emphasizes a cycle of constant improvement, where lessons from simulated attacks optimize the Blue Team's defenses, making cybersecurity more effective and resilient.

Keywords: *Defense, Integration, Threats, Resilience.*

Glosario

Análisis de vulnerabilidades: Proceso de identificar debilidades en sistemas y aplicaciones que podrían ser explotadas por atacantes.

Ataques de phishing: Técnica de ingeniería social utilizada para engañar a las personas y obtener información confidencial, como contraseñas o datos bancarios.

Blue Team: Equipo de seguridad responsable de defender los sistemas y redes de una organización contra amenazas cibernéticas.

Ciberataques: Acciones maliciosas dirigidas a sistemas informáticos, redes o datos con el fin de causar daño, robar información o interrumpir servicios.

Ciberdefensa: Conjunto de estrategias y acciones destinadas a proteger los activos digitales de una organización contra amenazas cibernéticas.

Ciberseguridad: Prácticas y tecnologías diseñadas para proteger sistemas informáticos, redes y datos de ataques cibernéticos.

Ciclo de mejora continua: Proceso iterativo de evaluación y ajuste de estrategias de seguridad para adaptarse a las amenazas en evolución.

Defensas proactivas: Medidas de seguridad implementadas para prevenir ataques antes de que ocurran.

Defensas reactivas: Acciones tomadas para responder a incidentes de seguridad después de que ocurren.

Estrategias de seguridad: Planes y políticas diseñadas para proteger los activos digitales de una organización contra amenazas cibernéticas.

Hacking ético: Uso de técnicas de hacking para identificar vulnerabilidades en sistemas con el permiso del propietario.

Intrusión en sistemas: Acceso no autorizado a sistemas informáticos o redes.

Red Team: Equipo de seguridad responsable de simular ataques cibernéticos para identificar vulnerabilidades en los sistemas de una organización.

Respuestas a incidentes: Proceso de detección, análisis y contención de incidentes de seguridad.

Sinergia: Colaboración y cooperación entre equipos para lograr un objetivo común.

Vulnerabilidad: Debilidad en un sistema o aplicación que podría ser explotada por un atacante.

Introducción

Las organizaciones se enfrentan a un número creciente de amenazas cibernéticas, cada vez más sofisticadas y persistentes. La protección de datos y sistemas se ha convertido en una prioridad crítica, exigiendo estrategias de seguridad robustas y adaptativas. Este trabajo de grado se centra en la sinergia estratégica entre los equipos Red Team y Blue Team, actores clave en la ciberseguridad organizacional. El Red Team, a través de la simulación de ataques, identifica vulnerabilidades, mientras que el Blue Team se encarga de la defensa y respuesta a incidentes. La colaboración efectiva entre estos equipos es fundamental para fortalecer la postura de seguridad y mejorar la resiliencia ante las amenazas.

Este estudio analiza los desafíos y beneficios de la colaboración entre Red Team y Blue Team, destacando la importancia de un ciclo de mejora continua. Se exploran los roles, funciones y metodologías de cada equipo, así como el marco legal y normativo que rige la ciberseguridad. El objetivo es proponer estrategias que optimicen la interacción entre estos equipos, permitiendo una defensa más efectiva y una respuesta ágil ante los ataques. A través de este análisis, se busca resaltar cómo la sinergia entre Red Team y Blue Team puede transformar la ciberseguridad organizacional, convirtiéndola en un proceso dinámico y proactivo, capaz de anticipar y mitigar las amenazas en un entorno digital en constante evolución.

Justificación

La justificación de este trabajo radica en la creciente necesidad de mejorar la ciberseguridad en las organizaciones debido a la sofisticación y frecuencia de los ciberataques. Los equipos **Red Team** y **Blue Team** desempeñan roles cruciales en este contexto: el **Red Team** identifica vulnerabilidades a través de simulaciones de ataques, mientras que el **Blue Team** se enfoca en la defensa activa y la respuesta ante incidentes. Sin embargo, la falta de una colaboración eficaz entre ambos equipos puede generar brechas de seguridad que los atacantes pueden explotar. Este trabajo justifica la importancia de fomentar la sinergia entre ambos equipos, ya que su colaboración puede optimizar las estrategias de seguridad, permitir una respuesta más rápida ante amenazas y mejorar la resiliencia de la organización frente a ataques cibernéticos. Además, busca resaltar cómo una integración más estrecha de estos equipos puede proporcionar una defensa más robusta y efectiva en un entorno digital cada vez más peligroso.

Objetivos

Objetivo General

Analizar la sinergia estratégica entre los equipos **Red Team** y **Blue Team** en ciberseguridad, destacando cómo su colaboración puede mejorar la defensa ante ciberamenazas y optimizar la postura de seguridad en las organizaciones.

Objetivos Específicos

Realizar el análisis de la legislación relacionada con delitos informáticos.

• Realizar el análisis sobre el ejercicio de Pentesting.

• Realizar la explicación de las herramientas y servicios utilizados en la ciberseguridad.

• Evidenciar la implementación de un “banco de trabajo” en un entorno local para realizar el Pentesting.

• Brindar una guía para la identificación de un problema específico en temas éticos y legales

• Analizar un problema ético legal en un acuerdo de confidencialidad

• Utilizar herramientas y procedimientos para dar solución al escenario propuesto de acuerdo con los pasos del Pentesting.

• Análisis del problema de seguridad que permita dar solución al fallo identificado al interior de una organización.

• Usar herramientas de seguridad para dar identificar fallos en el escenario propuesto.

• Analizar el ataque del escenario propuesto y realizar la explotación de vulnerabilidades en el escenario propuesto.

• Evidenciar de forma práctica la explotación de la vulnerabilidad identificada

• Analizar y plantear acciones necesarias para contener un ataque en tiempo real.

• Realizar el informe de acciones de Hardening a implementar para poder evitar que sucedan ataques de seguridad informática.

• Analizar las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

• Análisis sobre la pertinencia de trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team.

• Análisis sobre las funciones y características principales de un SIEM.

• Informe de elección de 3 herramientas que permitan contener ataques informáticos. • Formular Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.

• 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.

1. Conceptos equipos de seguridad

Analisis de la legislación relacionada con delitos informáticos.

Delitos informáticos en Colombia.

Colombia cuenta con un marco legal específico para la salvaguarda de su ciberespacio, materializado en la **Ley 1273 de 2009**. Esta legislación no solo modificó el Código Penal, sino que creó una categoría legal novedosa: la 'protección de la información y de los datos[1]', con el propósito de blindar los sistemas que operan mediante las Tecnologías de la Información y las Comunicaciones (TIC).

El cuerpo de esta ley se estructura para criminalizar dos grandes grupos de conductas. Un primer apartado aborda los crímenes que atentan directamente contra la **integridad, confidencialidad y disponibilidad de la información**. Un segundo capítulo se dedica a los **ataques informáticos** y otras actividades ilícitas relacionadas. A partir de su entrada en vigor, los delitos informáticos comenzaron a ser penalizados con **penas de prisión** que pueden ir de 3 a 10 años, sumado a **sanciones económicas** que varían entre 100 y 1.500 salarios mínimos legales mensuales. Adicionalmente, la ley prevé un **incremento de la pena**, que oscila entre un tercio y la mitad, en aquellos casos donde los delitos se perpetran en escenarios de mayor riesgo, como redes y sistemas gubernamentales, por parte de funcionarios públicos, o con motivaciones terroristas.

[1] 1SIC. (2009). Ley 1273 de 2009 (pp. 1) Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Protección de datos personales

El marco legal colombiano en materia de privacidad de la información personal está definido por la **Ley 1581 de 2012**, una disposición que establece las reglas generales para la **protección de datos personales**.[2] Esta legislación fue concebida para orientar a todas las organizaciones, tanto estatales como privadas, que manejan información sensible de los individuos.

La Ley 1581 confiere a los ciudadanos un **derecho fundamental** sobre sus propios datos, facultándolos a ejercer control directo sobre cómo se utiliza su información. Esto incluye la prerrogativa de **consultar, actualizar, corregir y, crucialmente, decidir si autorizan su manejo**. Con ello, se busca asegurar el **respeto por la privacidad**, así como la **transparencia en el procesamiento de los datos**, garantizando que los individuos puedan acceder a su información o restringir su uso cuando lo consideren necesario.

Fases del pentesting

En el panorama actual de la ciberseguridad, donde los ataques informáticos representan una amenaza diaria y omnipresente, persiste una laguna significativa en la concienciación y la adopción de medidas de protección por parte de numerosas entidades, tanto en el ámbito privado como en el público. Pese a la constante difusión de noticias sobre incidentes de seguridad, la importancia de salvaguardar los datos y la información no ha sido plenamente asimilada. No obstante, se observa una tendencia creciente en el número de organizaciones que reconocen esta necesidad.

[2] FUNCION PUBLICA. Ley 1581 de 2012 (pp. 1) Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Para abordar esta problemática, una de las estrategias fundamentales es la implementación del **Hacking Ético**, que se materializa a través de las denominadas **Pruebas de Penetración (Pentesting)**. Estas evaluaciones de seguridad se ejecutan sobre los sistemas informáticos existentes en una organización y se guían por metodologías estructuradas que facilitan su desarrollo y documentación. Entre las metodologías de mayor reconocimiento y uso global se encuentran el *Open Source Security Testing Methodology Manual (OSSTMM)*, el *Open Web Application Security Project (OWASP)* y el *Information Systems Security Assessment Framework (ISSAF)*.

El presente informe detalla las fases generales de las pruebas de penetración, enmarcadas en la filosofía del Hacking Ético y siguiendo las directrices establecidas por la guía técnica **NIST SP 800-115**. Este marco metodológico se compone de cuatro etapas esenciales:

Planificación (Planning)

Esta etapa inaugural del pentesting es de carácter preparatorio y estratégico. Su propósito primordial es la definición exhaustiva del alcance y los límites de la prueba, así como la especificación de los escenarios a simular. Durante esta fase, se configuran los equipos de trabajo y se establecen acuerdos formales de privacidad y confidencialidad, los cuales deben estar rigurosamente alineados con el marco legal y normativo aplicable a la ejecución del ejercicio de penetración. Es crucial destacar que, en esta fase, no se lleva a cabo ninguna actividad que implique el uso de herramientas o aplicaciones de seguridad activas sobre los sistemas objetivo; es un período de organización y formalización puramente.

Descubrimiento (Discovery)

La fase de Descubrimiento se centra en la recolección minuciosa y la obtención de la máxima cantidad de información posible sobre el objetivo de la prueba. Esta etapa comprende la recopilación y el escaneo de datos, así como la búsqueda proactiva de vulnerabilidades. Para ello, se emplean diversas técnicas y herramientas. Por ejemplo, la Ingeniería Social permite la obtención de información y datos sensibles mediante tácticas de engaño y suplantación de identidad dirigidas a los usuarios, utilizando métodos como *Phishing*, *Vishing* o *Smishing*. Complementariamente, herramientas como Nmap son esenciales para el escaneo de red, permitiendo identificar puertos abiertos y servicios activos en los sistemas informáticos. Esto facilita una etapa subsiguiente de descubrimiento más profundo, orientada a la identificación de vulnerabilidades específicas del sistema, para lo cual se pueden usar soluciones como Nessus, reconocida por su capacidad para realizar análisis de vulnerabilidades exhaustivos en diversos sistemas operativos. La profundidad y calidad de la información obtenida en la fase de Descubrimiento son determinantes para el éxito de la prueba de penetración.

Ataque (Attack)

Esta etapa operacional es donde se ejecuta la vulneración activa de los sistemas informáticos. La fase de Ataque pone de manifiesto la efectividad de las etapas previas de Planificación y Descubrimiento, ya que un buen entendimiento del objetivo y sus debilidades es crucial para el éxito. En ocasiones, durante esta fase, puede ser necesario realizar un proceso iterativo de retroalimentación hacia la fase de Descubrimiento (loopback). Esto permite refinar la información obtenida o buscar nuevos vectores de ataque si el intento inicial no es fructífero, con el objetivo de idear un ataque potencialmente más eficaz.

Los objetivos primordiales en la fase de Ataque son generalmente dos: el acceso inicial al sistema y la posterior elevación de privilegios. Para el primer objetivo, se procede con la aplicación o ejecución de un *exploit*, que es un componente de software diseñado para aprovechar una vulnerabilidad específica del sistema y obtener una entrada. La selección o construcción de un *exploit* efectivo puede requerir conocimientos avanzados en lenguajes de programación y el análisis de vulnerabilidades previamente identificadas. El segundo objetivo, la elevación de privilegios, busca alcanzar un control total de administración sobre el sistema comprometido, lo que confiere al pentester la capacidad de demostrar el máximo impacto potencial de la vulnerabilidad.

Reporte (Reporting)

La fase final del pentesting es la de Reporte, cuyo propósito es la entrega de un informe ejecutivo detallado y comprensible. Este documento debe sintetizar todas las actividades realizadas, las pruebas ejecutadas, las vulnerabilidades identificadas, los riesgos asociados y, fundamentalmente, las recomendaciones claras y accionables para corregir las debilidades y brechas de seguridad, minimizando así los riesgos inherentes a los sistemas informáticos. Es imperativo que el informe esté redactado en un lenguaje accesible para la alta gerencia y los tomadores de decisiones, permitiéndoles comprender cabalmente las implicaciones de los hallazgos y facilitar la adopción de las medidas correctoras más adecuadas para fortalecer la postura de seguridad de la organización[3].

