Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

Freddy Alexander León Neira

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería – ECBTI.

Especialización en Seguridad Informática.

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

Bucaramanga – Santander

Mayo, 2025.

Dedicatoria

Dedico este logro con todo mi corazón a mi querida esposa, Paula Alejandra Arciniegas. Gracias por ser mi roca, mi compañera incansable y mi mayor apoyo en cada momento, por tus palabras de aliento especialmente en los días difíciles o en las noches largas, por creer en mí cuando yo dudaba. Tu amor y paciencia me dieron fuerzas para seguir adelante. Sin ti, este camino habría sido más duro.

A mis hijos, AnaLu, Juan y Mateo, ustedes son la luz que ilumina mi vida. Cada sonrisa, cada abrazo, cada pregunta curiosa "¿Papi te falta mucho para terminar?, quiero jugar contigo" y cada instante compartido me recuerdan la importancia de luchar por un futuro mejor y qué vale la pena esforzarse. Espero que este logro les inspire a perseguir sus sueños con valentía y pasión.

A mi madre, cuyo amor incondicional y ejemplo de perseverancia han sido mi guía constante. Gracias por enseñarme con tu vida que la dedicación y el sacrificio siempre tienen recompensa.

Y de manera muy especial, a mi tía Omaira Neira, quien ha estado a mi lado incondicionalmente, brindándome su cariño, consejos y apoyo en los momentos más importantes. Tu presencia ha sido un verdadero regalo que me ha sostenido en los momentos más difíciles.

A todos ustedes, les entrego mi más profunda gratitud y todo mi amor. Este logro es tan suyo como mío.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a mi tutor, por su guía paciente, sus valiosas observaciones y su compromiso con mi proceso de formación. Agradezco también a todos mis profesores, quienes, con su conocimiento y dedicación, han enriquecido mi visión sobre la ciberseguridad. A mis compañeros de estudio, por su colaboración, sus debates enriquecedores y el espíritu de equipo que hizo más llevadero este desafío. Un reconocimiento especial a todos los colegas que han trabajado y siguen trabajando en el campo de la ciberseguridad; su innovación y esfuerzo constante han sido fuente de inspiración y aprendizaje. Finalmente, agradezco a todas las personas y entidades que, de una u otra forma, han contribuido con recursos, apoyo técnico y motivación para que este proyecto sea una realidad.

Resumen

Este informe presenta las competencias técnicas, legales y de gestión necesarias para los Blue Team y Red Team en la dimensión de la seguridad cibernética organizacional, se analizan los marcos legislativos colombianos en el contexto de delitos informáticos y protección de datos personales, así como las etapas y herramientas claves en la ejecución de pruebas de penetración.

Incluye el trabajo práctico de las herramientas Metasploit, Nmap, OpenVAS entre otras, como los servicios en línea ExploitDB, CVE, a través de la implementación de un escenario controlado o un banco de trabajo virtual, se vuelve evidente la importancia de la formación técnica y del conocimiento del entorno legal para tomar decisiones más sólidas en lo relacionado con la defensa y la respuesta a incidentes en infraestructuras TI.

Palabras clave**:** análisis forense, auditoría informática, blue team, ciberseguridad, contención de incidentes, CVE, delitos informáticos, gestión de incidentes, Metasploit, Nmap, OpenVAS, pentesting, red team, resiliencia organizacional, SIEM, virtualización.

Abstract

This report presents the technical, legal, and management skills required for Blue Teams and Red Teams in the area of organizational cybersecurity. It analyzes Colombian legislative frameworks in the context of cybercrime and personal data protection, as well as the key stages and tools for conducting penetration tests.

It includes practical work with Metasploit, Nmap, and OpenVAS tools, among others, as well as the online services ExploitDB and CVE. Through the implementation of a controlled scenario or virtual workbench, the importance of technical training and knowledge of the legal framework for making more sound decisions regarding defense and incident response in IT infrastructures becomes evident.

Keywords**:** blue team, CVE, cybersecurity, cybercrime, forensic analysis, incident containment, incident management, IT auditing, Metasploit, Nmap, OpenVAS, organizational resilience, pentesting, red team, SIEM, virtualization.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Anexos

Glosario

Análisis forense digital: Proceso de identificación, preservación, análisis y presentación de datos informáticos con el fin de investigar incidentes de seguridad, delitos informáticos o fraudes. Permite obtener evidencia válida para procedimientos legales (Casey, E. 2011).

Auditoría informática: Evaluación sistemática de los sistemas de información de una organización para verificar la integridad, confidencialidad y disponibilidad de los datos, así como el cumplimiento de normativas y políticas internas (Pathak, 2014).

Blue Team: Equipo responsable de la defensa activa de la infraestructura tecnológica de una organización. Su labor es detectar, responder y mitigar incidentes de seguridad, así como fortalecer la resiliencia del entorno ante ataques (Colbert et al., 2020).

Ciberseguridad: Conjunto de prácticas, procesos y tecnologías diseñadas para proteger sistemas, redes y datos frente a ataques, daños o accesos no autorizados (Craigen et al., 2014).

Contención de incidentes: Acciones tomadas para limitar el alcance y el impacto de un incidente de seguridad, evitando su propagación y facilitando la recuperación (NIST SP 800-61r2, 2012).

CVE (Common Vulnerabilities and Exposures): Sistema de referencia pública que proporciona identificadores únicos para vulnerabilidades conocidas de software, facilitando el intercambio de información entre organizaciones (MITRE, 2024).

Delitos informáticos: Conductas ilícitas que afectan la confidencialidad, integridad o disponibilidad de los sistemas y datos informáticos, tales como acceso no autorizado, sabotaje o fraude digital (Congreso de la República de Colombia, 2009).

ExploitDB: Base de datos pública de exploits y vulnerabilidades, utilizada por profesionales de seguridad para identificar y analizar debilidades en sistemas y aplicaciones (Exploit Database, 2024).

Gestión de incidentes: Proceso estructurado para identificar, analizar, responder y recuperarse de incidentes de seguridad informática, minimizando el daño y restaurando las operaciones normales (ENISA, 2016).

Metasploit: Plataforma de software utilizada para desarrollar, probar y ejecutar exploits contra sistemas informáticos, ampliamente empleada en pruebas de penetración (pentesting) (Maynor, 2011).

Nmap: Herramienta de código abierto para escaneo de redes y detección de hosts y servicios, utilizada en la fase de reconocimiento y análisis de vulnerabilidades (Lyon, 2009).

OpenVAS: Framework de código abierto para la gestión y escaneo de vulnerabilidades, que permite identificar debilidades en sistemas y aplicaciones (OpenVAS, 2024).

Pentesting (Pruebas de penetración): Metodología que simula ataques reales para identificar y explotar vulnerabilidades en sistemas, redes o aplicaciones, con el objetivo de fortalecer la seguridad (ENISA, 2016).

Red Team: Equipo encargado de simular ataques reales a la infraestructura de una organización, utilizando técnicas ofensivas para evaluar la eficacia de los controles y la respuesta del Blue Team (Colbert et al., 2020).

Resiliencia organizacional: Capacidad de una organización para anticipar, resistir, adaptarse y recuperarse de incidentes adversos, manteniendo sus funciones críticas (ISO 22316:2017).

SIEM (Security Information and Event Management): Herramienta que recopila, correlaciona y analiza eventos de seguridad provenientes de diferentes fuentes, facilitando la detección y respuesta a incidentes (Scarfone & Mell, 2007).

Virtualización: Tecnología que permite crear entornos virtuales (máquinas virtuales) sobre hardware físico, facilitando la simulación y prueba de escenarios de ciberseguridad (Rosenblum & Garfinkel, 2011).

Introducción

La creciente aparición de la digitalización de los procesos empresariales y gubernamentales ha experimentado una vasta expansión de las superficies de amenazas a las organizaciones puesto que se exponen a nuevas amenazas de mayor sofisticación y resistencia.

Nace así la ciberseguridad como un componente esencial de la sustentabilidad y continuidad de negocio, asimismo que exige el formar equipos de Blue Team y Red Team, ambos son equipos que operan bajo un estricto régimen de normatividad en Colombia.

La intersección de los conocimientos técnicos avanzados, la aplicación del marco normativo y las habilidades de gestión es el núcleo de los profesionales en ciberseguridad para anticipar, detectar, repeler amenazas y proteger los activos digitales mientras que se garantiza la regulación legal.

Justificación

La presente investigación remite a la emergente urgencia de afrontar y mejorar las cualidades de ciberseguridad en el país, si se refiere el incremento de ciberataques sobre las infraestructuras críticas, entidades públicas y privadas, la sofisticación en cuestiones de técnicas con las que son dominadas por sus actores malintencionado. Si bien la normatividad nacional que enriquece con la Ley 1273 de 2009 en contra de los delitos informáticos; y la Ley 1581 de 2012 para la protección de datos personales, proporcionan un marco de referencia para cualquier organización que administre información sensible.

La creación de normas no es suficiente para incrementar el nivel de ciberseguridad, así las cosas, el equipo de ciberseguridad debe adquirir competencias para análisis forense, pruebas de penetración, gestión de seguridad de los incidentes y el dominio de herramientas especializadas, asimismo, la administración de la documentación indicada con el reporte obtenido del ejercicio de Pentesting y las normas vigentes.

En el mismo aspecto la virtualización de entornos controlados y la simulación de ataques reales les permite validar con mayor contundencia la efectividad de los controles utilizados y facilitar la cooperación de mejora continua en temas de ciberseguridad.

Objetivos

Objetivo General

Fortalecer la ciberseguridad organizacional colombiana, mediante la implementación de escenarios controlados de ataque y defensa con equipos Red Team y Blue Team, aplicando metodologías de Pentesting y análisis forense y vinculando el cumplimiento normativo como pilar fundamental para la protección integral de los activos digitales, con el fin de fortalecer la resiliencia y la capacidad de respuesta ante incidentes de seguridad.

Objetivos Específicos

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Analizar el alcance ético y legal del acuerdo de confidencialidad, identificando contravenciones a la normatividad vigente y desarrollar estrategias para mitigar el riesgo de incidentes de ciberseguridad.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Capítulo 1. Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Anexo 1 – Escenario 1

Situación Problema: Montaje Banco De Trabajo.

CyberFort Technologies requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de **CyberFort Technologies**. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

De manera simultánea **CyberFort Technologies** requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

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

Ley 1273 de 2009: Delitos Informáticos.

Esta Ley divulgada el 5 de enero de 2009 se creó para modificar el Código Penal en Colombia frente a los delitos TICS. Se presenta con el fin de prevenir el acceso no autorizado a datos y sistemas informáticos, atentados de seguridad y viceversa. Al respecto, se tratan los siguientes aportes:

Tipificación de nuevos delitos: Artículos 269A hasta 269D, que tipifica falta de valores en computadoras; infracción a la confidencialidad y seguridad de datos; atentado informático y daño causado por virus.

Condenas Penales: Pueden alcanzar 120 meses de prisión y multas de 1.500 SMLV o máximas vigentes si comete uno de los delitos.

Protección a Infraestructuras Críticas: Cobertura de infraestructuras tales como sistemas públicos, financieros y de salud.

La ley se expuso en respuesta al aumento de las pérdidas económicas ante delitos informáticos en 2007 que superaron los 6,6 billones de pesos colombianos. Proporciona medios preventivos y punitivos para frenar comportamientos como el phishing, las clonaciones de tarjetas y maniobras fraudulentas de transacciones electrónicas.

Tabla 1

Ciberdelitos contenidos en la Ley 1273 de 2009.

Clasificación de la Protección	***Articulo***	***Delitos***	***Composición del Punible Según Verbo Rector y Modalidad***
Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los	269A	Acceso abusivo a un sistema informático.	El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se

sistemas informáticos			mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
	269B	Obstaculización ilegítima de sistema informático o red de telecomunicaciones.	El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.
	269C	Interceptación de datos informáticos.	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un

		sistema informático que los transporte.
269D	Daño informático	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
269E	Uso de software malicioso	El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.
269F	Violación de datos personales	El que, sin estar facultado para ello, con provecho propio o de un tercero,

		obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
269G	Suplantación de sitios web para capturar datos personales.	El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes / El que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente

			en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
De los atentados informáticos y otras infracciones	269I	Hurto por medios informáticos y semejantes	El que, superando medidas de seguridad informáticas, realice la conducta [hurto] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.
	269J	Transferencia no consentida de activos	El que, con ánimo de lucro y valiéndose de alguna manipulación

	informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.

Nota. Normatividad sobre delitos informáticos con base en la documentación de la Policía Nacional de Colombia. Fuente. (Congreso de la República de Colombia, 2009).

Ley 1581 de 2012 para la Protección de Datos Personales.

Esta ley establece categorías de datos, quiénes se encargan de ellos y qué mecanismos de vigilancia y control se aplican, definiendo también el procedimiento a seguir y las sanciones con cierto desorden natural para proteger y cuidar la información de la ciudadanía registrada en cualquier base de datos del territorio nacional, se busca impedir, en la mayoría de los casos, cualquier forma de operación, recolección, almacenamiento, uso, circulación o tratamiento realizados por organizaciones públicas y privadas, o incluso por ambas de manera indistinta.

Su objetivo principal es, en esencia, garantizar la privacidad y la intimidad de los colombianos, salvaguardando los derechos fundamentales vinculados a la información personal; se apoya en el principio de confidencialidad para promover un uso correcto de los datos y en la

integridad para mantener su estructura y sentido, recordando siempre que todo debe hacerse sin dejar de lado lo humano.

Política de Seguridad Digital (CONPES 3854 de 2016).

Mejora los esfuerzos nacionales de ciberseguridad a través de la provisión de capacidades avanzadas que incluyen entrenamiento ofensivo y despliegue de tecnologías emergentes.

Decreto 338 de 2022.

Delinea los lineamientos sobre protección de la infraestructura de información crítica y gestión de riesgos en el país.

1.2. En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o Pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del Pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del Pentesting.

Planificación y Definición de Alcance.

En esta etapa, se definen así los objetivos, los límites y las metodologías del Pentest. Por ejemplo, es la definición de los sistemas objetivo y conseguir autorizaciones y permisos legales que eviten responsabilidades. Existen herramientas como Microsoft Project o Jira para el control del calendario y los recursos, aunque no se mencionan expresamente en los resultados.

Reconocimiento e Investigación.

"Reconocimiento Pasivo & Activo": Obtención de información enfocada en la red del sistema como direcciones IP, dimensiones de lo que representa dentro de la Infraestructura TI. Nmap es utilizado para determinar hosts activos y servicios expuestos, que pude ser observado en el escaneo donde se pueden detectar puertos abiertos y versiones de software, entre otros.

Escaneo de Vulnerabilidades.

Herramientas automatizadas OpenVAS (Greenbone) o Nessus investigan los sistemas de fallos conocidos. En ambientes de pruebas sirve para revelar vulnerabilidades en servicios de tipo HTTP y bases de datos generando informe detallado de riesgos y posibles explotaciones.

Explotación.

En esta etapa, es conseguir ventajas para acceder a los sistemas mediante alguna de esas vulnerabilidades o fallas identificadas en la etapa de "Escaneo de Vulnerabilidades" y deben ser aprovechadas para poder acceder al sistema. Metasploit es un marco de trabajo modular donde puedo ejecutar exploits como "*multi/http/apache_normalize_path_rce*" para comprometer Servers Web vulnerables, es igualmente eficaz cuando se integra a base de datos como ExploitDB permitiendo la selección de ataques adecuados.

Post-Explotación y Mantenimiento de Acceso.

Tras lograr el acceso, es indispensable permanecer en el sistema y existen backdoors o elevación de privilegios. Además, por ejemplo, el uso de Meterpreter desde Metasploit que hace labores como acumulación de credenciales y desplazamiento lateral en la red.

Elaboración de Informes.

El informe completo incluye las descripciones de las vulnerabilidades, explotaciones ejecutadas y recomendaciones. establecido un modelo de plantilla o adoptar las sugeridas por Tarlogic Security con pautas de las secciones como evidencia mediante capturas de pantalla y riesgo priorizado basado en CVSS.

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

Herramientas:

Metasploit:

Metasploit es un marco de trabajo de pruebas de penetración desarrollado por Rapid7, contiene exploits, payloads, y módulos auxiliares. Utilidad para la demostración de vulnerabilidad para comprometer servicios FTP y HTTP utilizando scripts configurados para comprometer sistemas.

Nmap:

Como escáner de red, Nmap busca identificar dispositivos activos, puertos abiertos y el sistema operativo de los dispositivos. Dado en un entorno de prueba controlado, el comando "*nmap -sV -O 192.168.1.3*" puede revelar servicios que incluyen vsftpd 2.3.4 y Apache 2.2.8; datos vitales para la orientación del ataque.

OpenVas

Más allá de las pruebas de rendimiento constantemente comparativas, OpenVAS es un escáner de vulnerabilidades de código abierto que utiliza pruebas automáticas para detectar fallos de seguridad. En concurrencia, OpenVAS requiere poco recurso de la maquina objetivo y no afecta el ancho de banda por lo que es ideal su implementación debido a la NO afectación de la sincronía en producción.

Servicios en línea:

ExploitDB

OpenSource ExploitDB que es desarrollada y mantenida por Offensive Security. Se accede a la base haciéndola pasar por herramientas como searchsploit que filtran vulnerabilidades buscando por plataforma o tipo ataque.

CVE

Common Vulnerabilities and Exposures (CVE), identifica vulnerabilidades de codificación único. CVE-2023-2825 describe la vulnerabilidad crítica en GitLab permitiendo ejecución remota de código, así mismo, su identificación facilita la priorización en la aplicación de parches de seguridad o actualización de versiones de software dentro de las organizaciones.

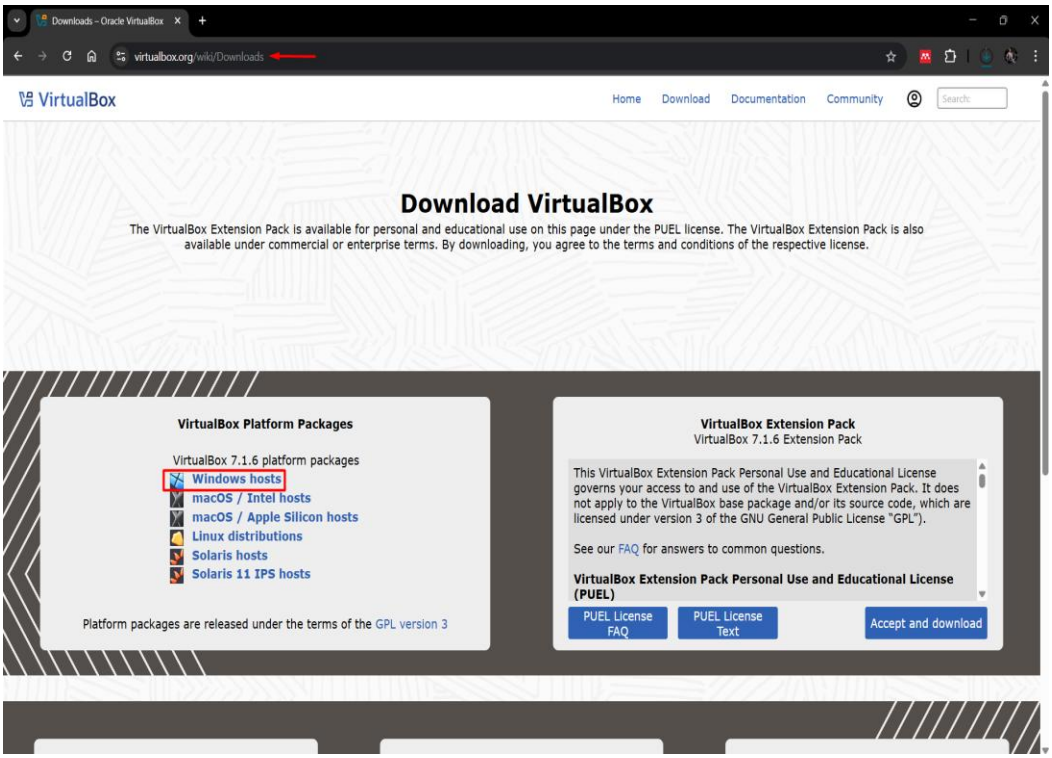
1.4. Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá

trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

Paso A: Descargar la Herramienta Virtualizadora "Virtualbox" en su Última Versión.

