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

Camilo Andres Joya Gutierrez

Asesor

Luis Fernando Zambrano

Universidad Nacional abierta y a distancia-UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

Seminario Especializado

Junio de 2025

Esta página opcional

_____

Nombre Director de Trabajo de Grado

_____ _____

Jurado Jurado

2025

Dedicatoria

Dedico este trabajo a mi familia, quienes han sido mi mayor fuente de apoyo, motivación y paciencia a lo largo de este proceso de formación. A cada uno de ellos, gracias por confiar en mí y brindarme la fortaleza necesaria para continuar y alcanzar cada objetivo. También dedico este logro a todos los profesionales que, con ética y compromiso, contribuyen diariamente a construir un entorno digital más seguro para las organizaciones y las personas.

Agradecimientos

Agradezco en primer lugar a Dios por darme la salud, la disciplina y la perseverancia para culminar esta etapa.

Extiendo mi agradecimiento a los docentes y tutores del seminario, cuyo conocimiento, orientación y exigencia académica fueron clave para mi crecimiento profesional en el área de la ciberseguridad.

Agradezco también a mis compañeros de formación, con quienes compartí aprendizajes, dudas, experiencias y colaboraciones que enriquecieron significativamente este proceso.

Contenido

Lista de Tablas

Lista de Figuras

Glosario

Término	Definición
Ataque informático	Acción deliberada para comprometer la confidencialidad, integridad o disponibilidad de sistemas de información.
Blue Team	Equipo de seguridad encargado de la defensa de la infraestructura TI, el monitoreo, la detección y la contención de incidentes.
Red Team	Equipo de ciberseguridad ofensiva que simula ataques reales para evaluar la efectividad de las defensas de la organización.
Ciberseguridad	Conjunto de técnicas, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos frente a ataques digitales.
Contención	Conjunto de acciones destinadas a frenar o aislar un ataque en curso para minimizar su impacto en la infraestructura tecnológica.
MS17-010 / EternalBlue	Vulnerabilidad crítica en sistemas Windows que permite ejecución remota de código a través del protocolo SMBv1. Explotada por herramientas como WannaCry.
SMBv1	Protocolo de red obsoleto para el intercambio de archivos, vulnerable a múltiples ataques como EternalBlue.
Metasploit	Framework de pruebas de penetración que permite a los Red Teams ejecutar exploits, payloads y módulos de post-explotación.
Meterpreter	Shell avanzada que se utiliza dentro de Metasploit para controlar un sistema comprometido, permitiendo ejecución remota de comandos y captura de información.
Wireshark	Herramienta de análisis de tráfico de red que permite visualizar paquetes y detectar comportamientos maliciosos en tiempo real.
Snort	Sistema de detección de intrusos (IDS) que analiza el tráfico de red para identificar patrones asociados a amenazas o ataques.
TCPView	Herramienta de Microsoft que muestra en tiempo real las conexiones de red y los procesos asociados en un sistema Windows.
Chainsaw	Herramienta forense para analizar registros de eventos de Windows utilizando técnicas de detección basadas en Sigma rules.
Hardening	Proceso de reforzamiento de la seguridad de un sistema mediante la desactivación de servicios innecesarios, actualizaciones y configuración segura.
SIEM (Security Information and Event Management)	Plataforma que centraliza, analiza y correlaciona eventos de seguridad generados por distintos dispositivos en una red.

Nmap	Herramienta utilizada para escanear redes, descubrir hosts activos, puertos abiertos y servicios.
IDS (Intrusion Detection System)	Sistema que monitorea el tráfico de red o sistema en busca de comportamientos anómalos o no autorizados.
Actuación ética	Conjunto de principios y normas que deben seguir los profesionales de ciberseguridad en la ejecución de simulaciones, análisis forense y pruebas de penetración.
Responsabilidad legal	Obligación de actuar bajo el marco jurídico vigente, garantizando el respeto a la privacidad, integridad y propiedad de los sistemas evaluados.
Análisis forense	Técnica que permite recolectar, preservar y examinar evidencia digital posterior a un incidente de seguridad.
Vulnerabilidad	Debilidad o falla en un sistema que puede ser explotada por un atacante para comprometer su seguridad.
Payload	Código malicioso que se ejecuta tras la explotación de una vulnerabilidad, permitiendo acciones como acceso remoto o exfiltración de datos.
Reverse Shell	Técnica que permite al atacante establecer una conexión desde el sistema víctima hacia su propio sistema para obtener control.
Firewall	Mecanismo de seguridad que controla el tráfico entrante y saliente según reglas definidas, bloqueando conexiones no autorizadas.
SMB (Server Message Block)	Protocolo de red para compartir archivos e impresoras entre dispositivos en una red. Su versión 1 es insegura.
CIS Benchmarks	Guías de configuración segura desarrolladas por el Center for Internet Security para proteger sistemas operativos y aplicaciones.

Resumen

Este informe presenta el análisis técnico de los escenarios abordados en los ejercicios de Blue Team y Red Team durante el seminario de Ciberseguridad. A través de la simulación de ataques reales como el exploit EternalBlue (MS17-010) y el despliegue de herramientas defensivas como Wireshark, Snort y hardening del sistema operativo Windows, se evaluaron vulnerabilidades críticas y se formularon estrategias de contención eficaces. El informe concluye con recomendaciones prácticas orientadas a mejorar la postura de seguridad de una organización desde un enfoque ofensivo y defensivo.

***Palabras clave*:** Blue Team, IDS, Meterpreter, Red Team, SMBv1.

Abstract

This report presents the technical analysis of the scenarios addressed in the Blue Team and Red Team exercises during the Cybersecurity seminar. Through the simulation of real attacks such as the EternalBlue exploit (MS17-010) and the deployment of defensive tools such as Wireshark, Snort and Windows OS hardening, critical vulnerabilities were evaluated and effective containment strategies were formulated. The report concludes with practical recommendations aimed at improving an organization's security posture from both an offensive and defensive approach.

Keywords**:** Blue Team, IDS, Meterpreter, Red Team, SMBv1.

Introducción

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en una necesidad urgente más que en una opción. Las amenazas informáticas son cada vez más sofisticadas, y las organizaciones deben estar preparadas para enfrentarlas no solo desde la defensa, sino también desde la comprensión profunda de cómo piensan y actúan los atacantes. Por ello, abordar la ciberseguridad desde un enfoque integral implica desarrollar habilidades tanto defensivas (Blue Team) como ofensivas (Red Team).

Este informe recopila las actividades realizadas durante un proceso de formación especializado, centrado en simular escenarios reales de ataque y defensa. A través de la práctica con herramientas como Metasploit, Wireshark, Snort y otras soluciones de código abierto, fue posible experimentar cómo se ejecutan ataques conocidos —como el basado en la vulnerabilidad MS17-010 (EternalBlue)— y cómo contenerlos mediante estrategias técnicas, análisis forense y endurecimiento de sistemas.

Una parte esencial de este proceso fue aplicar el pensamiento adversarial, es decir, aprender a pensar como un atacante para anticiparse a sus acciones y fortalecer las defensas de los sistemas. Esta mentalidad permite diseñar respuestas más efectivas, identificar puntos débiles antes de que sean explotados, y mejorar continuamente las políticas y configuraciones de seguridad.

El propósito de este informe no es solo mostrar los resultados de las prácticas, sino también reflexionar sobre la importancia de combinar análisis técnico, criterio estratégico y ética profesional para enfrentar los desafíos actuales en seguridad informática.

Objetivos

Objetivo General

Formular estrategias efectivas de ciberseguridad mediante la simulación y análisis de ataques reales, para fortalecer la infraestructura tecnológica de una organización.

Objetivos Específicos

- Simular un ataque real utilizando la vulnerabilidad MS17-010 desde un entorno Red Team.
- Implementar y validar acciones de detección y contención desde el enfoque Blue Team.
- Evaluar herramientas de análisis forense, captura de red y defensa activa.
- Proponer recomendaciones que fortalezcan la seguridad basada en la experiencia del laboratorio.

Desarrollo del informe

Etapa 1 – Conceptos equipos de Seguridad

Legislación en Colombia sobre delitos informáticos y protección de datos personales

En Colombia, el crecimiento exponencial del uso de internet ha traído consigo un aumento en los riesgos asociados a los delitos informáticos. En respuesta, el país ha establecido un marco normativo que busca proteger tanto la información digital como los datos personales de los ciudadanos.

Una de las leyes más relevantes en este ámbito es la Ley 1273 de 2009, que modificó el Código Penal colombiano e incorporó un nuevo bien jurídico tutelado: la protección de la información y de los datos. Esta ley introdujo el Título VII BIS en el Código Penal, bajo el nombre de "De la protección de la información y de los datos", y estableció sanciones específicas para conductas como el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones, el daño informático y el uso de software malicioso.

En particular, el Artículo 269A establece penas para quien, sin autorización, acceda total o parcialmente a un sistema informático protegido con medidas de seguridad. Este artículo reconoce la importancia de salvaguardar la confidencialidad y disponibilidad de los sistemas y representa una base legal clave para la persecución de ciberdelitos.

Complementariamente, la Ley 1581 de 2012 regula el tratamiento de datos personales. Esta norma establece principios fundamentales como la legalidad, finalidad, libertad, veracidad, seguridad y confidencialidad en el manejo de la información personal.

También otorga a los ciudadanos derechos como el acceso, rectificación, actualización y supresión de sus datos personales, y establece obligaciones claras para las organizaciones que los gestionan.

El Decreto 1377 de 2013 fue emitido para reglamentar parcialmente la Ley 1581, especialmente en lo relacionado con la autorización de uso de datos recolectados antes de la entrada en vigencia de la norma. Este decreto obligó a las empresas a obtener el consentimiento de los titulares de los datos para continuar con su tratamiento.

Por su parte, la Ley 1266 de 2008 regula el tratamiento de datos personales financieros, crediticios y comerciales. Establece los principios y procedimientos para el reporte, acceso y corrección de la información financiera en las bases de datos administradas por las centrales de riesgo.

Etapas del pentesting y herramientas

El pentesting, o prueba de penetración, es una técnica usada en ciberseguridad para evaluar qué tan vulnerable es un sistema o red. Estas pruebas se hacen siguiendo una serie de pasos organizados.

Reconocimiento:

Aquí se recopila toda la información posible del objetivo. Se puede hacer de manera pasiva (sin interactuar) o activa (interactuando con el sistema). Por ejemplo, con la herramienta Nmap podemos descubrir qué puertos están abiertos o qué servicios están activos en una máquina (Lyon, 2009).

1. **Escaneo:**

En esta etapa se identifican posibles vulnerabilidades. Herramientas como Nessus u OpenVAS ayudan a detectar fallas que podrían ser explotadas por un atacante (Greenbone Networks, 2024).

2. **Obtener acceso:**

Con las vulnerabilidades ya identificadas, se intenta ingresar al sistema. Aquí es donde se usa Metasploit, una plataforma muy conocida que permite ejecutar exploits de forma controlada (Rapid7, 2024).

3. **Mantener acceso:**

El atacante busca quedarse dentro del sistema sin ser detectado. Se puede usar Netcat o establecer un reverse shell para mantener la conexión.

4. **Borrar evidencias:**

Una vez cumplido el objetivo, se eliminan los registros de la intrusión. Herramientas como Meterpreter, que ya viene con Metasploit, tienen funciones para limpiar logs o esconderse en el sistema.

5. **Reporte:**

Al final, se documenta todo lo encontrado. Herramientas como Dradis ayudan a organizar los hallazgos, presentar capturas de pantalla y entregar recomendaciones claras (Dradis Framework, 2023).

En Israel, por ejemplo, se aplican estas etapas de forma avanzada desde centros de inteligencia como la Unidad 8200. Allí, el pentesting se ve como una estrategia de defensa nacional, y se utiliza inteligencia artificial para predecir ataques (CyberArk, 2023).

Herramientas de ciberseguridad

Metasploit:

Es una de las herramientas más utilizadas en pruebas de penetración. Permite lanzar ataques simulados para verificar si las vulnerabilidades pueden ser explotadas. Además, su uso es ideal para aprender técnicas ofensivas de manera controlada (Rapid7, 2024).

Nmap:

Es una herramienta de escaneo de redes. Sirve para conocer el estado de los puertos, qué sistemas operativos están corriendo y qué servicios están activos (Lyon, 2009).

OpenVAS:

Sistema de escaneo de vulnerabilidades de código abierto. Es muy útil para hacer auditorías de seguridad automatizadas (Greenbone Networks, 2024).

ExploitDB:

Es una base de datos pública donde los expertos comparten códigos de exploits y vulnerabilidades conocidas. Se consulta frecuentemente para investigar posibles amenazas (Offensive Security, 2024).

CVE:

El sistema de Common Vulnerabilities and Exposures (CVE) sirve para identificar fallas de seguridad con un número único. Por ejemplo, una vulnerabilidad en Windows puede tener un código CVE que ayuda a rastrear su gravedad y soluciones (MITRE, 2024).

Tabla 1

Herramientas de Ciberseguridad: Definición, Uso y Aplicación en Colombia

Herramienta / Servicio	Definición breve	Uso principal en ciberseguridad	Ejemplo aplicado en Colombia
Metasploit	Framework de código abierto para pruebas de penetración y explotación.	Permite simular ataques reales para validar vulnerabilidades.	Usado por equipos de seguridad en la DIJIN y universidades como la ECCI en simulaciones de pruebas éticas (Rapid7, 2024).

Nmap	Herramienta de escaneo de red y detección de servicios/puertos.	Identificación de puertos abiertos y dispositivos en red.	Utilizada en pruebas de seguridad por estudiantes de Ingeniería en la U. Distrital y en auditorías de entidades públicas (Lyon, 2009).
OpenVAS	Escáner de vulnerabilidades de código abierto.	Detección automática de fallas en infraestructura de red.	Aplicada por consultoras en Bogotá para auditorías de seguridad en PYMES y entidades bancarias (Greenbone Networks, 2024).
ExploitDB	Base de datos de exploits públicos y vulnerabilidades conocidas.	Investigación de fallas explotables en software y hardware.	Utilizada por el Ejército Nacional y CERT Colombia para verificar amenazas documentadas (Offensive Security, 2024).

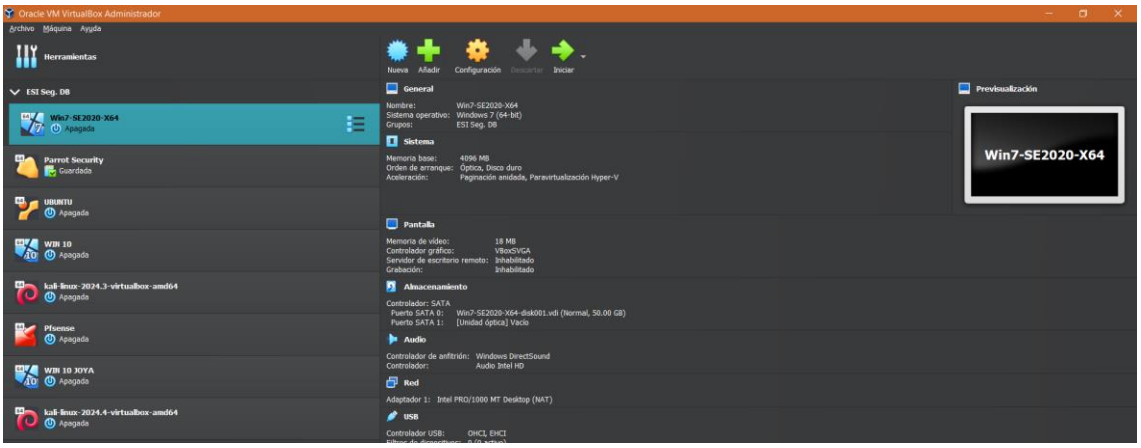
CVE (Common Vulnerabilities and Exposures)	Sistema de identificación estandarizada de vulnerabilidades.	Permite conocer el nivel de riesgo de una vulnerabilidad.	Referenciado por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) en alertas oficiales (MITRE, 2024).

***Nota**:* Esta tabla contiene la descripción de la clara y explicativa de las h**erramientas de ciberseguridad** con **ejemplos aplicados al contexto colombiano. Fuentes :** Greenbone Networks. (2024). *OpenVAS - Vulnerability Scanning*. https://www.greenbone.net, Lyon, G. (2009). *Nmap Network Scanning*. Insecure.Com LLC. MITRE. (2024). *Common Vulnerabilities and Exposures (CVE).* Offensive Security. (2024). *Exploit Database*. https://www.exploit-db.com Rapid7. (2024). *Metasploit Framework*. https://www.rapid7.com

Configuración del banco de trabajo WIN7 Y KALI

Figura 1

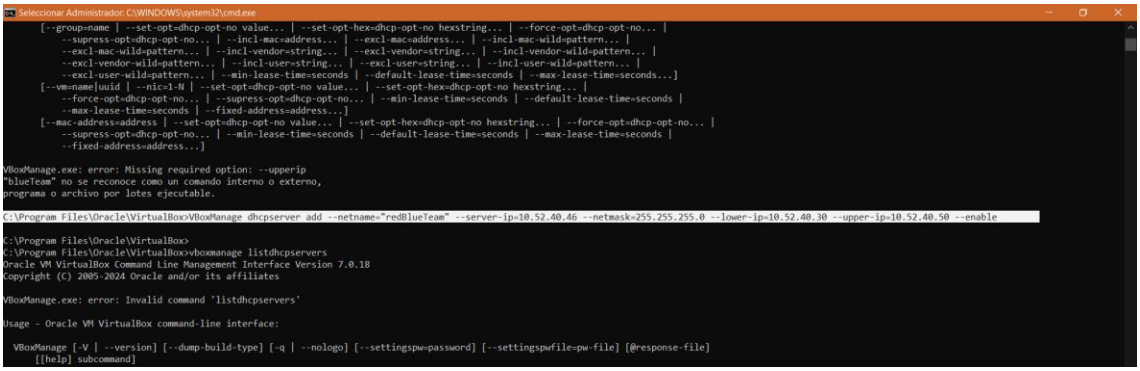
Oracle VirtualBox con las maquinas virtuales WIN7 Y KALI



Nota: La imagen muestra el entorno de laboratorio con sistemas Windows 7 y Kali Linux preconfigurados en formato. OVA, listos para actividades técnicas**. Fuentes:** Autor *(Joya, 2025).*

Figura 2

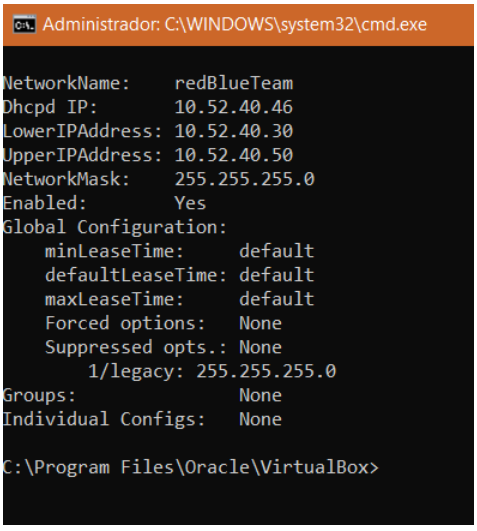
Configuración del DHCP



Nota: Se efectúa la configuración del DHCP mediante la consola de Win10 del usuario haciendo la apertura de una terminal CMD, abriendo la ruta del programa en el archivo local y se introduce el siguiente comando para configuración de los parámetros de la red local, *VBoxManage dhcpserver add --netname="redBlueTeam" --server-ip=10.52.40.46 --netmask=255.255.255.0 --lower-ip=10.52.40.30 --upper-ip=10.52.40.50 –enable.* **Fuentes:** Autor *(Joya, 2025).*

Figura 3

Verificación de los parámetros de la configuración de DHCP



Nota: Se efectúa la verificación de los parámetros de red interna los cuales se configuran con la cedula del usuario. **Fuentes:** Autor *(Joya, 2025).*

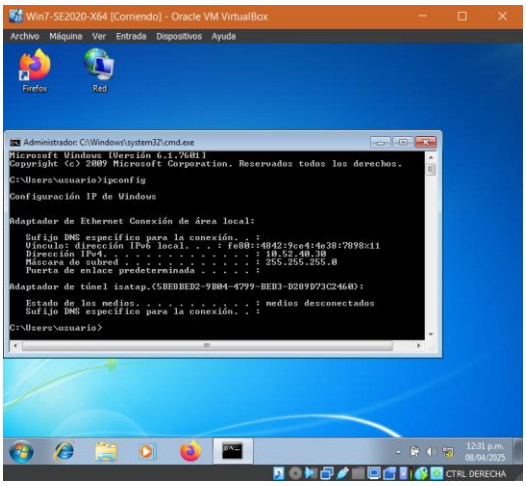
Figura 4

Ejecución de las 02 máquinas virtuales.

Nota: Se efectúa la ejecución de las 02 máquinas virtuales WIN7 Y Kali. **Fuentes:** Autor *(Joya, 2025).*

Figura 5

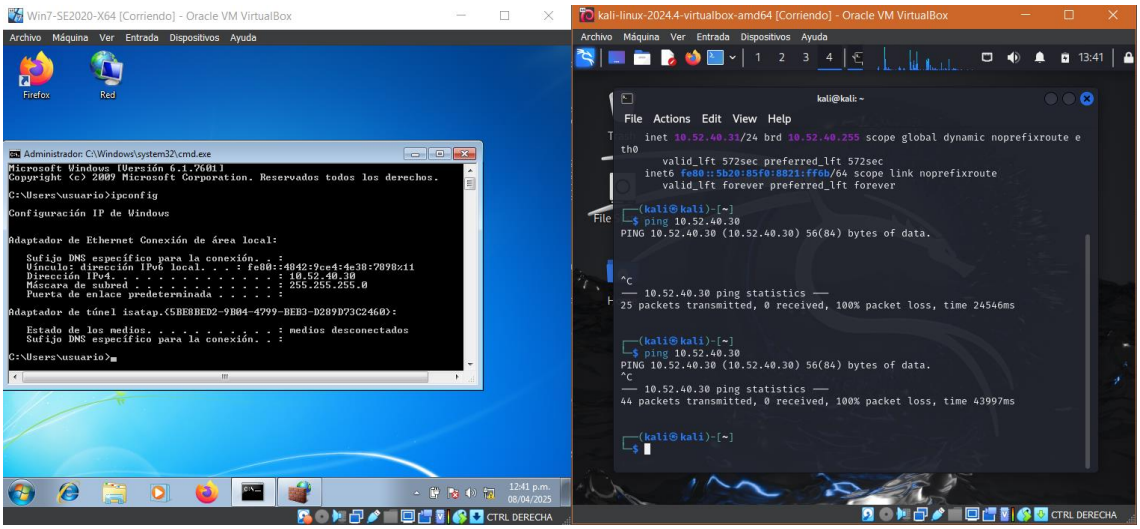
Verificación de los parámetros la red local maquina Win7.



Nota: Se efectúa la verificación la dirección IPV4, la cual es el numero de la cedula del autor, 10.52.40.30. **Fuentes:** Autor *(Joya, 2025).*

Figura 6

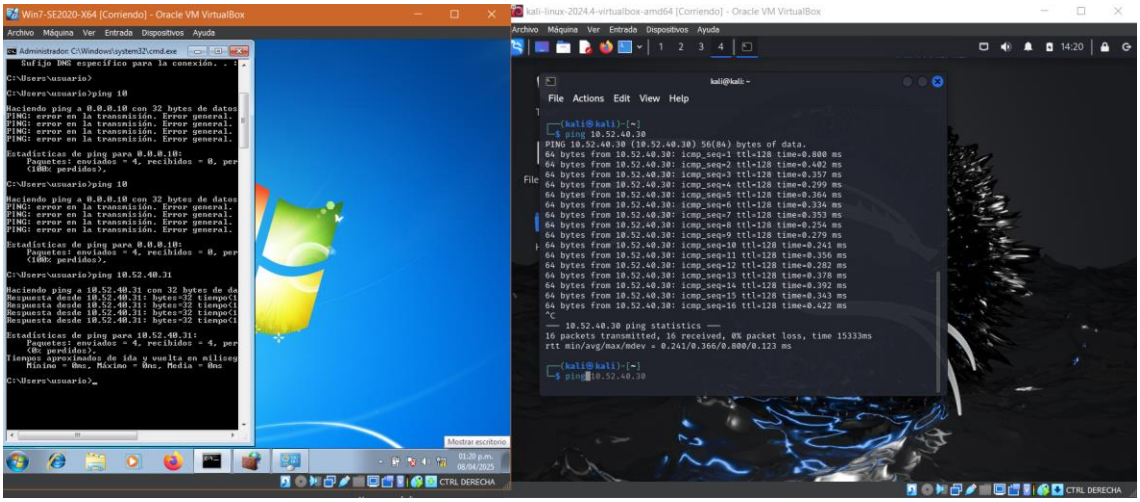
Verificación de la conexión entre las dos maquina virtuales WIN7/KALI.



Nota: Se envía un ping a la ip:10.52.40.30. **Fuentes:** Autor *(Joya, 2025).*

Figura 7

Verificación de la conexión entre las dos maquina virtuales WIN7/KALI.



Nota: Se envía un ping a la ip:10.52.40.30, de manera satisfactoria desde Kali a WIN7 y de la misma manera se envía un ping a la ip de KALI / IP: 10.52.40.31. **Fuentes:** Autor *(Joya, 2025).*

Etapa 2 – Actuación ética y legal

¿Se evidencia algún proceso ilegal y no ético en el Anexo 3 – Acuerdo?

Sí, se evidencian varios procesos ilegales y éticamente cuestionables en el Acuerdo de Confidencialidad estipulado por CyberFort Technologies. A continuación, se señalan los fragmentos irregulares:

Fragmento 1 – Cláusula Cuarta, numeral 3:

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

Fragmento 2 – Cláusula Cuarta, numeral 4:

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

Estos apartes obligan al firmante a ocultar información ilegal, lo cual representa una clara violación de la ética profesional y del orden jurídico colombiano, pues limita la posibilidad de cumplir con el deber ciudadano y profesional de denunciar actos delictivos.

Desde el punto de vista ético, encubrir actividades ilícitas va en contra del principio de integridad que debe tener cualquier profesional de la ingeniería o la seguridad informática, ya que promueve la complicidad en posibles delitos (Consejo Profesional Nacional de Ingeniería - COPNIA, 2019).

El Acuerdo contenido en el Anexo 3 incluye disposiciones que resultan legal y éticamente problemáticas, sobre todo teniendo en cuenta que fue elaborado por un abogado desvinculado por irregularidades y que no fue validado por la alta dirección, la cual incluso recomienda precaución al firmarlo. Este documento impone al receptor la obligación de considerar como confidencial información relacionada con posibles delitos informáticos, como interceptaciones ilegales y accesos no autorizados a sistemas, lo cual sugiere una intención de encubrir estas prácticas.

Asimismo, establece prohibiciones explícitas para denunciar ante las autoridades conductas irregulares, incluso si implican apropiación indebida de datos. También restringe la divulgación de información que pueda evidenciar actos ilícitos sin autorización de la empresa, y delega toda la responsabilidad jurídica al receptor en caso de que dicha información sea encontrada en su poder, eximiendo a la compañía de cualquier implicación legal. Estas cláusulas transgreden normas éticas y legales vigentes en Colombia, como la Ley 1273 de 2009, y colocan al profesional en una posición de vulnerabilidad, comprometiendo su integridad y su obligación de actuar conforme al interés público.

2. ¿Qué artículos de la Ley 1273 de 2009 se podrían estar vulnerando en el Acuerdo?

El Acuerdo podría vulnerar varios artículos de la **Ley 1273 de 2009**, que modifica el Código Penal colombiano para proteger la información y los datos informáticos. Estos son algunos de los artículos potencialmente infringidos:

Artículo 269A – Acceso abusivo a un sistema informático

El acuerdo menciona que se manejarán datos sensibles, incluyendo "accesos abusivos a sistemas informáticos", lo cual sugiere tolerancia a prácticas ilegales. Obligar al firmante a no denunciar estas acciones puede significar complicidad en dicho delito.

Artículo 269C – Interceptación de datos informáticos

Se hace alusión a "datos de chuzadas, interceptación de información", lo que es ilegal si no media una orden judicial. El Acuerdo impone una cláusula de silencio que contradice este artículo, al buscar evitar que dicha actividad sea reportada.

Artículo 269E – Uso de software malicioso

Aunque no se menciona directamente, la retención y manipulación indebida de información confidencial puede involucrar herramientas maliciosas. Al impedir su denuncia, el acuerdo puede facilitar indirectamente este delito.

Artículo 269F – Violación de datos personales

El uso y ocultamiento de información privada sin consentimiento también puede violar este artículo, especialmente si se impide denunciar estas prácticas ante las autoridades.

Según Guerrero (2012), la Ley 1273 busca “proteger el derecho fundamental a la intimidad y la información” y, por tanto, cualquier acuerdo que coarte la denuncia de violaciones a estos derechos podría constituir **una forma de encubrimiento penal**.

Tabla 2

Artículos vulnerados de la Ley 1273 de 2009 y aspectos éticos

Artículo vulnerado (Ley 1273 de 2009)	**Nombre del delito**	**Acción del acuerdo que lo vulnera**	**Explicación legal y ética**
Artículo 269A	Acceso abusivo a un sistema informático	Acceso a comunicaciones gubernamentales sin autorización	El uso de credenciales o privilegios adquiridos legítimamente para obtener acceso a información que no estaba autorizada constituye una violación a la privacidad del cliente y al sistema legal colombiano.
Artículo 269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	Alteración de servidores mediante herramientas forenses sin autorización expresa	La alteración o interferencia con sistemas del cliente sin consentimiento rompe con la confidencialidad y excede las funciones del contrato.
Artículo 269C	Interceptación de datos informáticos	Captura de correos electrónicos y documentos	La interceptación de comunicaciones privadas sin orden judicial o consentimiento explícito constituye ciberespionaje.
Artículo 269F	Violación de datos personales	Venta de información a terceros	Comercializar datos sensibles de un tercero sin su aprobación constituye una violación a los derechos fundamentales, como el habeas data.
Código de Ética COPNIA – Art. 1 y 11	Responsabilidad profesional e integridad	Uso indebido del conocimiento técnico para obtener beneficios personales	La ética profesional exige actuar con transparencia, proteger la información del cliente y no usar el

	conocimiento en contra del bien común.

Nota: Esta tabla contiene los artículos vulnerados de la ley 1273 de 2009 junto con aspectos éticos relacionados y las vulneraciones a la información, este tipo de comportamientos, si se descubrieran, constituirían una violación directa de los artículos mencionados de la Ley 1273 de 2009, además de abrir la puerta a procesos penales por espionaje y corrupción. **Fuentes :** Congreso de Colombia. (2009). *Ley 1273 de 2009*. Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y los datos. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34506, Consejo Profesional Nacional de Ingeniería (COPNIA). (2008). *Código de Ética Profesional*. https://www.copnia.gov.co

¿Aplicaría al trabajo en CyberFort Technologies bajo estas condiciones, según el código de ética del COPNIA?

No aplicaría al trabajo ofrecido por CyberFort Technologies, a pesar del salario elevado ($15.000.000 COP millones de pesos colombianos mensuales) y del contrato vitalicio. La razón principal es que dicho contrato infringe varios principios éticos fundamentales establecidos en el Código de Ética del COPNIA.

Justificación ética:

Artículo 1 – Responsabilidad Social:

"El ingeniero debe contribuir al bienestar de la sociedad, procurando siempre que su ejercicio profesional esté orientado a la mejora de la calidad de vida de las personas" (COPNIA, 2019).

Artículo 2 – Legalidad:

"El ingeniero debe ejercer su profesión conforme a las leyes, reglamentos y disposiciones éticas vigentes".

Artículo 7 – Denuncia de actos antiéticos:

"El ingeniero debe abstenerse de participar o tolerar actos corruptos o ilegales. En caso de conocerlos, tiene el deber de denunciarlos".

El acuerdo de confidencialidad, como ya se analizó, limita el derecho y deber del profesional de denunciar actos delictivos relacionados con ciberseguridad, lo cual pone en riesgo la integridad del ingeniero, su licencia profesional, y lo compromete legalmente.

Además, aceptar este trabajo sería incompatible con los valores de la ciberseguridad profesional, que incluyen la transparencia, la protección de la privacidad, y la promoción de una cultura de legalidad (Kizza, 2017).

Aceptar un empleo basado en un acuerdo que impone el silencio frente a delitos informáticos contradice los principios legales y éticos que rigen la ingeniería en Colombia. Según el Código de Ética del COPNIA, establecido en la Ley 842 de 2003, el profesional está obligado a denunciar cualquier acto ilícito del que tenga conocimiento (art. 31.f), se le prohíbe obtener beneficios a cambio de encubrir delitos (art. 32.j), no puede aceptar cargos que violen las normas legales (art. 34.a) y, aunque debe respetar la confidencialidad de la información, este deber no aplica en contextos delictivos (art. 39.a).

En el contexto colombiano, donde la lucha contra los delitos cibernéticos es una prioridad nacional, un ingeniero que acepte participar en actividades que oculten irregularidades no solo faltaría a su responsabilidad profesional, sino que también podría enfrentarse a consecuencias penales y la posible pérdida de su licencia, al ser considerado cómplice de actos que atentan contra la integridad institucional y la seguridad del Estado.

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

El caso de CyberFort Technologies representa una clara vulneración tanto de los principios éticos que rigen la ciberseguridad como del marco legal colombiano que regula el uso y tratamiento de la información. El hecho de que empleados de una empresa contratada para realizar una auditoría de seguridad hayan accedido y recopilado información sensible sin autorización, y posteriormente la hayan vendido en mercados ilegales, constituye no solo una falta grave de ética profesional, sino también múltiples delitos informáticos.

Desde el punto de vista ético, los expertos involucrados infringieron principios fundamentales como la confidencialidad, la integridad, la lealtad hacia el cliente y el respeto a la privacidad de la información. Toda relación profesional, especialmente en el ámbito de la ciberseguridad, debe basarse en la confianza, la transparencia y la protección de los intereses del cliente. Justificar el uso no autorizado de información con el argumento de "mejorar la seguridad" refleja una racionalización peligrosa que ignora los límites de la ética profesional.

Tabla 3

Análisis ético y legal del caso CyberFort Technologies

Aspecto analizado	Descripción
Violaciones éticas	*CyberFort Technologies* incumplió principios esenciales como la confidencialidad, la integridad y la lealtad hacia su cliente al acceder y comercializar información sensible sin consentimiento, lo que contraviene los códigos de conducta profesional.
Violaciones legales	Las acciones de la empresa podrían constituir delitos conforme a la **Ley 1273 de 2009**, que penaliza el acceso no autorizado a sistemas informáticos y la violación de datos personales. También incumple el **Decreto 1377 de 2013**, que reglamenta el manejo seguro de datos personales.
Recomendación 1: Contratos claros	Establecer cláusulas específicas que delimiten el alcance del acceso a la información y definan consecuencias ante cualquier uso indebido.
Recomendación 2: Principio de mínimo privilegio	Otorgar accesos temporales y estrictamente necesarios durante la auditoría, revocándolos inmediatamente después de su finalización.
Recomendación 3: Auditorías internas	Monitorear las actividades del personal mediante auditorías técnicas durante el proceso de revisión para prevenir abusos o accesos indebidos (ISO 27001, 2013).

Nota: Esta tabla contiene Análisis ético y legal del caso CyberFort Technologies **Fuentes :** Congreso de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se crea el tipo penal de protección de la información y de los datos*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492 Congreso de Colombia. (2013). *Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646 ICONTEC. (2013). *NTC-ISO/IEC 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos*. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación. International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*. Ginebra, Suiza.

Legalmente, las acciones descritas podrían ser procesadas bajo la Ley 1273 de 2009, que tipifica como delitos el acceso abusivo a sistemas informáticos (art. 269A), la interceptación de datos informáticos (art. 269C), y la violación de datos personales (art. 269F). Asimismo, se

violan disposiciones del Decreto 1377 de 2013, el cual exige que el tratamiento de información personal se realice bajo estándares estrictos de seguridad, confidencialidad y con autorización del titular de los datos.

En el contexto colombiano, este caso también pone en evidencia la necesidad de fortalecer los controles de contratación pública y privada en materia de servicios de ciberseguridad. Las entidades estatales y las empresas deben asegurarse de contratar únicamente a organizaciones certificadas, con políticas éticas robustas y mecanismos efectivos de supervisión interna. Además, este tipo de incidentes debe activar no solo acciones penales, sino también procesos de auditoría, sanciones contractuales y reformas institucionales que prevengan la repetición de estos hechos.

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

Las empresas de ciberseguridad, durante una auditoría, deben tener acceso únicamente a la información estrictamente necesaria para cumplir con los objetivos del servicio pactado. El principio de minimización de datos es clave en estos procesos: se accede solo a lo indispensable (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2013). Para evitar el uso indebido de la información, es indispensable firmar acuerdos de confidencialidad detallados y establecer protocolos de acceso, uso y almacenamiento de los datos.

Tabla 4

Buenas prácticas para el acceso a información sensible en auditorías de ciberseguridad

Categoría	Principio / Medida	Descripción / Aplicación	Marco normativo colombiano / Estándar aplicable
Acceso Responsable	Principio de necesidad	Acceder únicamente a la información estrictamente necesaria para la auditoría.	Ley 1581 de 2012, Art. 4 (Finalidad y necesidad)
	Alcance definido	El contrato debe especificar los sistemas y tipos de datos que serán auditados.	ISO/IEC 27001; Ley 1581 de 2012
	Minimización de datos	Utilizar la menor cantidad posible de datos reales; preferir entornos de prueba o datos anonimizados.	Ley 1581 de 2012; Decreto 1377 de 2013
	Finalidad específica	Todo acceso debe tener un propósito claro y legítimo, alineado con los objetivos de la auditoría.	Ley 1581 de 2012
	Consentimiento informado	El cliente debe autorizar explícitamente el acceso a la información, su uso y protección.	Ley 1581 de 2012 – Derechos del titular
Controles y Garantías	Contrato detallado	Incluir cláusulas que definan el alcance, confidencialidad, sanciones por violación y uso adecuado de los datos.	Código Civil Colombiano; ISO/IEC 27001

	Acuerdos de confidencialidad (NDA)	Establecer acuerdos que obliguen a mantener la confidencialidad, usar los datos solo para la auditoría y sancionar su incumplimiento.	Ley 1273 de 2009; Ley 842 de 2003 (COPNIA)
	Registro de actividad (Logs)	Documentar quién accede, cuándo, a qué datos y con qué propósito, manteniendo un registro detallado.	ISO/IEC 27001; Ley 1273 de 2009
	Autenticación y control de acceso	Implementar autenticación multifactorial (MFA) y permisos de acceso basados en roles.	Mejores prácticas internacionales; CISA; ISO
	Transferencia segura	Utilizar canales cifrados para la transmisión de información confidencial.	Ley 1273 de 2009
Supervisión y Auditoría	Supervisión del cliente	El cliente debe monitorear y validar en tiempo real el proceso de auditoría.	Contratación estatal; Política de seguridad digital
	Auditorías internas y externas	Realizar auditorías periódicas para revisar el cumplimiento de accesos, registros y obligaciones contractuales.	ISO/IEC 27001; Ley 1581 de 2012
	Responsabilidad contractual y legal	La empresa auditora será legalmente responsable si incumple los acuerdos establecidos.	Ley 1581 de 2012; Código Penal Colombiano
Selección del Proveedor	Reputación y trayectoria	Contratar empresas con referencias verificadas en auditorías seguras y de confianza.	Principio de precaución en contratación pública

	Certificaciones en seguridad	Verificar que el proveedor cumpla con estándares de seguridad reconocidos, como ISO 27001 o ISO 27701.	ISO; INCIBE; CISA

Nota: Esta tabla contiene Buenas prácticas para el acceso a información sensible en auditorías de ciberseguridad. **Fuentes :** Congreso de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se crea el tipo penal de protección de la información y de los datos*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492 Congreso de Colombia. (2013). *Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646 ICONTEC. (2013). *NTC-ISO/IEC 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos*. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación. International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*. Ginebra, Suiza.

Además, se deben implementar políticas de ética corporativa sólidas y capacitaciones continuas que fortalezcan la cultura del respeto a la privacidad del cliente. Las auditorías deben regirse por principios internacionales como los del Código de Ética del (ISC), el cual establece que los profesionales deben “proteger la sociedad, el bien común, la confianza pública y la infraestructura” (International Information System Security Certification Consortium, 2020).

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

Para evitar usos indebidos de herramientas forenses, las empresas de ciberseguridad deben establecer un marco robusto de gobierno corporativo. Entre los mecanismos clave se encuentran:

1. **Auditorías internas continuas y externas independientes**, que verifiquen los logs de acceso y actividad de los analistas de seguridad.
2. **Separación de funciones (SoD)**, donde el acceso a información crítica no recaiga en una sola persona, sino que exista una supervisión cruzada (Bishop, 2019).
3. **Monitoreo en tiempo real** mediante SIEM (Security Information and Event Management), lo que permite detectar comportamientos anómalos.
4. **Protocolos de autorización escalonada**, donde los análisis sensibles requieran aprobación de mandos superiores.

Estos mecanismos se alinean con la norma ISO/IEC 27001, que promueve controles estrictos de seguridad en el manejo de información confidencial (ISO, 2022).

Tabla 5

Mecanismos de Supervisión y Control para el Uso Ético de Herramientas Forenses en Empresas de Ciberseguridad

Categoría	Medida / Principio	Descripción / Aplicación	Marco Normativo / Estándar Aplicable

Controles de Acceso y Autorización	Acceso según roles y necesidad	Limitar el acceso a las herramientas de análisis forense a los empleados que realmente lo necesiten, definiendo permisos específicos según el rol de cada persona y el tipo de análisis requerido.	ISO/IEC 27001; Ley 1581 de 2012
	Autenticación multifactorial (MFA)	Implementar un sistema de autenticación multifactorial (MFA) para acceder a las herramientas y sistemas donde se almacenan los datos, añadiendo una capa extra de seguridad.	Mejores prácticas internacionales
	Listas de control de acceso (ACLs)	Configurar listas de control de acceso (ACLs) para garantizar que solo los usuarios autorizados puedan acceder a los sistemas y datos relacionados con el análisis forense.	ISO/IEC 27001
Registro y Auditoría Detallada	Registro completo de actividad	Mantener registros detallados de todas las actividades realizadas con las herramientas forenses, como el acceso, los datos analizados, el usuario, el momento de la actividad y las modificaciones realizadas.	ISO/IEC 27001; Ley 1273 de 2009
	Centralización y seguridad de logs	Los registros deben almacenarse en un sistema centralizado, seguro e inalterable, protegido contra accesos no autorizados y alteraciones.	ISO/IEC 27001
	Auditoría periódica de logs	Realizar auditorías regulares sobre los registros de actividad para detectar actividades	ISO/IEC 27001

		sospechosas, accesos no autorizados o comportamientos inusuales.	
Políticas y Procedimientos Claros	Política de uso aceptable	Definir una política clara sobre el uso de las herramientas forenses, especificando los usos permitidos y prohibidos y las sanciones por mal uso.	Ley 1581 de 2012; ISO/IEC 27001
	Procedimientos operativos estándar (POEs)	Establecer procedimientos detallados para realizar análisis forenses, incluyendo los pasos a seguir, la documentación requerida y las aprobaciones necesarias.	ISO/IEC 27001
	Protocolos de manejo de evidencia digital	Implementar protocolos rigurosos para garantizar la integridad y cadena de custodia de la evidencia digital durante todo el proceso de adquisición, análisis y disposición.	ISO/IEC 27001
	Aprobación para análisis sensibles	Para análisis de información muy sensible, se debe requerir la aprobación explícita de la gerencia o un comité encargado.	Código Penal Colombiano
Supervisión Técnica y Alertamiento	Sistemas de detección de anomalías	Implementar sistemas de monitoreo que alerten sobre actividades inusuales en el uso de las herramientas forenses, como patrones de uso anómalos.	ISO/IEC 27001
	Monitoreo en tiempo real	En algunos casos, se puede considerar el monitoreo en tiempo real del uso de herramientas dentro de los límites legales y de privacidad.	ISO/IEC 27001

	Integración con sistemas SIEM	Integrar los registros de las herramientas forenses con un sistema de gestión de eventos e información de seguridad (SIEM) para mejorar la correlación y análisis de eventos.	ISO/IEC 27001; CISA
Controles Humanos y Éticos	Selección rigurosa de personal	Realizar exhaustivas verificaciones de antecedentes y referencias para los empleados con acceso a herramientas forenses, asegurando que son de confianza.	Código Penal Colombiano; Ley 1581 de 2012
	Capacitación continua	Proveer entrenamiento regular sobre el uso ético y responsable de las herramientas forenses, así como las políticas de seguridad y las implicaciones legales del mal uso.	ISO/IEC 27001
	Código de conducta y ética profesional	Implementar y reforzar un código de conducta que promueva la integridad, la confidencialidad y el respeto por la privacidad de la información.	Ley 1581 de 2012
	Acuerdos de confidencialidad y no divulgación	Requerir que todos los empleados firmen acuerdos de confidencialidad que aborden específicamente el manejo de información sensible y el uso de herramientas forenses.	Ley 1273 de 2009; Ley 842 de 2003 (COPNIA)
	Evaluaciones de desempeño y revisiones éticas	Realizar evaluaciones periódicas de desempeño, incluyendo la conducta ética, y revisar	Código Penal Colombiano

		regularmente el uso de las herramientas para detectar posibles malas prácticas.	
	Canales de denuncia confidenciales	Establecer canales seguros y confidenciales para que los empleados puedan reportar posibles mal usos de las herramientas sin temor a represalias.	Ley 1581 de 2012
Auditorías Internas y Externas	Auditorías técnicas	Realizar auditorías técnicas periódicas para comprobar la correcta configuración y el cumplimiento de los controles de acceso, el registro de actividad y la seguridad de los sistemas utilizados.	ISO/IEC 27001
	Auditorías de cumplimiento	Llevar a cabo auditorías de cumplimiento para verificar que las políticas y procedimientos establecidos están siendo seguidos de manera adecuada.	ISO/IEC 27001
	Auditorías éticas	Considerar la realización de auditorías éticas para evaluar la cultura de la empresa y la comprensión de los principios éticos en el uso de las herramientas forenses.	ISO/IEC 27001

Nota: La implementación de mecanismos robustos de supervisión y control es esencial para garantizar el uso adecuado y ético de las herramientas de análisis forense en las empresas de ciberseguridad, minimizando el riesgo de accesos no autorizados y el uso indebido de la información sensible. Las medidas descritas están alineadas con los estándares internacionales y las normativas colombianas vigentes en materia de protección de datos, seguridad de la información y ética profesional. **Fuentes:** Congreso de Colombia. (2009). Ley 1273 de 2009. Por medio de la cual se crea el tipo penal de protección de la información y de los datos. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492. Congreso de

Colombia. (2013). Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646. ICONTEC. (2013). NTC-ISO/IEC 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación. International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. Ginebra, Suiza.

6. ¿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?

Ante un acto comprobado de ciberespionaje, el gobierno u organización afectada debe actuar con firmeza jurídica y política. Las medidas adecuadas incluyen:

- Rescisión inmediata del contrato y apertura de procesos penales, conforme a las leyes locales e internacionales sobre delitos informáticos (Ley 1273 de 2009 en Colombia, por ejemplo).
- Divulgación transparente a las autoridades competentes y, si aplica, al público, para minimizar el daño reputacional y demostrar compromiso con la legalidad (Tanczer et al., 2018).
- Reevaluación de políticas de contratación, incluyendo cláusulas de auditoría ética y penalizaciones ante incumplimientos contractuales.
- Restauración de confianza mediante campañas de ciberhigiene, fortalecimiento de la infraestructura y selección de nuevos proveedores con certificaciones reconocidas como ISO 27001 o SOC 2.

Además, deberían establecerse marcos de cooperación internacional que faciliten sanciones ejemplares y eviten la impunidad, promoviendo estándares éticos y legales comunes en la industria de ciberseguridad.

Tabla 6

Mecanismos de Supervisión y Control para el Uso Ético de Herramientas Forenses en Empresas de Ciberseguridad

Categoría	Acciones / Medidas	Descripción / Aplicación	Marco Normativo / Estándar Aplicable
Acciones Legales y Contractuales	Rescisión del contrato y sanción económica	Aplicar la cláusula de resolución anticipada en caso de incumplimiento grave, además de imponer cláusulas penales o demandar por perjuicios si están estipuladas en el contrato.	Código Civil Colombiano; Ley 1273 de 2009
	Denuncia penal formal ante la Fiscalía General de la Nación	Procesar a los responsables por delitos como acceso abusivo, interceptación y violación de datos, según la Ley 1273 de 2009 y el Código Penal Colombiano.	Ley 1273 de 2009; Código Penal Colombiano
	Colaboración internacional	En caso de que los hechos afecten a otros Estados (por ejemplo, si la información fue vendida a empresas extranjeras), activar mecanismos de cooperación judicial internacional, como los de INTERPOL.	INTERPOL; Ley 1273 de 2009

Medidas para Restaurar la Confianza	Auditoría independiente postincidente	Contratar una firma neutral y certificada para revisar los accesos, detectar vulnerabilidades y establecer el alcance del daño.	ISO/IEC 27001; Ley 1581 de 2012
	Informe público controlado	Comunicar de forma oficial y responsable los hechos a la ciudadanía y al Congreso, sin divulgar detalles sensibles, como parte de una política de transparencia institucional.	Ley 1581 de 2012
	Revisión del marco contractual de servicios de ciberseguridad	Modificar los contratos para incluir criterios éticos, cláusulas anticorrupción, responsabilidad civil y penal, y la obligatoriedad de implementación de estándares como ISO/IEC 27001 y 27701.	ISO/IEC 27001; Ley 1581 de 2012
	Certificación y vigilancia de empresas contratistas	Crear un registro nacional de empresas de ciberseguridad evaluadas por el Estado, similar al Registro Único Empresarial (RUES), para asegurar la fiabilidad de las contratistas.	Ley 1581 de 2012; RUES
Fortalecimiento Normativo y Políticas Públicas	Actualización del marco legal colombiano	Urge la creación de una regulación específica para empresas privadas de ciberseguridad en Colombia, incluyendo	Ley 1273 de 2009; Ley 1581 de 2012

		la responsabilidad empresarial en el manejo de datos clasificados, licenciamiento obligatorio para auditores forenses y regulación de la exportación/importación de software avanzado.	
	Creación de una Agencia Nacional de Ciberseguridad	Establecer una agencia similar al modelo de España (INCIBE) o EE. UU. (CISA) para supervisar el sector, emitir alertas de seguridad y realizar investigaciones sobre fraudes tecnológicos.	INCIBE; CISA
Cooperación Internacional y Listas Negras	Incluir empresas sancionadas en listas negras	Prohibir que empresas sancionadas por ciberespionaje puedan ser contratadas nuevamente por entidades públicas o privadas en Colombia.	Ley 1581 de 2012; normas internacionales
	Participación en alianzas regionales	Colombia puede fortalecer su participación en el Grupo de Acción de Ciberseguridad de la OEA para compartir alertas de riesgo y establecer estándares mínimos en contrataciones internacionales.	OEA

Nota: Las acciones y medidas descritas son fundamentales para garantizar el cumplimiento de las normativas legales y la restauración de la confianza en el sector de ciberseguridad, respondiendo de manera efectiva a incidentes de ciberseguridad y fortaleciendo la seguridad digital en el país. **Fuentes:** Congreso de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se crea el tipo penal de protección de la información y de los datos*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492 Congreso de Colombia. (2013). *Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 de 2012 sobre*

protección de datos personales https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646ICONTEC. (2013). *NTC-ISO/IEC 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos*. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*. Ginebra, Suiza.

Etapa 3 – Componente práctico – Prácticas simuladas

Herramientas de software utilizadas y comandos implementados

Como parte de la preparación del entorno de pruebas, se instalaron dos sistemas operativos proporcionados por el tutor: Kali Linux y Windows. Ambos fueron configurados dentro de una red virtual interna con el objetivo de permitir la comunicación directa entre las máquinas, condición fundamental para llevar a cabo tareas de análisis y evaluación de seguridad. La configuración de red asignó de forma manual la dirección IP 10.52.40.31 al sistema Kali Linux y la 10.52.40.30 al sistema Windows, siguiendo un criterio basado en el número de identificación personal del estudiante.

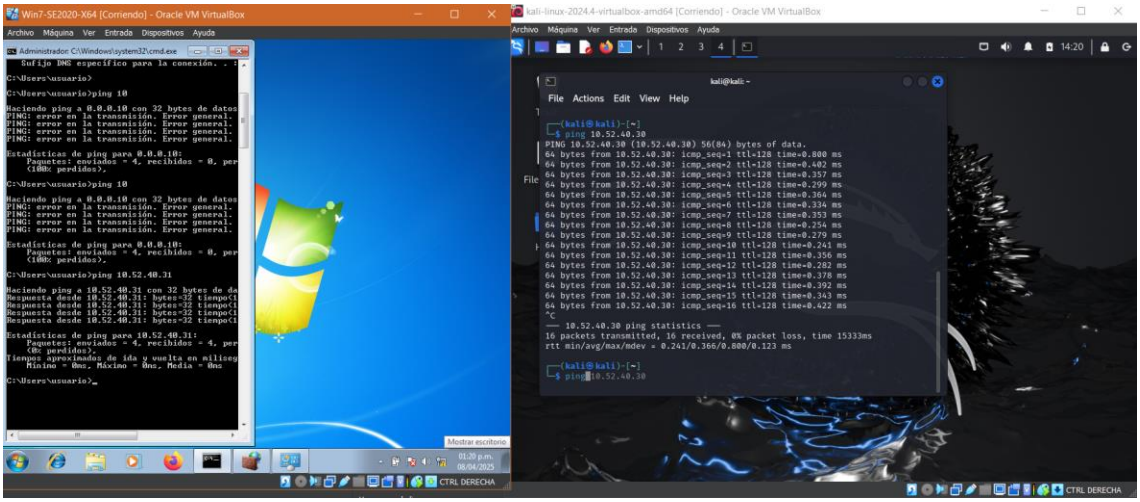
Para verificar la correcta asignación de las direcciones IP, en el sistema Kali Linux se accedió a la terminal, se obtuvieron privilegios de administrador mediante el comando sudo su, y se utilizó el comando ip address para consultar los parámetros de red. En el sistema Windows, por su parte, se abrió el símbolo del sistema (CMD) y se ejecutó el comando ipconfig, el cual mostró los detalles de la configuración de red correspondiente.

Posteriormente, antes de iniciar cualquier proceso de reconocimiento o análisis, se validó la conectividad entre las máquinas virtuales. La verificación consistió en ejecutar el comando ping desde la máquina atacante (Kali Linux) hacia la máquina objetivo (Windows), enviando paquetes ICMP tipo echo request a la dirección IP 10.52.40.30. La recepción de respuestas por parte del sistema destino confirmó que ambas máquinas estaban correctamente interconectadas dentro de

la red virtual, lo cual permitió continuar con el desarrollo de las pruebas de seguridad planificadas.

Figura 8

Verificación de la conexión entre las dos maquina virtuales WIN7/KALI.



Nota: Se envía un ping a la ip:10.52.40.30, de manera satisfactoria desde Kali a WIN7 y de la misma manera se envía un ping a la ip de KALI / IP: 10.52.40.31. **Fuentes:** Autor *(Joya, 2025).*

Datos e información usados en la identificación del fallo

Tabla 7

Fases usadas para el reconocimiento activo del Red Team.

Fase	Herramienta	Comando utilizado	Resultado esperado
Reconocimiento	nmap	nmap -sS -sV [IP_VM_Win7]	Detecta puertos abiertos, versiones de servicios.
Enumeración	nmap, enum4linux	enum4linux [IP_VM_Win7]	Información sobre usuarios, shares, etc.
Identificación y explotación	Metasploit	use exploit/windows/smb/ms17_010_eternalblue	Explota vulnerabilidad en SMB para obtener shell remota.
Post-Explotación	meterpreter, cmd	net user NombreApellido /add net localgroup Administrators NombreApellido /add	Crea usuario admin como PoC.
Escalada de privilegios	meterpreter script	run post/multi/recon/local_exploit_suggester	Sugerencia de exploits locales para escalar privilegios.

Nota: Esta tabla contiene la descripción de la clara y explicativa de las herramientas de usadas para la ejecución y desarrollo del anexo 4 escenario 3 enfocado a Red Team mediante el uso de reconocimiento activo mediante la herramienta Nmap y las fases a implementar **Fuentes :** elaboración propia del autor *(Joya, 2025).*

Reconocimiento

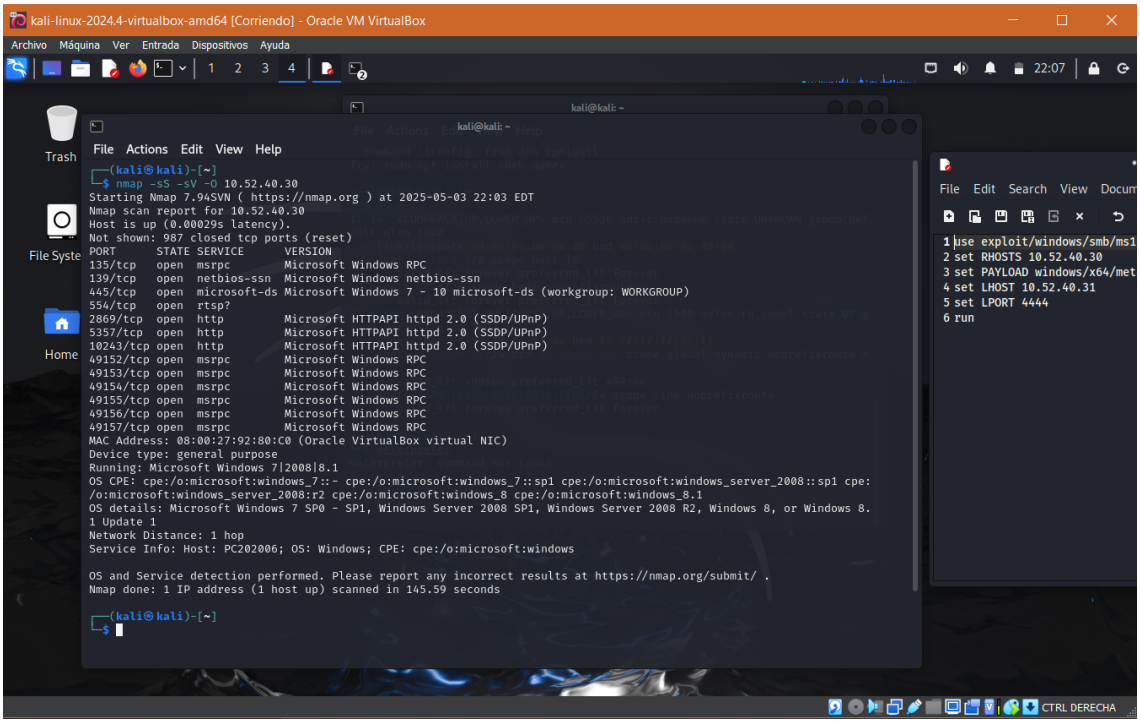
Luego de analizar el Anexo 4 correspondiente al Escenario 3, se procedió con la fase de reconocimiento, etapa fundamental en cualquier proceso de evaluación de seguridad, ya que permite identificar los servicios disponibles y los puertos abiertos en el sistema objetivo. Para esta tarea se utilizó la herramienta Nmap, ampliamente reconocida por su eficacia en tareas de escaneo de red. La ejecución del escaneo incluyó las opciones -sS, -sV y -O, las cuales permiten realizar un escaneo SYN (también conocido como escaneo furtivo o "half-open"), identificar

versiones de los servicios en ejecución y estimar el sistema operativo del host analizado, respectivamente. El comando específico utilizado fue:

nmap -sS -sV -O 10.52.40.30

Figura 9

Ejecución del comando Nmap



Nota: Durante la fase de reconocimiento, se llevó a cabo la identificación detallada de los servicios activos y los puertos habilitados en el sistema objetivo. Para esta tarea se utilizó la herramienta Nmap, en su versión 7.94SVN, reconocida por su precisión y versatilidad en el escaneo de redes**. Fuentes:** Autor *(Joya, 2025).*

El escaneo realizado reveló información técnica significativa. Entre los puertos abiertos detectados se encuentran el 135/tcp (msrpc), 139/tcp (netbios-ssn) y 445/tcp (microsoft-ds), todos ellos comúnmente asociados a servicios del sistema operativo Windows. Asimismo, se identificaron servicios activos como Microsoft SMB y HTTPAPI. A partir del análisis de las

firmas TCP/IP recolectadas, se estimó que el sistema operativo de la máquina objetivo corresponde a Windows 7 o Windows Server 2008 R2.

Un aspecto especialmente relevante fue la detección del puerto 445 abierto, el cual está asociado al protocolo SMB. Este hallazgo sugiere la existencia de una superficie de ataque potencial, dado que este protocolo ha sido históricamente vulnerable a múltiples exploits conocidos.

La información obtenida indica que el sistema comprometido corre Windows 7 y que contiene al menos una aplicación vulnerable que podría ser explotada para obtener acceso no autorizado.

En términos de riesgo, se identificó un posible vector de ataque que permitiría la ejecución remota de comandos (shell) o incluso la escalación de privilegios. Adicionalmente, según el análisis forense, se detectó la probable creación de una cuenta de usuario con privilegios de administrador sin la debida autorización, lo cual refuerza la hipótesis de una posible intrusión o explotación previa del sistema.

Enumeración

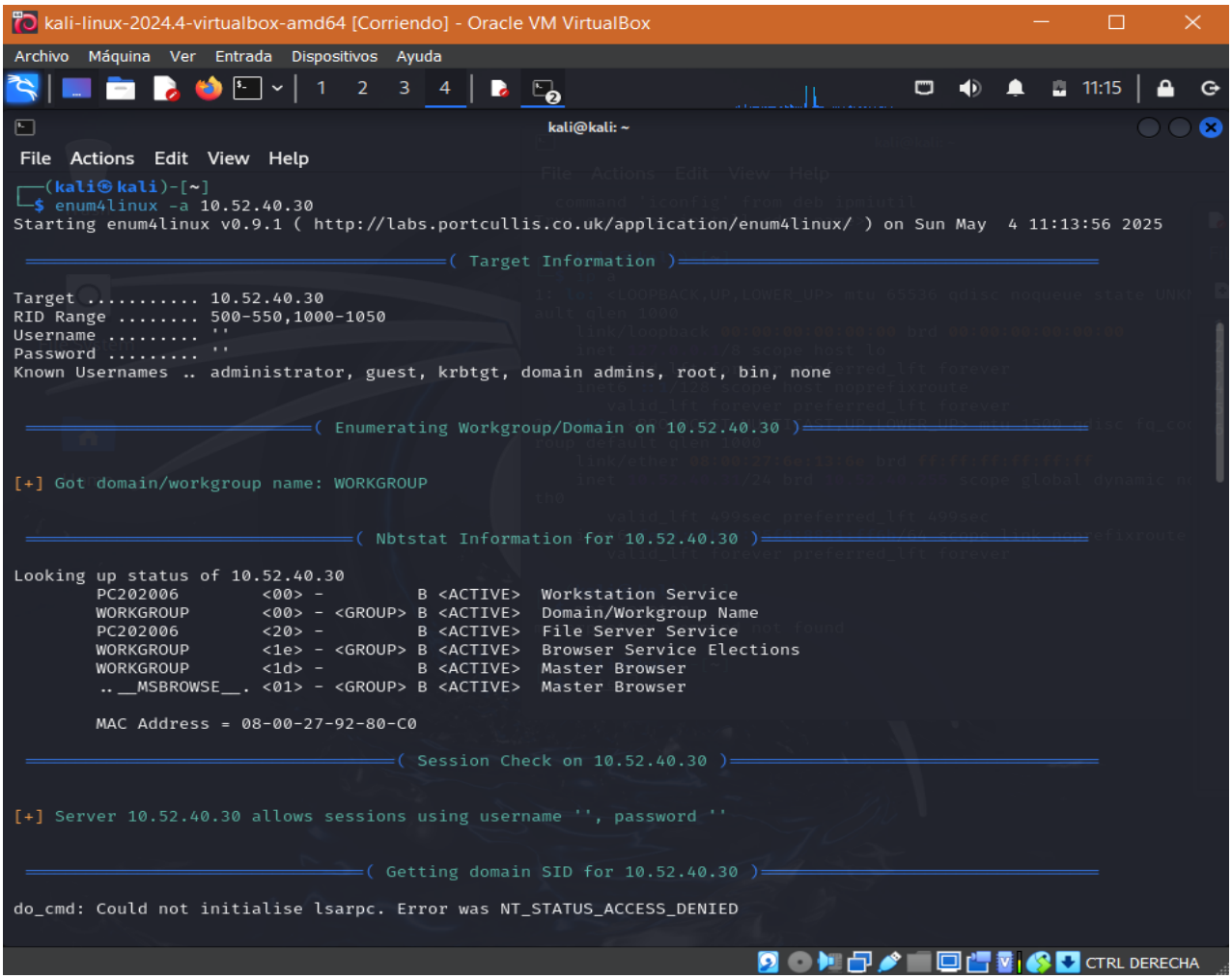
En el contexto del reconocimiento activo, se empleó la herramienta Enum4linux para llevar a cabo la enumeración de un sistema operativo Windows a través del protocolo SMB, sin requerir credenciales válidas. Esta utilidad, ampliamente utilizada en auditorías de seguridad, permite extraer información relevante como usuarios, grupos, recursos compartidos y configuraciones de red asociadas al servicio SMB.

El comando ejecutado fue el siguiente:

enum4linux -a 10.52.40.30

Figura 10

Enumeración del sistema mediante la herramienta Enum4linux



Nota: Ejecución de la fase de enumeración**. Fuentes:** Autor *(Joya, 2025), Cisco Talos. (2017, mayo 17). MS17-010: EternalBlue SMB Remote Windows Kernel Pool Corruption Exploit Analysis. https://www.talosintelligence.com/blog/2017/05/eternalblue.html ,Trustwave. (s.f.). Enum4linux – SMB enumeration tool for Linux. GitHub. https://github.com/CiscoCXSecurity/enum4linux ,Microsoft. (2017, marzo 14). Microsoft Security Bulletin MS17-010 – Critical. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010* .

El modificador -a instruye al programa para ejecutar todas las pruebas disponibles, lo cual resulta en una recolección integral de datos relacionados con los servicios SMB y NetBIOS del host objetivo.

Como resultado del análisis, se obtuvo la siguiente información:

- Nombre del equipo: PC202006
- Grupo de trabajo: WORKGROUP
- Servicios detectados: NetBIOS y SMB operativos

La evidencia recogida indica que el sistema objetivo mantiene habilitado el protocolo SMBv1, una versión obsoleta y vulnerable. Esta configuración respalda la hipótesis de exposición a la vulnerabilidad MS17-010, identificada por Microsoft en 2017 y frecuentemente explotada mediante el vector conocido como EternalBlue. La presencia de esta debilidad representa una amenaza significativa a la seguridad del sistema en cuestión.

Identificación y explotación

Durante las fases previas del análisis de seguridad, se recolectó un conjunto de datos que permitió identificar una posible debilidad crítica en el sistema evaluado. En particular, la detección del puerto 445 abierto, el uso del sistema operativo Windows 7 y la presencia activa del protocolo SMBv1 sin actualizaciones de seguridad aplicadas, orientaron la atención hacia una vulnerabilidad conocida en el entorno de Microsoft. Estas condiciones coincidían con las características de la vulnerabilidad MS17-010, comúnmente referida como EternalBlue, la cual ha sido ampliamente documentada en la literatura de ciberseguridad.

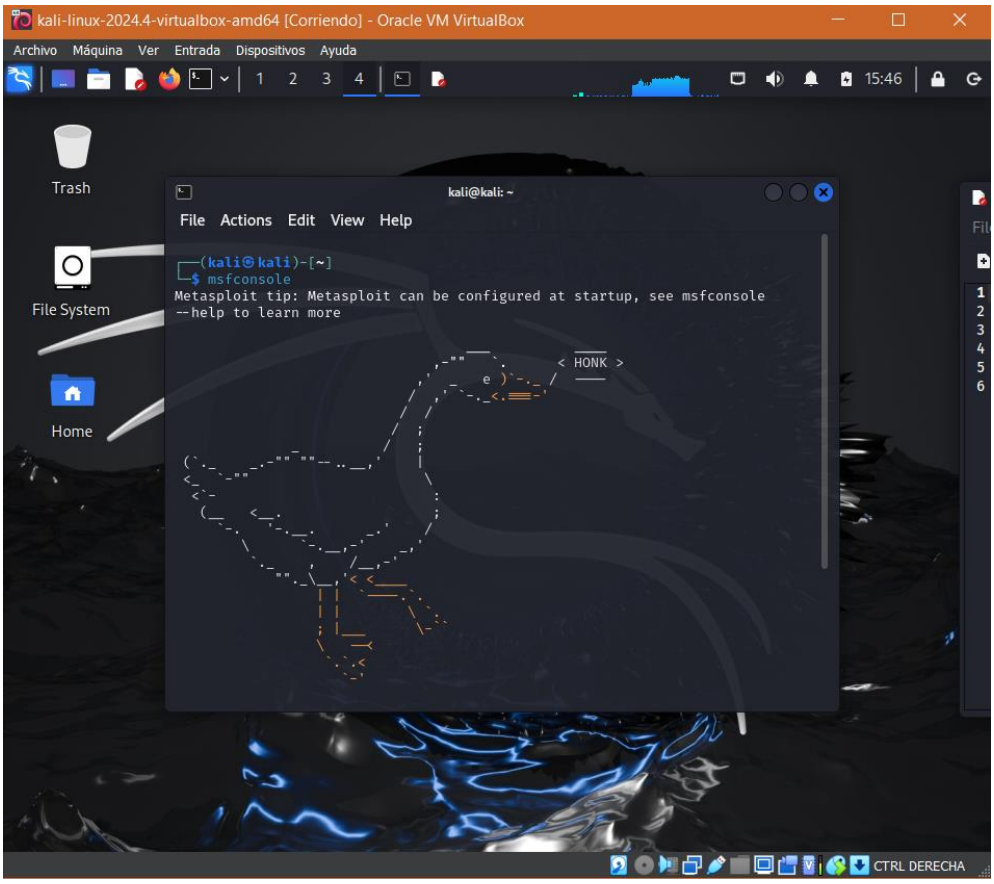
De acuerdo con el repositorio de vulnerabilidades CVE (Common Vulnerabilities and Exposures), esta falla específica, registrada bajo el identificador CVE-2017-0144, permite la ejecución remota de código malicioso sin necesidad de autenticación, aprovechando un error en el manejo de paquetes del protocolo SMB versión 1 (cve.org, 2017). Esta vulnerabilidad fue particularmente explotada en ataques a gran escala como WannaCry y NotPetya, lo que demuestra su criticidad.

Con el objetivo de verificar la exposición del sistema a dicha amenaza, se utilizó el framework Metasploit, herramienta estándar para pruebas de penetración. El proceso incluyó los siguientes pasos técnicos: primero, se accedió al entorno de Metasploit mediante el comando msfconsole. Luego, se localizó el módulo correspondiente mediante la instrucción search **ms17_010** y se seleccionó el módulo exploit/windows/smb/ms17_010_eternalblue. Posteriormente, se definieron los parámetros del ataque: la dirección IP del equipo víctima (RHOSTS), la del atacante (LHOST) y el tipo de carga útil a utilizar, que en este caso fue una shell inversa basada en Meterpreter.

Una vez configurados todos los valores, el ataque fue ejecutado con el comando run. El resultado fue positivo: se estableció una sesión remota activa con el sistema objetivo a través de Meterpreter, lo cual confirmó tanto la vulnerabilidad del entorno como la efectividad del exploit implementado.

Figura 11

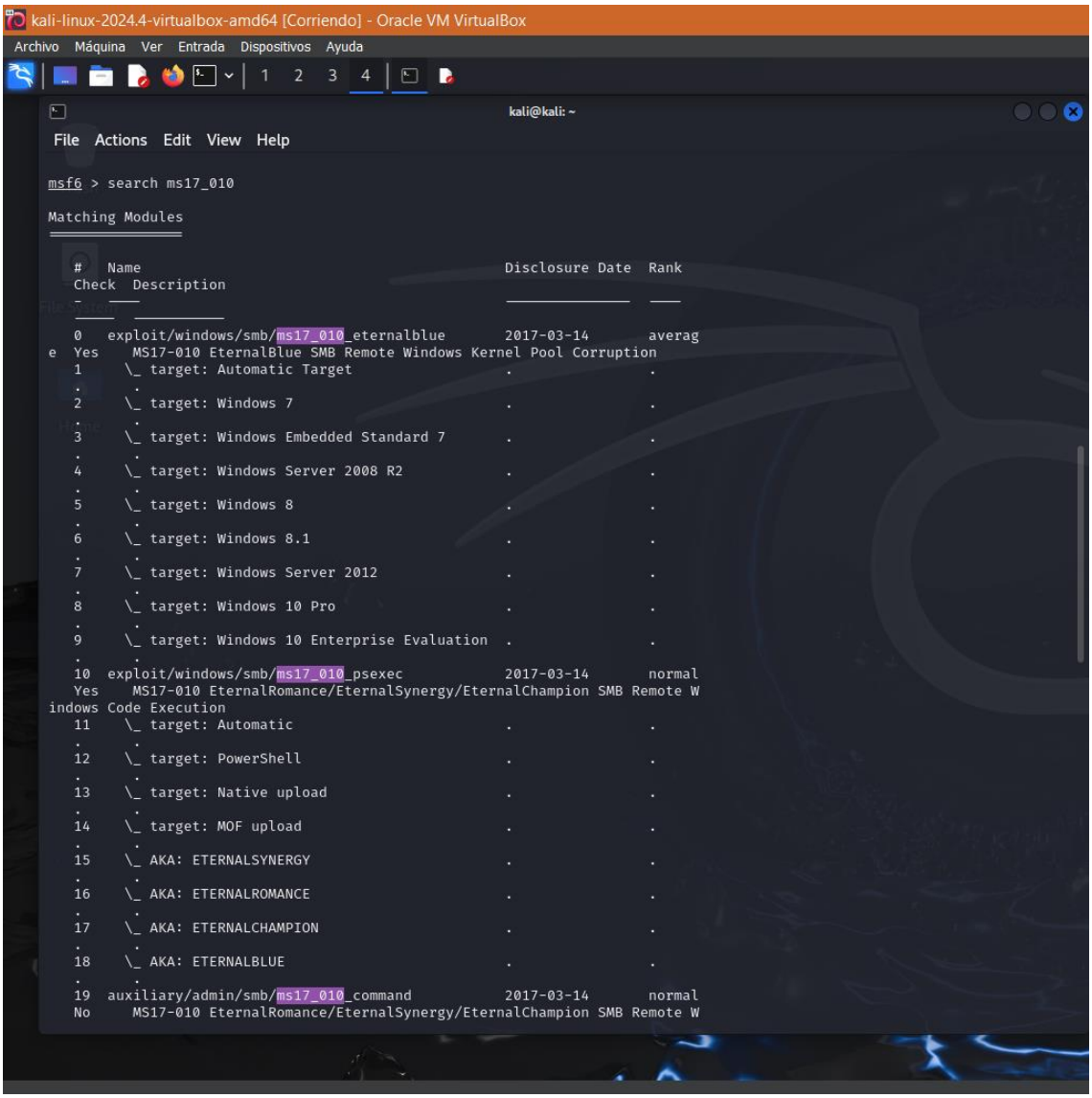
Uso de la herramienta Metasploit



Nota: Ejecución de la fase de explotación. **Fuentes:** *Autor (Joya, 2025).*

Figura 12

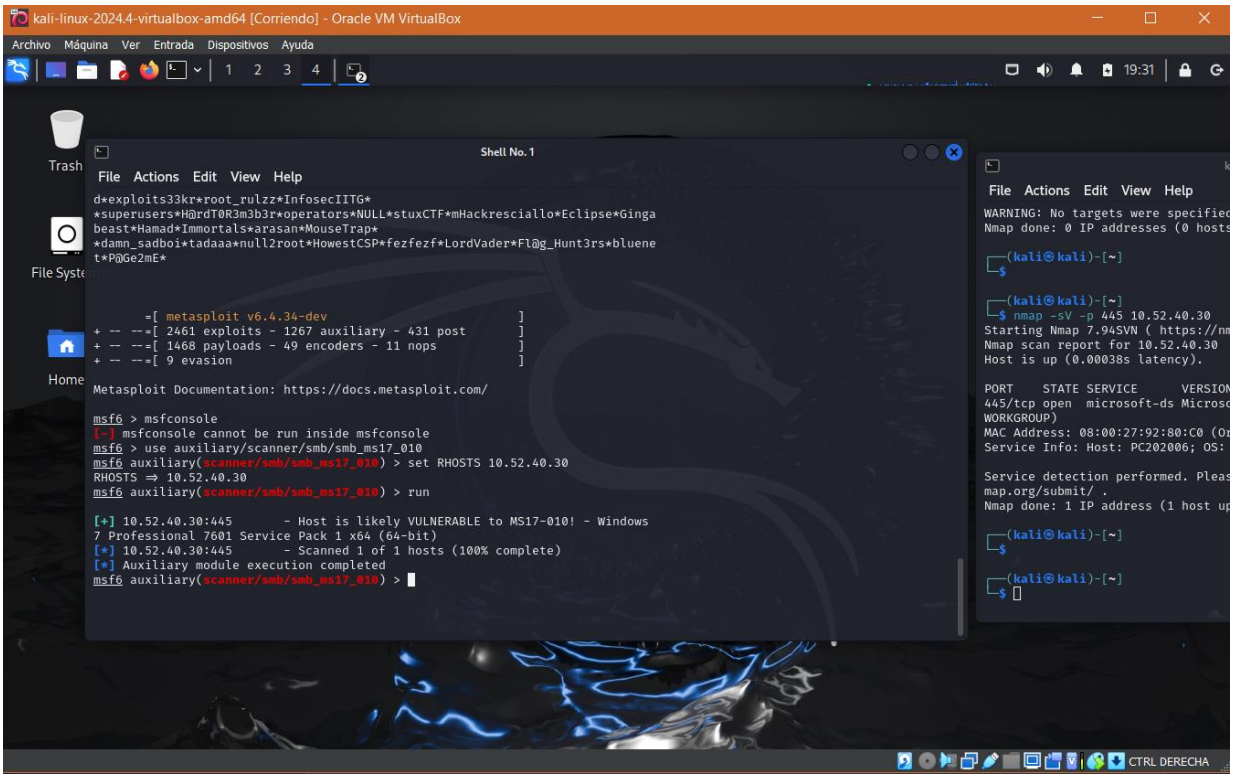
Ejecución del comando serch_ms17



Nota: Ejecución de la fase de identificación. **Fuentes:** *Autor (Joya, 2025).*

Figura 13

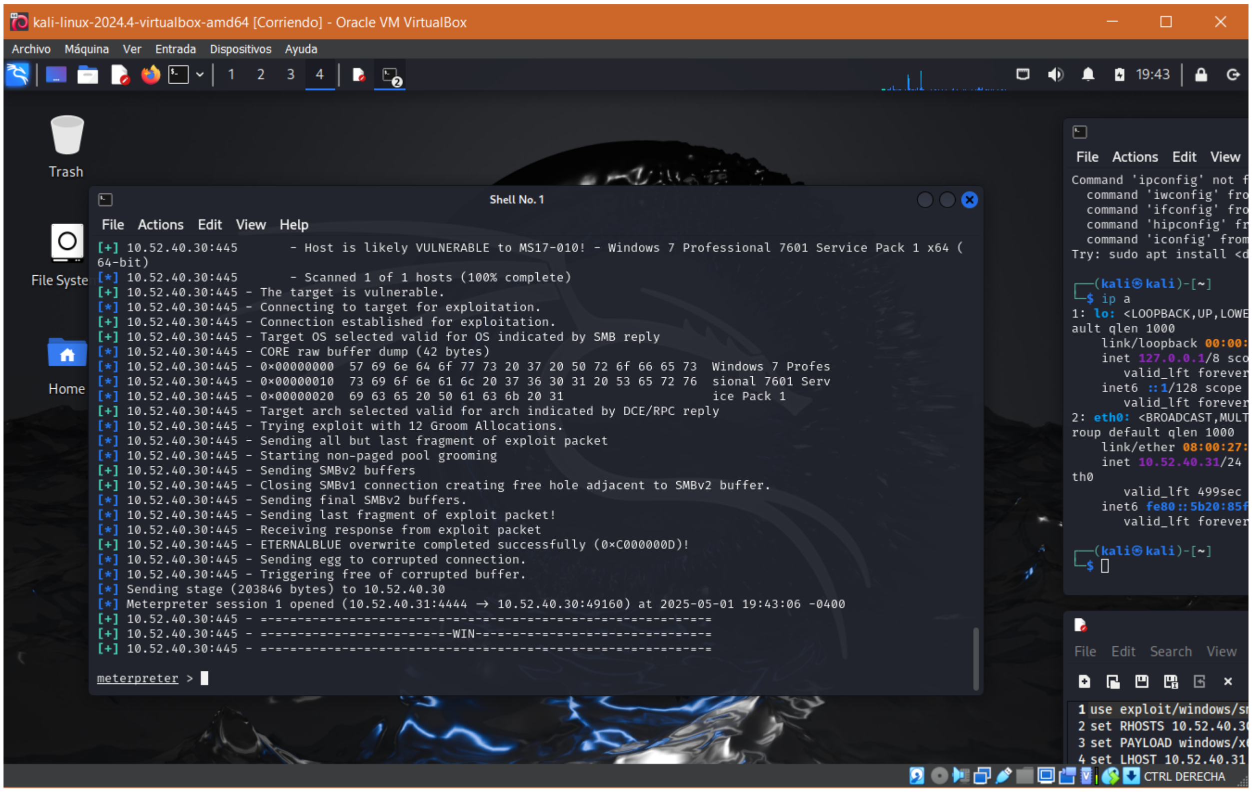
Explotar la vulnerabilidad y obtener acceso remoto



Nota: Mediante Meterpreter 7 se efectúa la explotación de la vulnerabilidad. **Fuentes:** *Autor (Joya, 2025).*

Figura 14

Ejecución exploit MS17-010 (EternalBlue)



Nota: Ejecución exitosa del exploit MS17-010 (EternalBlue). Se establece una sesión activa de Meterpreter sobre el sistema Windows 7 objetivo, permitiendo la ejecución remota de comandos y el inicio de tareas de post-explotación. **Fuentes:** *Autor (Joya, 2025).*

Post-explotación

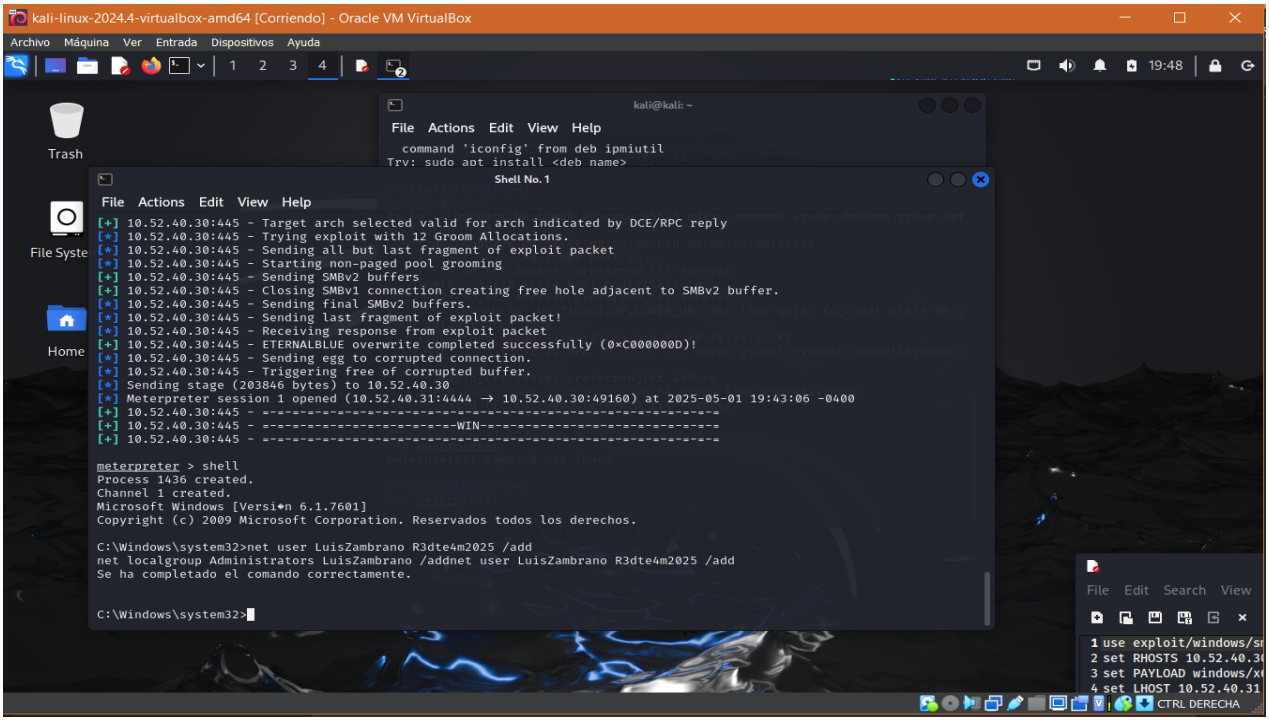
Una vez establecida la sesión remota mediante Meterpreter, se procedió a ejecutar una serie de comandos orientados a la escalada de privilegios y a la creación de un usuario con permisos administrativos como prueba de concepto (Proof of Concept, PoC). El proceso inició con el comando getuid, utilizado para identificar el usuario actual bajo el cual se están ejecutando las instrucciones en el sistema comprometido. Este paso permite verificar si la sesión se obtuvo con privilegios elevados, lo cual es común en el contexto de la vulnerabilidad MS17-010, donde usualmente se adquiere acceso con nivel SYSTEM, el privilegio más alto en sistemas Windows.

Posteriormente, se ejecutó el comando getsystem, que intenta escalar privilegios de forma automática para alcanzar dicho nivel. Finalmente, mediante el comando shell, se accedió directamente a una interfaz de línea de comandos del sistema objetivo, desde la cual es posible ejecutar instrucciones arbitrarias, gestionar usuarios, servicios, y realizar otras acciones típicas de la fase de post-explotación.

Estas acciones permiten confirmar no solo la explotación exitosa de la vulnerabilidad, sino también la capacidad de manipular el sistema comprometido con privilegios administrativos, lo cual representa un riesgo crítico de seguridad si no se aplican los parches correspondientes.

Figura 15

Ejecución exploit MS17-010 (EternalBlue)

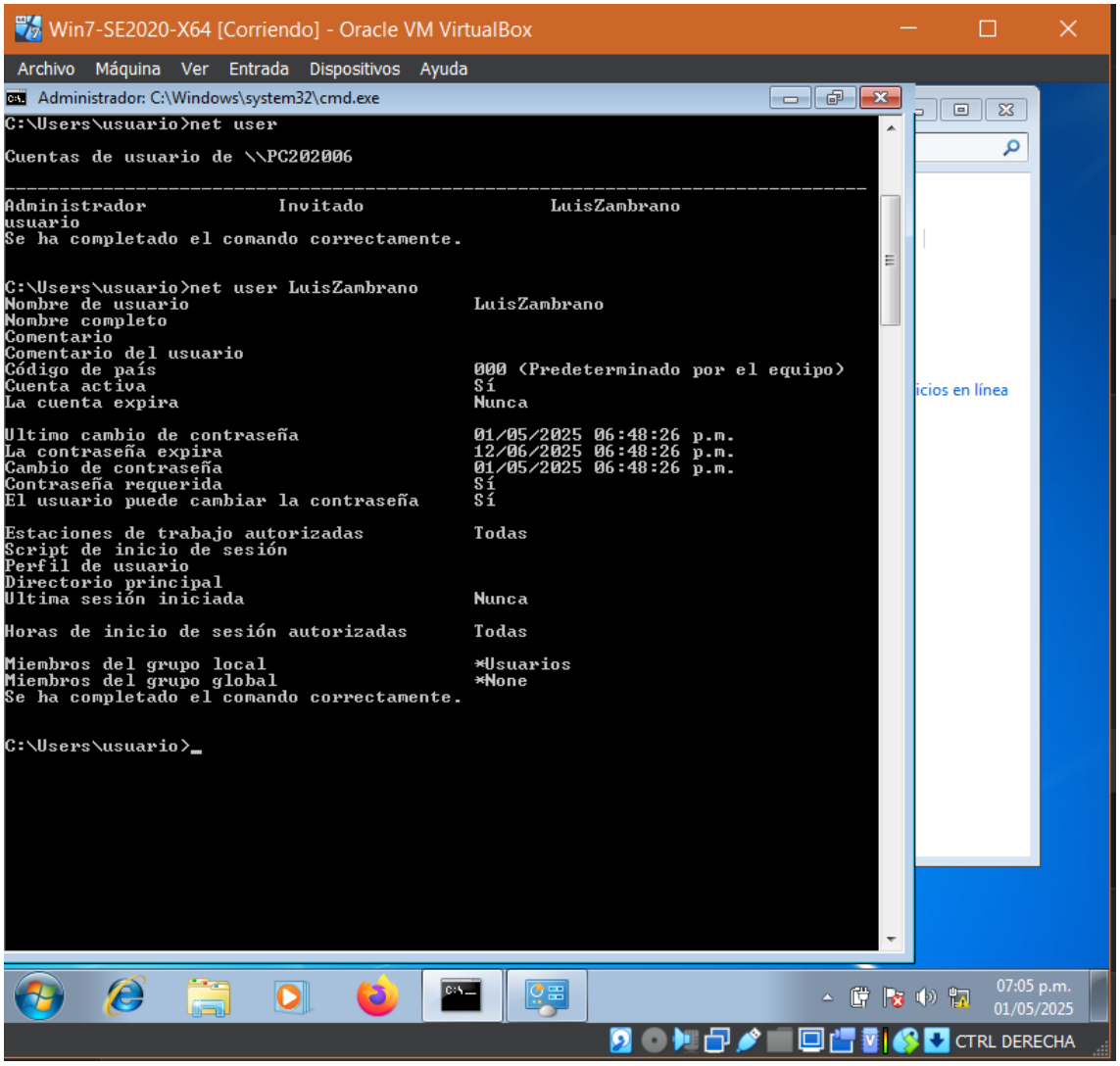


Nota: Explotación exitosa de la vulnerabilidad MS17-010 (EternalBlue) y ejecución de comandos de post-explotación. Se observa la apertura de una sesión Meterpreter con privilegios elevados, seguida de la transición a una shell del sistema donde se crea un nuevo usuario con privilegios de administrador ("LuisZambrano"). El comando se ejecuta correctamente, confirmando el control total del sistema remoto. **Fuentes:** *Autor (Joya, 2025).*

Finalmente, se procedió a verificar la creación exitosa del usuario en el sistema Windows comprometido. Esta validación permitió confirmar que el laboratorio se ejecutó correctamente, desde la detección de la vulnerabilidad hasta la explotación y post-explotación, evidenciando el control total sobre el sistema objetivo y la efectividad del procedimiento realizado.

Figura 16

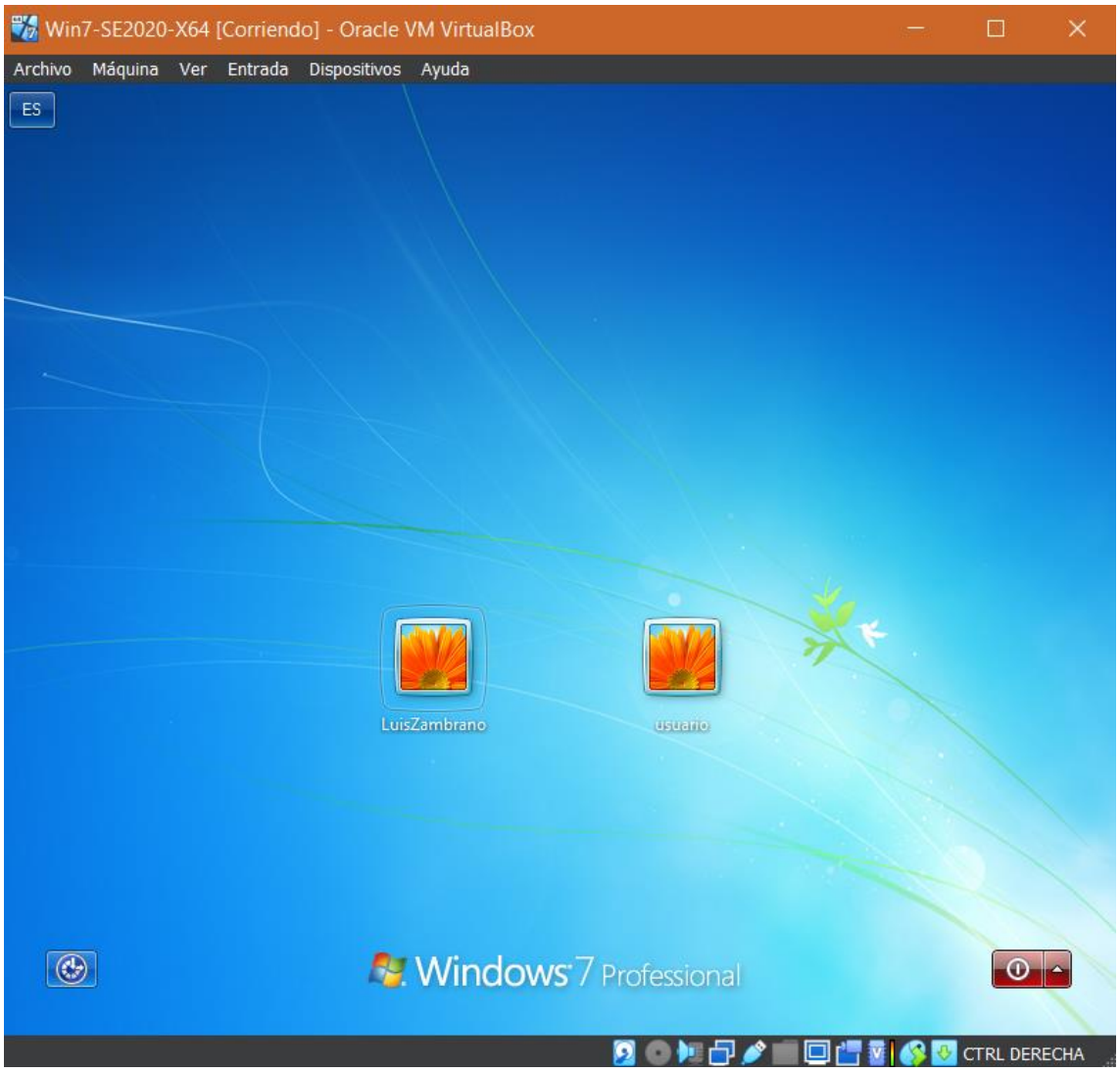
Verificación de la creación de usuario creado desde la consola de Win7



Fuentes: *Autor (Joya, 2025)*

Figura 17

Verificación de la creación de usuario creado desde el inicio de Win7-SE2020-X64



Fuentes: *Autor (Joya, 2025)*

Análisis del Impacto del Ataque mediante la Vulnerabilidad MS17-010 en Sistemas Windows

La presente investigación analiza las consecuencias de un ataque dirigido a sistemas operativos Windows, específicamente Windows 7, mediante la explotación de la vulnerabilidad crítica identificada como MS17-010, también conocida como EternalBlue. Esta debilidad, presente en implementaciones obsoletas del protocolo SMBv1, permite a actores maliciosos ejecutar código de forma remota sin necesidad de autenticación previa.

Impacto Específico de la Explotación

A través del envío de paquetes manipulados al puerto TCP 445, el atacante puede establecer una conexión con la máquina objetivo, sin requerir credenciales válidas. Este acceso no autorizado se facilita por la exposición del servicio SMBv1, que responde de manera vulnerable ante solicitudes maliciosas.

Ejecución de código con privilegios elevados

Una vez completada la explotación, se logra la ejecución remota de código con privilegios de nivel SYSTEM. Este nivel de acceso equivale a un control completo sobre el equipo comprometido, permitiendo al atacante ejecutar cualquier tipo de operación.

Implementación de persistencia mediante puertas traseras

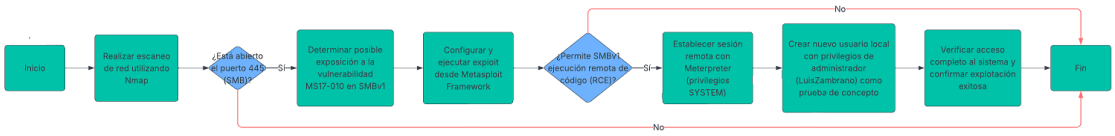
Utilizando un payload como Meterpreter, se establece una sesión inversa (reverse shell) que permite al atacante mantener acceso oculto y continuo a la máquina afectada, aún después de reinicios o desconexiones temporales.

Escalamiento de privilegios y creación de usuarios con acceso administrativo

Desde la sesión remota establecida, el atacante puede crear cuentas locales con privilegios elevados, como se evidenció en la creación del usuario "LuisZambrano". Esta acción garantiza un acceso persistente al sistema sin necesidad de repetir la explotación inicial.

Figura 18

Diagrama del ataque



Fuentes: *Autor (Joya, 2025)*

Etapa 4 – Contención de ataques informáticos

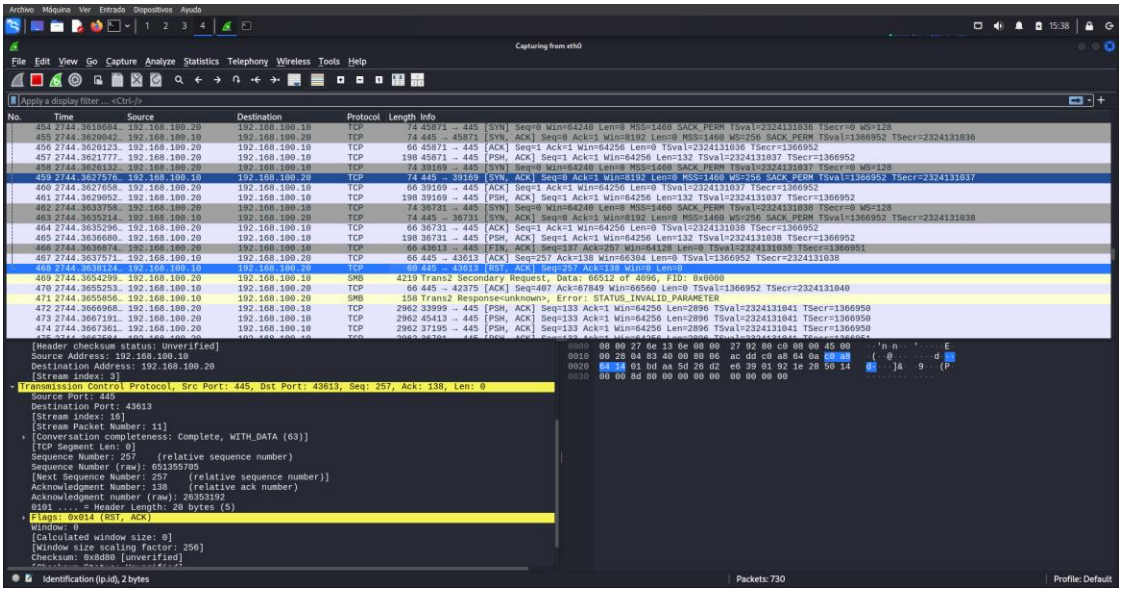
En un contexto donde los ataques informáticos avanzan en sofisticación y frecuencia, la función del equipo Blue Team se vuelve esencial en la defensa activa de los sistemas informáticos. En el escenario planteado por CyberFort Technologies, se presenta un ataque en tiempo real que explota la vulnerabilidad crítica MS17-010 en sistemas Windows obsoletos con SMBv1 habilitado. A partir de este contexto, se desarrolla el siguiente análisis técnico desde una perspectiva avanzada de ciberseguridad, fundamentado en prácticas de defensa proactiva, pensamiento adversarial y hardening de sistemas, utilizando únicamente herramientas con licencia libre.

Respuesta Inmediata ante el Ataque (Análisis Técnico)

Ante un ataque en tiempo real basado en la vulnerabilidad MS17-010, el primer paso crítico dentro del rol de un equipo Blue Team sería identificar y contener inmediatamente la amenaza, priorizando la mitigación del vector de ataque activo para limitar la propagación y los daños.

Figura 19

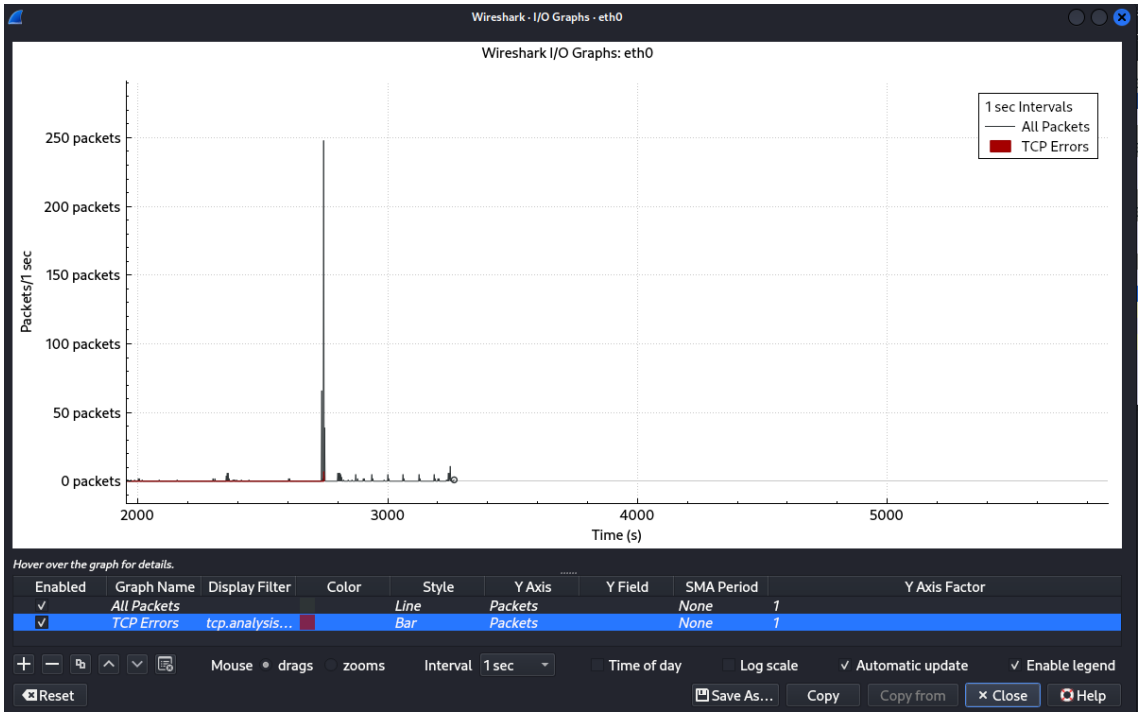
Uso de la herramienta Wireshark



Nota: Wireshark capturó el tráfico de red durante el ataque, permitiendo identificar las acciones del atacante con la máquina comprometida. **Fuente:** (Joya, 2025).

Figura 20

Datos de todos los paquetes en el ataque



Nota: Wireshark permite visualizar gráficamente el flujo de información intercambiado con la máquina comprometida. **Fuente:** (Joya, 2025).

2.1 Aislamiento de la máquina comprometida:

Lo primero sería aislar la máquina Windows comprometida de la red para detener cualquier comunicación externa e interna que permita la propagación del ataque, en particular si se trata de un ransomware como WannaCry o NotPetya, los cuales explotaron la vulnerabilidad MS17-010 mediante el puerto 445/TCP, "*esta acción se basa en la contención activa del incidente, que debe ejecutarse antes del análisis forense para evitar daños mayores"* (Scarfone & Mell, 2007).

Análisis en vivo validación de logs y procesos activos:

Luego del aislamiento, se utilizarían herramientas GPL o gratuitas como:

1. Sysinternals Suite (especialmente Process Explorer y TCPView) para observar procesos sospechosos y conexiones a través de SMB.
2. Wireshark para capturar y analizar tráfico SMB hacia/desde la máquina afectada.
3. Event Viewer para revisar logs de seguridad y sistema, buscando actividades inusuales relacionadas con el acceso remoto o ejecución de comandos.

Estas herramientas permiten verificar si el exploit EternalBlue ha sido utilizado, caracterizado por tráfico anómalo en el puerto 445/TCP. Validar si el sistema tiene aplicado el parche correspondiente a la vulnerabilidad MS17-010 (publicado por Microsoft en marzo de 2017). En caso de estar ausente, se confirma un fallo crítico de gestión de parches, lo cual es un hallazgo relevante para el reporte posterior.

El protocolo SMBv1 es inherentemente inseguro y ha sido descontinuado por Microsoft. Su explotación mediante EternalBlue permite ejecución remota de código sin autenticación (Microsoft, 2017). La estrategia inmediata debe enfocarse en:

1. Cortar el acceso al puerto 445 a través de reglas en el firewall de Windows Defender o desde la infraestructura de red.
2. Comprobar mediante *Get-SmbServerConfiguration* en PowerShell si SMBv1 está habilitado.

3. Ejecutar *netstat -an | findstr 445* para detectar conexiones abiertas y tasklist para vincular procesos sospechosos.

Captura de datos y evidencia:

Tabla 8

Herramientas GPL recomendadas del Blue Team.

Herramienta	Función
Wireshark	Captura de paquetes de red
Volatility	Análisis de memoria RAM
NetworkMiner	Extracción de artefactos de red
Sysmon + Wazuh	Registro de eventos avanzados

Nota: Este análisis inmediato permite al analista evaluar el alcance del ataque y preparar una respuesta contenida dentro de los lineamientos del NIST SP 800-61.

Medidas de Hardenización para Prevenir Reincidencias

Para evitar que un ataque como el ejecutado mediante la vulnerabilidad MS17-010 vuelva a producirse, es fundamental aplicar medidas de hardenización del sistema operativo y la red, con enfoque preventivo y de defensa en profundidad. El objetivo del hardening es reducir la superficie de ataque mediante la aplicación de controles técnicos. Las medidas propuestas incluyen:

a. Aplicación inmediata de parches de seguridad

La primera línea de defensa es mantener todos los sistemas actualizados con los últimos parches de seguridad. El parche MS17-010 corrige la vulnerabilidad que permite la ejecución

remota de código a través del protocolo SMBv1. “*La falta de aplicación de parches es una de las causas principales de incidentes de ciberseguridad graves” (Scarfone & Mell, 2007).*

b. Desactivación del protocolo SMBv1

SMBv1 es un protocolo obsoleto, vulnerable y no seguro. Su desactivación reduce significativamente el riesgo de explotación.

Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol"

Microsoft recomienda desactivar SMBv1 como medida de hardenización básica desde 2017 (Microsoft, 2017).

c. Segmentación de red y control de tráfico

Implementar segmentación de red para que los sistemas vulnerables no puedan ser accedidos lateralmente desde otras subredes. Además, se deben bloquear puertos no utilizados (como 445/TCP) mediante firewalls internos.

Acciones:

1. Configurar firewalls locales para negar acceso al puerto 445.
2. Implementar ACLs (Access Control Lists) en switches y routers.

d. Uso de autenticación multifactor (MFA)

Restringir el acceso administrativo a la red o servicios sensibles mediante MFA, reduciendo el riesgo de movimientos laterales en caso de compromisos de credenciales.

e. Monitoreo y detección de intrusiones

Implementar sistemas IDS/IPS basados en software libre como Snort o Suricata para detectar patrones de ataque como EternalBlue. "*El monitoreo de red en tiempo real permite una rápida respuesta ante intentos de explotación" (Scarfone & Mell, 2007).*

f. Revisión y limitación de cuentas administrativas

Reducir la superficie de ataque minimizando el número de cuentas con privilegios elevados y aplicando el principio de mínimos privilegios.

g. Copias de seguridad seguras y desconectadas

Asegurar backups periódicos, almacenados fuera de línea, para recuperar información en caso de un ataque exitoso de ransomware, que suele explotar MS17-010.

Tabla 9

Herramientas GPL recomendadas del Blue Team.

Medida	Justificación técnica
Deshabilitar SMBv1	El protocolo está obsoleto y vulnerable.
Aplicar parches automáticos	Previene que vulnerabilidades conocidas sean explotadas.
Implementar MFA	Reduce el riesgo de uso de credenciales comprometidas.
Segmentar redes con VLAN	Limita la lateralización del atacante.
Aplicar AppLocker	Controla qué ejecutables pueden correr en el sistema.

Nota: Estas acciones se alinean con los controles CIS v8, particularmente los controles 4, 5 y 7, orientados a la gestión de configuraciones, control de cuentas y protección contra malware.

Blue Team vs. Equipo de Respuesta a Incidentes

Aunque ambos equipos tienen funciones clave en la ciberseguridad defensiva, existen diferencias importantes en su propósito, alcance y enfoque operativo. A continuación, se explican con claridad estas diferencias:

a. Blue Team: Defensa proactiva y continua

El Blue Team es responsable de la defensa activa y continua de la infraestructura tecnológica de una organización. Su función principal es prevenir, detectar y contener ataques cibernéticos antes de que generen impacto. Para lograr esto, se apoya en herramientas de monitoreo, análisis de tráfico, correlación de eventos, pruebas de penetración defensivas y hardenización de sistemas.

Principales funciones del Blue Team:

1. Implementar controles de seguridad (firewalls, IDS/IPS, SIEM).
2. Analizar vulnerabilidades y aplicar parches.
3. Configurar alertas y reglas de detección.
4. Ejecutar simulacros de ataque (ej. purple teaming).
5. Evaluar continuamente la postura de seguridad.

"El Blue Team trabaja de manera constante en la mejora de la seguridad, incluso cuando no hay ataques en curso" (Scarfone & Mell, 2007).

b. Equipo de Respuesta a Incidentes Informáticos (CSIRT/CERT): Mitigación reactiva especializada

El equipo de Respuesta a Incidentes Informáticos (también conocido como CSIRT – Computer Security Incident Response Team) entra en acción cuando un incidente de seguridad ha sido detectado o reportado. Su enfoque es reactivo, centrado en la contención, erradicación, recuperación y análisis posterior del incidente.

Principales funciones del equipo de respuesta:

1. Identificar el tipo y alcance del incidente.
2. Aislar los sistemas comprometidos.
3. Realizar análisis forense digital.
4. Coordinar la recuperación de los sistemas.
5. Comunicar y documentar el incidente.

"Este equipo puede estar integrado dentro del Blue Team, pero actúa bajo procedimientos formales y escalables en casos de emergencia" (West-Brown et al., 2003).

Tabla 10

Comparación entre Blue Team y Equipo de respuesta a incidentes.

Característica	Blue Team	Equipo de Respuesta a Incidentes
Enfoque principal	Prevención y detección continua	Investigación y contención post-incidente
Tiempo de acción	Permanente	Reactivo ante eventos
Herramientas utilizadas	IDS, SIEM, hardening, monitoreo continuo	Forense, snapshots, reporte de incidentes
Integración con otros equipos	Colaboración con Red Team y DevSecOps	Coordinación con legal y cumplimiento

Nota: Ambos equipos son esenciales para una estrategia de ciberseguridad holística, pero cumplen roles complementarios.

Tabla 11

Diferencia clave enfoque BLUE TEAM proactivo vs. CSIRT reactivo

Aspecto	Blue Team	Respuesta a Incidentes (CSIRT)
Enfoque	Proactivo (prevención)	Reactivo (respuesta)
Activación	Permanente	Se activa ante incidentes confirmados
Herramientas utilizadas	SIEM, EDR, análisis de vulnerabilidades	Forense digital, análisis de malware
Objetivo principal	Fortalecer la seguridad	Mitigar y resolver incidentes
Tiempo de acción	Antes y durante un posible ataque	Durante y después del ataque

Nota: Ambos equipos son esenciales para una estrategia de ciberseguridad holística, pero cumplen roles complementarios.

5. Utilidad del CIS para el Blue Team

Dentro de un equipo Blue Team, el uso del CIS (Center for Internet Security) es fundamental para establecer, implementar y mantener estándares de seguridad sólidos y comprobados, conocidos como CIS Benchmarks y CIS Controls. Estas guías permiten elevar el nivel de protección de los sistemas tecnológicos de una organización de forma estructurada y basada en buenas prácticas reconocidas globalmente.

El Center for Internet Security (CIS) provee directrices estructuradas que permiten:

- Estandarizar configuraciones seguras con CIS Benchmarks.
- Evaluar el cumplimiento mediante herramientas como CIS-CAT.
- Priorizar medidas según riesgo operativo.

Estas guías son utilizadas por agencias federales y empresas Fortune 500, permitiendo al Blue Team aplicar mejoras de seguridad medibles y verificables (CIS, 2024).

Principales fines del uso del CIS en un equipo Blue Team

a. Hardenización de sistemas (CIS Benchmarks)

Uno de los principales usos del CIS es la hardenización del sistema operativo, aplicaciones y servicios. Los CIS Benchmarks son listas detalladas de configuraciones recomendadas, clasificadas por nivel de criticidad (por ejemplo, para Windows Server, Linux, bases de datos, navegadores, etc.).

Ejemplo: En el contexto del ataque por MS17-010 en Windows, se utilizarían los CIS Benchmarks para Windows para asegurar que:

1. SMBv1 esté desactivado.

2. El acceso remoto esté restringido.

3. Las políticas de contraseñas sean robustas.

"Estas configuraciones reducen drásticamente la superficie de ataque" (CIS, 2024).

b. Evaluación y mejora continua de la postura de seguridad (CIS Controls)

El CIS también proporciona los CIS Controls (anteriormente conocidos como Critical Security Controls), una lista priorizada de acciones defensivas diseñadas para mitigar las amenazas cibernéticas más comunes.

Ejemplos clave para Blue Team:

Control 4: Uso controlado de privilegios administrativos.

Control 7: Protección de puertos de red y servicios innecesarios.

Control 8: Implementación de monitoreo y auditoría.

"Estos controles permiten construir una estrategia de defensa basada en riesgo, adaptable al tamaño y madurez de la organización" (CIS, 2024).

c. Auditoría de cumplimiento

El CIS permite a los equipos Blue Team realizar auditorías de cumplimiento de configuración mediante herramientas como OpenSCAP, Lynis, o scripts automatizados que comparan las configuraciones reales del sistema con los benchmarks establecidos.

d. Capacitación y desarrollo de políticas

El CIS también proporciona documentación valiosa para educar al equipo técnico, desarrollar políticas organizacionales y justificar decisiones de seguridad ante la dirección ejecutiva o entes reguladores.

Funciones y Características del SIEM

Un SIEM (Security Information and Event Management, por sus siglas en inglés) es una solución tecnológica utilizada por los equipos de ciberseguridad —como el Blue Team— para la detección, análisis, respuesta y gestión de eventos de seguridad en tiempo real o retrospectivo. Su objetivo principal es proporcionar visibilidad centralizada de la seguridad de una organización mediante el análisis de registros y eventos generados por distintos sistemas tecnológicos.

Funciones principales de un SIEM

a. Recolección y correlación de registros

Un SIEM recopila eventos de seguridad desde múltiples fuentes: firewalls, servidores, routers, sistemas operativos, bases de datos, aplicaciones y dispositivos de seguridad. Luego, correlaciona estos eventos para detectar patrones que podrían indicar actividades maliciosas. **Ejemplo:** Si un usuario falla múltiples intentos de inicio de sesión en varios sistemas y luego accede exitosamente desde una IP externa, el SIEM puede generar una alerta.

b. Monitoreo en tiempo real

El SIEM permite un monitoreo continuo de los eventos, facilitando la detección temprana de incidentes y la activación de alertas automatizadas ante comportamientos anómalos.

c. Generación de alertas

Basado en reglas definidas por analistas o plantillas preconfiguradas, el SIEM genera alertas de seguridad ante eventos sospechosos, como escaneos de puertos, escalamiento de privilegios, movimientos laterales o conexiones desde ubicaciones no autorizadas.

d. Análisis forense y trazabilidad

Un SIEM mantiene un histórico detallado de los eventos, permitiendo el análisis forense posterior a un incidente. Esto es esencial para identificar cómo ocurrió el ataque, qué sistemas se vieron comprometidos y qué datos fueron afectados.

e. Cumplimiento normativo

Muchas normas de seguridad como ISO/IEC 27001, PCI-DSS, HIPAA, y GDPR requieren monitoreo de eventos de seguridad y trazabilidad. Un SIEM facilita el cumplimiento de estos estándares mediante reportes automáticos y almacenamiento de logs.

Tabla 12

Características de SIEM

Característica	Descripción
Centralización	Agrega eventos de múltiples fuentes en una sola plataforma.
Correlación de eventos	Detecta ataques complejos mediante la relación de eventos aparentemente aislados.
Automatización	Genera alertas automáticas y puede integrarse con SOAR para respuesta automatizada.
Escalabilidad	Puede adaptarse a infraestructuras pequeñas o grandes.
Visualización de datos	Paneles gráficos (dashboards) para facilitar el análisis de seguridad.

Nota: Los SIEM permiten implementar detecciones personalizadas basadas en TTPs del framework MITRE ATT&CK.

Ejemplos de herramientas SIEM (licencia libre o GPL)

1. Wazuh: Basado en OSSEC, con capacidades avanzadas de SIEM.
2. ELK Stack (Elasticsearch, Logstash, Kibana): Popular para la centralización y visualización de logs.
3. Security Onion: Plataforma que integra varias herramientas para detección, monitoreo y análisis forense.

Importancia del SIEM para el Blue Team

Para un equipo Blue Team, el SIEM es una herramienta estratégica porque permite:

1. Anticiparse a amenazas mediante análisis de comportamiento.
2. Responder rápidamente a incidentes de seguridad.
3. Analizar ataques pasados para mejorar defensas futuras.
4. Cumplir con auditorías y normativas de seguridad.

Herramientas de Contención de Ataques (Software y Hardware)

Las herramientas de contención de ataques informáticos tienen como función principal detener la propagación del ataque, aislar sistemas comprometidos, y minimizar el impacto dentro de la infraestructura tecnológica de una organización. A diferencia de las herramientas de detección, que se enfocan en identificar amenazas, las de contención se activan para frenar o interrumpir la actividad maliciosa.

Tabla 13

Herramientas de contención de Ataques.

Item	Herramienta	Tipo (Hardware/Software)	Descripción técnica y función de contención	Ejemplo(s)
	Firewall de próxima generación (NGFW)	Hardware / Software	Inspecciona el tráfico de red en tiempo real con capacidades avanzadas como inspección profunda de paquetes (DPI), filtrado por aplicaciones, control de usuarios y detección de amenazas. Permite	pfSense (GPL), Palo Alto, FortiGate

		bloquear tráfico malicioso, cerrar conexiones activas, y segmentar reglas por zonas de seguridad. Ideal para contener movimientos laterales y ataques de red.	
Segmentación de red (VLANs / Zonas)	Configuración / Hardware	Permite dividir la red física en subredes lógicas aisladas (VLANs), lo que **limita la propagación de ataques** al impedir que un dispositivo comprometido acceda libremente a otros segmentos. Es una medida clave de contención al permitir el confinamiento de un ataque en una sola zona o red sin afectar los servicios críticos.	VLANs en Cisco/Mikrotik, firewalls UTM
EDR (Endpoint Detection and Response)	Software	Herramientas instaladas en endpoints que permiten **detectar, investigar y contener amenazas**. Algunas soluciones EDR permiten **aislar remotamente un equipo de la red**, terminar procesos maliciosos y revocar sesiones activas. Aunque su enfoque es también de detección, sus funciones de contención son esenciales frente a amenazas persistentes.	Wazuh (GPL), OSSEC, CrowdStrike
NAC (Network Access Control)	Hardware / Software	Controla qué dispositivos pueden acceder a la red corporativa. Si un equipo no cumple políticas de seguridad, el NAC puede **denegar el acceso o ubicar al dispositivo en una red aislada**, evitando la propagación de malware o accesos no autorizados. Útil en redes empresariales con múltiples dispositivos y usuarios.	PacketFence (GPL), Cisco ISE
Honeypots activos con respuesta dinámica	Software	Sistemas señuelo diseñados para atraer a los atacantes. Algunos honeypots avanzados, como Cowrie, pueden **generar reglas automáticas de bloqueo** (por ejemplo, en el firewall) cuando detectan interacciones maliciosas. Esto permite **engañar al atacante y proteger los activos reales**, mientras se bloquea su IP o comportamiento a futuro.	Cowrie, T-Pot, Dionaea
WAF (Web Application Firewall)	Hardware / Software	Inspecciona y filtra el tráfico HTTP/HTTPS que va dirigido a aplicaciones web. Permite **bloquear ataques como SQL Injection, XSS, file inclusion, etc.** en tiempo real, impidiendo que lleguen al servidor de aplicaciones. Es crucial para contener ataques dirigidos a sitios web o APIs expuestas a internet.	ModSecurity (GPL), NAXSI, AWS WAF

Nota: Estas herramientas actúan como línea directa de defensa, limitando el avance del atacante sin necesidad de intervención humana inmediata.

Pensamiento Adversarial en la Ciberdefensa

El pensamiento adversarial, técnica proveniente del ámbito militar, consiste en anticiparse al comportamiento del atacante. En ciberseguridad, esto se traduce en:

- Crear entornos honeypot para estudiar comportamiento malicioso.
- Simular ataques con Purple Team para validar defensas.
- Aplicar red teaming continuo para mejorar capacidades del Blue Team.

Referentes como Wang et al. (2020) destacan que este enfoque permite una mejor comprensión del ciclo de vida del ataque y fomenta respuestas más eficientes.

Conclusiones

La evolución acelerada de las tecnologías digitales en Colombia ha traído consigo oportunidades, pero también desafíos significativos en materia de seguridad y protección de la información. Esta realidad demanda una respuesta integral, donde la ciberseguridad no se limite a reacciones técnicas aisladas, sino que incorpore visión estratégica, pensamiento adversarial y un marco normativo sólido. El presente trabajo evidenció, a través de simulaciones prácticas y análisis técnico, la importancia de adoptar metodologías ofensivas (Red Team) y defensivas (Blue Team) como pilares complementarios para evaluar y fortalecer la postura de seguridad de las infraestructuras tecnológicas.

Desde el plano legal, instrumentos como la Ley 1273 de 2009 y la Ley 1581 de 2012 han sido fundamentales para tipificar los delitos informáticos y garantizar el derecho a la protección de datos personales. No obstante, se hace necesaria una actualización continua de la legislación y su articulación con marcos internacionales como la ISO/IEC 27001 y el Convenio de Budapest, con el fin de enfrentar amenazas cada vez más sofisticadas, como el ciberespionaje, el ransomware y la explotación de vulnerabilidades persistentes (Microsoft, 2017; ISO, 2022).

La experiencia práctica adquirida mediante el uso de herramientas como Metasploit, Nmap y OpenVAS permitió comprender el ciclo completo de una intrusión, desde el reconocimiento hasta la explotación y la obtención de acceso remoto. Particularmente, el caso de la vulnerabilidad MS17-010, aún vigente en infraestructuras desactualizadas, reafirmó la

necesidad de políticas rigurosas de parcheo, eliminación de servicios inseguros como SMBv1, y monitoreo continuo de puertos críticos como el 445/TCP (Mitre, 2023; Rapid7, 2017).

En paralelo, el trabajo defensivo destacó el valor de soluciones de contención, tanto propietarias como de código abierto, como Wazuh, ModSecurity y análisis de tráfico con Wireshark. Estas herramientas, alineadas con los controles del Center for Internet Security (CIS, 2024), demostraron que es posible lograr una respuesta efectiva incluso con recursos limitados, siempre que exista planificación, formación y cultura organizacional en ciberseguridad.

El pensamiento adversarial, entendido como la capacidad de anticiparse a las técnicas y comportamientos del atacante, se consolidó como una competencia crítica para la ciberdefensa moderna (Wang et al., 2020). Este enfoque permite no solo detectar fallas antes de que sean explotadas, sino también diseñar defensas más inteligentes, resilientes y adaptables al entorno cambiante de amenazas.

Finalmente, este proceso de aprendizaje y aplicación práctica reafirma que la ciberseguridad debe ser concebida como una responsabilidad compartida entre el Estado, el sector privado, la academia y la sociedad civil. Más allá del cumplimiento normativo, se requiere un compromiso ético, una visión preventiva y una inversión constante en talento humano altamente capacitado. Solo así será posible construir entornos digitales seguros, resilientes y acordes a los retos del siglo XXI.

Referencias Bibliográficas

Bishop, M. (2019). Computer security: Art and science (2nd ed.). Addison-Wesley.

Center for Internet Security. (2024). CIS Controls v8. https://www.cisecurity.org

Congreso de Colombia. (2008). Ley 1266 de 2008. https://www.funcionpublica.gov.co

Congreso de Colombia. (2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y los datos. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34506

Congreso de Colombia. (2012). Ley 1581 de 2012. https://www.sic.gov.co

Consejo Profesional Nacional de Ingeniería – COPNIA. (2019). Código de Ética Profesional de los Ingenieros. https://www.copnia.gov.co

Departamento Nacional de Planeación (DNP). (2020). Documento CONPES 3995: Política Nacional de Confianza y Seguridad Digital. https://www.dnp.gov.co

Dradis Framework. (2023). Collaborative Information Sharing. https://dradisframework.com

ENISA. (2021). Good practices for incident response teams. https://www.enisa.europa.eu

Greenberg, A. (2018). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Doubleday.

Greenbone Networks. (2024). OpenVAS - Vulnerability Scanning. https://www.greenbone.net

Guerrero, J. A. (2012). La ley 1273 de 2009 y su impacto en la protección de los datos personales y la ciberseguridad en Colombia. Revista Digital de Derecho Informático. https://revistas.unal.edu.co/index.php

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

International Information System Security Certification Consortium. (2020). Code of ethics. https://www.isc2.org/Ethics

International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems. https://www.iso.org/isoiec-27001-information-security.html

Kizza, J. M. (2017). Ethical and social issues in the information age (6th ed.). Springer.

Lyon, G. (2009). Nmap network scanning. Insecure.Com LLC.

Microsoft. (2017). Microsoft Security Bulletin MS17-010 - Critical. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Microsoft. (2023). Sysinternals Suite. https://docs.microsoft.com/en-us/sysinternals

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). Política de seguridad digital. https://mintic.gov.co

MITRE. (2023). CVE-2017-0144. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

MITRE. (2024). ATT&CK Framework. https://attack.mitre.org

MITRE. (2024). Common Vulnerabilities and Exposures (CVE). https://www.cve.org

ModSecurity. (2024). Open Source Web Application Firewall. https://modsecurity.org

Offensive Security. (2024). Exploit Database. https://www.exploit-db.com

OCDE. (2013). Directrices sobre la protección de la privacidad y flujos transfronterizos de datos personales. https://www.oecd.org/sti/ieconomy/oecdguidelinesonprivacy.htm

Presidencia de la República. (2013). Decreto 1377 de 2013. https://www.funcionpublica.gov.co

Rapid7. (2017). Metasploit module: exploit/windows/smb/ms17_010_eternalblue. https://docs.rapid7.com/metasploit/ms17_010_eternalblue/

Rapid7. (2024). Metasploit Framework. https://www.rapid7.com

Rowe, N., & Rrushi, J. (2016). Introduction to cyberdeception. Springer.

SANS Institute. (2018). Detecting and preventing lateral movement. https://www.sans.org/white-papers/38980/

Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy (NIST SP 800-41 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-41r1

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2022). Guide to general server security. NIST SP 800-123.

Skoudis, E., & Liston, T. (2013). Counter hack reloaded: A step-by-step guide to computer attacks and effective defenses. Prentice Hall.

Stewart, J. M., Chapple, M., & Gibson, D. (2021). CISSP (ISC)² certified information systems security professional official study guide (9th ed.). Wiley.

Symantec. (2017). What you need to know about the WannaCry ransomware. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware

Tanczer, L. M., López, O., & Carr, M. (2018). Cybersecurity: Politics, governance and conflict in cyberspace. Zed Books.

Wang, P., Lu, J., & Liu, L. (2020). Adversarial thinking in cybersecurity: Applying military concepts to cyber defense. ACM Computing Surveys, 53(6), 1–36.

Wazuh. (2024). The open source security platform. https://wazuh.com

Link enlace al video de socialización:

https://youtu.be/inyxpfj8LYs?si=PBQfq7B9hAUAvb7q


Objetivos del Informe Técnico
UNAD
Universidad Nacional Abierta y a Distancia
ACREDITADA EN ALTA CALIDAD
Objetivo General
Formular estrategias efectivas mediante simulaciones
Objetivos Específicos
Simular ataques reales
Aplicar medidas de contención
Proponer mejoras críticas y profesionales
Imagen 1
Número de denuncias por delitos informáticos en Colombia
NUMERO DE DENUNCIAS POR DELITOS INFORMATICOS EN COLOMBIA
Capacidades técnicas, legales y de gestión para equipos blue team y red team
Camilo Andres JOI...
Estadísticas
Editar vídeo
0
Compartir
Guardar