[3] **NIST.** (2007). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Herramientas de ciberseguridad

Metasploit framework

Metasploit es una plataforma robusta de seguridad informática de código abierto que se ha consolidado como un componente indispensable en el arsenal de los profesionales de las pruebas de penetración. Su arquitectura, basada en un *framework* modular, integra una vasta colección de *exploits*, *payloads*, *auxiliares* y *encoders*. Esta amplia gama de recursos permite a los pentesters ejecutar pruebas de penetración altamente fiables y versátiles. La vitalidad de su comunidad de desarrolladores y usuarios se refleja en la constante actualización de sus módulos, lo que garantiza su relevancia frente a las amenazas emergentes. Una de las mayores ventajas de Metasploit radica en su versatilidad multietapa, ya que puede ser utilizado en diversas fases del ciclo de vida del pentesting, desde la identificación de puertos y la detección de vulnerabilidades hasta la explotación exitosa y la escalada de privilegios en los sistemas objetivo.[4]

Nmap

Nmap (Network Mapper) es una utilidad de código abierto fundamental para la auditoría y el descubrimiento de redes. Su función principal es el escaneo exhaustivo de puertos y la identificación de servicios en hosts y dispositivos conectados a una red. Mediante el análisis de las respuestas de los paquetes enviados, Nmap es capaz de determinar qué sistemas están activos, qué puertos están abiertos, qué servicios están escuchando en esos puertos (incluyendo versiones de software), e incluso la identificación del sistema operativo. La información recopilada por Nmap es esencial para la fase de reconocimiento de un pentesting, ya que proporciona un mapa

---

Rapid7. (s. f.). *Metasploit Framework*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://www.rapid7.com/products/metasploit/

detallado de la superficie de ataque potencial, facilitando la detección de configuraciones erróneas y la búsqueda de vulnerabilidades conocidas asociadas a los servicios expuestos.

OpenVAS

OpenVAS (Open Vulnerability Assessment System) es una plataforma integral de escaneo de vulnerabilidades de código abierto, capaz de operar en una amplia variedad de entornos y sistemas operativos. Se destaca por su extensa base de datos de Vulnerability Tests (NVTs), que es alimentada y actualizada continuamente por su activa comunidad. Esta característica le permite identificar una gran cantidad de vulnerabilidades conocidas, configuraciones erróneas y fallos de seguridad en los sistemas informáticos. La capacidad de OpenVAS para realizar análisis profundos y sistemáticos lo convierte en una herramienta indispensable en cualquier metodología de prueba de penetración, proporcionando una evaluación exhaustiva del estado de seguridad de los activos de TI y facilitando la priorización de las tareas de remediación.

Servicios en Línea; Exploit-DB

Exploit-DB es un repositorio público en línea de *exploits* y *shellcode*, mantenido por Offensive Security. Funciona como una base de datos centralizada que compila y categoriza vulnerabilidades conocidas junto con el código PoC (Proof of Concept) o el *exploit* funcional necesario para su aprovechamiento. Este servicio web permite a los investigadores y profesionales de la seguridad acceder y descargar libremente estos *exploits* para su uso en entornos controlados, como pruebas de penetración o investigación de seguridad. Su valor radica en la constante expansión de su contenido, alimentado por contribuciones de una vasta

comunidad global de expertos en ciberseguridad, lo que lo convierte en un recurso invaluable para mantenerse al día con las últimas técnicas de explotación.

CVE (Common Vulnerabilities and Exposures)

CVE (Common Vulnerabilities and Exposures) es un estándar internacional para la identificación y catalogación unívoca de vulnerabilidades de seguridad y exposiciones de información. Cada entrada en la base de datos CVE se designa con un CVE-ID único (ej. CVE-XXXX-YYYY), que consiste en un identificador, una breve descripción del defecto de seguridad y referencias a informes o avisos relacionados. El objetivo primordial del sistema CVE es proporcionar un método estandarizado y común para describir y referenciar vulnerabilidades de seguridad conocidas públicamente. Esto facilita el intercambio de información sobre riesgos, la coordinación de esfuerzos de parcheo y la gestión de la postura de seguridad, permitiendo a las organizaciones y a los profesionales de la ciberseguridad identificar rápidamente la naturaleza y el impacto de una vulnerabilidad específica.

Banco de trabajo

La construcción de un entorno de pruebas aislado y controlado, conocido como banco de trabajo o laboratorio virtualizado, es un requisito fundamental para la ejecución segura y efectiva de pruebas de penetración. Para ello, se requiere la instalación de software de virtualización, como VirtualBox para sistemas Windows, que permite emular un escenario de pruebas local. Este laboratorio se configura replicando las condiciones del entorno objetivo o los escenarios definidos en la guía práctica, proporcionando un espacio seguro para el desarrollo y la validación de las técnicas de ataque y defensa sin afectar sistemas de producción.

Descarga de VirtualBox

Con el fin de establecer el entorno virtualizado, se procede a la descarga oficial del software VirtualBox. La versión compatible con el sistema operativo Windows se obtiene directamente desde la página web oficial del proyecto: https://www.virtualbox.org/wiki/Downloads. Esta descarga asegura la adquisición de la última versión estable y segura del hipervisor, indispensable para la configuración del laboratorio de pruebas.[5]

Fuente: Elaboración propia

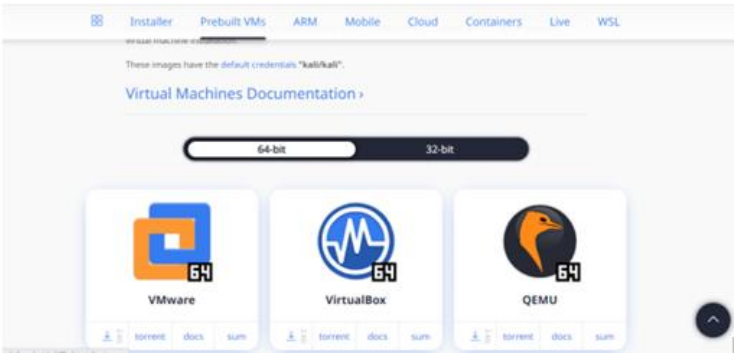
Figura 1. Instalación VirtualBox

Obtención de la Distribución Kali Linux

Para la configuración del entorno de laboratorio virtualizado, se procede con la descarga de la distribución **Kali Linux**. Se ha optado por la **imagen preconfigurada para VirtualBox**, disponible directamente desde el repositorio oficial del proyecto. Esta opción simplifica el proceso de despliegue al incluir las optimizaciones necesarias para operar eficientemente dentro

[5] Oracle VM VirtualBox. (s. f.). *Downloads – Oracle VM VirtualBox*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://www.virtualbox.org/wiki/Downloads

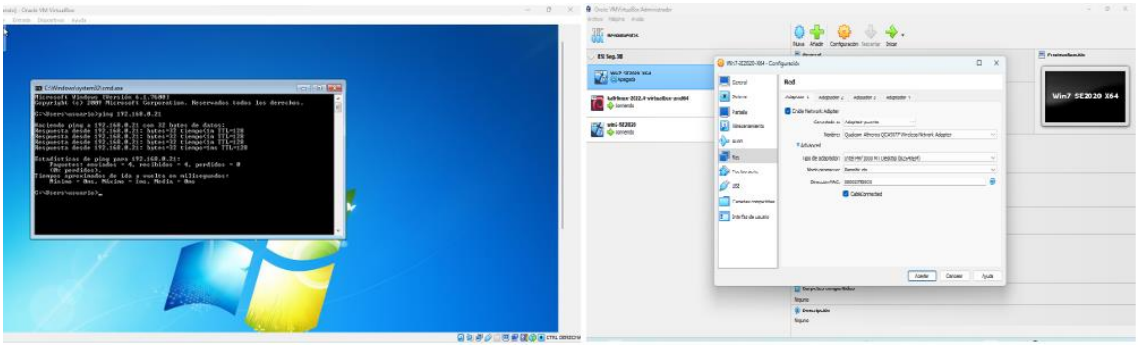
de una máquina virtual, evitando configuraciones manuales adicionales. La descarga se realiza accediendo al siguiente enlace: https://www.kali.org/get-kali/#kali-virtual-machines.



Fuente: Elaboración propia

Figura 2. Descarga Kali Linux.

Comunicación entre las máquinas Windows 32 bits y Windows 7 64 bits - Configuración de Red en VirtualBox para todas las máquinas tipo Adaptador de Puente:



Fuente: Elaboración propia

Figura 3. Configuracion maquinas virtuales para laboratorios.

2. Actuacion ética y legal

-¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

-Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273[6].

Tras un análisis del Anexo 2 – Escenario 2 y el Anexo 3 – Acuerdo de Confidencialidad, **afirmo rotundamente que se evidencian varios procesos ilegales y no éticos estipulados en dicho acuerdo.**

1.Argumentación de los Procesos Ilegales y No Éticos:

Obligación de No Denunciar Actividades Sospechosas de Espionaje **(Cláusula Cuarta, numeral 3):** Este es un punto flagrantemente ilegal y profundamente antiético. Obligar a la parte receptora (el potencial empleado) a "no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros" contraviene directamente el deber ciudadano de denunciar delitos y obstruye la justicia. Un acuerdo de confidencialidad legítimo busca proteger secretos comerciales e información sensible, no encubrir actividades criminales.

[6] SIC. (2009). Ley 1273 de 2009 (pp. 1-4) Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Fragmento Ilegal: "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."

2.Abstención de Denunciar y Publicar Información Confidencial e Ilegal (Cláusula Cuarta, numeral 4): Similar al punto anterior, esta cláusula exige que la parte receptora se "abstenga de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas." Esto implica un compromiso de silencio ante la comisión de actos ilícitos dentro de la organización, lo cual es inaceptable desde una perspectiva legal y ética. Un profesional de la ciberseguridad tiene la responsabilidad ética y, en muchos casos, legal de reportar actividades ilegales.

Fragmento Ilegal: "Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."

3.Definición de Información Confidencial que Incluye Actividades Ilícitas (Cláusula Segunda, numeral 2): La definición de "Información Confidencial" es alarmantemente amplia e incluye explícitamente "datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'." Al incluir estas actividades ilegales dentro de la definición de información confidencial que no debe ser divulgada, el acuerdo busca proteger la comisión de delitos y silenciar a quienes puedan tener conocimiento de ellos. Esto pervierte el propósito legítimo de un acuerdo de confidencialidad.

Fragmento Ilegal: "...datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”. parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

4.Cláusula de Solución de Controversias que Exime de Responsabilidad Legal y Penal a CyberFort Technologies (Cláusula Octava): Esta cláusula establece que "En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies." Esto es un intento de transferir la responsabilidad por posibles actos ilegales cometidos por la organización al individuo que recibe la información, lo cual es jurídicamente cuestionable e inherentemente injusto. La responsabilidad penal es personal e intransferible.

Fragmento Ilegal: "En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies."

Artículos de la Ley 1273 de 2009 (Ley de Delitos Informáticos) que Podrían Vulnerarse: [7]

[7] Colombia. Congreso de la República. (2009, 6 de enero). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.* Diario Oficial No. 47.223. Recuperado de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Considerando los fragmentos ilegales identificados en el Anexo 3 – Acuerdo, varios artículos de la Ley 1273 de 2009 podrían verse vulnerados, tanto por las acciones que aparentemente la organización busca proteger como por la imposición de silencio a los potenciales empleados:
Artículo 269A. Acceso abusivo a un sistema informático: Si CyberFort Technologies estuviera involucrada en "accesos abusivos a sistemas informáticos" (mencionado explícitamente en la definición de información confidencial), y el acuerdo buscara silenciar a quienes tuvieran conocimiento de ello, se estaría obstaculizando la persecución de este delito.

Por qué se vulnera: El acuerdo busca proteger la información relacionada con este delito, impidiendo su denuncia y posible investigación.

Artículo 269B. Interceptación de datos informáticos: De manera similar, si la organización realizara "interceptación de información" (también mencionada en la definición de información confidencial) y el acuerdo prohibiera su divulgación, se estaría protegiendo la comisión de este delito.
Por qué se vulnera: El acuerdo busca mantener en secreto la información sobre esta actividad ilícita, evitando su denuncia y sanción.

Artículo 269C. Daño informático: Aunque no se menciona explícitamente en la definición, si dentro de las actividades de la organización existieran acciones que causaran "daño, deterioro, destrucción, alteración o supresión de datos informáticos, o de un sistema de tratamiento de información o de sus partes o componentes lógicos", y el acuerdo buscara ocultarlo, se estaría obstaculizando la aplicación de la ley.

Por qué se vulnera: El acuerdo podría interpretarse como un intento de encubrir información relacionada con este tipo de daño, impidiendo su denuncia.

Artículo 269D. Uso de software malicioso: Si la organización desarrollara o utilizara "software malicioso" y el acuerdo buscara proteger esta información, se estaría dificultando la aplicación de la ley contra este delito.

Por qué se vulnera: El acuerdo podría obligar al silencio sobre la existencia y uso de software malicioso.

Artículo 454. Obstrucción a la justicia: La obligación de "no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros" y la abstención de denunciar información ilegal podrían constituir obstrucción a la justicia, ya que impiden que las autoridades competentes tengan conocimiento de posibles delitos y puedan investigarlos.

Por qué se vulnera: Estas cláusulas buscan activamente impedir que se informe a las autoridades sobre actividades potencialmente criminales.

- ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Mi respuesta es NO, no aplicaría a este trabajo en CyberFort Technologies, a pesar del atractivo sueldo de $15.000.000 de pesos colombianos mensuales y el contrato vitalicio.

Mi argumentación se basa en principios éticos fundamentales, la integridad profesional y las directrices establecidas por el Código de Ética para Ingenieros en Colombia, según lo dispuesto por el Consejo Profesional Nacional de Ingeniería (COPNIA).

Argumentación de mi Decisión Negativa:

Integridad y Ética Profesional: Como profesional de la ciberseguridad, mi labor primordial es garantizar la seguridad, la integridad y la legalidad de los sistemas de información. El acuerdo propuesto por CyberFort Technologies me obligaría, explícitamente, a ser cómplice de potenciales actividades ilícitas al no denunciarlas y, peor aún, al mantenerlas en secreto. Esto va en contra de mi juramento profesional y mis principios éticos fundamentales. El dinero y la estabilidad laboral no pueden justificar la participación o el encubrimiento de actos ilegales.