Figura 1

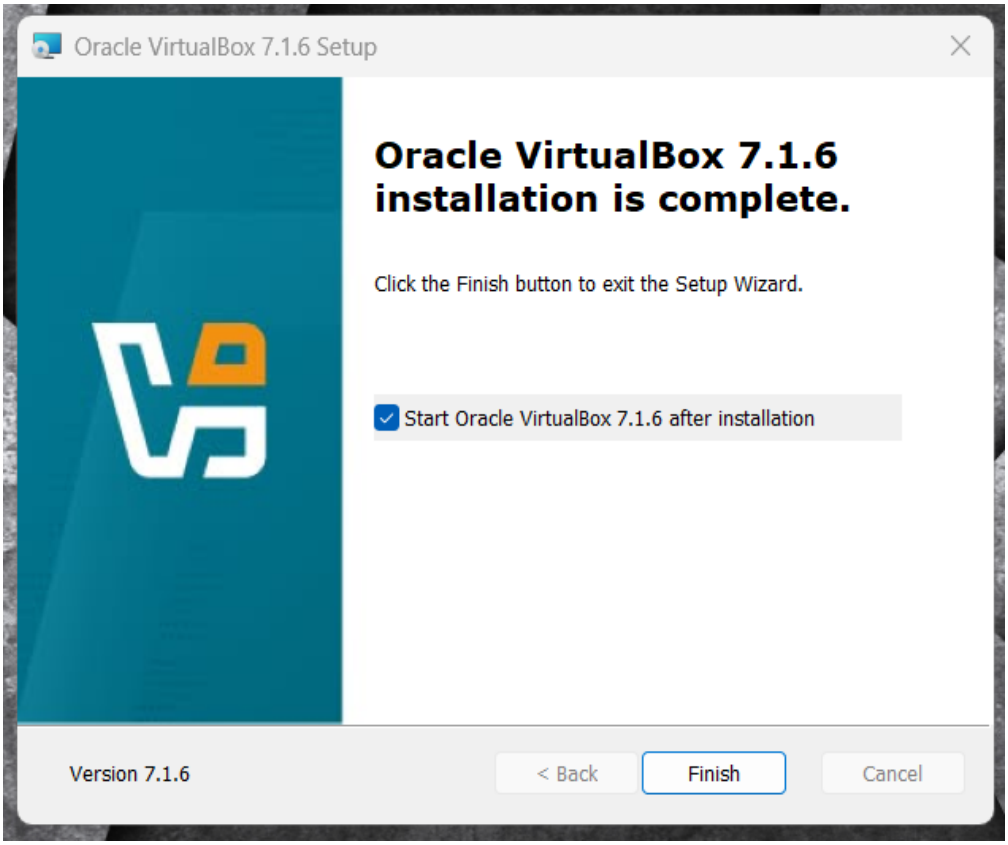
Descarga del Software de Virtualización VirtualBox.



Nota. Captura de pantalla donde se evidencia la descarga de la última versión de VirtualBox.

Figura 2

Instalación de VirtualBox.

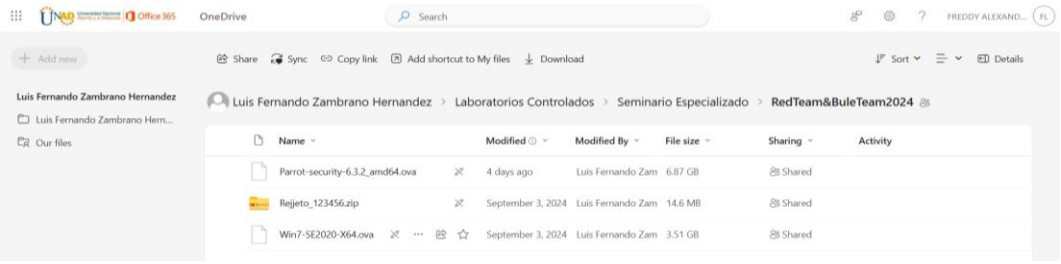


Nota. Captura de pantalla donde se evidencia la instalación del software de virtualización VirtualBox en su última versión disponible.

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad ingrese al enlace: RedTeam&BuleTeam2024, el cual contiene lo requerido para el montaje del banco de trabajo, las imágenes en formato *.OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un sistema operativo Windows y un sistema operativo Kali Linux.

Figura 3

Ingreso al Repositorio de Imágenes.

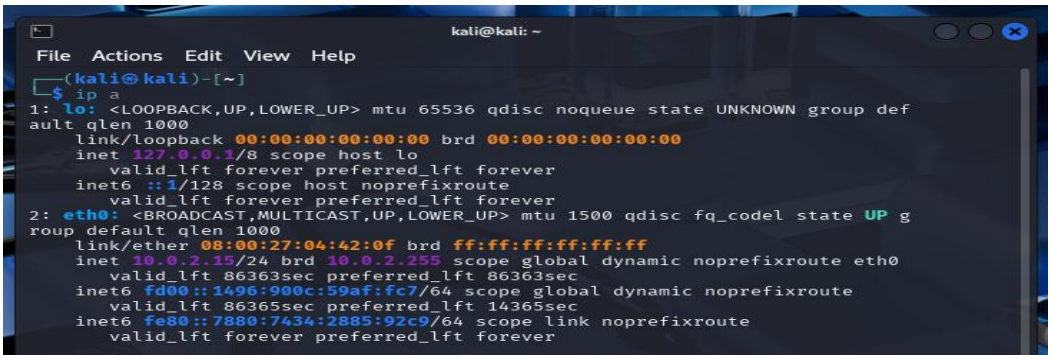


Nota. Captura de pantalla donde se evidencia el ingreso al repositorio para realizar las descargas de las imágenes proporcionadas para la implementación del escenario controlado denominado "Banco de Trabajo".

Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Figura 4

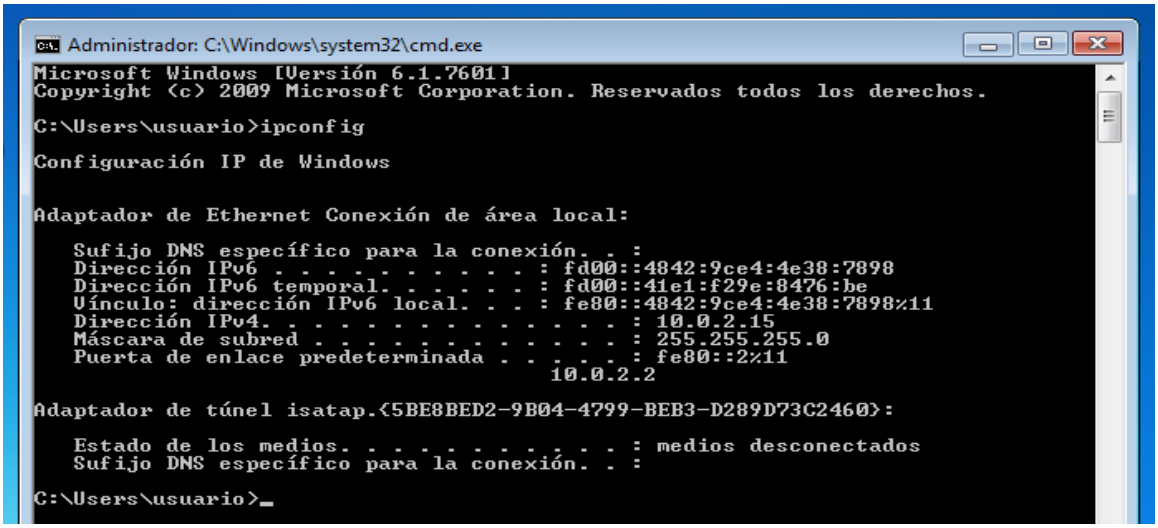
Verificación del Direccionamiento IP en Kali Linux.



Nota. Captura de pantalla desde la terminal de la VM con Kali Linux para verificar el segmento de red en el que se encuentra.

Figura 5

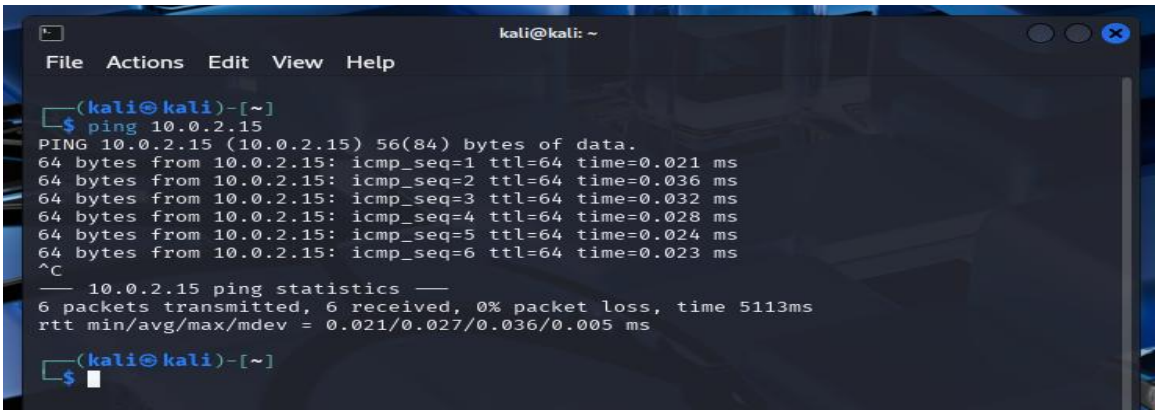
Direccionamiento IP de la VM Win7



Nota. Captura de pantalla donde se evidencia la configuración del direccionamiento IP de la VM con Windows 7.

Figura 6

Ping desde VM Kali Linux a VM Win7

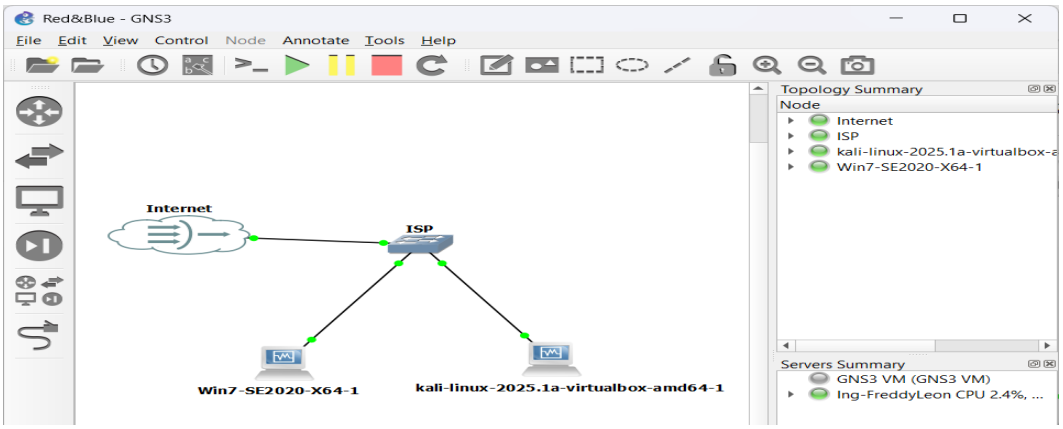


Nota. Captura de pantalla donde se evidencia la realización de Ping desde la VM Kali Linux a VM Win7.

Paso D: Evidenciar con Printscreen el Montaje del Banco de Trabajo y Explicar cómo se Encuentra Desplegado "Características Técnicas de Hardware".

Figura 7

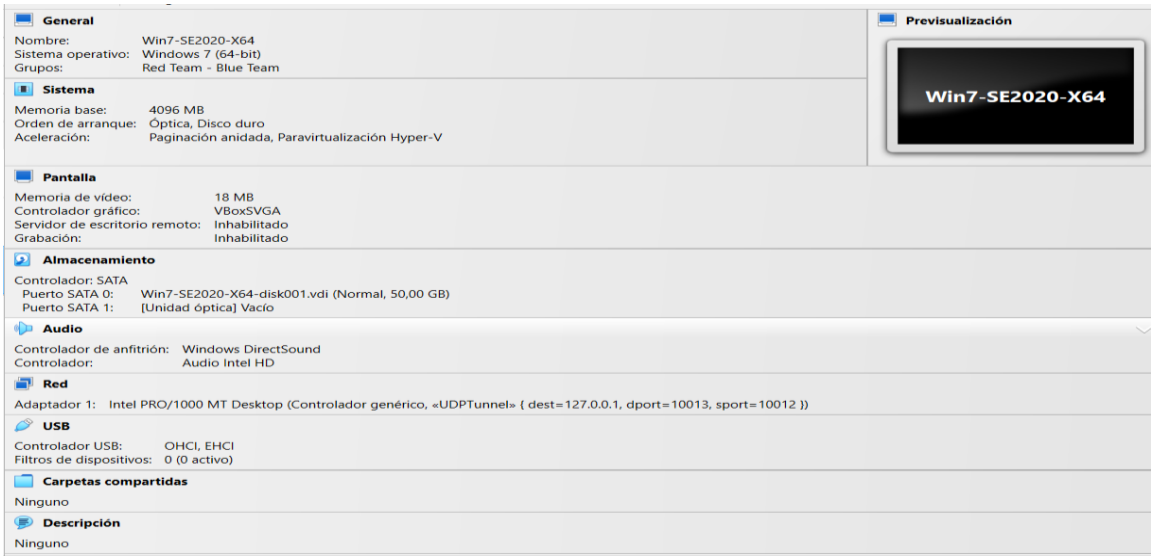
Topología Anexo 1 – Escenario 1.



Nota. Captura de pantalla de la Topología diseñada para el desarrollo del Escenario 1, bajo metodología de ambiente controlado utilizando la herramienta GNS3.

Figura 8

Características Técnicas Win7.



Nota. Captura de pantalla de las características técnicas de hardware VM Windows 7 x64.

Figura 9

Características Técnicas Kali Linux.

Nota. Captura de pantalla de las características técnicas de hardware VM Kali Linux 2025.

Capítulo 2. Analizar el Alcance Ético y Legal del Acuerdo de Confidencialidad, Identificando Contravenciones a la Normatividad Vigente y Desarrollar Estrategias para Mitigar el Riesgo de Incidentes de Ciberseguridad.

Anexo 2 – Escenario 2

Situación Problema: Análisis legal.

La organización **CyberFort Technologieses** una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

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 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 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 equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de VirtualBox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

2.1.¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Procesos Ilegales y No Éticos Evidenciados en el Anexo 3-Acuerdo.

El Acuerdo de Confidencialidad adjunto como Anexo 3-Acuerdo posee cláusulas que, desde la visual ética y legal, son cuestionables. Siendo específico, se dispone que el receptor "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.". Se específica sobre mantener un nivel de reserva, incluso en "procesos ilegales", que se descubran y se obtengan dentro de CyberFort Technologies.

Primera Cláusula: Ocultamiento de Procesos Ilegales.

Establece que "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".

Esta prohibición es, por lo tanto, inequívocamente ilegal, ya que:

A. Expresamente reconoce la "existencia" de un proceso ilegal en la organización.
B. Intenta forzar a las personas que no denuncien actividades ilegales ante las autoridades competentes.
C. Pretende transformar al firmante en cómplice de posibles delitos al coartarlo con condiciones y silenciarlo frente a la comisión de delitos.

Segunda Cláusula: Definición de Información Confidencial.

De la definición de la confidencialidad de la información acuerdos infundiéndoles que “datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos””.

Entonces la organización está definiendo “confidencial” como plácidamente el robo de datos, sin tener en cuenta en un sentido completamente denotativo configuración de un hecho punible dentro de las leyes colombianas, literalmente hablando de la Ley 1273 de 2009.

Cuarta Cláusula: Prohibición de Denuncia

Por parte del receptor el acuerdo incluye "3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros." y "4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.".

Son, por lo tanto, claramente ilegales toda vez que:

A. Decrete revocaciones del deber civil como ciudadanos de denunciar la comisión de delitos.
B. Intentan destruir contractualmente la facultad de denunciar las actividades ilegales.
C. La ley no permitirá que acuerdos en privado regulen los principios legales, la constitución y las Leyes.

Octava Cláusula: Eximición de Responsabilidad

La cláusula de solución de controversias también establece: "En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un

abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies."

La finalidad de esta estipulación es:

A. Transferir cada vez la totalidad de la responsabilidad legal para con el receptor de la información.
B. No imponerle al dueño de la organización o a quien haga sus veces, la responsabilidad legal por sus actos propios de delincuencia.
C. Fortalecer una protección legislativa ilegitima para futuras indagatorias.

Análisis Ético y Legal.

Éticamente: Limita el derecho de denuncia, lo cual puede traducirse como un mecanismo para favorecer la impunidad al dejar a los seres responsables, implicados, o testigos sin hablar con las autoridades sobre las actividades que podrían ser delitos.

Jurídicamente: Obligando a no denunciar abatirá la colaboración de la justicia indicada para desvelar si se tratan de delitos, lo que favorece que se establezcan perpetuamente actividades criminales dentro de organización.

2.2. Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Tabla 2

Vulneraciones a la Ley 1273 de 2009.

Cláusula del Acuerdo	***Artículo Vulnerado (Ley 1273)***	***Descripción del Delito***	***Argumento Legal***
Primera: Prohibición de divulgar procesos ilegales	Artículo 269F: Violación de datos personales	Obtención, divulgación o uso no autorizado de datos personales con provecho propio o de terceros.	La cláusula fomenta el encubrimiento de actividades ilegales, lo cual incluye la apropiación y uso indebido de datos personales protegidos por la ley.
Segunda: Definición de información confidencial (incluye datos obtenidos mediante chuzadas e interceptación)	Artículo 269C: Interceptación de datos informáticos	Interceptar sin autorización datos informáticos en su origen, destino, o dentro de un sistema informático.	La inclusión de "chuzadas" e interceptación como información confidencial valida prácticas ilegales que están penalizadas por la ley.
Cuarta: Prohibición de denunciar actividades	Artículo 269A: Acceso abusivo a un sistema informático	Acceder sin autorización a sistemas informáticos	Al prohibir la denuncia de actividades

sospechosas (puntos 3 y 4)		protegidos o mantenerse en ellos contra la voluntad del propietario.	sospechosas, la cláusula protege actos ilícitos como el acceso abusivo a sistemas informáticos.
Octava: Eximición de responsabilidad legal para CyberFort Technologies	Artículo 269I: Hurto por medios informáticos y semejantes	Manipulación o suplantación en sistemas informáticos para obtener beneficios ilícitos.	Esta cláusula busca eximir a la empresa de responsabilidad penal, lo cual es contrario al principio legal que establece que los responsables deben enfrentar las consecuencias legales.

Nota. Detalle de las cláusulas del acuerdo de confidencialidad de CyberFort Technologies que vulneran la Ley 1273 de 2009. Fuente Congreso de la República de Colombia, 2009.

2.3.¿Existiendo procesos poco confiables en el "anexo 3 – Acuerdo", usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la

organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros.

Como especialista en ciberseguridad, mi experticia en seguridad informática, y después de una revisión exhaustiva del compendio documental suministrado, “Anexo 3 Acuerdo de Confidencialidad” que la organización CyberFort Technologies propone para celebrar el contrato, mi posición profesional se declara con firmeza e irrevocablemente en una declinación in terminis de la oferta laboral, aun teniendo en cuenta la alta suma de dinero en contraprestación mensual que otorga la aceptación del contrato.

La génesis de esta denegación no es la “historia por quedar bien”, por así decirlo, ante las prácticas empresariales de CyberFort Technologies, sino una convicción instituida en ética y derecho, fundamentada en las estipulaciones detalladas de las poco éticas cláusulas del precitado acuerdo.

Firmar el acuerdo sería expresar de forma directa una transgresión abierta a la praxis de cualquier ingeniería enfocada en la ciberseguridad e incurrir en prácticas ilícitas que contravienen las leyes colombianas.

La diferencia la hace la incidencia abierta de las cláusulas del contrato contra el Código de Ética del COPNIA (Consejo Profesional Nacional de Ingeniería), que está ahí para garantizar la integridad y rectitud en la profesión mientras ejercen la Ingeniería en Colombia.

El “código” del COPNIA impone un estándar de comportamiento a los ingenieros honestos con la consigna del “ipso facto” siempre en público, la autenticidad absoluta, la integridad sin fractura, la frente limpia y una responsabilidad social sin cuestionamientos.

