Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

José David Buelvas Cuello

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Dedico este trabajo, con profunda gratitud y cariño, a mi familia, quienes han sido el fundamento y la fortaleza en cada paso de este camino académico. A mi esposa, compañera incondicional, cuyo amor, comprensión y apoyo constante me impulsaron a perseverar incluso en los momentos más exigentes. Su paciencia, dedicación y confianza en mis capacidades han sido una fuente invaluable de motivación.

A mis hijos, que con su alegría, palabras sinceras y abrazo oportuno me recordaron siempre el propósito de seguir creciendo personal y profesionalmente. Ellos son la inspiración diaria que me impulsa a ser un mejor ejemplo y a demostrarles que la constancia, el esfuerzo y la disciplina permiten alcanzar cualquier meta.

A mi familia en general, por su respaldo, por creer en mí y por acompañarme en este proceso con palabras de aliento y gestos que, aunque pequeños, significaron mucho. Cada logro alcanzado en este trabajo también les pertenece, pues han sido un pilar fundamental en mi formación y crecimiento.

Agradecimientos

Agradezco profundamente a la Universidad Nacional Abierta y a Distancia (UNAD) por brindarme la oportunidad de formarme académica y profesionalmente en un entorno que promueve la autonomía, la disciplina y el aprendizaje significativo. Su compromiso con la educación de calidad ha sido fundamental en el desarrollo de las competencias que hoy aplico con convicción y responsabilidad.

Extiendo mi sincero agradecimiento a los tutores y al director de curso, quienes, con su orientación, dedicación y acompañamiento constante, contribuyeron de manera decisiva al fortalecimiento de mis conocimientos. Sus aportes académicos, retroalimentaciones oportunas y disposición para resolver inquietudes fueron esenciales para avanzar con claridad en cada una de las etapas del proceso formativo.

A mis compañeros de estudio, quienes con su colaboración, participación activa y espíritu de trabajo en equipo enriquecieron significativamente las discusiones y actividades académicas. Cada intercambio de ideas, cada aporte y cada experiencia compartida reforzaron la construcción colectiva del conocimiento y alimentaron un ambiente de respeto y aprendizaje mutuo.

Resumen

El presente documento analiza de manera integral las cuatro etapas del ejercicio académico de ciberseguridad centrado en la interacción operativa entre los equipos Red Team y Blue Team, con el propósito de comprender los procesos de ataque, defensa, detección y contención dentro de un entorno controlado. En las primeras fases se examinan las acciones ofensivas del Red Team, evidenciando la explotación de vulnerabilidades críticas como Rejetto HFS (CVE-2014-6287) y EternalBlue (MS17-010), así como los vectores y técnicas empleados para comprometer sistemas Windows. Posteriormente, el enfoque se traslada al Blue Team, donde se detallan las acciones iniciales ante un incidente en tiempo real, incluyendo la identificación del origen del ataque, la preservación de evidencia, la revisión de conexiones activas, la validación de procesos y la contención mediante aislamiento de equipos comprometidos. Asimismo, se plantea un conjunto de medidas de hardening basadas en estándares internacionales como CIS Benchmarks y guías CCN-STIC, orientadas a reducir la superficie de ataque y evitar la repetición de intrusiones. El estudio también profundiza en las diferencias funcionales entre Blue Team y CSIRT, resaltando sus roles complementarios dentro del ciclo de respuesta. Además, se incluyen análisis sobre el uso del CIS en la defensa organizacional, las capacidades de un SIEM para la correlación de eventos y tres herramientas críticas de contención. En conjunto, este trabajo ofrece una visión completa del ciclo ofensivo–defensivo, destacando la importancia de la prevención, la respuesta estructurada y la mejora continua en la seguridad de la información.

***Palabras clave*:** ciberseguridad, defensa, hardening, incidentes, ofensiva.

Abstract

The present document provides a comprehensive analysis of the four stages of the academic cybersecurity exercise focused on the operational interaction between Red Team and Blue Team, with the purpose of understanding attack, defense, detection, and containment processes within a controlled environment. The initial phases examine the offensive actions of the Red Team, highlighting the exploitation of critical vulnerabilities such as Rejetto HFS (CVE-2014-6287) and EternalBlue (MS17-010), as well as the vectors and techniques used to compromise Windows systems. Subsequently, the focus shifts to the Blue Team, detailing the initial actions taken during a real-time incident, including the identification of the attack source, preservation of digital evidence, review of active connections, validation of system processes, and containment through host isolation. Additionally, a set of hardening measures is proposed based on international standards such as CIS Benchmarks and CCN-STIC guidelines, aimed at reducing the attack surface and preventing repeated intrusions. The study also explores the functional differences between the Blue Team and the CSIRT, emphasizing their complementary roles within the response cycle. Furthermore, the analysis includes the use of CIS for organizational defense, the capabilities of a SIEM for event correlation, and three critical containment tools. Overall, this work offers a complete view of the offensive–defensive cycle, highlighting the importance of prevention, structured response, and continuous improvement in information security.

Keywords**:** cybersecurity, defense, hardening, incidents, offense.

Tabla de Contenido

Resumen....4

Glosario....14

Introducción....17

Justificación....19

Objetivos....21

Objetivo General....21

Objetivos Específicos....21

Desarrollo de la Actividad....22

Etapa 1: Fundamentos de Operaciones Red Team y Blue Team....22

Anexo 1– Escenario 1: Situación problema: Montaje Banco de trabajo....22

Análisis Delitos informáticos y protección de datos personales en Colombia....23

Etapas del pentesting....25

Definición de las herramientas de Ciberseguridad....26

Herramientas....26

Servicios en línea....27

Configuración Banco de Trabajo....28

Figuras....28

Etapa 2: Ética Profesional y Marco Normativo en Operaciones de Seguridad....36

Anexo 2– Escenario 2: Situación problema: SecureNova Labs....36

Análisis Anexo 3 – Acuerdo....37

1)Procesos ilegales y no Éticos evidenciados en el Acuerdo de la empresa SecureNova Labs....37

2)Artículos de la Ley 1273 de 2009 vulnerados....40

3)Decisión profesional frente a la oferta laboral 41

4)Acceso a información sensible en auditorías 42

5) Mecanismos de supervisión para evitar abusos en análisis forense 42

6) Respuesta ante actos de ciberespionaje cometidos por proveedores 44

Etapa 3: Componente práctico - Prácticas simuladas 46

Ejercicio 1 47

Fase 1 – Reconocimiento y Escaneo 49

Fase 2 – Identificación y validación de vulnerabilidades. 52

Fase 3 – Explotación 53

Ejercicio 2 59

Fase 1 – Reconocimiento y Escaneo 62

Fase 2 –Validación de vulnerabilidades 66

Fase 3 – Explotación 68

1)Herramientas y Comandos Utilizados – Escenario Red Team 77

2)Datos del Anexo 4 – Escenario 3 que ayudaron a identificar el fallo de seguridad 79

3)Herramienta utilizada para detectar falla de seguridad. 79

4)¿Cómo afecta el ataque a las máquinas Windows encontradas en la red? 81

Etapa 4 Respuesta y Contención ante Incidentes de Seguridad 82

1)Acciones iniciales ante un ataque en tiempo real (Equipo Blue Team) 82

2)¿Qué medidas de hardenización propondría para que el ataque no se repita? 84

3)¿Cuáles son las diferencias entre un equipo Blue Team y un equipo de Respuesta a Incidentes? 85

4)¿Para qué utilizaría CIS (Center for Internet Security) dentro de un equipo Blue Team? 86

5)Funciones y características principales de un SIEM 87

6)¿Herramientas de contención de ataques informáticos (hardware o software) 88

Etapa 5: Análisis, Reporte y Comunicación de Resultados Técnicos 90

Evidencias de Sustentación 90

Conclusiones 91

Recomendaciones 93

Referencias Bibliográficas 96

Apéndices 102

Lista de Figuras

Figura 1 *Descarga VirtualBox* 28

Figura 2 *Instalación VirtualBox* 29

Figura 3 *VirtualBox instalado en el escritorio* 30

Figura 4 *Archivos Banco de Trabajo* 31

Figura 5 *Validación componentes equipo host* 32

Figura 6 *Validación creación máquinas virtuales Windows 7 & Parrot* 33

Figura 7 *Verificación IP equipo Host* 33

Figura 8 *IP máquina virtual Windows 7* 34

Figura 9 *IP máquina virtual Parrot* 35

Figura 10 *IP Evidencia comunicación maquinas banco de trabajo* 35

Figura 11 *IP Instalación banco de trabajo maquinas Windows 7 & Kali Linux* 46

Figura 12 *Configuración IP Ejercicio 1 Windows 7* 47

Figura 13 *Configuración IP Ejercicio 1 Kali Linux* 47

Figura 14 *Verificación comunicación maquina Windows VS Maquina de Kali Linux* 48

Figura 15 *Verificación comunicación maquina Kali Linux Vs Maquina Windows 7* 48

Figura 16 *Desactivación Firewall maquina Windows 7* 48

Figura 17 *Comando 1 Actualización del entorno de Kali Linux con el comando apt update* 49

Figura 18 *Comando 2 Actualización del entorno de Kali Linux con el comando apt full-upgrade -y* 50

Figura 19 *Comando 3 nmap -sS -sV -T4 -p- Escaneo de Puertos TCP y detección de servicios* 50

Figura 20 *Comando 4 – nmap -O 10.10.11.112 Detección Sistema Operativo* 51

Figura 21 *Comando 5 – Escaneo con scripts por defecto y verificación de seguridad* 51

Figura 22 *Comando 6 – Escaneo de vulnerabilidades con scripts NSE* 52

Figura 23 *Inicio de Metasploit* 53

Figura 24 *Búsqueda del módulo EternalBlue* 54

Figura 25 *Selección y configuración del módulo comando show options* 55

Figura 26 *Configuración de RHOSTS y LHOST* 55

Figura 27 *Ejecución exitosa del exploit* 56

Figura 28 *Verificación de sistema y privilegios* 56

Figura 29 *Acceso a la shell del sistema* 57

Figura 30 *Creación de usuario persistente paso 1* 57

Figura 31 *Creación de usuario persistente paso 2* 57

Figura 32 *Creación de usuario en la Interfax de Windows* 58

Figura 33 *Verificación usuario en maquina Windows 7* 58

Figura 34 *Instalación aplicación Rejetto* 59

Figura 35 *Configuración IP Máquina Windows 7* 60

Figura 36 *Configuración IP Maquina Kali Linux* 60

Figura 37 *Verificación Ping entre máquinas* 61

Figura 38 *Inicio servidor HFS- HTTP.* 61

Figura 39 *Escaneo rápido con el comando nmap -sS -sV -T4 -p-* 62

Figura 40 *Detección de sistema operativo comando nmap -O* 62

Figura 41 *Escaneo completo comando nmap -sS -sV -sC -O -T4 -p- 192.168.200.7* 63

Figura 42 *Escaneo exhaustivo de vulnerabilidades comando nmap -sS -sV -p- --script "vuln" -T4 192.168.200.7* 64

Figura 43 *Resultado del escaneo Nessus* 66

Figura 44 *Inicio consola Metasploit* 68

Figura 45 *Ejecución comando msf > search apache_range_dos* 69

Figura 46 *Ejecución comando use 0 y show options* 69

Figura 47 *Ejecución ataque de Denegación de Servicio (DoS)* 70

Figura 48 *Interfaz gráfica del software HFS – HTTP File Server 2.3 (Build 288)* 71

Figura 49 *Inicio herramientas Metasploit.* 72

Figura 50 *Ejecución comando search hfs* 72

Figura 51 *Ejecución show options* 73

Figura 52 *Configuración ataque creación usuario* 73

Figura 53 *Ejecución comando sysinfo verificación usuario* 74

Figura 54 *Creación de usuario JoseBuelvasC con privilegios* 75

Figura 55 *Creación de usuario JoseBuelvasC maquina Windows 7* 75

Figura 56 *Eliminación de usuario JoseBuelvasC maquina Windows 7* 76

Figura 57 Eliminación de usuario JoseBuelvasC interfaz maquina Windows 7 76

Figura 58 *Diagrama del Ataque* 81

Lista de Tablas

Tabla 1 *Etapas del Pentesting* 25

Tabla 2 *Principales hallazgos del Escaneo Nmap* 65

Tabla 3 *Vulnerabilidades encontradas Nessus* 67

Lista de Apéndices

Apéndice A..... 102

Glosario

Aislamiento de red:

Estrategia de protección que implica desactivar o restringir la conexión de un dispositivo afectado para prevenir la expansión de un ataque o el robo de datos.

Análisis forense digital:

Método especializado que facilita la recolección, conservación y análisis de pruebas digitales para establecer cómo se desarrolló un evento de seguridad y cuáles fueron sus consecuencias.

Blue Team:

Grupo responsable de proteger de manera activa y pasiva la infraestructura tecnológica, encargado de identificar, analizar, responder y controlar los incidentes de seguridad.

Ciberataque:

Acción deliberada llevada a cabo por una persona con malas intenciones para influir en la disponibilidad, integridad o privacidad de un sistema o recurso tecnológico.

Ciberseguridad:

Campo que tiene como objetivo salvaguardar infraestructuras, conexiones e información ante agresiones, destrucción o entradas no permitidas a través de medidas, normativas y herramientas específicas.

CIS (Center for Internet Security):

Entidad que crea normativas, directrices y regulaciones para reforzar la configuración de sistemas y optimizar la seguridad de las organizaciones (CIS Security, 2020).

Contención:

Fase de la respuesta ante incidentes centrada en frenar o restringir el progreso de un ataque a través de medidas como el aislamiento de redes, la interrupción de procesos o la limitación de accesos.

CSIRT (Computer Security Incident Response Team):

Grupo de expertos responsable de administrar, examinar y reaccionar ante eventos de seguridad en una entidad, utilizando métodos organizados de indagación y reducción de riesgos.

EDR (Endpoint Detection and Response):

Herramienta de protección que observa, identifica y facilita la reacción ante riesgos en dispositivos finales, con características como separación, detención de procesos y evaluación del comportamiento.

Exploit:

Método o código empleado para explotar una debilidad y llevar a cabo actividades no permitidas en un sistema o servicio.

Hardening:

Método para proteger un sistema a través de la remoción de configuraciones vulnerables, desactivación de servicios que no son necesarios, implementación de actualizaciones y mejora de aspectos de seguridad.

Incidente de seguridad:

Suceso que influye o puede influir de manera desfavorable en la disponibilidad, integridad o privacidad de la información o de los sistemas tecnológicos.

Movimiento lateral (Lateral Movement):

Estrategia utilizada por un agresor para moverse dentro de la red interna una vez que ha tomado el control de un primer equipo, con el objetivo de acceder a otros sistemas o información.

Persistencia:

Grupo de métodos que emplea un agresor para asegurar que tiene acceso permanente a un sistema que ha sido vulnerado, incluso tras reinicios o esfuerzos de restauración.

Red Team:

Grupo responsable de implementar simulaciones de ataques auténticos de forma controlada para analizar la situación de seguridad de una entidad y identificar debilidades susceptibles de ser aprovechadas.

SIEM (Security Information and Event Management):

Sistema que reúne, ajusta y relaciona eventos de seguridad de diversas fuentes con el fin de identificar conductas inusuales y facilitar la reacción ante incidentes (Moreno, 2015).

SMB (Server Message Block):

Protocolo de comunicación en la red que se emplea para el intercambio de archivos y el uso de impresoras en entornos Windows, el cual puede ser aprovechado si se usa versiones que presentan fallas como SMBv1.

Vulnerabilidad:

Vulnerabilidad en un sistema, programa o ajuste que puede ser utilizada por un agresor para afectar su rendimiento o protección.

Introducción

En la actualidad, la seguridad informática se ha vuelto un componente crucial para asegurar los sistemas de información, dado el aumento de las amenazas en línea, la mayor complejidad de los ataques cibernéticos y la dependencia tecnológica de las empresas y organizaciones. Esta situación requiere un fortalecimiento constante de la infraestructura tecnológica, así como la capacitación de profesionales que sepan entender y enfrentar las dinámicas tanto ofensivas como defensivas presentes en el ámbito digital. Dentro de este marco, las metodologías de Red Team y Blue Team constituyen un enfoque integral para evaluar la seguridad, detectar vulnerabilidades reales y aplicar medidas efectivas de protección, contención y recuperación.

El objetivo de este documento es llevar a cabo un análisis minucioso de las cuatro fases del ejercicio académico enfocado en el estudio práctico del ciclo de ciberseguridad tanto ofensiva como defensiva. En las etapas iniciales, se estudia el trabajo del Red Team, con un énfasis en el reconocimiento, la explotación de las vulnerabilidades y la obtención de acceso utilizando técnicas de intrusión reales. A continuación, el análisis se dirige hacia el Blue Team, que se encarga de identificar, responder y reducir los incidentes de seguridad, además de fortalecer el sistema mediante medidas de hardening basadas en estándares internacionales como los CIS Benchmarks y las guías CCN-STIC. Este enfoque permite entender no solo la ejecución de los ataques, sino también la manera de gestionarlos, detenerlos y prevenirlos desde una perspectiva organizacional.

Además, se añaden aspectos esenciales como la función del CSIRT, el empleo de herramientas especializadas para la correlación de eventos (SIEM), la relevancia de la contención en tiempo real y la implementación de mecanismos técnicos que busquen mejorar la resistencia del sistema. A lo largo del texto, se explican los conceptos básicos que respaldan esta

metodología de investigación y se lleva a cabo un análisis crítico sobre la importancia de emplear enfoques tanto proactivos como reactivos para proteger los activos informáticos. Finalmente, se presentan conclusiones fundamentadas en los resultados obtenidos, con el objetivo de reforzar el aprendizaje académico y fomentar la adopción de buenas prácticas en ciberseguridad.

Justificación

El análisis de las metodologías Red Team y Blue Team es crucial en la actualidad, ya que el aumento de ciberincidentes y la complejidad de las amenazas digitales exigen respuestas cada vez más robustas, organizadas y alineadas con buenas prácticas a nivel internacional. La creciente dependencia de la tecnología por parte de entidades tanto públicas como privadas hace indispensable entender a fondo cómo surgen los ataques, qué vulnerabilidades pueden ser aprovechadas y cuáles son las estrategias más efectivas para prevenir, identificar y reducir efectos negativos. Por esta razón, tratar este asunto desde un enfoque operativo y analítico ayuda a mejorar las habilidades técnicas de los profesionales en formación, al mismo tiempo que fomenta una perspectiva crítica sobre la seguridad en situaciones reales.

La ejecución del ejercicio académico que incluye las cuatro fases del proceso ofensivo y defensivo se justifica por su contribución al aprendizaje práctico, haciéndole posible al estudiante no solo detectar errores en la infraestructura tecnológica, sino también vivir todo el proceso de ataque, respuesta y recuperación. Esta actividad supervisada ofrece una comprensión completa del comportamiento de un agresor y, al mismo tiempo, de las acciones que debe realizar un defensor para enfrentar un evento de seguridad en tiempo real. También posibilita vincular el conocimiento teórico con la aplicación técnica de herramientas, regulaciones, marcos de referencia y métodos de análisis forense.

Asimismo, es fundamental mejorar la capacitación en ciberseguridad a través de simulaciones que reflejen escenarios reales, ya que muchas organizaciones no cuentan con prácticas locales que combinen enfoques tanto ofensivos como defensivos. Este estudio ayuda a reducir esa diferencia al examinar vulnerabilidades, métodos de explotación, sistemas de detección, contención y endurecimiento, basándose en normas como los CIS Benchmarks, las guías CCN-STIC y los enfoques de respuesta a incidentes. Analizar esto no solo ayuda a

entender los peligros actuales, sino que también ofrece elementos esenciales para crear estrategias de defensa más efectivas.

Finalmente, este estudio tiene razón de ser por su influencia tanto en el ámbito académico como en el profesional, dado que los saberes obtenidos pueden constituir un fundamento para investigaciones venideras, mejoras en normativas de seguridad, aumento de las habilidades institucionales y la creación de perfiles especializados en la administración de incidentes. Mediante este enfoque holístico, se pretende ofrecer herramientas tanto teóricas como prácticas que faciliten una respuesta adecuada a las amenazas actuales y ayuden en la creación de entornos tecnológicos más seguros y resistentes.

Objetivos

Objetivo General

Analizar el impacto de las metodologías Red Team y Blue Team en la evaluación, detección y mitigación de vulnerabilidades dentro de un entorno de laboratorio, con el fin de comprender sus principales causas, efectos y posibles estrategias de mejora en la seguridad de la información.

Objetivos Específicos

Identificar los factores que permiten el desarrollo de vulnerabilidades explotables en sistemas Windows dentro del entorno de laboratorio, mediante la recopilación y el análisis tanto teórico como práctico del ciclo ofensivo del Red Team.

Analizar los elementos que intervienen en la detección, respuesta y contención de incidentes gestionados por el Blue Team, a partir de la evaluación de conexiones, procesos, registros del sistema y mecanismos de preservación de evidencia.

Examinar las medidas de hardening aplicables al entorno analizado, tomando como referencia estándares internacionales como CIS Benchmarks y lineamientos CCN-STIC, con el fin de reducir la superficie de ataque y prevenir la repetición de intrusiones.

Evaluar la utilidad de herramientas de monitoreo, correlación y contención, tales como SIEM, firewalls y EDR, para comprender su aporte en la mejora continua de la postura de seguridad organizacional.

Desarrollo de la Actividad

Etapa 1: Fundamentos de Operaciones Red Team y Blue Team

La ciberseguridad moderna demanda un enfoque estratégico que combine capacidades ofensivas para fortalecer la protección de la infraestructura tecnológica de las organizaciones. En este contexto, los equipos Red Team y Blue Team desempeñan un papel esencial, ya que permiten evaluar la efectividad de los controles, identificar vulnerabilidades y diseñar estrategias de defensa basadas en la evidencia técnica.

De acuerdo con Arroyo (2025), la sinergia entre ambos equipos se ha convertido en un componente crítico para garantizar la resiliencia corporativa frente a amenazas avanzadas. Este informe analiza de manera técnica y argumentada los fundamentos operativos de estas unidades, integrando elementos legales, metodológicos y tecnológicos que sustentan su quehacer profesional. Asimismo, se presenta la configuración de un banco de trabajo virtual que permite aplicar técnicas estudiadas en entorno controlado.

Anexo 1– Escenario 1: Situación problema: Montaje Banco de trabajo

El escenario planteado por SecureNova Labs, requiere la configuración de un entorno basado software de código abierto, empleando máquinas virtuales Windows y Parrot montadas en VirtualBox, este laboratorio permitirá realizar actividades de alto nivel técnico, garantizando aislamiento, control y seguridad. El proceso incluye validar la comunicación entre maquinas. que las políticas públicas y las instituciones académicas trabajen conjuntamente para garantizar una inclusión real, promoviendo tanto la infraestructura como la capacitación adecuada.