Responsabilidad Social y Legal: El Código de Ética para Ingenieros en Colombia, y en general cualquier marco ético profesional, enfatiza la responsabilidad social y legal de los ingenieros. Aceptar un contrato que me obligue a no denunciar delitos me haría partícipe, por omisión, de cualquier actividad ilegal que la organización pudiera estar llevando a cabo. Esto no solo es moralmente inaceptable, sino que también podría acarrearme consecuencias legales en el futuro.

Independencia de Juicio Profesional: El Código de Ética de COPNIA promueve la independencia de juicio profesional. Aceptar un acuerdo que me dicte qué información debo ocultar y a quién no debo denunciar comprometería gravemente mi capacidad para ejercer un juicio profesional independiente y ético. Mi deber es con la seguridad y la legalidad, no con el encubrimiento de posibles malas prácticas de una organización.

Precedente Peligroso: Aceptar un empleo bajo estas condiciones sentaría un precedente peligroso para mi carrera y para la profesión en general. Validaría la idea de que la seguridad y la ética pueden ser comprometidas por beneficios económicos, lo cual socava la confianza pública en los profesionales de la ciberseguridad.

Riesgos Personales y Profesionales: Trabajar en un entorno donde se promueve el silencio ante la ilegalidad me expondría a riesgos personales y profesionales significativos. Podría verme involucrado en investigaciones futuras, ser considerado cómplice o, en el mejor de los casos, trabajar en un ambiente de desconfianza y falta de transparencia.

Consideraciones del Código de Ética para Ingenieros (COPNIA):

Cabe resaltar algunas conductas del código de ética:

Honestidad e Integridad: Actuar con rectitud, honradez y veracidad en el ejercicio de la profesión. El acuerdo propuesto claramente atenta contra estos principios.

Responsabilidad Social: Contribuir al bienestar y al progreso de la sociedad, lo cual implica denunciar actividades que puedan ser perjudiciales o ilegales.

Cumplimiento de la Ley: Respetar y cumplir las leyes y normas vigentes. El acuerdo me obligaría a incumplir mi deber de denunciar delitos.

Secreto Profesional: El secreto profesional debe ejercerse dentro del marco de la ley y la ética, no para encubrir actividades ilícitas.

Independencia y Objetividad: Mantener la independencia de criterio y evitar conflictos de interés que puedan comprometer el ejercicio profesional ético.[8]

-Deberá analizar el caso problema "Ciberespionaje y Ética en CyberFort Technologies" (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

El acceso a información sensible por parte de las empresas de ciberseguridad durante una auditoría debe limitarse estrictamente a lo necesario para cumplir con el alcance específico del servicio contratado. Este acceso debe estar claramente definido y acordado en el contrato de servicios, con un propósito legítimo de evaluación y mejora de la seguridad.

Las empresas de ciberseguridad no deben tener un acceso irrestricto a toda la información del cliente. El principio de mínimo privilegio debe aplicarse rigurosamente: solo se debe otorgar el acceso a la información y los sistemas que sean absolutamente esenciales para llevar a cabo las pruebas y análisis necesarios.

Además, debe existir una justificación clara y documentada para cada nivel de acceso otorgado. Cualquier acceso que exceda el alcance acordado o que no tenga una justificación directa en la mejora de la seguridad debe considerarse una extralimitación y una potencial violación de la confianza.

[8] COPNIA. Código de Etica para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (pp. 1-20) Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

¿Cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Garantizar que el acceso a información sensible no sea explotado de manera indebida requiere una combinación de medidas técnicas, legales y éticas:

Acuerdos Contractuales Sólidos: Los contratos deben definir claramente el alcance del acceso, las responsabilidades de la empresa de ciberseguridad en cuanto a la protección de la información, las cláusulas de confidencialidad estrictas y las consecuencias legales en caso de incumplimiento.

Políticas Internas y Procedimientos Robustos: Las empresas de ciberseguridad deben implementar políticas internas claras sobre el manejo de la información del cliente, el acceso privilegiado, la supervisión de las actividades de sus empleados y los protocolos de respuesta ante incidentes de seguridad internos.

Controles de Acceso y Monitoreo Técnico: Se deben implementar controles técnicos para limitar el acceso a la información sensible únicamente a las cuentas y sistemas necesarios, y durante el tiempo estrictamente requerido. El monitoreo continuo de las actividades de los empleados con acceso privilegiado y el registro detallado de sus acciones (logging) son cruciales para detectar y prevenir posibles abusos.

Auditorías Internas y Externas: Realizar auditorías periódicas, tanto internas como por terceros independientes, puede ayudar a verificar el cumplimiento de las políticas y procedimientos de seguridad y a identificar posibles vulnerabilidades o malas prácticas.

Formación y Concientización Ética: Es fundamental capacitar a los profesionales de ciberseguridad en los principios éticos de su profesión, la importancia de la confidencialidad y

las consecuencias legales de la mala praxis. Fomentar una cultura organizacional basada en la integridad y la responsabilidad es esencial.

Supervisión y Segregación de Funciones: Implementar la segregación de funciones, de modo que diferentes personas sean responsables de diferentes aspectos del acceso y el manejo de la información, puede reducir el riesgo de abuso por parte de un solo individuo. La supervisión constante de las actividades sensibles también es crucial.

Mecanismos de Rendición de Cuentas: Debe haber mecanismos claros para que los clientes puedan reportar sospechas de abuso y para que las empresas de ciberseguridad investiguen y sancionen cualquier conducta inapropiada de sus empleados.

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Para evitar el uso no autorizado o éticamente cuestionable de herramientas avanzadas de análisis forense por parte de empleados, las empresas de ciberseguridad deberían implementar los siguientes mecanismos de supervisión y control:

Políticas de Uso Estrictas y Detalladas: Definir claramente qué herramientas pueden utilizarse, para qué propósitos específicos y bajo qué circunstancias. Establecer las consecuencias del uso indebido.

Control de Acceso Granular: Implementar sistemas de autenticación y autorización robustos, limitando el acceso a las herramientas y a los datos analizados solo a personal autorizado y para tareas específicas.

Registro y Auditoría Exhaustiva (Logging): Mantener registros detallados de quién accede a qué herramientas, cuándo y qué acciones realizan. Implementar sistemas de auditoría automatizados para detectar actividades sospechosas.

Monitorización en Tiempo Real: Utilizar software de monitorización para supervisar la actividad de los empleados que utilizan herramientas forenses, identificando patrones de uso inusuales o potencialmente maliciosos.

Segregación de Funciones: Asignar diferentes responsabilidades a distintos empleados en el proceso de análisis forense, evitando que una sola persona tenga control total sobre las herramientas y los datos.

Aprobación y Supervisión de Casos: Requerir la aprobación de un superior para el uso de herramientas forenses en cada caso específico y establecer una supervisión regular de las actividades realizadas.

Análisis de Comportamiento y Detección de Anomalías: Implementar sistemas de análisis de comportamiento para identificar desviaciones de los patrones de uso normales que puedan indicar un uso no autorizado.

Inspecciones y Auditorías Internas Periódicas: Realizar inspecciones sorpresa y auditorías internas para verificar el cumplimiento de las políticas y detectar posibles irregularidades en el uso de las herramientas.

Formación y Concientización Continua: Educar a los empleados sobre la ética profesional, las políticas de la empresa y las consecuencias legales del uso indebido de herramientas forenses.

Acuerdos de Confidencialidad y No Divulgación Reforzados: Establecer acuerdos legales que prohíban estrictamente el uso no autorizado de la información y las herramientas, con cláusulas de confidencialidad post-empleo.

Mecanismos de Alerta y Respuesta a Incidentes: Implementar sistemas de alerta temprana para detectar posibles usos indebidos y tener protocolos claros para responder a incidentes de seguridad internos.

Evaluación y Actualización Continua de Controles: Revisar y actualizar periódicamente los mecanismos de supervisión y control para adaptarse a nuevas amenazas y a la evolución de las herramientas forenses.

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente

Cuando se descubre ciberespionaje por una empresa de ciberseguridad contratada, la respuesta inmediata de gobiernos y organizaciones debe ser una investigación exhaustiva, la ruptura del contrato, la notificación a los afectados, la colaboración con otras agencias y acciones legales contundentes. Es crucial evaluar los daños y perjuicios ocasionados.

Para restaurar la confianza y prevenir futuros incidentes, se deben implementar medidas como la transparencia y comunicación abierta, la revisión rigurosa de la contratación de proveedores, el fortalecimiento de la supervisión y las cláusulas contractuales, el desarrollo de legislación más robusta, el fomento de la ética profesional, la inversión en capacidades internas, la cooperación público-privada y la concientización sobre los riesgos. La respuesta debe ser firme y ejemplarizante para disuadir estas conductas y reconstruir la confianza perdida.

En primer lugar, el caso del contrato de reclutamiento en CyberFort Technologies revela la existencia de cláusulas ilegales y no éticas que buscan proteger actividades ilícitas y silenciar a los empleados, lo cual contraviene la ley colombiana y los principios fundamentales de la ética

profesional en ciberseguridad. Aceptar un acuerdo de esta naturaleza comprometería la integridad del profesional y podría acarrear consecuencias legales.

En segundo lugar, el escenario de ciberespionaje por parte de una empresa de ciberseguridad subraya la crítica importancia de la ética, la confianza y la legalidad en la prestación de servicios de seguridad digital. El abuso de acceso privilegiado y la venta de información confidencial constituyen una grave violación de la confianza y pueden acarrear serias consecuencias legales y reputacionales. Para prevenir estos incidentes, es fundamental implementar mecanismos robustos de supervisión, control y rendición de cuentas, tanto a nivel de las empresas de ciberseguridad como en los procesos de contratación y gestión por parte de los clientes. La respuesta ante tales actos debe ser firme y ejemplarizante para restaurar la confianza y asegurar la integridad del sector.

3. Ejecucion pruebas de intrusion

En el mundo actual, donde la información es oro, las empresas se enfrentan a un enemigo invisible pero muy peligroso: las fugas de datos. Imagina que la información valiosa de una empresa se está escapando, como agua por un agujero, desde uno de sus computadores. Aquí es donde entra en juego el equipo "Red Team", como detectives de la ciberseguridad. Su primera misión es encontrar ese agujero, descubrir por dónde se está yendo la información.

Lo que sabemos hasta ahora es que el computador sospechoso tiene una "puerta trasera" en forma de una aplicación insegura que funciona en Windows. Alguien con malas intenciones podría usar un "truco" (exploit) para colarse por esa puerta, tomar el control del computador (obtener un "Shell") y hasta convertirse en el "dueño" del sistema (escalar privilegios).

Para entender qué está pasando, el equipo forense, como si hubiera tomado una foto del momento del crimen, nos ha dado una copia exacta del disco duro del servidor. Como expertos en encontrar estas "puertas traseras", nuestra tarea es revisar esa copia, encontrar la falla de seguridad y, si es posible, usar ese "truco" para demostrar cómo un atacante podría tomar el control, ¡incluso creando un nuevo "dueño" del computador! Esto es como mostrar a los jefes cómo de fácil podría ser el ataque, para que entiendan el peligro real.

Objetivos de la prueba de intrusion

Analizar la posible fuga de información en un equipo Windows, identificar la vulnerabilidad de la aplicación instalada que la facilita, demostrar su explotación mediante la creación de un usuario administrador, y documentar detalladamente el proceso para presentar una Prueba de Concepto.

Identificar y describir las herramientas de software empleadas en cada fase del pentesting realizado para analizar el escenario 3 del anexo 4, adjuntando evidencia de los comandos ejecutados y los resultados obtenidos.

Listar y describir los datos e información proporcionados en el anexo 4 – escenario 3 que fueron fundamentales para la identificación del fallo de seguridad específico explotable en la máquina Windows.

Determinar la herramienta utilizada para la identificación de los fallos de seguridad presentes en la máquina Windows y especificar el puerto de red que abre la aplicación vulnerable identificada en el anexo.

Explicar de manera detallada y con el apoyo de representaciones gráficas el impacto del ataque simulado en la máquina Windows, describiendo las consecuencias de la explotación de la vulnerabilidad.

Documentar exhaustivamente cada uno de los pasos técnicos ejecutados durante el proceso de explotación de la vulnerabilidad en la máquina Windows 7, incluyendo las evidencias correspondientes para cada etapa.

Herramientas utilizadas para la resolución del Escenario Red Team en el Marco del Pentesting

Para abordar de manera sistemática el desafío planteado en el escenario Red Team, se recurrió a un abanico de herramientas de software especializadas, cada una desempeñando un rol crucial dentro de las etapas metodológicas del pentesting:

Nmap (Network Mapper): El Ojo Explorador de la Red. Esta versátil utilidad multiplataforma se erigió como el punto de partida para la fase de reconocimiento. Su capacidad para sondear la infraestructura digital permitió cartografiar el panorama de la red, revelando la presencia de puertos activos, los servicios que los atienden y las versiones de los sistemas operativos subyacentes. Esta inteligencia inicial resultó fundamental para delimitar el perímetro de análisis y enfocar los esfuerzos posteriores.

Nessus: El Detector de Debilidades y Prescriptor de Soluciones. Una vez establecido el mapa de la red, Nessus entró en acción como un motor de escaneo avanzado. Su función principal radicó en la identificación exhaustiva de posibles vulnerabilidades presentes en los sistemas y servicios detectados. Más allá de la mera detección, Nessus ofreció valiosas recomendaciones y posibles mitigaciones para cada debilidad encontrada, culminando su análisis en un informe detallado que clasificó los hallazgos según su nivel de criticidad.