Jamás aceptaría un empleo elegido ad hoc vinculado a un pacto preexistente que de forma expresa oculte la existencia de “procesos ilegales” cometidos en la organización, es decir, abusar arbitrariamente de la posición dominante del contrato con el fin de vulnerar intereses generales o particulares de una persona o empresa. El ocultamiento de actividades ilícitas contempladas en el acuerdo atenta contra la seguridad, el bienestar y la confianza de la sociedad las cuales deben ser protegidas reciamente por cualquier profesional de ingeniera.

Asimismo, la aceptación del empleo contempla una vida de silencio frente a las actividades sospechosas de espionaje o cualquier otro proceso en el que intervenga la utilización de la información de otra persona, no solo viola el principio de retórica sino también el de justicia que cualquier ingeniero debe seguir.

En consecuencia, la integridad, cuyo contenido definido es rectitud moral y coherencia entre el pensamiento y la acción, se incumple de plano desde el instante en que se acepte una posición que implica la participación en hechos ilegales por acción u omisión.

La ciberseguridad, en esencia, es una disciplina basada en la confianza y la transparencia; un profesional que encubre los delitos ataca la razón de ser de la existencia de su profesión.

2.4. Deberá analizar el caso problema “Ciberespionaje y Ética en CyberFort Technologies” (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

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

La progresiva dependencia de las organizaciones en servicios de ciberseguridad fundamenta posturas críticas sobre los límites de la ética y la legalidad de la forma del tratamiento de la información sensible durante los procesos de auditorías.

Según lo anterior se puede establecer que las empresas de ciberseguridad deberían solo tener acceso a la información sensible de sus clientes en la medida necesaria y estricta del acuerdo de confidencialidad y limitándose al objetivo concreto en el que se dirige la auditoría, es decir, identificar y remediarse vulnerabilidades o amenazas.

Dicho acceso debe estar claramente definido y los límites de autorización establecidos explícitamente en el contrato, denotando qué datos pueden ser revisados; cuánto tiempo estarán abiertos; y con qué finalidad, para preservar el acceso sin que se explote de manera indebida, lo establecido anteriormente debe seguir las siguientes medidas:

Principio de privilegios al mínimo: Auditores con el mínimo acceso requerido para su trabajo, no existen accesos globales.

Registro histórico y supervisión en tiempo real: Todas las acciones tomadas en términos de la auditoría deben quedar registradas en logs inmutables, supervisados en tiempo real para detectar accesos indebidos o usuarios no autorizados.

Contratos o acuerdos de confidencialidad estrictos: Incluir cláusulas específicas de confidencialidad. No se permite el uso o divulgación de la información no autorizada; fijando sanciones severas para cualquier caso de incumplimiento.

Eliminar información sobrante después de la auditoría: No debe quedar acceso a ninguna información sensible que se haya permitido con el acceso concedido una vez finalizado el trabajo de auditoría.

Auditorías forenses e independientes: Verificaciones significativas posteriores para asegurarse de que el auditor no explotó su acceso ni filtro información.

El ejemplo de CyberFort Technologies demuestra que presentaban las medidas anteriores, algunos empleados usaban el acceso para espionaje y venta ilegal de información, lo que violaba la ética profesional y la confiabilidad del cliente, el acceso solo se debe estar limitando y basado en el entorno de donde y quien, dando protección y supervisión para evitar accesos abusivos y propender la privacidad de la información del cliente.

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

Como experto en ciberseguridad, evalúo la situación de CyberFort Technologies desde una perspectiva de enfoque más holístico basado en técnicas y ética de algunos aspectos legales. El caso muestra una falla sistémica en los controles de inspección interna de la empresa, los cuales les permite a sus empleados a usar herramienta sofisticada con fines no permitidos directamente con la intención de obtener y comprometer la confidencialidad y confianza de sus clientes.

Técnicamente hablando, la incapacidad de controlar el uso de las herramientas de análisis forense supone una vulnerabilidad crucial. Los sistemas diseñados para investigar los incidentes de seguridad y recopilar evidencia proveen un poder muy pronunciado a quienes les dan uso.

Sin una supervisión adecuada, resulta peligroso porque pueden ser utilizados maliciosamente excluyendo las funciones originales de cada herramienta y convertirlas en armas letales para la extracción, pérdida y uso indebido de información sensible.

Éticamente, el comportamiento de los empleados de CyberFort Technologies se consolida a partir de un punto extremadamente inmoral y viola la confianza generada por los clientes en la organización, el personal utiliza acceso indebido para recopilar estas evidencias sin autorización y posteriormente venderlo a terceros o a ciberdelincuentes organizados, esto representa una traición a sus clientes.

Legalmente, la conducta de los empleados de CyberFort Technologies podrían tener resultados nefastos. El acceder de forma no autorizada a sistemas comerciales y la recuperación de información confidencial son ilícitos estipulados actualmente en la legislación colombiana.

Para asegurarse de que este tipo de comportamientos o incidentes no vuelvan a ocurrir, las empresas de ciberseguridad deben implantar una serie de controles y supervisión, entre ellas:

Control de Acceso Granular: Limitar el acceso a herramientas de análisis forense a solo el personal específico, definiendo funciones y compromisos claros a cada funcionario.

Monitorización Continua: Implantar sistemas de vigilancia y auditoría que inspeccionen todas las actividades de las herramientas de análisis forense incluyendo el conjunto de comandos ejecutados, datos accedidos y los resultados.

Políticas Claras de Uso: Establecer políticas internas para el uso específico de las herramientas forenses, dejando establecido los ámbitos de lo que se pueden y no se puede usar, con las sanciones disciplinarias explicitas.

Formación Ética y Concienciación: Promover la formación continua del personal sobre ética profesional, responsabilidad de la información utilizada, uso ilícito de las herramientas forenses y supervisión a la toma de decisiones que provocan acciones legales.

Auditorías Internas y Externas: Llevar a cabo auditorias periódicas y minuciosas para reducir el incumplimiento de las políticas y su efectividad.

En conclusión, el caso CyberFort Technologies pone de manifiesto la necesidad de implementarse controles internos efectivos y la creación de círculos éticos dentro de las compañías de ciberseguridad.

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

Los gobiernos y las organizaciones en la actualidad enfrentan un conflicto crítico en lo relacionado a la ética profesional, la confidencialidad de la información, y desde un punto de vista más analítico diría que enfrentar el reto de seleccionar el personal con la idoneidad adecuada y que sea integro en su actuar, frente a los procesos de auditoría que lleven a cabo es más complejo de lo que parece, por lo tanto, si se descubre que una empresa de ciberseguridad esta realizado procedimientos de ciberespionaje la respuesta debe ser implacable, deben ser aplicadas por igual a las empresas a nivel comercial, como a los empleados que ejecuten las acciones ilícitas, igualmente, se deben articular acciones diplomáticas entre gobiernos para fortalecer la mitigación de futuras conductas análogas.

Los gobiernos y las organizaciones afectadas deben iniciar investigaciones penales exhaustivas de forma inmediata, presentando cargos contra los profesionales, las empresas y sus

representantes legales, con el fin de acarrear prisión, multas y anulación de licencias y tarjetas profesionales, de igual manera interponer acciones civiles que apliquen sanciones pecuniarias con el fin de resarcir el daño causado, si el caso es que la empresa que realiza el ilícito no está domiciliada en el país buscar la cooperación diplomática para poder aplicar las sanciones que den lugar y sean aplicables en la normativa vigente.

Capítulo 3. Demostrar Vulnerabilidades en un Sistema Informático a Partir del Uso de Metodologías y Técnicas de Intrusión.

Anexo 4 – Escenario 3

Situación Problema: Análisis Red Team.

La primera misión del equipo Red Team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación vulnerable bajo un Windows; esta aplicación al parecer tiene asociado un exploit que puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque. Dentro de la indagación, también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

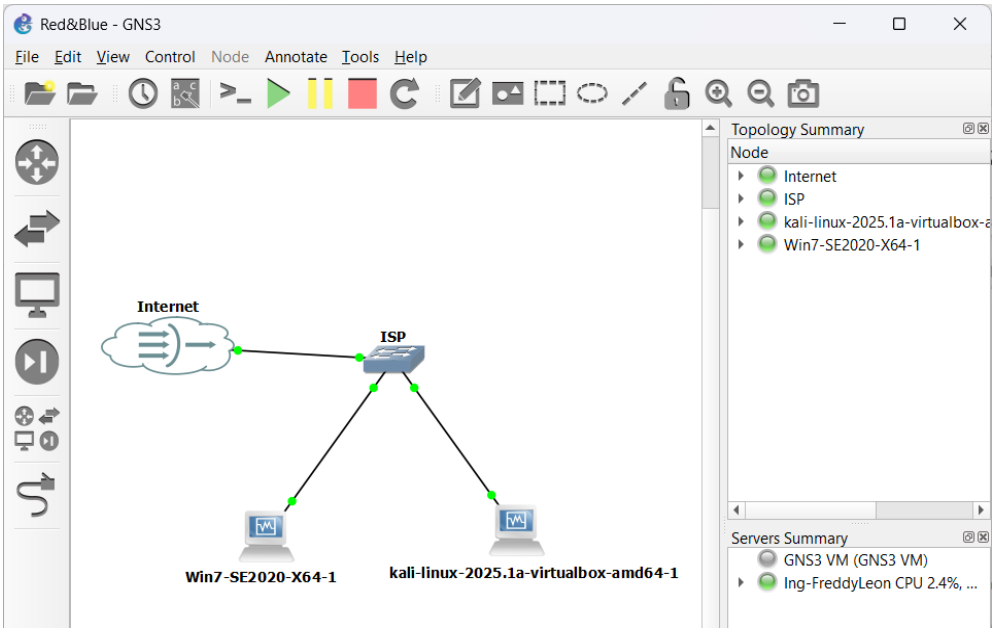
El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

3.1. Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

Topología de Red del Escenario Controlado.

Figura 10

Topología Anexo 4 – Escenario 3.



Nota. Captura de pantalla de la Topología diseñada para el desarrollo del Escenario 3, bajo metodología de ambiente controlado utilizando la herramienta GNS3.

Fases del Pentesting.

Fase de Reconocimiento.

En esta fase se utilizó la herramienta NMAP, realizando la identificación y descubrimiento de la red, con el fin de localizar el objetivo a atacar.

¿Qué es Nmap?

Es una herramienta de código abierto para la exploración de redes y la auditoría de seguridad. Fue diseñada para escanear rápidamente redes grandes, aunque funciona

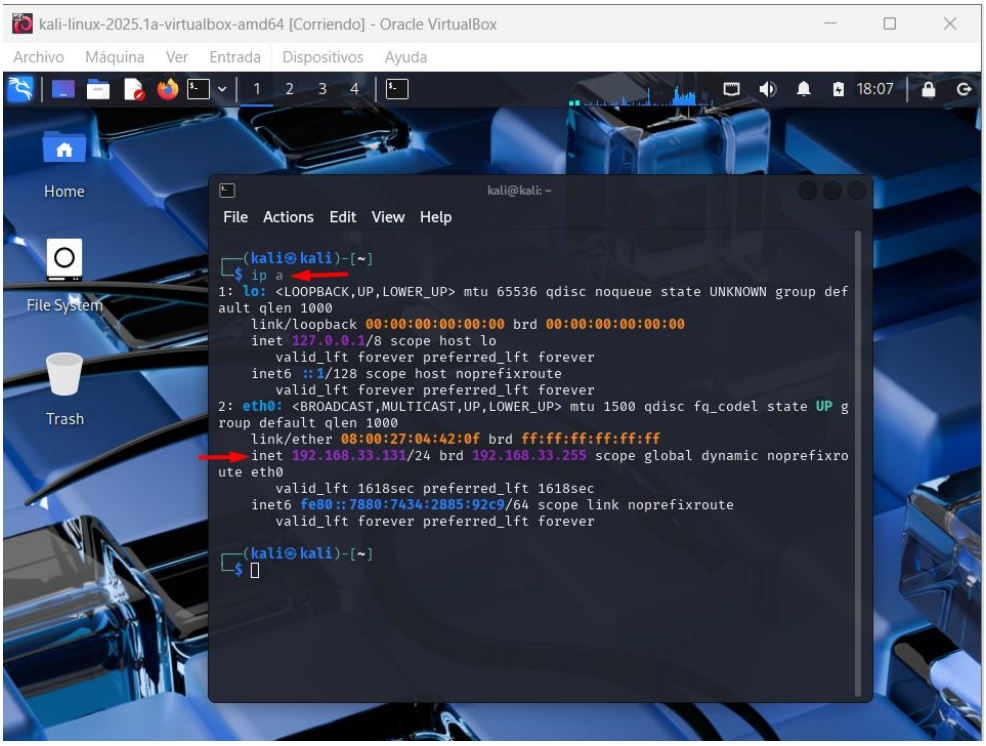
correctamente con hosts individuales. Nmap utiliza paquetes IP sin procesar de forma innovadora para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y versiones del SO) ejecutan, qué tipo de filtros de paquetes/cortafuegos utilizan y muchas otras características. Si bien Nmap se utiliza habitualmente para auditorías de seguridad, muchos administradores de sistemas y redes lo encuentran útil para tareas rutinarias como el inventario de red, la gestión de calendarios de actualización de servicios y la monitorización del tiempo de actividad de hosts o servicios. (Smith et al., 2021)

Con el fin de darle un nivel natural a las pruebas realizadas y como un cazador que acecha a su presa en la penumbra, se adoptó un enfoque realista en el Pentesting, concentrándose únicamente en el rango de direccionamiento IP donde habita la máquina atacante, armada con una distribución de Kali Linux. A diferencia de un análisis indiscriminado y sin dirección, esta metodología, precisa y contenida, permitió que una vez identificado el rango IP, se desplegara el escaneo con la herramienta NMAP.

Se procede a ejecutar desde la terminal de la maquina atacante el comando ip -a para verificar el rango ip en el cual se encuentra, dando como resultado la dirección 192.168.33.131/24.

Figura 11

Identificación del Rango IP VM Kali Linux.



Nota. Captura de pantalla de la ejecución del comando ip -a en la terminal de la VM Kali Linux, para identificar el Rango IP en el cual se encuentra.

Una vez identificado el Rango IP, se procedió a ejecutar la herramienta NMAP la cual nos permitirá identificar hosts activos, puertos abiertos, versiones de los sistemas operativos, entre otros, para realizar este descubrimiento ejecutaremos el siguiente comando nmap -O -T4 -v --osscan-guess --max-retries 3 --min-hostgroup 64 <Rango IP>.

Explicación del Comando.

Tabla 3

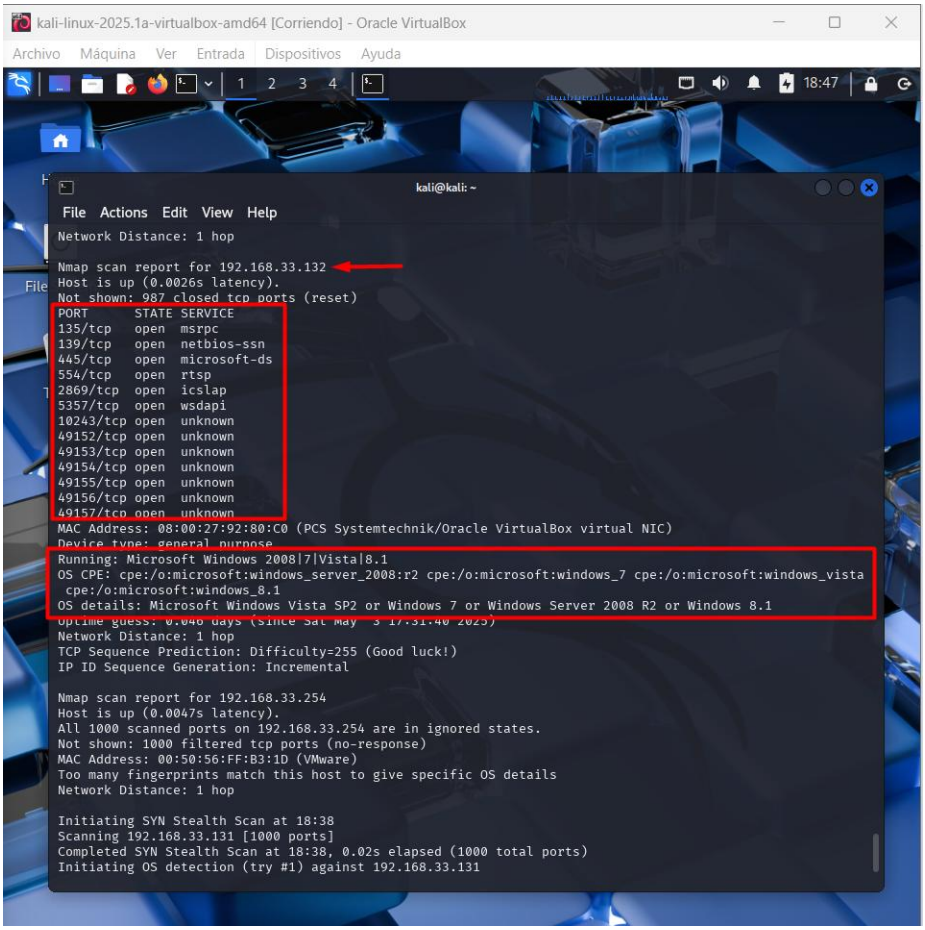
Explicación del comando utilizado para el descubrimiento de la red.

Opción	***Descripción***
-O	Habilita la detección del sistema operativo.
-T4	Usa una velocidad rápida sin ser extremadamente agresiva.
-v	Muestra salida detallada (verbose).
--osscan-guess	Fuerza a adivinar el sistema operativo si no es certero.
--max-retries 3	Reduce la cantidad de reintentos para agilizar el proceso.
--min-hostgroup 64	Aumenta el número de hosts escaneados en paralelo.

Nota. Comando utilizado en la fase de descubrimiento para detectar Host Activos, Dirección IP, Sistema Operativo probable, Puertos Abiertos, Servicios Desplegados.

Figura 12

Resultado del Comando para descubrimiento de Red.



Nota. Captura de pantalla donde se evidencia la ejecución del comando para el descubrimiento e identificación del objetivo dentro de la red.

Los puertos descubiertos al escanear pueden parecer inocentes, pero en manos expertas están listo para ser explotados. El apaciguamiento ante un sistema al parecer equilibrado, con estos accesos abiertos convirtiéndose en puertas entreabiertas, con las llaves en manos de un atacante.

Los puertos abiertos 135, 139 o 445 no son nada inocentes. Son llaves maestras del que maneja el ecosistema Windows, instruyendo a convertir en inevitable lo oculto en raras habilidades desde Microsoft RPC, NetBIOS y SMB, se almacena lo que le permitiría al atacante vulnerar con familiaridad.

El caso de MS17-010 lo ilustra con crudeza: Si bien en el aire puede parecer un fantasma olvidado, tal vulnerabilidad es una fantasía que recorre los pasillos de las PCs olvidadas por quienes no han cerrado esa vieja herida. Como el castillo sin centinela no cabalgará nadie, es un sistema sin parches, ¿uno que los cerró hace 15 años? puede ser una entrada abierta; un caballo de Troya Digital.

Tal es el caso de NetBIOS y SMB entonces estos espías silenciosos le facilitan el acceder a información crucial sin autenticarse en campos de actividad: nombres de usuario, dispositivos y recursos compartidos acceden sin atreverse a hacerlo. El administrador sale a relucir con comodidad, para el atacante es el mapa de cómo llegar al tesoro.

Los puertos que fluyen sin nombre (49152-49158) serían como las cortaduras escondidas de los murales absurdos: ocultar todavía no es suficiente, no por ello se ven menos perjudiciales. Si no garantizan puertas, entre otras actividades, son subsiguientes a servicios como DCOM o RPC que abren puertas traseras para el acceso de administradores no autorizados.

Fase de Escaneo de Vulnerabilidades.

Identificado el host objetivo se procede a realizar el escaneo especifico con tal de recopilar la mayor información de las posibles vulnerabilidades que se puedan explotar posteriormente, por medio de la herramienta NMAP ejecutamos el comando nmap -sS -sV -O -p- --script vuln,smb-vuln*,ssh-auth-methods -vv 192.168.33.132.

Explicación del Comando.

Tabla 4

Explicación del Comando para la Detección de Vulnerabilidades.

