Capacidades técnicas, legales y de gestión para los equipos red team y blue team

Edisen Nesrley Rincón Arévalo

Asesor

Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Programa Ingeniería de Sistemas

Bogotá

2025

Resumen

Este documento expone los resultados obtenidos tras la ejecución de pruebas en un entorno controlado, aplicando técnicas y herramientas utilizadas por los equipos Red Team y Blue Team para la identificación de brechas de seguridad, la evaluación del nivel de vulnerabilidad del sistema y la implementación de soluciones destinadas al fortalecimiento de la seguridad empresarial, además, se incluye un análisis del marco legal vigente en Colombia en materia de ciberseguridad y protección de datos personales. Asimismo, se presentan diversas herramientas empleadas tanto por los equipos de seguridad informática como por los ciberdelincuentes, con el propósito de comprender sus aplicaciones y riesgos asociados.

Por último, se plantean conclusiones derivadas de los hallazgos obtenidos y una serie de recomendaciones orientadas a la adopción de medidas estratégicas que optimicen la protección de los sistemas informáticos.

***Palabras clave*:**

- Ciberseguridad
- Vulnerabilidad
- Explotación
- Pentesting
- Mitigación

Abstract

This document presents the results obtained after executing tests in a controlled environment, applying techniques and tools used by the Red Team and Blue Team to identify security breaches, assess system vulnerability levels, and implement solutions aimed at strengthening corporate security. It also includes an analysis of the current legal framework in Colombia regarding cybersecurity and personal data protection. It also presents various tools used by both IT security teams and cybercriminals, with the aim of understanding their applications and associated risks.

Finally, it presents conclusions derived from the findings and a series of recommendations aimed at adopting strategic measures to optimize the protection of IT systems.

Keywords:

1. Cybersecurity
2. Vulnerability
3. Exploitation
4. Pentesting
5. Mitigation

Glosario

- Ciberseguridad: Conjunto de prácticas, tecnologías y procesos diseñados para proteger la infraestructura digital, datos y sistemas contra ataques cibernéticos (Ciberseguridad, 2025).
- Cisco ASA y Firewall: Dispositivos y software para controlar y filtrar tráfico de red (Cisco, n.d.-a).
- CVE: Sistema de identificación de vulnerabilidades en software y hardware (CVE, n.d.).
- ExploitDB: Base de datos de exploits y vulnerabilidades (ExploitDB, n.d.).
- Explotación (Exploitation): Proceso por el cual un atacante aprovecha una vulnerabilidad para acceder, manipular o dañar un sistema o datos (Jones, 2020).
- IDS/IPS: Sistemas de detección y prevención de intrusiones en red (McAfee, n.d.).
- *Ley 1273 de 2009*: Penaliza delitos informáticos y regula la protección de la información y datos digitales (Policía Nacional de Colombia, n.a.).
- *Ley 1581 de 2012*: Regula la protección de datos personales, asegurando derechos y obligaciones para el manejo de información personal en Colombia (Ley 1581, 2012).
- Metasploit: Framework para realizar evaluaciones de seguridad, creación de exploits y simulación de ataques (Metasploit, 2025).
- Mitigación: Conjunto de acciones destinadas a reducir el riesgo o el impacto de amenazas o vulnerabilidades en un sistema (Tǫ́werwall, n.d.).
- Nmap: Herramienta de análisis de redes para detección de hosts y vulnerabilidades (Manish, 2025).

- OpenVAS: Escáner de vulnerabilidades de código abierto (Greenbone Networks, 2025).
- Pentesting (Pruebas de penetración): Evaluación controlada de la seguridad que simula ataques para identificar vulnerabilidades en sistemas y redes (Kumar & Kumari, 2020).
- SIEM: Sistema de Gestión de Información y Eventos de Seguridad para análisis y respuesta en tiempo real (IBM, n.d.-a).
- Vulnerabilidad: Debilidad en un sistema, aplicación o infraestructura que puede ser explotada por actores maliciosos para comprometer su integridad, confidencialidad o disponibilidad (NVD, n.d.).

Contenido

Lista de Tablas

Lista de Figuras

Introducción

En el ámbito de la ciberseguridad, las pruebas de penetración son un mecanismo esencial para identificar vulnerabilidades y evaluar la resiliencia de los sistemas ante posibles ataques. Estas pruebas se desarrollan bajo metodologías especializadas y son ejecutadas por los equipos Red Team y Blue Team, cuya interacción permite una evaluación integral de los riesgos y la implementación de estrategias de protección eficaces.

Los Red Teams simulan ataques reales, empleando técnicas avanzadas similares a las utilizadas por hackers y ciberdelincuentes para comprometer infraestructuras digitales.

Entre las herramientas más utilizadas por los atacantes destacan Metasploit y Nmap, las cuales permiten la identificación y explotación de fallos de seguridad, en contraposición, los Blue Teams diseñan e implementan mecanismos defensivos, analizando los intentos de intrusión para mejorar la respuesta ante amenazas.

La integración de pruebas de penetración mediante esta dinámica Red & Blue Team ofrece beneficios significativos, como la identificación temprana de vulnerabilidades, el fortalecimiento de protocolos de seguridad y la optimización de los mecanismos de defensa frente a ataques dirigidos.

Este enfoque proactivo contribuye al desarrollo de estrategias de ciberseguridad más robustas y adaptadas a las amenazas emergentes, garantizando la protección de los activos digitales de una organización.

Justificación

El desarrollo de este trabajo responde a la necesidad de fortalecer el conocimiento sobre pruebas de penetración, una práctica esencial en el ámbito de la ciberseguridad. La creciente sofisticación de los ataques informáticos exige el diseño de estrategias defensivas más robustas, donde los equipos Red Team y Blue Team desempeñan un papel fundamental en la identificación y mitigación de vulnerabilidades dentro de los sistemas digitales de una organización.

Este estudio permite analizar las tácticas utilizadas por atacantes y profesionales de seguridad, así como evaluar la eficacia de herramientas como Metasploit y Nmap entre otras, las cuales son empleadas tanto para la explotación de fallas como para la implementación de medidas de protección, además, se aborda el marco legal colombiano en materia de ciberseguridad y protección de datos, proporcionando una perspectiva regulatoria clave para el manejo adecuado de incidentes y el cumplimiento normativo.

La realización de este análisis facilita la comprensión de los riesgos asociados a las brechas de seguridad, contribuyendo al diseño de estrategias preventivas que optimicen la protección de los activos digitales empresariales y refuercen la postura de seguridad frente a amenazas emergentes.

Objetivos

Objetivo General

Construir un informe técnico que analice y sintetice las técnicas empleadas por los equipos Red Team y Blue Team para el fortalecimiento de la seguridad digital en un entorno empresarial, permitiendo la evaluación crítica de sus estrategias y la aplicación efectiva de medidas de protección.

Objetivos Específicos

Aplicar metodologías de pruebas de penetración (Pentesting) para identificar vulnerabilidades en los sistemas de seguridad digital, validando su eficacia en la detección de amenazas.

Implementar marcos de trabajo que alineen las estrategias de ciberseguridad de los equipos Red Team y Blue Team, favoreciendo una respuesta coordinada ante posibles riesgos y vulnerabilidades.

Utilizar herramientas de ciberseguridad adoptadas por los equipos Red Team y Blue Team para realizar evaluaciones de seguridad, explotaciones simuladas y análisis de vulnerabilidades en entornos controlados.

Interpretar los resultados obtenidos en las pruebas de laboratorio, formulando recomendaciones para optimizar metodologías y fortalecer la postura de seguridad digital de la organización.

Marco Legal en Colombia

En los últimos veinte años, el incremento de la digitalización de la información por medio de múltiples plataformas que se interconectan por internet ha aumentado, hoy en día ya prácticamente toda la información se maneja de forma digital, se almacena en servidores o discos duros, los cuales tienen acceso a internet, las redes sociales y las empresas tienen gran cantidad de información de tipo personal y a veces confidencial sobre usuarios y clientes, esta información puede ser muy valiosa para personas mal intencionadas que buscan lucrarse con esos datos o perjudicar la reputación de alguien o alguna persona.

Al digitalizar toda la información se han creado mecanismos de almacenamiento digital que tienen vulnerabilidades en sus sistemas de seguridad, estas son explotadas por ciberdelincuentes que se apoderan de datos personales y clasificados lo que constituye un delito según la normatividad nacional.

En Colombia se estableció un marco normativo que regula los delitos informáticos, y la protección de datos personales, las dos principales leyes fundamentales son la Ley 1273 del año 2009 la cual penaliza los delitos informáticos y la Ley 1581 del año 2012 que se encarga de la protección de datos personales.

Delitos Informáticos en Colombia

El Código Penal se actualiza al establecer un nuevo bien judicial protegido: “Protección de la Información y los Datos”. Esto busca salvaguardar de una manera integral aquellos sistemas que emplean tecnologías relacionadas con la información y las comunicaciones. La Ley 1273 de 2009, en el contexto legal colombiano, incorporó nuevas infracciones vinculadas a los delitos cibernéticos, definiendo comportamientos delictivos tales como:

- Acceso indebido a un sistema informático (Artículo 269A): Se castiga a quien ingrese sin permiso a un sistema de computación, lo que abarca la adquisición ilegal de datos o permanecer en el sistema en oposición a quien posee el derecho a impedirlo.
- Interferencia indebida en un sistema informático (Artículo 269B): Quien frene la operatividad o acceso a un sistema de computación y la información que alberga, sin tener la debida autorización para hacerlo.
- Intercepción de datos (Artículo 269C): Se penaliza la captura de información transmitida por redes informáticas sin el consentimiento del titular.
- Daño informático (Artículo 269D): Se considera delito la modificación, daño o supresión de información en un sistema informático.
- Uso de Programas Maliciosos (Artículo 269E) Se considera un delito producir, adquirir, traficar o instalar software de tipo malicioso dentro del territorio nacional incluyendo programas que causen daños en los sistemas computacionales.
- Vulneración de datos personales (Artículo 269F): Es un delito sacar provecho propio o de un tercero mediante la sustracción, intercambio o divulgación de información personal contenida en archivos o bases de datos.
- Suplantación de sitios Web (Artículo 269G): Es delito desarrollar, diseñar o ejecutar páginas electrónicas, enlaces o ventanas emergentes que suplanten sitios web con el objetivo de sustraer información sensible o datos personales.

Esta ley es necesaria para establecer una protección de la información y la seguridad cibernética, sin embargo, es motivo de grandes controversias ya que algunas personas argumentan que las penas establecidas no son lo suficientemente fuertes para disuadir a los delincuentes que practicas estas acciones criminales. **(Policía Nacional de Colombia. n.a.)**

Protección de Datos Personales

El congreso de la República de Colombia decretó mediante la ley estatutaria 1581 de 2012 una reglamentación enfocada en la protección de datos personales. Esta legislación reconoce el derecho de los ciudadanos a tener conocimiento, actualizar y modificar la información que sobre ellos se maneja y se encuentra registrada en las bases de datos que puedan hacerlos propensos de tratamiento en cualquier entidad de orden público o privado. No aplicará esta ley a los sistemas de información que tengan como fin la seguridad nacional y la defensa del territorio, el seguimiento y control de lavado de activos o la financiación de actividades terroristas, tampoco aplicará a la información de inteligencia y contrainteligencia, o los sistemas de información y archivos reglamentados por la ley 266 de 2008 y la ley 79 de 1993.

Entre sus disposiciones más relevantes se encuentran:

- Consentimiento informado Artículo 9: Se requiere que las entidades obtengan autorización expresa de los titulares de los datos antes de realizar cualquier tratamiento de su información personal.
- Derechos de los propietarios de los datos Artículo 8: Los ciudadanos tienen derechos fundamentales, como el acceso de forma gratuita a sus datos personales, la rectificación y la destrucción de sus datos personales.
- Informar de manera clara y expresa Artículo 12: Los ciudadanos tienen derecho a ser informados sobre el manejo de sus datos personales
- Responsabilidad de las entidades Artículo 17: Las empresas que manejan datos personales deben establecer protocolos de seguridad adecuados, que garanticen la

protección de la información, avalando el pleno y eficiente ejercicio del derecho de Hábeas Data.

- Autoridad encargada de la protección de datos Artículo 19: La superintendencia de Industria y Comercio será la encargada de ejercer la vigilancia y control, garantizando que se respeten los derechos y garantías de los datos de las personas, según lo establecido por esta ley.

El debate en torno a esta ley se centra en la efectividad de su aplicación y en la capacidad de las entidades para cumplir con las obligaciones establecidas. Algunos críticos argumentan que la falta de recursos y capacitación en las organizaciones dificulta la implementación efectiva de la ley.

Intersección entre la Protección de los Datos Personales y los Delitos Informáticos

La correspondencia entre la normatividad sobre delitos informáticos y la protección de datos es crucial. Los ciberdelitos pueden comprometer la seguridad de los datos personales, lo que a su vez plantea interrogantes sobre la responsabilidad de las entidades en caso de una violación de datos. Este aspecto ha llevado a un llamado a la creación de un marco normativo más integral que aborde de manera conjunta ambos temas.

Pruebas de Penetración – Pentesting

Las pruebas de penetración son herramientas clave para identificar deficiencias en el diseño de la arquitectura de seguridad, así como en las redes, la programación y el desarrollo inseguro de aplicaciones. Estas evaluaciones de seguridad en la red ayudan a localizar vulnerabilidades tanto en la infraestructura interna como externa, permitiendo evaluar la efectividad de los mecanismos de protección implementados por la organización. Además, al realizar pruebas en aplicaciones web, es posible detectar debilidades vinculadas a la seguridad del diseño y la programación, ejecutándose directamente en los navegadores o aplicaciones complementarias usadas por la empresa. En el caso de las redes inalámbricas, estas pruebas verifican si los dispositivos móviles, como laptops, teléfonos y tabletas conectados a redes Wi-Fi y Bluetooth, son suficientemente seguros para manejar y resguardar datos confidenciales. Por último, el Pentesting relacionado con ingeniería social evalúa la preparación de los empleados ante amenazas potenciales de grupos delictivos, proporcionando una visión clara sobre la conciencia de los trabajadores respecto a la ciberseguridad en la empresa.

Tipos de Pruebas de Penetración

Pruebas de Penetración de Caja Negra

Las pruebas de caja negra, o black box, son aquellas en las que el pentester no posee información previa sobre los sistemas a evaluar. Su objetivo es recopilar la mayor cantidad de datos posibles sobre la red o el sistema en cuestión. Aunque se espera un resultado específico, el método para alcanzarlo no está claro. El pentester no tiene acceso al código fuente, pero sí examina la cobertura del sistema y lleva a cabo análisis sobre flujos de datos y rutas.

Pruebas de Penetración de Caja Blanca

Conocidas como pruebas de caja blanca o pruebas completas, en este enfoque el pentester tiene acceso total a los datos del sistema, incluyendo detalles de la red, esquemas, código fuente, información sobre sistemas operativos y listas de direcciones IP. Aquí se simula un ataque desde el interior de la organización, como si el atacante tuviera conocimiento profundo de su funcionamiento, intentando robar información mediante su familiaridad con el sistema.

Pruebas de Penetración de Caja Gris

En las pruebas de caja gris, el evaluador cuenta con cierta información, lo que lo posiciona como un atacante externo que ha accedido ilegalmente a algunos datos o archivos de la empresa. Sin embargo, no tiene acceso al código fuente ni a detalles sobre las funciones del sistema, y se enfrenta a la infraestructura externa de la organización, como sus servidores web y de red, realizando la evaluación desde una ubicación remota fuera de las instalaciones.

Pruebas de Penetración Encubiertas

Este tipo de pruebas se llevan a cabo sin el conocimiento de la mayoría de los miembros de la organización, incluyendo al personal de seguridad de TI que se encarga de proteger y responder ante potenciales ciberataques.

Etapas de las Pruebas de Penetración

Las pruebas de penetración son más que un simple chequeo; comprenden un conjunto de técnicas que buscan explorar la seguridad de un sistema, para ver qué tan bien defiende sus barreras y ofrecer soluciones a las vulnerabilidades que se descubren en el proceso.

Este es un proceso estructurado el cual consta de las siguientes fases:

Planeación y Preparación

Primero, toca definir qué se busca lograr. Esto lo fijan en conjunto el pentester y el cliente. Un objetivo clave podría ser detectar las debilidades de seguridad del sistema y encontrar la mejor manera de fortalecer la protección de la información.

Reconocimiento

Luego viene la parte de reunir toda la información relevante sobre el sistema que se va a testear, es como una fase de recopilación pasiva, donde se recolectan datos importantes que ayudarán a trazar una estrategia y a elegir las herramientas correctas para la prueba.

Descubrimiento

En esta etapa, el pentester utiliza distintas herramientas tecnológicas. Algunas funcionan automáticamente, mientras que otras requieren un toque manual, el objetivo aquí es encontrar las vulnerabilidades. Es crucial escanear los dispositivos para identificar los puertos abiertos y averiguar qué servicios están corriendo, hay que mapear la red, los servidores y todos los dispositivos conectados, herramientas como NMAP, OpenVAS y Metasploit son muy útiles en esta fase.

Análisis de la Información

Aquí es donde se analizan los resultados obtenidos de las pruebas, se evalúa si realmente se lograron los objetivos y se identifican los riesgos a los que está expuesto el sistema. Herramientas como Maltego son geniales para visualizar las relaciones entre la información recopilada, y Recon-ng es ideal para el análisis de datos OSINT.

Intentos de Intrusión Activos

Esta etapa implica poner a prueba las vulnerabilidades detectadas para ver qué riesgos reales enfrenta el sistema, es particularmente crucial en sistemas que requieren una alta integridad, ya

que las vulnerabilidades necesitan ser cuidadosamente abordadas antes de realizar cualquier limpieza crítica, se utilizan herramientas como Metasploit para administrar estas pruebas y llevar a cabo evaluaciones de seguridad.