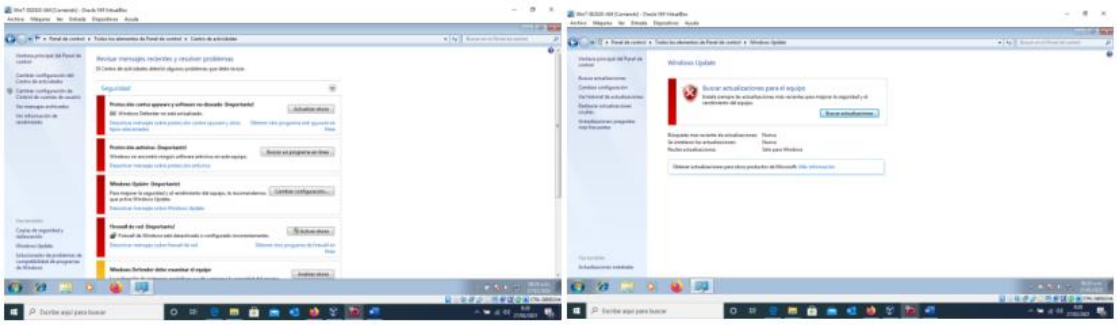
Metasploit Framework: El Arsenal de Penetración y Fortificación. En las etapas de explotación y post-explotación, el Metasploit Framework se convirtió en la herramienta central. Este entorno de código abierto y sin costo proporcionó un vasto repertorio de exploits y payloads

diseñados para probar las defensas de seguridad de un sistema. Su flexibilidad no solo facilitó la simulación de ataques controlados, sino que también ofreció mecanismos para comprender las debilidades desde la perspectiva del atacante, permitiendo así implementar estrategias de protección más robustas y efectivas.

En la etapa inicial de la investigación, se llevó a cabo una exhaustiva recopilación de datos inherentes a la infraestructura digital de la organización objetivo. Este proceso de adquisición de inteligencia se centró en la identificación precisa de los sistemas operativos en ejecución y el software implementado en su entorno operativo. Para esta labor de reconocimiento primario, se empleó estratégicamente la utilidad Nmap (Network Mapper). Esta herramienta demostró su valía al permitir la inspección detallada del estado de los puertos de red, discerniendo entre aquellos que permanecían accesibles o inaccesibles dentro del flujo operacional cotidiano. Adicionalmente, Nmap facilitó la extracción de atributos distintivos asociados a cada servicio en funcionamiento, proporcionando una visión granular de la arquitectura de red y sus componentes.

Como medida preparatoria esencial para la subsiguiente fase de evaluación de vulnerabilidades, se procedió a la desactivación temporal del firewall nativo del sistema operativo Windows en el entorno de pruebas controlado. Esta acción se consideró imprescindible para asegurar la ejecución sin obstáculos de las operaciones de análisis de seguridad requeridas por la organización. La desactivación del firewall permitió una inspección profunda de las potenciales debilidades del sistema y un análisis exhaustivo de sus dinámicas operacionales internas, sin la interferencia de las reglas de filtrado de tráfico preestablecidas.

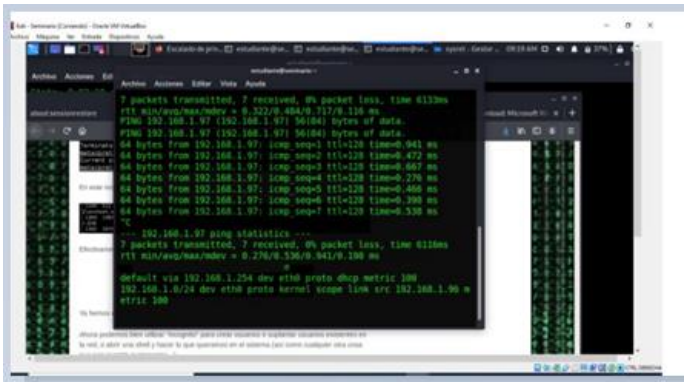
Paso 1 Desactivación de firewall de la maquina virtual



Fuente: Elaboración propia

Figura 4. Desactivación de firewall de la maquina virtual

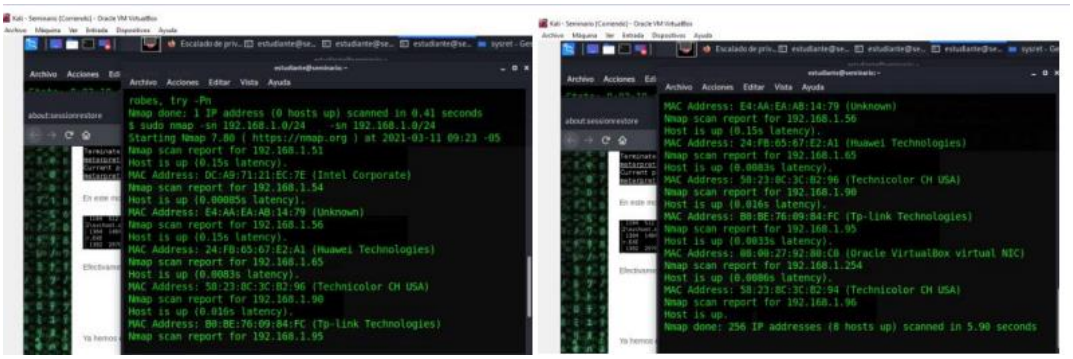
Paso 2. Identificación del enrutamiento



Fuente: Elaboración propia

Figura 5. Identificación del enrutamiento

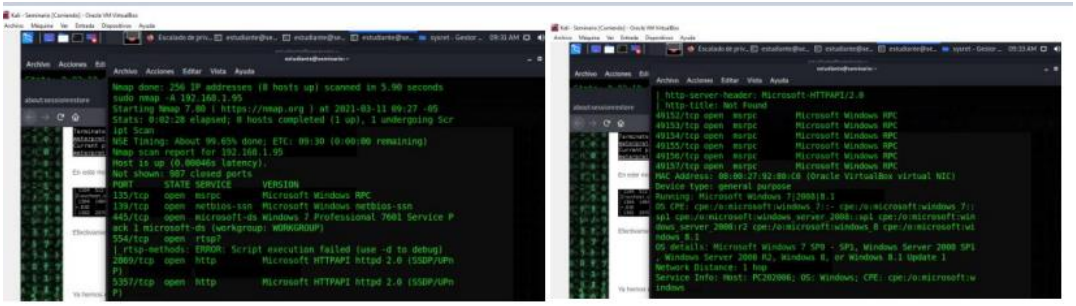
Paso 3: Dispositivos conectados a la red



Fuente: Elaboración propia

Figura 6. Dispositivos conectados a la red

Paso 4: identificación de puertos y servicios



Fuente: Elaboración propia

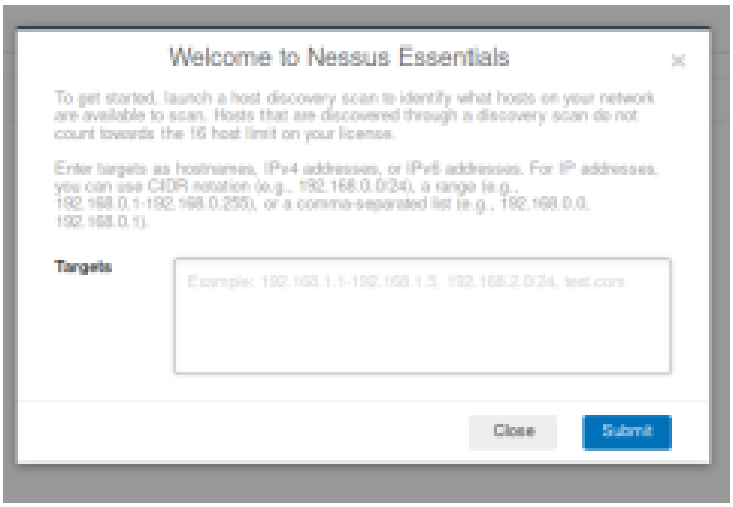
Figura 6. identificación de puertos y servicios

Etapa de Evaluación de Debilidades: Verificación de la Eficacia de la Penetración Mediante el Análisis Proactivo de Vulnerabilidades

En esta crucial fase del ejercicio, se llevó a cabo una valoración exhaustiva de los resultados obtenidos en las etapas precedentes de simulación de intrusión. El foco principal se centró en discernir el nivel de éxito alcanzado por las estrategias de penetración implementadas, lo cual se

realizó a través de un análisis meticuloso y una búsqueda proactiva de vulnerabilidades latentes. Este punto representó el momento determinante para calibrar la eficiencia intrínseca del proceso de penetración en su totalidad. El conjunto de herramientas primordiales desplegadas para esta tarea analítica comprendió a **Nessus** y **Nmap.** La sinergia de estas utilidades posibilitó la identificación de las características de riesgo y la evaluación de la estabilidad general del sistema, todo ello en función de los diversos factores de vulnerabilidad detectados.

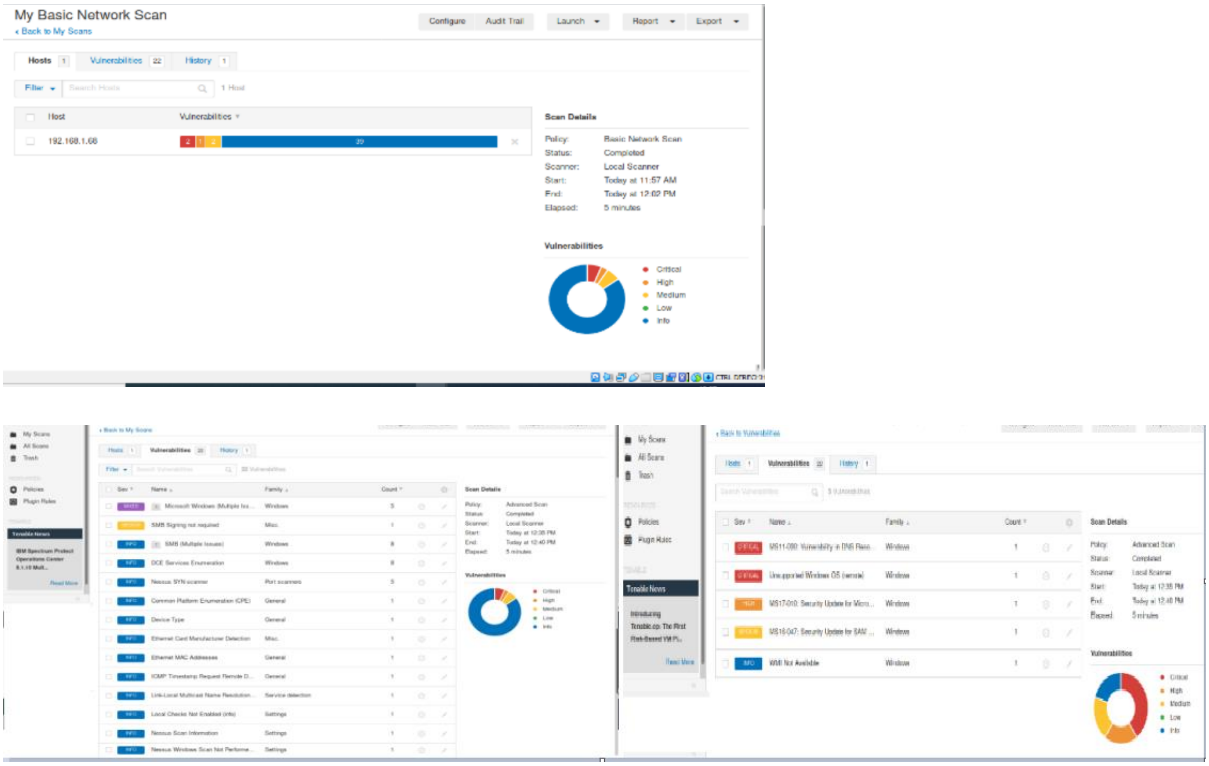
Paso 5: Analisis de vulnerabilidades NESSUS.



Fuente: Elaboración propia

Figura 7. Analisis de vulnerabilidades NESSUS.

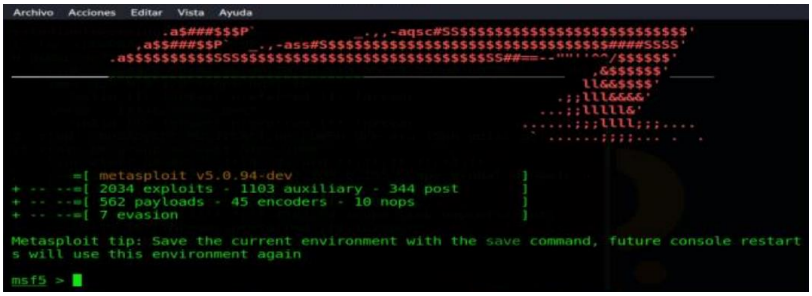
Paso 6 ejecución de NESSUS



Fuente: Elaboración propia

Figura 8. Analisis de vulnerabilidades NESSUS.

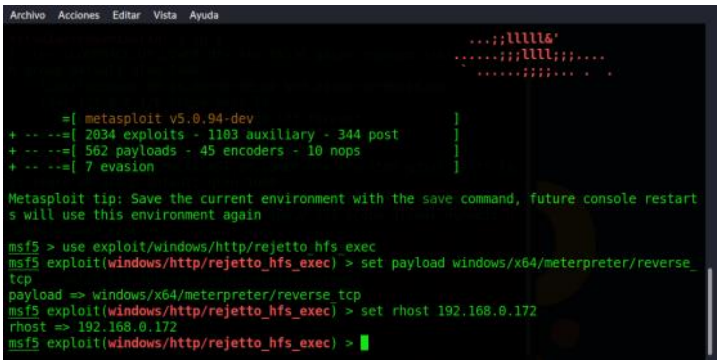
Fase 7: explotación (ingreso a la consola para ejecutar el exploit)



Fuente: Elaboración propia

Figura 9. explotación (ingreso a la consola para ejecutar el exploit)

En la prosecución de la fase de explotación, y habiendo identificado una potencial vía de intrusión a través de la vulnerabilidad asociada a Rejetto HTTP File Server versión 2.3, se procedió a la configuración precisa del componente de carga maliciosa (payload). Para este propósito, se seleccionó el payload **windows/x64/meterpreter/reverse_tcp**. Esta elección estratégica se fundamentó en su capacidad para establecer una comunicación bidireccional encubierta, proporcionando una consola interactiva y avanzada para la manipulación remota del sistema comprometido. Acto seguido, se especificó la dirección IP del objetivo vulnerable, la cual se definió mediante la directiva **rhost**, asignándole el valor **192.168.0.172**. Esta acción direccionó el payload de manera inequívoca hacia la máquina identificada como susceptible de explotación.