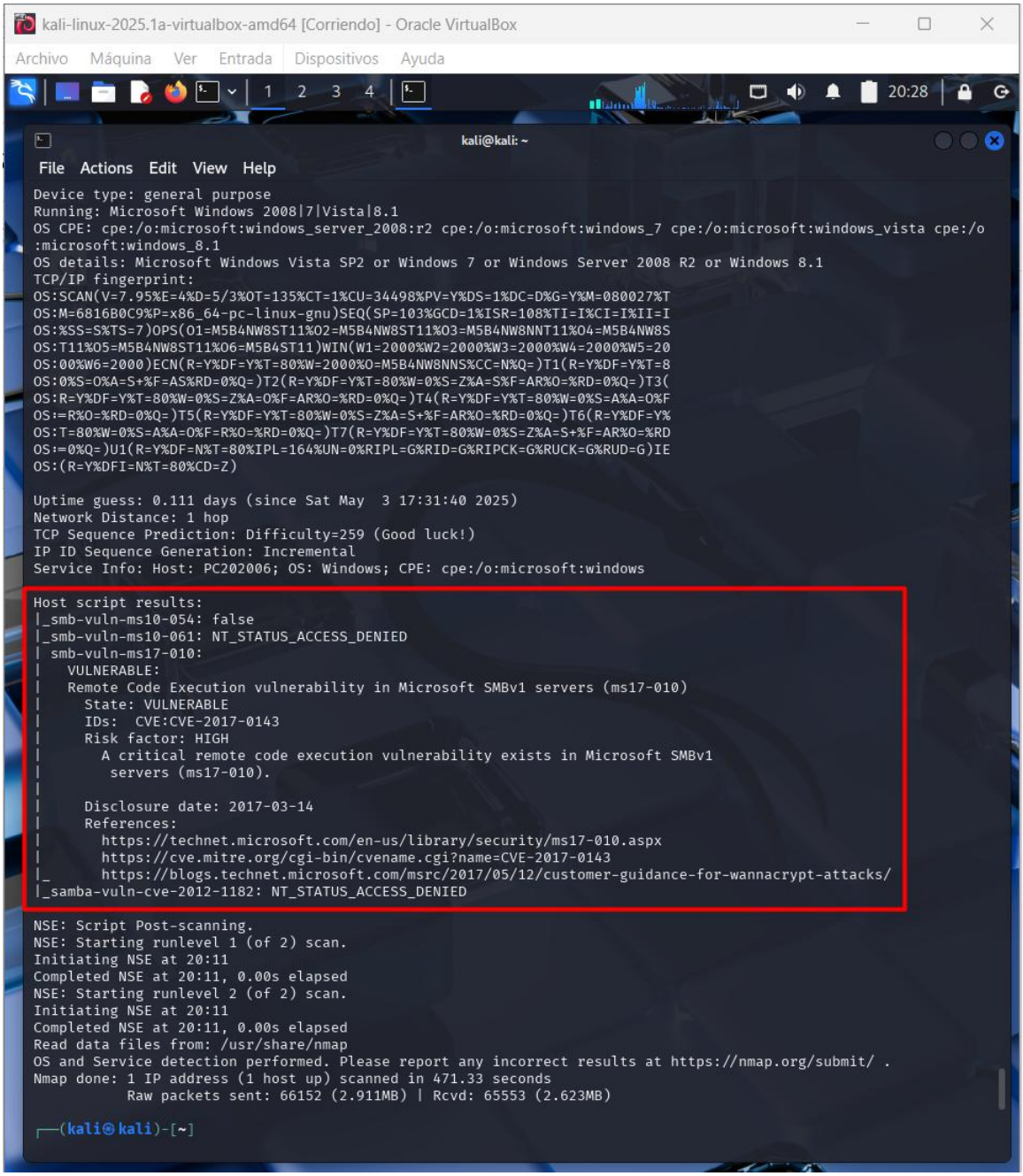
Opción	***Significado***	***Función / Descripción***
-sS	Escaneo SYN (Stealth Scan)	Envía paquetes SYN a los puertos. No establece conexión completa (semiabierto). Más sigiloso y menos detectable por firewalls o registros.
-sV	Detección de versiones	Intenta identificar las versiones exactas de los servicios encontrados en los puertos abiertos.
-O	Detección del sistema operativo	Analiza las respuestas del host para inferir qué sistema operativo está ejecutando.
-p-	Escaneo de todos los puertos (0-65535)	Escanea **todos** los puertos TCP, no solo los 1000 más comunes (que es el valor por defecto).

--script vuln,smb-vuln,ssh-auth-methods*	Uso de scripts NSE (Nmap Scripting Engine)	Ejecuta scripts de seguridad específicos: vuln: Escaneo general de vulnerabilidades. smb-vuln*: Todos los scripts de vulnerabilidad SMB. ssh-auth-methods: autenticación SSH.
-vv	Modo verboso (nivel 2)	Proporciona salida más detallada en tiempo real durante el escaneo.
192.168.33.132	Dirección IP del objetivo	Host específico para escanear. En este caso, una máquina dentro de una red local.

Nota. Tabla con la explicación detallada del comando utilizado con la herramienta NMAP de Kali Linux en la detección de vulnerabilidades en la máquina de Windows 7.

Figura 13

Resultado del Escaneo de Vulnerabilidades.



Nota. Evidencia gráfica que documenta los hallazgos del escaneo de vulnerabilidades ejecutado en el host analizado.

A continuación, se exponen detalles relevantes revelados por la herramienta NMAP luego del escaneo.

Tabla 5

Reporte Detallado de Hallazgos de Vulnerabilidades.

Categoría	***Detalle***
IP del Host	192.168.33.132
MAC Address	08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Sistema Operativo	Microsoft Windows 7 (posible: Vista SP2, Server 2008 R2, Windows 8.1)
Workgroup	WORKGROUP
Distancia de red	1 salto (misma red local)
Puertos abiertos	**Puerto** 135/tcp 139/tcp 445/tcp 554/tcp 2869/tcp 5357/tcp 10243/tcp 49152/tcp 49153/tcp 49154/tcp 49155/tcp

	49156/tcp 49157/tcp
Vulnerabilidades	**MS17-010 (EternalBlue):** VULNERABLE (CVE-2017-0143, ejecución remota de código en SMBv1, riesgo crítico) **MS10-054:** No vulnerable **MS10-061:** Acceso denegado **CVE-2012-1182 (Samba):** Acceso denegado
Servicios Web	Microsoft HTTPAPI httpd 2.0 en puertos 2869, 5357, 10243 Scripts ejecutados: XSS, CSRF, JSONP, WordPress, descarga de código fuente, etc. **Resultado:** No se encontraron vulnerabilidades web relevantes (no XSS, no CSRF, no WordPress, no endpoints JSONP, no descargas de código fuente)

Nota. Explicación detallada del resultado del escaneo, los servicios y las vulnerabilidades detectados en el host Windows 7 escaneado.

Detalle de CVE-2017-0143

El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario mediante paquetes manipulados, lo que se conoce como "vulnerabilidad de

ejecución remota de código SMB en Windows". Esta vulnerabilidad es diferente de las descritas en CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148. (CVE. 2017).

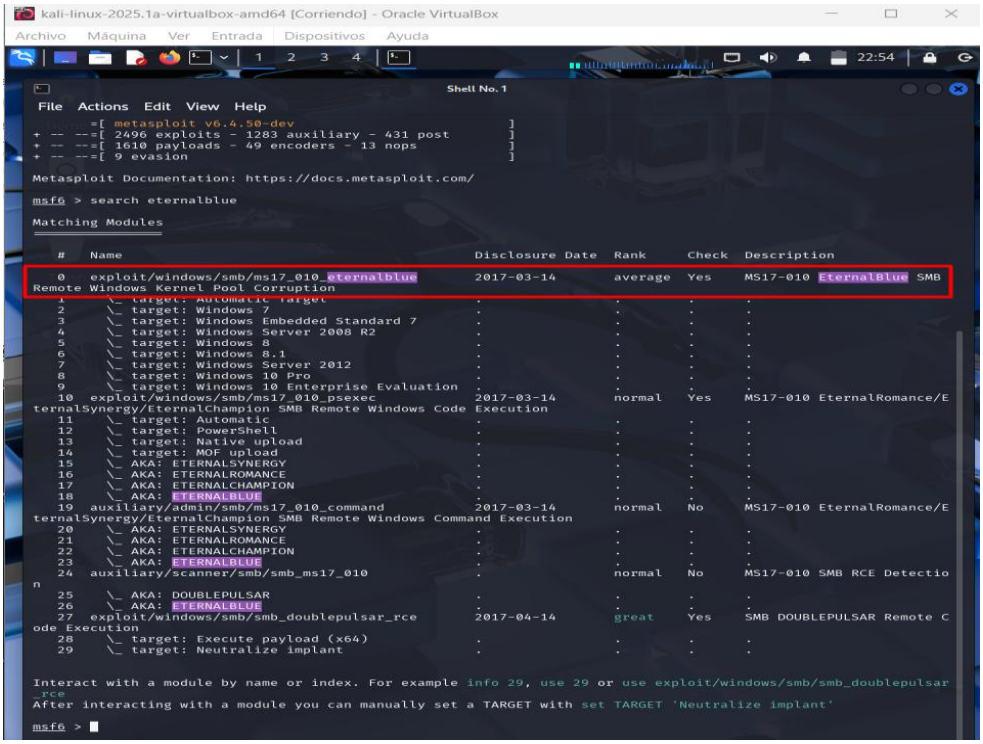
Fase de Explotación

En esta fase se utilizó la herramienta Metasploit Framework, poniendo a prueba la vulnerabilidad encontrada y lograr determinar si suponen una amenaza real y son explotables.

Antes de iniciar un ataque debemos verificar si el exploit existe, esto lo hacemos con el comando search eternalblue.

Figura 14

Verificación de la existencia del Exploit EternalBlue.

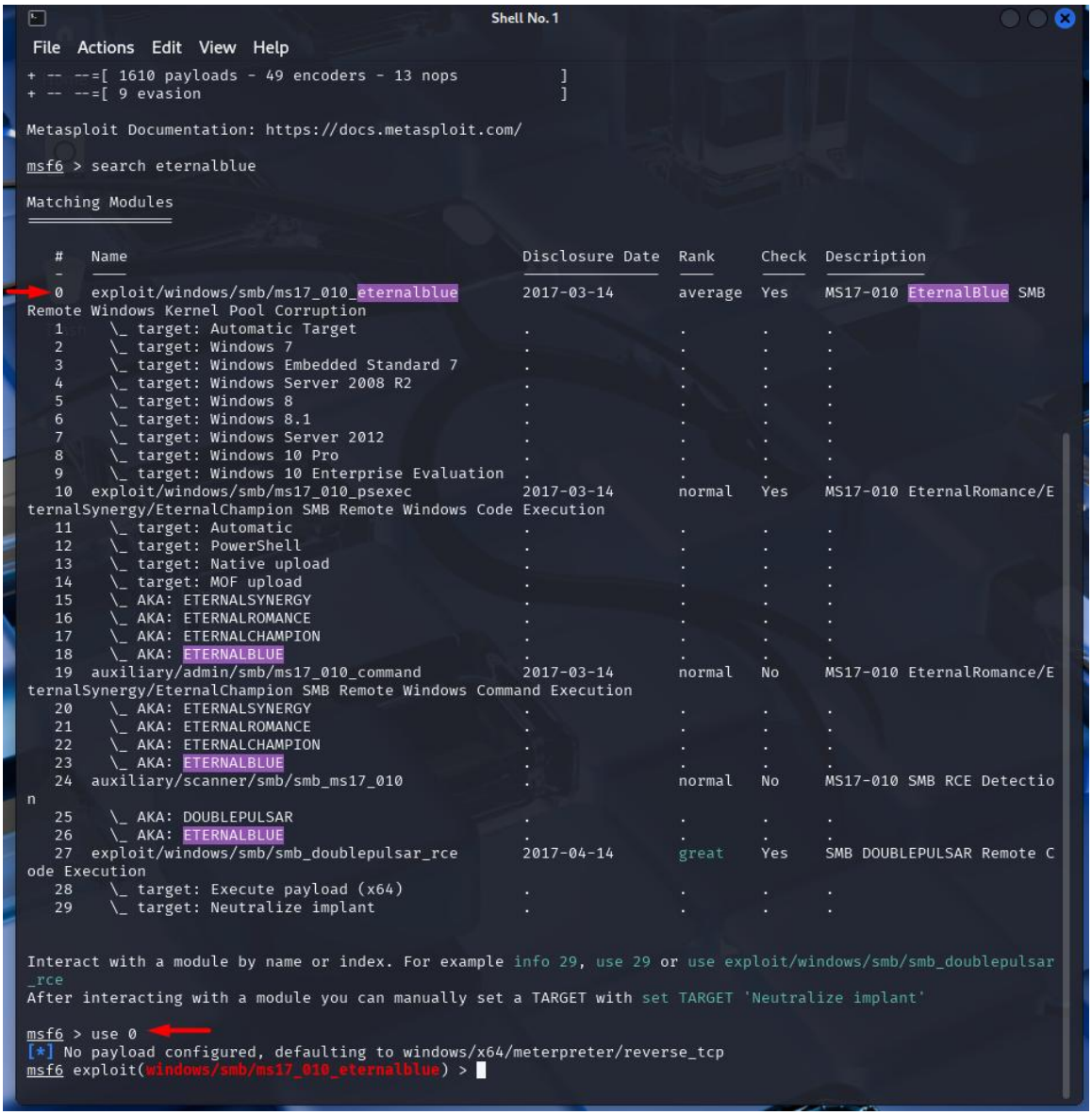


Nota. Evidencia gráfica que documenta la ejecución del comando para la verificación de la existencia del exploit.

Luego de comprobar la existencia del exploit y de saber que su identificador es el cero "0" utilizamos el comando use 0 para cargar el exploit.

Figura 15

Selección del Exploit a Utilizar.

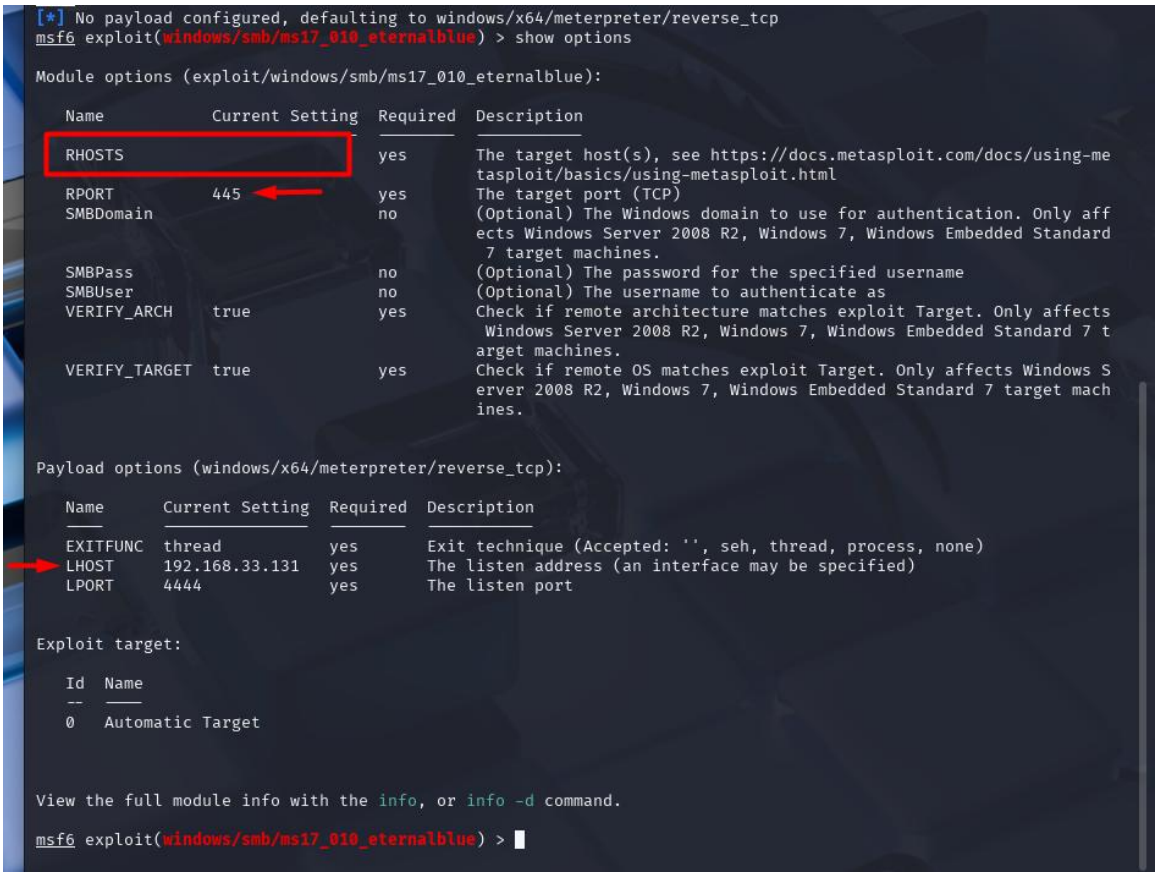


Nota. Registro visual de la selección del Exploit a ejecutar para aprovechar la vulnerabilidad de la maquina Windows 7.

Realizado lo anterior, verificamos las opciones del Exploit seleccionado con el comando show options.

Figura 16

Verificación de Opciones de Configuración del Exploit.

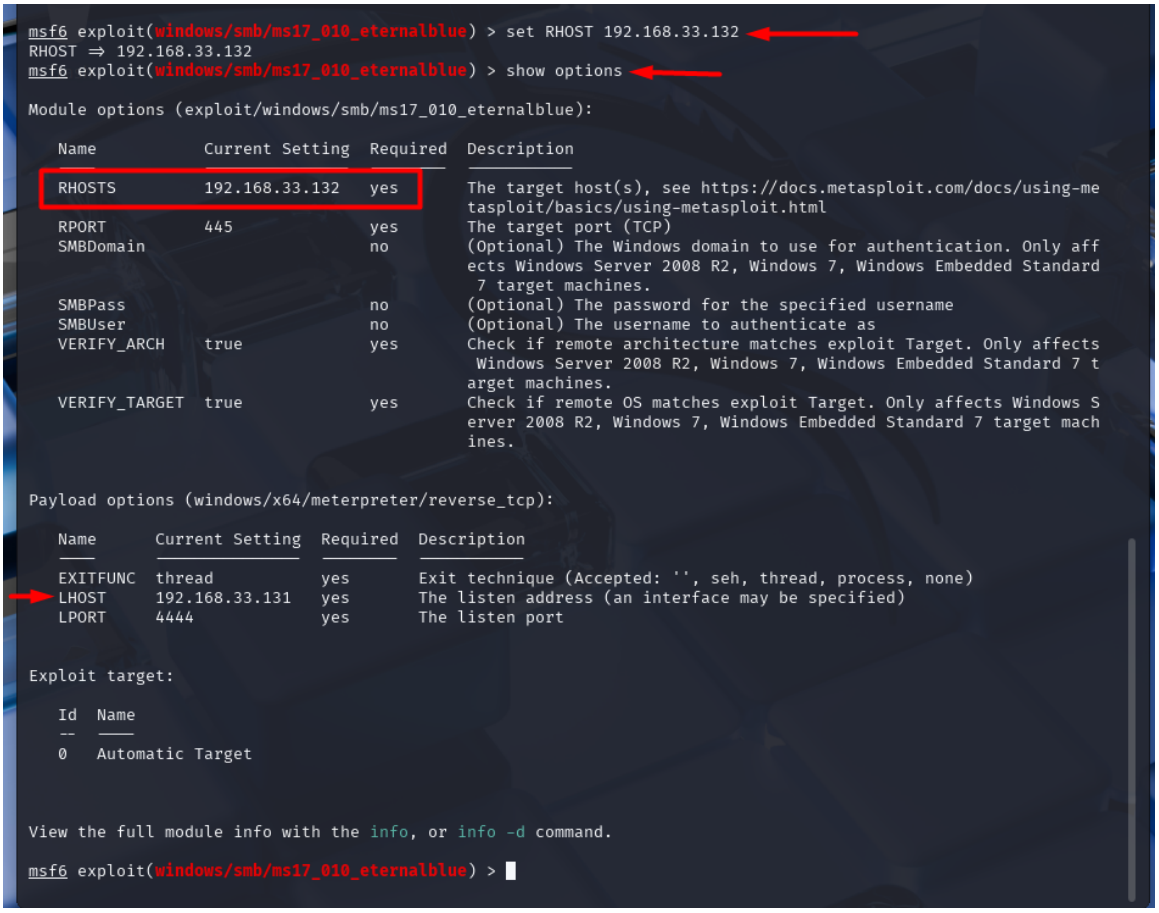


Nota. Evidencia gráfica de la configuración detallada del módulo de explotación windows/smb/ms17_010_eternalblue dentro del entorno Metasploit Framework.