Preparación del Informe

Finalmente, se genera un informe que detalla todo el proceso y analiza las vulnerabilidades y los riesgos descubiertos, se identifican los riesgos críticos y las posibles consecuencias si un ciberdelincuente aprovechara esas debilidades, el informe también incluye recomendaciones para corregir las vulnerabilidades y sugerencias para prevenir futuros ataques al sistema basadas en los hallazgos obtenidos.

Herramientas Tecnológicas Utilizadas Durante un Pentesting

Las pruebas de penetración, conocidas también como Penetration Testing, son llevadas a cabo por expertos en ciberseguridad que se especializan en el hacking ético, estos profesionales no solo dominan el ámbito de la seguridad, sino que también poseen habilidades de programación que les permiten utilizar diversas herramientas para identificar vulnerabilidades y aprovechar las debilidades halladas, por ello, es esencial contar con ciertas herramientas tecnológicas, que pueden ir desde aplicaciones portátiles hasta sistemas operativos diseñados especialmente para este trabajo.

Algunas de esas herramientas son las siguientes:

Metasploit

Es un programa de código abierto diseñado para realizar evaluaciones de seguridad y análisis de penetración en sistemas operativos, aplicaciones y dispositivos, su funcionalidad incluye la identificación de fallos de seguridad y la administración de pruebas orientadas a validar la existencia de riesgos, este framework combina un conjunto eficiente de utilidades para crear pruebas de penetración y desarrollar exploits, permitiendo explorar servicios y determinar sus vulnerabilidades, una vez detectadas, se evalúa si dichas fallas constituyen amenazas reales, analizando el potencial impacto y los daños que un ataque podría ocasionar en la brecha de seguridad, además, resulta imprescindible verificar si hay controles de mitigación ausentes que no hayan sido considerados, este procedimiento ofrece una perspectiva clara del posible impacto frente a un ataque real.

Metasploit incluye una base de datos de exploits que posibilitan la ejecución directa de ataques simulados en equipos remotos, permitiendo examinar las consecuencias derivadas de esta intrusión.

Algunas de sus principales características son:

- Permite una simulación de ataques con la cual podemos identificar vulnerabilidades ya sea en SO, dispositivos o aplicaciones.
- Incluye una base de datos de exploits que los usuarios pueden utilizar para realizar pruebas de vulnerabilidades específicas y analizar sus consecuencias.
- Ofrece una amplia colección de módulos que abarcan desde exploits y payloads hasta herramientas auxiliares de post-explotación.
- Nos facilita el descubrimiento de debilidades en los servicios y sistemas, permitiéndonos hacer una evaluación de su gravedad y posibles impactos.
- Ayuda a automatizar varias etapas del proceso de pruebas de seguridad, permitiéndonos ahorrar tiempo y recursos.
- Permite una integración con otros sistemas ya que es compatible con una gran variedad de herramientas de seguridad, lo que le permite ampliar su alcance y funcionalidad.
- Esta herramienta además permite llevar a cabo pruebas en sistemas remotos, evaluando la seguridad a distancia.
- Su interfaz es amigable, ofrece una consola de comandos como una interfaz gráfica, lo que le permite adaptarse a diferentes niveles de experiencia de los usuarios.

Estas capacidades hacen del Metasploit Framework una solución versátil y esencial para profesionales de la ciberseguridad.

Metasploit se ha utilizado en numerosos escenarios de pruebas de penetración para demostrar vulnerabilidades de seguridad, por ejemplo, un caso típico podría ser el uso del exploit

"EternalBlue" que aprovecha una vulnerabilidad en el protocolo SMB de Windows, con Metasploit, un profesional de seguridad podría cargar este exploit, apuntar a un sistema vulnerable y, si tiene éxito, obtener acceso remoto al equipo objetivo, esto permite evaluar el impacto potencial de un ataque real y reforzar las medidas de seguridad.

Es importante destacar que estas herramientas deben usarse exclusivamente con fines éticos y legales, como en auditorías de seguridad autorizadas.

NMAP

Network Mapper (NMAP) es una herramienta de código abierto diseñada para el análisis de redes, su funcionamiento se basa en el envío de paquetes IP sin procesar, lo que le permite identificar servicios en ejecución en dispositivos remotos, es capaz de determinar qué equipos están activos, inspeccionar los puertos, reconocer el tipo y la versión del sistema operativo, además de detectar la presencia de firewalls y su configuración. Aunque originalmente es una herramienta de línea de comandos pensada para Linux, su compatibilidad se extiende a sistemas Windows y Mac, asegurando su versatilidad.

Esta utilidad facilita la exploración completa de redes, permitiendo una visualización detallada de su estructura, su uso resulta sencillo gracias a comandos básicos, aunque también admite instrucciones avanzadas para un análisis más profundo, entre sus capacidades destaca la identificación de servicios como servidores web o DNS, adicionalmente, ofrece la posibilidad de realizar pruebas de vulnerabilidad mediante scripts alojados en el motor de scripting integrado.

Aunque está orientada a la consola, NMAP también dispone de una interfaz gráfica que permite representar dinámicamente la red, lo que enriquece la presentación de informes de manera clara y comprensible, además, incluye funcionalidades como la captura de paquetes sin procesar, tanto los destinados al dispositivo local como los presentes en medios compartidos,

también ofrece herramientas para filtrar paquetes según reglas definidas por el usuario y transmitir datos directamente a la red, facilitando la recopilación de información sobre el tráfico existente.

Estas capacidades se soportan mediante un controlador instalado en la capa de red del núcleo del sistema operativo y una serie de archivos DLL adicionales, cabe destacar que NMAP no está diseñado para modificar, filtrar o bloquear el tráfico generado por otros programas en el mismo dispositivo, su función se limita a detectar paquetes en tránsito por la red, lo que lo excluye de aplicaciones como gestores de tráfico, programadores de QoS o firewalls personales.

OPENVAS

El Open Vulnerability Assessment Scanner (OpenVAS) es una solución de código abierto diseñada para identificar y evaluar posibles vulnerabilidades en sistemas informáticos, esta herramienta permite realizar análisis tanto manuales como programados, abarcando un amplio espectro de pruebas para detectar fallos de seguridad. Desde su desarrollo en 2009 por Greenbone Networks, OpenVAS ha sido una parte integral de las distribuciones de seguridad como Kali Linux, donde se encuentra preinstalado y listo para su configuración. **(Micucci. 2023)**

Esta herramienta incluye una interfaz de línea de comandos (OpenVAS CLI) y una interfaz gráfica basada en la web, conocida como Greenbone Security Assistant, además, puede integrarse con el framework Metasploit para llevar a cabo pruebas de explotación de vulnerabilidades. OpenVAS opera mediante dos servicios principales: el OpenVAS Manager, encargado de gestionar y clasificar los resultados del análisis, así como de administrar las bases de datos y usuarios; y el OpenVAS Scanner, que ejecuta las pruebas de vulnerabilidad de red conocidas como Network Vulnerability Tests (NVT). Estas pruebas están organizadas en familias según su naturaleza, lo que facilita su selección y configuración.

Entre sus capacidades, OpenVAS permite realizar análisis autenticados y no autenticados, soportando una amplia gama de protocolos industriales y de internet, su diseño incluye opciones de ajuste de rendimiento, lo que lo hace ideal para escaneos a gran escala, además, cuenta con un lenguaje de programación interno que posibilita la implementación de pruebas personalizadas para detectar vulnerabilidades específicas. **(Greenbone Networks. 2025)**

Exploitdb

ExploitDB se presenta como una plataforma en línea que centraliza información sobre vulnerabilidades de seguridad y exploits de software, su propósito es ofrecer un recurso confiable y accesible para especialistas en ciberseguridad, analistas e investigadores, facilitando el estudio y comprensión de fallos que puedan comprometer diversos sistemas operativos y aplicaciones, a través de esta herramienta, las organizaciones pueden identificar riesgos potenciales y desarrollar estrategias de mitigación eficaces.

Principales características:

ExploitDB destaca por su extensa base de datos, donde se detalla información sobre las vulnerabilidades reportadas, incluyendo especificaciones sobre las versiones afectadas del software y ejemplos de código que ilustran cómo explotar las debilidades encontradas, cada registro suele acompañarse de una descripción técnica, enlaces adicionales para profundizar y, en muchos casos, el identificador CVE (Common Vulnerabilities and Exposures), lo que simplifica la localización de amenazas críticas.

La plataforma también proporciona un avanzado sistema de búsqueda que permite filtrar información por tipo de vulnerabilidad, programa afectado o palabras clave, mejorando la experiencia de usuario, así mismo, cuenta con una activa comunidad de expertos que contribuyen

regularmente, reportando nuevos fallos y compartiendo conocimientos que enriquecen la base de datos.

Ejemplos de uso

Casos de Uso Entre los usos más comunes de ExploitDB, los analistas de seguridad recurren a esta herramienta para investigar vulnerabilidades antes de instalar actualizaciones en infraestructuras críticas, por ejemplo, pueden analizar si existen exploits disponibles y evaluar los riesgos asociados a su entorno. Los investigadores, por su parte, estudian patrones históricos de vulnerabilidades documentadas para mejorar su comprensión de las tendencias en seguridad y fortalecer sus habilidades técnicas.

Beneficios y ventajas

Una de las mayores fortalezas de ExploitDB radica en la actualización constante de su repositorio, permitiendo a las empresas mantenerse al día con los últimos hallazgos en ciberseguridad, además, al ser una herramienta colaborativa, fomenta el intercambio de conocimientos entre profesionales, potenciando una respuesta más eficiente frente a amenazas emergentes.

CVE

El sistema conocido como Common Vulnerabilities and Exposures **(CVE. n.d)** tiene como propósito clasificar y asignar identificadores únicos a vulnerabilidades y exposiciones identificadas en software y hardware; esta iniciativa busca optimizar el intercambio de información entre especialistas en ciberseguridad, fomentando la comprensión de riesgos en distintas plataformas y fortaleciendo las estrategias de protección informática. Cada registro en el catálogo CVE contiene un código exclusivo, una descripción técnica sobre la falla identificada y, en ocasiones, enlaces que ofrecen mayor detalle para quienes requieren información adicional.

Aspectos Fundamentales:

Entre las ventajas del sistema CVE se destaca su formato estandarizado, que permite a usuarios de diferentes niveles de experiencia analizar con precisión los detalles de cada vulnerabilidad, cada identificador contiene un código alfanumérico y una descripción que explica la naturaleza del fallo, los métodos para explotarlo y, en algunos casos, los posibles efectos en sistemas específicos, además, CVE proporciona vínculos a boletines de seguridad ofrecidos por los desarrolladores y a otras plataformas relevantes, como la National Vulnerability Database (NVD) , lo que facilita su integración en procesos de análisis de riesgos. **(Shonstak. 2014)**

La base de datos se sustenta en la colaboración activa de su comunidad de usuarios, quienes pueden reportar nuevas vulnerabilidades y actualizar información existente, asegurando que los datos reflejen los más recientes hallazgos en el campo.

Ejemplos de uso:

Aplicaciones en Seguridad. El sistema CVE es una herramienta invaluable para los profesionales de seguridad informática, permitiéndoles consultar vulnerabilidades específicas que podrían impactar su infraestructura, por ejemplo, al recibir notificación de una nueva entrada en CVE, las empresas pueden investigar de forma inmediata el nivel de exposición de sus sistemas y definir medidas preventivas, asimismo, los equipos que gestionan incidentes, utilizan CVE para documentar y analizar vulnerabilidades explotadas en escenarios activos, contribuyendo a respuestas más precisas y rápidas.

Ventajas Operativas:

El uso de CVE facilita la comunicación entre distintos sectores gracias a su terminología unificada, lo que resulta especialmente útil al trabajar con diversos productos y servicios de diferentes proveedores, además, al incluir evaluaciones de gravedad, CVE permite priorizar

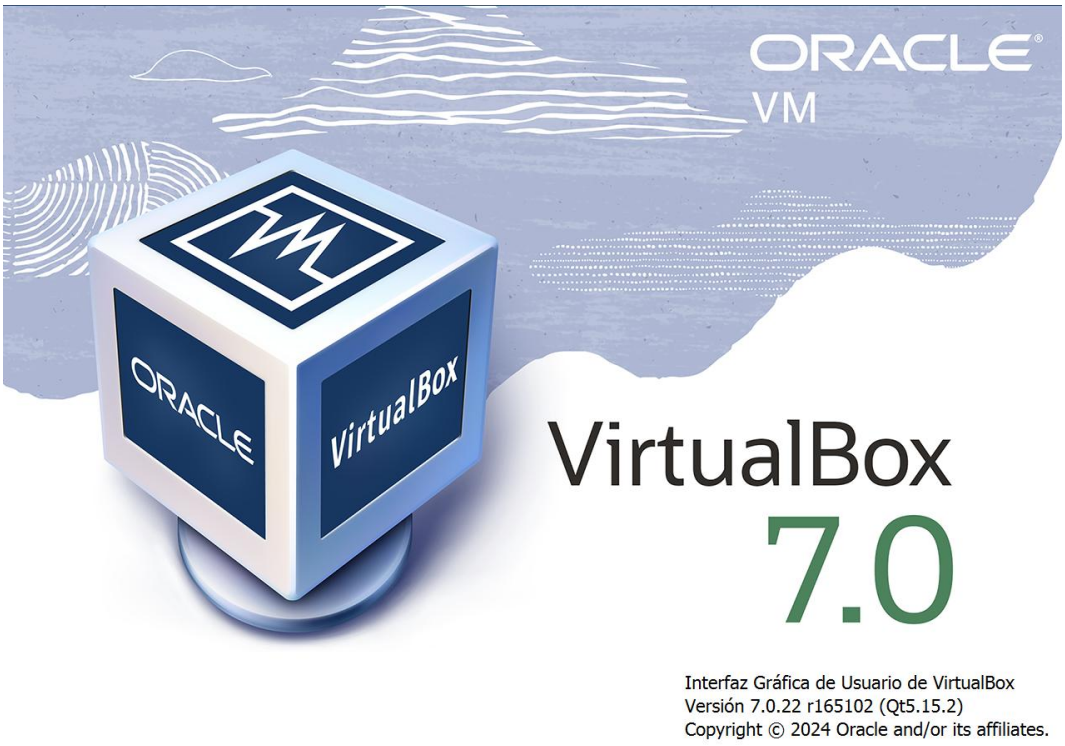
recursos para atender las amenazas más críticas, en combinación con otras herramientas, CVE se convierte en un referente central para mejorar la seguridad general de una organización.

Banco de Trabajo

Se establecerá un banco de trabajo o laboratorio que contará con un software de virtualización, permitiendo la virtualización de diversos sistemas operativos. Para este caso, se empleará VirtualBox en su versión 7.0.

Figura 1

Máquina Virtual



Fuente: Elaboración Propia

El laboratorio se inicia con la instalación de un sistema operativo Windows 7

Figura 2

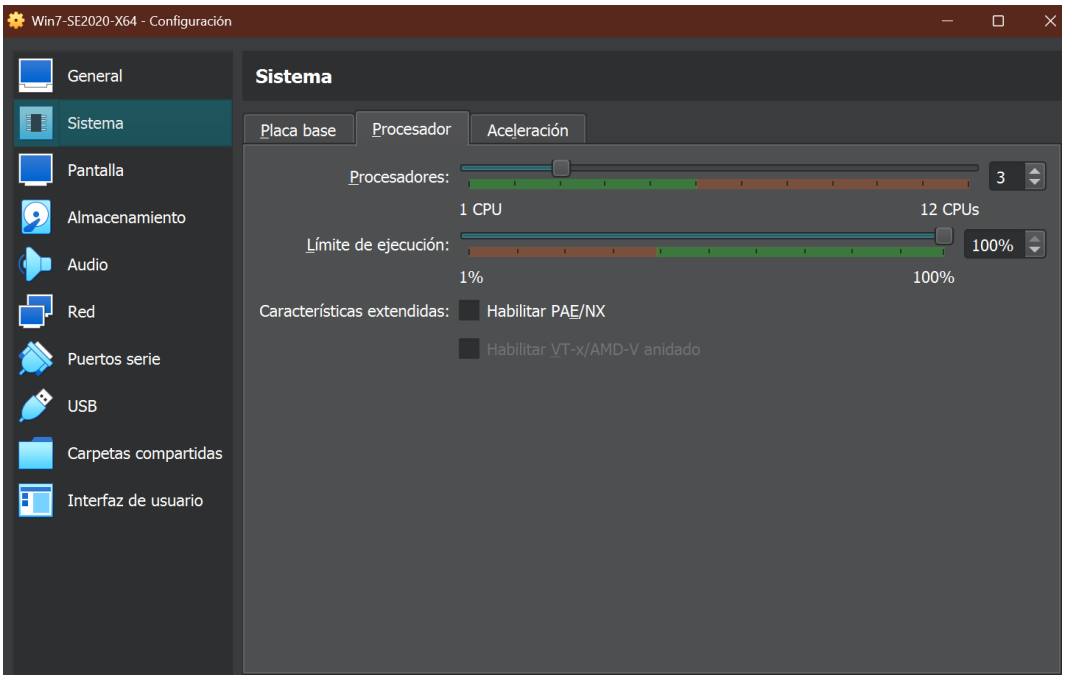
Instalación de Windows 7 en VirtualBox

Fuente: Elaboración Propia

Se configura la máquina virtual de la siguiente manera:

Figura 3

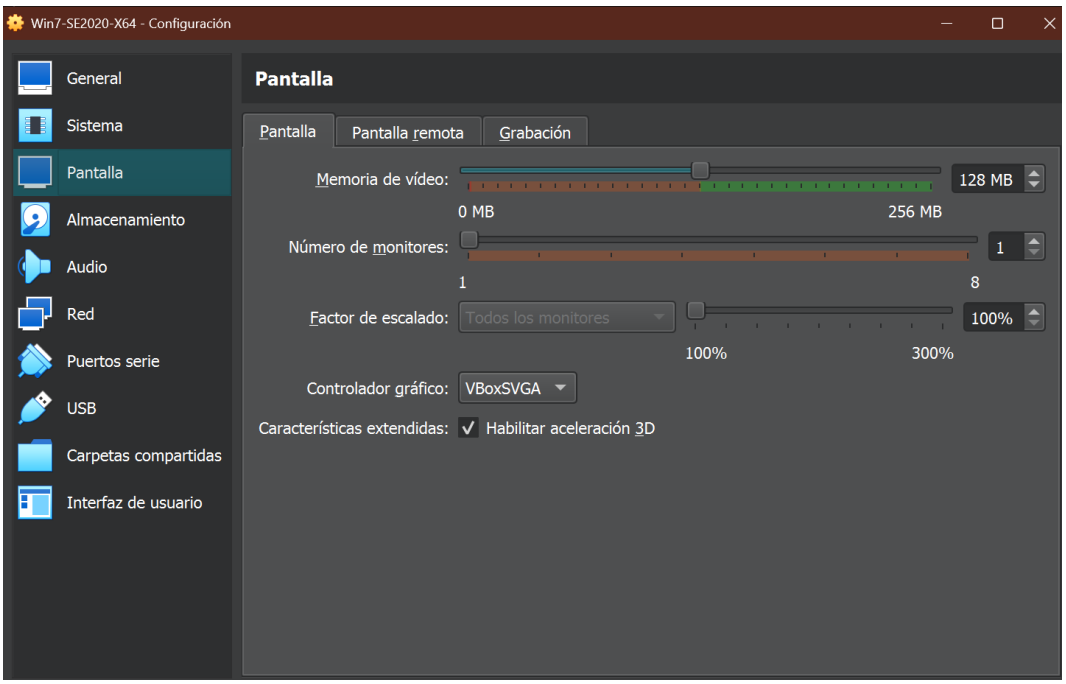
Configuración MV Sistema



Fuente: Elaboración Propia

Figura 4

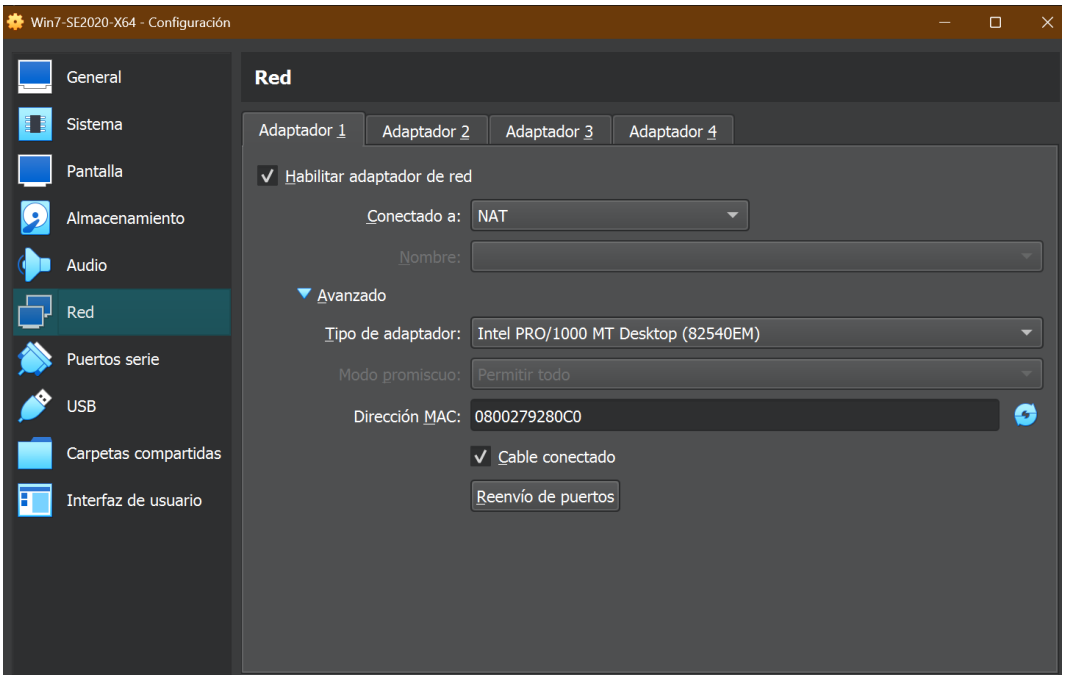
Configuración MV Pantalla



Fuente: Elaboración Propia

Figura 5

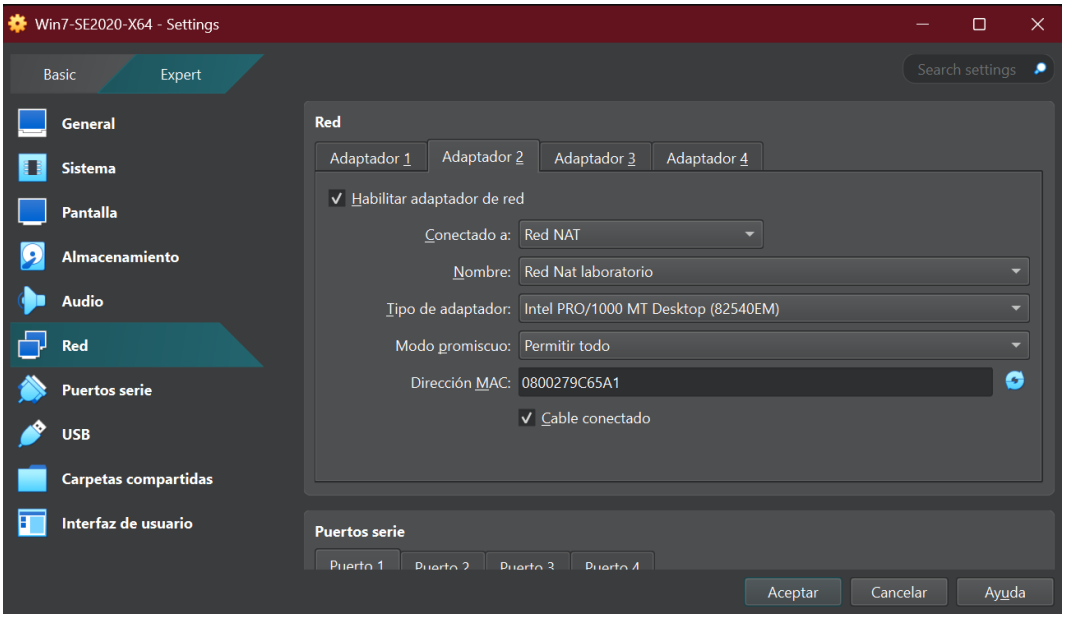
Configuración MV RED adaptador 1



Fuente: Elaboración Propia

Figura 6

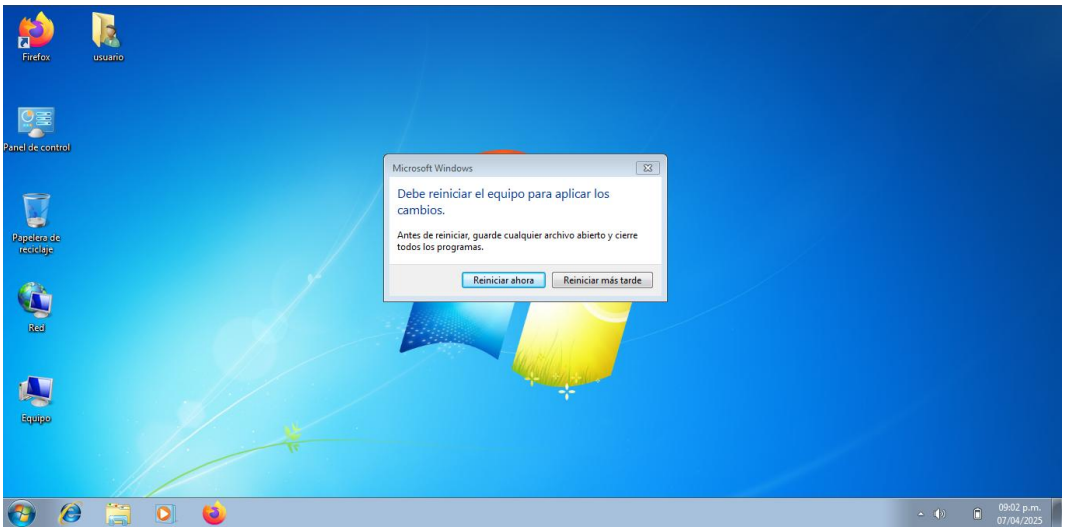
Configuración MV RED Adaptador 2



Fuente: Elaboración Propia

Figura 7

Windows 7 Instalado

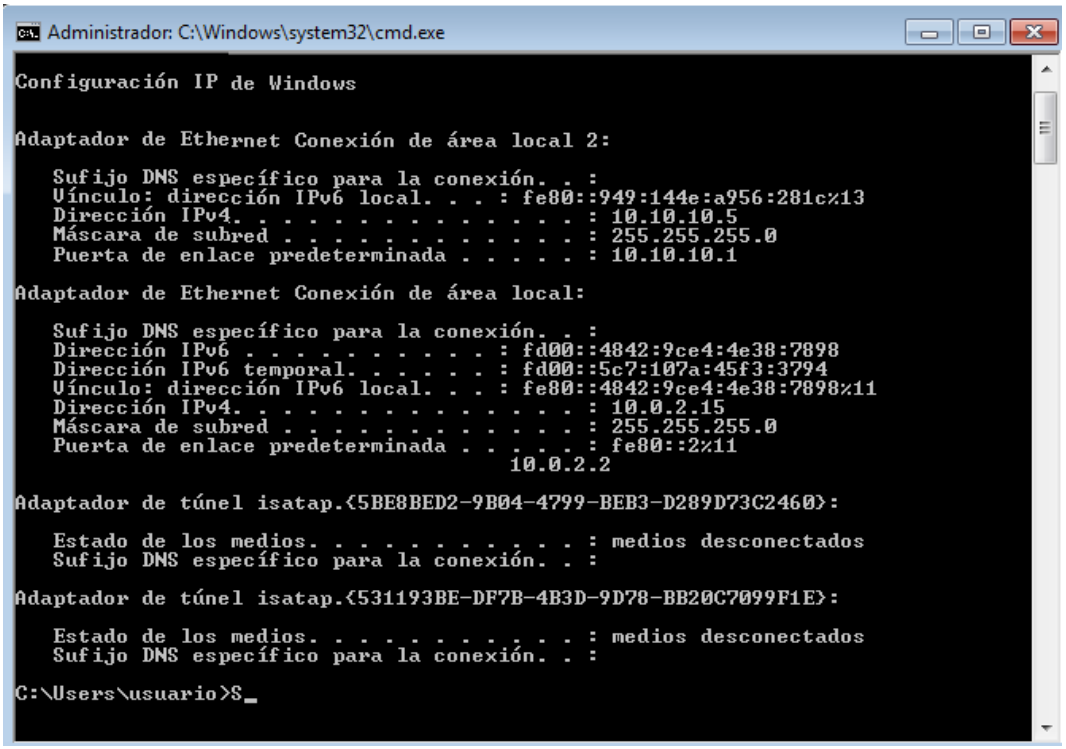


Fuente: Elaboración Propia

La dirección IP de esta máquina es 10.10.10.5

Figura 8

IP MV Windows 7

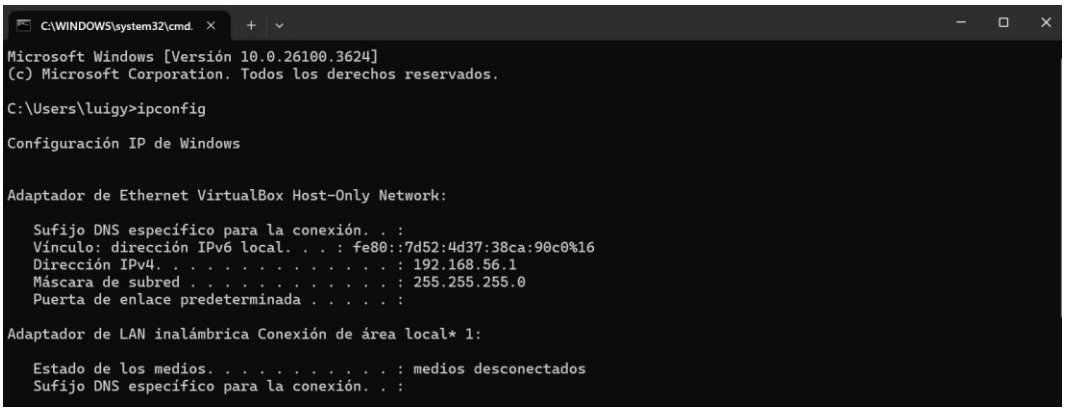


Fuente: Elaboración Propia

La dirección IP del Sistema Operativo huésped es 192.168.56.1

Figura 9

IP Windows 11 SO Anfitrión

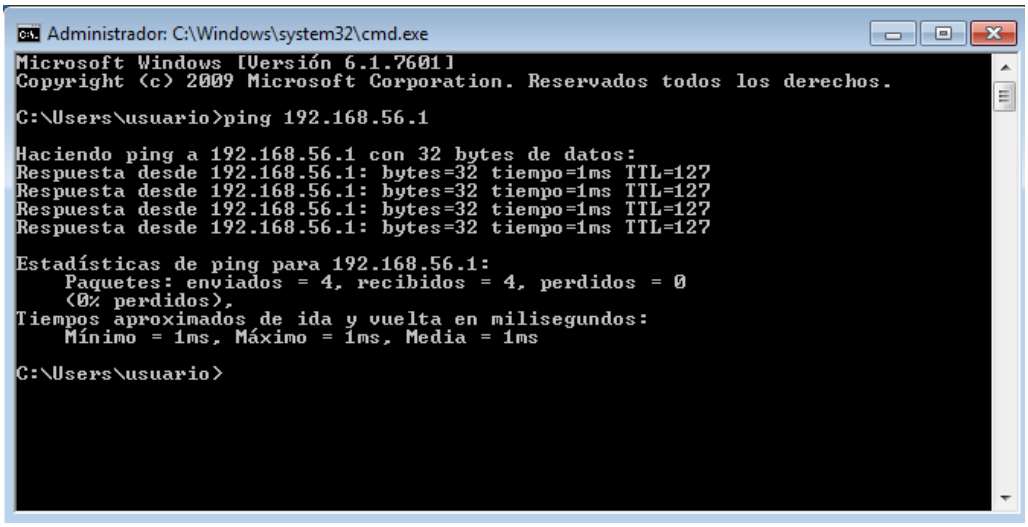


Fuente: Elaboración Propia

Se ejecuta una prueba de conectividad mediante el envío de paquetes ICMP desde la máquina virtual con Windows 7 hacia el sistema operativo huésped, verificando la respuesta para validar la conexión.