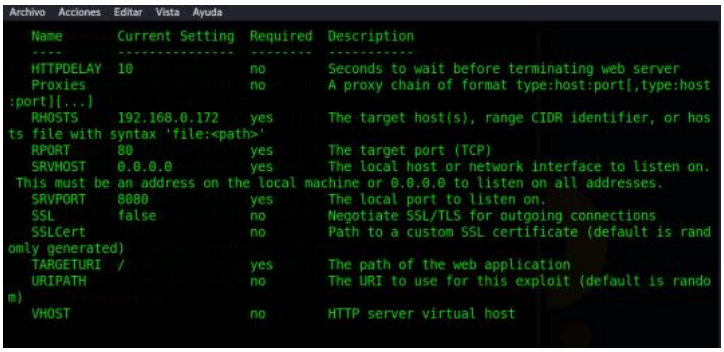


Fuente: Elaboración propia

Figura 10. explotación (ingreso a la consola para ejecutar el exploit)

Confirmación de los Parámetros de Ejecución: Verificación de la Configuración del Módulo de Explotación

Previo al lanzamiento de la secuencia de explotación, se llevó a cabo una minuciosa verificación de los parámetros de configuración establecidos para el módulo en uso. A través del comando **show options**, se inspeccionó detalladamente cada una de las variables configurables, asegurando que los valores asignados, tales como la dirección IP del objetivo (rhost) y la configuración del payload seleccionado, concordaran precisamente con los requerimientos de la estrategia de ataque diseñada. Esta etapa de confirmación se consideró un paso crítico para mitigar posibles errores de ejecución y garantizar la correcta focalización del exploit hacia el sistema vulnerable identificado.



Fuente: Elaboración propia

Figura 11. explotación (ingreso a la consola para ejecutar el exploit)

Análisis de las herramientas y comando ejecutados:

Durante la fase de reconocimiento e identificación de activos dentro del entorno computacional de la organización, se logró establecer la presencia de una aplicación específica, **Rejetto HTTP File Server versión 2.3**, ejecutándose sobre un sistema operativo **Windows 7** con arquitectura de 64 bits en una de las estaciones de trabajo bajo análisis.

Identificación de Vector de Ataque Potencial:

La información recabada reveló la existencia de un escenario de amenaza asociado a un exploit conocido para la aplicación Rejetto v. 2.3. Este exploit presenta la capacidad de establecer una conexión de Shell reversa, lo que implicaría la posibilidad de obtener acceso remoto no autorizado al sistema comprometido.[9]

Evaluación de la Viabilidad de una Sesión Meterpreter:

Se procedió a analizar la factibilidad de lograr una sesión Meterpreter como resultado de la explotación. Meterpreter, un payload avanzado dentro del framework Metasploit, ofrece una interfaz interactiva y rica en funcionalidades para la manipulación post-explotación del sistema objetivo, lo que representa un vector de control significativo.

Análisis de la Potencial Escalación de Privilegios:

Paralelamente, se investigó la posibilidad de llevar a cabo una escalación de privilegios tras una potencial intrusión inicial. El objetivo de esta indagación se centró en determinar si la explotación exitosa de la vulnerabilidad podría allanar el camino para la creación de una cuenta de usuario con privilegios de administrador dentro del sistema operativo comprometido, lo que representaría un nivel de control aún mayor sobre el activo afectado.

Análisis de vulnerabilidades encontradas con aplicativo NESSUS

A continuación, se presenta una caracterización técnica de las vulnerabilidades relevantes identificadas durante la fase de análisis, destacando su naturaleza, potencial impacto y criticidad:

[9] Rejetto. (s. f.). *HFS: HTTP File Server*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://hfs.rejetto.com/

MS11-030 (Crítico): Vulnerabilidad en el Formato de Paquetes DNS de Windows. Esta falla de seguridad reside en la implementación de la característica de formato de nombres de dominio (DNS) en sistemas operativos Windows. Su explotación exitosa permite a atacantes manipular las consultas de resolución de nombres de multidifusión de enlace (Link-Local Multicast Name Resolution - LLMNR) de manera maliciosa. Un atacante podría aprovechar esta debilidad para inyectar y ejecutar código arbitrario dentro del contexto de la cuenta NetworkService, un servicio con privilegios significativos en el sistema, lo que podría resultar en un control sustancial sobre el sistema afectado.

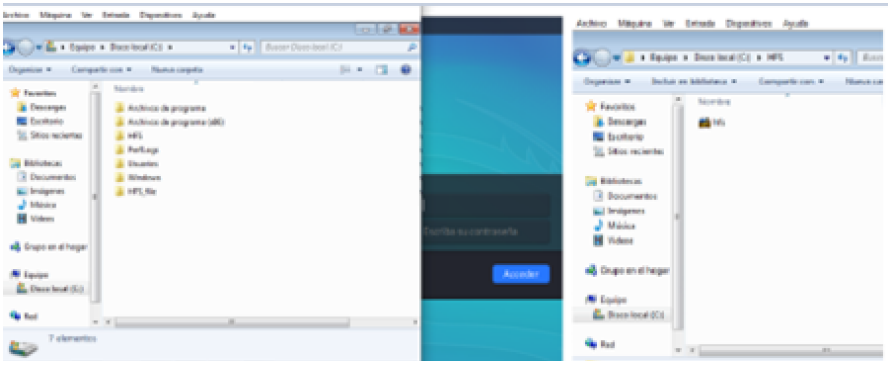
Unsupported windows OS remote (Crítico): Detección de Sistema Operativo Windows No Soportado (Vulnerable Remotamente). La identificación de una versión de sistema operativo Windows que ha alcanzado el fin de su ciclo de vida de soporte oficial representa una vulnerabilidad crítica inherente. Estos sistemas carecen de las actualizaciones de seguridad más recientes, lo que los expone a un amplio espectro de vulnerabilidades conocidas y potencialmente no parcheadas. Un atacante remoto podría explotar estas debilidades para llevar a cabo intrusiones y comprometer la seguridad del sistema sin necesidad de interactuar directamente con él.

MS17-010 (Alto): Vulnerabilidad de Ejecución Remota de Código en Microsoft Server Message Block (SMB) (EternalBlue). Esta vulnerabilidad de alto riesgo se encuentra en la forma en que el protocolo Server Message Block (SMB) de Microsoft procesa ciertas solicitudes. Un atacante remoto no autenticado podría enviar peticiones especialmente crafted al servidor SMB vulnerable, lo que podría resultar en la ejecución de código arbitrario en el sistema

objetivo. Dada la amplia utilización del protocolo SMB para compartir archivos e impresoras en redes Windows, esta vulnerabilidad tiene un potencial de propagación y un impacto significativo.

MS16-047 (Medio): Vulnerabilidad de Elevación de Privilegios Remota en el Protocolo del Administrador de Cuentas de Seguridad (SAM). Esta vulnerabilidad de severidad media radica en una falla en la negociación del nivel de autenticación durante las comunicaciones del protocolo del Administrador de Cuentas de Seguridad (SAM) a través de canales de llamadas a procedimiento remoto (RPC). Un atacante podría aprovechar esta debilidad para lograr una degradación en el nivel de autenticación establecido, lo que potencialmente podría permitirle ejecutar acciones con privilegios superiores a los que inicialmente poseía en el sistema remoto.

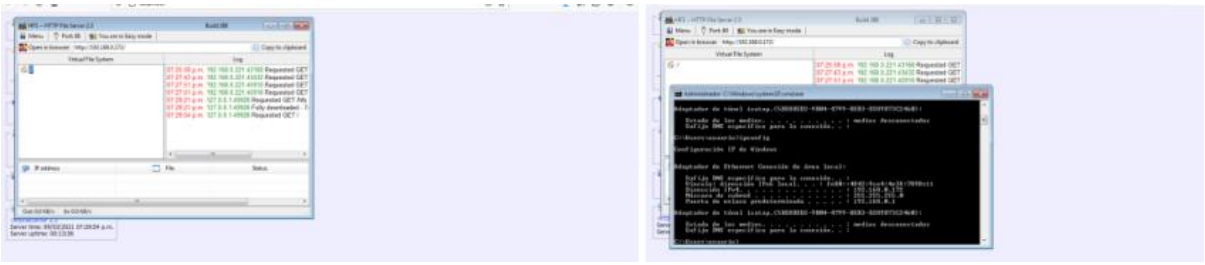
Después del anterior análisis se procedió a instalar la herramienta HFS en la maquina win7 x 64.



Fuente: Elaboración propia

Figura 12. herramienta HFS

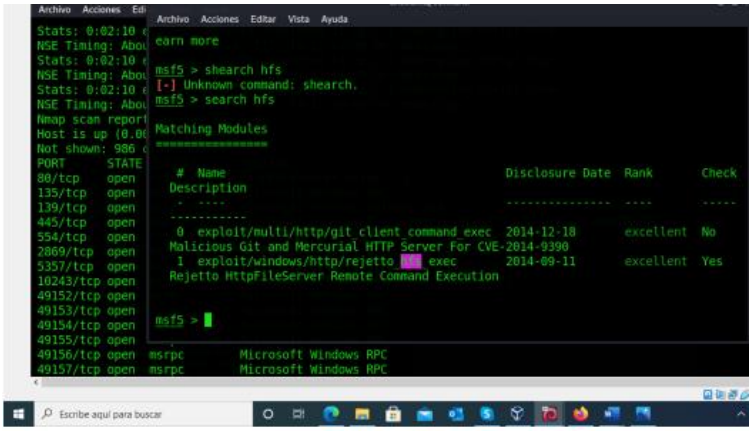
Identificación de los procesos de ejecución HFS



Fuente: Elaboración propia

Figura 13. Identificación de los procesos de ejecución HFS

búsqueda HFS. Search HFS.[10]

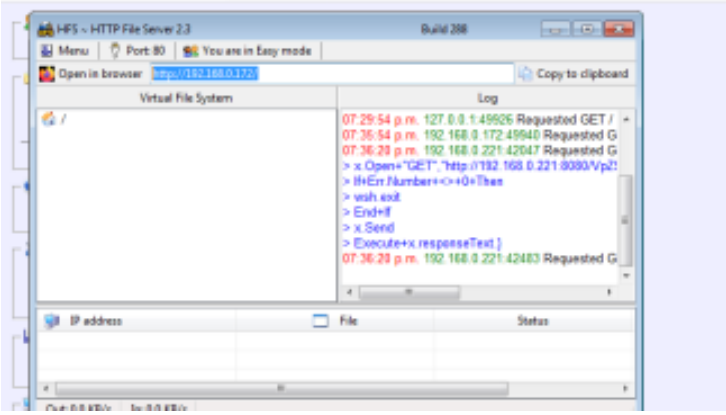


Fuente: Elaboración propia

Figura 14. búsqueda HFS. Search HFS.

[10] Ethical Hacking. CÓMO USAR SEARCHSPLOIT PARA ENCONTRAR EXPLOITS(2018).Disponible en: https://blog.ehcgroup.io/2018/11/27/01/00/39/4198/como-usarsearchsploit-para-encontrar-exploits/hacking/ehacking/

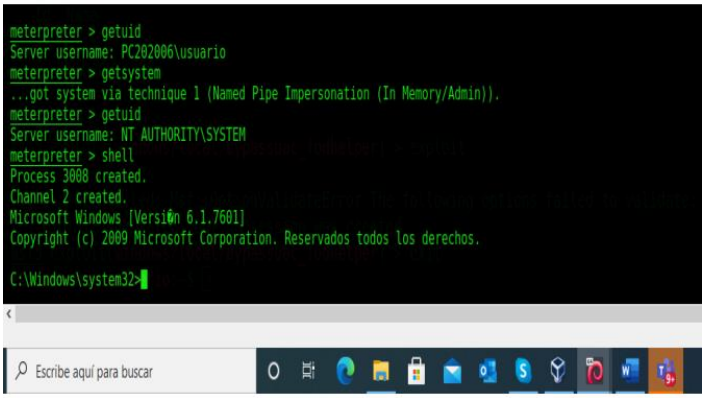
Analisis de ejecucion rejjeto 2.3



Fuente: Elaboración propia

Figura 15. Analisis de ejecucion rejjeto 2.3

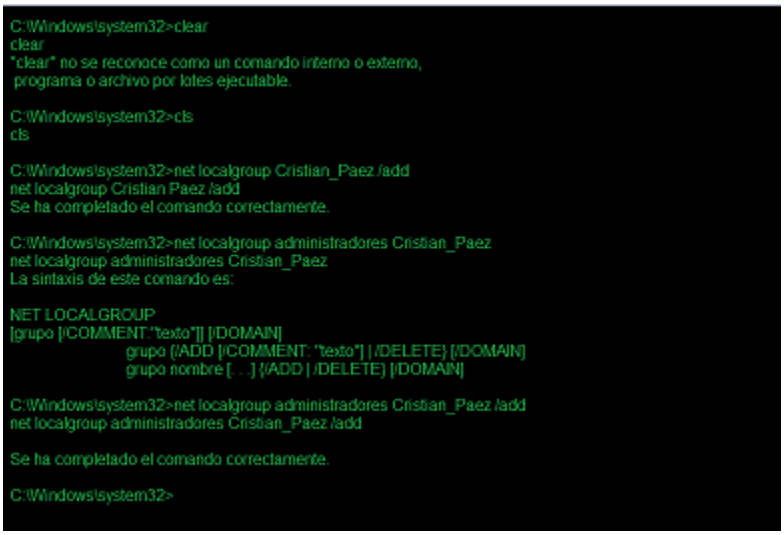
Ingreso a shell



Fuente: Elaboración propia

Figura 16. Ingreso a shell

Creación del usuario con privilegios de administrador (Cristian Paez)



Fuente: Elaboración propia

Figura 17. Creación del usuario con privilegios de administrador (Cristian Paez)

Evidencia creación del usuario **Cristian Paez** como administrador

Fuente: Elaboración propia

Figura 18. Evidencia creación del usuario **Cristian Paez** como administrador

La ejecución exitosa de la explotación de la vulnerabilidad en el sistema Windows 7 y la posterior creación de una cuenta de usuario con privilegios de administrador permiten extraer las siguientes conclusiones significativas para el presente ejercicio de Red Team:

Vulnerabilidad Confirmada y Explotable: Se ha validado la existencia de una vulnerabilidad crítica en la aplicación Rejetto HTTP File Server versión 2.3, la cual puede ser explotada remotamente para obtener acceso no autorizado al sistema operativo subyacente. La facilidad con la que se logró la ejecución de código y el establecimiento de una sesión Meterpreter subraya la severidad del fallo de seguridad.