La configuración la ajustamos según nuestro objetivo para ejecutar un ataque de tipo Remote Code Execution (RCE), lo que se debe hacer es asignar la ip de la maquina objetivo en el apartado RHOSTS mediante el comando set RHOST 192.168.33.132

Figura 17

Asignación de IP Objetivo.

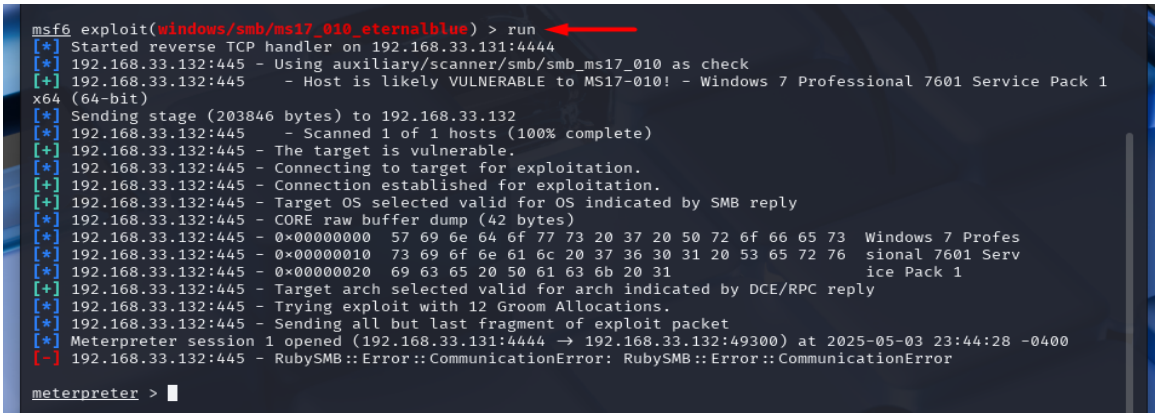


Nota. Captura de pantalla donde se evidencia la asignación de la dirección IP de la maquina objetivo.

En este momento tenemos completamente configurado el exploit para poder atacar la maquina Windows 7, solo queda ejecutar un el comando run y esperar a que nos de control de remoto de la máquina víctima.

Figura 18

Ejecución Comando run.

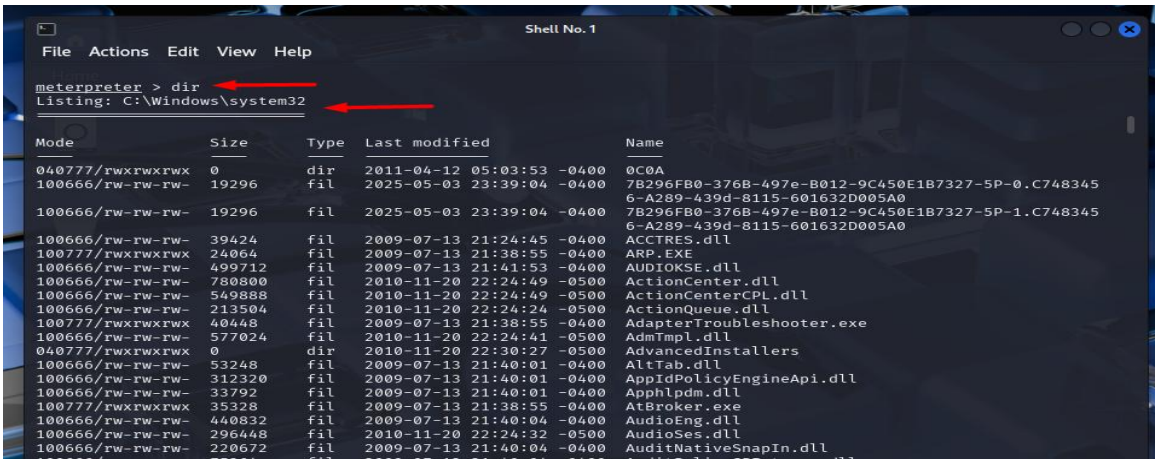


Nota. Captura de pantalla donde se evidencia la ejecución del comando run y se lanza el ataque, el cual nos permite tener acceso a la maquina objetivo.

Con el fin de evidenciar el control de la maquina ejecutamos el comando dir con el fin de listar los archivos que se encuentran en el objetivo.

Figura 19

Ejecución Comando dir.



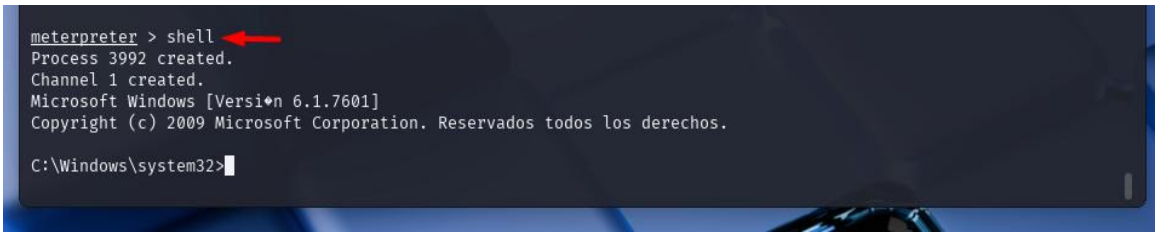
Nota. Captura de pantalla de la ejecución del comando dir desde el meterpreter.

Fase de Post Explotación.

Desde la sesión activa de Meterpreter en la maquina comprometida, procedemos con la creación del usuario FreddyLeon, estableciendo con esto un acceso persistente y controlado sobre el host objetivo, iniciamos abriendo un shell en la máquina víctima mediante la ejecución del comando shell.

Figura 20

Ejecución del Shell en la Maquina Comprometida.

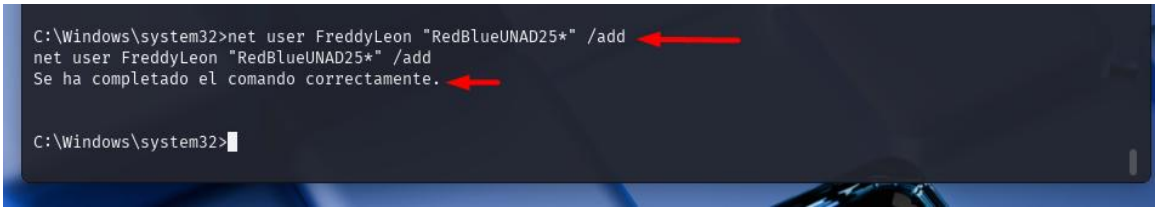


Nota. Evidencia gráfica de la ejecución de un Shell en la maquina víctima desde el Meterpreter.

En este punto de la explotación procedemos a la creación del usuario FreddyLeon, mediante la ejecución del comando net user FreddyLeon "RedBlueUNAD25*" /add

Figura 21

Creación de Usuario.

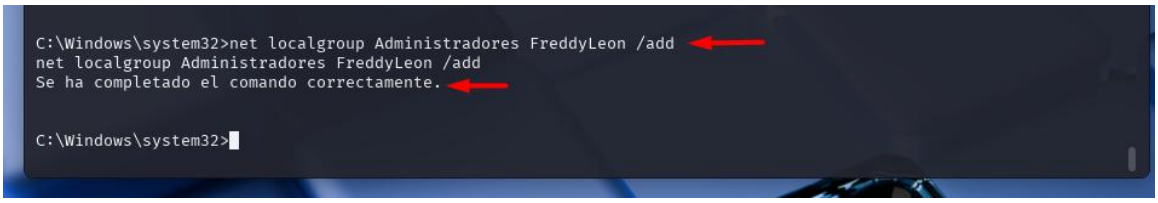


Nota. Evidencia gráfica de la creación del usuario FreddyLeon desde el Meterpreter.

Una vez creado el usuario se procede a la elevación de privilegios como administrador, mediante la ejecución del comando net localgroup Administradores FreddyLeon /add

Figura 22

Elevación de Privilegios de Usuario.



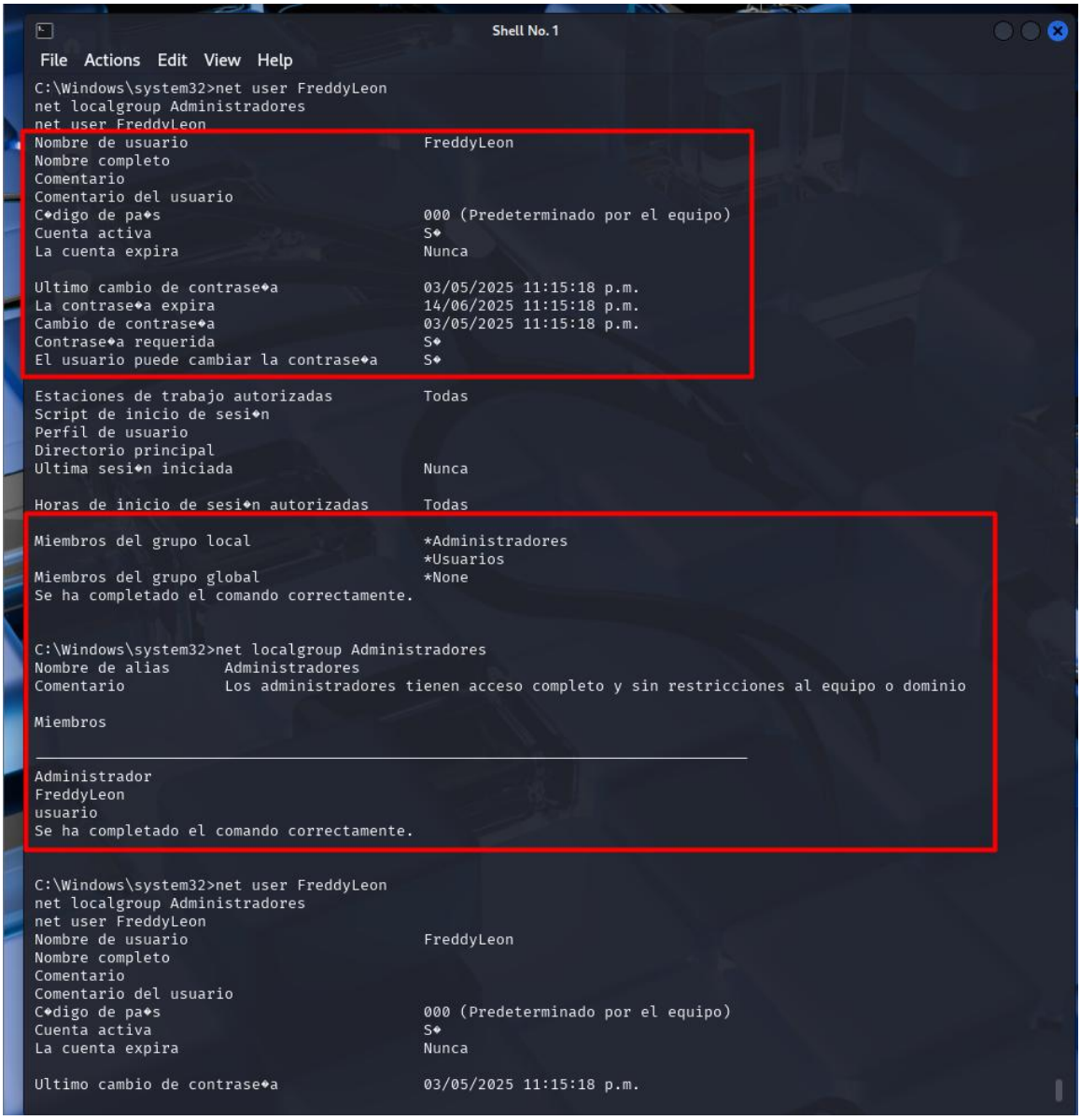
Nota. Captura de pantalla donde se evidencia la elevación de privilegios al usuario FreddyLeon.

Es así como un cerrajero no solo hace una llave, sino que, además de hacerla, también tiene que verificar que la puerta abra a la vez sin romperla. Tras la creación del usuario y asignada la contraseña, este paso de elevar los privilegios del usuario al nivel de Administrador, no se hace al azar, sino que constituye un paso estratégico en una táctica para asegurar que el persistente acceso al sistema comprometido pueda mantenerse.

Se verifica el trabajo meticulosamente para asegurar que el usuario haya sido creado y configurado correctamente, no es técnicamente un formalismo, sino una afirmación de que el acceso obtenido allí ya existe y que es funcional, estable y discreto. Así se constituye una entrada moderada a la máquina víctima sin hacer ruido.

Figura 23

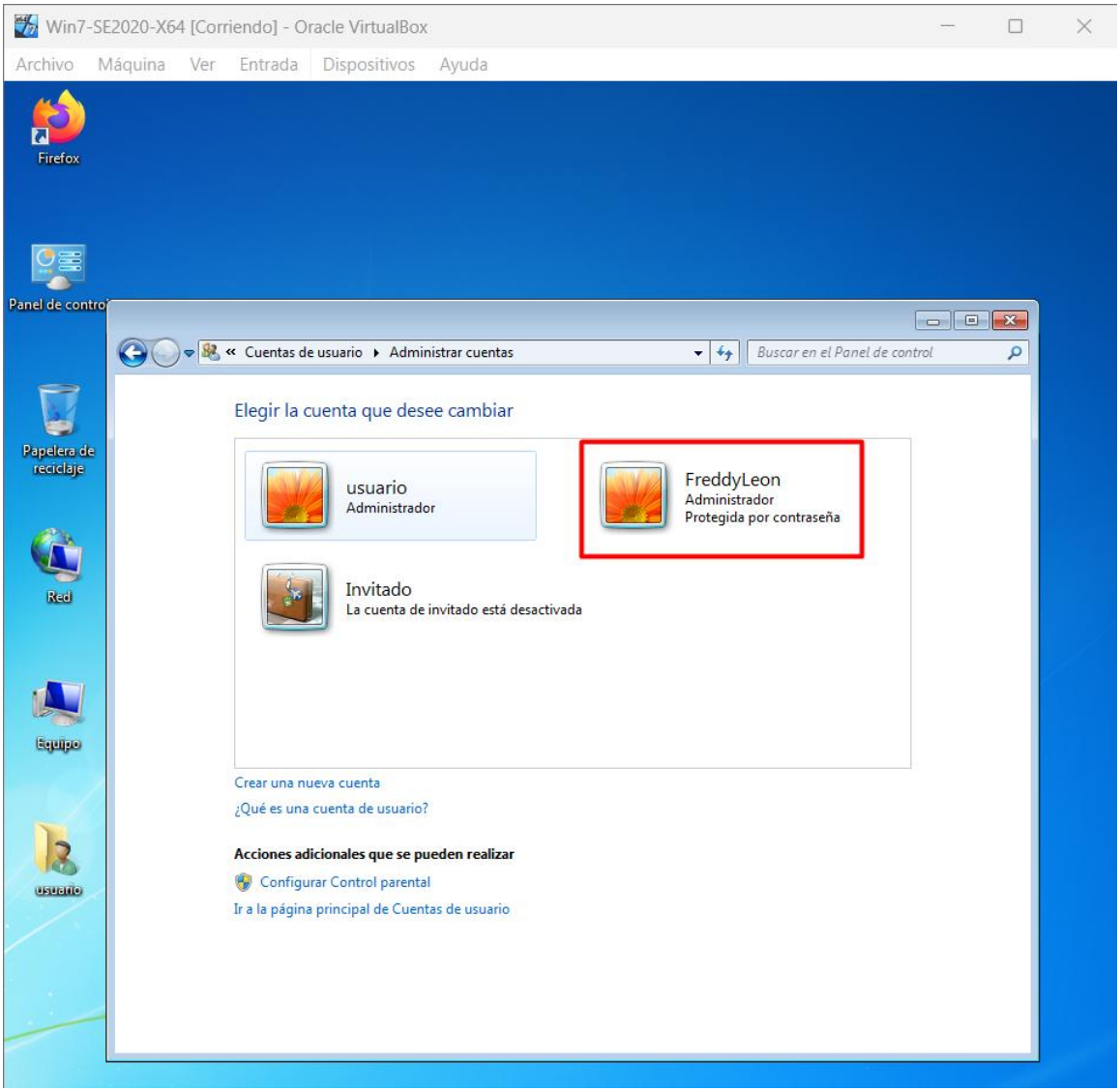
Verificación de Usuario y Privilegios.



Nota. Captura de pantalla donde se evidencia que el usuario FreddyLeon aparece como miembro del grupo Administradores.

Figura 24

Verificación de Usuario desde Máquina Víctima.



Nota. Captura de pantalla tomada desde el entorno gráfico de la máquina atacada donde se evidencia el usuario creado, la elevación de privilegios como Administrador y que está protegido por contraseña.

Fase de Análisis y Reporte.

Análisis de Seguridad – Host Windows 7 (192.168.33.132)

Fecha: 03 de mayo de 2025

Elaborado por: Freddy Alexander León Neira

Tabla 6

Resumen Ejecutivo Resultados Pentesting.

Ítem	***Detalle***
Host Analizado	192.168.33.132
Sistema Operativo	Microsoft Windows 7 (posible Vista SP2, Server 2008 R2, Windows 8.1)
MAC Address	08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Workgroup	WORKGROUP
Distancia de red	1 salto (misma red local)
Puertos y servicios abiertos	135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 554/tcp (rtsp?), 2869/tcp (http/Microsoft HTTPAPI 2.0), 5357/tcp (http/Microsoft HTTPAPI 2.0), 10243/tcp (http/Microsoft HTTPAPI 2.0), 49152-49157/tcp (msrpc)
Vulnerabilidades detectadas	- **MS17-010 (EternalBlue, CVE-2017-0143):** Ejecución remota de código vía SMBv1. - **Otros scripts SMB:** ms10-054 (no vulnerable), ms10-061 (acceso denegado), samba-vuln-cve-2012-1182 (acceso

	denegado). - **Servicios HTTP:** No se detectaron vulnerabilidades web (XSS, CSRF, JSONP, WordPress, etc.).
Riesgos principales	- Compromiso total del sistema (acceso remoto como administrador). - Propagación de malware/ransomware (WannaCry, NotPetya). - Amplia superficie de ataque por múltiples servicios y puertos expuestos. - Sistema operativo sin soporte oficial, sin parches futuros.
Evidencia de explotación	- Se demostró la explotación de MS17-010 creando el usuario administrador “FreddyLeon” en el sistema objetivo, validando la criticidad del riesgo.
Mitigaciones críticas	1. Descargar e instalar el parche oficial de Microsoft: MS17-010 Security Update. 2. Seguir las instrucciones oficiales de Microsoft para deshabilitar SMBv1 en el sistema. 3. Migrar a una versión de Windows soportada (Windows 10 o superior) para recibir actualizaciones de seguridad continuas.
Mitigaciones adicionales	1. Restringir acceso a puertos 135, 139, 445 y servicios web solo a redes autorizadas mediante firewall. 2. Cerrar puertos y servicios innecesarios.

	3. Revisar políticas de contraseñas y considerar autenticación multifactor. 4. Realizar escaneos periódicos de vulnerabilidades y monitoreo continuo.
Conclusión	El host tiene una vulnerabilidad crítica explotable del cual se administra el sistema. Dichas mitigaciones de seguridad deben ser aplicadas de forma urgente para prevenir incidentes de seguridad, pérdida de datos y los servicios aniquilados.

Nota. Tabla detallada, basada en el escaneo Nmap, el análisis de riesgos y explotación de vulnerabilidades.

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

Los elementos más relevantes del anexo 4 – escenario 3 que permitieron identificar el fallo de seguridad específico (MS17-010/EternalBlue) fueron:

a) Detección del puerto 445/tcp abierto y el servicio SMB activo en Windows 7.
b) Resultado del script smb-vuln-ms17-010 de Nmap, que confirma la vulnerabilidad.
c) Identificación del sistema operativo Windows 7, conocido por ser vulnerable si no está actualizado.
d) Referencias a CVE-2017-0143 y fuentes oficiales, que validan la criticidad del hallazgo.