Figura 10

Prueba de conexión MV a SO Huésped

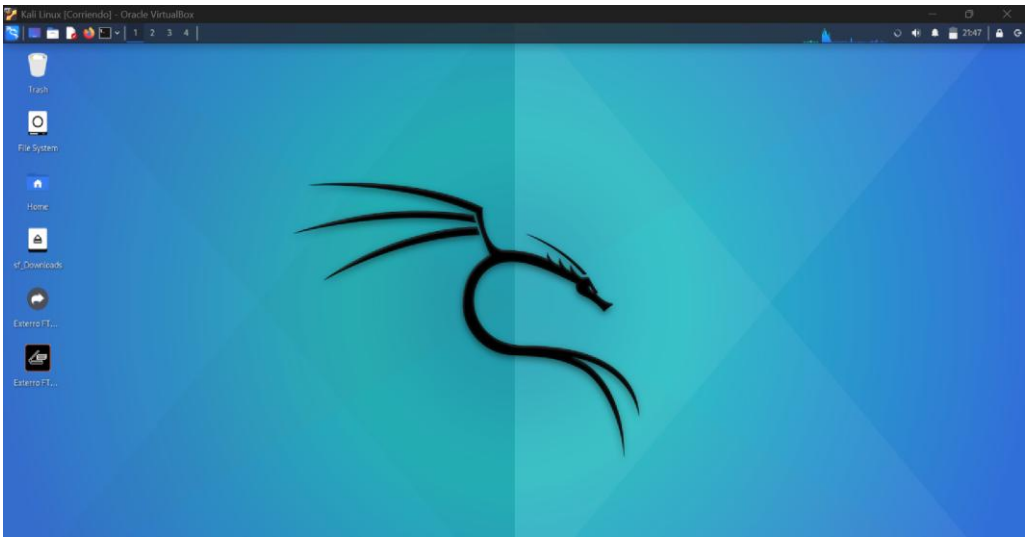


Fuente: Elaboración Propia

La siguiente máquina virtual que se instala y configura en el laboratorio es Kali Linux

Figura 11

Kali Linux

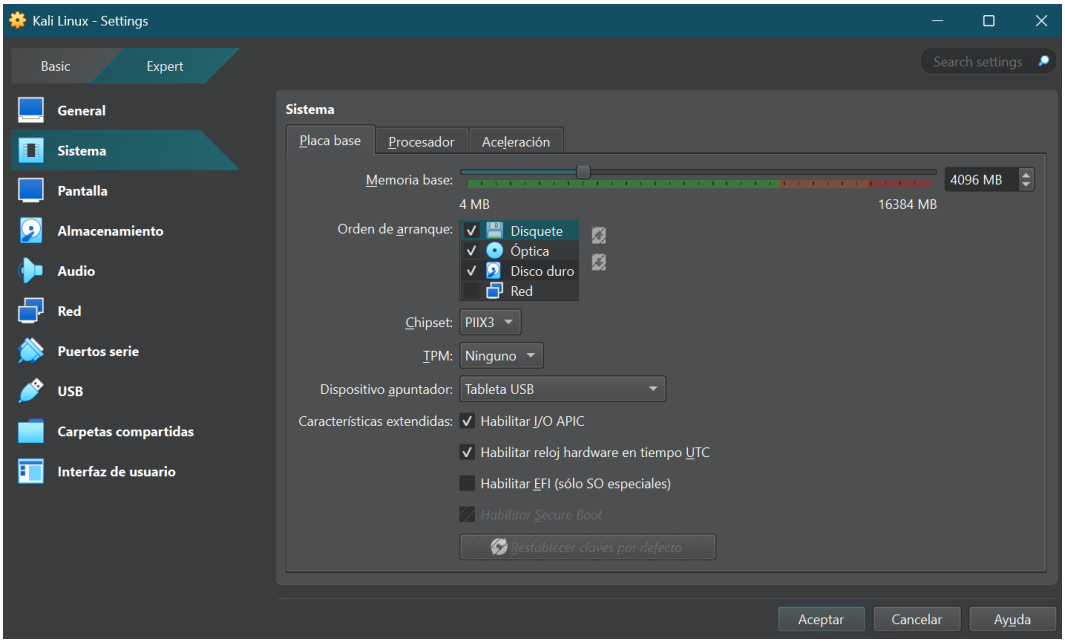


Fuente: Elaboración Propia

La configuración de la máquina virtual es la siguiente:

Figura 12

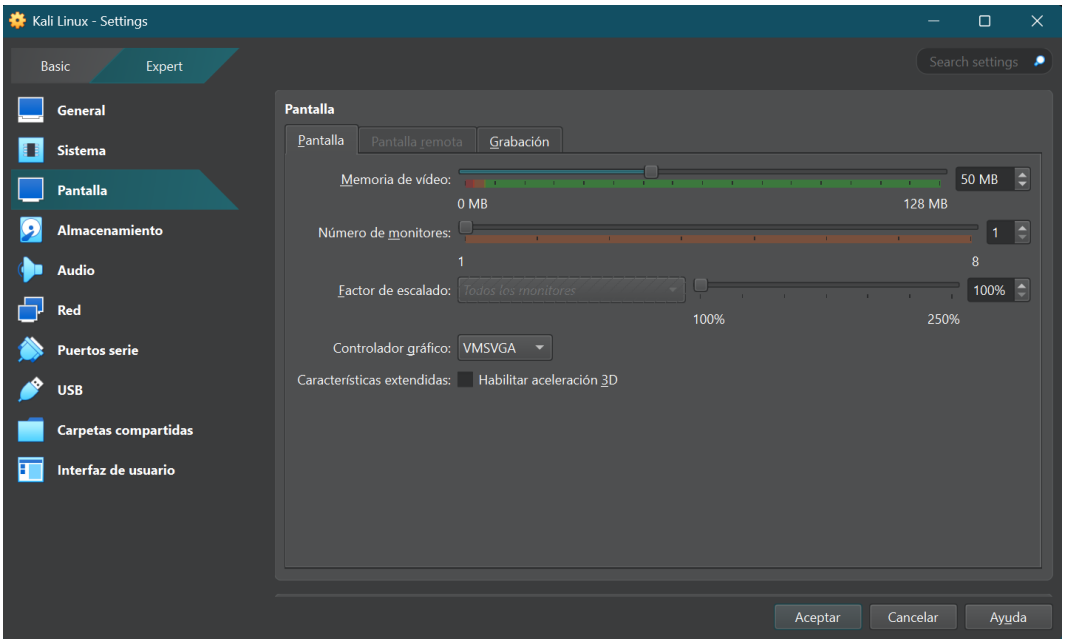
Configuración del Sistema Kali Linux



Fuente: Elaboración Propia

Figura 13

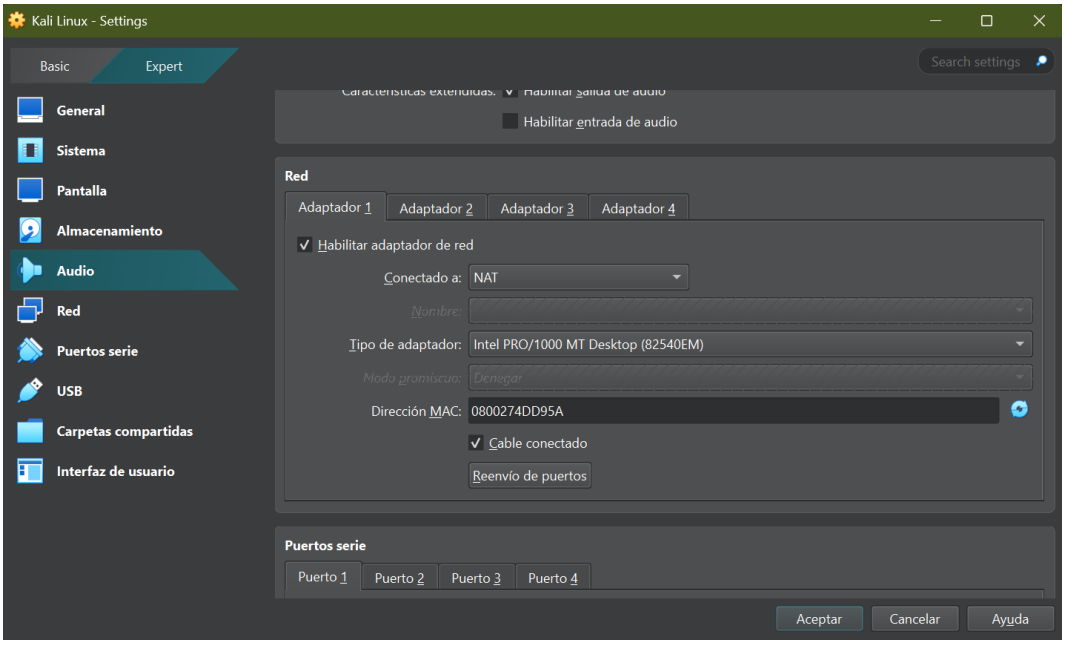
Configuración Pantalla Kali Linux



Fuente: Elaboración Propia

Figura 14

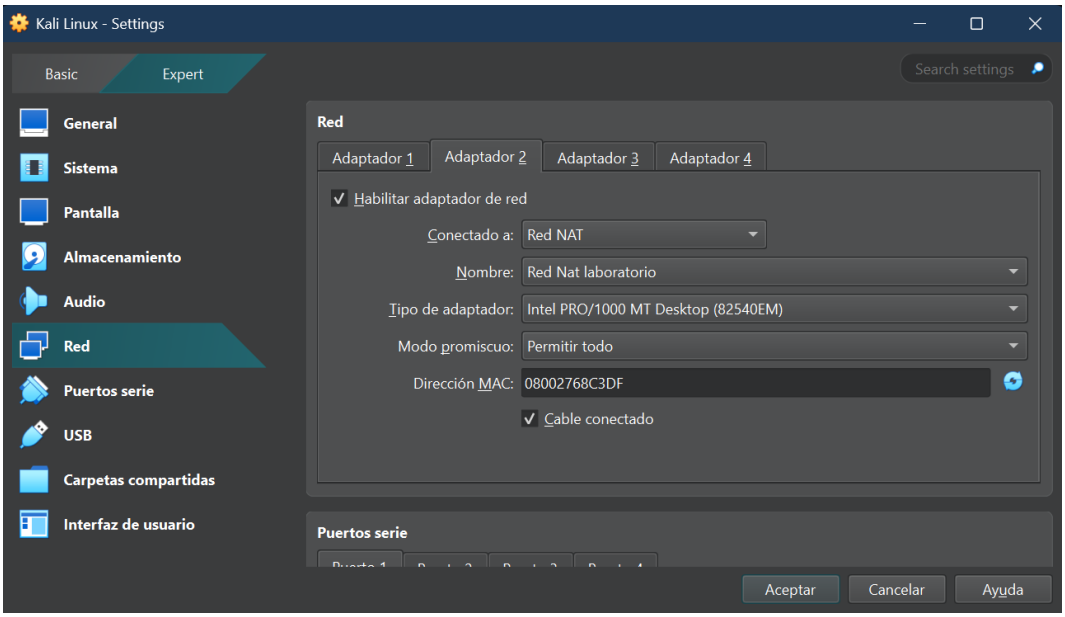
Configuración de Red Adaptador 1 Kali Linux



Fuente: Elaboración Propia

Figura 15

Configuración de red Adaptador 2 Kali Linux

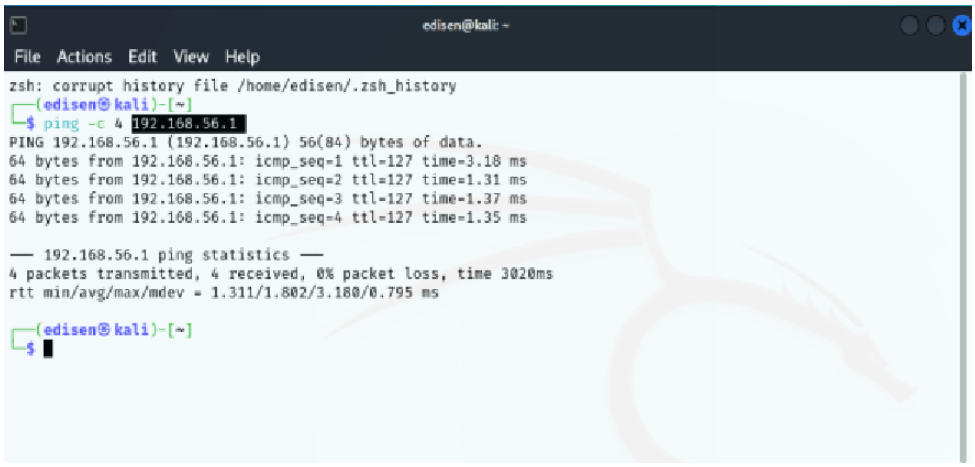


Fuente: Elaboración Propia

Se ejecuta una prueba de conectividad mediante el envío de paquetes ICMP desde la máquina virtual Kali Linux hacia el sistema operativo huésped, verificando la respuesta para validar la conexión.

Figura 16

Validación conexión Kali con SO anfitrión

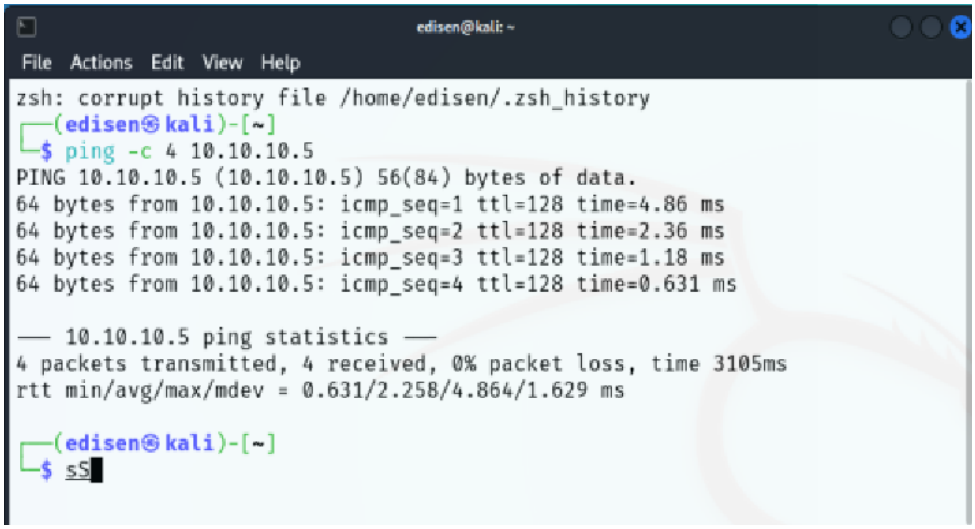


Fuente: Elaboración Propia

Se verifica la conectividad entre las máquinas virtuales mediante el envío de paquetes ICMP desde Kali Linux hacia la máquina con Windows 7, cuya dirección IP es 10.10.10.5.

Figura 17

Conexión entre Kali y W7



Fuente: Elaboración Propia

Actuación Ética y Legal

Según lo leído en el anexo 2 – escenario 2 y anexo 3 – acuerdo, se pueden determinar las siguientes conclusiones:

Este acuerdo de confidencialidad presenta varias disposiciones que podrían ser consideradas ilegales o poco éticas, especialmente en relación con la Ley 1273 de 2009 de Colombia, que protege la información y los datos digitales **(Policía Nacional de Colombia. n.a.)**. Algunos puntos críticos incluyen:

- Prohibición de denunciar actividades ilegales (Capítulo Primero del contrato - Objeto): La cláusula que impide a la parte receptora denunciar ante las autoridades actividades sospechosas de espionaje o apropiación de información de terceros podría vulnerar el Artículo 269F de la Ley 1273, que sanciona la violación de datos personales.

- Interceptación y acceso abusivo a sistemas informáticos (Capítulo 2 del contrato - Definición de información confidencial): La mención de "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos" sugiere posibles vulneraciones del Artículo 269A (Acceso abusivo a un sistema informático) y Artículo 269C (Interceptación de datos informáticos) de la Ley 1273.

- Exención de responsabilidad legal para CyberFort Technologies (Capitulo 8 del contrato – Solución de Controversias) La cláusula que obliga al receptor de información ilegal a contratar un abogado privado y exime de responsabilidad a la empresa podría ser considerada una estrategia para evitar consecuencias legales, lo que podría ser cuestionable desde una perspectiva ética y legal.

- Restricción de divulgación de información ilegal (Capítulo cuarto - Obligaciones de la parte receptora): La obligación de no denunciar ante las autoridades actividades sospechosas de espionaje incluyendo procesos en donde se intervenga la apropiación de información de terceros, deja dudas sobre los propósitos reales de la compañía, los cuales van en contravía de la ética y profesionalismo con que se debe actuar en los casos de manejo de información confidencial de los clientes

- La obligación de no revelar información ilegal sin consentimiento de la empresa podría entrar en conflicto con principios de transparencia y denuncia de delitos.

- Este acuerdo parece diseñado para proteger a CyberFort Technologies de cualquier posible denuncia o responsabilidad legal, lo que plantea serias preocupaciones éticas y legales

Dado que el contrato presenta disposiciones que podrían vulnerar principios éticos y legales, es importante considerar los estándares del Código de Ética Profesional de COPNIA. Este código establece que los ingenieros deben actuar con integridad, transparencia y

responsabilidad social, evitando cualquier participación en actividades que comprometan la legalidad o la ética profesional.

Si el acuerdo de confidencialidad impide la denuncia de actividades ilegales y busca eximir de responsabilidad a la empresa, esto podría contradecir los principios de honestidad y respeto por la ley que COPNIA exige a los profesionales de la ingeniería, además, aceptar un trabajo bajo estas condiciones podría generar riesgos legales y reputacionales.

Personalmente evaluaría si la empresa está dispuesta a modificar el contrato alineándolo con los principios éticos y legales, de no ser así, me replantearía si en verdad vale la pena aceptar una propuesta de trabajo bajo estas condiciones, ya que este contrato plantea riesgos éticos y legales, pero intentaría llegar a un acuerdo con la empresa en los siguientes términos:

- Solicitaría aclaraciones: Antes de tomar una decisión, preguntaría a la empresa sobre las disposiciones que me generan preocupación, ¿Están dispuestos a ajustar el contrato para eliminar cláusulas problemáticas, como la prohibición de denuncia de actividades ilegales?

- Consultaría con un experto legal: Un abogado especializado en derecho laboral o ciberseguridad me podría ayudar a analizar el contrato en detalle asesorándome sobre sus implicaciones, también podría orientarme en caso de que decida presentar una denuncia o solicitar cambios.

- Investigaría si otras empresas en el sector manejan contratos de confidencialidad con términos similares, si encuentro diferencias significativas, podría usarlas como argumento para solicitar ajustes.

- Evaluaría la tolerancia al riesgo: Considerando lo que implica estar en una empresa que impone este tipo de restricciones, teniendo en cuenta cómo podría afectar mi reputación o

incluso exponerme a una responsabilidad legal en un futuro, si el contrato exige la ocultación de información ilegal, podría verme obligado a decidir entre cumplir el acuerdo o actuar éticamente.

- Negociaría términos: Si la empresa realmente quiere contratarme, podría proponer modificaciones al acuerdo que alineen su contenido con la ética profesional y la legislación vigente, un enfoque diplomático podría abrir la puerta a ajustes razonables.

- Exploraría otras oportunidades: Si la empresa no está dispuesta a modificar el acuerdo consideraría buscar alternativas laborales en compañías con valores alineados con los principios de transparencia y legalidad.

En este tipo de situaciones, es clave actuar con cautela y no apresurarse a aceptar condiciones que podrían comprometer mi integridad profesional.

Un ejemplo de mi solicitud podría ser el siguiente:

Asunto: Solicitud de aclaraciones sobre acuerdo de confidencialidad

Estimados representantes de CyberFort Technologies,

Me dirijo a ustedes con el propósito de solicitar aclaraciones respecto a ciertos aspectos del acuerdo de confidencialidad que me ha sido presentado en el marco del proceso de selección de personal. Quisiera asegurarme de que los términos del acuerdo cumplen con los estándares legales y éticos aplicables en Colombia, en especial con la Ley 1273 de 2009 y el Código de Ética Profesional del COPNIA.