Compromiso Total del Sistema Potencial: La obtención de una sesión Meterpreter con privilegios de SYSTEM demuestra el potencial para un compromiso total del sistema afectado. Un atacante con estas capacidades podría realizar una amplia gama de acciones maliciosas, incluyendo la exfiltración de información sensible, la instalación de software malintencionado, la manipulación de archivos y la interrupción de servicios críticos.

Escalada de Privilegios Exitosa: La capacidad de crear una cuenta de usuario con privilegios de administrador evidencia una escalada de privilegios exitosa. Esta acción permite al atacante mantener persistencia en el sistema, incluso si la vulnerabilidad inicial es parcheada o el servicio vulnerable se desactiva. La nueva cuenta de administrador se convierte en una puerta trasera permanente para el acceso no autorizado.

Impacto Significativo en la Seguridad de la Organización: La presencia de una vulnerabilidad explotable que permite el acceso remoto y la escalación de privilegios representa un riesgo significativo para la seguridad de la organización. La fuga de información, el objetivo inicial del ejercicio, se ve facilitada enormemente por este nivel de acceso. Además, la capacidad de crear cuentas de administrador podría permitir a un atacante expandir su control a otros sistemas dentro de la red.

Necesidad Urgente de Mitigación: Los resultados de este ejercicio de Red Team resaltan la necesidad urgente de implementar medidas de mitigación para abordar la vulnerabilidad identificada en Rejetto HTTP File Server. Esto incluye la actualización a una versión segura, la desinstalación del software si no es esencial, o la implementación de controles de seguridad perimetrales y de host para limitar la exposición y el impacto potencial de un ataque.

Eficacia de las Técnicas de Red Team: El ejercicio demuestra la eficacia de las metodologías y herramientas del Red Team para identificar y explotar vulnerabilidades reales en los sistemas de la organización. Esta capacidad es crucial para evaluar la postura de seguridad actual y para proporcionar información actionable para la mejora de las defensas.

Prueba de Concepto para la Alta Dirección: La creación exitosa de un usuario administrador sirve como una Prueba de Concepto (PoC) clara y contundente para la alta dirección. Demuestra de manera práctica el impacto potencial de la vulnerabilidad y la necesidad de invertir en medidas de seguridad proactivas.

En resumen, la explotación exitosa de la vulnerabilidad y la creación de un usuario administrador evidencian una brecha de seguridad crítica que podría tener consecuencias graves para la confidencialidad, integridad y disponibilidad de la información y los sistemas de la organización. Se requiere una acción inmediata para remediar esta situación y fortalecer la postura de seguridad general.

4. Contención de ataques informaticos

De manera individual usted deberá leer el problema que se encuentra en el anexo 5 – escenario 4 referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

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

Ante un ataque en tiempo real, la prioridad absoluta es la **contención y la preservación de la evidencia**. Centraría un protocolo de respuesta a incidentes inmediato, con argumentos técnicos sólidos utilizando herramientas de código abierto como se indica en el Anexo 5.

Prioridad Máxima: Contención Rápida y Preservación del Estado (Kill Chain Interruption)

Al encontrarme frente a un ataque informático en tiempo real, la acción inicial y más crítica es **interrumpir la cadena de ataque (kill chain)** para **contener la propagación del daño** y, simultáneamente, **preservar la mayor cantidad de evidencia digital posible** para un análisis forense posterior.

A continuación detallo los pasos técnicos iniciales y por qué:

1-Evaluación Rápida del Impacto y Alcance (Triaje de Incidentes):

Indagación: La primera pregunta sería: "¿Qué sistemas están afectados y cuál es la naturaleza aparente del ataque?" Buscaría rápidamente signos de compromiso en la máquina Windows objetivo (CPU/RAM elevadas, actividad de red inusual, procesos desconocidos). La experiencia previa con la vulnerabilidad de Rejetto HFS 2.3 y la creación de un usuario administrador me orientaría a buscar actividad post-explotación asociada a ese vector.

Acción Técnica:

Aislamiento de Red (Micro-segmentación/Air Gap): Lo primero sería **desconectar la máquina Windows de la red corporativa**. Esto puede ser un puerto de red físico, deshabilitar la interfaz de red, o configurar reglas de firewall temporales para bloquear todo el tráfico saliente y entrante, excepto el necesario para la gestión de la máquina (si la contención física no es inmediata). Esto evita la propagación lateral del ataque a otros sistemas y la exfiltración de datos.

Monitoreo Activo de Procesos y Conexiones (Herramientas GPL):

Netstat (Built-in en Windows): Ejecutaría netstat -ano para identificar todas las conexiones de red activas, sus estados, y los IDs de proceso (PID) asociados. Esto me permitiría ver conexiones salientes sospechosas (C2 - Command & Control) o servicios de escucha no autorizados.

Sysinternals Suite (Sysmon, Procmon, Process Explorer - si se pudiera instalar antes del ataque, sino, para análisis de la copia forense): Aunque no es GPL, Process Explorer es una herramienta fundamental para ver árboles de procesos, identificar procesos maliciosos

camuflados y observar sus conexiones de red. Sysmon, si estuviera previamente desplegado, sería invaluable para la telemetría. Dado el "no presupuesto", buscaría alternativas como "Tasklist" y "Netstat" que vienen en el propio Windows.

Comandos de Powershell/CMD: Utilizaría comandos como tasklist /svc, sc queryex para listar servicios y whoami /priv para verificar privilegios del usuario actual si logré acceso.

2- Captura del Estado Volátil para Análisis Forense (Forensic Readiness):

Indagación: "¿Qué información volátil (RAM, conexiones activas, procesos) se está perdiendo en este momento y cómo puedo capturarla?" La memoria RAM contiene el estado actual del atacante, incluyendo procesos, claves y datos.

Acción Técnica (Herramientas GPL/Nativas):

Volcado de Memoria RAM: Aunque las herramientas premium como Mandiant (anteriormente FireEye) o Redline son ideales, en un escenario sin presupuesto, se buscarían soluciones como **FTK Imager Lite** (versión gratuita de AccessData, aunque no es puramente GPL, a menudo se usa en entornos educativos por su capacidad de volcado de RAM) o se consideraría el uso de scripts de PowerShell o herramientas específicas de volcado si existieran opciones GPL. El objetivo es obtener una imagen forense de la memoria RAM para análisis posterior.

Captura de Tráfico de Red (en el punto de contención): Si es posible en el punto de aislamiento (por ejemplo, en un switch gestionado), se configuraría un SPAN port o port mirroring para capturar el tráfico de red de la máquina antes de un aislamiento total. Esto se

analizaría con **Wireshark** (GPL) en una máquina segura para identificar patrones de comunicación maliciosos, exfiltración de datos o comandos de C2.

3- Identificación Preliminar del Vector de Intrusión (IOCs):

Indagación: "¿Cómo entró el atacante y qué Indicadores de Compromiso (IOCs) puedo identificar rápidamente?" Me enfocaría en el puerto 8080 (o 8895 si es el caso) y la aplicación Rejetto HFS 2.3, ya que son el vector de ataque conocido.

Acción Técnica:

Revisión de Logs de Eventos de Windows: Accedería al Visor de Eventos de Windows (Event Viewer) para buscar entradas anómalas: intentos de inicio de sesión fallidos, creación de usuarios (especialmente "cristian paez" o similar), cambios en el firewall, errores de aplicaciones o servicios relacionados con Rejetto HFS.

Análisis de Archivos y Directorios Modificados Recientemente: Buscaría archivos recién creados o modificados en directorios temporales, de usuario, o de la propia aplicación Rejetto HFS, que podrían ser artefactos del exploit o del payload.

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?

De acuerdo al ejercicio realizado propondría las siguientes medidas de *hardening.*

1-Parcheo y Actualización de Software y Sistema Operativo:

Prioridad Máxima: Actualizar o Remover Rejetto HTTP File Server: La vulnerabilidad central fue la versión 2.3 de Rejetto HFS. La medida más directa es **actualizar Rejetto HFS a una versión no vulnerable** o, preferiblemente, **desinstalarlo** si no es una aplicación crítica y esencial para las operaciones de la organización. Si es indispensable, evaluar alternativas más seguras.

Actualización de Windows 7: El escenario mencionó que el sistema era Windows 7, y se detectaron vulnerabilidades como **UNSUPPORTED WINDOWS OS (REMOTO) (Crítico)**, **MS11-030 (Crítico)**, **MS17-010 (Alto)** y **MS16-047 (Medio)**. Windows 7 ya no cuenta con soporte oficial de Microsoft, lo que significa que no recibe parches de seguridad. La medida de *hardening* ideal y más robusta es la **migración urgente a un sistema operativo moderno y con soporte activo** (ej., Windows 10/11 o una distribución de Linux adecuada), asegurando que todas las actualizaciones de seguridad estén instaladas y se mantengan al día automáticamente. Esto abordaría directamente las vulnerabilidades "UNSUPPORTED WINDOWS OS" y otras que se encuentran parcheadas en versiones más recientes.

2-Gestión de Puertos y Servicios (Principio de Mínimo Privilegio y Exposición):

Restricción de Puertos: Es fundamental que solo los puertos estrictamente necesarios para la operación de la empresa estén abiertos. En este caso, si Rejetto HFS usaba un puerto específico (como el 8895 o el 8080 en el ejemplo del Red Team), se debería bloquear ese puerto en el firewall perimetral y en el firewall del host.

Deshabilitación de Servicios Innecesarios: Realizar una auditoría de los servicios en ejecución en el sistema operativo Windows y deshabilitar aquellos que no sean esenciales. Servicios como SMB (afectado por MS17-010) deben ser configurados de forma segura, o deshabilitados si no se usan, y sus versiones más antiguas deben ser parchadas o deshabilitadas.

3-Endurecimiento del Firewall de Host (Windows Firewall):

Activación y Configuración Estricta: Si se desactivó el firewall de Windows para el análisis de Red Team, la primera medida post-ataque sería **activarlo y configurarlo con reglas de "denegar por defecto"** para el tráfico entrante y saliente, permitiendo explícitamente solo el tráfico y los servicios absolutamente necesarios para las funciones de la máquina. Esto actúa como una primera línea de defensa a nivel de host.

4-Gestión de Cuentas y Privilegios (Principio de Mínimo Privilegio):

Eliminación del Usuario Malicioso: El usuario "Cristian Paez" o cualquier otro usuario creado por el atacante con privilegios de administrador debe ser **eliminado inmediatamente** y de forma segura.

Auditoría de Cuentas de Usuario: Realizar una auditoría completa de todas las cuentas de usuario existentes en el sistema Windows, eliminando las cuentas no autorizadas o inactivas.

Políticas de Contraseñas Fuertes: Implementar y hacer cumplir políticas de contraseñas complejas y rotación periódica para todas las cuentas, especialmente las de administrador.

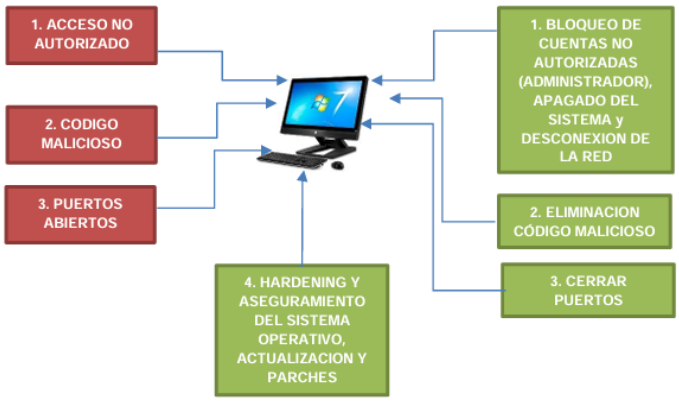
Implementación de LAPS (Local Administrator Password Solution) o Soluciones Similares: Para entornos de dominio, LAPS ayuda a gestionar contraseñas únicas y aleatorias para las cuentas de administrador locales.

5-Monitoreo y Detección Continuos (Visibilidad del Entorno):

Implementación de SIEM/Log Management: Centralizar los logs de eventos de Windows (Security, System, Application) y de la aplicación Rejetto HFS (si se mantiene) en un sistema de gestión de eventos e información de seguridad (SIEM) como **ELK Stack (Elasticsearch, Logstash, Kibana)** o **Splunk (versión gratuita/comunidad)** para una monitorización en tiempo real y detección de anomalías. Esto permitiría identificar intentos de ataque o actividades post-explotación.