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

Nmap fue la herramienta utilizada. Se empleó para realizar un escaneo de puertos, detección de servicios y ejecución de scripts de seguridad (como smb-vuln-ms17-010) que permitieron identificar vulnerabilidades específicas en la máquina Windows.

La aplicación específica vulnerable es SMB (Server Message Block), que utiliza el puerto 445/tcp.

Esto se evidencia en el reporte Nmap: 445/tcp open microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

Este puerto es el canal por el cual se detectó la vulnerabilidad crítica MS17-010 (EternalBlue) en el sistema Windows.

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

Si comparamos la seguridad de una máquina Windows con la muralla de una ciudad antigua, las puertas de seguridad, es decir, los puertos de red, después de todo son muy importantes y deben estar bajo continua observación, solo permitiendo el paso con permisos.

Sin embargo, cuando el resultado del escaneo muestra que la puerta 445, lo que corresponde al servicio SMB el que se encuentra abierto de par en par, denota un fallo grave e inminente dentro del sistema.

La puerta completa de entrada a la ciudad está abierta, es decir, hay un fallo en la cerradura que le permite a cualquier intruso, con el conocimiento de la cerradura, sin tener prisa y tomándome su tiempo realizar el ataque Eternal Blue, una amenaza mediante la que el experto

ciberdelincuente ocupa la cerradura MS17-010. No necesita violentar la puerta o llamar la atención.

Una vez que haya ingresado, el intruso podrá moverse con libertad, crear malas llaves (usuarios con privilegios), abrir puertas traseras, robar información, incluso prender fuego a archivos (instalar ransomware).

El equipo Windows no se encuentra actualizado, razón que lo hace accesible para un ataque visto de esta manera, sin actualizaciones ni protección adecuada queda expuesto a todo tipo de ataques. Un agresor lo hará desde cualquier posición de alcance de red fiable siguiendo la vulnerabilidad sin necesidad de saber contraseñas o incluso acceder físicamente.

El impacto es devastador, la información pierde su confidencialidad, integridad y disponibilidad, esto sería, por ejemplo, la creación del usuario FreddyLeon con privilegios de administrador, haciéndose dueño del sistema.

Asimismo, “es como una plaga” que se propaga a otras ciudades o máquinas enlazadas, replicando el daño masivamente, exactamente como ocurrió con WannaCry y NotPetya.

Para ilustrarlo visualmente las piedras lanzadas por el atacante podríamos decir que, no encuentran resistencia alguna para cruzar la muralla y dejan una brecha al caer por la que diversas amenazas pueden entrar, entonces, aquel que gaste su tiempo para encontrar esa grieta o brecha de seguridad encontrará la entrada para controlar totalmente el sistema, es mejor fortalecer cada puerta y actualizarse de cerraduras vigentes en nuestro entorno digital.

Capítulo 4. Formular Estrategias de Contención Mediante el Análisis de Riesgos y Vulnerabilidades en una Infraestructura TI.

Anexo 5 – Escenario 4

Situación Problema: Análisis Blue Team.

CyberFort Technologies solicita a sus integrantes de Blue Team contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. **CyberFort Technologies** le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

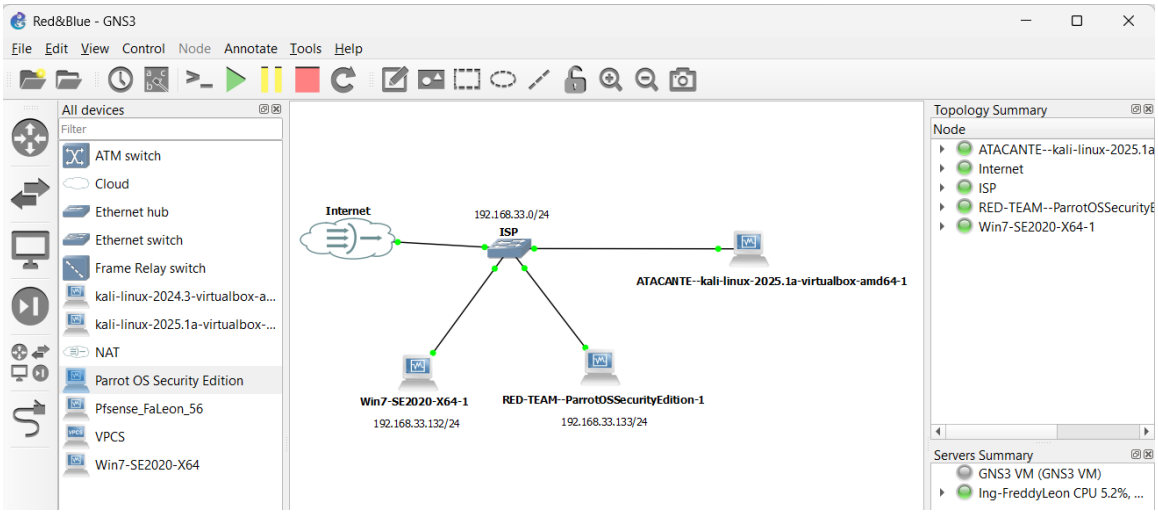
4.1.¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Como especialista en Seguridad Informática y miembro del equipo Red Team, enfatizo que la respuesta debe ser ejecutada con inmediatez, sistemática y recolectando la mayor evidencia técnica para la respectiva documentación del incidente y la respuesta para repeler el ataque, combinando conocimientos de tácticas adversarias y metodologías de respuesta a incidentes.

Topología de Red del Escenario Controlado.

Figura 25

Topología Anexo 5 – Escenario 4.



Nota. Captura de pantalla de la Topología diseñada para el desarrollo del Escenario 4, bajo metodología de ambiente controlado utilizando la herramienta GNS3.

4.1.1. Evaluación Inicial y Contención

4.1.1.1. Identificación del Perímetro de Compromiso

Determinar de forma rápida y exhaustiva comprobando el alcance del ataque, estableciendo objetivos específicos tales como:

- Identificar el alcance y vector del ataque.
- Contener la amenaza para evitar propagación.
- Preservar evidencia para análisis forense.

Tabla 7

Acciones Técnicas.

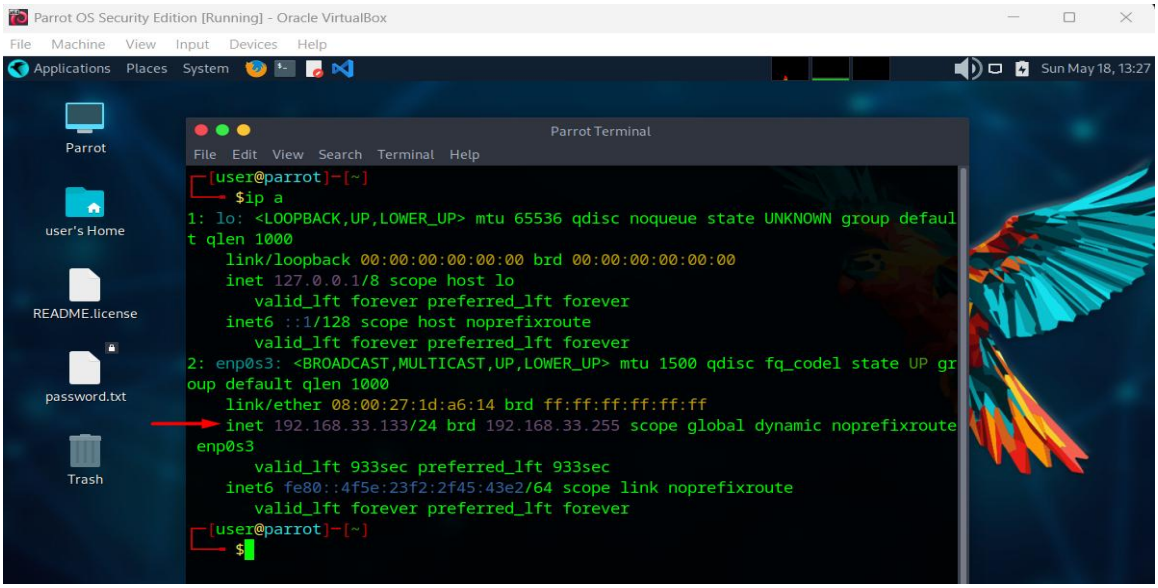
Paso	***Acción***	***Herramienta GPL***	***Justificación Técnica***
1	Escaneo de red para identificar hosts afectados y puertos abiertos	Nmap	Permite detección activa de hosts comprometidos y servicios expuestos, crucial para delimitar perímetro de ataque (Hilt & Zahravi, 2023).
2	Captura y análisis de tráfico sospechoso	Wireshark	Inspección profunda de paquetes para detectar comunicación con C2 y patrones anómalos.
3	Aislamiento de sistemas comprometidos	-	Desconexión física o lógica para evitar movimientos laterales.
4	Revocación de credenciales comprometidas	-	Previene escalada y persistencia del atacante.

Nota. Enfoque detallado con argumentos técnicos y herramientas GPL para realizar la evaluación inicial y la contención rápida.

Paso 1: Escaneo de red para identificar hosts afectados y puertos abiertos.

Figura 26

Identificación del Rango IP VM Parrot.

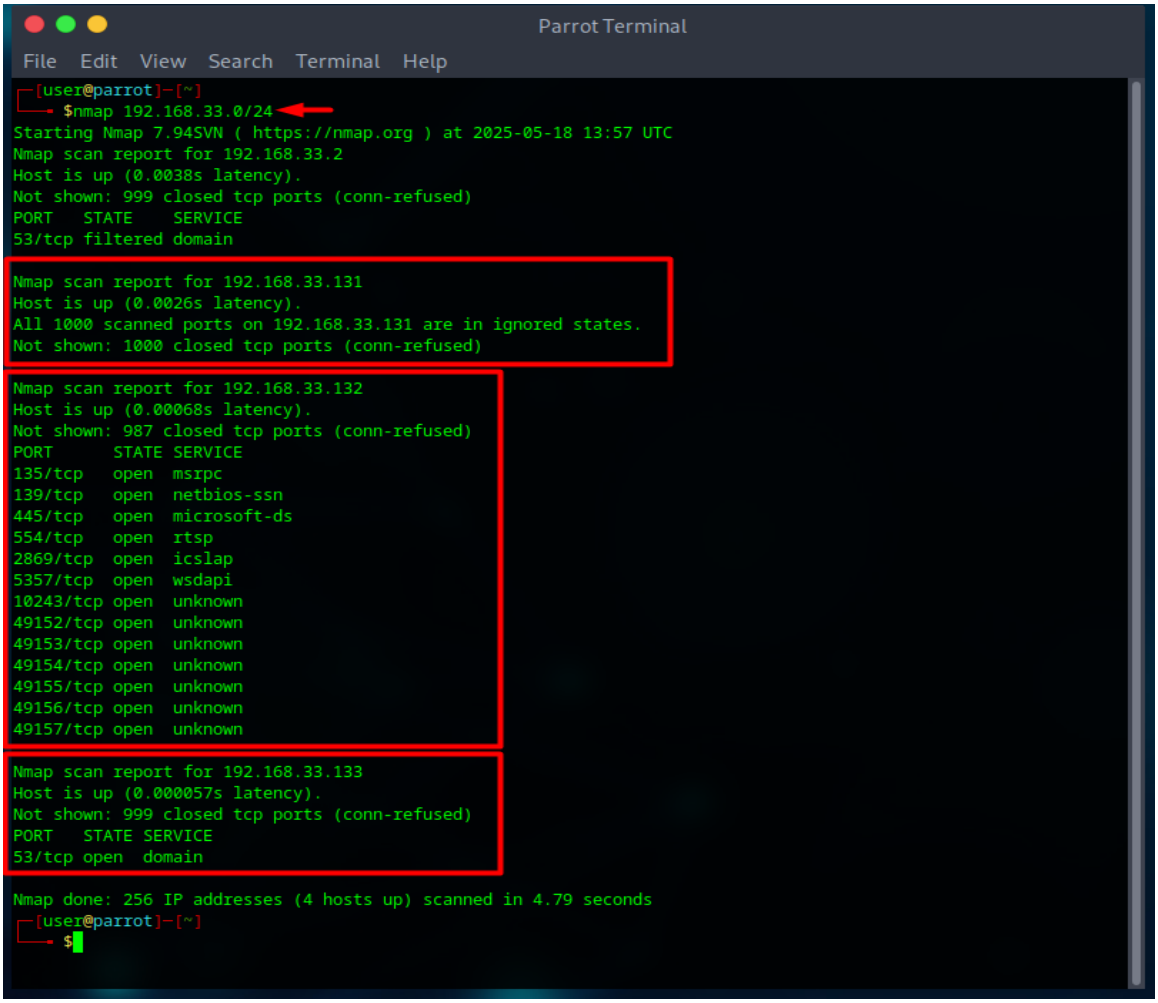


Nota. Captura de pantalla de la ejecución del comando ip -a en la terminal de la VM Parrot, para identificar el Rango IP en el cual se encuentra.

Una vez identificado el rango de red en la cual nos encontramos y el direccionamiento IP conocido por la organización, procedemos a lanzar un escaneo de red con el fin de detectar intrusos en la red, los cuales estén ejecutando ataques cibernéticos que denoten alteraciones en los sistemas, alteraciones en los datos, eliminación de información, inyección de malware, creación de backdoors, entre otras acciones maliciosas que pongan el riesgo la confidencialidad, integridad y disponibilidad de la información.

Figura 27

Escaneo de Red.



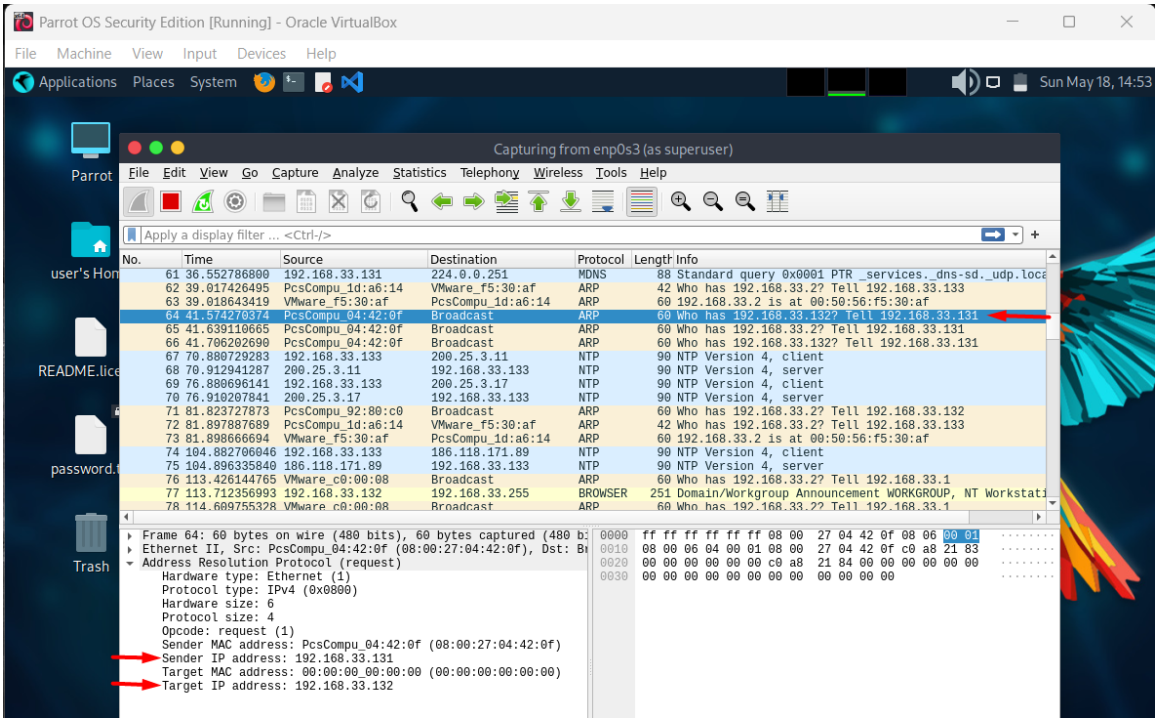
Nota. Evidencia gráfica que documenta la ejecución del comando para la identificación de hosts.

El objetivo principal de realizar el escaneo es la identificación de los diferentes dispositivos dentro de la red local y los respectivos servicios expuestos, determinando de forma preliminar la hipótesis del incidente de seguridad.

Paso 2: Captura y análisis de tráfico sospechoso.

Figura 28

Captura de Trafico de Red Herramienta Wireshark.



Nota. Evidencia gráfica que documenta los hallazgos de la captura del tráfico de Red mediante la herramienta Wireshark.

Con la ejecución de esta técnica se logra evidenciar el comportamiento de la resolución de direcciones en red, identificando interacciones entre dos dispositivos uno conocido dentro de la red local y el otro no, definiendo un patrón anómalo en las solicitudes de ARP.

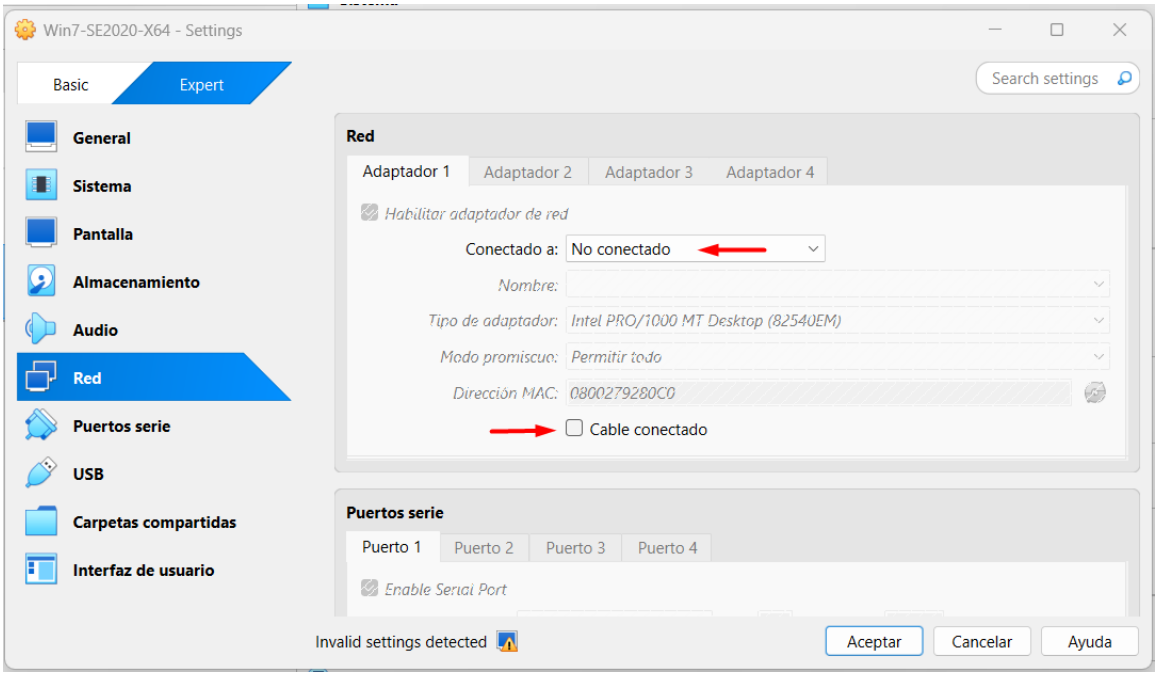
La solicitud identificada revela que el host con dirección IP 192.168.33.131 el cual no se encuentra relacionado en la identificación del direccionamiento IP de la organización, intenta averiguar la dirección MAC del host 192.168.33.132, lo cual ratifica que aún no tiene esa

dirección en su cache de ARP, patrón típico de un escaneo pasivo o la ejecución de la etapa de descubrimiento de red previa a un ciberataque.

Paso 3: Aislamiento de sistemas comprometidos.

Figura 29

Desconexión Física para Evitar Movimientos Laterales.



Nota. Evidencia gráfica que documenta la desconexión de los hosts comprometidos.

El objetivo de realizar la técnica de desconexión del host es inicialmente contener el incidente de forma drástica, evitando que el ciberdelincuente se propague por la red e igualmente preservar la evidencia forense para su posterior recolección y análisis, con el fin de identificar el vector de ataque, la extensión y el compromiso del ataque.

4.1.2. Recolección de Evidencia Forense.

La finalidad de esta fase o técnica se centra en examinar detalladamente el equipo comprometido por medio de la generación de artefactos, identificando el vector de ataque recolección de evidencia, reconstrucción de la línea de ataque.