Análisis Delitos informáticos y protección de datos personales en Colombia.

En Colombia, la salvaguarda de la información personal y los datos se ha vuelto muy relevante por el notable progreso tecnológico y el incremento de los crímenes digitales. La nación cuenta con un conjunto de legislaciones y regulaciones que rigen el tratamiento correcto de la información, junto con las penalizaciones para aquellos que cometan infracciones vinculadas a la ciberseguridad.

- Ley 1273 de 2009 – Delitos informáticos: Esta ley modificó el código penal de Colombia para proteger la información y los datos almacenados en los sistemas informáticos. Esta norma se encarga de tipificar conductas como el acceso no autorizado, la intervención o captación de datos, los daños a sistemas, el uso de software malicioso y los fraudes informáticos. Su finalidad es salvaguardar la confidencialidad, integridad y disponibilidad de la información digital, estableciendo sanciones penales para quienes vulneren estos principios (Congreso de la República de Colombia 2009).

- Ley 1581 de 2012 – Protección de datos personales: En esta ley se establece el marco general para el tratamiento de datos personales en Colombia definiendo principios como legalidad, libertad, finalidad, veracidad, transparencia, seguridad y confidencialidad, que deben cumplir todas las entidades públicas y privadas que manejen información personal. Además, garantiza a los titulares derechos como conocer, actualizar, corregir o eliminar sus datos, y asigna a la Superintendencia de Industria y Comercio la autoridad para supervisar y asegurar el cumplimiento de la normativa (Congreso de la República de Colombia 2012).

- Decreto 1377 de 2013 – Reglamentación de la Ley 1581: Este decreto se encarga de reglamentar la Ley 1581 de 2012 y proporciona lineamientos para su aplicación, especialmente en lo referente a la obtención de autorizaciones para el tratamiento de datos personales recolectados antes de la entrada en vigencia de la ley. Su propósito es facilitar la

correcta implementación del régimen de protección de datos en organizaciones públicas y privadas (Congreso de la República de Colombia 2012).

- Ley 1266 de 2008 – Habeas data financiero y crediticio: Esta ley es conocida como la Ley de Habeas Data financiero y crediticio, regula el manejo de datos personales en bases de datos financieras, crediticias, comerciales y de servicios. Esta norma garantiza a los titulares el derecho a acceder, actualizar y corregir su información, y establece obligaciones para las entidades que administran o consultan datos en centrales de riesgo. Su propósito es equilibrar la protección de la privacidad con la necesidad de contar con información precisa para las actividades económicas y financieras (Congreso de la república de Colombia 2008).
- Ley 1712 de 2014 – Transparencia y acceso a la información pública: En esta ley se establece el marco para garantizar la transparencia y el acceso de los ciudadanos a la información pública en Colombia. Aunque promueve la divulgación de datos gubernamentales, también define límites para proteger la información personal y confidencial, asegurando que las entidades públicas gestionen adecuadamente los datos sensibles y respeten la privacidad de los individuos (Congreso de la república de Colombia 2014).
- Ley 1621 de 2013 – Actividades de inteligencia y contrainteligencia: Esta ley se encarga de regular las actividades de inteligencia y contrainteligencia del Estado colombiano, estableciendo que estas deben desarrollarse bajo el respeto a los derechos fundamentales, especialmente la privacidad y la protección de los datos personales. La norma introduce principios como necesidad, proporcionalidad y confidencialidad, y fija controles estrictos para la recolección, manejo y conservación de la información obtenida en estas operaciones (Congreso de la república de Colombia 2013).

- Decreto 255 de 2022 – Normas corporativas vinculantes y buenas prácticas: Este decreto moderniza el régimen de protección de datos personales en el ámbito empresarial al regular las Normas Corporativas Vinculantes (NCV), las cuales permiten la transferencia internacional de datos dentro de grupos empresariales bajo estándares comunes de seguridad y privacidad. Asimismo, promueve la adopción de certificaciones y buenas prácticas para fortalecer la gestión de la privacidad y aumentar la confianza de los usuarios en el tratamiento de su información (Ministerio de Comercio, Industria y Turismo [MinCIT], 2022).

Etapas del pentesting

Las etapas del pentesting conforman un proceso estructurado que permite evaluar la seguridad de sistemas, redes y aplicaciones mediante la simulación controlada de ataques reales. Este enfoque facilita identificar y explotar vulnerabilidades antes de que puedan ser utilizadas por actores maliciosos. Cada fase del proceso incluye actividades específicas y herramientas técnicas que apoyan la identificación de riesgos y el fortalecimiento de las defensas (SANS Institute, 2021; OWASP Foundation, 2023; Zhang, Xing & Li, 2025).

Tabla 1

Etapas del Pentesting

Etapa	Descripción	Herramienta
Planificación y alcance	Definir objetivos, alcance, sistemas.	Documentación
Reconocimiento	Recolección pasiva de información.	Maltego
Escaneo y Enumeración	Identificación puertos abiertos y servicios	Nmap, Nessus
Análisis de Vulnerabilidades	Evaluación y priorización vulnerabilidades	OpenVAS
Explotación	Aprovechamiento de vulnerabilidades	Metasploit.
Post-explotacíon	Escalada Privilegios	PowerShell scripts

Reporte y Remediación	Documentar hallazgos	Dradis.

Fuente. Autoría Propia

La tabla anterior se muestra de manera clara y secuencial las etapas fundamentales del pentesting, iniciando con la Planificación y Alcance, donde se definen los objetivos, el entorno a evaluar y los acuerdos éticos y legales; seguida del Reconocimiento, fase en la que se recolecta información pública del objetivo mediante técnicas OSINT. Posteriormente, en Escaneo y Enumeración, se identifican puertos, servicios y posibles vectores de ataque. La etapa de Análisis de Vulnerabilidades permite detectar fallos y priorizar riesgos, lo que conduce a la Explotación, donde se validan de forma controlada las debilidades identificadas. Luego, en la fase de Post-explotación, se analiza el impacto del acceso obtenido y las posibilidades de movimiento lateral. Finalmente, la etapa de Reporte y Remediación documenta los hallazgos y presenta recomendaciones para corregir las vulnerabilidades, cerrando así el proceso metodológico del pentesting.

Definición de las herramientas de Ciberseguridad.

Herramientas

- Metasploit: es una herramienta de código abierto utilizada ampliamente en ciberseguridad para realizar pruebas de penetración, ya que permite diseñar, evaluar y ejecutar exploits con el objetivo de identificar vulnerabilidades en sistemas y aplicaciones. Su arquitectura modular incorpora componentes para el escaneo, la explotación y la post-explotación, lo cual facilita la simulación de ataques controlados y la evaluación de la seguridad de un entorno tecnológico (Universidad Carlos III de Madrid, 2025).

- Nmap: una herramienta de código abierto utilizada para escanear redes y detectar dispositivos activos, puertos abiertos y servicios en ejecución, permitiendo construir un mapa detallado de la superficie de ataque durante la fase de reconocimiento en pruebas de penetración. Además, su capacidad para identificar versiones de software asociadas a los servicios facilita la detección de vulnerabilidades potenciales (Universidad Estatal Península de Santa Elena, 2025).
- OpenVas: Es un escáner automatizado que facilita la detección de fallos de seguridad en sistemas y aplicaciones mediante el análisis de configuraciones, puertos y servicios. Es un instrumento perfecto para llevar a cabo análisis detallados de diferentes activos y presentar vulnerabilidades conocidas, lo que permite identificar cuáles deben ser atendidas primero (Greenbone, 2025; Greenbone Community, 2025).

Servicios en línea

- Es un repositorio público que se renueva de manera continua e incluye vulnerabilidades públicas, exploits y herramientas relacionadas. Usualmente se emplean para hallar pruebas de concepto o códigos concretos que aprovechan vulnerabilidades reconocidas. Esto posibilita que los pentesters examinen y reproduzcan ataques auténticos con el objetivo de conducir pruebas y adquirir conocimientos (Wikipedia, 2025).
- CVE: Es un sistema estándar para nombrar y clasificar vulnerabilidades conocidas, en el que cada una de ellas tiene un identificador único (por ejemplo, CVE-2020-1234) que incluye únicamente la naturaleza del error y las referencias. Esta nomenclatura permite a los expertos comunicarse con las herramientas y acceder a información precisa sobre actualizaciones o riesgos (Fortinet, 2024).

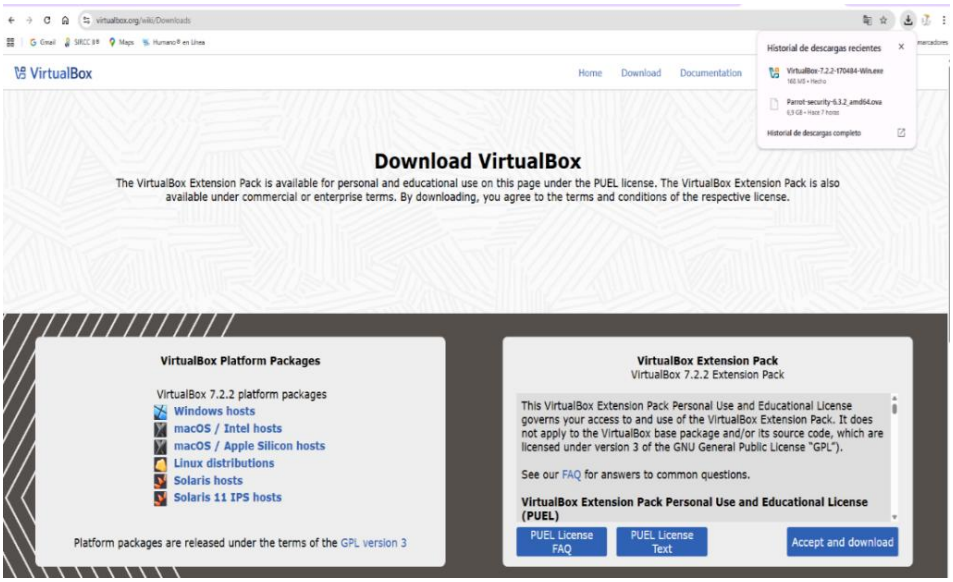
Configuración Banco de Trabajo

- Paso 1: Se realiza la descarga e Instalación de VirtualBox: Este paso consiste en obtener e instalar VirtualBox, la cual será la plataforma donde se ejecutarán las máquinas virtuales, esta descarga se realizará desde la página oficial, se descargará el instalador y se realizaran una serie de pasos guiados en los que se acepta la licencia, se seleccionan componentes por defecto y finalmente se completa la instalación.

Figuras

Figura 1

Descarga VirtualBox

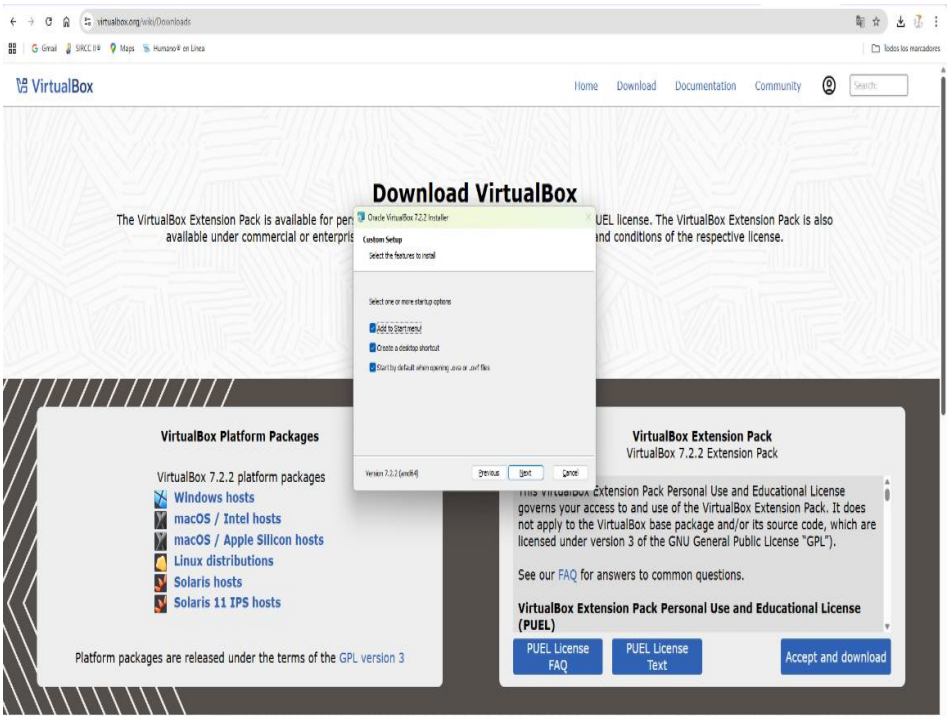


Fuente. Autoría Propia

En la imagen anterior se puede visualizar el proceso de descarga de la herramienta VirtualBox desde la página y luego continuar con el proceso de instalación oficial, este paso es crucial ya que esta nos proporciona los recursos necesarios para simular múltiples sistemas operativos de manera simultánea, permitiendo la interacción entre ellos como si se tratara de un entorno real de red corporativa.

Figura 2

Instalación VirtualBox



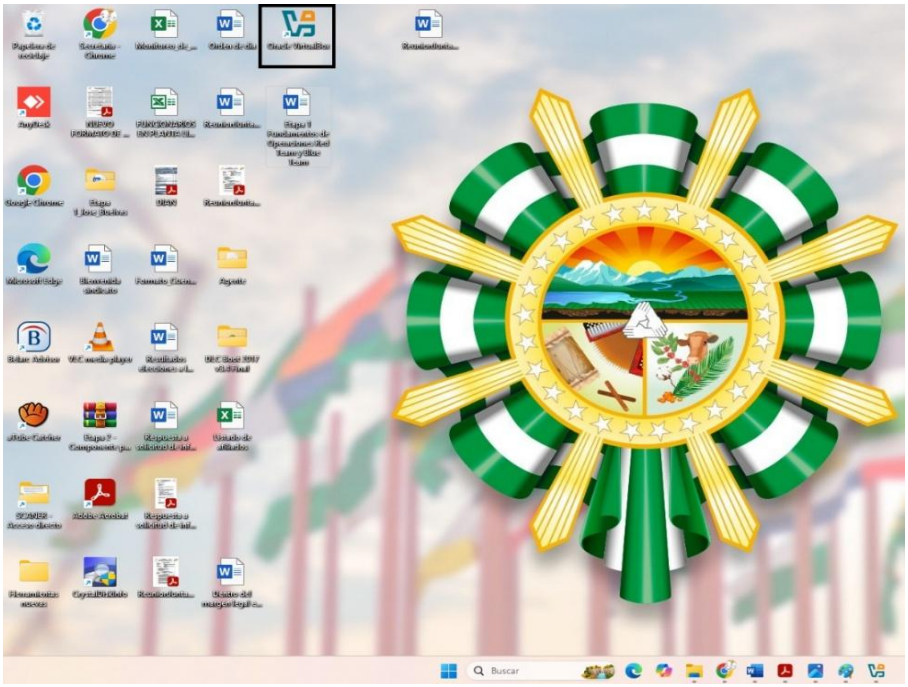
Fuente. Autoría Propia

Una vez se realice el proceso de descarga se dará doble clic en el instalador y se procede a realizar una serie de pasos sugeridos por el asistente del instalador. Primero, se muestra una ventana inicial donde se debe hacer clic en “Next” para comenzar la configuración. Luego, el instalador presenta los términos y condiciones, los cuales deben aceptarse para continuar. Posteriormente, aparece una nueva ventana donde nuevamente se selecciona “Next”, confirmando las opciones predeterminadas de instalación. En la siguiente etapa, el sistema solicita autorización mediante un mensaje emergente, por lo que se debe hacer clic en “Yes” para permitir que el instalador continúe. El asistente muestra una pantalla con los componentes predeterminados, los cuales se dejan tal como aparecen y se avanza con “Next”. A continuación, se utiliza la opción “Install” para iniciar el proceso de instalación. El sistema despliega una barra

de progreso donde se puede observar cómo avanza la instalación. Finalmente, al concluir el proceso, se presenta una última pantalla donde se debe hacer clic en “Finish” para completar y cerrar el instalador.

Figura 3

VirtualBox instalado en el escritorio



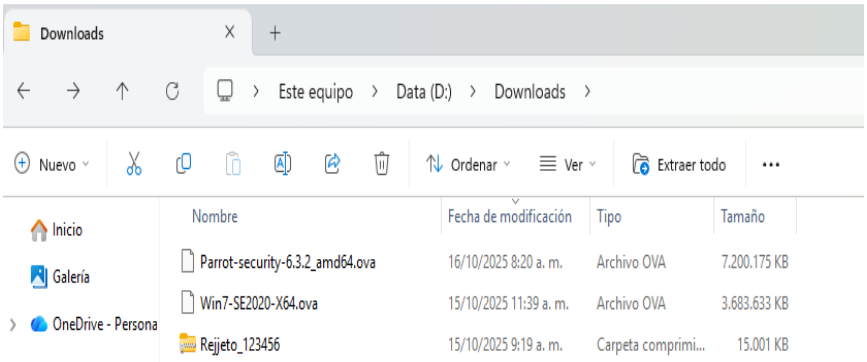
Fuente. Autoría Propia

En la imagen anterior se puede observar la herramienta instalada en el escritorio del equipo host.

- Paso 2: Para llevar a cabo la instalación del banco de trabajo, se procederá a descargar las imágenes proporcionadas en la guía de aprendizaje que se encuentra en el siguiente enlace: RedTeam&BlueTeam2025. Estas incluyen Windows 7 y Parrot, que funcionarán como máquina víctima y máquina atacante, respectivamente.

Figura 4

Archivos Banco de Trabajo



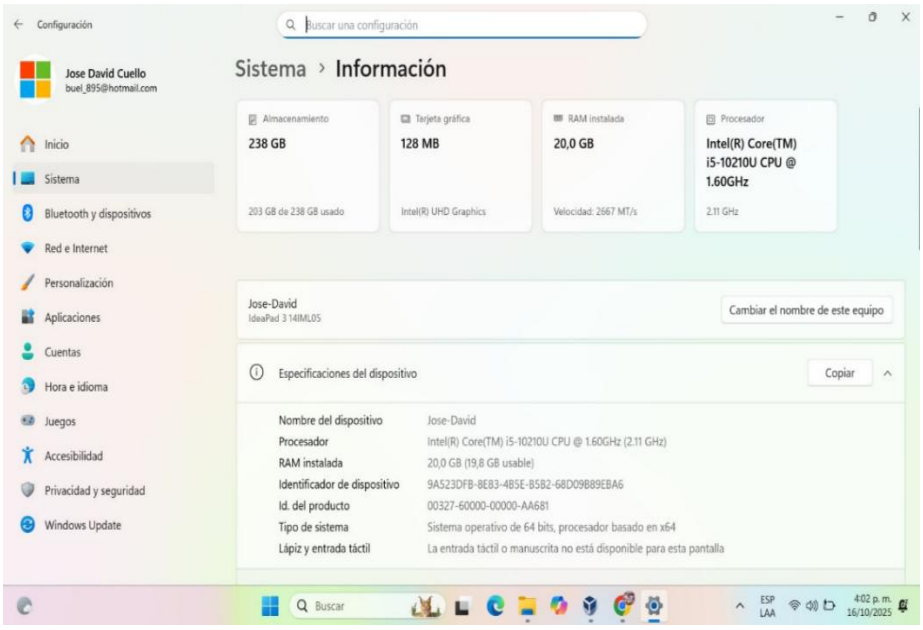
Fuente. Autoría Propia

En la imagen anterior se puede observar la descarga de los archivos proporcionados para la instalación del banco de trabajo.

- Paso 3: La Validación del Hardware del Equipo Host: Antes de montar las máquinas, se valida que el equipo host cuente con los recursos necesarios: suficiente memoria RAM, procesador con virtualización habilitada y espacio en disco. También se verifica el tipo de conexión de red disponible, ya que será necesario configurar la comunicación entre el host y las máquinas virtuales. Este paso previene fallas de rendimiento y garantiza que el banco de trabajo funcione correctamente durante las prácticas de pentesting.

Figura 5

Validación componentes equipo host



Fuente. Autoría Propia

En la imagen anterior se puede observar la validación de los componentes del equipo host

- Paso 4: Montaje y Configuración de las Máquinas Virtuales en VirtualBox se generan o se traen las máquinas virtuales. El procedimiento comienza con la carga de la imagen ISO de Windows 7 y luego la de Parrot. Se arrancan cada una de las máquinas para comprobar que funcionan adecuadamente y se modifica su configuración de red a modo adaptador puente, lo que permite que las máquinas reciban una dirección IP dentro del mismo rango que la computadora anfitriona. Finalmente se verifica la comunicación entre las máquinas mediante ping, lo que confirma que el laboratorio está correctamente configurado para ejecutar pruebas de reconocimiento, explotación y defensa. Este paso es clave porque crea el escenario donde se pondrán en práctica las técnicas Red Team (ataque) y Blue Team (detección y defensa).

Figura 6

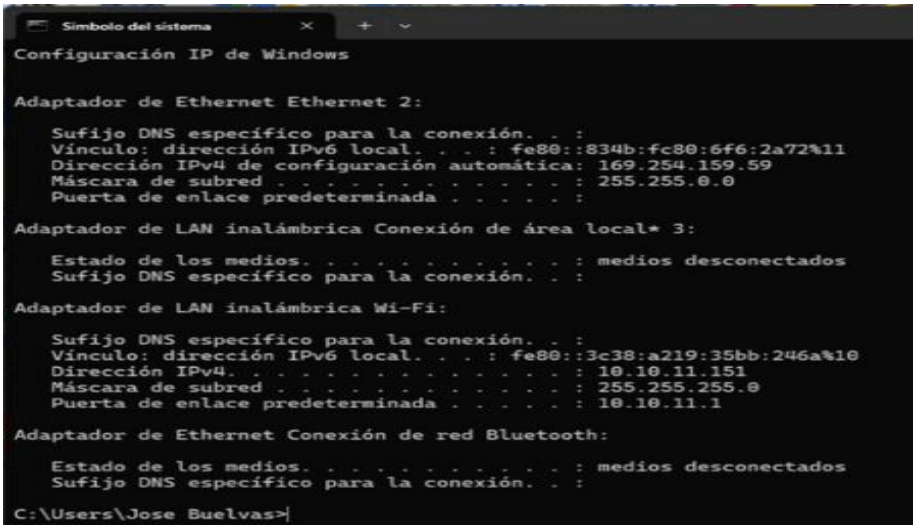
Validación creación máquinas virtuales Windows 7 & Parrot

Fuente. Autoría Propia

En la imagen anterior se puede observar que tanto la maquina la creación de ambas máquinas virtuales.

Figura 7

Verificación IP equipo Host

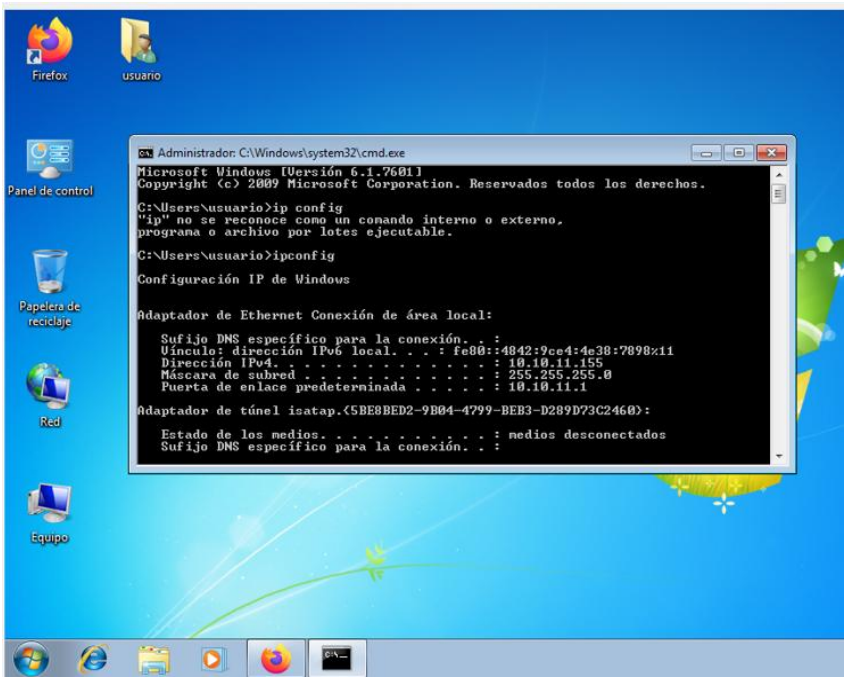


Fuente. Autoría Propia

En la imagen anterior se puede observar se puede observar la dirección IP que se le ha otorgado al equipo host 10. 10. 11. 151, la cual fue otorgada de forma automática.

Figura 8

IP máquina virtual Windows 7

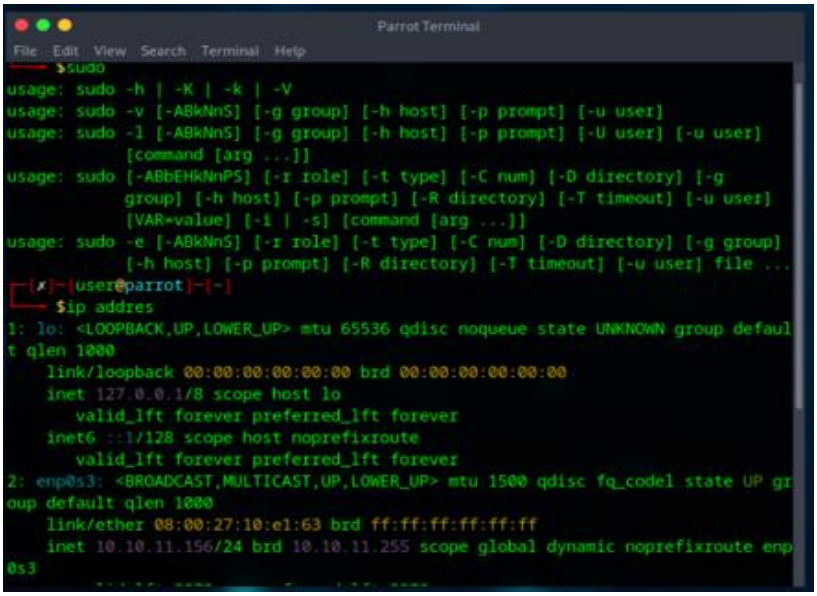


Fuente. Autoría Propia

En la imagen anterior, se puede observar la IP que obtiene automáticamente la máquina virtual de Windows 7, que es 10. 10. 11. 155. Esto nos permite entender que los dispositivos están enlazados en el mismo segmento de red.

Figura 9

IP máquina virtual Parrot

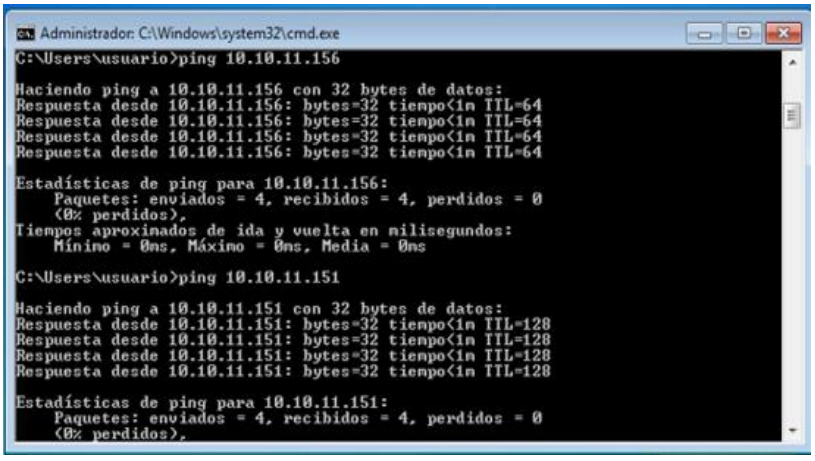


Fuente. Autoría Propia

De la misma manera, llevamos a cabo la comprobación de la dirección IP que asignaron a la computadora con Parrot 10. 10. 11. 156.

Figura 10

IP Evidencia comunicación maquinas banco de trabajo



Fuente. Autoría Propia

Cuando los equipos están conectados al mismo segmento de red, procedemos a hacer ping para comprobar la comunicación entre ellos. En la imagen anterior se puede ver que los equipos tienen comunicación porque hemos verificado que cuando hacemos ping en las IP asignadas a estas máquinas, los paquetes enviados son recibidos.

Etapa 2: Ética Profesional y Marco Normativo en Operaciones de Seguridad

En esta etapa se enfoca en el estudio estructurado de los principios éticos y el marco jurídico aplicable a las operaciones de seguridad informática. En esta fase se busca que se comprenda la responsabilidad legal y moral que recae sobre los equipos Red Team y Blue Team en el desarrollo de actividades de ciberseguridad dentro de una organización. l análisis ético y legal se fundamenta en escenarios prácticos que evidencian riesgos reales asociados a la mala praxis profesional.

Anexo 2– Escenario 2: Situación problema: SecureNova Labs

Se presenta una situación en la que SecureNova Labs, durante un proceso de reclutamiento, proporciona a los candidatos un contrato elaborado por un abogado que fue despedido por problemas en su desempeño, y este no fue verificado por la alta dirección. Este panorama ilustra cómo la falta de supervisión sobre los documentos legales puede dar lugar a cláusulas que son incompatibles con la normativa legal y los valores éticos de la profesión, perjudicando la solidez del proceso y exponiendo a los candidatos a obligaciones inapropiadas. Además, el texto resalta la relevancia funcional de los equipos Red Team y Blue Team, así como el empleo de un laboratorio técnico virtual para la evaluación de habilidades.

Análisis Anexo 3 – Acuerdo

Se evidencia cláusulas problemáticas que contravienen principios éticos y normas legales. Entre los puntos más críticos se encuentran disposiciones que obligan al aspirante a no denunciar actividades ilegales, no reportar sospechas de espionaje y mantener en reserva información ilícita, lo cual vulnera el deber ciudadano de denunciar delitos y contradice la responsabilidad profesional de proteger a la sociedad y actuar con transparencia. Además, el acuerdo exige guardar información ilegal incluso si proviene de actos delictivos, lo cual podría convertir al receptor en cómplice de actividades prohibidas por la ley colombiana. Estas cláusulas demuestran una manipulación indebida del concepto de "información confidencial", ampliándolo más allá de los límites legales aceptables.

1)Procesos ilegales y no Éticos evidenciados en el Acuerdo de la empresa SecureNova Labs

Una vez que se lleva a cabo una revisión minuciosa, se puede observar claramente la presencia de actividades ilegales y moralmente cuestionables en el contenido del contrato ofrecido por la empresa SecureNova Labs. Este documento incluye diversas cláusulas que van en contra de la ley 1273 de 2009, poniendo en riesgo los derechos constitucionales y desconociendo los principios éticos que guían la profesión de ingeniería, tal como lo define el Consejo Profesional Nacional de Ingeniería (COPNIA, 2015).

- Fragmento 1 – Acceso abusivo e interceptación ilegal de datos "*Se considerará confidencial la información referente a datos de chuzadas, interceptación de información y accesos abusivos a sistemas informáticos."* Este texto define como "confidencial" la información procedente de actividades ilícitas, como la escucha de

comunicaciones y el acceso indebido a sistemas informáticos. Estas acciones son catalogadas como delitos según los artículos 269A (acceso indebido) y 269C (intercepción ilegal) de la Ley 1273 de 2009. Al considerar estas acciones como "confidenciales", el acuerdo intenta proteger conductas ilegales, ignorando el principio de legalidad en el ámbito penal y fomentando un marco contractual que va en contra de la ética profesional. (Congreso de la República de Colombia, 2009).

- Fragmento 2 – Prohibición de denunciar delitos *"El receptor se compromete a no denunciar ante las autoridades actividades sospechosas de espionaje o apropiación de información de terceros."* Este fragmento representa un incumplimiento claro del artículo 95 de la Constitución, que establece que todos los ciudadanos deben ayudar a las autoridades y reportar crímenes. También infringe el artículo 441 del Código Penal, que se refiere a no denunciar. Desde una perspectiva ética, el COPNIA requiere que el ingeniero comunique cualquier amenaza a la seguridad pública. Esta disposición intenta establecer un acuerdo de silencio que dificulta la denuncia de actividades ilícitas, comprometiendo la integridad profesional y la responsabilidad moral de evitar daños a otras personas COPNIA (2015, art. 4).

- Fragmento 3 – Silencio frente a información ilegal *"El receptor deberá abstenerse de denunciar y publicar la información confidencial e ilegal que conozca o reciba."* Este fragmento representa una inconsistencia legal, ya que designa como "confidencial" información que es claramente "ilegal". Ningún convenio privado puede impedir la denuncia de un crimen en conformidad con el sistema constitucional y penal colombiano. Esta normativa infringe los principios éticos del COPNIA, que exigen rechazar pactos que impliquen transgresiones a la ley y a los valores morales. Aparte de

promover la ocultación de delitos, pone al receptor en riesgo de enfrentar responsabilidades penales por complicidad o encubrimiento COPNIA (2015, art. 7).

- Fragmento 4 – Transferencia ilegal de responsabilidad penal *"En caso de hallarse información ilegal en manos del receptor, este deberá acudir a un abogado privado y dejar exenta de toda responsabilidad penal a SecureNova Labs."* Esta cláusula tiene como objetivo asignar al empleado la carga penal asociada a acciones ilegales realizadas por la compañía. Esta medida infringe el artículo 29 de la Constitución, que establece que cada persona debe ser responsable de sus actos y prohíbe transferir la responsabilidad penal a otras personas a través de pactos privados. Esta práctica va en contra de los principios de transparencia, justicia y responsabilidad profesional que se mencionan en el Código de Ética del COPNIA. Asimismo, representa un intento consciente de entorpecer la justicia (COPNIA, 2015, art. 3).

- Síntesis de irregularidades éticas y legales: Los fragmentos del Acuerdo demuestran que la compañía busca regularizar prácticas ilícitas como el espionaje, la interceptación de comunicaciones, el acceso indebido a sistemas informáticos y la ocultación de información ilegal. Estas acciones infringen la Ley 1273 de 2009, el Código Penal de Colombia, la Constitución Nacional y el Código de Ética del COPNIA, además de chocar con los principios de legalidad, transparencia y protección de datos que establece el Ministerio TIC (MINTIC).

2)Artículos de la Ley 1273 de 2009 vulnerados.

El acuerdo vulnera varios artículos de la Ley 1273 de 2009, entre ellos:

- Artículo 269A – Acceso abusivo a un sistema informático: Este artículo establece que quien acceda a un sistema informático, ya sea este seguro o no, sin el debido permiso y con la intención de obtener datos o control sobre él (Congreso de la República de Colombia, 2009, art. 269A). el Acuerdo El acuerdo legitima este delito al declarar "confidenciales" acciones que implican accesos no autorizados, lo cual constituye una vulneración abierta del orden jurídico. De esta manera el Acuerdo no solo encubre la violación penal, sino que también intenta resguardar a la compañía y sus trabajadores de las repercusiones legales, vulnerando de esta manera el principio de la legalidad penal el cual se encuentra establecido en el Artículo 6 de la Constitución Política de Colombia.

- Artículo 269C – Interceptación de datos informáticos: Este Artículo establece las sanciones para aquellos que intercepten los datos a las trasmisiones por medios digitales sin una orden judicial o sin el consentimiento del propietario (Congreso de la República de Colombia, 2009, art. 269C). en el Acuerdo se menciona de manera explícita la existencia de "datos relacionados con interceptaciones y espiados", lo que se incluye en la información confidencial. La inclusión de "chuzadas" como información protegida normaliza la interceptación ilegal, atentando contra el derecho fundamental al habeas data, tal como se establece en el Artículo 15 de la Constitución Política de Colombia (1991).

- Artículo 269F – Violación de datos personales: Este Articulo se encarga de sancionar a quien, sin permiso, logre obtener, alterar o revelar información personal que se encuentren en la base de datos o registros (Congreso de la República de Colombia,

2009, art. 269F). El acuerdo obliga a ocultar información obtenida ilícitamente, lo que contraviene directamente la protección de datos personales. Esta cláusula va en contra de los principios de transparencia y de los propósitos legítimos establecidos por Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2022).

- Artículos 269B, 269E y 269G: En este Articulo se establece como un delito el desarrollo, la comercialización o la utilización de Software que se usen para afectar los sistemas informáticos, datos o redes (Congreso de la República de Colombia, 2009, art. 269E). Aunque no mencionados explícitamente, las prácticas descritas facilitan obstrucción de sistemas, uso de software malicioso y suplantación de identidades.

3)Decisión profesional frente a la oferta laboral

El análisis del acuerdo laboral revela la presencia de cláusulas ilegales y contrarias a la ética profesional, razón por la cual se concluye que no es viable aceptar la oferta de SecureNova Labs. Dichas cláusulas promueven prácticas asociadas a delitos informáticos, como interceptación de comunicaciones, acceso no autorizado y manipulación de datos, conductas tipificadas y sancionadas por la Ley 1273 de 2009. Además, aceptar este tipo de condiciones vulneraría los lineamientos del Código de Ética del COPNIA (2015), que exige al ingeniero actuar con honradez, legalidad y responsabilidad social. En particular, los artículos 4 y 7 obligan a rechazar encargos ilegales y a denunciar actos que comprometan la seguridad pública. Por tanto, firmar un contrato que limite la denuncia o encubra actividades ilícitas implicaría una participación directa en prácticas antiéticas y potencialmente delictivas.

4)Acceso a información sensible en auditorías

El acceso a información sensible por parte de empresas de ciberseguridad durante una auditoría debe limitarse estrictamente a lo necesario y estar autorizado, documentado y regulado contractualmente conforme a los principios de legalidad, confidencialidad y mínima exposición (MINTIC, 2022). Para evitar usos indebidos, se requiere la implementación de controles como acuerdos de confidencialidad que no obstaculicen la denuncia de delitos, trazabilidad de accesos, privilegios temporales con autenticación robusta y auditorías externas que garanticen transparencia. Según el Código de Ética del COPNIA, el ingeniero debe actuar con honestidad y dentro del marco legal, por lo que el manejo de datos sensibles debe realizarse de manera justificada, responsable y sometida a supervisión, para preservar la integridad del proceso y la confianza del cliente (Guarnizo Portela, 2024).

5) Mecanismos de supervisión para evitar abusos en análisis forense

La utilización de tecnologías sofisticadas para la investigación forense digital requiere estrictos niveles de supervisión, debido a que permiten obtener, duplicar y examinar datos muy delicados. Por ello, las organizaciones de ciberseguridad necesitan implementar sistemas integrales de monitoreo y control, centrados en evitar malversaciones, como una forma de asegurar la ética profesional y la legalidad de sus operaciones.

- Control técnico y acceso: Los controles técnicos y de acceso deben garantizar que cada empleado utilice únicamente los recursos necesarios mediante el principio de mínimo privilegio, complementado con gestión de accesos privilegiados, autenticación multifactor y auditorías permanentes. Las investigaciones forenses deben realizarse en laboratorios controlados para evitar accesos o copias no autorizadas de datos

sensibles. Además, las tecnologías de monitoreo en tiempo real permiten detectar actividades anómalas o intentos de uso indebido de herramientas, fortaleciendo la trazabilidad y la responsabilidad operativa del analista.

- Supervisión administrativa y auditoría interna: La supervisión administrativa en entornos de ciberseguridad requiere protocolos formales de autorización y control jerárquico para que toda actividad forense sea aprobada y verificada mediante informes documentados. Asimismo, deben realizarse auditorías internas y externas periódicas que evalúen el cumplimiento ético, los niveles de acceso y la correcta aplicación de las políticas de seguridad y confidencialidad. Además, la separación de funciones es esencial para evitar conflictos de interés, garantizando que quienes ejecutan los análisis no sean quienes revisan o validan los resultados, reduciendo así el riesgo de manipulación o encubrimiento de evidencias.

- Marco ético y formación profesional: El marco ético en ciberseguridad exige que los profesionales actúen con honestidad, imparcialidad y respeto a la ley, conforme al Código Ético del COPNIA (2015). Para garantizar este cumplimiento, las empresas deben ofrecer formación continua en ética digital, normatividad y responsabilidad profesional, de modo que los trabajadores comprendan las consecuencias legales y disciplinarias del uso indebido de herramientas forenses. Asimismo, es necesario implementar canales de denuncia seguros y confidenciales que faciliten el reporte de conductas irregulares, fortaleciendo la transparencia institucional y promoviendo una cultura de integridad dentro de los equipos de ciberseguridad.

- Marco legal y rendición de cuentas: El marco legal exige el estricto cumplimiento de la Ley 1273 de 2009, que tipifica delitos como el acceso abusivo a sistemas informáticos y la violación de datos personales. El uso indebido de herramientas

forenses puede constituir una infracción penal cuando implica obtener, modificar o divulgar información sin autorización. Por ello, las empresas deben establecer cláusulas contractuales y disciplinarias que sancionen con rigor cualquier manipulación inadecuada de datos y garantizar la notificación oportuna a las autoridades en caso de indicios de actividades ilícitas, fortaleciendo la rendición de cuentas y la responsabilidad institucional.

6) Respuesta ante actos de ciberespionaje cometidos por proveedores

Si una compañía de ciberseguridad se dedica a realizar actos de espionaje informático, la confianza que mantiene la relación entre el proveedor y su cliente se ve afectada. Es esencial que tanto los gobiernos como las organizaciones afectadas actúen con determinación legal, técnica y moral para sancionar las acciones ilegales, restaurar la confianza institucional y prevenir su repetición en el futuro.

- Respuesta inmediata, investigación y acciones legales: La respuesta inmediata ante un caso de espionaje requiere una investigación forense y legal exhaustiva para identificar el alcance del incidente, los sistemas afectados y los responsables. Conforme a la Ley 1273 de 2009, estas acciones pueden constituir delitos como acceso indebido, violación de datos personales e interceptación de comunicaciones, por lo que deben ser denunciadas ante las autoridades competentes. Además, es necesario revocar de forma inmediata los contratos y accesos de la empresa implicada y activar los planes de contingencia y recuperación recomendados por el MINTIC, con el fin de proteger la integridad de la información y mitigar el impacto reputacional.
- Medidas administrativas y sancionatorias: Las medidas administrativas y sancionatorias deben incluir la imposición de sanciones contractuales y disciplinarias, así como la inhabilitación temporal o definitiva de las empresas que incurran en prácticas

ilícitas, impidiéndoles contratar con el Estado. Las entidades de control, como la Superintendencia de Industria y Comercio y el Ministerio de Defensa, deben fortalecer la supervisión mediante criterios de certificación, auditoría y cumplimiento ético para los proveedores de ciberseguridad. Además, la creación de registros públicos de empresas sancionadas promueve la transparencia y evita que organizaciones con antecedentes de espionaje continúen operando bajo nuevas identidades o contratos.

- Restauración de la confianza y fortalecimiento institucional: La restauración de la confianza institucional requiere reforzar los mecanismos de gobernanza digital mediante nuevos procesos de selección y supervisión de proveedores, apoyados en certificaciones como ISO/IEC 27001 e ISO/IEC 27701. Internamente, las entidades deben crear comités de ética digital y designar oficiales de cumplimiento (CISO) para supervisar relaciones con terceros y garantizar el cumplimiento de las políticas de seguridad y privacidad. Conforme al Código de Ética del COPNIA (2015), los ingenieros deben actuar con integridad y responsabilidad social, por lo que la recuperación de la confianza implica no solo medidas tecnológicas, sino también reformas éticas y culturales dentro de las organizaciones y empresas de ciberseguridad.

- Prevención y políticas a largo plazo: La prevención a largo plazo requiere que los gobiernos implementen políticas públicas orientadas a fortalecer la ciber ética, regular a los proveedores de ciberseguridad y asegurar la responsabilidad penal de las empresas. Esto incluye crear marcos nacionales de certificación que evalúen transparencia y buenas prácticas antes de contratar servicios, así como promover la cooperación internacional en la investigación de delitos informáticos. Además, es esencial desarrollar programas de educación y sensibilización digital para funcionarios y ciudadanos, con el fin de fomentar la comprensión de los riesgos del ciberespionaje y

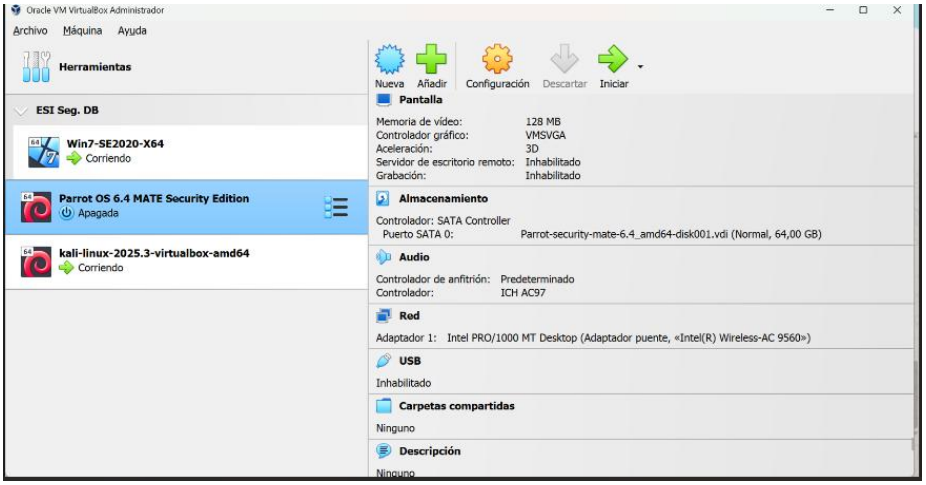
promover una cultura de denuncia y transparencia que fortalezca la ciberseguridad nacional (Guarnizo Portela, 2024).

Etapa 3: Componente práctico - Prácticas simuladas

En esta Etapa se presentan dos ejercicios de pruebas de intrusión orientado al rol del Red Team, aplicando metodologías ofensivas para evaluar la seguridad de un entorno que incluye dos máquinas virtuales: Windows 7 como objetivo y Kali Linux como sistema atacante. El propósito central es identificar, explotar y documentar vulnerabilidades reales mediante herramientas como Nmap, Nessus y Metasploit.

Figura 11

IP Instalación banco de trabajo maquinas Windows 7 & Kali Linux



Fuente. Autoría Propia

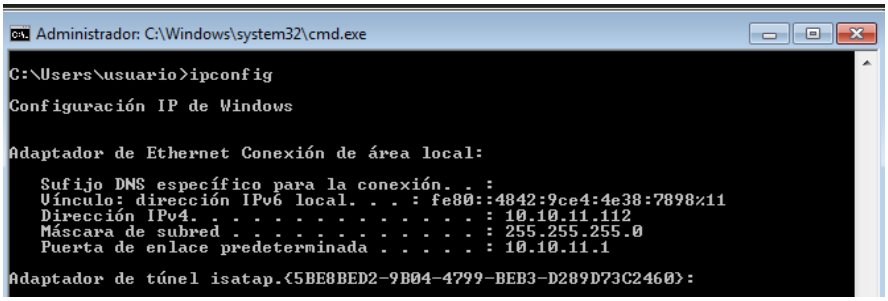
En la imagen anterior se puede visualizar la instalación del banco de trabajo el cual será de gran ayuda para desarrollar habilidades prácticas para anticipar y mitigar amenazas en entornos reales, especialmente cuando se trata de sistemas obsoletos como Windows 7, los cuales presentan múltiples vectores de ataque debido a servicios inseguros, falta de actualizaciones y configuraciones incorrectas.

Ejercicio 1

El ejercicio inicia con la configuración del laboratorio, donde se verifican las direcciones IP, máscara de red y conectividad entre las máquinas. Esta fase confirma que el entorno está correctamente configurado para iniciar las pruebas ofensivas.

Figura 12

Configuración IP Ejercicio 1 Windows 7

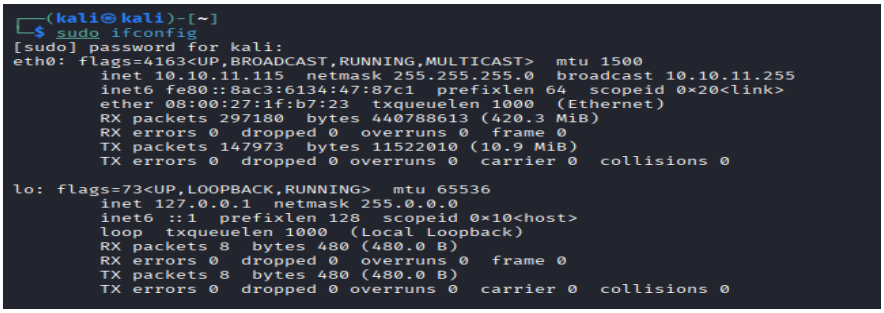


Fuente. Autoría Propia

En la imagen anterior se muestra que la computadora con Windows 7 está conectada a la red de la siguiente forma: Dirección IP 10. 10. 11. 112, Máscara de Subred 255. 255. 255. 0 y una puerta de enlace 10. 10. 11. 1.

Figura 13

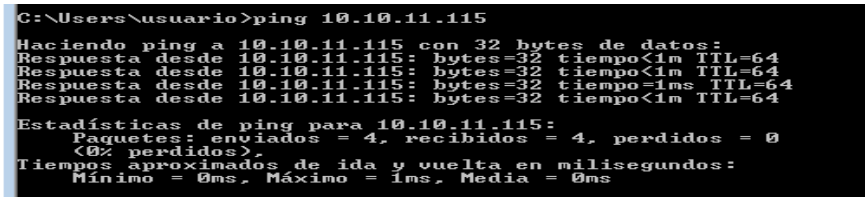
Configuración IP Ejercicio 1 Kali Linux



Fuente. Autoría Propia

Figura 14

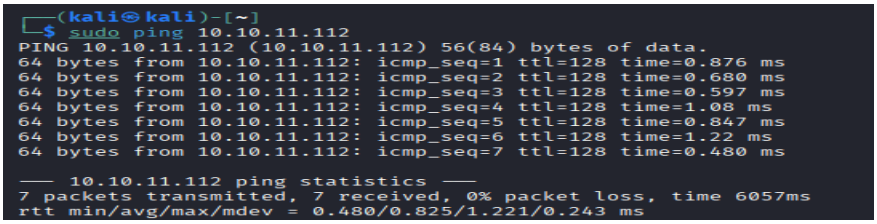
Verificación comunicación maquina Windows VS Maquina de Kali Linux



Fuente. Autoría Propia

Figura 15

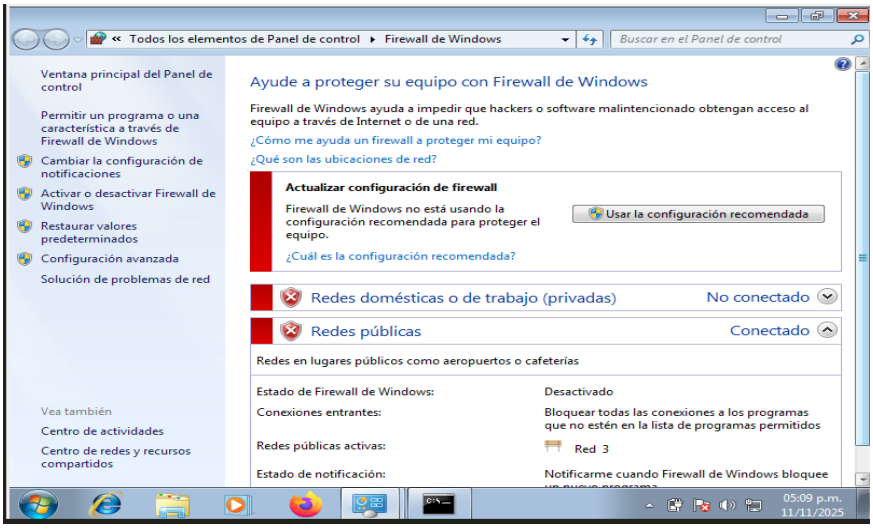
Verificación comunicación maquina Kali Linux Vs Maquina Windows 7



Fuente. Autoría Propia

Figura 16

Desactivación Firewall maquina Windows 7



Fuente. Autoría Propia

En la imagen anterior se muestra evidenciar el firewall de la máquina de Windows 7 está desactivado, lo cual es esencial para llevar a cabo el laboratorio controlado.

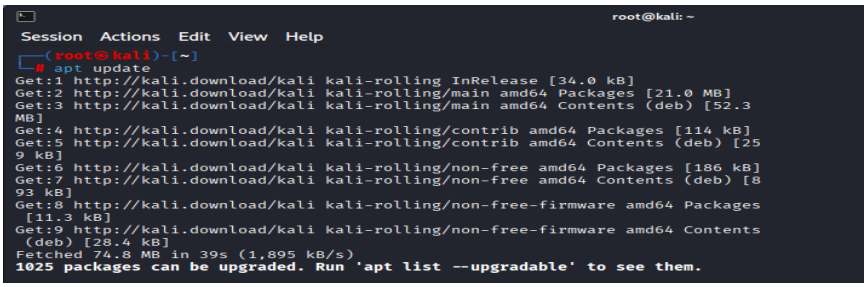
A continuación, se detallan las herramientas de software empleadas y organizadas en función de las etapas de un pentesting:

Fase 1 – Reconocimiento y Escaneo

Se actualiza el sistema Kali Linux mediante apt update y apt full-upgrade -y, lo cual garantiza compatibilidad y ejecución estable de Metasploit. Posteriormente, se ejecuta un escaneo Nmap completo para identificar puertos abiertos, servicios activos y el sistema operativo objetivo. El hallazgo principal fue el servicio SMB vulnerable en el puerto 445, asociado a MS17-010 (EternalBlue).

Figura 17

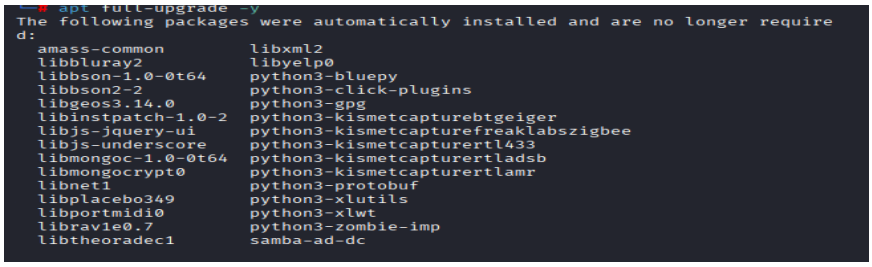
Comando 1 Actualización del entorno de Kali Linux con el comando apt update



Fuente. Autoría Propia

Figura 18

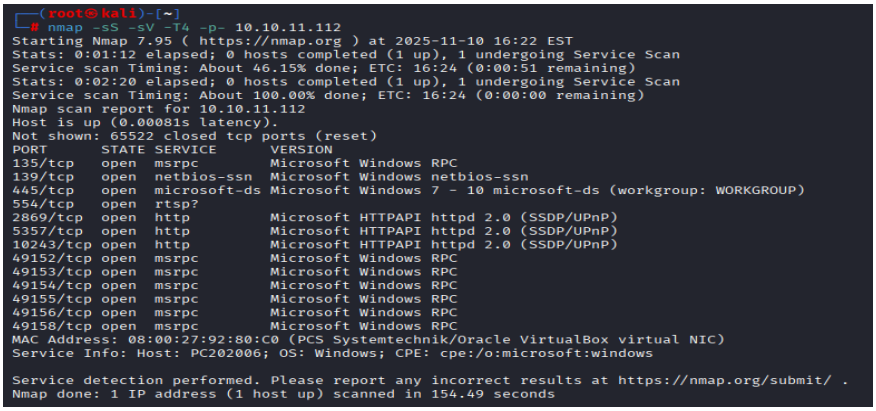
Comando 2 Actualización del entorno de Kali Linux con el comando apt full-upgrade -y



Fuente. Autoría Propia

Figura 19

Comando 3 nmap -sS -sV -T4 -p- Escaneo de Puertos TCP y detección de servicios

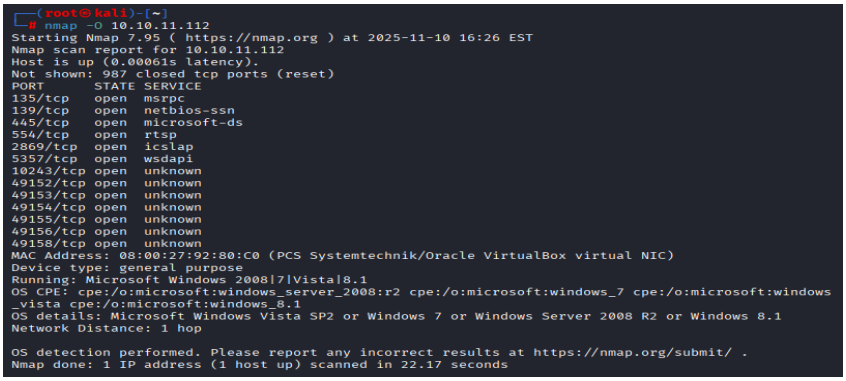


Fuente. Autoría Propia

La imagen previa muestra la realización del comando nmap -sS -sV -T4 -p- 10.10.11.112, que tiene como objetivo identificar todos los puertos abiertos y los servicios que opera la máquina virtual de Windows 7 a la que se dirige. La máquina tiene habilitados los servicios asociados a SMB (Server Message Block) en el puerto 445, que son habituales en Windows; esto indica un posible vector de ataque. Asimismo, el hecho de que Windows 7 esté presente señala que es un sistema operativo anticuado con vulnerabilidades críticas conocidas.

Figura 20

Comando 4 – nmap -O 10.10.11.112 Detección Sistema Operativo

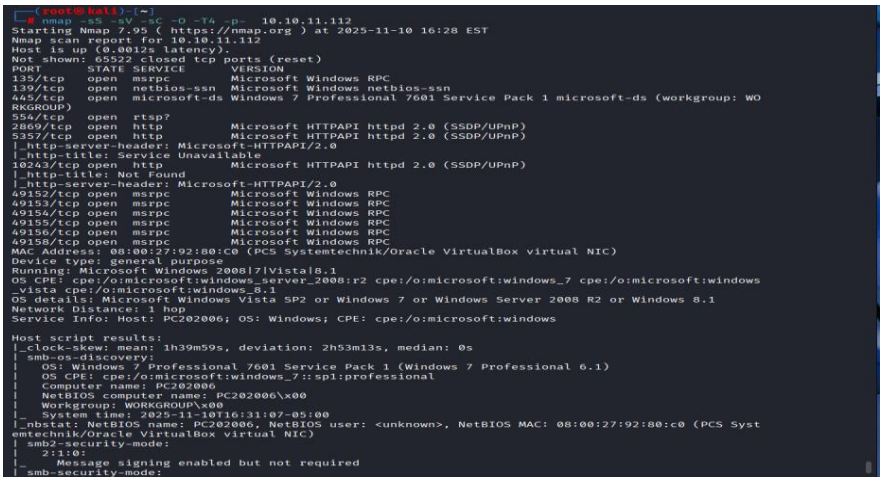


Fuente. Autoría Propia

La ejecución del comando nmap -O 10.10.11.112, que busca determinar el sistema operativo, es visible en la imagen anterior y será muy útil para ajustar la estrategia de explotación. En la detección se verifica que el host está ejecutando Windows 7 Professional Service Pack 1 (x64), una versión susceptible a varios exploits SMB, incluyendo MS17-010 (EternalBlue).

Figura 21

Comando 5 – Escaneo con scripts por defecto y verificación de seguridad



Fuente. Autoría Propia

La imagen previa permite observar la implementación del script NSE por defecto de Nmap con el propósito de recabar información adicional acerca de la configuración del servicio SMB. La firma de mensajes SMB está deshabilitada, lo que reduce la autenticación y propicia los ataques Man-in-the-Middle o la inyección de tráfico malicioso.

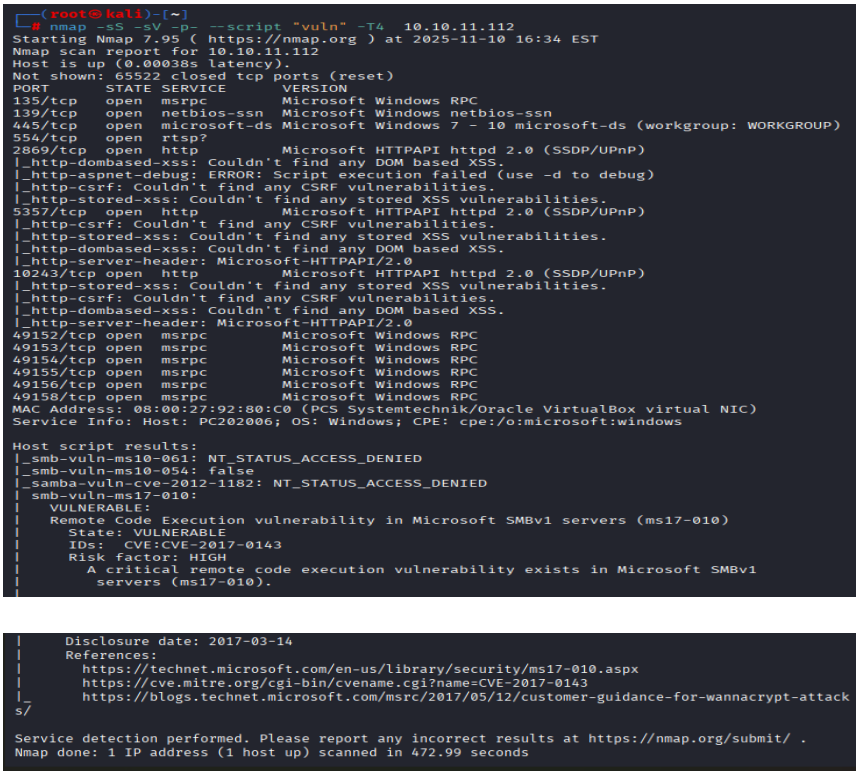
Fase 2 – Identificación y validación de vulnerabilidades.

El propósito de esta etapa es verificar la vulnerabilidad en SMBv1 y comenzar a explotar de manera controlada el sistema, se utilizará la herramienta Metasploit Framework,

Se emplea esta herramienta porque nos proporciona módulos automáticos que pueden identificar vulnerabilidades y explotarlas con exactitud y supervisión, evitando perjudicar al sistema.

Figura 22

Comando 6 – Escaneo de vulnerabilidades con scripts NSE



Fuente. Autoría Propia

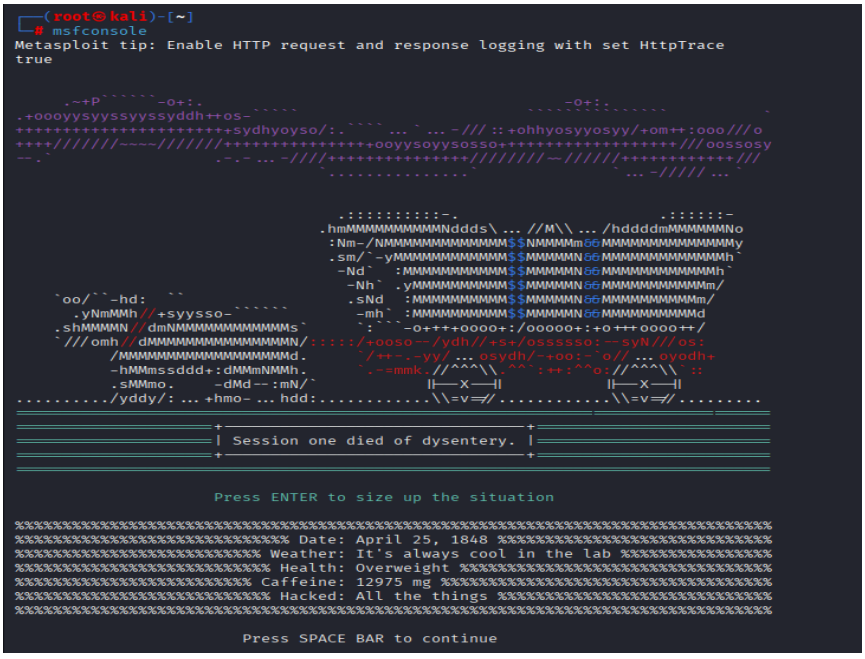
La aplicación del comando nmap -sS -sV -p- --script "vuln" -T4 10.10.11.112, cuyo propósito era detectar vulnerabilidades existentes en los servicios activos, se muestra en la imagen anterior. Se puede notar que el host es susceptible a MS17-010 (EternalBlue), una falla crítica que posibilita la ejecución remota de código sin necesidad de autenticación previa.

Fase 3 – Explotación

Se inicia Metasploit, se selecciona el módulo windows/smb/ms17_010_eternalblue, y se configuran los parámetros necesarios: dirección IP víctima, dirección IP atacante y payload reverse_tcp. Al ejecutar el exploit, se obtiene una sesión Meterpreter con privilegios SYSTEM, lo que equivale a control total del sistema.

Figura 23

Inicio de Metasploit

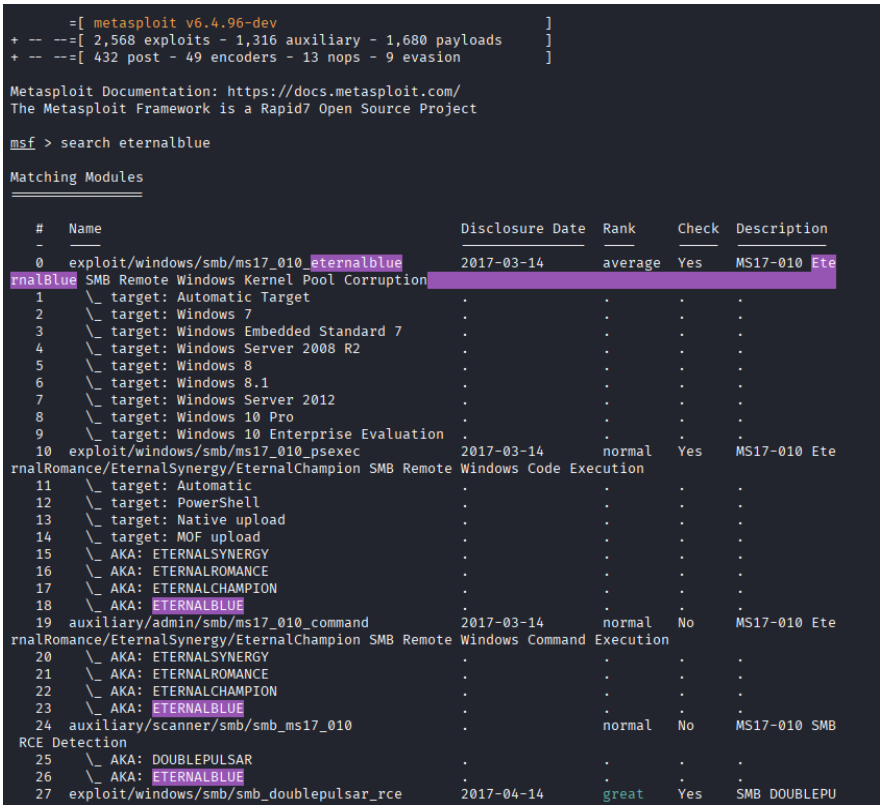


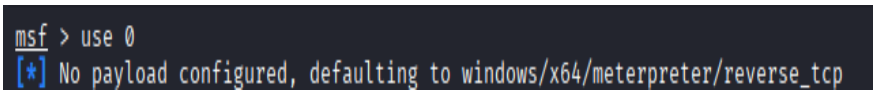
Fuente. Autoría Propia

En la imagen anterior se puede evidenciar el inicio en la consola Metasploit en la terminal de Kali Linux ejecutando el comando *msfconsole.*

Figura 24

Búsqueda del módulo EternalBlue



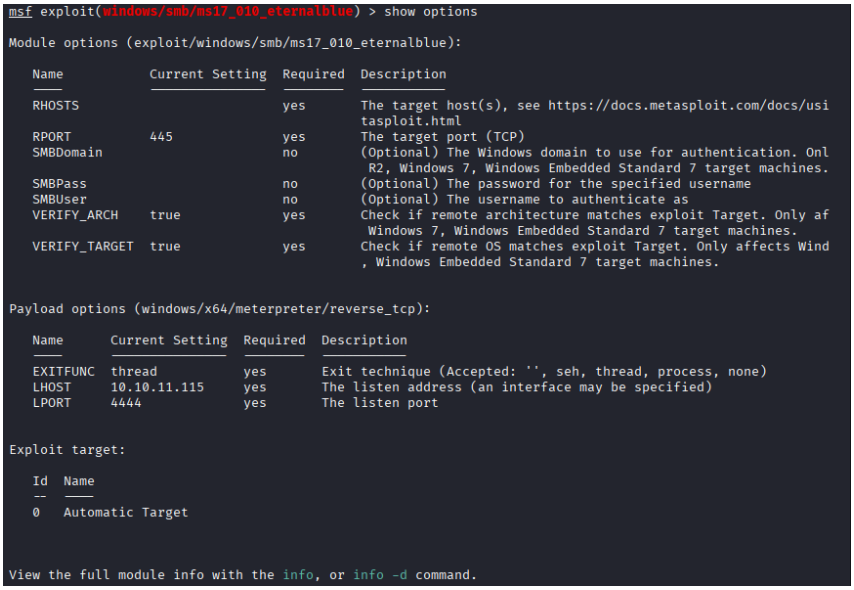


Fuente. Autoría Propia

En la imagen de arriba se puede ver cómo se lleva a cabo el comando search eternalblue, que nos ayuda a ver los exploits disponibles para comprometer el sistema. En esta ocasión, se elegirá el exploit 0 exploit/windows/smb/ms17_010_eternalblue Rank: great utilizando el comando use 0.

Figura 25

Selección y configuración del módulo comando show options

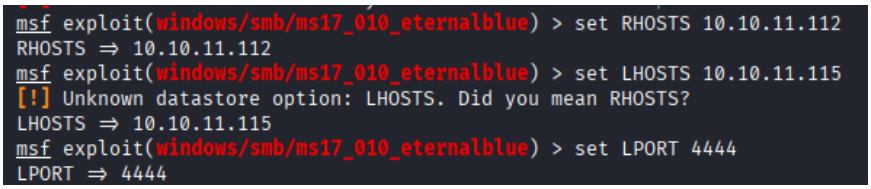


Fuente. Autoría Propia

En la imagen previa, al ejecutar el comando show options, se exhiben las opciones configurables del módulo que está activo (el exploit que se ha seleccionado) y del payload relacionado.

Figura 26

Configuración de RHOSTS y LHOST

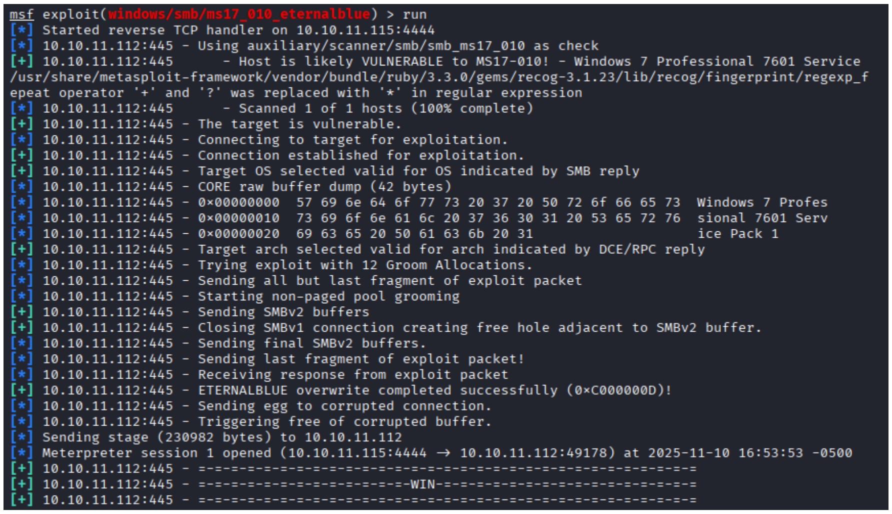


Fuente. Autoría Propia

En la imagen previa, se puede observar cómo están establecidos el host víctima (RHOSTS 10.10.11.112) y el host atacante (LHOST 10.10.11.115). También se muestra el puerto de escucha (LPORT 4444), que será el encargado de recibir la conexión inversa.

Figura 27

Ejecución exitosa del exploit

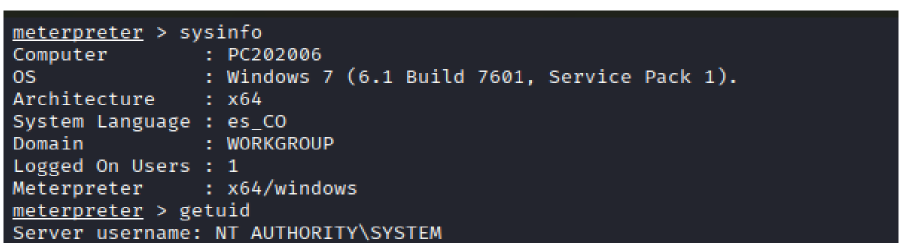


Fuente. Autoría Propia

Después de configurar el módulo, tal como se puede ver en la imagen número 16, se ejecuta el comando run. El propósito de este comando es ejecutar el exploit, tal como se muestra en la imagen. Esto nos permite acceder de manera remota con privilegios elevados a través de la sesión Meterpreter.

Figura 28

Verificación de sistema y privilegios

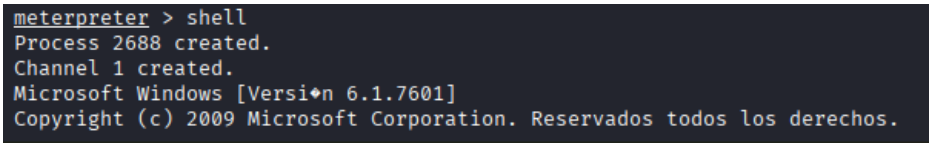


Fuente. Autoría Propia

En la imagen de arriba se muestra la verificación de privilegios que se logró al ejecutar los comandos sysinfo y getuid. Así, se obtuvo control total del sistema con privilegios SYSTEM, el nivel más elevado en Windows.

Figura 29

Acceso a la shell del sistema

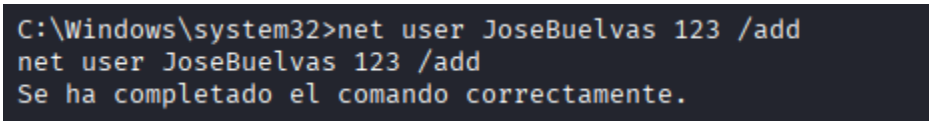


Fuente. Autoría Propia

La imagen anterior muestra que, al ejecutar el comando Shell, se obtiene acceso a una consola remota en la máquina atacada. Esto posibilita la ejecución de órdenes directamente en el sistema afectado.

Figura 30

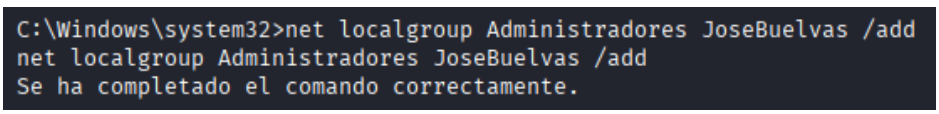
Creación de usuario persistente paso 1



Fuente. Autoría Propia

Figura 31

Creación de usuario persistente paso 2

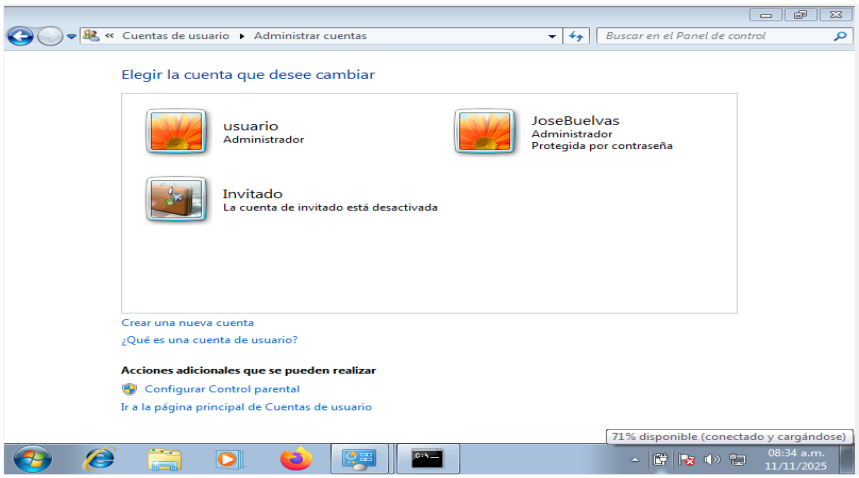


Fuente. Autoría Propia

Las imágenes previas muestran que se estableció un usuario local con el nombre de JoseBuelvas, quien tiene privilegios de administrador, asegurando la persistencia en el sistema comprometido.

Figura 32

Creación de usuario en la Interfax de Windows

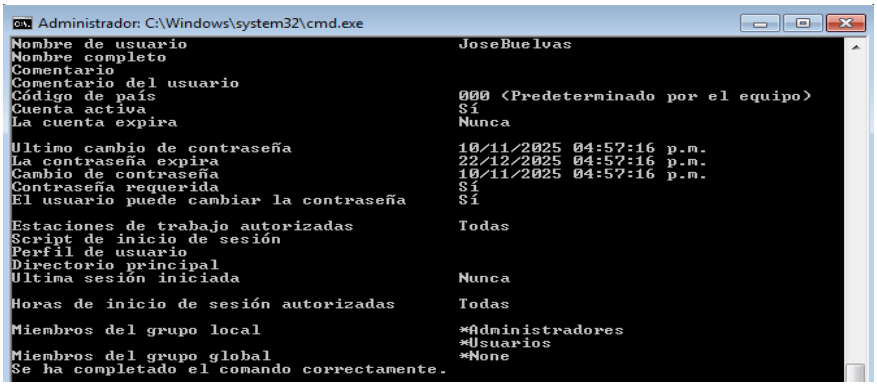


Fuente. Autoría Propia

La imagen anterior demuestra que se pudo crear el usuario con privilegios de administrador.

Figura 33

Verificación usuario en maquina Windows 7



Fuente. Autoría Propia

La imagen de arriba demuestra que el usuario fue creado, usando el comando *net user* JoseBuelvas.

Ejercicio 2

En el segundo caso, Windows 7 ejecuta Rejetto HFS 2.3, un servidor HTTP que presenta vulnerabilidades ante varios CVE. Se constata que hay conexión entre los dos dispositivos y se comprueba la exposición del puerto 80.

Figura 34

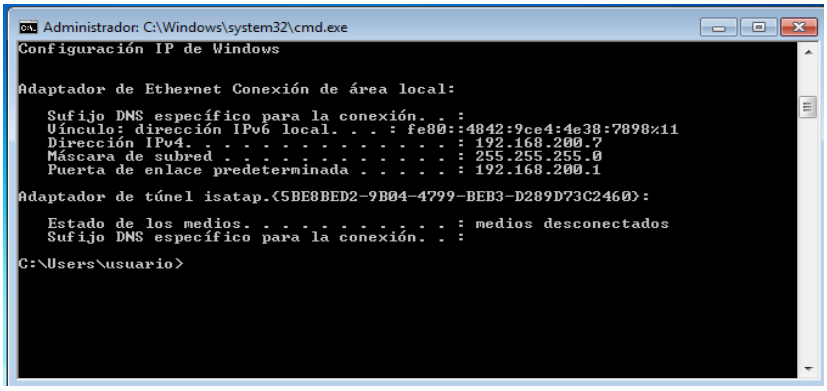
Instalación aplicación Rejetto

Fuente. Autoría Propia

En la imagen anterior se puede evidenciar que la aplicación está instalada en la máquina virtual de Windows 7.

Figura 35

Configuración IP Máquina Windows 7

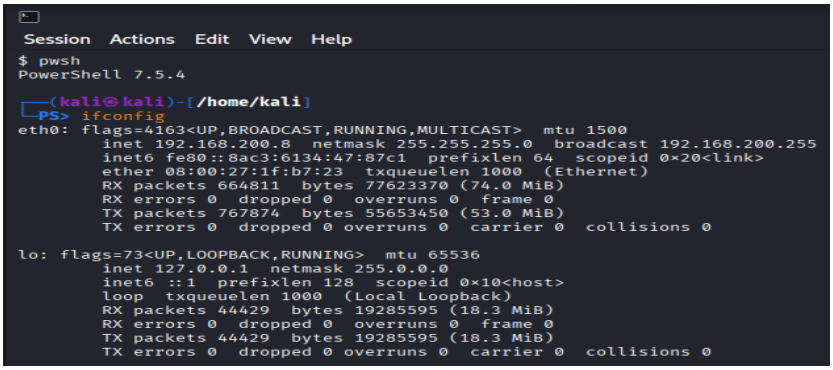


Fuente. Autoría Propia

La imagen previa muestra la configuración de la máquina virtual de Windows 7, que cuenta con una puerta de enlace (192.168.200.1), una dirección IP (192.168.200.7) y una máscara de red (255.255.255).

Figura 36

Configuración IP Maquina Kali Linux

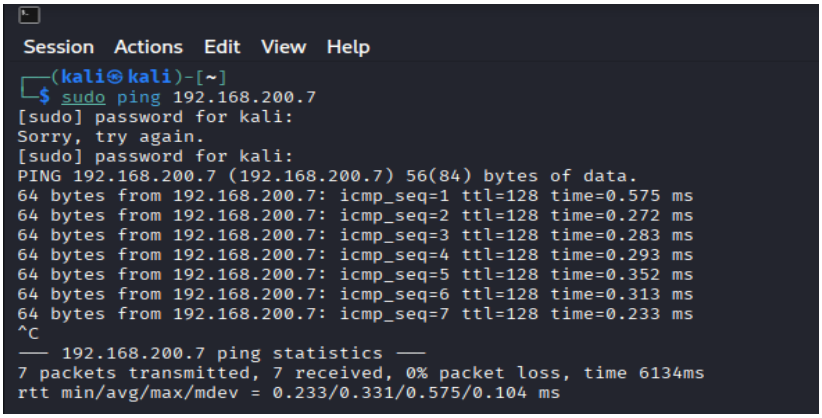


Fuente. Autoría Propia

La configuración de la máquina virtual de Kali Linux está visible en la imagen anterior. Esta cuenta con una puerta de enlace 192.168.200.255, una máscara de red 255.255.255.0 y una dirección IP 192.168.200.8.

Figura 37

Verificación Ping entre máquinas

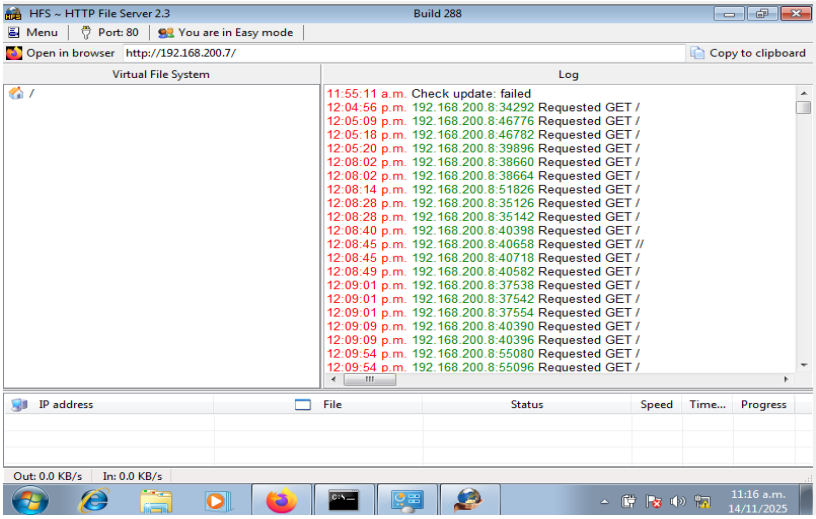


Fuente. Autoría Propia

La imagen anterior muestra que hay comunicación entre las dos máquinas virtuales, lo que significa que ambas están conectadas a la misma red.

Figura 38

Inicio servidor HFS- HTTP.



Fuente. Autoría Propia

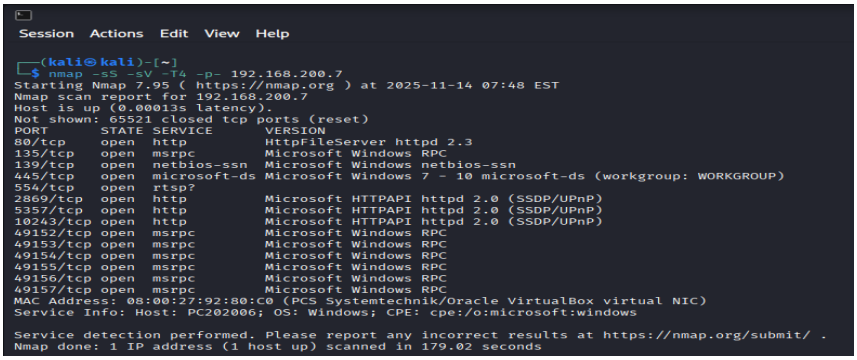
En la imagen de arriba se observa que el servidor HFS (HTTP File Server) versión 2.3 está en funcionamiento en la computadora víctima con dirección IP 192.168.200.7.

Fase 1 – Reconocimiento y Escaneo

Nmap muestra tanto un conjunto de puertos vulnerables como la aparición de servicios inseguros, por ejemplo, SMB y HFS 2.3, e identifica Windows 7 SP1. Scripts NSE identifican debilidades críticas como Apache Range DoS y CVE-2014-6287 (RCE).

Figura 39

Escaneo rápido con el comando nmap -sS -sV -T4 -p-



Fuente. Autoría Propia

Se está llevando a cabo un escaneo total y agresivo de la dirección IP 192.168.200.7, con el comando nmap -sS -sV -T4 -p-, que rastrea todos los puertos, determina las versiones de los servicios y aplica una técnica rápida.

Figura 40

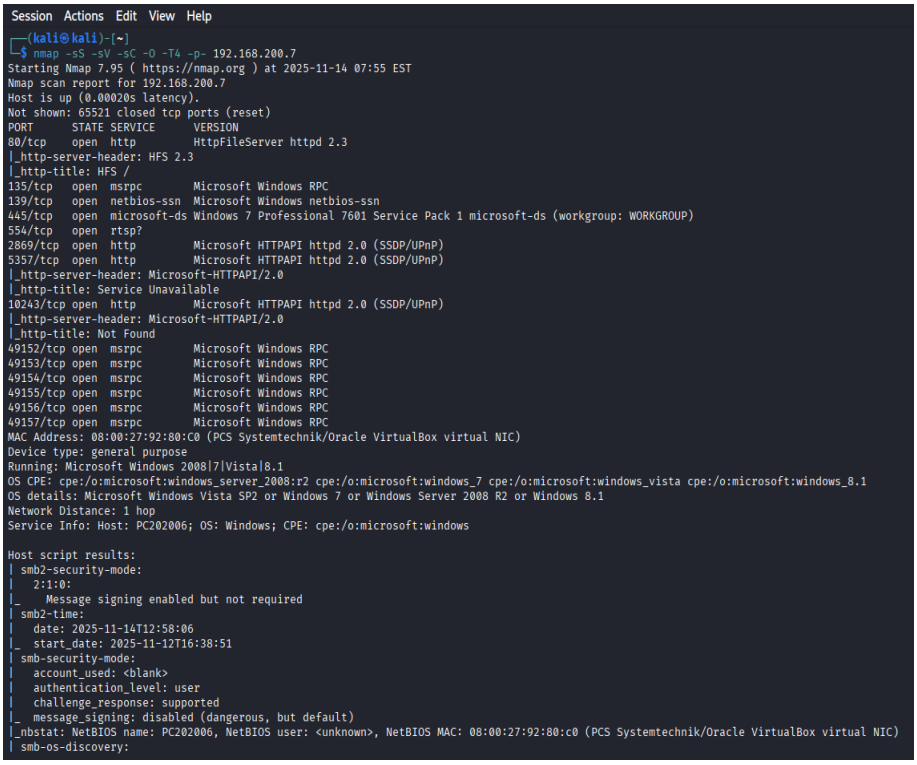
Detección de sistema operativo comando nmap -O

Fuente. Autoría Propia

Al ejecutar el comando nmap -O 192. 168. 200. 7, se está llevando a cabo un análisis del sistema operativo de la máquina que se quiere investigar. Esto permite identificar la versión, el tipo de dispositivo, la cantidad de saltos (hops) y los servicios disponibles que pueden ser útiles para su identificación.

Figura 41

Escaneo completo comando nmap -sS -sV -sC -O -T4 -p- 192.168.200.7

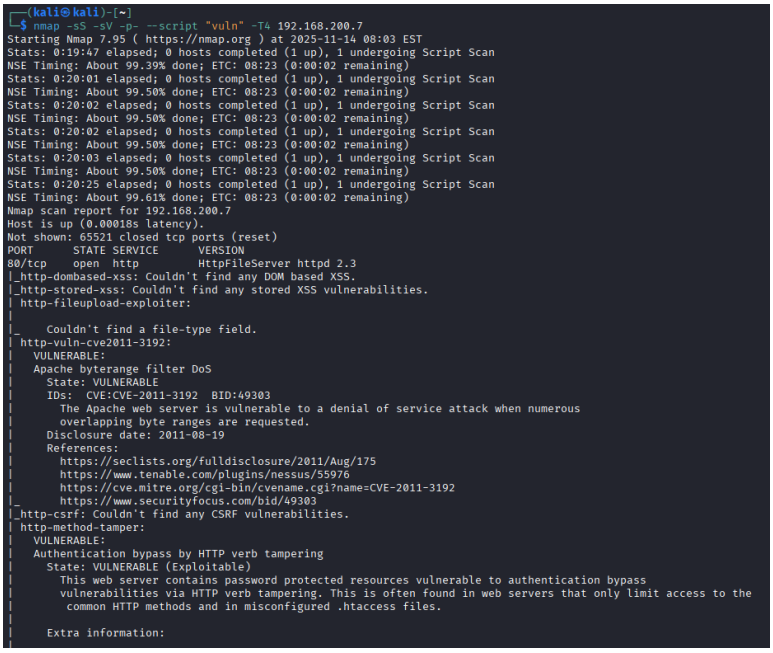


Fuente. Autoría Propia

Con la ejecución del comando se lleva a cabo un análisis exhaustivo, intenso y detallado de la máquina virtual con Windows 7, lo que permite recopilar datos clave para un ataque controlado. Se puede observar que el sistema operativo es Windows 7 Profesional SP1, con HFS 2. 3 susceptible, SMB sin firma, puertos RPC accesibles y un sistema con vulnerabilidad potencial conocida como ETERNALBLUE.

Figura 42

Escaneo exhaustivo de vulnerabilidades comando nmap -sS -sV -p- --script "vuln" -T4 192.168.200.7



Fuente. Autoría Propia

Con la ejecución de este comando, se lleva a cabo un análisis de vulnerabilidades completamente automatizado en la máquina que utiliza Windows 7 con la dirección IP 192. 168. 200. 7. Su propósito es detectar CVEs, debilidades en sitios web y vulnerabilidades en el protocolo SMB que podrían ser manipuladas. La máquina en cuestión presenta diversas vulnerabilidades de gran gravedad, incluyendo EternalBlue, lo que la coloca en un nivel de riesgo muy alto. Se logran reconocer debilidades críticas como: MS17-010 – EternalBlue (RCE), manipulación de métodos HTTP (eliminación de autenticación) y CVE-2011-3192 (Denegación de servicio – Apache Range). También se identifican servicios tales como: HFS 2. 3 (vulnerable a RCE por CVE-2014-6287), RPC, SMB y HTTPAPI.

Tabla 2

Principales hallazgos del Escaneo Nmap

Categoría	Descripción
Puertos Abiertos	80/tcp (HttpFileServer 2.3), 445, 135, 139, 10243, 2869, 5357 — servicios Windows SMB/RPC/HTTPAPI.
Sistema Operativo	Windows 7 / Windows Server 2008 R2 / Windows Vista.
Grupo de Trabajo	WORKGROUP
Vulnerabilidades	MS17-010 (EternalBlue) y CVE-2011-3192 (Apache ByteRange DoS) confirmadas. Posible HTTP Verb Tampering.
Resultado de Scripts NSE	Sin XSS, CSRF ni File Upload. Solo vulnerabilidades confirmadas: MS17-010 y CVE-2011-3192.
Archivos Exportados	nmap_aggressive.nmap, nmap_aggressive.gnmap, nmap_aggressive.xml.

Fuente. Autoría Propia

La tabla presenta un resumen estructurado de los principales hallazgos identificados durante el escaneo Nmap. En cuanto a los puertos abiertos, se detecta la exposición del servicio HttpFileServer 2.3 en el puerto 80/tcp, junto con varios puertos asociados a servicios internos de Windows —incluyendo SMB (445/tcp) y múltiples puertos de RPC y HTTPAPI— lo que indica una superficie de ataque amplia en un sistema legado. El sistema operativo identificado corresponde a versiones antiguas de Windows, específicamente Windows 7, Windows Server 2008 R2 o Windows Vista, todas ya fuera de soporte y con vulnerabilidades conocidas.

El equipo pertenece al grupo de trabajo WORKGROUP, una configuración por defecto común en entornos no corporativos o de baja gestión centralizada. En la sección de

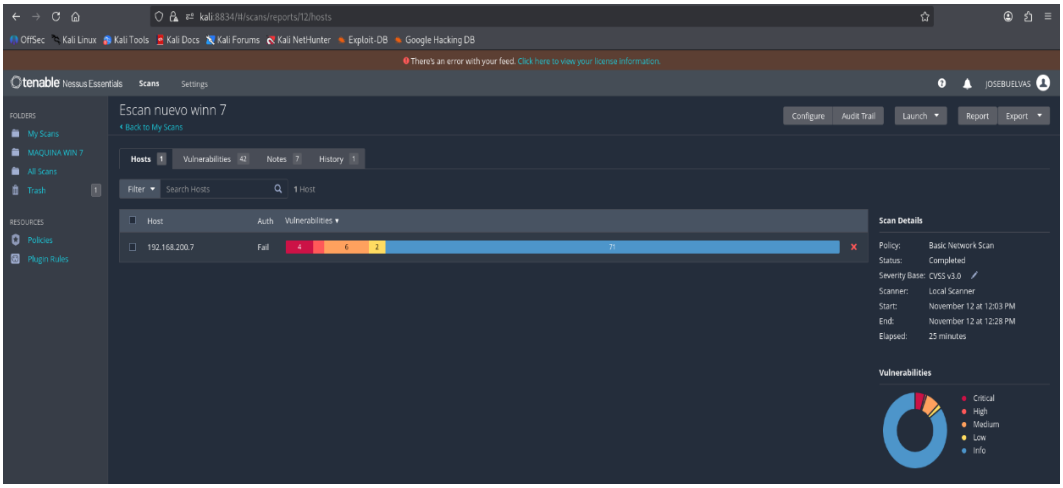
vulnerabilidades, la tabla confirma dos fallas críticas: MS17-010 (EternalBlue), que permite ejecución remota de código a través de SMB, y CVE-2011-3192, asociada a ataques de denegación de servicio contra servidores Apache mediante peticiones ByteRange maliciosas. También se señala un posible caso de HTTP Verb Tampering, que podría facilitar eludir autenticación en aplicaciones web.

Fase 2 –Validación de vulnerabilidades

Nessus verifica la gravedad del sistema: presenta 4 vulnerabilidades críticas, 6 de alto riesgo y varias alertas complementarias. Resalta la vulnerabilidad Rejetto HFS RCE, clasificada como crítica debido a que permite la ejecución remota de código.

Figura 43

Resultado del escaneo Nessus



Fuente. Autoría Propia

En la imagen de arriba se presenta un servidor con diversas vulnerabilidades y elevados, lo que es habitual en versiones antiguas de sistemas operativos de Windows o en aquellos sin actualizaciones. Nessus verifica que la máquina virtual es altamente susceptible a intrusiones,

sobre todo al fallar el proceso de autenticación, lo que indica que las debilidades pueden ser detectadas desde la red sin necesidad de privilegios.

Tabla 3

Vulnerabilidades encontradas Nessus

Severidad	Cantidad	Color
Criticas	4	Rojo
Altas	6	Naranja
Medias	2	Amarillo
Bajas	71	Azul
Informativas	No visibles	

Fuente. Autoría Propia

La tabla anterior se presenta un resumen cuantitativo de las vulnerabilidades identificadas por el escáner Nessus, clasificadas según su nivel de severidad. Se reportan 4 vulnerabilidades críticas, representadas en color rojo, las cuales corresponden a fallas con alto potencial de explotación que permiten comprometer de manera inmediata la integridad, confidencialidad o disponibilidad del sistema. Estas requieren atención inmediata debido a su impacto operativo y riesgo elevado. En la categoría de severidad alta, Nessus detectó 6 vulnerabilidades, señaladas en color naranja. Estas fallas, aunque no tan peligrosas como las críticas, aún representan riesgos significativos que pueden ser aprovechados por atacantes para escalar privilegios, exfiltrar datos o interrumpir servicios esenciales. Las vulnerabilidades de nivel medio suman 2 hallazgos, marcadas en color amarillo. Este tipo de fallas puede no ser directamente explotable o requiere condiciones específicas, pero contribuyen a debilitar la postura de seguridad general del sistema

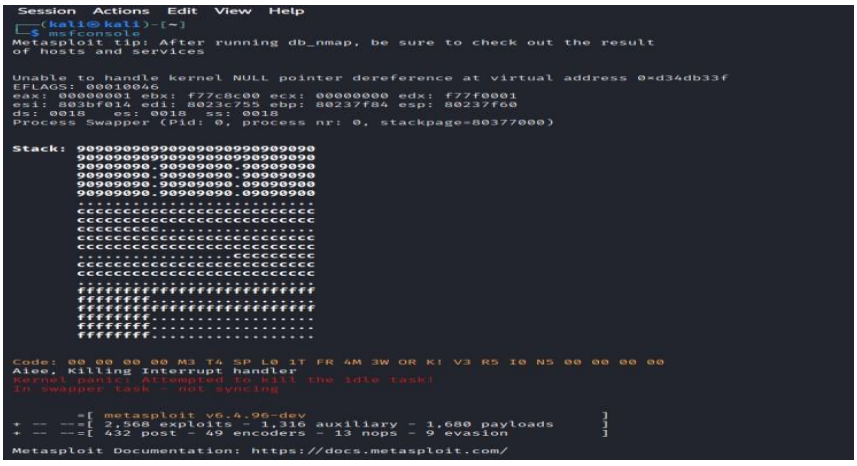
si no se gestionan adecuadamente. la mayor cantidad de registros corresponde a las vulnerabilidades bajas, con 71 hallazgos, representadas en color azul. Estas usualmente están asociadas a configuraciones no óptimas, información expuesta o buenas prácticas incumplidas. Aunque su impacto individual es limitado, su volumen sugiere oportunidades de mejora en la higiene de seguridad del sistema. Se hace referencia a la categoría informativa, la cual no es visible en esta tabla, pero que suele complementar los análisis de Nessus mediante advertencias o detalles adicionales sobre configuraciones, servicios detectados o buenas prácticas recomendadas.

Fase 3 – Explotación

En esta fase se inicia el framework Metasploit y se procede con la explotación de la vulnerabilidad crítica presente en el servicio Rejetto HFS 2.3, ejecutado en la máquina víctima Windows 7.

Figura 44

Inicio consola Metasploit

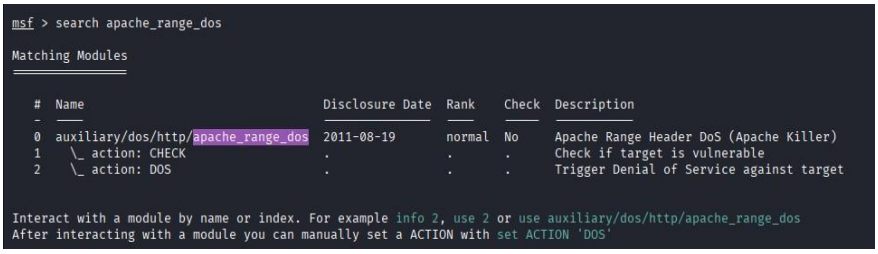


Fuente. Autoría Propia

En la imagen anterior se presenta el comienzo de la herramienta Metasploit empleando el comando *msfconsole* desde la consola de Kali Linux.

Figura 45

Ejecución comando msf > search apache_range_dos

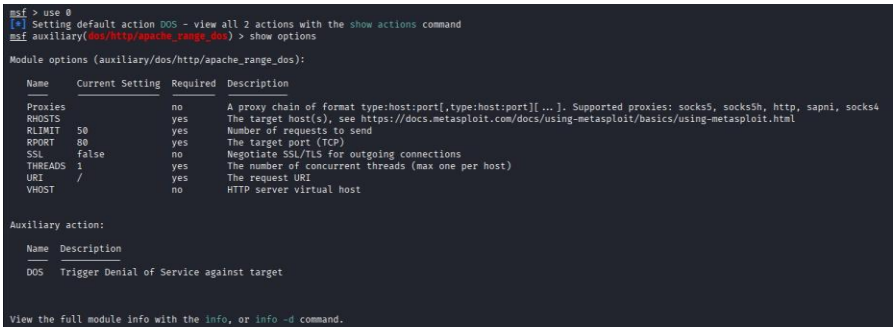


Fuente. Autoría Propia

Al llevar a cabo el comando *search apache_range_dos* como se observa en la imagen previa, Metasploit presenta el módulo auxiliar destinado a examinar o provocar un ataque DoS en servidores Apache que tienen vulnerabilidades.

Figura 46

Ejecución comando use 0 y show options

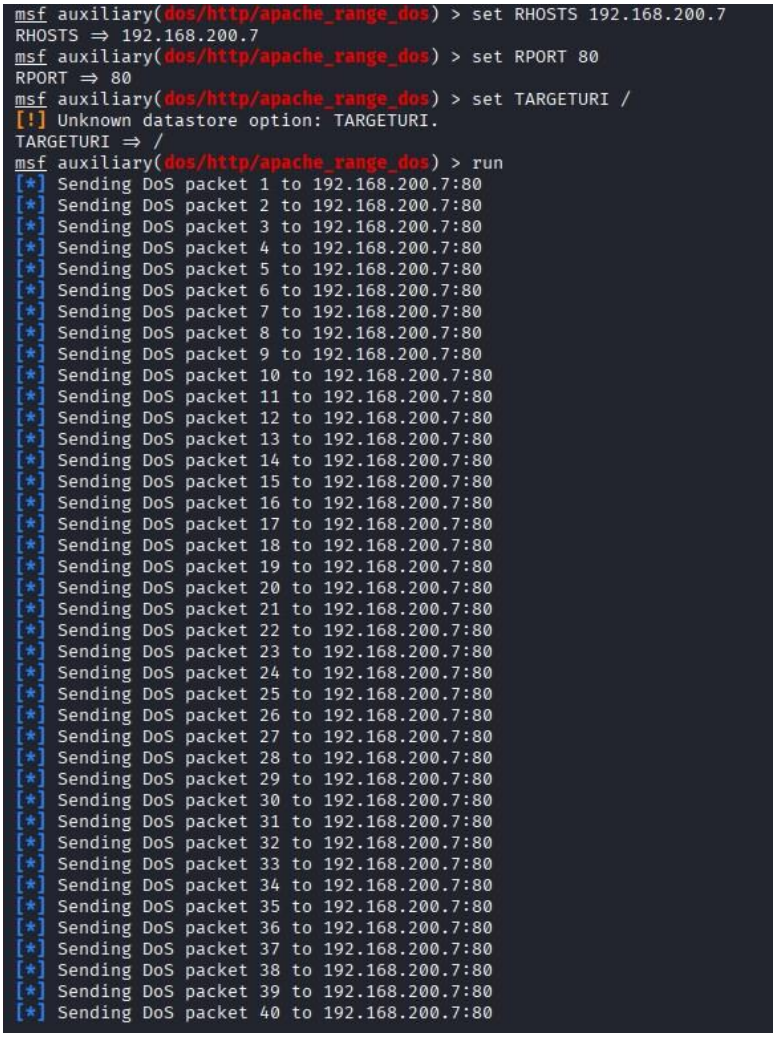


Fuente. Autoría Propia

En la imagen previa se puede ver cómo se lleva a cabo el comando use 0, que nos da la posibilidad de iniciar el módulo auxiliar. Tras completar este paso, ingresamos el comando show options para configurar el ataque de denegación de servicios.

Figura 47

Ejecución ataque de Denegación de Servicio (DoS)



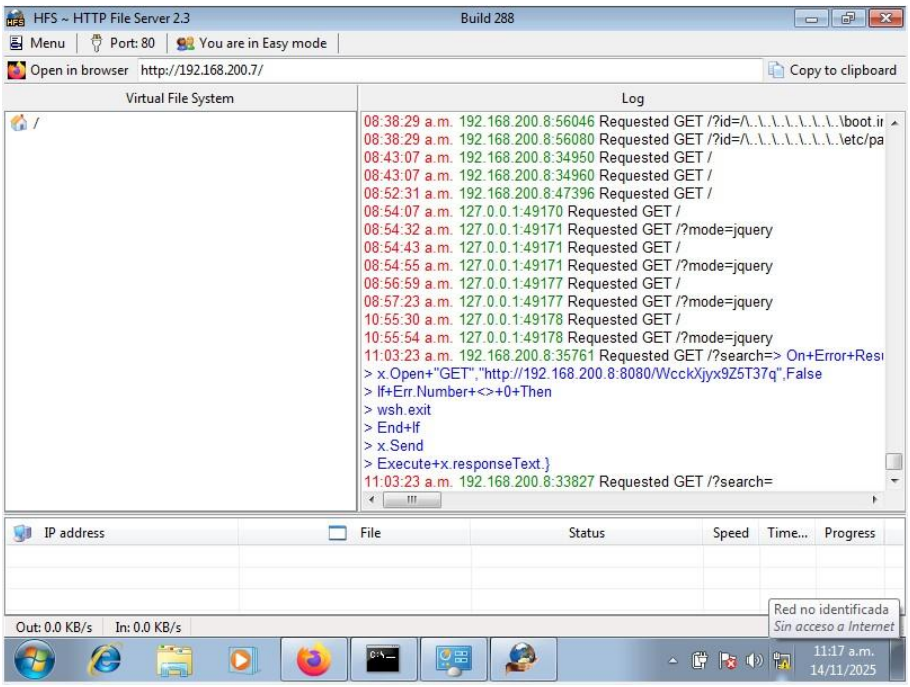
Fuente. Autoría Propia

Se puede ver en la imagen anterior cómo se lleva a cabo el ataque de denegación de servicio. Para ello, fueron empleados los siguientes comandos: set RHOSTS 192.168.200.7, que corresponde a la dirección IP objetivo; set RPORT 80, que equivale al puerto objetivo; y set TARGETURI, que establece la ruta concreta del sitio web. Luego de la configuración, nos presenta las líneas que señalan que se están mandando varias peticiones al servidor Apache del anfitrión objetivo (192.168.200.7) para agotar los recursos del servidor web y provocar el error

DoS de Apache Range Header, el cual congestiona la gestión de rangos HTTP y tiene el potencial de causar un bloqueo o una caída del servicio.

Figura 48

Interfaz gráfica del software HFS – HTTP File Server 2.3 (Build 288)

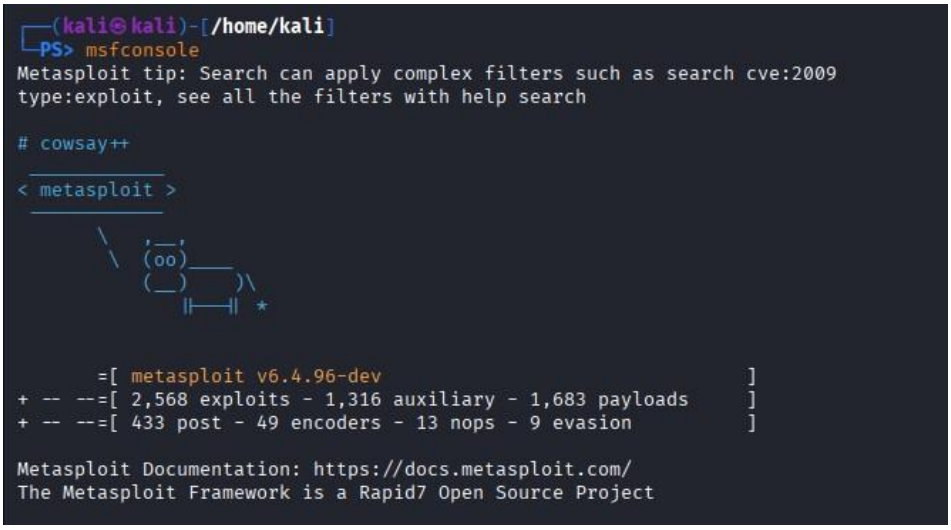


Fuente. Autoría Propia

Se puede ver en la imagen anterior el software HFS, con su interfaz gráfica, que muestra la realización del ataque de denegación de servicios. Cuando este proceso se haya completado, abriremos otra consola de Metasploit para vulnerar la máquina objetivo y crear un usuario con perfil administrativo.

Figura 49

Inicio herramientas Metasploit.

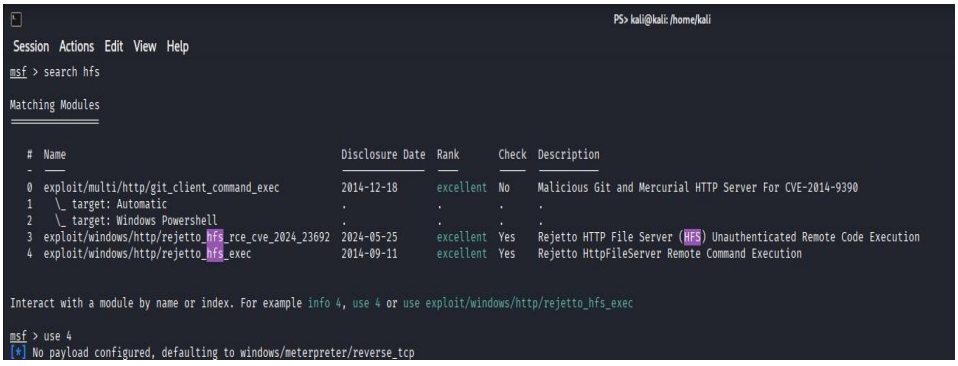


Fuente. Autoría Propia

El comienzo de la herramienta Metasploit se puede ver en la imagen anterior, donde se emplea el comando msfconsole desde la terminal de Kali Linux.

Figura 50

Ejecución comando search hfs



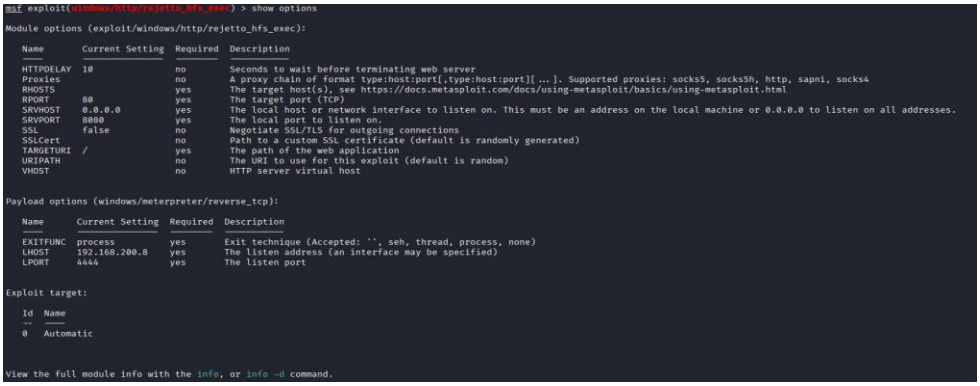
Fuente. Autoría Propia

La imagen anterior ilustra la ejecución del comando search hfs, que posibilitará la búsqueda de exploits. Metasploit devuelve una variedad de módulos, incluyendo dos exploits

relevantes para HFS: uno es más reciente (CVE-2024-23692) y el otro es más antiguo (CVE-2014-6287). Luego, se escoge el módulo rejetto_hfs_exec con use 4, y Metasploit automáticamente determina el payload por defecto (windows/meterpreter/reverse_tcp).

Figura 51

Ejecución show options

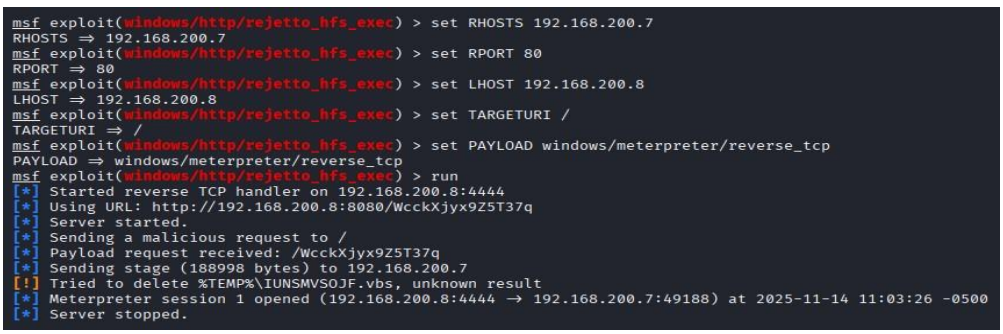


Fuente. Autoría Propia

La imagen precedente muestra que se lleva a cabo el comando show options, lo que permitirá visualizar los parámetros a considerar, como la dirección y puerto local de escucha, el tipo de payload usado y las opciones particulares de la conexión. De esta manera, se preparará para realizar un ataque remoto contra una máquina vulnerable.

Figura 52

Configuración ataque creación usuario

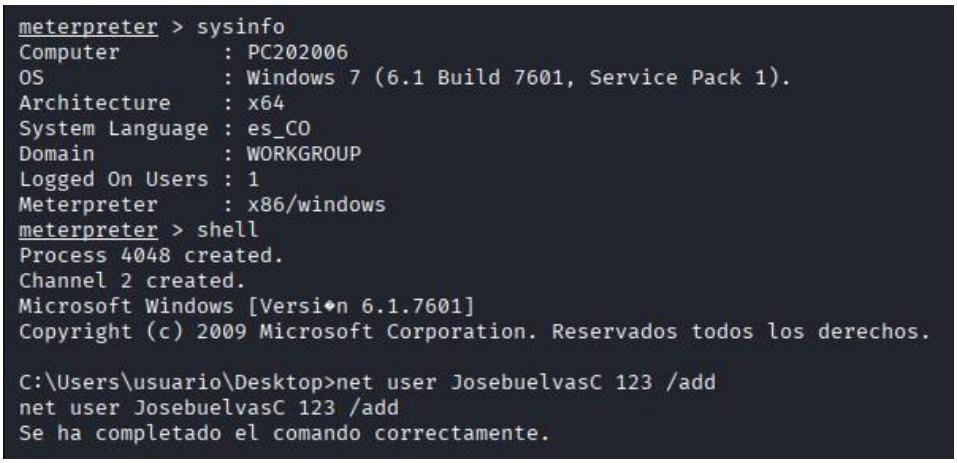


Fuente. Autoría Propia

En la imagen anterior cómo se ejecuta el exploit en Metasploit, usando el módulo "windows/http/rejetto_hfs_exec". Se identifican instrucciones para definir las opciones RHOSTS (la dirección del objetivo: 192.168.200.7), LHOST (la dirección local que recibe la conexión: 192.168.200.8), RPORT (puerto del servicio: 80), TARGETURI (ruta objetivo: /) y el payload "windows/meterpreter/reverse_tcp". Una vez que se ha configurado, el exploit ("run") se ejecuta y un handler TCP inverso se inicia en el puerto 4444, con la esperanza de conseguir una conexión del objetivo. Al terminar, el exploit logra establecer una sesión Meterpreter con la computadora objetivo (192.168.200.7) después de enviar una solicitud maliciosa, lo cual confirma que se ha realizado exitosamente un acceso remoto. Al final, el servidor se apaga y el proceso concluye correctamente.

Figura 53

Ejecución comando sysinfo verificación usuario



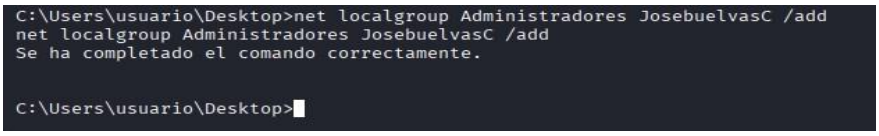
Fuente. Autoría Propia

La imagen precedente muestra que se lleva a cabo el comando show options, lo que permitirá visualizar los parámetros a considerar, como la dirección y puerto local de escucha, el tipo de payload usado y las opciones particulares de la conexión. De esta manera, se preparará para realizar un ataque remoto contra una máquina vulnerable. En la imagen previa se puede

observar una sesión activa en Meterpreter dentro de Metasploit, operando en un ordenador con Windows 7 (x64, Service Pack 1). El comando "net user JosebuelvasC 123 /add" se emplea en la terminal para establecer un nuevo usuario local que recibe el nombre de "JosebuelvasC" y tiene una contraseña "123". El sistema comprueba que el comando se ha llevado a cabo exitosamente, lo cual indica que el nuevo usuario fue agregado satisfactoriamente a la máquina víctima.

Figura 54

Creación de usuario JoseBuelvasC con privilegios

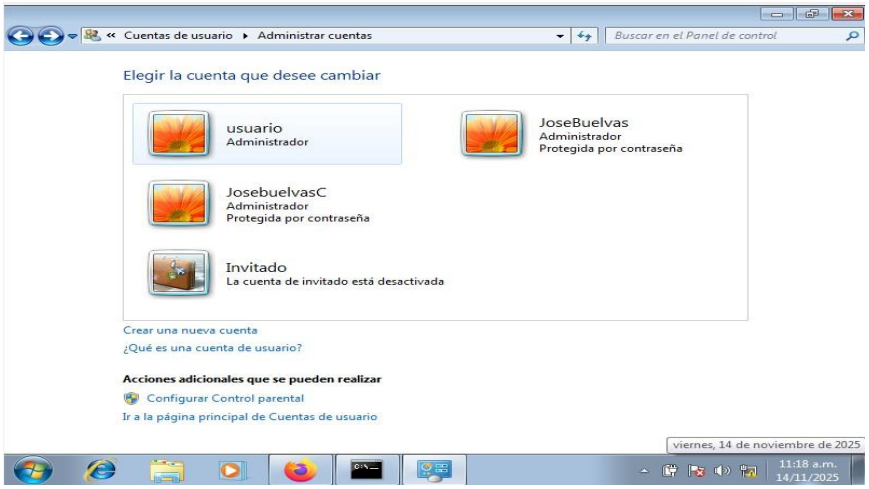


Fuente. Autoría Propia

En el anterior, se puede observar que en la máquina víctima se creó el usuario JoseBuelvasC con privilegios de administrador.

Figura 55

Creación de usuario JoseBuelvasC maquina Windows 7



Fuente. Autoría Propia

La anterior muestra que en la interfaz de la máquina virtual se creó el usuario JoseBuelvasC, quien tiene privilegios de administrador.

Figura 56

Eliminación de usuario JoseBuelvasC maquina Windows 7

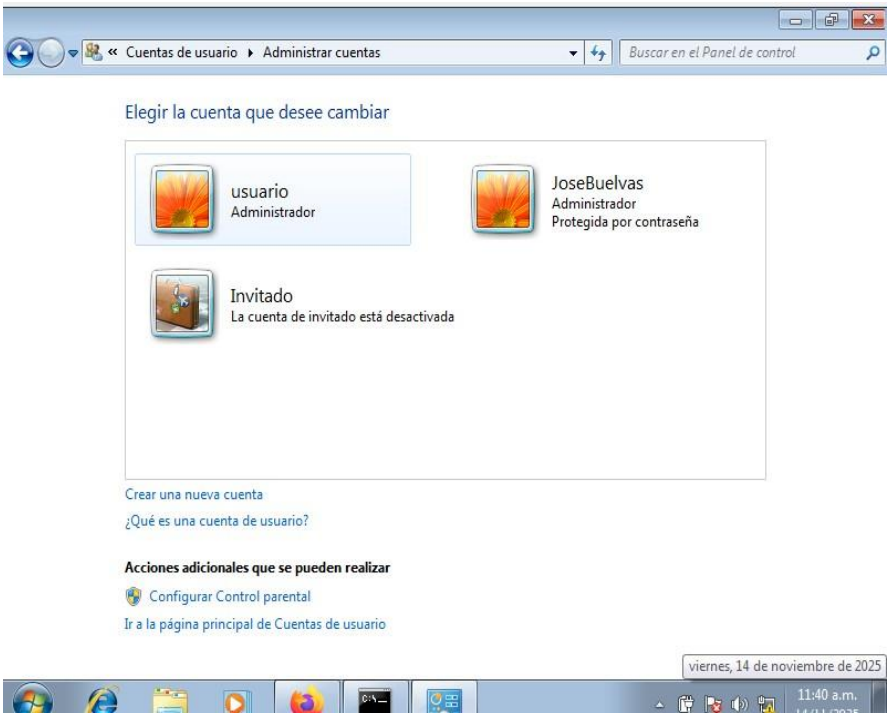
```
C:\Users\usuario\Desktop>net user JosebuelvasC /delete
net user JosebuelvasC /delete
Se ha completado el comando correctamente.
```

Fuente. Autoría Propia

La anterior muestra que en la interfaz de la máquina virtual se creó el usuario JoseBuelvasC, quien tiene privilegios de administrador.

Figura 57

Eliminación de usuario JoseBuelvasC interfaz maquina Windows 7



Fuente. Autoría Propia

Se puede observar en la anterior que el usuario JoseBuelvasC fue eliminado de la interfaz de la máquina virtual.

1)Herramientas y Comandos Utilizados – Escenario Red Team

Fase 1: Reconocimiento y Escaneo Inicia

En esta etapa se aplicó el programa Nmap, que es un software de código abierto utilizado para reconocer dispositivos y servicios en una red. Su método de escaneo permite encontrar puertos abiertos, servicios activos, versiones de software y sistemas operativos, lo que lo convierte en una herramienta esencial durante la fase de exploración, se utilizó el siguiente comando: *nmap -sS -sV -sC -O -T4 -p- 192.168.200.7*

Fase 2: Identificación y Validación de Vulnerabilidades

La fase de Identificación y Validación de Vulnerabilidades, apoyada en el uso combinado de Nmap (NSE) y Nessus, permitió obtener un diagnóstico preciso y confiable del estado de seguridad de la Máquina-1. Mientras Nmap proporcionó una exploración activa y detallada mediante scripts especializados capaces de detectar fallas críticas en servicios expuestos, Nessus complementó este análisis con una evaluación automatizada basada en bases de datos actualizadas de CVE, clasificando riesgos, severidades y configuraciones inseguras. La correlación de los resultados identificó dos vulnerabilidades altamente críticas —MS17-010 (EternalBlue) y CVE-2014-6287— que, combinadas con un sistema operativo desactualizado, la ausencia de firewall y servicios expuestos sin protección, configuraron un entorno susceptible a compromisos severos. Esta fase fue determinante, ya que no solo confirmó la existencia de debilidades explotables, sino que también estableció los vectores específicos que serían utilizados posteriormente en la fase de explotación con Metasploit, se utilizaron los siguientes comandos*: nmap --script vuln 192.168.200.7* se encarga de detectar vulnerabilidades generales

incluyendo HFS y SMB, comando *nmap --script smb-vuln-ms17-010 192.168.200.7* se utiliza para confirmar si el sistema es vulnerable al exploit EternalBlue (MS17-010) y el comando *nmap --script http-vuln-cve2014-6287 -p 80 192.168.200.7* el cual se utiliza para detectar la vulnerabilidad de Rejetto HFS 2.3 (CVE-2014-6287).

Fase 3: Explotación

La explotación del sistema objetivo fue completamente exitosa gracias a la correcta ejecución y secuencia de comandos dentro de Metasploit Framework. El proceso inició con *msfconsole,* que habilitó el entorno de explotación y permitió la selección del módulo adecuado mediante search hfs seguido de use 4, correspondiente al exploit para Rejetto HFS 2.3 (CVE-2014-6287). Posteriormente, la configuración precisa de los parámetros del objetivo, empleando comandos como set RHOSTS 192.168.200.7, set RPORT 80 y set TARGETURI, definió la ruta, el servicio vulnerable y la dirección IP afectada. Para establecer la vía de retorno del *payload*, se configuró también set LHOST, garantizando una sesión remota estable. La explotación se consolidó al ejecutar el módulo configurado, lo que permitió obtener una sesión Meterpreter en la Máquina-1. Con los comandos *sysinfo y shell* se verificó el acceso total al sistema operativo Windows 7 SP1, confirmando que la vulnerabilidad había sido aprovechada correctamente. A partir de allí, se realizaron acciones de post-explotación que evidencian el alcance total del compromiso: creación de un usuario persistente mediante *net user JoseBuelvasC 123 /add* y posterior limpieza del rastro de acceso con net user JoseBuelvasC /delete. El conjunto de comandos utilizados demuestra que el sistema carecía de controles de seguridad esenciales, lo que permitió ejecutar código remoto, establecer persistencia y operar sin restricciones dentro del sistema. Esta fase evidencia que la explotación fue posible debido a vulnerabilidades críticas no mitigadas y a la ausencia de medidas de protección como parches, firewall activo y

endurecimiento del sistema. La secuencia de acciones confirma un compromiso total de la confidencialidad, integridad y disponibilidad del equipo afectado.

2)Datos del Anexo 4 – Escenario 3 que ayudaron a identificar el fallo de seguridad

El error principal que se aprovechó fue la debilidad en el servidor HTTP Rejetto HFS 2.3, lo cual posibilitó la ejecución de código de forma remota (CVE-2014-6287). Esta debilidad, junto con la ausencia de actualizaciones en el sistema operativo y la desactivación del cortafuegos, facilitó un acceso completo a Máquina-1.

Asimismo, la información recogida en el Anexo 4 corroboró que la máquina presentaba múltiples vectores de exposición que incrementaron significativamente el riesgo de explotación. El sistema operativo Windows 7 SP1, sin soporte y con vulnerabilidades conocidas, los servicios inseguros como SMB y HTTP, la presencia del servidor HFS vulnerable, el firewall desactivado y los resultados de los escaneos de Nmap y Nessus confirmaron que el host era altamente susceptible a ataques remotos. En conjunto, estos elementos permitieron no solo identificar rápidamente el fallo principal, sino también validar que la máquina podía ser comprometida sin autenticación, permitiendo al atacante obtener una sesión Meterpreter de alto privilegio y establecer persistencia dentro del sistema.

3)Herramienta utilizada para detectar falla de seguridad.

El análisis de seguridad realizado sobre Máquina-1, mediante el uso del comando avanzado *nmap -sS -sV -sC -O -T4 -p- 192.168.200.7,* permitió identificar de forma precisa los vectores de ataque presentes en un sistema operativo altamente vulnerable como Windows 7. Este comando ejecuta un escaneo completo de todos los puertos TCP, empleando un SYN scan sigiloso (-sS), detección de versiones de servicios (-sV), ejecución de scripts NSE por defecto (-sC), y una estimación del sistema operativo (-O). Gracias a esta combinación de parámetros, fue posible obtener un panorama detallado de la superficie de exposición del host.

Los resultados del escaneo revelaron vulnerabilidades críticas que comprometen tanto la seguridad del sistema como su capacidad defensiva. En el servicio SMB, se identificó la presencia de MS17-010 (EternalBlue), una vulnerabilidad ampliamente documentada que permite ejecución remota de código sin autenticación. A nivel del servicio HTTP, se detectó el servidor Rejetto HFS 2.3, afectado por el fallo CVE-2014-6287, también capaz de permitir ejecución remota de comandos. Ambos hallazgos se consideran de alto impacto debido a que pueden explotarse de manera remota y automatizada.

La detección del servidor HFS 2.3 escuchando en el puerto 80, corroborada mediante el escaneo Nmap, fue particularmente relevante. Este servicio, señalado en los datos del Anexo, opera sin medidas de protección adicionales y permite al atacante enviar solicitudes especialmente diseñadas para activar el exploit correspondiente. Esta condición permitió que Metasploit ejecutara con éxito el módulo de explotación para HFS RCE, obteniendo acceso remoto directo al sistema comprometido.

En conjunto, el escaneo realizado no solo permitió identificar vulnerabilidades críticas, sino que también confirmó que la infraestructura carecía de mecanismos de protección como firewall activo, parches actualizados o restricciones en los servicios expuestos. Esta combinación de factores facilitó la explotación completa de Máquina-1, demostrando la efectividad del uso de Nmap en la fase de reconocimiento y validación técnica dentro de un escenario Red Team.

4)¿Cómo afecta el ataque a las máquinas Windows encontradas en la red?

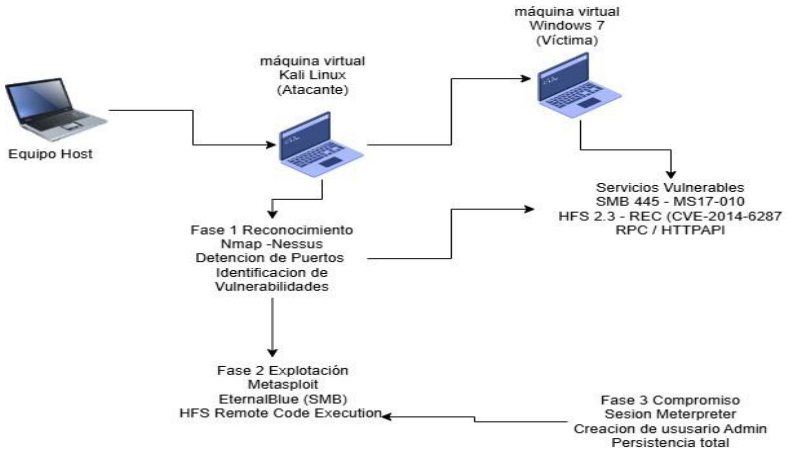
El ataque realizado por el Red Team afectó de manera crítica a las máquinas Windows de la red debido a la presencia de servicios vulnerables, configuraciones inseguras y un sistema operativo obsoleto. En el caso de Máquina-1 (Windows 7), el escaneo con Nmap y Nessus permitió identificar vulnerabilidades graves como MS17-010 (EternalBlue) en el servicio SMB y CVE-2014-6287 en el servidor HTTP Rejetto HFS 2.3.

Estas fallas pudieron explotarse de forma remota mediante Metasploit, permitiendo al atacante obtener una sesión Meterpreter con privilegios elevados. Con este acceso, se ejecutaron comandos directamente en el sistema, se creó un usuario persistente con rol administrativo y posteriormente se eliminaron rastros de las acciones realizadas para dificultar la detección.

En conjunto, el ataque comprometió totalmente la confidencialidad, integridad y disponibilidad de Máquina-1, demostrando que la ausencia de actualizaciones, la ejecución de servicios vulnerables y la desactivación del firewall facilitaron el acceso no autorizado y el control remoto absoluto del sistema.

Figura 58

Diagrama del Ataque



Fuente. Autoría Propia

El diagrama muestra el proceso completo del ataque realizado por el Red Team contra una máquina Windows 7 vulnerable. Desde una máquina virtual Kali Linux, el atacante inicia la Fase 1 de reconocimiento, utilizando Nmap y Nessus para detectar puertos abiertos y vulnerabilidades críticas como MS17-010 (EternalBlue) en SMB y CVE-2014-6287 en el servidor Rejetto HFS 2.3. Con esta información, se pasa a la Fase 2 de explotación, donde Metasploit se usa para ejecutar exploits remotos, logrando comprometer los servicios SMB y HTTP de la víctima mediante ejecución de código remoto.

Finalmente, en la Fase 3 de compromiso, el atacante obtiene una sesión Meterpreter, crea un usuario administrador persistente y asegura control total sobre la máquina Windows 7. El diagrama representa así el flujo de ataque desde el reconocimiento hasta la obtención de persistencia y el dominio completo del sistema.

Etapa 4 Respuesta y Contención ante Incidentes de Seguridad

1)Acciones iniciales ante un ataque en tiempo real (Equipo Blue Team)

Ante la detección de un ataque activo, el Blue Team debe ejecutar un conjunto de acciones críticas orientadas a identificar, contener y preservar evidencia del incidente sin comprometer la integridad del sistema. El primer paso consiste en determinar la naturaleza, el alcance y el origen del ataque, siguiendo metodologías formales de gestión de incidentes como las planteadas por Zambrano, Peña Hidalgo y Cárdenas Corral (2024).

Para ello, se inicia una inspección inmediata del tráfico de red y las conexiones activas, utilizando herramientas nativas como *netstat* -ano, lo cual permite identificar puertos explotados—por ejemplo 80/TCP asociado a Rejetto HFS o 445/TCP relacionado con SMB y la vulnerabilidad EternalBlue—además de conexiones no autorizadas vinculadas a *shells* reversos o *payloads* maliciosos. Conforme a la guía CCN-STIC-495 (2018), este análisis inicial de red es

fundamental para detectar explotación, movimiento lateral o persistencia remota dentro del sistema.

Posteriormente, se verifica la integridad del sistema operativo, revisando procesos activos, servicios relacionados con conexiones sospechosas y el estado de las cuentas locales mediante comandos como *tasklist /svc* y net user. Estas validaciones permiten identificar signos inequívocos de compromiso, tales como creación de usuarios administrativos no autorizados, procesos anómalos o módulos vinculados a actividades de explotación, coherente con lo planteado por Zambrano et al. (2024).

Una vez confirmado el compromiso, se procede con una contención inmediata, aislando el host sin apagarlo para evitar la pérdida de evidencia volátil. Esto puede lograrse deshabilitando la interfaz de red o trasladando el equipo a una VLAN de cuarentena, prácticas recomendadas por el CSIRT Académico UNAD (2024) para limitar la capacidad del atacante de seguir explotando el sistema o realizar exfiltración de datos.

Con el sistema ya controlado, se inicia la recolección de evidencia volátil, como memoria RAM, conexiones activas, procesos y registros del sistema, asegurando la cadena de custodia para facilitar un análisis forense riguroso. La preservación correcta de esta evidencia es uno de los pilares de la respuesta profesional a incidentes (Zambrano et al., 2024).

Finalmente, se procede a documentar detalladamente cada acción realizada, los hallazgos, las pruebas obtenidas y la posible causa raíz del incidente. Esto asegura la trazabilidad del proceso y se alinea con los lineamientos del CCN-STIC-495 (2018), permitiendo un análisis técnico preciso y transparente en etapas posteriores.

2)¿Qué medidas de hardenización propondría para que el ataque no se repita?

Para prevenir que el ataque vuelva a producirse, se requiere una estrategia de hardenización orientada a corregir las vulnerabilidades explotadas, mejorar la configuración del sistema y reducir la superficie de ataque. El compromiso del equipo Windows se originó por dos fallas críticas: Rejetto HFS (CVE-2014-6287) y EternalBlue (MS17-010), por lo que la mitigación debe iniciar con la aplicación inmediata de parches de seguridad, especialmente la actualización MS17-010. Según INCIBE (2019), mantener los sistemas actualizados es una de las medidas más efectivas para impedir ataques basados en vulnerabilidades conocidas.

Asimismo, es indispensable deshabilitar SMBv1, ya que es un protocolo obsoleto y altamente inseguro. De acuerdo con el CCN-STIC-495 (2018), retirar estándares inseguros y migrar a SMBv2/SMBv3 reduce significativamente el riesgo de explotación remota. Paralelamente, debe habilitarse y reforzarse el firewall del sistema, aplicando reglas restrictivas para evitar accesos no autorizados a puertos críticos como 445/TCP y 80/TCP, alineado con las recomendaciones de CIS Security (2020).

Otra medida esencial es actualizar o eliminar el servidor vulnerable Rejetto HFS 2.3, ya que su vulnerabilidad de ejecución remota permite un control total del sistema. También se debe eliminar cualquier cuenta creada por el atacante y revisar los privilegios administrativos, aplicando el principio de mínimo privilegio, tal como sugieren Zambrano et al. (2024).

Para garantizar una configuración segura de forma integral, se recomienda aplicar los CIS Benchmarks para Windows 7, que incluyen la desactivación de servicios innecesarios, políticas estrictas de contraseñas, auditorías avanzadas y controles de permisos. CIS Security (2020) documenta que estas pautas mitigan un porcentaje significativo de ataques comunes.

Finalmente, debido a que Windows 7 está en estado *End of Life*, se sugiere su reemplazo por un sistema operativo con soporte vigente, ya que la falta de actualizaciones convierte al equipo en un objetivo atractivo para atacantes.

3)¿Cuáles son las diferencias entre un equipo Blue Team y un equipo de Respuesta a Incidentes?

Las diferencias entre un Blue Team y un equipo de Respuesta a Incidentes se basan en su misión, enfoque operacional y momento de intervención dentro del ciclo de defensa organizacional. El Blue Team se encarga de la defensa proactiva y continua, orientada a prevenir ataques mediante actividades de monitoreo, análisis de vulnerabilidades, hardening, revisión de configuraciones e implementación de controles de seguridad como los CIS Benchmarks. Rapid7, Jyothi y Karri (2011) señalan que su función principal es mantener la integridad, disponibilidad y confiabilidad de los sistemas, fortaleciendo la postura de seguridad diariamente.

En contraste, el CSIRT/IRT actúa de manera reactiva, interviniendo únicamente cuando un incidente ya ha ocurrido o está en curso. Su labor consiste en identificar, contener, erradicar y recuperar los sistemas afectados siguiendo procesos formales definidos en metodologías como las de Zambrano, Peña Hidalgo y Cárdenas Corral (2024) y el estándar NIST 800-61. Este equipo aplica técnicas de análisis forense, recolección de evidencia, evaluación de impacto y restauración de servicios para minimizar daños y restablecer la operación normal.

Mientras el Blue Team trabaja permanentemente para reducir la probabilidad de un ataque exitoso, el CSIRT/IRT interviene para mitigar sus consecuencias cuando el ataque supera las defensas. Tal como indica la guía CCN-STIC-495 (2018), ambos roles se complementan: uno protege de manera continua y el otro actúa ante eventos críticos, permitiendo un ciclo integral de defensa y resiliencia organizacional.

4)¿Para qué utilizaría CIS (Center for Internet Security) dentro de un equipo Blue Team?

El Center for Internet Security (CIS) es una herramienta esencial para el Blue Team, ya que proporciona estándares internacionales de configuración segura que permiten reducir la superficie de ataque, fortalecer la infraestructura tecnológica y prevenir incidentes antes de que ocurran. Según CIS Security (2020), sus Benchmarks ofrecen guías detalladas y validadas para asegurar sistemas operativos, dispositivos de red y aplicaciones críticas, convirtiéndose en un elemento clave de la defensa proactiva.

Dentro del Blue Team, el CIS se utiliza principalmente para aplicar medidas de hardening, deshabilitando servicios innecesarios, reforzando políticas de autenticación, activando auditorías avanzadas y configuraciones de seguridad estrictas. INCIBE (2019) destaca que muchas intrusiones exitosas se relacionan directamente con configuraciones débiles o no actualizadas, por lo que el uso del CIS contribuye a mitigar este tipo de vulnerabilidades.

Asimismo, el CIS permite definir líneas base de seguridad, garantizando que todos los sistemas mantengan niveles mínimos y uniformes de protección. Esto facilita la detección de configuraciones incorrectas o desviaciones que representen riesgos adicionales. Igualmente, el Blue Team emplea los Benchmarks para realizar evaluaciones de cumplimiento, verificando que los equipos se ajusten a las mejores prácticas y apoyando auditorías internas, como lo recomienda Zambrano, Peña Hidalgo y Cárdenas Corral (2024).

Finalmente, el uso de los CIS Controls ayuda a reducir significativamente la superficie de ataque, especialmente mediante controles relacionados con inventarios de activos, gestión de vulnerabilidades y configuraciones seguras. CIS Security (2020) señala que la implementación adecuada de estos controles puede prevenir más del 80% de los ataques comunes, demostrando su relevancia operativa dentro del Blue Team.

5)Funciones y características principales de un SIEM

Un SIEM (Security Information and Event Management) es una plataforma centralizada que permite gestionar y analizar eventos de seguridad provenientes de múltiples dispositivos para detectar amenazas en tiempo real. Según Moreno (2015), su función principal es unificar, procesar y correlacionar grandes volúmenes de logs generados por firewalls, servidores, aplicaciones, redes y endpoints, ofreciendo una visión global del entorno tecnológico.

Entre sus funciones esenciales se encuentra la recolección y centralización de logs, donde el SIEM recopila eventos de distintos sistemas, los normaliza y los almacena de forma organizada, facilitando al analista la detección de comportamientos anómalos que serían difíciles de identificar de manera individual. Otra función clave es la correlación de eventos, que permite analizar eventos aislados y combinarlos para identificar patrones de ataque, convirtiendo registros simples en información contextualizada que genera alertas oportunas.

El SIEM también ofrece alertas en tiempo real, lo que permite al Blue Team responder rápidamente ante comportamientos sospechosos, reduciendo el impacto de los incidentes, tal como lo recomienda el CSIRT Académico UNAD (Zambrano et al., 2024). Asimismo, integra capacidades de análisis histórico y forense, esenciales para reconstruir la secuencia de un ataque, determinar su origen y documentar la evidencia de manera fiable.

Entre sus características técnicas destacan la normalización de datos, la integración con inteligencia de amenazas (Threat Intelligence), dashboards visuales, reportes automatizados y, en soluciones modernas, capacidades de automatización para respuesta (SOAR). Además, el SIEM contribuye al cumplimiento normativo, facilitando auditorías y reportes alineados con marcos como ISO 27001, GDPR o las guías CCN-STIC.

En conjunto, un SIEM es una herramienta fundamental para la defensa organizacional, al permitir la detección temprana de amenazas, el análisis profundo de incidentes y el fortalecimiento de la gobernanza en ciberseguridad.

6)¿Herramientas de contención de ataques informáticos (hardware o software)

Las herramientas de contención permiten detener o limitar un ataque en curso, evitando su propagación y reduciendo el impacto sobre los sistemas afectados. A diferencia de las herramientas de detección, su función principal es intervenir activamente durante un incidente. Según Zambrano, Peña Hidalgo y Cárdenas Corral (2024), la contención es una fase esencial dentro de la respuesta a incidentes, pues busca preservar la estabilidad operativa y minimizar daños.

Entre las herramientas más relevantes se encuentran los firewalls UTM o Next-Generation Firewalls, que bloquean tráfico malicioso, cierran puertos vulnerables y permiten segmentar o aislar redes comprometidas. Su uso impide conexiones sospechosas y frena el movimiento lateral del atacante, como recomiendan las guías del CCN-CERT (2018).

Otra herramienta fundamental son los EDR o HIDS con capacidades de contención, los cuales permiten aislar endpoints, detener procesos maliciosos, bloquear archivos sospechosos y evitar la ejecución de payloads o malware. Estas soluciones facilitan una respuesta directa ante el ataque, actuando sobre el equipo comprometido de manera automatizada o manual.

Finalmente, las herramientas de control de aplicaciones, como AppLocker o SRP, bloquean la ejecución de software no autorizado mediante listas blancas, lo que evita la ejecución de scripts, binarios o exploits utilizados por el atacante. Según CIS Security (2020), este enfoque reduce significativamente la capacidad del adversario para ejecutar herramientas maliciosas o mantener persistencia.

En conjunto, estas herramientas constituyen mecanismos eficaces de contención activa, permitiendo interrumpir la comunicación del atacante, detener procesos peligrosos o impedir la ejecución de código malicioso, alineándose con las buenas prácticas de contención definidas por el CSIRT Académico UNAD y los controles de seguridad recomendados por CIS.

Etapa 5: Análisis, Reporte y Comunicación de Resultados Técnicos

Evidencias de Sustentación

Video de sustentación del informe final: https://youtu.be/l2EGUi0E_JE

Conclusiones

La Etapa 1 estableció las bases teóricas y prácticas necesarias para entender cómo se relacionan los ataques y la defensa en el ámbito de la ciberseguridad. Se demostró que una revisión eficaz de la situación de seguridad demanda tanto métodos de reconocimiento y recopilación de información (OSINT, escaneos activos) como una adecuada elección de herramientas y enfoques para cada etapa del pentesting. La organización del banco de trabajo y la preparación de entornos virtuales mostraron que la capacidad de repetir experimentos y el aislamiento son elementos esenciales para llevar a cabo pruebas seguras y controladas. Como conclusión fundamental, esta fase destaca que la preparación (incluyendo planificación, alcance y consideraciones éticas) es tan crucial como la ejecución técnica; sin una estrategia clara y límites definidos, las pruebas pueden acarrear problemas legales y operativos. Recomendación: establecer procesos formales de planificación y supervisión en el laboratorio que incluyan normas, autorizaciones y registros de actividades antes de realizar ejercicios ofensivos.

La Etapa 2 demostró que la dimensión ética y normativa está unida al trabajo técnico en el campo de la ciberseguridad. El estudio del caso (SecureNova Labs) reveló que cláusulas contractuales mal redactadas pueden dar pie a acciones ilegales o poner en riesgo la situación laboral del profesional; de igual forma, se detectaron varias leyes colombianas (Ley 1273, Ley 1581, decretos) que establecen límites en cuanto a responsabilidades y prohibiciones. La conclusión más importante es que llevar a cabo prácticas técnicas sin un entendimiento profundo de la legalidad y la ética aumenta la probabilidad de causar daño social y enfrenta a las personas a consecuencias penales. Sugerencia: implementar capacitación obligatoria en temas de ética, legislación y responsabilidad contractual para todo el personal involucrado en pruebas de intrusión o análisis forense, así como establecer procedimientos internos para la revisión legal antes de formalizar contratos con terceros.

En la Fase 3 se llevaron a cabo pruebas en un entorno controlado para validar vectores de ataque reales y evaluar la efectividad de herramientas como Nmap, Nessus y Metasploit. Las explotaciones exitosas (MS17-010 / EternalBlue y Rejetto HFS CVE-2014-6287) mostraron que los sistemas desactualizados, los servicios vulnerables y los firewalls apagados crean una superficie de ataque que permite el compromiso completo del host (acceso a sesión Meterpreter y persistencia). El ejercicio demostró que la combinación de reconocimiento, escaneo automatizado y explotación modular facilita una intrusión que se puede repetir y medir. Lección importante: la existencia de sistemas sin soporte y configuraciones deficientes es el riesgo más común. Sugerencia: dar prioridad a un programa de gestión de actualizaciones, un inventario de recursos y la reducción de servicios expuestos como acciones inmediatas para mitigar riesgos.

La Etapa 4 evidenció la relevancia de tener una reacción organizada, enfocada en preservar pruebas, contener sin apagar los sistemas, y realizar una documentación cuidadosa. Las medidas de identificación (como netstat, revisión de procesos y cuentas), aislamiento (con VLAN o cuarentena), recopilación de pruebas volátiles y el análisis forense posterior son acciones esenciales para minimizar el daño y facilitar la atribución técnica. También se constató que la implementación de estándares (CIS Benchmarks) y herramientas (como SIEM para correlaciones, EDR y NGFW para contención) es fundamental para mejorar la madurez en la defensa. Enseñanza práctica: la habilidad para gestionar eficazmente un incidente en escenarios con recursos escasos se basa más en un buen manejo de los procedimientos que en tener únicamente herramientas comerciales a disposición. Sugerencia: crear y practicar planes de respuesta (playbooks) que incorporen procedimientos de contención utilizando herramientas gratuitas y nativas, además de mantener un programa continuo de fortificación alineado a los estándares de CIS.

Recomendaciones

Con base en los hallazgos identificados durante el desarrollo del ejercicio académico, las pruebas de intrusión realizadas por el Red Team, las acciones de detección y contención ejecutadas por el Blue Team y el análisis del marco ético y normativo, se formulan las siguientes recomendaciones orientadas a mejorar la seguridad de la información desde los niveles técnico, táctico y organizacional, con el fin de reducir los riesgos detectados y fortalecer la postura de ciberseguridad institucional.

Recomendaciones técnicas: Se recomienda actualizar y modernizar los sistemas operativos y servicios expuestos en la infraestructura tecnológica, eliminando el uso de plataformas obsoletas como Windows 7, las cuales ya no cuentan con soporte oficial y presentan vulnerabilidades críticas ampliamente documentadas, como MS17-010 (EternalBlue). La permanencia de sistemas sin parches incrementa significativamente el riesgo de ejecución remota de código y compromete la confidencialidad, integridad y disponibilidad de la información (Microsoft, 2017; National Institute of Standards and Technology [NIST], 2020).

Asimismo, es indispensable implementar procesos de hardening basados en estándares internacionales, especialmente los CIS Benchmarks, orientados a deshabilitar servicios innecesarios, protocolos inseguros como SMBv1, configuraciones por defecto y cuentas con privilegios excesivos. Estas prácticas reducen la superficie de ataque y fortalecen la postura de seguridad frente a amenazas conocidas y emergentes.

De igual forma, se recomienda fortalecer las capacidades de detección y monitoreo mediante la integración de soluciones SIEM, EDR y firewalls de nueva generación, que permitan la correlación de eventos, la identificación temprana de comportamientos anómalos y la contención automatizada de incidentes. El monitoreo continuo de registros del sistema y del

tráfico de red resulta fundamental para detectar ataques en fases iniciales y minimizar su impacto operativo (Moreno, 2015; NIST, 2022).

Finalmente, se sugiere aplicar segmentación de red y controles de acceso bajo el principio de mínimo privilegio, con el fin de limitar el movimiento lateral de los atacantes una vez comprometido un activo, práctica recomendada para reducir el alcance de los incidentes de seguridad y aumentar la resiliencia de la infraestructura tecnológica, en concordancia con el enfoque de gestión de incidentes definido en la norma ISO/IEC 27035:2016 y sustentado en el modelo propuesto por Salinas Pérez (2025).

Recomendaciones tácticas: Desde una perspectiva táctica, se recomienda formalizar y documentar procedimientos claros de respuesta a incidentes, alineados con marcos de referencia como NIST SP 800-61 e ISO/IEC 27035, que definan roles, responsabilidades, flujos de comunicación y tiempos de actuación ante eventos de seguridad. La ausencia de estos procedimientos incrementa el tiempo de respuesta y dificulta la contención efectiva de los ataques (NIST, 2018; ISO/IEC, 2016).

Adicionalmente, se aconseja realizar ejercicios periódicos de simulación que integren operaciones Red Team y Blue Team, con el propósito de evaluar la efectividad de los controles implementados, mejorar la coordinación operativa y fortalecer las capacidades del personal técnico. Estas prácticas permiten identificar brechas reales de seguridad y fomentan la mejora continua de los procesos de defensa (Arroyo, 2025).

Asimismo, se recomienda reforzar las capacidades de análisis forense digital, garantizando la adecuada preservación de evidencias, la trazabilidad de las acciones ejecutadas y la correcta documentación de los incidentes. Estas acciones resultan esenciales tanto para la toma de decisiones técnicas como para el soporte de procesos legales y disciplinarios derivados de eventos de seguridad (Casey, 2011).

Recomendaciones organizacionales: A nivel organizacional, se recomienda fortalecer el gobierno de la seguridad de la información mediante la definición y actualización de políticas que regulen el acceso a los sistemas, el uso de herramientas de ciberseguridad y la gestión de la información sensible. Dichas políticas deben alinearse con la normativa colombiana vigente, en particular la Ley 1273 de 2009 y la Ley 1581 de 2012, con el fin de garantizar el cumplimiento legal y la protección de los datos personales (Congreso de la República de Colombia, 2009; Congreso de la República de Colombia, 2012).

Se sugiere crear o consolidar un CSIRT institucional que trabaje de manera articulada con el Blue Team, asegurando una gestión integral de los incidentes desde la detección hasta la recuperación y la mejora posterior. La existencia de equipos formales de respuesta incrementa la madurez organizacional y reduce el impacto de los eventos de seguridad (ENISA, 2023).

Se sugiere crear o consolidar un CSIRT institucional que trabaje de manera articulada con el Blue Team, asegurando una gestión integral de los incidentes desde la detección hasta la recuperación y la mejora posterior. La existencia de equipos formales de respuesta incrementa la madurez organizacional y reduce el impacto de los eventos de seguridad (ENISA, 2023).

Finalmente, se recomienda establecer mecanismos de supervisión, auditoría y rendición de cuentas sobre las actividades de seguridad informática, incluyendo canales de denuncia seguros y procesos de evaluación periódica de proveedores. Estas medidas favorecen la transparencia, previenen abusos y fortalecen la confianza institucional en la gestión de la seguridad de la información (Guarnizo Portela, 2024).

Referencias Bibliográficas

Arroyo, E. (2025). *Sinergia de Equipos Red Team y Blue Team en la Protección de Entornos Corporativos.* https://repository.unad.edu.co/handle/10596/74595

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.* https://engineering.nyu.edu/sites/default/files/2020-09/CS-GY%206963%20Digital%20Forensics.pdf

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

Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información* https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoración_y_evaluación_de_riesgos_de_ciberseguridad__Pag_publicado.pdf

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

Congreso de la República de Colombia. (1991). *Constitución Política de Colombia.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Congreso de la República de Colombia. (2008) *Ley estatutaria 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información.* http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congreso de la República de Colombia. (2008) *Ley estatutaria 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.* http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal en materia de delitos informáticos.* http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2012). *Ley estatutaria 1581 de 2012* http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la República de Colombia. (2013) *Ley estatutaria 1621 de 2013 Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones"* http://www.secretariasenado.gov.co/senado/basedoc/ley_1621_2013.html

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

Ministerio de Comercio, Industria y Turismo. (2022). *Decreto 255 del 23 de febrero de 2022, por el cual se adiciona la Sección 7 al Capítulo 25 del Ministerio de Comercio, Industria y Turismo*. https://www.mincit.gov.co/normatividad/decretos/2022/decreto-255-del-23-de-febrero-de-2022

Fortinet. (2024). *What is Common Vulnerabilities and Exposures (CVE)? Fortinet Cyber Glossary.* https://www.fortinet.com/lat/resources/cyberglossary/cve

Greenbone Community Documentation. (2025). *Architecture of Greenbone Community Edition and OpenVAS Scanner.* https://greenbone.github.io/docs/latest/architecture.html

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia [Monografía de pregrado,* https://repository.unad.edu.co/handle/10596/41392

INCIBE. (2019). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas. Instituto Nacional de Ciberseguridad.* https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas

Microsoft Corporation. (2017). *Security bulletin MS17-010: Vulnerabilities in Microsoft Windows SMB Server.* https://learn.microsoft.com/en-us/security-updates/Securitybulletins/2017/ms17-010

Microsoft. (2017). *Security Bulletin MS17-010 – Critical. Microsoft.* https://learn.microsoft.com/en-us/security-updates/Securitybulletins/2017/ms17-010

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

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

National Institute of Standards and Technology. (2018). *Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). U.S. Department of Commerce.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology. (2020). *Guide to enterprise patch management technologies (SP 800-40 Rev. 3/R4).* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

National Institute of Standards and Technology. (2020). *Guide to enterprise patch management technologies (NIST Special Publication 800-40 Rev. 3). U.S. Department of Commerce.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

National Institute of Standards and Technology. (2022). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). U.S. Department of Commerce.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

OWASP Foundation. (2023). *OWASP Web Security Testing Guide (versión online). The OWASP Foundation.* https://owasp.org/www-project-web-security-testing-guide/latest/

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

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

Salinas Perez, J. *Modelo de gestión de incidentes de seguridad de información para una entidad estatal peruana que gestiona desastres, con base en la norma ISO/IEC 27035: 2016.* https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/667940/Salinas_PJ.pdf?sequence=17

SANS Institute. (2021). *Penetration testing: Overview of the process and stages. SANS Institute.* https://www.sans.org/security-resources/glossary-of-terms/penetration-testing

Superintendencia de Industria y Comercio. (2025, agosto 11). *Gobierno nacional impulsa reforma clave de la Ley de Protección de Datos Personales en Colombia.* https://sedeelectronica.sic.gov.co/noticias/gobierno-nacional-impulsa-reforma-clave-de-la-ley-de-proteccion-de-datos-personales-en-colombia

Universidad Carlos III de Madrid. (2025). *Herramientas de análisis: Metasploit (Trabajo académico).* https://e-archivo.uc3m.es/bitstreams/309357e2-bb2c-47a0-bd74-79ea6e4b6f71/download

Universidad Estatal Península de Santa Elena. (2025). *Uso de la herramienta Nmap para el análisis y escaneo de redes (Trabajo académico). Repositorio institucional.* https://repositorio.upse.edu.ec/bitstream/46000/12932/1/UPSE-TTE-2025-0005.pdf

Wikipedia contributors. (2025). *ExploitDB. En Wikipedia, The Free Encyclopedia. Recuperado de* https://en.wikipedia.org/wiki/ExploitDB

Zambrano Hernández, L. F., Peña Hidalgo, H. J., & Cárdenas Corral, J. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad. Sello Editorial UNAD.*

Zhang, W., Xing, J., & Li, X. (2025). *Penetration testing for system security: Methods and practical approaches. arXiv.* https://arxiv.org/abs/2505.19174

Apéndices

Apéndice A

Resultado de revisión en Turnitin