Uso de EDR (Endpoint Detection and Response) o Equivalentes GPL: Si bien las soluciones EDR suelen ser de pago, se buscarían herramientas de código abierto como **OSSEC** o **Wazuh** (ambas GPL) para la detección de intrusiones a nivel de host (HIDS). Estas herramientas pueden monitorear la integridad de archivos, actividad de procesos y configuraciones del sistema, alertando sobre cambios sospechosos que podrían indicar un compromiso.

Estrategia de contención



Fuente: Elaboración propia

Figura 19. Estrategia de contención

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

Distinción entre Blue Team y Equipo de Respuesta a Incidentes

Aunque a menudo se les agrupa o se les confunde debido a su misión compartida de proteger los activos de una organización, el **Blue Team** y el **Equipo de Respuesta a Incidentes** operan con enfoques, horizontes temporales y especializaciones tácticas distintos dentro del marco de la ciberseguridad defensiva.

El Blue Team: La Vanguardia Defensiva y el Monitoreo Proactivo

El Blue Team representa la **línea de defensa operativa y estratégica continua** de una organización. Su misión principal es la **protección proactiva** de los sistemas, redes y datos, lo que implica un ciclo constante de hardening, monitoreo y detección de amenazas. Sus responsabilidades abarcan:

Prevención y Fortificación: Implementan y mantienen controles de seguridad (ej., firewalls, IPS/IDS, EDR, segmentación de red, gestión de vulnerabilidades, parches, hardening de sistemas). Su trabajo consiste en construir barreras y endurecer la infraestructura para hacerla más resistente a los ataques.

Detección Continua: Operan sistemas de monitoreo (SIEM, plataformas de análisis de logs, herramientas de visibilidad de red) para identificar anomalías, actividades sospechosas o indicadores de compromiso (IoCs) en tiempo real o casi real. Buscan patrones, alertas y comportamientos que puedan preceder o señalar un ataque en curso.

Análisis y Amenaza Inteligente: Utilizan *threat intelligence* para entender las tácticas, técnicas y procedimientos (TTPs) de los adversarios, anticipando posibles ataques y ajustando las defensas.

Mejora Continua (Shift Left): Realizan auditorías internas, ejercicios de *red teaming* (con el Red Team) y pruebas de penetración para descubrir y remediar debilidades antes de que sean explotadas.

Blue Team es el **guardián diario que vigila las murallas, las repara, y las fortalece constantemente, mientras está atento a cualquier intento de asedio.** Su enfoque es **mantener la higiene de seguridad** y **detectar intrusiones antes de que se conviertan en crisis.**

El Equipo de Respuesta a Incidentes Los Especialistas en Crisis y Recuperación

El IR Team es una **unidad especializada que se activa específicamente cuando un incidente de seguridad ha ocurrido, está en progreso, o ha sido confirmado.** Su rol es intrínsecamente reactivo y se centra en la gestión de crisis. Su metodología sigue fases bien definidas, como las establecidas por el NIST (Preparación, Detección y Análisis, Contención, Erradicación y Recuperación, y Actividades Post-Incidente):

Contención: Su prioridad inicial es limitar el alcance y el impacto del incidente. Esto puede implicar aislar sistemas comprometidos, bloquear comunicaciones maliciosas o deshabilitar cuentas.

Erradicación: Una vez contenido, el objetivo es eliminar la causa raíz del incidente, como el malware, las puertas traseras o las configuraciones de acceso no autorizadas.

Recuperación: Trabajan para restaurar los sistemas y servicios afectados a su estado operativo normal y seguro, asegurando que las operaciones críticas puedan reanudarse con mínima interrupción.

Análisis Forense: Realizan una investigación profunda para entender cómo ocurrió el incidente, qué sistemas fueron afectados, qué datos fueron comprometidos y quién fue el atacante. Esto genera inteligencia que retroalimenta al Blue Team.

Lecciones Aprendidas: Documentan el incidente y sus lecciones para mejorar los procesos de seguridad y prevención futuros.

El IR Team es, por lo tanto, el **"equipo de bomberos" cibernético que se lanza a la acción cuando la alarma ya suena y el fuego está declarado.** Su especialidad es **apagar el incendio, evaluar los daños, y reconstruir para evitar futuras conflagraciones similares.**

Interconexión y Diferencias Clave:

Temporalidad: El Blue Team opera de forma continua y proactiva, mientras que el IR Team opera de forma puntual y reactiva frente a incidentes específicos.

Alcance: El Blue Team tiene un alcance más amplio, centrado en la postura de seguridad general. El IR Team tiene un alcance más estrecho y profundo, centrado en la gestión de un incidente particular.

Objetivo Principal: El Blue Team busca prevenir y detectar. El IR Team busca contener, erradicar y recuperar tras una violación.

Habilidades: Aunque hay solapamiento, el Blue Team a menudo tiene más experiencia en configuración de seguridad, monitoreo y análisis de vulnerabilidades, mientras que el IR Team sobresale en análisis forense digital, *malware analysis* y gestión de crisis.

4. ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS “Center For Internet Security”, usted lo utilizaría para qué fin?

Si como miembro de un Blue Team me indican que debo trabajar con los **CIS (Center for Internet Security) Benchmarks y Controls**, los utilizaría para el siguiente fin primordial:

Utilización de los CIS Benchmarks y Controls en el Contexto del Blue Team:

Dentro de un equipo Blue Team, los **CIS Benchmarks** y los **CIS Critical Security Controls (CIS Controls)** son herramientas y guías de referencia de valor incalculable que utilizaría para:

Establecimiento y Mantenimiento de una Postura de Seguridad Robusta (Hardening Proactivo):

Propósito: Los CIS Benchmarks proporcionan configuraciones de seguridad prescriptivas y consensuadas por expertos para sistemas operativos (como Windows 7, aunque para versiones más recientes tendríamos benchmarks actualizados), aplicaciones, dispositivos de red y entornos de nube. Los utilizaría como la **guía principal para el endurecimiento (hardening) de los sistemas**, asegurando que nuestras máquinas y aplicaciones estén configuradas con las mejores prácticas de seguridad conocidas. Esto incluye ajustar configuraciones de firewall, políticas de contraseñas, configuraciones de servicios, permisos de archivos, etc.

Argumento Técnico: Al implementar las recomendaciones del CIS Benchmark para Windows, como la desactivación de servicios no esenciales, la aplicación de políticas de bloqueo de cuentas, o la configuración segura de servicios SMB, se reduce significativamente la superficie de ataque y se dificulta la explotación de vulnerabilidades conocidas o de día cero. Esto va directamente en línea con el objetivo de prevenir ataques antes de que ocurran.

Evaluación Continua de la Higiene de Seguridad y Detección de Desviaciones (Auditoría y Conformidad):

Propósito: Los CIS Controls (especialmente los primeros y más fundamentales como el Control 1: Inventario y Control de Activos de Hardware, o el Control 3: Gestión Continua de Vulnerabilidades) proporcionan una hoja de ruta priorizada de acciones de seguridad. Los Benchmarks, por su parte, se utilizan para auditar y validar la conformidad de nuestros sistemas con esas configuraciones de seguridad. Utilizaría los Benchmarks para **escanear y comparar la configuración actual de nuestras máquinas** (incluida la máquina Windows 7 analizada) **contra las recomendaciones del CIS**, identificando cualquier desviación que represente una debilidad de seguridad.

Argumento Técnico: Herramientas de código abierto como OpenSCAP o scripts personalizados pueden automatizar la verificación de la conformidad con los CIS Benchmarks. Identificar y remediar estas desviaciones de forma proactiva es fundamental para cerrar las brechas que un Red Team o un atacante real podrían explotar, como la presencia de versiones de software sin parches (ej. Rejetto HFS 2.3) o servicios innecesarios.

Priorización de Esfuerzos de Mitigación y Respuesta (Gestión de Riesgos)[11]:

Propósito: Los CIS Controls no solo listan acciones, sino que las priorizan (Control 1-5 son básicos y cruciales). Los utilizaría para **enfocar nuestros recursos limitados en las medidas de seguridad que ofrecen el mayor retorno de inversión en protección**. Si, por ejemplo, los CIS Controls priorizan la gestión de vulnerabilidades y el parcheo, eso confirmaría la necesidad de actualizar o retirar aplicaciones como Rejetto HFS.

Argumento Técnico: Al alinear nuestras acciones con los CIS Controls, nos aseguramos de abordar los vectores de ataque más comunes y efectivos, como la explotación de vulnerabilidades conocidas (CVEs) o la escalada de privilegios a través de configuraciones débiles, que fueron centrales en el ataque simulado de Red Team. Esto permite al Blue Team ser más eficiente en la asignación de sus esfuerzos defensivos.

Explique y redacte las funciones y características principales de lo que es un SIEM.

SIEM: El Centro de Inteligencia y Coordinación de la Ciberdefensa

Un **SIEM (Security Information and Event Management)** es una solución integral de software que combina las funciones de **SIM (Security Information Management)** y **SEM (Security Event Management)**. Su propósito fundamental es proporcionar a las organizaciones una **visibilidad centralizada y correlacionada** de sus eventos de seguridad y de información a

[11] Mintic 2014, Gestión de Incidentes, (Pag 29), https://www.mintic.gov.co/gestionti/615/articles5482_G21_Gestion_Incidentes.pdf

lo largo de toda su infraestructura de TI, permitiendo la detección temprana de amenazas, el cumplimiento normativo y una respuesta a incidentes más eficiente.[12]

Funciones Principales:

Recopilación y Normalización de Logs (Log Collection & Normalization):

El SIEM ingiere datos de eventos (logs) de una miríada de fuentes heterogéneas: sistemas operativos (Windows Event Logs, Syslog de Linux), aplicaciones (servidores web, bases de datos), dispositivos de red (firewalls, routers, switches), sistemas de detección de intrusiones (IDS/IPS), antivirus, etc.

Posteriormente, normaliza estos logs, es decir, los transforma a un formato común y estructurado. Esto es crucial porque diferentes fuentes generan logs con formatos y terminologías variadas.[13]

Correlación de Eventos (Event Correlation):

Esta es la función distintiva y más poderosa de un SIEM. No solo recolecta logs, sino que los analiza en tiempo real o casi real para encontrar relaciones y patrones entre eventos que, de forma aislada, podrían parecer insignificantes. Por ejemplo, múltiples intentos de inicio de sesión fallidos en una cuenta seguidos por un inicio de sesión exitoso desde una IP inusual.

[12] IMPLEMENTACION DE UN GESTOR DE SEGURIDAD DE LA INFORMACION Y GESTION DE EVENTOS (SIEM). Juan David Pedroza Arango. Universidad de San Buenaventura. Medellín 2016, http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedr oza_2016.pdf

Utiliza reglas predefinidas y, en SIEMs más avanzados, algoritmos de machine learning (ML) y análisis de comportamiento de usuarios y entidades (UEBA) para identificar secuencias de eventos que indican un posible ataque o una violación de política.[14]

Alertas y Notificaciones (Alerting & Notifications):

Cuando el SIEM detecta un patrón correlacionado que coincide con una regla de amenaza o un umbral de anomalía, genera una alerta.

Estas alertas se envían a los analistas de seguridad a través de diversos canales (correo electrónico, SMS, paneles de control, integración con sistemas de gestión de tickets) para que puedan investigar y responder.

Análisis Forense y Búsqueda de Amenazas (Forensic Analysis & Threat Hunting):

Almacena grandes volúmenes de datos de logs a largo plazo, lo que permite a los analistas de seguridad realizar búsquedas históricas detalladas para investigar incidentes pasados o realizar actividades proactivas de *threat hunting* (búsqueda de amenazas).

Proporciona capacidades de búsqueda avanzadas y visualizaciones para explorar los datos, identificar Indicadores de Compromiso (IoCs) y entender la cronología de un ataque.

[14] Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Generación de Informes y Cumplimiento Normativo (Reporting & Compliance):

Ayuda a las organizaciones a cumplir con diversas normativas y estándares (GDPR, HIPAA, PCI DSS, SOX) al proporcionar informes predefinidos y personalizables que demuestran la monitorización de seguridad y la gestión de eventos.

Facilita la auditoría de la actividad del usuario y del sistema para asegurar la adherencia a las políticas internas.

Características Principales:

Centralización: Agrega logs de toda la infraestructura en un único repositorio, ofreciendo una vista unificada.

Tiempo Real: Capacidad de procesar y correlacionar eventos a medida que ocurren, permitiendo una detección y respuesta rápidas.

Escalabilidad: Diseñado para manejar volúmenes masivos de datos de logs (terabytes al día) y escalar a medida que crece la infraestructura de la organización.

Automatización: Puede automatizar ciertas respuestas a incidentes (ej., bloqueo de IP sospechosas a través de integración con firewalls) o la creación de tickets.

Contextualización: Enriquece los datos de los logs con inteligencia de amenazas (feeds de IoCs, reputación de IPs) y datos de contexto de activos para mejorar la precisión de las alertas y reducir los falsos positivos.

Retención de Datos: Almacena logs de forma segura y accesible para auditorías y análisis forenses durante períodos prolongados, según los requisitos de cumplimiento.

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Herramientas de Contención en Ciberseguridad: Bloqueando la Propagación del Ataque

Las herramientas de contención son aquellas que, una vez detectado un ataque, se utilizan activamente para **limitar su alcance, prevenir su propagación y minimizar el daño continuo** a los sistemas y datos de la organización. A diferencia de las herramientas de detección que alertan sobre la presencia de una amenaza, las de contención actúan directamente para mitigar el incidente.