El procedimiento debe seguir una metodología estricta, la cual se describe a continuación:

4.1.2.1.Preparación.

Consiste en crear un entorno forense aislado utilizando una maquina física o virtual dotada exclusivamente de herramientas forenses, igualmente, la disponibilidad de medios de almacenamiento limpios y etiquetados, con la capacidad suficiente para el almacenamiento de los volcados de memoria y los snapshots, finalmente para preservar la cadena de custodia se deben tener listos los formularios para ser diligenciados y una vez verificados los procedimientos se deben plasmar sus respectivas firmas realizando a su vez el sellado de las unidades.

4.1.2.2.Adquisición Remota de Memoria, Archivos y Registros.

Tabla 8

Procedimiento Forense Detallado.

Paso	***Acción***	***Herramientas / Comandos***
1	**Captura de memoria “viva”**	FTK Imager, Belkasoft RAM Capturer

	• Volcar memoria RAM completa en archivo .raw. • Calcular hash SHA-256 del volcado.	
2	**Adquisición de discos**	dd if=/dev/sdX of=/mnt/forense/sistema.dd bs=4M
	• Imágen bit a bit de todos los volúmenes. • Hash SHA-256 de cada imagen.	
3	**Recolección de logs**	Copia de <SystemRoot>\System32\winevt\Logs*.evtx
	• Eventos de seguridad, sistema y aplicación. • Logs de antivirus y firewall local.	
4	**Captura de registro de red**	Archivo PCAP antes de aislamiento (Wireshark)

5	**Documentación de metadatos de evidencia**	UUID, hora UTC, nombre del analista, ubicación
6	**Montaje forense en solo-lectura**	mount -o ro,loop sistema.dd /mnt/forense/ro

Nota. Tabla con la explicación detallada del procedimiento Forense a realizar.

4.1.3. Análisis de Evidencias.

A continuación, se detalla el tipo de análisis, la actividad a realizar y se sugieren algunas herramientas para realizar el análisis.

Tabla 9

Detalle del Análisis de las Evidencias.

Tipo de análisis	***Actividad***	***Herramientas / Comandos***
Análisis de memoria	Buscar procesos maliciosos inyectados. Detectar conexiones de red "live".	Volatility (pslist, malfind, netscan)
Análisis de disco	Identificar archivos nuevos o modificados (timeline). Detectar rutas de persistencia.	md5deep/sha256deep, fls, tsk_recover
Examen de logs	Correlacionar timestamps de eventos.	Visores de EVTX (wevtutil), Log2Timeline

	Revisar intentos de autenticación fallidos y elevaciones.	
IoC y artefactos	Extraer hashes SHA-256 de binarios maliciosos. Registrar IPs y dominios de C2. Listar rutas de archivos sospechosos.	hashdeep, grep, exportación CSV/STIX-TAXII

Nota. Tabla con la explicación detallada del procedimiento del análisis de evidencias.

4.1.4. Informe de Resultados.

Una vez finalizada la etapa del análisis, se consolida un informe detallado y estructurado donde se exponen el alcance del incidente, su impacto en el host comprometido, las acciones o técnicas ejecutadas para contener el ataque, cronología detallada de los eventos y el diagrama de propagación del ataque.

En lo relacionado con los Indicadores de Compromiso (IoC) se registrarán los hashes, IPs, URLs, Dominios, puertos sospechosos y logs del sistema operativo, asimismo, se relacionarán los artefactos forenses recopilados volcados de RAM, copias de discos, capturas del tráfico de red todos con sus respectivas cadenas de custodia, igualmente, se detallan los formatos de entrega como documentos pdf, pptx, csv o json.

El documento también incluirá las respectivas recomendaciones de fortalecimiento y controles que permitan mitigar futuros ataques o incidentes y por último se proyecta un plan de verificación de post-remediación el cual garantiza el endurecimiento de la infraestructura TI y la restauración segura del equipo comprometido.

Figura 30

Esquema de Detección y Respuesta a Incidentes.

Nota. Gráfica que denota las fases para la detección y respuesta a incidentes de ciberseguridad.

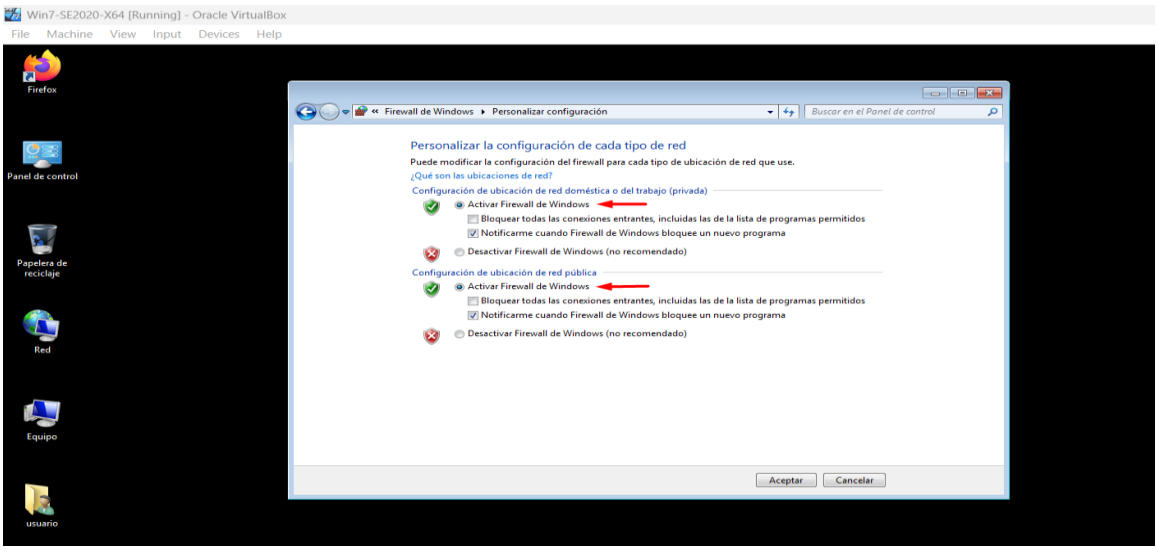
4.2.¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team, qué medidas de hardenización propondría para que el ataque no se repita?

Hardenización Post-Ataque para Mitigar Vulnerabilidades

4.2.1. Activación del Firewall en Equipo comprometido.

Figura 31

Activación Firewall de Windows.



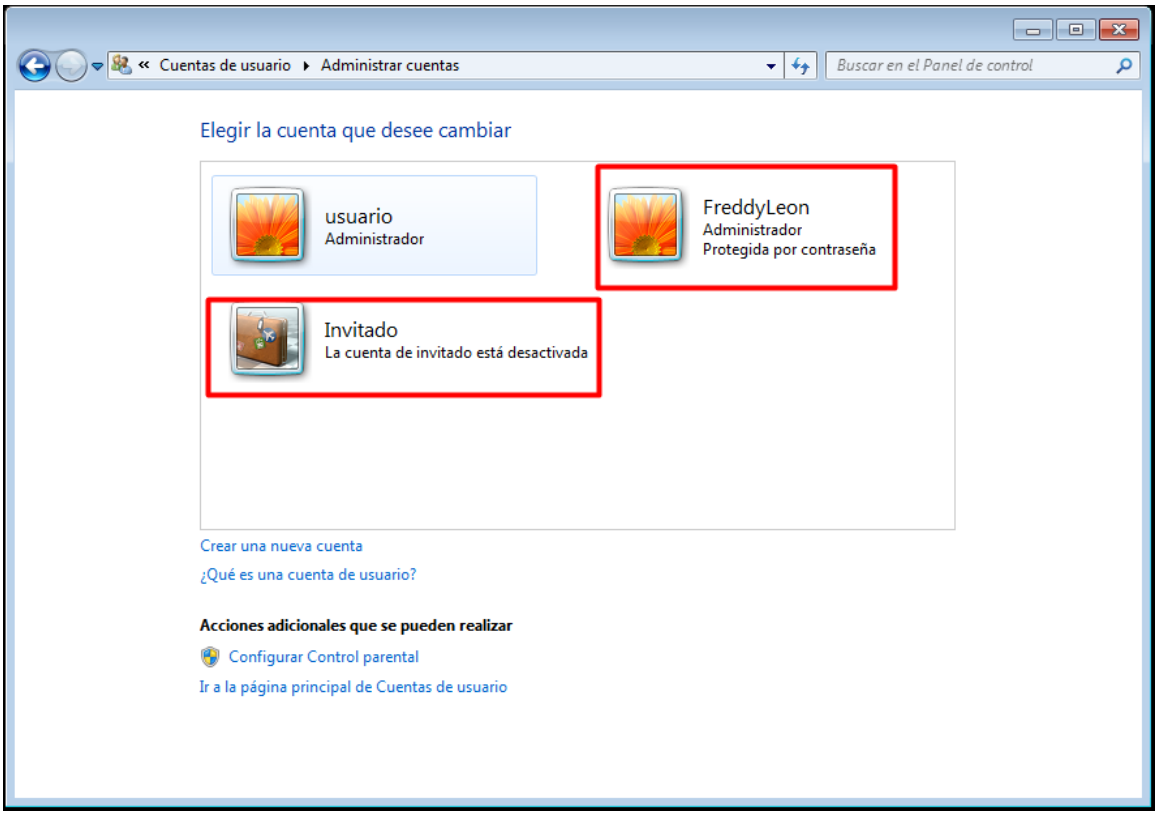
Nota. Evidencia gráfica que documenta la activación del Firewall de Windows en el host comprometido.

Se puede identificar que el sistema operativo carece de un antivirus que permita adicionar una capa de seguridad adicional, se recomienda la instalación de un antivirus con licencia original.

4.2.2. Verificación y Desactivación o Eliminación de Usuarios.

Figura 32

Cuentas de Usuario Equipo Win 7 x64.



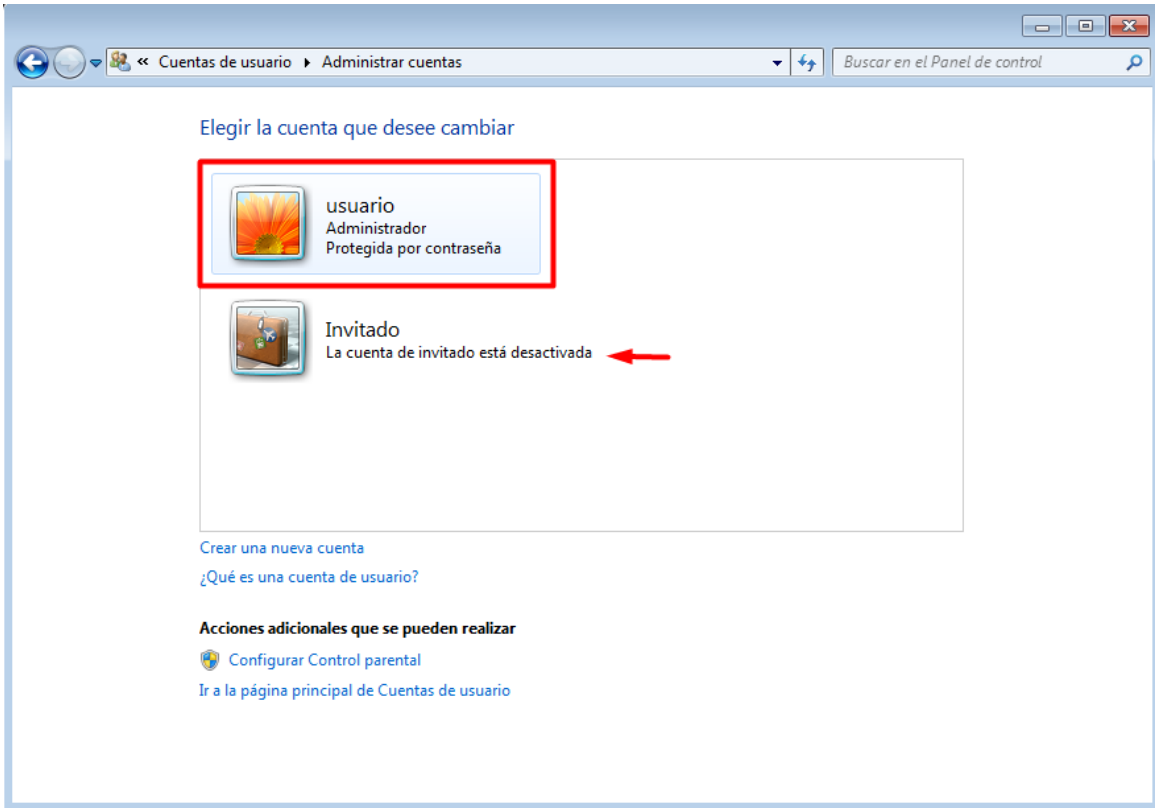
Nota. Evidencia gráfica que documenta las cuentas de usuario dentro del host comprometido.

Con la ejecución de esta medida se está verificando la existencia de una cuenta de usuario no autorizado la cual posee privilegios de Administrador, igualmente se puede validar que la cuenta de usuario invitado se encuentra desactivada y adicionalmente que la cuenta del usuario

autorizado no se encuentra protegida por contraseña, razón por la cual se procede a realizar la eliminación de la cuenta no autorizada y la creación de una credencial para la cuenta autorizada.

Figura 33

Cuentas de Usuarios Autorizados.



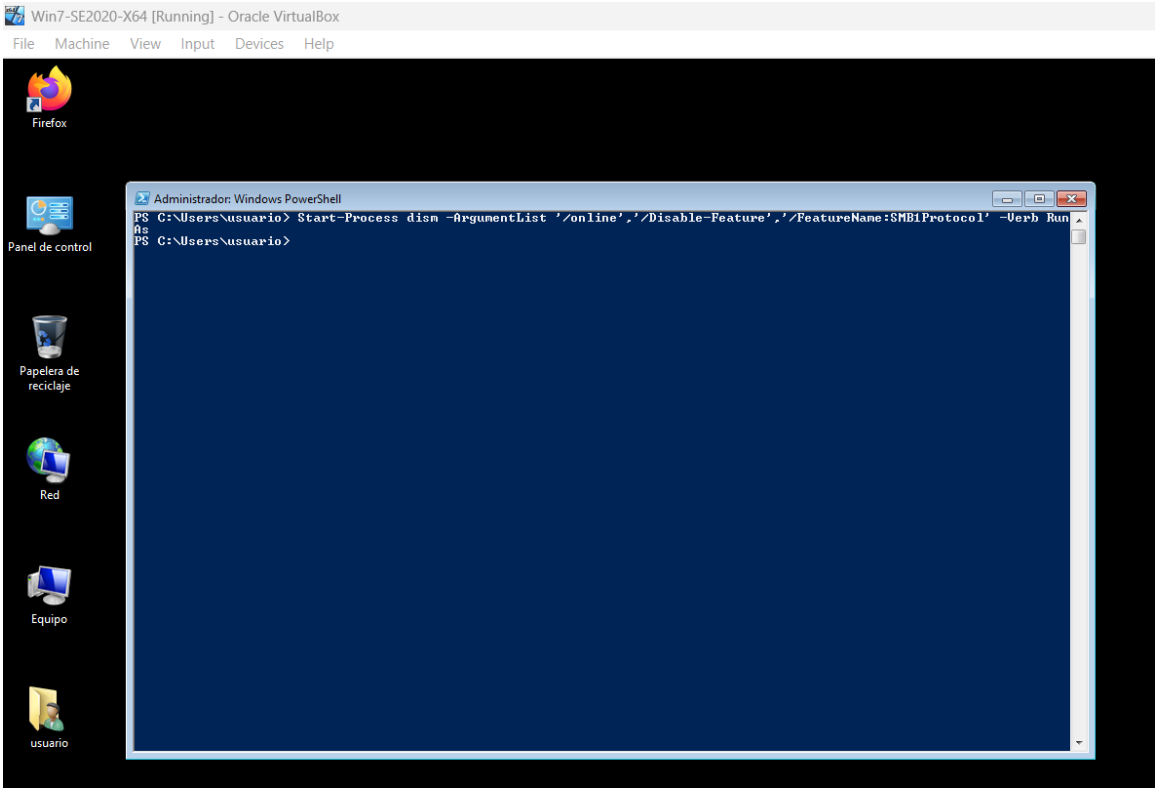
Nota. Evidencia gráfica que documenta la cuenta de usuario autorizada, protegida por contraseña y con privilegios de Administrador dentro del host comprometido.

4.2.3. Deshabilitación de Protocolo SMBv1.

Desde PowerShell se elimina el vector de ataque para EternalBlue, mediante la ejecución del comando Start-Process dism -ArgumentList '/online','/Disable-Feature','/FeatureName:SMB1Protocol' -Verb RunAs

Figura 34

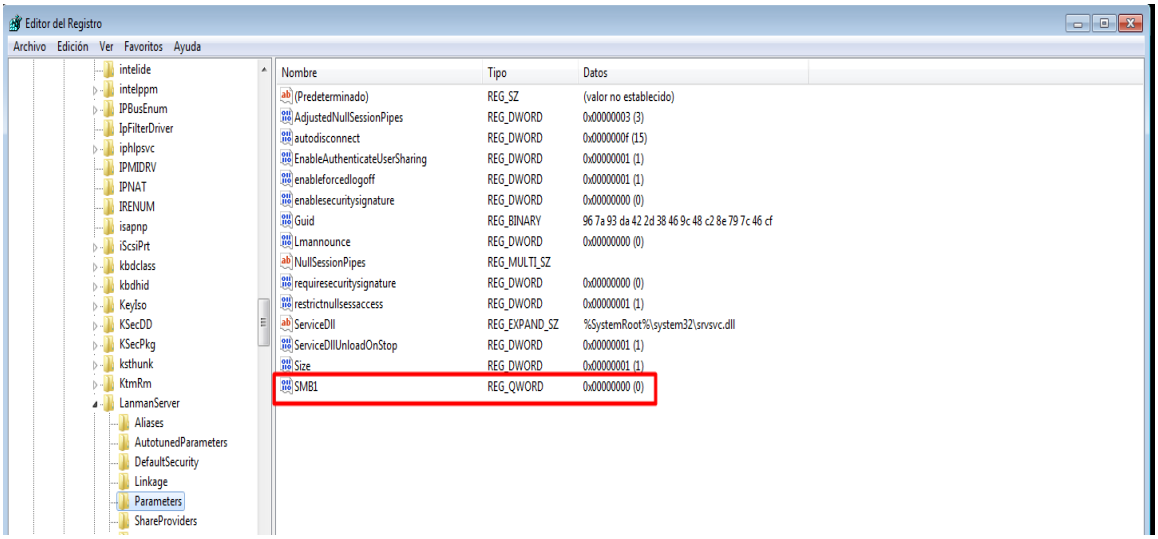
Ejecución del comando en PowerShell.



Nota. Evidencia gráfica que documenta la ejecución del comando para deshabilitar el protocolo SMBv1.

Figura 35

Modificación del Regedit.



Nota. Evidencia gráfica que documenta el bloqueo permanente a nivel de kernel del protocolo SMBv1.

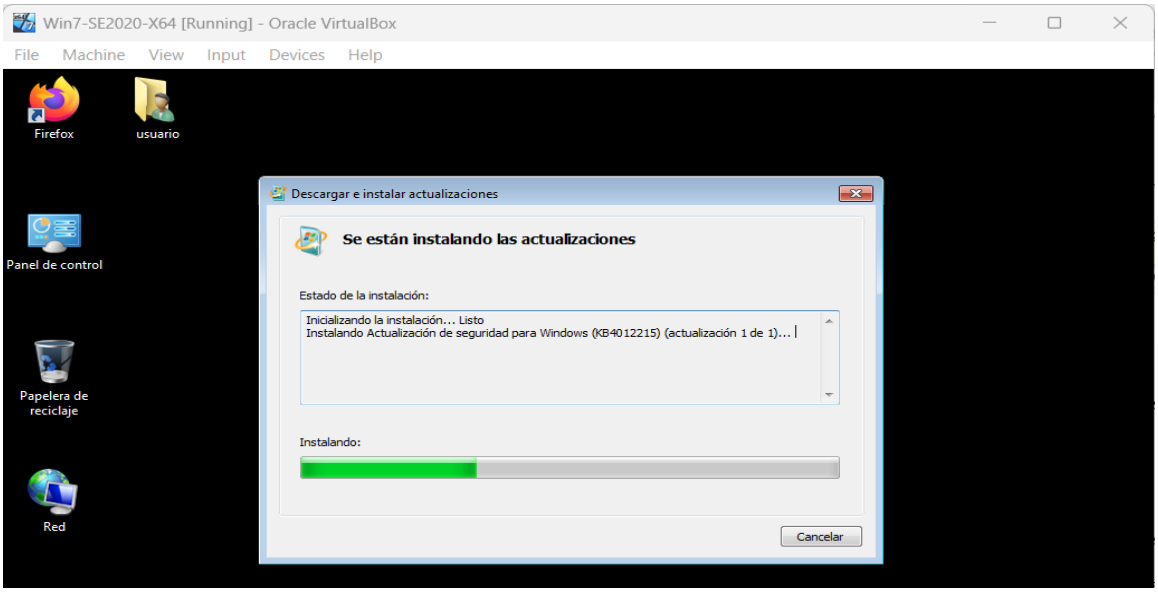
El boqueo se realiza en la siguiente ruta del registro HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 = 0

4.2.4. Gestión de Parches y Actualizaciones.

Una vez identificado el problema de seguridad del equipo, la vulnerabilidad existente la cual fue aprovechada por el atacante se procede a realizar la configuración de las actualizaciones automáticas, pero como se trata de un sistema operativo Windows 7 el cual en la actualidad no existe soporte por parte del fabricante se procede a la búsqueda del respectivo parche y su instalación.

Figura 36

Instalación del parche MS17-010.



Nota. Evidencia gráfica que documenta la instalación del parche de seguridad que corrige la vulnerabilidad EternalBlue.

4.2.5. Segmentación de Red y Control de Accesos

Realizar el Subneteo de la red es una tarea urgente por realizar, así como el análisis y selección de la implementación de una DMZ o el establecimiento de una arquitectura Zero Trust dentro de la organización con el propósito de reducir la superficie de ataque, limitando movimientos laterales del atacante.

Así mismo la creación de controles de acceso y políticas estrictas definidas y aplicadas dentro de un Active Directory crean una sinergia en ciberseguridad y se alinean de cierta manera con los estándares internacionales de ciberseguridad brindando una mayor capacidad de respuesta a futuros incidentes.

4.2.6. Monitoreo Proactivo y Detección de Anomalías.

El monitoreo continuo y la detección de eventos sospechosos se convierten en un pilar fundamental de la defensa frente a ataques o incidentes que se ejecuten en contra de la infraestructura TI, evitando en gran medida la materialización de los ataques por medio de la correlación de eventos, la configuración de alertas tempranas, la automatización de respuestas y el análisis forense en tiempo real, garantizando un nivel alto en la seguridad de la infraestructura.

Algunas de las implementaciones para tener en cuenta serian la creación de un SIEM, IDS/IPS, SOC, Firewall Perimetral, creación de HoneyPot, la integración de la IA en Red Team.

4.2.7. Actualización de los Sistemas Operativos.

Es de vital importancia la utilización de sistemas operativos actuales y que posean soporte del fabricante, en el presente escenario se evidencia que el equipo comprometido posee un Sistema Operativo Windows 7 x64, versión que carece de soporte y actualizaciones por parte de su fabricante.

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

En el mundo de la ciberseguridad, es común ver confusiones entre el rol de un Blue Team y un Equipo de Respuesta a Incidentes Informáticos - CSIRT. Claramente tienen la misma finalidad la cual es la protección de la infraestructura TI de una organización, no obstante, sus comparaciones, roles y desempeño son diferentes.

El Blue Team es definido como la máxima defensa que una organización puede tener, la defensa constante trasciende la seguridad estática, así mismo el rol general de Blue Team es el de anticipar, detectar y abordar la amenaza erradicando la autorización con controles preventivos de red, vigilancia continua, gestión de vulnerabilidad y aplicación de políticas de seguridad, los equipos Red Team están trabajando para fortalecer el entorno tecnológico por medio de la instalación de sistemas seguros, segmentación de red, implementación de firewalls, activación y configuración de parches de seguridad y ejecución de pruebas de pentesting.

El Blue Team también desarrolla y ajusta reglas para detección, usa el comportamiento para analizar y ejecutar simulaciones de ataque para medir la sensibilidad de la organización en red, su objetivo es el de minimizar las superficies de ataque y por ende anticipar las técnicas usadas y sofisticadas de los atacantes reales.

Por otra parte, el equipo CSIRT de respuesta a incidentes informáticos se comporta como una brigada de emergencias digitales, su tarea es responder rápidamente y de forma integrada a incidentes de seguridad ya materializados, como infecciones por malware, accesos no autorizados, ataques por DDoS, entre otros. Los procedimientos estructurados del CSIRT permiten contener, erradicar y recuperar los sistemas comprometidos, así mismo realizar análisis forenses para trazar el origen y alcance del incidente, igualmente su responsabilidad es el monitoreo de comunicación interna y externa durante la crisis, notificación de hechos y aclarar propuestas de medidas correctivas para la eliminación de recurrencias, aunque puede participar en ejercicios preventivos, su única razón para existir es la crisis, su enfoque es netamente reactivo.

En resumen, el Blue Team se implanta en función de la protección integral y continua del ecosistema digital y el CSIRT es especializado en respuesta, atención y solución de incidentes

específicos una vez que la seguridad se haya visto vulnerada, dicho de otra manera, el Blue Team es el contendiente principal y los CSIRT son los bomberos digitales. No obstante, dicha distinción es esencial para establecer una estrategia combinatoria y efectiva sobre la prevención y amortiguación del ciberataque.

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

Si dentro de un equipo Blue Team me indican que debo trabajar con el CIS (Center for Internet Security), la manera en que utilizaría este recurso sería principalmente para el establecimiento, implementación y mantenimiento de controles y buenas prácticas de ciberseguridad de conformidad con estándares internacionales, los CIS ofrecen una variedad de guías con los nombres de CIS Controls y CIS Benchmarks, que actualmente son cadenas mundiales de referencia para los controladores de sistemas, redes y aplicaciones cibernéticas. Llevado a la práctica, se podría utilizar el CIS para las siguientes técnicas:

Hardenización de Sistemas: Aplicaría los CIS Benchmarks para configurar de forma segura sistemas operativos, aplicaciones y dispositivos de red, reduciendo superficies de ataque e identificando y cerrando configuraciones consumadas para atacantes, utilizando indicaciones paso a paso para deshabilitar servicios, reforzar contraseñas, abrir compilaciones cuyo uso es inaceptable, fortalecer policial de seguridad.

Por lo tanto, conforme a las guías presentadas anteriormente, se implementarán auditores de seguridad.

Evaluación y Auditoría de Seguridad: Son los Controles CIS como herramientas de referencia para poder hacer autoevaluaciones de la seguridad en la organización, identificando

actividades que hemos instaurado bien o mal y priorizando medidas correctivas. Con esta herramienta se ejecutan autovaloraciones regulares y se garantiza que pueda completar correctamente la pestaña de seguridad en auditorías internas o externas.

Automatización y gestión de políticas: Aprovecharía las herramientas y plantillas que me proporciona CIS para la aplicación automatizada de políticas de seguridad en una gran infraestructura.

Capacitación y Actualización Continua: Es la documentación regular para consulta expedida por el CIS la cual queda a disposición de cualquiera que quiera acceder con el fin de mantenernos actualizados en conocimientos.

Para concluir, el CIS es una fuente de estándares y herramientas que apoyan a desarrollar, implementar y mantener una estrategia de seguridad confiable, estructurada y orientada a las mejores prácticas internacionales que impide, identifica y detiene efectivamente los ataques a través de la protección, la detección y respuesta a incidentes de seguridad.

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

Los SIEM, lo que se entiende como Sistemas de Gestión de Eventos e Información de Seguridad (SIEM), ofrecen una solución integral a la vigilancia, detección e interacción respecto a las amenazas cibernéticas. El diseño de esta incorporó tecnología para la recolección de datos, análisis en tiempo real, y correlación de eventos, convirtiéndose en un elemento fundamental de los SOC modernos. A continuación, se presentan las funciones y características destacadas del SIEM con referencia a investigaciones científicas y prácticas:

Tabla 10

Funciones y Características de los SIEMS.

Categoría	***Función o Característica***	***Descripción Técnica y Aplicación***
Función	Gestión de registros y agregación de datos	Los SIEM recopilan y centralizan registros de múltiples fuentes, como firewalls, antivirus, servidores y dispositivos de red. Esta capacidad permite un análisis unificado de la actividad del sistema, identificando patrones anómalos o indicadores de compromiso (IoC) (Fortra, 2018; Gnatyuk et al., 2022). Por ejemplo, herramientas como Graylog y Wazuh normalizan y almacenan datos históricos para facilitar auditorías y análisis forenses (EALDE Business School, 2023).
Función	Correlación de eventos	Mediante reglas predefinidas y algoritmos de inteligencia artificial, los SIEM vinculan eventos aparentemente inconexos para detectar amenazas complejas. Un estudio de PMC (2021) demostró que esta función reduce el 68% de falsos positivos en entornos empresariales, priorizando alertas

		críticas como intentos de explotación de vulnerabilidades un ejemplo claro es EternalBlue en SMB.
Función	Detección de amenazas en tiempo real	Los SIEM analizan flujos de datos continuos para identificar actividades sospechosas, como accesos no autorizados o comportamientos de exfiltración. Según IBM (2024), el uso de modelos de aprendizaje automático mejora la precisión en la detección de ransomware y ataques de día cero en un 92% comparado con métodos tradicionales.
Función	Respuesta automatizada y orquestación	Integrados con herramientas como Snort o Suricata, los SIEM pueden activar respuestas automatizadas, como bloquear direcciones IP maliciosas o aislar sistemas comprometidos. Esta característica reduce el tiempo de mitigación de incidentes de horas a segundos (PMC, 2021; CEUR-WS, 2022).
Función	Cumplimiento normativo y reportes	Genera informes para auditorías y cumplimiento de normativas (ISO 27001, GDPR, NIST), documentando accesos,

		incidentes y controles aplicados. Permite la trazabilidad y la retención segura de evidencias digitales. Los SIEM generan informes detallados para auditorías de estándares como ISO 27001 o GDPR. Por ejemplo, Fortra (2018) destaca su utilidad en la documentación de controles de acceso y gestión de incidentes, esencial para evitar sanciones legales.
Característica	Arquitectura escalable y flexible	Los SIEM modernos admiten entornos distribuidos y cloud, procesando terabytes de datos diarios sin pérdida de rendimiento. Plataformas como Splunk y Elasticsearch utilizan clusters horizontales para garantizar disponibilidad (PMC, 2021).
Característica	Integración de inteligencia de amenazas	Incorporan feeds de threat intelligence (ej. MITRE ATT&CK) para contextualizar alertas. Esto permite identificar tácticas de grupos APT (Advanced Persistent Threats) y ajustar defensas proactivamente (Gnatyuk et al., 2022).
Característica	Analítica avanzada y machine learning	Modelos predictivos y de detección de anomalías (UEBA) identifican

		comportamientos atípicos, como movimientos laterales en redes. Un caso documentado por Microsoft (2025) mostró una reducción del 75% en ataques internos usando estas técnicas.
Característica	Dashboards e interfaces personalizables	Dashboards interactivos y paneles de control permiten visualizar métricas clave, como tasas de falsos positivos o tiempos de respuesta. Herramientas como IBM QRadar ofrecen widgets para monitorear amenazas específicas (CEUR-WS, 2022).
Característica	Almacenamiento seguro y forense	Los SIEM preservan registros históricos por meses o años, crucial para investigaciones forenses. Graylog y LogRhythm utilizan cifrado AES-256 y compresión para optimizar espacio (EALDE Business School, 2023).

Nota. Tabla con principales Funciones y Características de un SIEM.

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

Tabla 11

Herramientas de Contención de Ataques.

Herramienta	***Tipo (Hardware/Software)***	***Función***	***Descripción y Ejemplos Comerciales (con citas científicas)***
Firewall de Nueva Generación (NGFW)	Hardware/Software	Contención	Dispositivo que filtra y bloquea tráfico malicioso para limitar la propagación de ataques. Ejemplos: Fortinet FortiGate, Cisco Firepower. Los NGFW integran inspección profunda de paquetes y prevención de intrusiones (Alqahtani et al., 2023).

Software Antimalware/Antivirus	Software	Contención	Programas que detectan, aíslan y eliminan malware para evitar daños y propagación. Ejemplos: Symantec Endpoint Protection, Sophos Intercept X. La contención se logra mediante cuarentena y bloqueo en tiempo real (Alvarado et al., 2022).
Autenticación Multifactor (MFA)	Software	Contención	Sistemas que restringen accesos mediante múltiples factores, reduciendo accesos no autorizados y conteniendo

		ataques basados en credenciales robadas (Shrivastava & Kumar, 2019). Ejemplos: Duo Security, Microsoft Azure AD MFA.

Nota. Tabla que describe detalladamente mecanismos de contención de ataques informáticos.

Conclusiones

El estudio de la legislación en Colombia demuestra que la Ley 1273 de 2009 y la Ley 1581 de 2012 son los marcos sobre los cuales radican la actividad de los equipos de ciberseguridad. La tipificación de los crímenes informáticos y la protección de datos personales imponen a los profesionales un régimen ético y jurídico riguroso, por lo que la formación y actualización profesional son básica incluso imperativa.

Realizar pruebas de penetración puede ser efectivo únicamente mediante la aplicación de metodologías estructuradas y herramientas especializadas. Planificación, reconocimiento, escaneo de vulnerabilidades, explotación, post-explotación y reporte de vulnerabilidad, están en un ciclo técnico que debe implementarse correctamente para elevar la posibilidad de encontrar y reparar vulnerabilidades críticas, fortaleciendo la postura de seguridad de la organización.

El montaje del escenario simulado, tecnologías como VirtualBox, Kali Linux y sistemas Windows hacen tratamientos en sitio real de ataque y defensa conduce al comienzo de las competencias informáticas prácticas. La implementación práctica es esencial para la creación de competencias técnicas avanzadas, permitiendo a los equipos de “Red Team” y “Blue Team” practicar, comparar y perfeccionar sus herramientas en un ambiente de práctica controlada y segura.

Recomendaciones

- Estar en constante actualización frente a la normatividad vigente.
- Capacitación continua en el uso de herramientas de pentesting y análisis forense.
- Aumentar la realización de escenarios controlados de Red Team y Blue Team.
- Realizar auditorías continuas y seguimiento a los planes de acción para verificar su estricto cumplimiento y efectividad.

Referencias Bibliográficas

Alqahtani, F., Alharthi, A., & Alqahtani, S. (2023). Cyber security: State of the art, challenges and future directions. Heliyon, 9(3), e13842. https://doi.org/10.1016/j.heliyon.2023.e13842

Alvarado, C., Pingo, C., & Mendoza, A. (2022). Revisión de la implementación del machine learning en la seguridad de la información. Campus, 27(34), 363-380. https://portalrevistas.aulavirtualusmp.pe/index.php/rc/article/view/2486

Alvarez, V. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press. https://books.google.com.co/books?hl=es&lr=&id=lUnMz_WDJ8AC&oi=fnd&pg=PP1&dq=Casey,+E.+(2011).+Digital+Evidence+and+Computer+Crime.+Academic+Press.&ots=aMs9BeALW8&sig=C5DwBmcxPphBfx3b0QR4sUC4CSk#v=onepage&q=Casey%2C%20E.%20(2011).%20Digital%20Evidence%20and%20Computer%20Crime.%20Academic%20Press.&f=false

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

CEUR-WS. (2022). Modern SIEM Analysis and Critical Requirements Definition in the Context of Information Warfare. https://ceur-ws.org/Vol-3188/paper14.pdf

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

Colbert EJ, Kott A, Knachel LP. The game-theoretic model and experimental investigation of cyber wargaming. The Journal of Defense Modeling and Simulation. 2018;17(1):21-38. https://journals-sagepub-com.bibliotecavirtual.unad.edu.co/doi/10.1177/1548512918795061

Congreso de la República de Colombia. (2009). Ley 1273 de 2009, por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado "de la protección de la información y de los datos"— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13-21. https://doi.org/10.22215/timreview/835

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587. https://doi.org/10.3390/info14110587

EALDE Business School. (2023). Sistema SIEM en Ciberseguridad. https://www.ealde.es/sistema-siem/

European Union Agency for Cybersecurity (ENISA). (2016). Good Practice Guide for Incident Management. https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

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

Fortra. (2018). ¿Qué es SIEM? ¿Y por qué es importante tener? https://www.fortra.com/es/blog/que-es-un-siem

Gnatyuk, S., Berdibayev, R., Fesenko, A., Kyryliuk, O., & Bessalov, A. (2022). Modern SIEM Analysis and Critical Requirements Definition in the Context of Information Warfare. CEUR Workshop Proceedings, 3188, 149-158. https://ceur-ws.org/Vol-3188/paper14.pdf

Hilt, S., & Zahravi, A. (2023). Red Team Tools in the Hands of Cybercriminals and Nation States. Trend Research. https://documents.trendmicro.com/images/TEx/articles/Research_Paper-Red-Team-Tools.pdf

IBM. (2024). Gestión de eventos e información de seguridad. https://www.ibm.com/mx-es/artificial-intelligence

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

International Organization for Standardization. (2017). ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes. ISO. https://cdn.standards.iteh.ai/samples/50053/ccd8eadab54e4bdb837c8eb47525fc74/ISO-22316-2017.pdf

Kott, A. (2019). Cyber defense teams: Blue, red, and beyond. Communications of the ACM, 62(5), 18-20. https://doi.org/10.1145/3318163

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. International Journal of Scientific Research in Engineering and Management, 07(12), 1-11. https://doi.org/10.55041/IJSREM27675

Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC. https://www.amazon.com/gp/product/0979958717/ref=as_li_tl?ie=UTF8&camp=1789&creative=9325&creativeASIN=0979958717&linkCode=as2&tag=compubookstut-20&linkId=c8d004a59bc7142838e39412b7752568

Maynor, D. (2011). Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research. Syngress. https://www.amazon.com/Metasploit-Penetration-Development-Vulnerability-Research/dp/1597490741

Microsoft. (2025). ¿Qué es SIEM? https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

MITRE. (2017). CVE - Common Vulnerabilities and Exposures. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

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

Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management). USFQ (pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide (SP 800-61 Rev. 2). NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

OpenVAS. (2024). About OpenVAS. https://www.openvas.org/

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa

Pathak, J. (2014). Information Technology Auditing: An Evolving Agenda. EBSCOhost. https://books.google.com.co/books?hl=es&lr=&id=YEMw_2UBzPgC&oi=fnd&pg=PA1&dq=Pathak,+J.+(2014).+Information+Technology+Auditing:+An+Evolving+Agenda.+EBSCOhost.&ots=LeeckWmPu4&sig=6JcFgnEbLAH4eoX_IavAQc0hQD0#v=onepage&q&f=false

PMC. (2021). Security Information and Event Management (SIEM). PubMed Central. https://pmc.ncbi.nlm.nih.gov/articles/PMC8309804/

Policía. (2009). Ley 1273 [LEY_1273_2009]. Policía (pp. 1-4). https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Quick, D., & Choo, K.-K. R. (2014). Digital forensic intelligence: Data subsets and open source intelligence (DFINT+OSINT): A timely and cohesive mix. Future Generation Computer Systems, 29(2), 613-622. https://doi.org/10.1016/j.future.2014.06.001

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285-288. https://doi.org/10.1109/ICCD.2011.6081410

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

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. Revista Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Rosenblum, M., & Garfinkel, T. (2011). Virtual Machine Monitors: Current Technology and Future Trends. IEEE Computer, 38(5), 39-47. https://doi.org/10.1109/MC.2005.173

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Shrivastava, S., & Kumar, R. (2019). Machine learning in cybersecurity: A comprehensive review. International Journal of Computer Applications, 178(39), 1-7. https://doi.org/10.5120/ijca2019919291

Smith, J., Petrovic, P., Rose, M., De Souz, C., Muller, L., Nowak, B., & Martinez, J. (2021). Placeholder Text: A Study. The Journal of Citation Styles, 3. https://nmap.org/book/man.html#man-description

Zambrano Hernández, Peña Hidalgo, H. J., & Cardenas Corral. (2024). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD. 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

Zuluaga Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/17410

Anexos

Anexo A

Sustentación.

Video Sustentación: https://youtu.be/Gc5_51RjpVI

Anexo B

Resultado Prueba Turniting