De manera específica, agradecería su orientación sobre los siguientes puntos:

1. Prohibición de denuncia de actividades sospechosas: En el acuerdo se menciona que la parte receptora se compromete a no denunciar ante las autoridades actividades sospechosas de espionaje o apropiación de información de terceros. ¿Podrían aclararme el

propósito de esta disposición y cómo se alinea con la legislación vigente en materia de transparencia y responsabilidad legal?

2. Mención de acceso abusivo a sistemas informáticos e interceptación de información: Se hace referencia a información considerada confidencial que incluye términos como "datos de chuzadas, interceptación de información y accesos abusivos a sistemas informáticos". ¿Podrían confirmarme que el manejo de esta información cumple con la normativa de protección de datos y que no vulnera disposiciones como el artículo 269A y 269C de la Ley 1273?

3. Exención de responsabilidad de CyberFort Technologies: En la cláusula sobre solución de controversias se indica que, en caso de que la información ilegal o confidencial sea encontrada en manos del receptor, este deberá acudir a un abogado privado y dejar exenta de responsabilidad a la empresa. ¿Podrían explicarme el alcance de esta disposición y si existen precedentes legales que sustenten esta exención de responsabilidad?

Agradecería su respuesta para poder tomar una decisión informada sobre mi participación en el proceso de selección.

Quedo atento a sus comentarios y agradezco de antemano su disposición para aclarar estos puntos.

Ciberespionaje y Ética

¿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?

Según la ley estatutaria 1581 del 2012 Las empresas de ciberseguridad deben tener acceso a la información estrictamente necesaria para evaluar vulnerabilidades y riesgos durante una auditoría de seguridad, este acceso debe estar regulado por acuerdos de confidencialidad y protocolos de seguridad que garanticen que la información sensible no sea utilizada de manera indebida **(Archivo General de la Nación. n.a.)**

Además, el Decreto 1377 de 2013 reglamenta parcialmente la Ley 1581 y establece requisitos específicos para el tratamiento de datos personales, incluyendo la necesidad de acuerdos de confidencialidad y protocolos de seguridad **(Función Pública. n.a.)**

- Acuerdos de confidencialidad: Antes de la auditoría, se debe firmar un contrato que establezca límites claros sobre el uso y protección de la información.

- Acceso restringido: La empresa auditora solo debe acceder a los datos estrictamente necesarios para la evaluación, evitando la recopilación excesiva.

- Cifrado y anonimización: Se pueden aplicar técnicas de cifrado y anonimización para proteger datos sensibles sin comprometer la auditoría.

- Supervisión y auditoría interna: La empresa auditada debe monitorear el acceso y uso de la información por parte de los auditores.

- Cumplimiento normativo: Es fundamental que la auditoría cumpla con regulaciones de protección de datos y estándares de seguridad.

El manejo responsable de la información es clave para mantener la confianza entre las empresas y sus clientes.

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

Para evitar el uso indebido de herramientas avanzadas de análisis forense en empresas de ciberseguridad, es fundamental implementar mecanismos de supervisión y control rigurosos. Algunas estrategias clave son:

- Políticas de acceso restringido: Limitar el uso de herramientas forenses solo a empleados autorizados y en contextos específicos de auditoría o investigación.

- Monitoreo y auditoría continua: Implementar registros detallados de actividad y auditorías periódicas para detectar usos no autorizados de herramientas forenses.

- Capacitación en ética y cumplimiento: Implementar un programa de capacitación y educación a los empleados enfocado en los riesgos legales y éticos del uso indebido de herramientas de análisis forense.

- Autorización previa para investigaciones: Requerir aprobación formal antes de realizar cualquier análisis forense, asegurando que se cumplan los protocolos establecidos.

- Uso de entornos controlados: Ejecutar análisis forenses en entornos aislados y protegidos para evitar la manipulación de datos sensibles.

- Sanciones claras: Establecer consecuencias legales y disciplinarias para quienes utilicen herramientas forenses con fines no autorizados.

Estas medidas ayudan a garantizar que las herramientas de análisis forense sean utilizadas de manera responsable y alineada con principios éticos.

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

Cuando un gobierno u organización descubre que una empresa de ciberseguridad ha cometido actos de ciber espionaje, es crucial actuar con rapidez y firmeza para mitigar el daño, restaurando la confianza y previniendo futuros incidentes, algunas medidas clave incluyen:

1. Investigación y sanciones

- Auditoría forense: Realizar una investigación exhaustiva para determinar el alcance del espionaje y las posibles víctimas.

- Acciones legales: Aplicar sanciones conforme a la legislación vigente, incluyendo multas, revocación de licencias o incluso acciones penales contra los responsables.

- Transparencia: Publicar un informe detallado sobre el incidente para demostrar compromiso con la seguridad y la legalidad.

2. Restauración de confianza

- Revisión de contratos: Evaluar y modificar los acuerdos con proveedores de ciberseguridad para incluir cláusulas más estrictas sobre ética y cumplimiento.

- Comunicación con afectados: Informar a las partes afectadas sobre el incidente y las medidas tomadas para proteger sus datos.

- Fortalecimiento de normativas: Implementar regulaciones más estrictas para evitar que empresas con antecedentes de espionaje operen en el sector.

3. Prevención de futuros incidentes

- Supervisión continua: Establecer mecanismos de monitoreo y auditoría para detectar irregularidades en tiempo real.

- Capacitación en ética: Instruir a empleados y proveedores sobre la importancia de la seguridad y el cumplimiento normativo.

- Colaboración internacional: Trabajar con organismos globales para compartir información sobre amenazas y mejorar la ciberseguridad a nivel mundial.

Estos pasos ayudan a garantizar que el incidente no se repita y que la confianza en los servicios de ciberseguridad se mantenga.

Prueba de Penetración Red Team

Las pruebas de penetración (Penetration Testing) son cruciales para identificar las vulnerabilidades existentes en redes empresariales, aplicaciones y sistemas informáticos, que pudieran ser explotadas por algún atacante o persona maliciosa, existen diferentes metodologías de Pentesting las cuales están estructuradas en fases **(Zhao et al., 2018)**, este proceso está estructurado en etapas en las cuales se realiza un reconocimiento, escaneo, una fase de explotación, escalada de privilegios y análisis de los resultados esperados, garantizando siempre un enfoque sistemático y repetible, terminando con una documentación en donde se plasman los procedimientos, herramientas, resultados, conclusiones y recomendaciones **(Alsamadi & Khreishah. 2019).**

Según una planificación cuidadosa acompañada de una documentación detallada es fundamental para que las pruebas de penetración sean efectivas, estas deben brindar recomendaciones precisas que permitan mitigar los riesgos identificados y corregir las brechas existentes **(Kumar & Kumari. 2020).**

El ejercicio se llevó a cabo en un laboratorio dentro de un entorno controlado, configurado en dos máquinas virtuales: una con Windows 7 y otra con Kali Linux, estas plataformas fueron utilizadas para la ejecución de pruebas de penetración, permitiendo el análisis de vulnerabilidades y la evaluación de técnicas de explotación.

En la primera etapa RECONOCIMIENTO, se realizó con un análisis de la máquina Windows desde la máquina Kali, utilizando la herramienta NMAP.

Esta es una herramienta de código abierto que se utiliza para el escaneo de redes y la búsqueda de vulnerabilidades, es muy empleada en las auditorias de seguridad, la gestión de redes y en las pruebas de penetración **(Manish. 2025)**.

Opera mediante el envío de paquetes a las máquinas conectadas a la red, para luego analizar las respuestas y determinar información clave como:

- Identificación de los puertos que se encuentran abiertos
- Inferir el sistema operativo de los dispositivos
- Identificar las versiones de software en ejecución
- Realizar análisis avanzados con el objetivo de buscar vulnerabilidades conocidas.

Según los datos suministrados en el anexo 4 escenario 3, existe la posibilidad de que haya una aplicación instalada en Windows 7 la cual tiene asociado un exploit con el cual se puede obtener acceso a través de Shell y desde allí empezar una escalada de privilegios, por lo tanto, lo primero que debemos hacer es identificar cuáles son las aplicaciones que están instaladas y cuales servicios están corriendo en Windows, esto se hace con el comando:

nmap -p- -sV --script=vuln <IP_Windows_7>

en donde -p escanea todos los puertos, -sV identifica las versiones de todos los servicios y –script=vuln ejecuta los scripts que detectan las vulnerabilidades.

1. Se detectó una vulnerabilidad crítica la MS17-010 (CVE-2017-0143), la cual, permite la ejecución remota en servidores SMBv1, esto quiere decir que un atacante puede tomar control del sistema sin autenticación, su riesgo es ALTO, esta vulnerabilidad fue explotada por EternalBlue un exploit utilizado en el ataque de WannaCry.

2. Servicios abiertos con posibles riesgos: Puerto 3389 (RDP - Remote Desktop Protocol) Estado: Abierto, pero con timeout en ssl-cc-ccs-injection esto puede indicar problemas de configuración

3. Puertos 5357 y 10243 (Microsoft HTTPAPI - SSDP/UPnP) se encuentran abiertos sin vulnerabilidades detectadas, sin embargo, UPnP puede ser explotado por atacantes de la red.

Figura 18

Primer escaneo con NMAP

Fuente: Elaboración Propia

Lo siguiente es realizar una búsqueda de exploits asociados a la vulnerabilidad encontrada utilizando la herramienta Metasploit incluida en Kali Linux, según esta es una herramienta de código abierto desarrollada en el año 2003 por H.D. Moore. Es utilizada en

pruebas de penetración y auditorias de seguridad, contiene una amplia base de datos con una colección de vulnerabilidades y métodos de explotación, se adapta a distintos escenarios de pruebas permitiendo la integración de módulos personalizados, opera mediante una consola de comandos, así como una interfaz gráfica, funciona en sistemas operativos de Linus, Windows y macOS, su principal uso es para identificar y remediar cualquier vulnerabilidad existente, también es utilizada por los ciberdelincuentes para explotar las vulnerabilidades de un sistema objetivo **(Ciberseguridad. 2025).**

Esta herramienta tiene cinco módulos clasificados según la tarea que realicen:

1. Cargas útiles: estos son códigos de Shell con instrucciones para realizar acciones predeterminadas
2. Exploits: son secuencias de comandos utilizadas para aprovechar las vulnerabilidades de un sistema o aplicación
3. Publicaciones: Permiten la recopilación de información profunda para infiltrarse más en un sistema luego de la explotación.
4. Codificadores: Ocultan las cargas útiles en tránsito, garantizando que se entreguen correctamente al sistema de destino, evitando su detección por los antivirus, IDS o IPS.
5. NOP: estos crean secuencias aleatorias de los bytes con el fin de evitar los IDS
6. Auxiliares: estos son módulos auxiliares que incluyen escaneos de puertos, vulnerabilidades entre otras herramientas de explotación.

Ejecutando el comando ***search eternalblue*** se inicia la búsqueda de un exploit asociado a la vulnerabilidad encontrada

Figura 19

Búsqueda de Exploit con Metasploit

Fuente: Elaboración Propia

Efectivamente existe un exploit el número 0 el cual se ejecutará de la siguiente forma con el comando ***use 0***

Figura 20

Ajuste configuración metasploit 1

Fuente: Elaboración Propia

Es necesario realizar unos ajustes en la configuración, por lo tanto, se ejecuta el comando ***show options*** para determinar los datos faltantes

Figura 21

Ajuste configuración Metasploit 2

Fuente: Elaboración Propia

Es necesario indicarle la IP de la máquina objetivo, esto se hace por medio del comando

Set RHOST 10.10.10.5

Figura 22

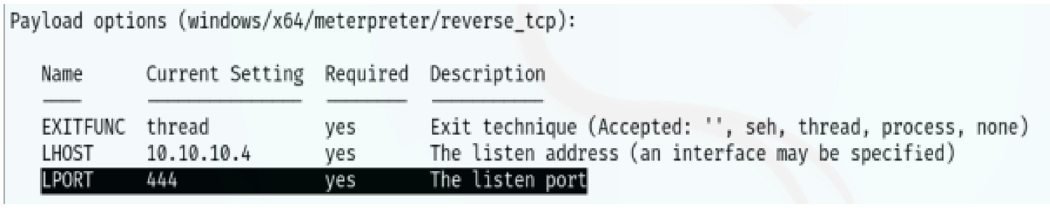
Ingreso IP equipo atacante

Fuente: Elaboración Propia

Luego se ingresa el puerto libre de la máquina atacante, por lo general se utiliza el puerto 444 o 443

Figura 23

Ingreso puerto libre máquina atacante

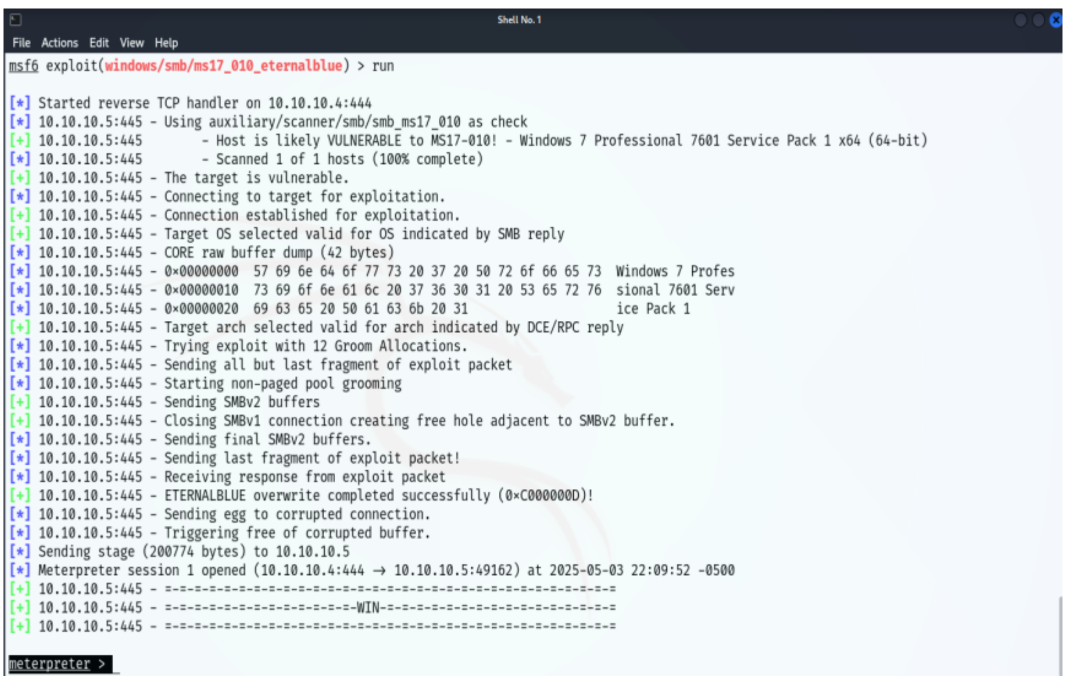


Fuente: Elaboración Propia

Se corre el exploit con el comando ***run*** y se obtiene el control de la máquina Windows

Figura 24

Ejecución de exploit

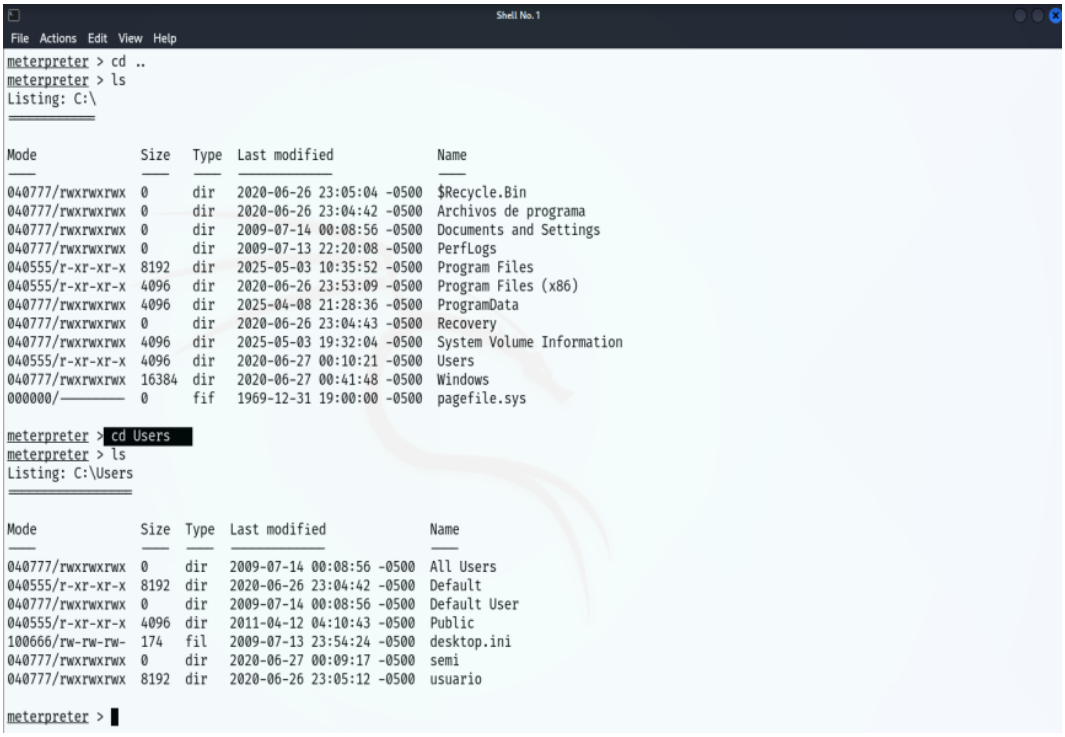


Fuente: Elaboración Propia

Ya dentro del sistema se procede a crear un usuario con privilegios, para validar que se está en el sistema se ubica en el disco C por medio de comandos (*cd.) y* luego en la capeta user se listan los usuarios que existen en el sistema con el comando ***cd user***

Figura 25

Listado de Usuarios existentes



Fuente: Elaboración Propia

Para la creación del usuario con privilegios se realiza el siguiente procedimiento, como ya se encuentra dentro del sistema Windows por medio de Meterpreter se digita el comando use incognito para ingresar a la extensión incognito

Figura 26

Ingresar la extensión incognito

Fuente: Elaboración Propia

Luego se digita el comando add_user “EdisenRincon” “2025” (Usuario y contraseña)

Figura 27

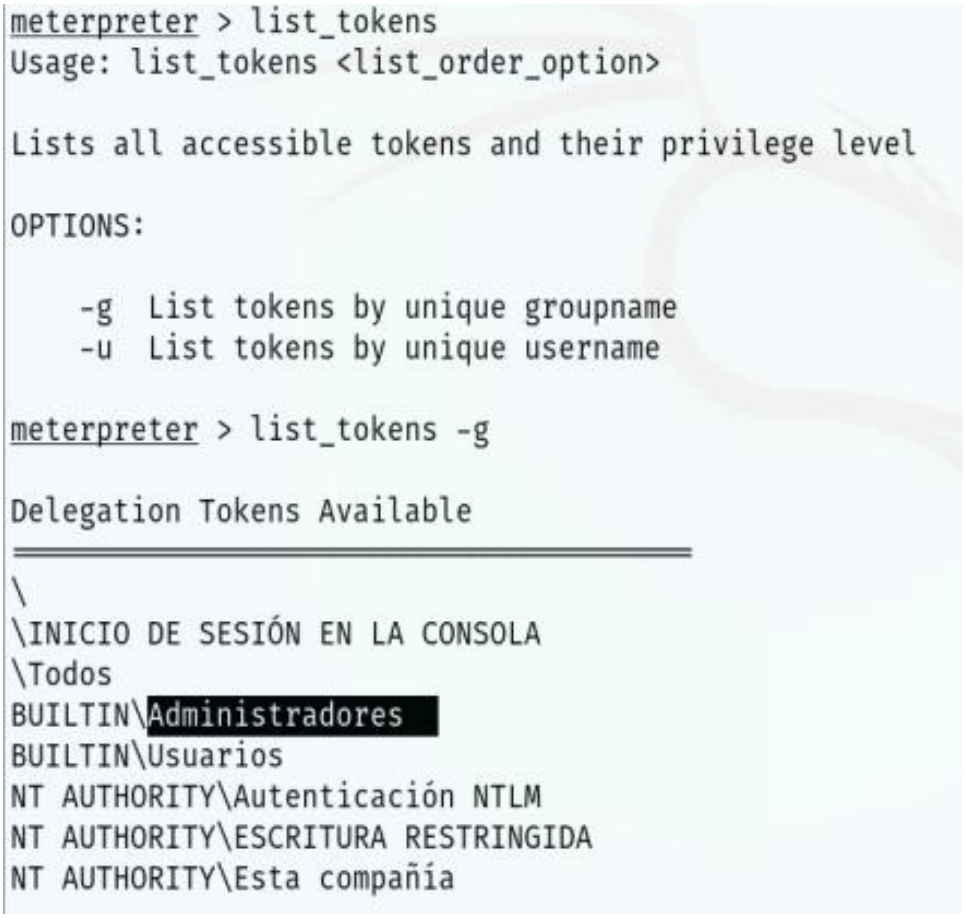
Crear Usuario y contraseña

Fuente: Elaboración Propia

El usuario ya se creó, pero no pertenece a ningún grupo por lo tanto no tiene privilegios, se procede a listar los grupos existentes para saber dónde incluir el usuario creado, con el comando ***list_tokens -g***

Figura 28

Listado grupo de usuarios



Fuente: Elaboración Propia

Ya identificado el grupo al que se debe añadir el usuario creado, que en este caso es el grupo de Administradores, lo siguiente es agregarlos con el comando

add_localgroup_user "Administradores" "EdisenRIncon"

Figura 29

Ingreso usuario creado al grupo de Administradores

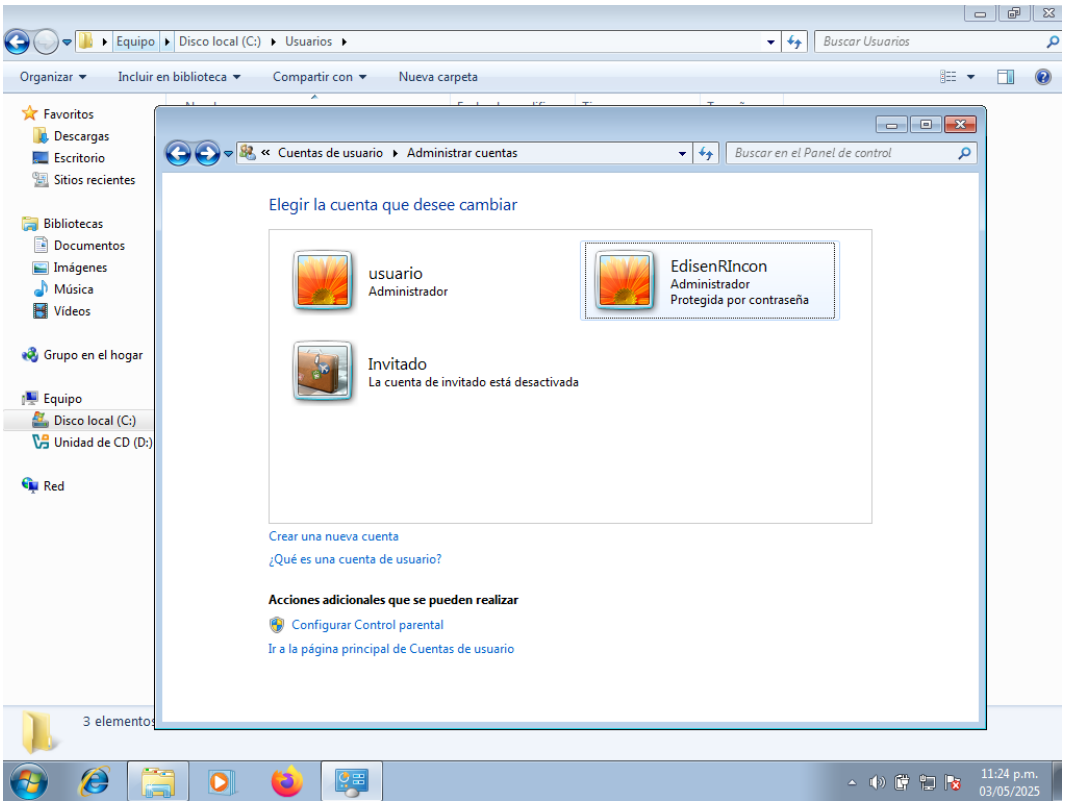
```
meterpreter > add_localgroup_user "Administradores" "EdisenRIncon"
[*] Attempting to add user EdisenRIncon to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
```

Fuente: Elaboración Propia

Se valida en la máquina Windows que el usuario si exista

Figura 30

Validación de existencia Usuario con Privilegios



Fuente: Elaboración Propia

Ataque Ms17-010

Según el equipo de Fortra Alert Logic El ataque conocido como MS17-010 se refiere a una vulnerabilidad crítica en Microsoft Windows explotada por la herramienta EternalBlue, este fallo permite la ejecución remota de código y ha sido la base para ataques masivos, siendo el ransomware WannaCry uno de los ejemplos más notorios. Estudios técnicos realizados demostraron que esta vulnerabilidad permitía la ejecución remota de código aprovechando fallos en el protocolo SMB (Server Message Block) permitiendo la propagación de un ataque **(Equipo De Fortra Alert Logic. 2017)**.

El ataque mediante EternalBlue se describe en las siguientes fases:

1. Fase de reconocimiento y selección del Objetivo: esta fase se lleva por medio de un escaneo de las redes en donde se identifican los dispositivos que utilicen Windows sin haber aplicado el parche MS17.010

2. Envío de Paquetes Maliciosos: el atacante envía estos paquetes a través del protocolo SMB, estos están diseñados para provocar un error en el procesamiento del sistema, desencadenando la ejecución del código malicioso en el dispositivo vulnerable.

3. Explotación: Se compromete la integridad del sistema, instalando el payload

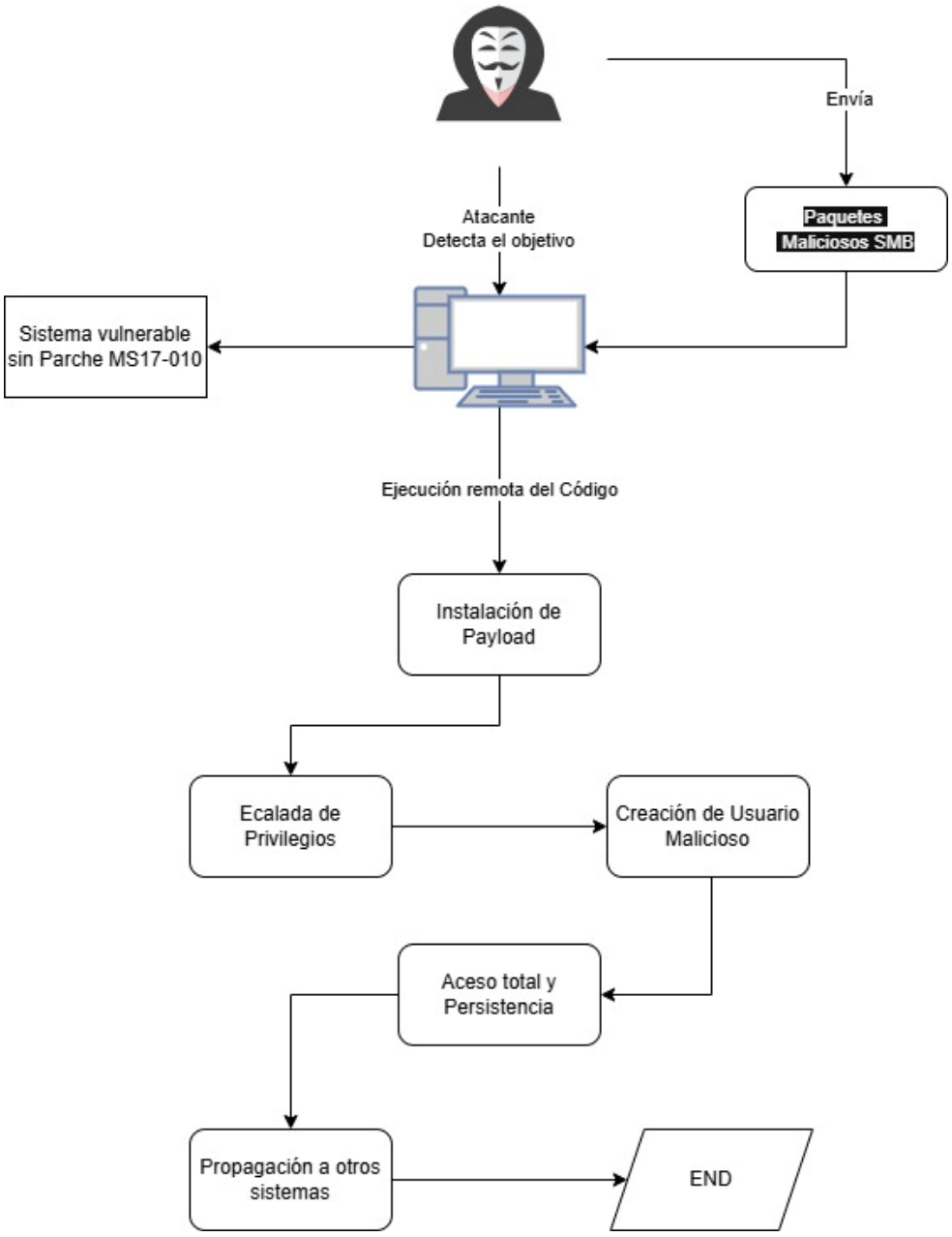
4. Escalada de privilegios: luego de la ejecución inicial del código, el atacante procede a escalar privilegios, aprovechándose de otras vulnerabilidades del sistema con el fin de obtener un mayor control accediendo a todos los recursos

5. Creación de un Usuario Malicioso y Persistencia: luego de tener el control sobre el sistema, se crean cuentas de usuario maliciosas para garantizar el acceso continuo inclusive tras un reinicio del sistema

6. Propagación y movimiento Lateral: el atacante utiliza el sistema comprometido para lanzar ataques contra otros dispositivos que se encuentren en la misma red, utilizando técnicas de movimiento lateral, buscando otras máquinas vulnerables.

Figura 31

Esquema Ataque.



Fuente: Elaboración Propia

Prueba de Contención Blue Team

¿Qué Sería lo Primero que Indagaría y Haría si Llegara a Encontrarse un Ataque en Tiempo Real?

Desde la perspectiva de un equipo Blue Team, ante un ataque en tiempo real donde solo se cuente con herramientas de licencia GLP (General Public License), lo primero es enfocar las acciones en la identificación rápida, la contención inicial y la preservación de la evidencia, la rápida respuesta y la capacidad de análisis son un factor fundamental para minimizar el impacto del incidente informático **(NIST, 2012; SANS Institute, n.d.).**

Detección y Verificación Inicial

Se realiza una indagación en donde se verifica la naturaleza y autenticidad de la alerta, es importante descartar que se trata de un falso positivo antes de tomar decisiones, se debe buscar una correlación de eventos y anomalías en el comportamiento del sistema.

En caso de confirmar la amenaza se debe Acceder a los logs del SIEM (Security Information and Event Management) utilizando ELK, filtrando y correlacionando eventos sospechosos, por ejemplo, en un ataque a Windows 7 que busca crear un usuario privilegiado, se buscarían eventos de inicio de sesión exitosos y fallidos con patrones anómalos por contraseñas incorrectas o inicios de sesión desde IPs o usuarios poco comunes Event ID 4624/4625, creación de cuentas de usuario Event ID 4720, adición a grupos privilegiados Event ID 4728/4732/4756 o modificaciones en la política de seguridad local Event ID 4719, intento de deshabilitar el registro de eventos Event ID 4719 (Microsoft, n.d.).

Se debe realizar un análisis del flujo de datos en la red, utilizando una herramienta de detección de intrusiones de red (NIDS) como Zeek, la cual permite identificar patrones de tráfico de red poco comunes y conexión a puertos no estándar o direcciones IPs sospechosas, esta

herramienta también puede detectar la presencia de comandos y control C2 mediante la inspección de protocolos y la detección de firmas o heurísticas asociadas a malware. Zeek genera logs detallados de conexiones, HTTP, DNS, SSL/TLS, etc, que pueden ser analizados con Kibana para correlacionar con eventos de host, Suricata puede generar alertas basadas en reglas que indican actividad maliciosa.

Evaluación del Impacto y Contención Rápida del Ataque

Se debe determinar qué tan comprometido quedo el sistema, verificando si el ataque se propago o se encuentra aislado y qué datos se encuentran en riesgo, las acciones son las siguientes:

Realizar un análisis de procesos y conexiones en vivo para este caso por ser un SO Windows con Sysinternals que nos ayuda a entender el comportamiento del sistema operativo, esta no es una herramienta de licencia GLP pero viene con Windows, sus herramientas como Process Explorer y TCPView son invaluables para una primera mirada a un sistema Windows comprometido, para adherirse estrictamente a GPL, alternativas como psutil (biblioteca de Python) podrían usarse para scripts personalizados de monitoreo de procesos y redes, o la exploración de logs de auditoría de Windows si están siendo recolectados por herramientas GPL.

Aislar el equipo de la red mediante su desconexión del cable de red, en caso de

contar con una infraestructura de red que permita la segmentación dinámica con firewalls controlados vía API se pueden usar scripts para aplicar reglas de aislamiento de la máquina con los servicios esenciales para la investigación, importante el “network container” no apagar la máquina directamente para preservar la memoria volátil **(SANS Institute, n.d.).**

Realizar un volcado de memoria RAM utilizando la herramienta Volatility

Framework en la máquina comprometida, esta herramienta forense permite analizar el volcado de memoria extrayendo información crucial como los procesos de ejecución y sus rutas, las conexiones de red activas, las DLLs cargadas, los módulos de kernel, los argumentos de línea de comando, incluso el historial de los comandos ejecutados en algunos casos, todos estos datos nos permitirán identificar malware en memoria, las herramientas utilizadas por el atacante y los artefactos de persistencia.

Notificación y Preservación de la Evidencia

Se debe determinar a quien se le debe notificar y comenzar con el proceso de preservación de la evidencia con el objetivo de realizar una futura investigación forense con un enfoque en la integridad de los datos:

Seguir el plan de respuestas a incidentes establecido, notificando el respectivo equipo de respuesta de incidentes CSIRT y la parte administrativa o gerencia, esta comunicación debe ser clara y oportuna **(NIST, 2012).**

Se debe crear una imagen forense del Disco duro del equipo, utilizando la herramienta dd (Disk Duplicator) esta herramienta es de distribución Linux y permite crear una imagen forense bit a bit del disco duro, esto permite asegurar que todos los datos, incluyendo el espacio no asignado y sistema operativo sean capturados de manera inalterada.

Las acciones realizadas y apoyadas con el uso de herramientas de licencia de código abierto permiten a los Blue Team enfrentar de manera eficiente un ataque en tiempo real, logrando la contención y recolección de la evidencia para una investigación profunda.

¿Teniendo en Cuenta el Ataque Ejecutado Desde el Ejercicio de Red Team, Qué Medidas de Hardenización Propondría Para que el Ataque no se Repita?

El equipo Red Team luego lograr la vulneración del sistema y la creación de un usuario y escalada de privilegios a administrador en Windows7, nos da pie para crear medidas de hardening exhaustivas, que aborden tanto las vulnerabilidades técnicas explotadas como las debilidades en la configuración y las políticas de seguridad del sistema, si bien es cierto Windows 7 ya llego al fin de su ciclo de vida y ya no recibe soporte principal de Microsoft, algo que lo hace sumamente vulnerable **(CIS, 2020),** es fundamental implementar unas mejores prácticas con el objetivo de mitigar ataques conocidos en un futuro.

Las Medidas de Hardenización para prevenir la repetición del ataque son las siguientes:

Actualizaciones de Seguridad y Gestión Rigurosa de Parches

La falta de parches adecuados permite que se lleven a cabo la mayoría de los ataques de escalada de privilegios en los sistemas operativos antiguos, ya que sus vulnerabilidades son conocidas y públicamente divulgadas **(Portnox, n.d.; UpGuard, n.d.),** si bien es cierto que el soporte para Windows 7 ya ha finalizado, Microsoft ofreció algunas actualizaciones de seguridad a través de programas ESU.

Por lo tanto, es necesario priorizar las actualizaciones de seguridad disponibles, incluyendo las Extended Security Updates (ESU) **(BytePlus. 2025),** con esto se logra cerrar las brechas de seguridad que ya son conocidas y explotadas por los atacantes.

Se debe implementar un sistema de gestión de parches para asegurar que las máquinas que utilicen W7 reciban los parches de manera consistente y oportuna **(SecHard, n.d.).**

Principio de Mínimos Privilegios

Este principio restringe el acceso de usuarios y aplicaciones únicamente a los recursos y funciones estrictamente necesarios para su operación **(WafaiCloud, n.d.; Portnox. 2025).**

Por lo tanto, se debe reducir drásticamente el número de cuentas que gozan con privilegio de administrador y las cuentas de usuario estándar no deben tener permisos de administrador locales de forma predeterminada **(Microsoft. 2025).**

Se recomienda deshabilitar o renombrar la cuenta de Administrador que viene por defecto, ya que esta es un objetivo frecuente, una buena práctica es crear una cuenta alternativa que tenga configurada una contraseña fuerte **(ne Digital. 2025).**

Se debe habilitar el control de cuentas de usuario y configurarlo para pedir consentimiento para las operaciones administrativas, esto añade una capa de protección contra la ejecución no autorizada de programas **(BytePlus. 2025).**

Se deben otorgar permisos granulares a carpetas o archivos claves de registros críticos en lugar de otorgar permisos amplios, asegurándonos de que solo los usuarios o servicios autorizados pueden modificarlos.

Configuración Segura de los Servicios y Aplicaciones

Las aplicaciones mal configuradas con privilegios elevados permiten a los atacantes vulnerar los sistemas, por eso es necesario deshabilitar aquellos que no se usen, reduciendo así la superficie de ataque **(NinjaOne. 2025).**

Desinstalar cualquier software, controlador o librería que no sea estrictamente necesario en el sistema, ya que cada una de estas piezas puede introducir nuevas vulnerabilidades al sistema **(NinjaOne. 2025).**

Implementar listas blancas de aplicaciones que permitan que solo el software que sea aprobado y confiable se ejecute en el sistema, esto permite prevenir que los atacantes ejecuten herramientas maliciosas o scripts utilizados para la creación de usuarios y escalada de privilegios **(Portnox. 2025).** Windows 7 no tiene AppLocker, pero existen soluciones de terceros que se pueden aplicar.

Modernizar los protocolos de comunicación deshabilitando versiones antiguas e inseguras como SSL 3.0, TLS 1.0/1.1 y forzando el uso de TLS 1.2 o superior para todas las comunicaciones **(BytePlus. 2025).**

Fortalecimiento de las Políticas de Contraseñas y Autenticación

Un vector muy común en los ataques a los sistemas de seguridad son las contraseñas débiles, por eso es necesario implementar políticas de grupo para exigir contraseñas largas y con un mínimo de caracteres especiales y una combinación de letras mayúsculas y minúsculas con números **(CIS, 2020).**

Implementar políticas de envejecimiento de contraseñas con un tiempo determinado no mayor a 90 días, para reducir la ventana de exposición en caso de compromiso **(CIS, 2020).**

Configurar políticas de bloqueo de cuentas después de determinado número de intentos de inicio de sesión fallidos, con esto mitigaremos los ataques de fuerza bruta.

Es importante implementar la Autenticación Multifactor (MFA) esto añade una capa de seguridad significativa, sobre todo en los entornos de acceso remoto **(Portnox. 2025).**

Configuración de Firewall y Segmentación de Red

Los firewalls bien configurados limitan el tráfico de red controlando las comunicaciones que entran y salen al sistema y la segmentación aísla los activos más críticos de la compañía y evitando el desplazamiento lateral **(ne Digital, n.d.; BytePlus. 2025).**

Implementar soluciones IDS/IPS a nivel de red para monitorear el tráfico y detectar patrones de ataque o tráfico de datos sospechoso **(BytePlus. 2025).**

Auditorías y Monitoreo Continuo

Habilitar auditorias de seguridad exhaustivas sobre todo en los equipos que tengan W7, prestando atención a los eventos de creación de cuentas y adición de grupos, así como en los cambios de las políticas de seguridad e intentos fallidos de inicio de sesión.

Centralización de los logs de seguridad de W7 en un sistema SIEM para su análisis y correlación en tiempo real, esto permite una temprana detección de patrones anómalos que pueden indicar la ejecución de un ataque o escalada de privilegios.

Realizar una serie de auditorías de seguridad periódicas, incluyendo el escaneo de vulnerabilidades.

Diferencias Entre un Equipo Blueteam y un Equipo de Respuesta a Incidentes Informáticos

Los equipos azules tienen una misión más amplia y proactiva que los equipos de respuesta a incidentes, su principal objetivo es proteger los activos de manera continua, detectando amenazad y fortaleciendo la postura de seguridad general, su alcance es una cobertura amplia que abarca toda la infraestructura de seguridad de la organización, realizan un monitoreo continuo 24/7 de las redes, las aplicaciones y los sistemas buscando anomalías o actividades sospechosas mediante el uso de herramientas como los SIEM, EDR o IDS/IPS, identifican, evalúan y mitigan las debilidades do los sistemas y software mediante la aplicación de parches y hardening, implementan y mejoran los controles de seguridad mediante la implantación y configuración de firewalls, segmentación de red y configuración de políticas de acceso al

sistema, además realizan una constante investigación de las últimas amenazas y técnicas de ataque, adaptando el sistema de seguridad; también realizan una búsqueda proactiva de las amenazas persistentes no detectadas dentro de la red, se encargan de capacitar al personal de la organización sobre las mejores prácticas de seguridad y la concienciación sobre la ingeniería social y los errores humanos como factor determinante dentro del sistema de seguridad de la empresa, este grupo es un actor constantemente activo antes, durante y después de un incidente de seguridad informática.

Por otra parte los Equipos de Respuesta a Incidentes Informáticos también llamados CSIRT, son un grupo especializado y reactivo que se activa cuando ya se ha producido un incidente de seguridad, su objetivo principal es gestionar el incidente desde su detección hasta su contención y recuperación del sistema minimizando el daño directo y colateral, su alcance es específico para los incidentes de seguridad que ya se encuentran en curso, sus actividades principales se centran en el ciclo de vida de la respuesta a los incidentes de seguridad, confirmando la existencia de un incidente y determinando su alcance, naturaleza e impacto, luego se concentran en la contención del evento aislando el sistema previniendo la propagación del ataque, para seguir con la eliminación de la causa raíz del evento, por ejemplo software malicioso o acceso de los atacantes, para luego recuperar y restaurar los sistemas y servicios afectados, finalizando con la recolección y análisis de la evidencia con el fin de entender de qué manera ocurrió el evento, cuáles fueron las herramientas que utilizaron los ciberdelincuentes, las brechas de seguridad aprovechadas por estos y determinar los posibles responsables; documentan los hallazgos y proponen estrategias de mejora e implementación de herramientas de seguridad adicionales en caso de ser necesario.

En ocasiones los equipos Blue Team pueden formar parte del ITR Team o trabajar de la mano, mediante una relación sinérgica, aprendiendo de cada evento para fortalecer las medidas de seguridad de la corporación.

Tabla 1

Diferencias Blue Team & IR Team/CSIRT

Característica	Blue Team	Equipo de respuesta a incidentes IR Team/CSIRT
Misión Principal	Proteger y fortalecer la postura de seguridad general de manera continua, previniendo ataques y detectando amenazas.	Gestionar y resolver incidentes de seguridad que ya están ocurriendo, minimizando su impacto y restaurando la normalidad.
Enfoque	Proactivo y Preventivo (con capacidades de detección y respuesta)	Reactivo (se activa ante un incidente).
Cuando Actúa	Siempre activo, en el día a día, vigilando y mejorando las defensas.	Se activa cuando se detecta un incidente de seguridad, y sus actividades cesan una vez que el incidente está resuelto y se han extraído las lecciones.
Alcance	Amplio; toda la infraestructura y las políticas de seguridad.	Específico; enfocado en un incidente particular.
Relación con el Red Team	Defiende contra los ataques simulados por el Red Team para probar y mejorar las defensas.	Puede participar en ejercicios con el Red Team para probar la eficacia del plan de respuesta a incidentes.
Objetivo a Largo Plazo	Reducir la superficie de ataque y la probabilidad de que ocurran incidentes.	Reducir el tiempo de permanencia del atacante (Dwell Time) y el impacto de los incidentes.

Fuente: Elaboración propia

¿Si Dentro de un Equipo Blueteam le Indican que Debe Trabajar con Cis "¿Center For Internet Security", Usted lo Utilizaría Para qué Fin?

En el contexto de un equipo Blue Team, la integración del Center for Internet Security (CIS) resulta fundamental para establecer una postura de seguridad sólida basada en estándares reconocidos, su aplicación garantiza un enfoque estructurado para la protección de sistemas críticos dentro de una organización.

Las dos herramientas principales de CIS, los Controles CIS y los Puntos de Referencia CIS, representan marcos de seguridad desarrollados por expertos globales en ciberseguridad. Estas directrices proporcionan metodologías claras y priorizadas para endurecer configuraciones y reducir riesgos **(Ciegate Technologies, 2025).**

Endurecimiento de Sistemas y Aplicaciones

El CIS permite implementar políticas de hardening en sistemas operativos, aplicaciones y dispositivos de red, asegurando configuraciones seguras más allá de los valores predeterminados. Esto implica:

- Aplicación de Políticas de Grupo (GPO) para controlar accesos y auditorías en entornos Windows.
- Desactivación de servicios innecesarios para minimizar la superficie de ataque **(Trio MDM., 2024).**
- Gestión de cuentas y privilegios, adoptando el principio de mínimo privilegio.
- Configuración estricta de firewalls para restringir accesos no autorizados.

Evaluación Continua de la Postura de Seguridad

Las guías del CIS se convierten en una referencia esencial para auditar sistemas, permitiendo realizar:

- Escaneos de conformidad, comparando configuraciones actuales con benchmarks de seguridad **(Microsoft. 2025).**
- Identificación de brechas de seguridad, detectando configuraciones incorrectas que podrían ser explotadas por atacantes.

Fortalecimiento de la Detección y Monitoreo

Además de la prevención, los Controles CIS optimizan la detección de amenazas mediante la integración con herramientas como SIEM. En este proceso, es crucial:

- Centralizar la recolección de logs, asegurando la auditoría de eventos clave como la
- creación de usuarios y modificaciones en configuraciones críticas **(CISO Global, n.d.).**
- Desarrollar reglas de detección, creando alertas en SIEM basadas en patrones de actividad sospechosa **(Carbide, n.d.).**

Priorización de Inversión en Ciberseguridad

El CIS permite definir estrategias de inversión basadas en la reducción efectiva de riesgos. Esto facilita:

- Asignación eficiente de recursos, enfocando esfuerzos en controles que maximicen la seguridad.
- Comunicación del riesgo a nivel directivo, justificando decisiones basadas en marcos reconocidos **(Towerwall, n.d.).**

En conclusión, la integración del CIS dentro de un equipo Blue Team no solo fortalece la defensa contra amenazas digitales, sino que también optimiza la respuesta ante incidentes en tiempo real, proporcionando un marco estructurado para la seguridad organizacional.

Funciones y Características Principales de un SIEM

Un Security Information and Event Management (SIEM) es una solución esencial para la gestión centralizada de datos de seguridad en una organización, su principal función es agregar, analizar y correlacionar eventos de seguridad en tiempo real, permitiendo una rápida detección y respuesta ante incidentes **(IBM, n.d.-a)**. Al combinar capacidades de Gestión de Información de Seguridad (SIM) y Gestión de Eventos de Seguridad (SEM), proporciona una visión integral de la infraestructura de TI **(Ambit BST. 2021).**

Funciones Clave de un SIEM

- Gestión de registros y agregación de datos: Un SIEM recopila eventos de seguridad
- de múltiples fuentes, incluyendo firewalls, IDS/IPS, endpoints, sistemas operativos y bases de datos, normalizando la información para su análisis estructurado **(IBM, n.d.-a).**
- Correlación y análisis de eventos: Aplicando algoritmos de machine learning y
- heurísticas, un SIEM detecta patrones anómalos, como intentos de acceso sospechosos o actividad inusual dentro de la red **(Ambit BST 2021).**
- Monitoreo de incidentes y alertas: Cuando se identifica actividad maliciosa, el SIEM
- genera alertas priorizadas, visibles en dashboards, facilitando una respuesta rápida por parte del equipo de seguridad **(Check Point Software, n.d.; Microsoft, n.d.).**
- Investigación forense y búsqueda de datos históricos: Almacena eventos de
- seguridad para su análisis retrospectivo, permitiendo reconstruir la cadena de un ataque cibernético y evaluar su impacto
- Generación de informes y auditoría de cumplimiento: Produce reportes alineados

- con normativas como GDPR, HIPAA, PCI DSS e ISO 27001, asegurando que la organización cumple con estándares de seguridad **(Intervalle Technologies. 2024).**

Características Esenciales de un SIEM

- Centralización de logs en una única plataforma de monitoreo.
- Análisis en tiempo real, permitiendo respuestas inmediatas a amenazas.
- Integración con inteligencia de amenazas para detectar ataques conocidos **(IBM, n.d.-a).**
- Escalabilidad, asegurando la gestión de grandes volúmenes de datos.
- Automatización de respuesta mediante la integración con SOAR, optimizando los
    - flujos de trabajo de ciberseguridad **(IBM, n.d.-b).**

Herramientas de Contención de Ataques Informáticos Hardware o Software

La contención de ataques informáticos es esencial para limitar los daños tras detectar una amenaza, no se trata solo de identificar el ataque, sino también de actuar rápidamente para aislarlo y evitar que se propague o cause más daño.

Tres herramientas clave de contención son:

Firewalls (Hardware o Software)

Son como puertas de control en la red, que filtran el tráfico según reglas predefinidas **(Check Point Software, n.d.-a; Cisco, n.d.-a).** Cuando detectamos un ataque, podemos ajustarlos para bloquear direcciones IP sospechosas, cerrar puertos o restringir protocolos. Por ejemplo, un firewall Cisco ASA puede bloquear un IP malicioso, y en software, iptables en Linux ayuda a controlar aún más ese tráfico **(Juniper Networks, n.d.-a).**

Sistemas de Prevención de Intrusiones (IPS) en Modo de Bloqueo

Son sistemas que están en alerta y actúan en tiempo real para detener actividades maliciosas detectadas, a diferencia de los sistemas de detección pasiva, el IPS puede cerrar sesiones, bloquear IPs o poner en cuarentena archivos peligrosos automáticamente, ayudando a detener un ataque en medio de su curso **(IBM, n.d.-a; McAfee, n.d).** Ejemplos como Cisco Firepower o Snort, que puede configurarse en modo preventivo, muestran cómo estos sistemas se involucran activamente en la contención.

Aislamiento o Cuarentena de Endpoints

Este método se enfoca en el dispositivo final, como una computadora o servidor, que puede estar comprometido, mediante soluciones EDR como CrowdStrike o SentinelOne, si detectan comportamiento malicioso, pueden aislar ese equipo de la red antes de que el malware se propague o se exfiltren datos, esto se parece a poner en cuarentena a un animal enfermo para evitar que infecte a los demás **(CrowdStrike, n.d.; SentinelOne, n.d).**

Conclusiones

Regulación rigurosa del acceso a información sensible, La Ley 1581 de 2012 y el Decreto 1377 de 2013 establecen que las empresas de ciberseguridad solo deben acceder a la información estrictamente necesaria durante auditorías de seguridad, esto debe ser respaldado por acuerdos de confidencialidad claros, protocolos de seguridad, y mecanismos como cifrado, anonimización, y supervisión interna, con el fin de proteger los datos personales y evitar su uso indebido, esto destaca la importancia del cumplimiento normativo para mantener la confianza de los clientes.

Prevención del uso indebido de herramientas y acceso, para mitigar riesgos éticos, es fundamental implementar controles estrictos en el uso de herramientas de análisis forense, medidas como políticas de acceso restringido, monitoreo continuo, autorización previa para investigaciones, capacitación en ética y sanciones claras son esenciales para garantizar que el personal actúe de manera responsable y en alineación con los principios éticos y legales, esto no solo previene abusos, sino que también fortalece la reputación de la organización

El análisis identificó que el sistema Windows 7 - 10 es vulnerable a MS17-010 (CVE-2017-0143), lo que indica un alto riesgo de ejecución remota de código a través de SMBv1. Esta vulnerabilidad ha sido explotada en ataques como EternalBlue, lo que evidencia la importancia de mantener sistemas operativos actualizados y aplicar parches de seguridad.

Explotación y escalamiento de privilegios exitoso: La ejecución del exploit permitió obtener acceso al sistema y demostrar una Proof of Concept (PoC) mediante la creación de un usuario con privilegios administrativos, esto confirma que la vulnerabilidad es explotable y que un atacante con conocimientos técnicos puede tomar el control del sistema, lo que resalta la necesidad de implementar controles de acceso más estrictos.

Relevancia de los métodos de detección y evaluación: El uso de Nmap y Metasploit permitió identificar servicios expuestos y vulnerabilidades activas, lo que demuestra la efectividad de un enfoque sistemático en pruebas de penetración, la combinación de reconocimiento, explotación y escalamiento de privilegios proporciona una visión clara del impacto que una brecha de seguridad puede tener en un entorno corporativo.

Importancia de la mitigación y seguridad proactiva: La explotación exitosa de estas vulnerabilidades subraya la necesidad de aplicar medidas de seguridad como:

- Actualizar el sistema operativo y aplicar parches (MS17-010).
- Deshabilitar SMBv1 en equipos que no lo requieran.
- Configurar restricciones de acceso a RDP para evitar ataques de fuerza bruta y explotación de vulnerabilidades como BlueKeep.
- Monitorear el tráfico de red con herramientas de detección de intrusiones para identificar actividades sospechosas.

La respuesta efectiva ante un ataque en tiempo real por parte de un equipo Blue Team es posible con el uso estratégico de herramientas GLP, permitiendo la mitigación del impacto y la preservación de la evidencia forense; para ello, es fundamental priorizar la verificación rápida de alertas, la contención inmediata del activo comprometido y la recolección de datos almacenados en las memorias volátiles y persistentes, estableciendo una base sólida para investigaciones posteriores y la eventual erradicación de la amenaza.

Este enfoque debe alinearse con los principios de ciberseguridad y las metodologías proactivas propuestas por NIST y SANS, lo que garantiza una gestión estructurada y eficiente del incidente, asimismo, el fortalecimiento de las capacidades del equipo se optimiza mediante la adopción de herramientas accesibles y estratégicamente implementadas, permitiendo una mejor

defensa ante ataques dirigidos y contribuyendo al desarrollo de una postura de seguridad más resiliente.

La gestión de un ciberataque en tiempo real requiere que el equipo Blue Team implemente una metodología de respuesta ágil y estructurada, apoyada en su capacidad técnica para actuar bajo presión; la interpretación rápida de eventos de seguridad (Event IDs en Windows), la correlación de datos de red y host, y la aplicación de medidas de contención precisas determinan la diferencia entre un incidente controlado y uno que escala a un compromiso mayor.

El dominio de herramientas de código abierto y su integración dentro de un ecosistema de defensa, como un SIEM basado en ELK, no solo optimiza costos, sino que también fortalece la comprensión de los mecanismos de seguridad y la adaptabilidad de las soluciones a las necesidades específicas del entorno; este enfoque resulta fundamental para la protección de sistemas como Windows 7, mitigando intentos de escalada de privilegios y consolidando una postura de seguridad más resiliente.

La obsolescencia de Windows 7 supone un riesgo permanente, haciendo que las medidas de hardening sean solo paliativas, aunque la aplicación de principios como mínimo privilegio, gestión de parches y configuración de firewalls reduce vulnerabilidades, no elimina la exposición a nuevas amenazas sin soporte oficial, la única estrategia sostenible es la migración a sistemas con soporte activo.

Por otro lado, la prevención de ataques de escalada de privilegios y creación de usuarios maliciosos requiere un enfoque de seguridad por capas, no existe una única solución, sino una combinación de políticas de acceso, segmentación de red y monitoreo continuo mediante SIEM;

La detección rápida de anomalías y la auditoría de logs son esenciales para responder de manera efectiva y garantizar una seguridad operativa constante.

El CIS (Center for Internet Security) funcionaría como la columna vertebral para construir y mantener una defensa sólida y proactiva, permitiendo al equipo Blue Team no solo reaccionar a los ataques, sino principalmente prevenirlos y fortalecer la postura general de seguridad de la organización.

La integración del CIS dentro de un equipo Blue Team no solo fortalece la defensa contra amenazas digitales, sino que también optimiza la respuesta ante incidentes en tiempo real, proporcionando un marco estructurado para la seguridad organizacional.

El uso de un SIEM dentro de un Centro de Operaciones de Seguridad (SOC) ofrece visibilidad proactiva sobre la postura de seguridad de una organización, su capacidad para detectar amenazas avanzadas, optimizar respuestas y cumplir con regulaciones lo convierte en una herramienta indispensable para la protección de la infraestructura digital **(LRQA España, n.d.).**

Es importante recordar que las herramientas de contención deben usarse dentro de un plan de respuesta a incidentes bien estructurado, el cual defina claramente cuándo y cómo activar cada medida para reducir al máximo los daños **(SANS Institute, n.d).**

Recomendaciones

Para proteger los sistemas frente a amenazas como MS17-010 (EternalBlue) y otros ataques de escalamiento de privilegios, se recomienda implementar una combinación de medidas técnicas y administrativas, una estrategia de defensa estructurada puede ser la siguiente:

- Aplicación de parches y actualización del sistema instalando MS17-01: Microsoft liberó parches de seguridad que corrigen esta vulnerabilidad en Windows 7, 8 y 10.
- Actualizar Windows: Considerar la migración a versiones más recientes, ya que Windows 7 ha dejado de recibir soporte.
- Habilitar actualizaciones automáticas para garantizar que futuras vulnerabilidades sean corregidas a tiempo.
- Endurecimiento del protocolo SMB deshabilitando SMBv1 si no es necesario, ya que es un protocolo obsoleto y vulnerable:
- Restringir acceso a SMB con firewall y listas de control de acceso (ACLs).
- Monitorear tráfico SMB para detectar actividad sospechosa.
- Protección contra ataques de fuerza bruta en RDP
- Habilitar Network Level Authentication (NLA) para exigir autenticación antes de establecer una sesión de escritorio remoto.
- Configurar restricciones de acceso mediante políticas de grupo (`gpedit.msc`).
- Monitorear intentos de acceso con herramientas SIEM para detectar patrones de ataque.
- Implementación de mecanismos de detección y respuesta usando herramientas de detección de intrusos (IDS/IPS) como Suricata o Snort para identificar intentos de explotación.

- Registrar actividad sospechosa en Windows Event Viewer y Sysmon.
- Configurar análisis de logs con SIEM como Splunk o ELK Stack para correlacionar eventos maliciosos.
- Concienciación y capacitación en seguridad, capacitando al personal sobre las amenazas de ciberseguridad y cómo reconocer intentos de phishing y explotación.
- Ejecutar simulaciones de ataques (Red Team) para evaluar la preparación de la organización.
- Realizar auditorías de seguridad periódicas para identificar brechas antes de que sean explotadas.

Estas medidas ayudarán a prevenir ataques y garantizar un entorno más seguro

El fortalecimiento de la respuesta ante ataques en tiempo real requiere que los equipos Blue Team prioricen la capacitación y el uso de herramientas de código abierto como ELK, Zeek, Suricata, Volatility y dd, enfocadas en detección, contención y recolección de evidencia, la implementación de protocolos ágiles para la verificación de alertas y el aislamiento de activos minimiza el impacto de los incidentes.

Asimismo, la integración de un SIEM de código abierto, como ELK, permite centralizar y correlacionar logs de seguridad, mejorando la visibilidad del entorno y optimizando la capacidad de detección de anomalías, esta estrategia no solo reduce costos, sino que fortalece la respuesta del Blue Team, facilitando la identificación y mitigación de amenazas como la creación de usuarios maliciosos y la escalada de privilegios en sistemas vulnerables.

Aplicar medidas de hardening de manera consistente es fundamental para reducir la superficie de ataque y mitigar el riesgo significativamente, sin embargo, en este caso Windows 7

es un SO obsoleto sin soporte, se recomienda migrar a versiones más modernas y que tengan soporte.

Los equipos Blue Team deben trabajar con el Center for Internet Security /CIS) para fortalecer directamente sus capacidades defensivas ya que este ofrece un conjunto de estándares y directrices reconocidas globalmente las cuales proporcionan un enfoque estructurado basado en el consenso para la ciberseguridad.

Referencias Bibliográficas

Alsmadi, I., & Khreishah, A. (2019). A survey of penetration testing methodologies: Challenges and future directions. *IEEE Access, 7*, 147693-147711.

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

BytePlus. (2025). *Hardening error windows 7: Practical steps for secure legacy systems*. https://www.byteplus.com/en/topic/553787

Carbide. (n.d.). *Overview of the Center for Internet Security (CIS)*. https://support.carbidesecure.com/hc/en-us/articles/8118835587220-Overview-of-the-Center-for-Internet-Security-CIS

Center for Internet Security (CIS). (2020). *CIS Microsoft Windows 7 Workstation Benchmark*. https://itref.ir/uploads/editor/2f06a3.pdf

Check Point Software. (n.d.-a). *¿Qué es SIEM (Gestión de eventos e información de seguridad)?* https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/

Check Point Software. (n.d.-b). *Firewall*. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-a-firewall/

Ciberseguridad. (2025, mayo). *¿Qué es Metasploit Framework y cómo funciona?* https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Ciegate Technologies. (2025, mayo 1). *Center for Internet Security (CIS): Safeguarding Cyberspace with Benchmarks and Controls*. https://www.ciegate.com/cis-center-for-internet-security/

Cisco. (n.d.). *What is a Firewall?* https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Common Vulnerabilities and Exposures. (n.d.). *CVE - Common Vulnerabilities and Exposures*. https://cve.mitre.org/

CrowdStrike. (n.d.). *Endpoint Isolation: Contain Threats and Prevent Lateral Movement*. https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-isolation/

CVE. (n.d.). *Common Vulnerabilities and Exposures*. https://cve.mitre.org/

Decreto 1377 de 2013. (n.d.). *Decreto 1377 de 2013*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Equipo De Fortra Alert Logic. (2017, mayo). *WannaCry – Una propagación presentada por EternalBlue y DoublePulsar*. https://www.alertlogic.com/blog/wannacry-a-propagation-brought-to-you-by-eternalblue-and-doublepulsar-d18/

Exploit Database. (n.d.). *Exploit Database*. https://www.exploit-db.com/

ExploitDB. (n.d.). *Exploit Database*. https://www.exploit-db.com/

Greenbone Networks. (2025). *OpenVAS - Open Vulnerability Assessment Scanner*. https://www.greenbone.net/en/openvas/

Greenbone Networks. (2025). *OpenVAS - Vulnerability Scanner*.https://www.greenbone.net/en/openvas/

IBM. (2023, junio). *What is SIEM?* https://www.ibm.com/think/topics/siem

IBM. (n.d.-a). *Intrusion Prevention System (IPS)*. https://www.ibm.com/topics/intrusion-prevention-system

IBM. (n.d.-b). *SIEM - Security Information and Event Management* https://www.ibm.com/security/security-intelligence/siem

IBM. (n.d.-c). *¿Qué es la gestión de eventos e información de seguridad (SIEM)?* https://www.ibm.com/mx-es/topics/siem

Intervalle Technologies. (2024, abril). *SIEM Fundamentals: Definition, Functions, and Use Cases*. https://intervalle-technologies.com/blog/security-information-and-event-management-siem-explained/

Jones, A. (2020). Cybersecurity vulnerabilities: Exploitation techniques. *Cybersecurity Journal*, *15*(3), 45-60.

Jones, M. (2020). The importance of Exploits and Vulnerabilities in Cybersecurity. *Cybersecurity Journal*, *15*(2), 45-60.

Juniper Networks. (n.d.). *What is Network Segmentation?* https://www.juniper.net/us/en/research-library/network-segmentation/

Kumar, R., & Kumari, P. (2020). Penetration testing: Concepts and frameworks. *International Journal of Cyber Security*, *32*(4), 112-125.

Kumar, V., & Kumari, N. (2020). Penetration testing: Techniques, tools and challenges. *Journal of Cybersecurity*, *6*(2), 65-80.

Ley 1581 de 2012. (n.d.). *Ley de protección de datos personales*. https://www.sic.gov.co/

Ley Estatutaria 1581 de 2012. (n.d.). *Ley Estatutaria 1581 de 2012*. Normativa Archivo General de la Nación. https://normativa.archivogeneral.gov.co/ley-estatutaria-1581-de-2012/

Manish, S. (n.d.). *What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time*. Freecodecamp.org. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

Manish. (2025). *Nmap Network Scanner*. https://nmap.org/

McAfee. (n.d.-a). *Intrusion Detection and Prevention Systems*. https://www.mcafee.com/enterprise/en-us/security-awareness/intrusion-detection.html

McAfee. (n.d.-b). *What is an Intrusion Prevention System (IPS)?* https://www.mcafee.com/en-us/antivirus/intrusion-prevention-system.html

Metasploit. (2025). *Framework for Penetration Testing*. https://metasploit.help.rapid7.com/

Micucci, M. (2023). *Evaluación de vulnerabilidades usando OpenVAS*. Welivesecurity. Recuperado de https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

Microsoft. (2025, marzo). *Center for Internet Security (CIS) Benchmarks*. https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

Microsoft. (n.d.). *Improving security by protecting elevated-privilege accounts at Microsoft*. https://www.microsoft.com/insidetrack/blog/improving-security-by-protecting-elevated-privilege-accounts-at-microsoft/

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide* (Special Publication 800-61 Rev. 2). U.S. Department of Commerce.

NE Digital. (n.d.). *Las 7 etapas de Hardening de servidores Windows para proteger sistemas*. https://www.nedigital.com/es/blog/hardening-de-servidores-windows

NinjaOne. (2025, abril). *Mejores prácticas de hardening de sistemas para reducir riesgos [Checklist]*. https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

NVD - National Vulnerability Database. (n.d.). *NVD - National Vulnerability Database*. https://nvd.nist.gov/

Policía Nacional de Colombia. (n.d.-a). *Ley 1273 de 2009. Política de delitos informáticos*. https://www.policia.gov.co/

Policía Nacional de Colombia. (n.d.-b). *Normatividad Sobre Delitos Informáticos. Ley 1273 de 2009*. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos#:~:text=LEY%201273%20DE%202009,las%20comunicaciones%2C%20entre%20otras%20disposiciones.

Portnox. (n.d.). *What is Privilege Escalation?* https://www.portnox.com/cybersecurity-101/what-is-privilege-escalation/

SANS Institute. (n.d.). *Incident Response Policy*. https://www.sans.org/security-resources/policies/

SecHard. (n.d.). *Security Configuration Management*. https://sechard.com/files/Security%20Configuration%20Management.pdf

SentinelOne. (n.d.). *Network Control & Isolation*. https://www.sentinelone.com/platform/network-control-isolation/

Tówerwall, J. (n.d.). Security mitigation strategies. *Cyber Defense Review*, *12*(2), 78-84.

Towerwall. (n.d.). *Whitepapers: Top 18 Critical Security Controls from the Center for Internet Security*. https://towerwall.com/top-18-critical-security-controls-from-the-center-for-internet-security/

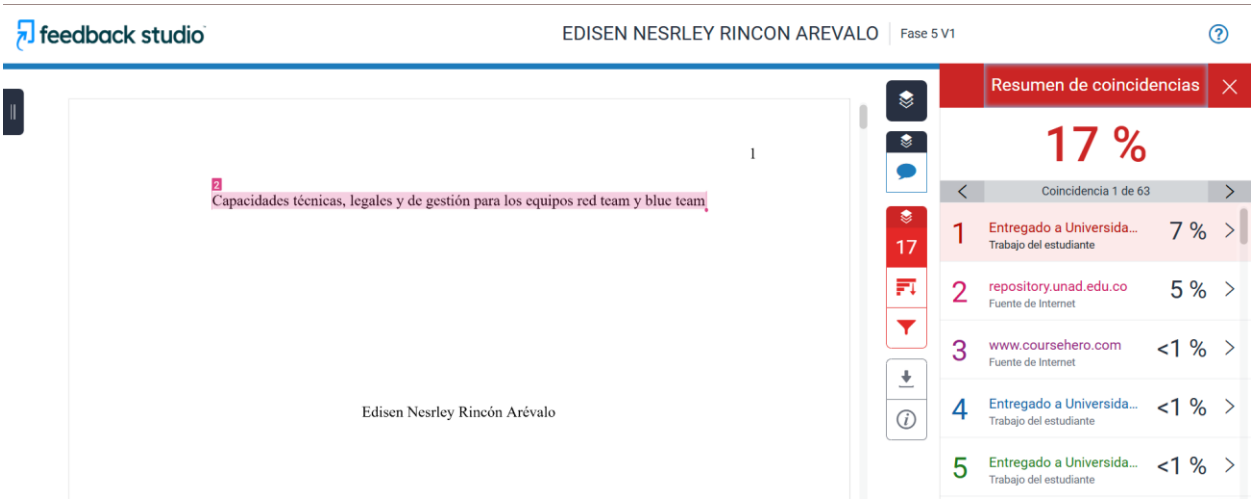
Trio MDM. (2024, octubre). *A Guide to the Center for Internet Security Controls*. https://www.trio.so/blog/center-for-internet-security-controls/

WafaiCloud. (2025, abril). *Implementing Least Privilege Access in Windows Server Environments*. https://wafaicloud.com/blog/implementing-least-privilege-access-in-windows-server-environments/

Zhao, L., Chen, X., & Wu, Y. (2018). A systematic methodology for penetration testing of enterprise networks. *Computers & Security*, *77*, 752-767.

Anexos

Resultado Prueba Antiplagio



Enlace Video de Sustentación

https://youtu.be/3ZczNNsGL6Y