Aquí se describen tres tipos de herramientas o mecanismos de contención esenciales:

Firewall de Siguiente Generación (NGFW) / Firewall de Aplicación Web (WAF) - Hardware/Software:

Función de Contención: Estos dispositivos o soluciones de software no solo filtran el tráfico basándose en puertos y protocolos (como los firewalls tradicionales), sino que también tienen la capacidad de **inspeccionar el contenido del tráfico (DPI - Deep Packet Inspection)**, identificar patrones de ataque conocidos, y aplicar políticas de seguridad a nivel de aplicación. En un contexto de contención, un NGFW o WAF puede ser reconfigurado rápidamente para **bloquear tráfico específico hacia o desde una IP comprometida**, **cerrar puertos vulnerables detectados**, **bloquear payloads maliciosos** (como los utilizados en la explotación de Rejetto HFS) o **denegar el acceso a recursos críticos** para una IP de origen sospechosa o a un tipo de

tráfico anómalo. Un WAF es particularmente efectivo para contener ataques dirigidos a aplicaciones web vulnerables, bloqueando la inyección de código o los intentos de ejecución remota antes de que lleguen al servidor.[15]

Características Principales:

Control Granular de Tráfico: Permite la creación de reglas de filtrado muy específicas basadas en usuarios, aplicaciones, contenido y comportamiento.

Prevención de Intrusiones (IPS): A menudo incluyen módulos IPS que detienen proactivamente exploits conocidos.

Análisis de SSL/TLS: Capaces de descifrar y analizar el tráfico cifrado para identificar amenazas ocultas.

Integración: Pueden integrarse con SIEMs para una respuesta automatizada a incidentes.

Sistema de Detección/Prevención de Intrusiones en el Host (HIDS/HIPS) / Software de Endpoint Detection and Response (EDR) - Software:

Función de Contención: Mientras que los HIDS (como OSSEC o Wazuh) son excelentes para detectar actividades sospechosas en el endpoint (ej. modificación de archivos críticos, creación de usuarios, cambios en el registro), las soluciones HIPS y EDR modernas van un paso más allá al ofrecer **capacidades activas de contención a nivel del host.** Esto significa que pueden **terminar procesos maliciosos**, **aislar el endpoint de la red** (lo que se conoce como "network quarantine" o "host isolation"), **eliminar archivos maliciosos**, o **revertir cambios no**

[15] OSSEC, Host Intrusion Detection for Everyone https://www.ossec.net/

autorizados en el sistema de archivos o el registro. En el caso de la máquina Windows 7 comprometida, un EDR podría haber detenido la ejecución del payload de Metasploit o aislado la máquina antes de que se pudiera crear el usuario administrador.

Características Principales:

Monitorización en Tiempo Real: Supervisan continuamente la actividad del sistema de archivos, procesos, memoria y red en el endpoint.
Capacidades de Respuesta: Permiten acciones automáticas o manuales de contención directamente en el endpoint afectado.
Visibilidad Profunda: Recopilan telemetría detallada del comportamiento del sistema, lo que ayuda en el análisis forense.
Análisis Comportamental: Utilizan heurísticas y análisis de comportamiento para detectar amenazas desconocidas.

Mecanismos de Segmentación de Red (VLANs, ACLs en Switches) - Hardware/Software (Configuración):
Función de Contención: Aunque no son herramientas "per se", los mecanismos de segmentación de red son estrategias de infraestructura que se utilizan para la contención. En caso de un ataque, la capacidad de **aislar rápidamente un segmento de red o un dispositivo específico** mediante la reconfiguración de VLANs (Virtual Local Area Networks) o Listas de Control de Acceso (ACLs) en switches gestionados es una forma efectiva de contención. Si la máquina Windows 7 estuviera comprometida, podríamos moverla a una VLAN de cuarentena o

aplicar una ACL en el switch para bloquear su comunicación con el resto de la red interna y externa, permitiendo solo el tráfico necesario para la remedia. Esto detiene la propagación lateral del ataque y la exfiltración de datos.[16]

Características Principales:

Separación Lógica: Permite dividir una red física en múltiples redes lógicas.

Control de Flujo: Las ACLs permiten controlar qué tráfico puede pasar entre diferentes segmentos o hacia/desde puertos específicos.

Flexibilidad: La reconfiguración de VLANs o ACLs puede hacerse de forma remota y rápida en switches gestionados, lo que es vital en una respuesta a incidentes en tiempo real.

Principio de Mínimo Privilegio de Red: Limita la comunicación entre sistemas, reduciendo la superficie de ataque y el impacto de una brecha.

Estas herramientas y estrategias de contención son vitales para el Blue Team, ya que transforman la detección de una amenaza en una acción concreta para mitigar el riesgo y proteger la infraestructura organizacional.

[16] CONFIGSERVER SECURITY AND FIREWALL (CSF), https://configserver.com/configserversecurity-and-firewall/

Recomendaciones estrategicas

Las siguientes recomendaciones están diseñadas para potenciar la resiliencia cibernética de las organizaciones, tanto en el desarrollo e implementación de las capacidades de Red Team y Blue Team, como en el fortalecimiento general de la postura de seguridad.

Habilitadores Clave para la Sinergia Red Team & Blue Team

Para el establecimiento y la consolidación de estrategias efectivas entre los equipos de simulación de ataque (Red Team) y defensa (Blue Team), es imperativo considerar los siguientes pilares:

Capital Humano Especializado: La columna vertebral de cualquier estrategia robusta de ciberseguridad reside en el talento humano. Es fundamental contar con profesionales altamente cualificados y expertos, con un dominio profundo en sus respectivas áreas de acción. Para el Red Team, esto implica perfiles con destrezas avanzadas en técnicas ofensivas y pensamiento lateral; para el Blue Team, expertos en detección, análisis forense y respuesta a incidentes. Se recomienda encarecidamente que este personal acredite su experticia mediante certificaciones internacionales específicas para roles ofensivos y defensivos en ciberseguridad, lo que valida su competencia y asegura la adhesión a los más altos estándares de la industria.

Acumulación de Experiencia Práctica: Más allá de la formación teórica, la experiencia operativa es un factor determinante en la eficacia de ambos equipos. La práctica constante en el análisis de vulnerabilidades, la formulación de controles defensivos, la detección y contención

proactiva de ataques, y la gestión de la recuperación post-incidente, permite a los equipos desarrollar una agudeza estratégica indispensable. Esta acumulación de conocimiento práctico es crucial para anticipar y neutralizar amenazas complejas, así como para diseñar respuestas ágiles frente a cualquier contingencia que pueda afectar la seguridad organizacional.

Compromiso y Respaldo de la Alta Dirección: El éxito de cualquier iniciativa de ciberseguridad, y especialmente la integración de capacidades Red Team y Blue Team, depende fundamentalmente del apoyo irrestricto de la alta gerencia. Este respaldo no solo legitima los esfuerzos de seguridad, sino que es vital para la asignación de los recursos financieros y tecnológicos necesarios. Una inversión estratégica en estos equipos y en una cultura de seguridad robusta representa una salvaguarda económica a futuro, minimizando las pérdidas potenciales derivadas de un incidente cibernético mayor.

Marco Ético y Legal Riguroso: Toda operación de ciberseguridad, especialmente las simulaciones de ataque realizadas por el Red Team, debe adherirse estrictamente a un sólido marco ético y legal. Es crucial que los equipos comprendan y respeten los límites de sus acciones para evitar consecuencias adversas, tanto para la organización como para los individuos. Por consiguiente, cualquier estrategia implementada debe estar intrínsecamente acompañada de un entorno normativo y legislativo claro, que garantice la ejecución de actividades de seguridad de forma segura, responsable y plenamente conforme con las leyes vigentes.

Link video sustentación: Video Seminario Red team Blue team.mp4

Conclusiones

Conclusiones y Aportes al Conocimiento en Ciberseguridad.

El desarrollo del presente Informe ha permitido consolidar una serie de hallazgos y conocimientos fundamentales desde la perspectiva de la ciberseguridad, articulando la teoría con la aplicación práctica.

Fundamentación de Capacidades en Seguridad Ofensiva y Defensiva: Este estudio ha enriquecido significativamente la comprensión de los roles especializados en ciberseguridad, específicamente los de los equipos Red Team y Blue Team. Asimismo, ha profundizado en el marco normativo colombiano aplicable a la protección de datos e información, y en la metodología para el establecimiento de un entorno de pruebas controlado ('banco de trabajo'). Esto sienta las bases esenciales para la ejecución estructurada de evaluaciones de seguridad en organizaciones y entidades, asegurando la adhesión a regulaciones nacionales y estándares internacionales de ciberseguridad.

Metodología Práctica para Pruebas de Seguridad: Se ha establecido un sólido precedente práctico para el desarrollo de futuras pruebas de seguridad en diversos niveles de complejidad. La experiencia de configurar y operar un laboratorio virtualizado con herramientas de código abierto ampliamente utilizadas, valida una metodología efectiva para la identificación y análisis de vulnerabilidades, lo que permite replicar escenarios de ataque-defensa de forma controlada y eficiente.

Clarificación del Marco Ético y Legal en Hacking Ético: La investigación ha desentrañado aspectos críticos sobre la legislación colombiana relativa a los delitos informáticos y ha clarificado los principios éticos que rigen la conducta de los profesionales en seguridad de la información. Este análisis es vital para comprender el alcance y las responsabilidades de los miembros de un Red Team y un Blue Team, subrayando la delicada línea entre la práctica del hacking ético y la transgresión ilegal. Se enfatiza la extrema sensibilidad de cruzar los límites éticos y normativos al ejecutar este tipo de labores.

Validación de Acuerdos de Confidencialidad y Legislación Aplicable: Los ejercicios prácticos y las actividades desarrolladas han reforzado la comprensión sobre la legislación colombiana en delitos informáticos y las implicaciones éticas. Este conocimiento es directamente aplicable a la formulación y validación de los acuerdos de confidencialidad que se establecen entre las organizaciones contratantes y los expertos en cibersegseguridad que integran los equipos Red Team y Blue Team, garantizando un marco de trabajo seguro y legalmente sólido.

Dominio Práctico en la Ejecución de Pentesting: La dimensión práctica de este trabajo ha sido fundamental, permitiendo la recreación y el seguimiento detallado de un ciclo completo de pentesting. Esta experiencia ha consolidado las habilidades para identificar vulnerabilidades en aplicaciones específicas mediante el uso de herramientas de software libre, y ha facilitado la creación de estrategias de trabajo eficientes para la detección de debilidades.

Identificación de Vulnerabilidades con Herramientas de Código Abierto: El estudio permitió la exitosa identificación de una vulnerabilidad utilizando herramientas de software libre. Esta experiencia no solo resalta la vital importancia de estas herramientas en las evaluaciones de

seguridad, sino que también proporcionó una invaluable oportunidad para el aprendizaje práctico de su sintaxis, funcionalidad y la metodología de aplicación en escenarios reales.

Impacto de la Preparación Previa y Material Académico: El conocimiento adquirido y el material didáctico suministrado a través del seminario previo fueron un pilar fundamental para la consecución exitosa del presente trabajo. La base teórica y las directrices previas resultaron ser un aporte decisivo para la planificación y la ejecución de las actividades propuestas, culminando en la consecución satisfactoria de los objetivos planteados.

Crucialidad de la Contención de Ataques en la Ciberdefensa: Se ha evidenciado que la contención de ataques es un componente ineludible de cualquier estrategia de seguridad empresarial moderna. Por ello, es imperativo que todo equipo Blue Team domine y aplique las mejores prácticas en contención, utilizando eficazmente las diversas herramientas disponibles. La disponibilidad de numerosas soluciones de software libre para la contención y detección de amenazas es una ventaja significativa, ya que permite a organizaciones de cualquier tamaño implementar defensas efectivas con una inversión de bajo costo, democratizando el acceso a capacidades críticas de ciberseguridad.

Estrategias para la Contención Efectiva de Incidentes: El trabajo práctico realizado no solo facilitó la identificación de un ataque específico, sino que también fue crucial para el diseño y la validación de estrategias adecuadas y eficaces para su contención inmediata, demostrando la capacidad de limitar el impacto de un incidente informático.

Referencia bibliograficas

Colombia. Congreso de la República. (2009, 6 de enero). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Diario Oficial No. 47.223. Recuperado de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

COPNIA. (s. f.). *Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares* (pp. 1-20). Recuperado de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

ConfigServer. (s. f.). *ConfigServer Security and Firewall (CSF)*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://configserver.com/configserversecurity-and-firewall/

Ethical Hacking. (2018, 27 de noviembre). *CÓMO USAR SEARCHSPLOIT PARA ENCONTRAR EXPLOITS*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://blog.ehcgroup.io/2018/11/27/01/00/39/4198/como-usarsearchsploit-para-encontrar-exploits/hacking/ehacking/

FUNCION PUBLICA. (2012). *Ley 1581 de 2012* (p. 1). Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Mintic. (2014). *Gestión de Incidentes* (p. 29). https://www.mintic.gov.co/gestionti/615/articles5482_G21_Gestion_Incidentes.pdf

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management)* (pp. 31-63). Usfq. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

NIST. (2007). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Oracle VM VirtualBox. (s. f.). *Downloads – Oracle VM VirtualBox*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://www.virtualbox.org/wiki/Downloads

OSSEC. (s. f.). *Host Intrusion Detection for Everyone*. https://www.ossec.net/

Pedroza Arango, J. D. (2016). *IMPLEMENTACION DE UN GESTOR DE SEGURIDAD DE LA INFORMACION Y GESTION DE EVENTOS (SIEM)*. Universidad de San Buenaventura. http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedroza_2016.pdf

Rapid7. (s. f.). *Metasploit Framework*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://www.rapid7.com/products/metasploit/

Rejetto. (s. f.). *HFS: HTTP File Server*. Recuperado el [Fecha de recuperación, p. ej., 25 de mayo de 2025], de https://hfs.rejetto.com/

SIC. (2009). *Ley 1273 de 2009* (p. 1). Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf