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

Milton Alexander Hernandez Cepeda

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Primero, agradezco a Dios por darme la fortaleza, la paciencia y la sabiduría necesarias para culminar con éxito este proyecto, incluso en los momentos más difíciles.

A mis padres y a mi familia, por su apoyo incondicional, por enseñarme con su ejemplo el valor del esfuerzo, la honestidad y la perseverancia, y por recordarme siempre que cada meta alcanzada es fruto del trabajo constante.

A mis amigos, quienes, con su compañía, palabras de aliento y comprensión me brindaron energía y motivación en este camino académico.

A mis tutores y docentes, por compartir no solo su conocimiento, sino también su orientación y confianza, guiando cada paso de mi formación.

Dedico igualmente este esfuerzo a todos los profesionales de la ciberseguridad, guardianes del mundo digital, quienes día a día trabajan con entrega para salvaguardar lo que se ha convertido en uno de los bienes más preciados de la humanidad: la información. Su compromiso es inspiración y ejemplo para quienes buscamos aportar a este campo.

Este logro es el reflejo del acompañamiento, la confianza y el apoyo de todos ellos, y a cada uno les dedico con gratitud este trabajo.

Agradecimientos

Antes que todo quiero expresar mi más sincero agradecimiento a las personas que me apoyaron eh hicieron posible la finalización de este trabajo. Agradecer al tutor y director de curso Christian Hernán Obando Ibarra por su gentil ayuda técnica en la construcción de este documento y en todo el conocimiento y fueron fundamentales para de este humilde proyecto.

Agradezco inmensamente a mis instructores por las guías y el apoyo académico, que recibí. Las enseñanzas constantes de motivación eh inspiración. Principalmente al Tutor Eduvin Trigos Sanches por toda la orientación y siempre tener la disponibilidad de estar dispuesto a colaborar me en resolver todas las dudas presentadas, la paciencia y con sabiduría reforzaron el crecimiento profesional y académico.

Es importante agradecer a los materiales disponibles entregados y proporcionados por la (UNAD) Universidad Nacional Abierta y a Distancia, toda la infraestructura y recursos prestados por la universidad fueron de gran apoyo para la realización de esta investigación.

Resumen

Esta propuesta contempla varios desafíos que se evidencian en lo largo de este documento sobre la seguridad informática, estos son asociados en la adaptación que se debe asumir en los servicios de la infraestructura en los momentos que se genera un crecimiento y/o las necesidades de la organización, Esta transición ofrece demasiados beneficios, aunque trae muchos casos de estudio que se requiere tener diferentes planes de trabajo y estrategias en cuanto a protecciones, sobre la seguridad es vital y fundamental tener un gran equipo de trabajo que permita abordar temas importantes como el control de quién accede y los perfiles de acceso que debe tener cada funcionario y el cómo se maneja la data o información de cada uno de los servicios prestados por la organización que son vitales para el buen funcionamiento, garantizando el continuismo de la organización de la manera más segura, al proteger la privacidad y confidencialidad de toda la información que en esta infraestructura se albergan o se encuentran en espacios virtuales. En esta propuesta se busca fortalecer las diferentes capacidades del equipo de Red Team y Blue Team para lograr la identificación y el abordar de manera eficiente las diferentes vulnerabilidades en todas las infraestructuras. Es importante declarar que se debe tener correctamente los servicios configurados y aplicar las diferentes medidas de control de seguridad eficaces para lograr proteger la confidencialidad y integridad y de la información almacenada en los medios digitales.

Palabras clave: ataque, ciberseguridad, incidentes, seguridad, vulnerabilidad.

Abstract

This proposal addresses several challenges that are evident throughout this document regarding cybersecurity. These are associated with the adaptation that must be made to infrastructure services as growth and/or organizational needs change. All organizations, companies of all sizes, begin with challenges related to scalability, flexibility, and cost efficiency. This raises different concerns regarding information security and protection against various cyber threats. This transition offers many benefits. Although it brings many case studies that require different work plans and strategies regarding protection, it is vital and fundamental to have a great team to address important issues such as controlling access and the access profiles that each employee must have, as well as how the data or information of each of the services provided by the organization is managed. These are vital for its proper functioning, ensuring the continuity of the organization in the most secure manner by protecting the privacy and confidentiality of all information hosted on this infrastructure or in virtual spaces. This proposal seeks to strengthen the various capabilities of the Red Team and Blue Team to efficiently identify and address various vulnerabilities across all infrastructures. It is important to note that services must be properly configured and various effective security control measures applied to protect the confidentiality and integrity of information stored on digital media.

Keywords: attacks, cybersecurity, incidents, security, vulnerabilities.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Blue Team:

Es un grupo como su palabra lo dice Team, este encargado de toda la defensa y análisis para la protección de los sistemas informáticos. Su principal función es detectar, prevenir y responder a incidentes de seguridad.

Ciberseguridad:

control que se genera para la protección de sistemas, redes y programas contra diferentes ataques digitales. Incluyendo diferentes medidas de prevención para la protección de la integridad, confidencialidad y disponibilidad de toda la información.

Cumplimiento legal:

se adhiere a las regulaciones y normativas de protección de datos.

Configuración adecuada:

Son ajustes realizados previa miente analizados y apoyados por reglas adecuadas para evitar posibles filtraciones y accesos a personal no autorizado, puede ser en los firewalls perimetrales los cuales son los generadores de los permisos de acceso.

Cifrado de datos:

Es una técnica que permite convertir la información en un formato cifrado - ilegible para la confidencialidad.

Detección de anomalías:

Permite la identificación de anomalías o comportamientos inusuales sobre un sistema que pueden incurrir a amenazas.

IAM:

(Gestión de Identidad y Acceso): es el proceso de gestionar o permite delimitar el flujo de quién tiene acceso a los recursos de una organización. Incluyendo la autenticación de funcionarios y la asignación de permisos.

ISO:

(International Organization for Standardization), es la entidad que constantemente genera estándares internacionales regulando el asertividad para asegurar la calidad, seguridad y eficiencia de productos y/o servicios.

Monitoreo constante:

Supervisión 7x24 de actividades en para detectar y responder a posibles incidentes, detectando amenazas, utilizando herramientas de monitoreo desarrolladas para el análisis de registros y riesgos generados.

NIST:

(Instituto Nacional de Estándares y Tecnología): Es la Agencia del gobierno de los Estados Unidos que genera o desarrolla estándares y directrices para las tecnologías, incluyendo temas relacionados con la ciberseguridad.

OWASP:

(Proyecto de Seguridad de Aplicaciones Web Abiertas): Esta Organización proporciona diferentes guías y herramientas para mejorar los diferentes niveles de la seguridad.

Parches y actualizaciones:

Correcciones y desarrollo mejorados sobre los sistemas y software que permite corregir diferentes vulnerabilidades y con fin de la seguridad.

Red Team:

El grupo Red este encargado de simular diferentes ataques para la identificación de vulnerabilidades en los sistemas de la organización. Sus principales objetivos son la evaluación de la seguridad de los sistemas, planeaciones y estrategias mediante diferentes pruebas de penetración y técnicas ofensivas.

Vulnerabilidades:

estas son las debilidades de un sistema que generalmente pueden ser explotadas por atacantes. Estas pueden ser causadas por errores de configuración, fallas en el software, prácticas de seguridad inadecuadas.

Introducción

La rápida evaluación de los servicios y las eras tecnológicos han traído numerosos retos que toda compañía debe conocer y adaptar sus estructuras en pro de la seguridad evidenciando beneficios, como puede ser la escalabilidad, flexibilidad y la reducción de costos operativos. Pero también ha planteado desafíos enormes que llevan al equipo de seguridad al tener un rol muy importante para las organizaciones, para enfrentar riesgos relacionados con la protección de datos, la importancia que esto trae se desarrolló el Blue Team y el Red Team, sobre la detección de amenazas y control de amenazas.

Este trabajo se enfoca en gestión de la seguridad en las estructuras de la organización, se propone una estrategia directa y proactiva que permita la identificación y mitigación de vulnerabilidades por parte de Red Team y Blue Team. En estos dos grandes equipos de trabajo debe ser notable el fortalecimiento de la integridad, seguridad y confiabilidad en el cual debe simular ataques para la identificación de las posibles vulnerabilidades, para así defender y proteger las diferentes estructuras contra estas amenazas.

Durante el desarrollo de este documento, se consideró diferentes puntos de vista y enfoques que nos permiten desarrollar los desafíos de seguridad. Se realiza una revisión íntegra de documentos y noticias existentes, que permitió la obtención de una visión integral y actualizada de las prácticas estratégicas estudiando las vulnerabilidades al detalle. Se recopila información de entrevistas y/o encuestas a varios expertos en seguridad como a profesionales de TI para el reconocimiento de los mejores lineamientos prácticos sobre las amenazas presentes y soluciones puestas en marcha.

Objetivos

Objetivo General

Analizar estrategias orientadas al fortalecimiento de las competencias de los equipos de seguridad estratégica, Red Team y Blue Team, enfocadas en la identificación y gestión eficiente de vulnerabilidades en infraestructuras organizacionales, para la gestión eficiente de análisis de las vulnerabilidades basadas mejorando la capacidad de identificar, analizar y generar respuestas rápidas y eficientes frente a las amenazas que su puedan presentar.

Objetivos Específicos

Revisar los marcos legales y riegos éticos para las competencias requeridas por los equipos Red Team, Blue Team y de seguridad estratégica en la gestión de vulnerabilidades dentro de infraestructuras de la organización.

Revisar las Vulnerabilidades presentadas en los sistemas vulnerables con herramientas tecnológicas ampliamente documentadas para la detección, análisis y respuesta a amenazas.

Examinar estrategias proactivas implementadas en para fortalecer la capacidad de respuesta ante incidentes de seguridad, permitiendo la detección de pronta respuesta, eficientes para lograr mitigar los impactos, Generados.

Generar informe con buenas prácticas que orienten la coordinación efectiva entre equipos Red Team y Blue Team en la protección de los activos críticos.

Contenido de trabajo

Fundamentos de Operaciones Red Team y Blue Team

En la siguiente Etapa conoceremos los criterios éticos y Legales sobre el marco legal Sobre una organización Frente al Equipo Red Team y Blue Team acciones

Margen Legal en Colombia

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales se quiere conocer que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

En Colombia, el marco legal que abarca los temas de delitos informáticos y de protección de datos personales en los últimos tiempos ha evolucionado por estar en la actualización y estar en los desafíos del entorno digital. La Ley 1273 de 2009 que representa una unión al modificar el Código Penal e incluir el Título VII BIS, el cual protege la información y los datos como nuevos bienes jurídicos. Esta Ley tipifica muchos delitos como el acceso abusivo de los sistemas informáticos, de igual manera genera una interceptación de datos como el daño informático y el uso de software mal intencionado. Adicionalmente, contempla diferentes sanciones penales que pueden llevar prisión hasta diferentes multas, todo depende de la gravedad que el delito sea consagrado, permitiendo a ser crimina torio las conductas que se puedan comprometer en la seguridad digital. (Abiri, G. 2025).

En la protección penal, de la Ley 1581 de 2012 el cual habla sobre el régimen general de la protección de datos personales. Esta norma se diseñó para garantía de los derechos de los ciudadanos sobre su información, también así mismo como conocer, actualizar, rectificar y suprimir sus datos. Adicionalmente introduce principios rectores como la legalidad, finalidad, libertad, seguridad y transparencia, el cual se debe guiar el tratamiento de datos por parte de

entidades privadas y públicas. La Superintendencia de Industria y Comercio (SIC) actúa como autoridad de control, con facultades para imponer sanciones administrativas en caso de incumplimiento.

Ahora El Decreto 1377 de 2013 reglamenta diferentes aspectos basados en la Ley 1581, se basa especialmente en todos los datos relacionados con información recolectadas. Este decreto explica los mecanismos para la obtención y la autorización de los titulares, reforzando las obligaciones de implementación de políticas de tratamiento de datos. Ahora la Ley 1266 de 2008 esta regula el manejo de información financiera y crediticia, también conocida como habeas data financiero, establece derechos sobre la veracidad y actualización de los datos reportados a las centrales de riesgo.

Finalmente, normas complementarias como la Ley 1621 de 2013, que regula las actividades de inteligencia y contrainteligencia del Estado, y la Ley 1486 de 2011, orientada a la protección de los datos de menores en entornos digitales, esto permite fortalecer el ecosistema normativo colombiano. Estas leyes buscan que sea equilibrada la seguridad nacional teniendo en cuenta la evolución de las tecnologías, generando leyes que permitan la protección de los derechos fundamentales, que puedan promover la educación digital y la cooperación interinstitucional para prevenir delitos informáticos. (Espinosa Garrido, C. B. 2022)

En conclusión, existen un conjunto de normatividad y leyes que están a disposiciones de un marco robusto que responde a las exigencias de la era digital, Aunque el medio o las aplicaciones de estas leyes sigue siendo un reto constante.

Con base a lo anterior realizo una tabla donde están reflejado el Marco Legal Colombiano sobre Delitos Informáticos y Protección de Datos Personales.

Tabla 1

Características Principales y Artículos

Ley / Decreto	Características Principales / artículos
Ley 1273 de 2009 – Protección de la Información y los Datos	- Creación del Título VII BIS en el Código Penal: "De la protección de la información y de los datos". - Acceso abusivo a sistemas informáticos (Art. 269A) - Obstaculización ilegítima de sistemas o redes (Art. 269B) - Intercepción de datos informáticos (Art. 269C) - Daño informático (Art. 269D) - Uso de software malicioso (Art. 269E) - Violación de datos personales (Art. 269F) - Suplantación de identidad (Art. 269H)
Ley 1581 de 2012 – Protección de Datos Personales	Legalidad, finalidad, libertad, veracidad, seguridad, transparencia, acceso y circulación restringida. - Derechos de los titulares: - Conocer, actualizar, rectificar, suprimir datos y revocar la autorización. - Responsables del tratamiento: - Deben implementar políticas de privacidad y responder ante la Superintendencia de Industria y Comercio (SIC).
Decreto 1377 de 2013 – Reglamentación de la Ley 1581	Establece mecanismos para obtener autorización de los titulares de datos recolectados previamente. - Define procedimientos para la actualización, rectificación y supresión de datos. - Refuerza la obligación de implementar políticas de tratamiento de datos.
Ley 1266 de 2008 – Habeas Data Financiero	Aplica a entidades que reportan y consultan información financiera. - Establece derechos de los titulares sobre la veracidad y actualización de sus datos. - Define tiempos de permanencia de la información negativa en centrales de riesgo.
Ley 1621 de 2013 – Inteligencia y Contrainteligencia	- Establece límites al uso de información recolectada por organismos de seguridad. - Prohíbe el uso de datos personales para fines distintos a los autorizados por ley. - Requiere autorización judicial para ciertas actividades de vigilancia.
Ley 1486 de 2011 – Protección de Menores en Internet	-Promueve campañas educativas sobre seguridad digital. - Establece medidas para prevenir el acceso de menores a contenidos inapropiados. - Refuerza la cooperación entre autoridades para investigar delitos contra menores en entornos digitales.

Nota. Esta Tabla Muestra el Marco legal de Delitos Informáticos.

Que es y Cuales son las Etapas del Pentesting

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.

Que es El penetration testing o pentesting es conocida como una técnica de ciberseguridad que permite simular diferentes ataques reales contra los sistemas, redes o aplicaciones, principal objetivo de descubrir las diferentes vulnerabilidades que pueden encontrar sen en todo el entorno empresarial, esta técnica permite localizar diferentes vulnerabilidades antes de que lo hagan los verdaderos actores maliciosos. Podemos decir que son diferentes herramientas, que nos permite evaluar la seguridad de nuestra organización, Permitiendo validar la efectividad de los controles defensivos y aplicando nuevas técnicas de defensa.

Las diferentes etapas de Pentesting son 7 las cuales se diferenciarán en la siguiente tabla, es importante declarar que las más conocidas y la metodología más estructurada. (Palutla, D. V 2025)

Tabla 2

Etapas de Pentesting

Etapa	Detalle
Planificación y Alcance	El objetivo de la prueba es definir el alcance (sistemas, redes, aplicaciones), o algun activo a evaluar (ip, dominios etc .) las reglas de compromiso como horarios y las limitaciones legales y técnicas, también se debe establecer los canales de comunicación y que criterios de éxito de las pruebas, Importante se debe evitar daños irreversibles o colaterales
Reconocimiento	- Se debe detallar el objetivo utilizando es decir las técnicas pasivas (OSINT, WHOIS, DNS, etc.) y activas (escaneo de puertos, fingerprinting), con esto se busca detallar un Mapa preliminar se debe recopilar información del medio atacante.
Escaneo y Enumeración	Esto nos permitirá validar los diferentes y posibles puntos débiles de la organización mediante herramientas como Nmap, Nessus o Nikto para hallar en los servicios, sistemas operativos, versiones entre otras las diferentes vulnerabilidades de ataque, aquí se debe llevar un listado que nos permita seleccionar los servicios vulnerables, como un servicio etc.
Explotación	Después de Lograr encontrar vulnerabilidades descubiertas se intentará explotar para obtener acceso no autorizado o escalar los privilegios de acceso, con diferentes técnicas ofensivas controladas, como vulnerabilidades de SQL, se puede lograr hacer inyecciones SQL, XSS, (Metasploit, ExploitDB) o desarrollo de exploits para la explotación del servicio, etc.
Post-Explotación	Se debe analizar cada impacto de los accesos obtenidos, validando la persistencia, movimiento lateral, extracción de datos, etc, así mismo se evaluará hasta qué punto un atacante podría comprometer un sistema.
Análisis y Reporte	Se debe generar informes o documentar los hallazgos, con el fin de clasificar las vulnerabilidades por nivel de criticidad eh impacto, para generar medidas de mitigación, este informe debe ser técnico, claro y comprendido para los responsables de seguridad y la gerencia.
Remediación y Validación	Se generarán las correcciones sugeridas y se debe realizar validaciones de verificación que indique que las vulnerabilidades han sido correctamente mitigadas.

Nota. Esta Tabla Muestra las características de las Etapas de Pentesting con su respectiva descripción de lo que se debe realizar en cada Etapa.

Herramientas que son de Vital Importancia

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 con el fin de generar una acción de seguridad en nuestra Organización. (Vera Mundaca 2023)

Tabla 3

Herramientas más Conocidas eh Importantes

Herramientas	¿Qué Es**?**	características
Metasploit:	es un framework de código abierto está diseñado para realizar pruebas de penetración, se pueden generar y desarrollar exploits que permitirá las validaciones de las vulnerabilidades en infraestructuras.	Tiene un sin número de exploits diseñados y listos para usar. Puede Permitir crear payloads personalizados (reverse shell, meterpreter). Una de adicional característica es soportar automatizaciones de ataques y scripting. Su desarrollo permite la integración con herramientas como Nmap, Nessus y Burp Suite.
Nmap:	es una herramienta muy conocida de escaneo de redes que nos permite descubrir hosts, puertos abiertos, servicios activos y configuraciones vulnerables	Permite el Escaneo TCP/UDP, y el detalle de de sistema operativos y servicios. Soporta scripts avanzados como NSE. Utilizado en reconocimiento y enumeración. Funciona en CLI y GUI (Zenmap). Este escaneo es un poco más rápido y personalizable.
OpenVas:	Es un escáner que permite buscar fallos de seguridad, vulnerabilidades de código abierto, analiza sistemas, redes y aplicaciones.	Esta Herramienta detecta vulnerabilidades conocidas basadas en CVE. Tiene una característica adicional que puede generar informes a un buen detalle asumiendo una clasificación de riesgos. Tiene un buen respaldo ya que cuenta con actualizaciones constantemente al no ser FREE También se conoce alternativas gratuitas a Nessus (Teanable)
Servicios en línea:	Son comúnmente conocidas como Pentesting as a Service (PTaaS) y estas son plataformas que ofrecen	Por ser web tiene accesos remotos a escáneres y simuladores de ataques, hay platafomas que ya vienen para ser integradas con CI/CD y DevSecOps., algo que adicionar es que puede

Herramientas	¿Qué Es**?**	características
	pruebas de penetración bajo demanda, de forma continua o automatizada.	generar informes en tiempo real y sus características interactivas, son más fáciles de recorrer, cuenta con una escalabilidad y cobertura global, se puede usar en infraestructura híbridas o en la nube
ExploitDB:	Es una base de datos pública que recopila información de exploits que han sido probados y son funcionales, proof-of-concepts (PoC) adicionalmente cuenta cun informes técnicos sobre vulnerabilidades conocidas	Es una distribución de Offensive Security, esta incluye exploits locales, remotos, web y shellcodes, se puede integrar con otras herramientas como SearchSploit de Kali Linux. Generalmente es una Fuente clave para investigadores y pentesters, cuenta con actualizaciones constantemente por la comunidad.
CVE:	Es un sistema de identificación estandarizado que permite identificar las versiones de las aplicaciones de vulnerabilidades públicas, como MITRE Corporation	Aquí podemos analizar que cada vulnerabilidad recibe un ID único conocido como CVE-2025-12345, esto Facilita la comunicación entre diferentes expertos que brindan soluciones adicionando que los mismos fabricantes generan actualizaciones para solventar las vulnerabilidades. Es muy comúnmente usado como referencia en escáneres, informes y parches.

Nota. Esta Tabla Muestra las características más comunes de estas mismas.

Banco De Trabajo Herramientas que son de Vital Importancia

Reconocimiento del “banco de trabajo” Sobre el Escenario 1 el cual trabajaremos las actividades solicitadas

Paso A: Descarga de Herramienta

Se realiza la descargar de la Herramienta de Virtualización “VirtualBox” en la última versión.

Figura 1

Descarga de Virtual Box

Nota. La Figura Muestra la evidencia de la descarga de la herramienta

Paso B: Descarga de Material de Trabajo

Una vez se realice apertura del foro se ingresa al enlace: RedTeam&BlueTeam2025, el cual contiene el material requerido para el montaje del banco de trabajo, En las imágenes. OVA existe: Un sistema operativo Windows y un sistema operativo Kali Linux.

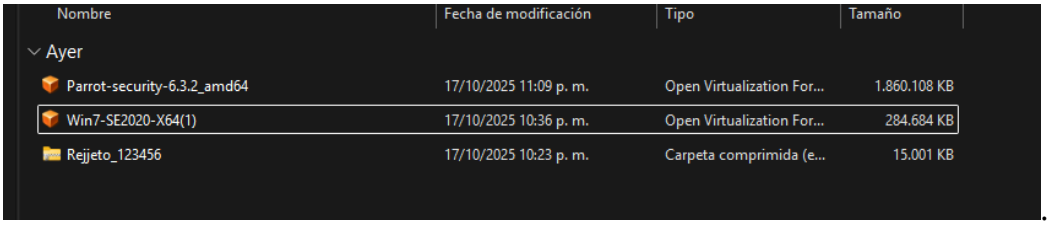
Figura 2

Validaciones del Material Para Descargar Desde la Web

Nota. se valida las características del material necesario para realizar la actividad y el detalle como son el peso de cada uno de este mismo.

Figura 3

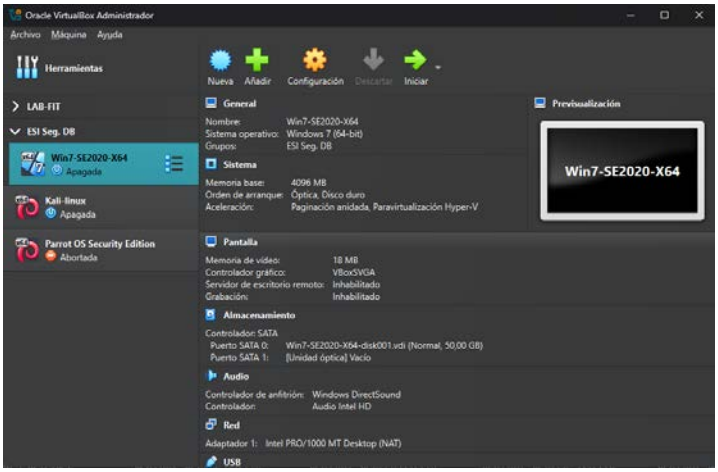
Descarga de Material



Nota. se realiza la descarga solicitada y validaciones de cada uno de los archivos necesarios.

Figura 4

Maquinas Ancladas a VirtualBox



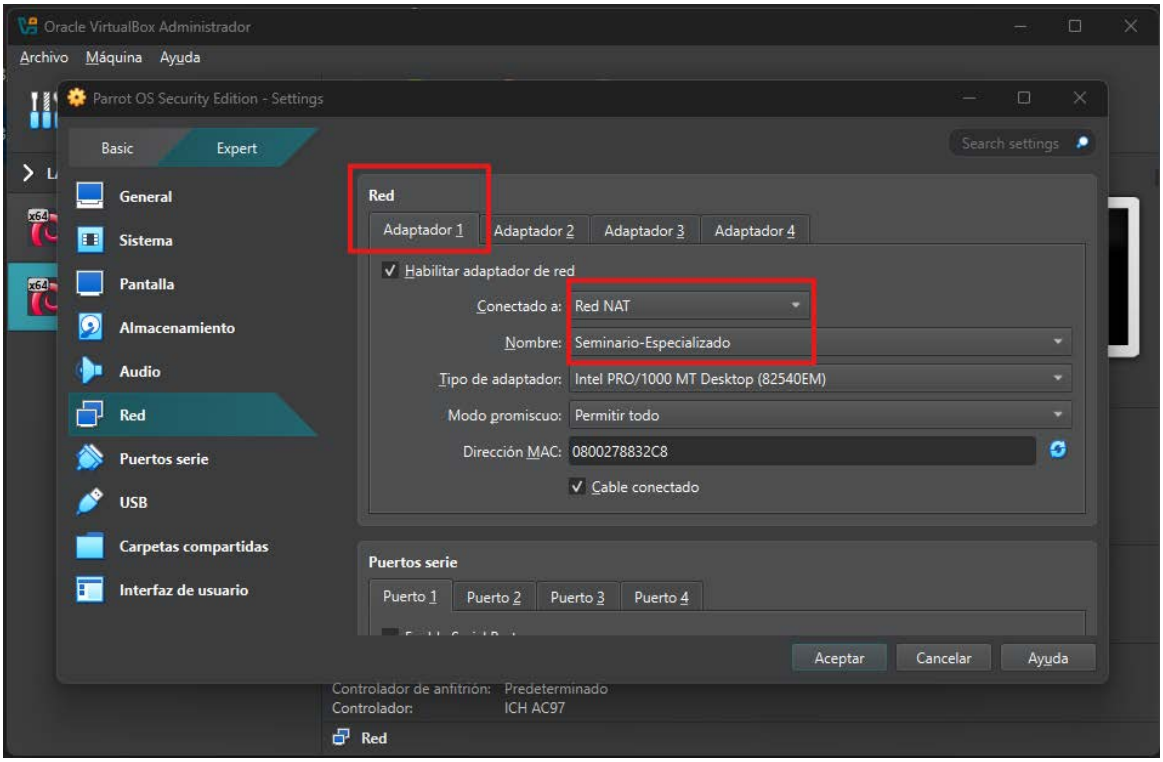
Nota. se exportan el punto ova y se realiza las configuraciones por defecto

Paso C: Validación de Comunicación

Para realizar la validación de la comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, se realiza unas configuraciones para generar un ambiente seguro y controlado para esto se crea una nueva tarjeta de red llamada Seminario Especializado,

Figura 5

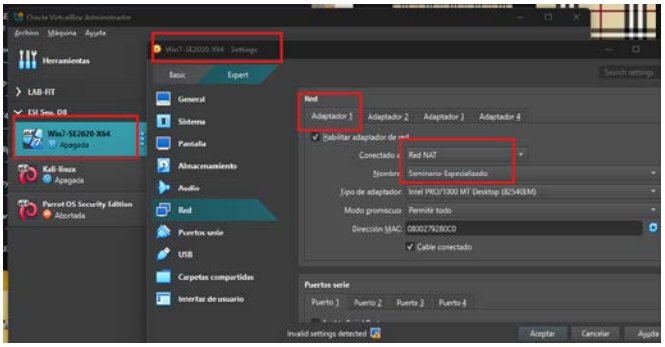
Configuración de Adaptadores de Red Parrot



Nota. Para generar un ambiente controlado, se realiza la configuración de cada una de las tarjetas de red de los equipos a trabajar.

Figura 6

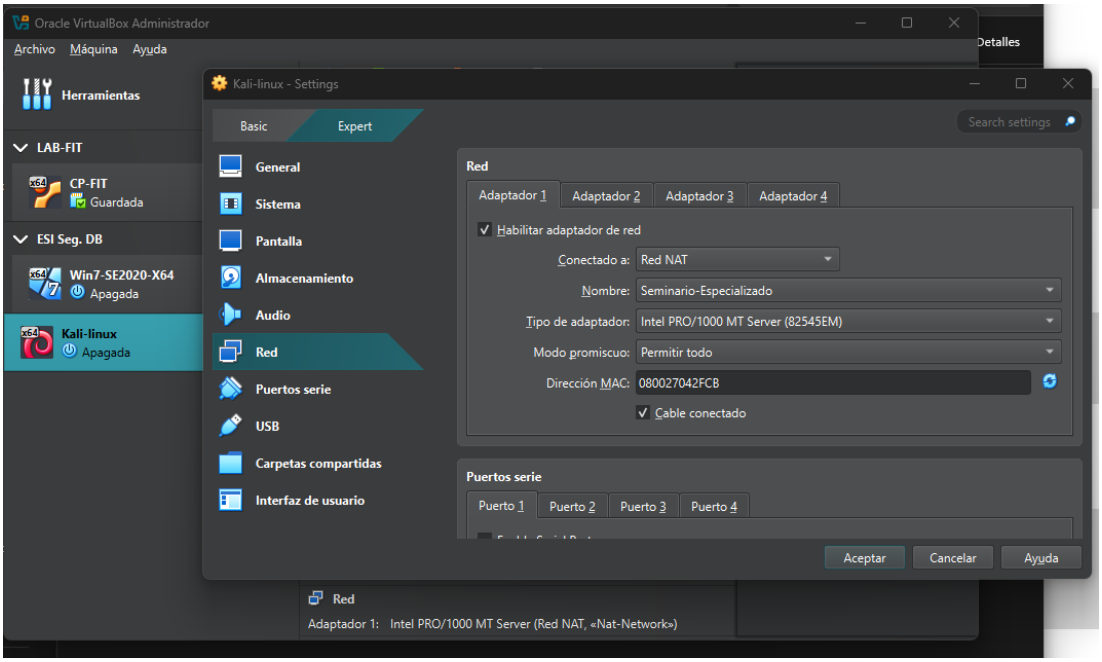
Configuraciones de Adaptadores de Red de Windows 7



Nota. se realiza la configuración de la tarjeta de red de Windows 7

Figura 7

Configuraciones de Tarjeta de Red de Kali Linux



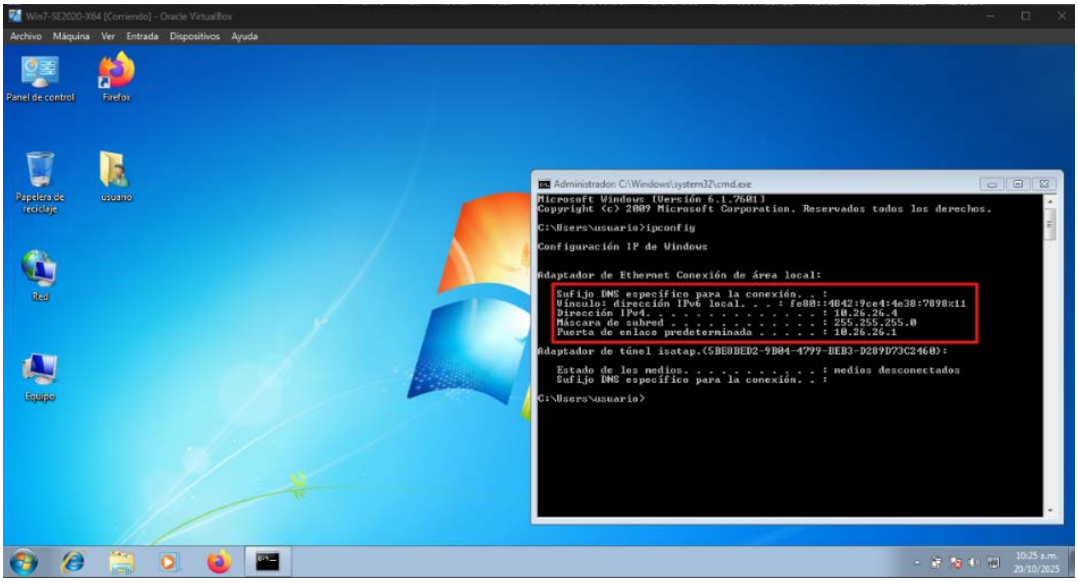
Nota. se realiza la configuración de la tarjeta de red de Kali-Linux

Paso D: Montaje de Banco de Trabajo

Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Figura 8

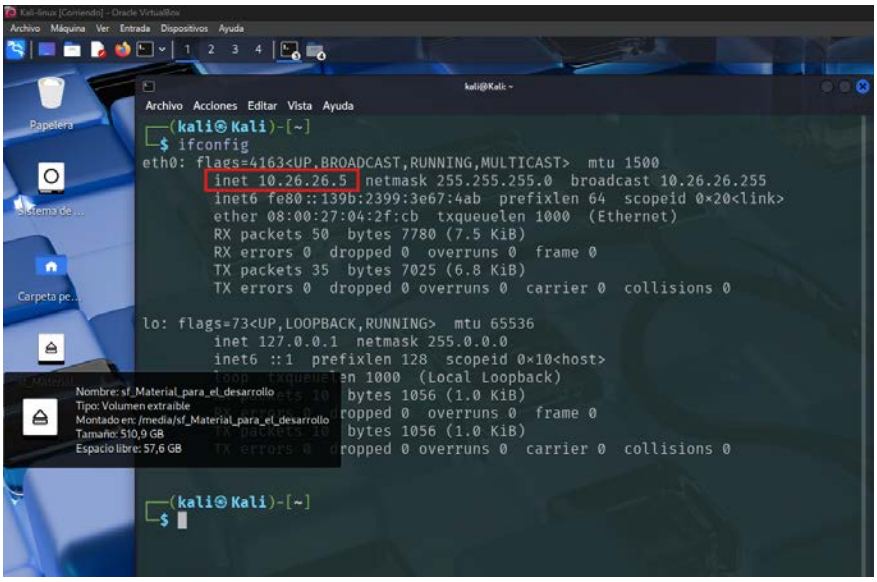
Direccionamiento Ip en Windows 7



Nota. se realiza las validaciones de direccionamiento Ip de la Maquina de Windows 7

Figura 9

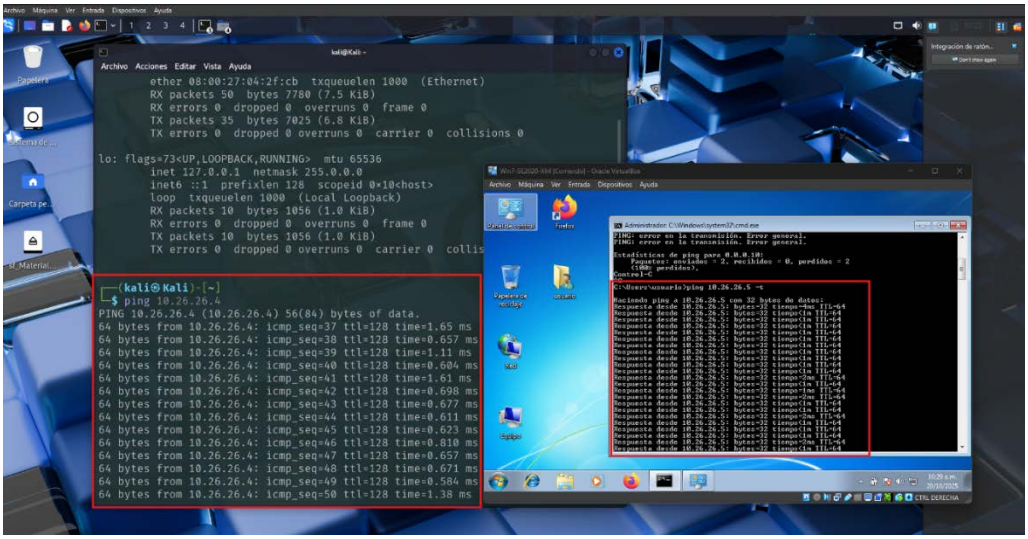
Direccionamiento de Ip en Kali-Linux



Nota. se realiza las validaciones de direccionamiento Ip de la Maquina de Kali-Linux

Figura 10

Evidencias de Conectividad entre Maquinas



Nota. se realiza las verifica conectividad entre máquinas Virtuales.

Ética Profesional y Marco Normativo en Operaciones de Seguridad

En la siguiente Etapa conoceremos los criterios éticos y Legales sobre el marco legal Sobre una organización Frente al Equipo Red Team y Blue Team acciones

En Colombia, el marco legal que abarca los temas de delitos informáticos y de protección de datos personales en los últimos tiempos ha evolucionado por estar en la actualización y estar en los desafíos del entorno digital. La Ley 1273 de 2009 que representa una unión al modificar el Código Penal e incluir el Título VII BIS, el cual protege la información y los datos como nuevos bienes jurídicos. Esta Ley tipifica muchos delitos como el acceso abusivo de los sistemas informáticos, de igual manera genera una interceptación de datos como el daño informático y el uso de software mal intencionado. Adicionalmente, contempla diferentes sanciones penales que pueden llevar prisión hasta diferentes multas, todo depende de la gravedad que el delito sea consagrado, permitiendo a ser crimina torio las conductas que se puedan comprometer en la seguridad digital. (Waseem 2025)

Tabla 4

Ley 1273 de 2009

Ley / Decreto	Características Principales / artículos
Ley 1273 de 2009 – Protección de la Información y los Datos	- Creación del Título VII BIS en el Código Penal: “De la protección de la información y de los datos”. - Acceso abusivo a sistemas informáticos (Art. 269A) - Obstaculización ilegítima de sistemas o redes (Art. 269B) - Intercepción de datos informáticos (Art. 269C) - Daño informático (Art. 269D) - Uso de software malicioso (Art. 269E) - Violación de datos personales (Art. 269F) - Suplantación de identidad (Art. 269H)

Nota. Esta Tabla Muestra Ley 1273 de 2009.

Margen Legal y Etico en Colombia

Se realiza lectura de los anexos y se orden las preguntas orientadoras:

Análisis del Anexo.

¿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.

* Teniendo en cuenta el contrato o el Anexo 3 – Acuerdo, se entiende que en la Clausula Primera. Objetivo: ***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 SecureNova Labs no podrán ser divulgados***. Se puede entender esta cláusula como una prohibición de divulgaciones a la no comunicación incluso autoridades legales, entraría como en contradicción con lo ético ya que se puede pensar que son instrucciones que impiden la denuncia de hechos delictivos que se puedan generar en esta Organización.

* Teniendo en cuenta el contrato o el Anexo 3 – Acuerdo, se entiende que en la cláusula segunda en el numeral 2 indica: ***Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"***. Se interpreta que al tener conocimiento que la información obtenida por medio ilegales o ilícitas como "***datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos*** confunde la conducta ética profesional, a una conducta delictiva, debido a que ordena a la protección de

material o frutos de conductas ilícitas con lo deberes de la integridad profesional, se debe tener en cuenta que todo material obtenido debe ser por medio de conductas legales. (Yalçın 2025)

* Teniendo en cuenta el contrato o el Anexo 3 – Acuerdo, se entiende que en la cláusula cuarta seguido del punto 3. Indica: ***No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.*** Se puede entender este hecho que Aparentemente esta Prohibido denunciar delitos, en esta cláusula se puede entender que como receptor esta prohibido denunciar actividades ilícitas, estoy puede generar controversia en normas públicas y deberes legales en la colaboración con autoridades y puede generarse protección de intereses públicos. (N.d.-a 2025)

* Teniendo en cuenta el contrato o el Anexo 3 – Acuerdo, se entiende que en la cláusula cuarta seguido el numeral 4. Indica: ***Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.*** En esta cláusula se Prohíbe al receptor las denuncias a las informaciones que se puedan considerar ilegales, esto implica que a pesar de las conductas o información entregada o recolectada por técnicas ilegales, no se debe informar ni denunciar, esto no debe ser un hecho de prohibición aclarando que el código profesional no puede a poyar hechos delictivos ni evitar la actuaciones de autoridades competentes.

* Teniendo en cuenta el contrato o el Anexo 3 – Acuerdo, se entiende que en la cláusula cuarta seguido el numeral 8, indica: ***Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.*** Genera una condición de responsabilidad frente a las entidades o autoridades penales, ya que puede generar se culpabilidad por recepción de material ilícito, esto genera un riesgo Penal (Juridicos) y riesgos Disciplinarios.

* Teniendo en cuenta el contrato o el Anexo 3 – Acuerdo, se evidencia en la Octava (Solucion de Controversias) en cual indica que frase: ***En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs,*** Fuente: Anexo 3 – Acuerdo, De acuerdo a este texto podemos interpretar que es un Riesgo de Coacción, debido a que exige que debe acudir a un abogado Privado se puede creer que es una cláusula abusiva y que el contratante se está exonerando de las responsabilidades penales, que traen consigo por la recepción de cualquier información ilegal o recibida por parte del contratante. (N.d.-a 2025)

Justificación de Respuesta

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.

Teniendo en cuenta el análisis anterior por diferentes párrafos y cláusulas de Dicho contrato y basados en los Artículos de la ley del 1273 se pueden versen vulnerados son los siguientes:

Tabla 5

Artículos de la Ley 1273

Artículo de la Ley 1273	Definición:
Artículo 269A — Acceso abusivo a un sistema informático	Según la redacción del documento Por contener expresiones que protegen o normalizan “accesos abusivos a sistemas informáticos”, el acuerdo puede facilitar la posesión, uso o encubrimiento de información obtenida mediante acceso no autorizado
Artículo 269B — Daño informático	Si la información protegida incluye material obtenido tras acciones que alteren, dañen o afecten la disponibilidad o funcionamiento de sistemas, el acuerdo puede amparar efectos vinculados a los supuestos sancionados por el artículo (delitos contra la integridad y disponibilidad de sistemas).
Artículo 269C — Interceptación ilícita de comunicaciones	La expresión de “interceptación de información” o “datos de chuzadas” en la definición de información confidencial puede dar soporte contractual a la posesión y tratamiento de comunicaciones interceptadas, conducta sancionada por el artículo 269C
Artículo 269D (y siguientes) — Otros atentados contra la confidencialidad, integridad y disponibilidad de datos y sistemas	Las guardas contractuales que protejan o impidan denunciar información derivada de prácticas como interceptaciones o accesos abusivos pueden entrar en conflicto con normas que tipifican distintas conductas informáticas ilícitas y sus modalidades, previstas en los numerales sucesivos del Título agregado por la Ley 1273.

Nota. texto consolidado de la Ley 1273 de 2009 (adición al Código Penal)

Usted Aplicaría a Este Trabajo

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, usted como experto en ciberseguridad aplicaría a este trabajo en SecureNova Labs, ¿dónde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

No aplicaría a este acuerdo – Contrato: de acuerdo con lo anteriormente escrito y mencionado debo aclarar que este contrato o acuerdo contractual no es una garantía de mis labores como profesional de ingeniería, debido a que impide mi correcto desarrollo profesional y ético, generando obstrucción a las investigaciones que se pueden presentar o den a lugar a delitos o denuncias informáticas.

En cuanto a mis labores, se observa diferentes irregularidades, como el acceso abusivo a sistemas informáticos, se obliga a tener colaboraciones de encubrimiento de información obtenida ilícita o actos como (Chuzadas) que no son cubiertas por la ética ni la Moral, adicionalmente se ven reflejadas las responsabilidades Judiciales y penales que la organización me tipifica por colaborar por las malas conductas de delitos informáticos, que la organización esta permitiendo en sus labores profesionales. (N.d.-b 2025)

Cumplimiento de la Ley. Todo ingeniero debe actuar conforme a la normativa vigente y ser cómplice ni participar en actividades ilícitas; La ética exige que se debe denunciar o colaborar cuando existan indicios de delito.

El Deber de la Protección de Interés Públicos. la seguridad, la salud y el medio ambiente deben prevalecer sobre intereses privados; Las decisiones técnicas en una Organización deben priorizar estos valores.

Integridad y Transparencia. El rechazo de las malas prácticas que impliquen encubrimiento, fraudes o manipulaciones de toda información; está en la obligación de reportar estas malas prácticas y las irregularidades que no legitimen conductas ilegales.

La Confidencialidad con Límites Legales. se debe proteger la información sensible, pero sin olvidar que no cuando la protección implique encubrir delitos o impedir la colaboración y/o participación con las autoridades; es de vital importancia que la confidencialidad sea condicionada a deberes superiores de legalidad y protección de terceros.

La Competencia y Diligencia. Indica que la obligación es desempeñar tareas dentro del ámbito técnico propio, con las actualizaciones permanentes y con el debido diligenciamiento profesional, en todos los deberes de la organización.

La Responsabilidad Profesional y Racionabilidad. incumplimientos éticos pueden dar lugar a sanciones disciplinarias por el organismo competente; el profesional debe estar consciente de consecuencias por obstruir investigaciones o participar en prácticas ilícitas.

Cualquier cláusula contractual que pretenda la prohibición o denunciar delitos o proteger material obtenido por medios ilícitos entra inmediatamente en conflicto directo con la argumentación del Código: Es decir que vulnera la obligación de legalidad, el deber de protección de interés público y la limitación de la confidencialidad frente a deberes legales. (N.d.-d 2025)

Análisis de Caso Problema

Deberá analizar el caso problema “Ciber espionaje y Ética en SecureNova Labs” (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:

A. ¿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?

Teniendo en cuenta la Ética profesional y la ley 1273 del 2009 se debe tener en cuenta que, aunque en el contrato o las cláusulas estén

El Código profesional respalda que se debe priorizar la denuncia y colaborar con las autoridades, cuando se legitime una protección contractual encubrimiento riesgos para terceros; las cláusulas contractuales no pueden eximir de esos deberes.

Supongamos que se nosotros como profesionales en la materia generamos alguna actividad ilícita o conocemos de malos procedimientos realizados por la organización y no decimos nada.

Este tipo de actividades aparte de ser unas infracciones con las leyes, el código ético trae consigo varios sansones penales y sansonatorias como son

Amonestación Escrita. Por faltas leves que no comprometan la seguridad pública ni la legalidad.

Suspensión Temporal de la Matrícula Profesional. Si se demuestra participación en actos contrarios a la ley, como encubrimiento de delitos informáticos, falsificación de documentos técnicos, o violación de normas de seguridad, será suspendida la matricula profesional por algun periodo como castigo

Cancelación Definitiva de la Matrícula Profesional. En casos graves, como complicidad en delitos que afecten la vida, el medio ambiente, la seguridad informática o el interés público.

Inhabilitación para Ejercer la Profesión. Cuando el profesional ha sido condenado penalmente por delitos relacionados con el ejercicio de la ingeniería. Estas sanciones se aplican tras un proceso disciplinario ante el Tribunal de Ética Profesional del COPNIA.

Las Sanciones según la Ley 1273 de 2009 (Delitos Informáticos)

La Ley 1273 adicionó al Código Penal colombiano el Título VII BIS, que protege la información y los datos. Las sanciones penales incluyen:

Tabla 6

Características Principales y Artículos

Delitos informáticos	Articulo	Sanciones penales.
Acceso abusivo a sistemas	269 A	48 A 96 Meses en prisión + una multa de 100 a 1.000 SMMLV
Interceptación ilícita de comunicaciones	269 C	48 A 96 Meses en prisión + una multa
Daño informático	269 B	16 A 72 Meses en prisión + una multa
Uso de software malicioso	269 E	48 A 96 Meses en prisión + una multa
Violación de datos personales	269 F	48 A 96 Meses en prisión + una multa
Suplantación de sitios web	269 G	48 A 96 Meses en prisión + una multa

Nota. texto consolidado de la Ley 1273 de 2009 (adición al Código Penal)

La complicidad o encubrimiento también puede ser castigado penalmente si el Profesional facilita, oculta o se beneficia de alguna de estas malas conductas.

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

Para evitar los usos indebidos de herramientas avanzadas las empresas de ciberseguridad deben implementar o tener buenos procedimientos robustos que permitan la supervisión, control que permita generar una cultura ética y conciencia Profesional, con el fin de generar estructuras con buenas prácticas internacionales y principios éticos profesionales. (Gao, X 2025)

Debe Contar con Controles Técnicos y de Acceso. Se debe tener una línea de defensa, asegurada en el cual cada empleado solo pueda acceder a las funciones y datos estrictamente necesarios para su rol. Teniendo en cuenta las herramientas de forenses deben estar protegidas por autenticación multifactor y monitoreo continuo, con registros detallados en cada acción realizada. Adicionalmente, se deben establecer alertas automáticas ante comportamientos anómalos, como por ejemplo accesos fuera de horario o consultas a información no asignada. Considerando que estas medidas permiten detectar y prevenir el uso indebido antes de que se materialice.

Políticas Internas Claras y Vinculantes. Toda empresa de ciberseguridad debe tener políticas formales y avaladas por la organización con el fin de regular el uso de herramientas forenses. Estas deben aclarar y definir las prácticas permitidas, así mismo dar indicaciones de las prohibiciones y consecuencias acarrea su incumplimiento. Para este uso es fundamental que toda solicitud debe estar respaldado por un requerimiento formal, con trazabilidad y autorización. Los contratos laborales y acuerdos de confidencialidad deben mantener cláusulas específicas adicionando la ética profesional y digital, agregando el uso legítimo de herramientas y sanciones por abuso. Esto generara un marco normativo interno que refuerza la responsabilidad individual.

Supervisión Ética y Legal. Más allá de los controles técnicos, es importante establecer mecanismos de supervisión que ayuden a la evaluación y el comportamiento ético de los profesionales. Se debe generar comités de ética tecnológica o de cumplimiento, esto serviría para revisar casos sensibles, como validar solicitudes de análisis y resolver dilemas éticos. Se debe generar auditorías internas periódicas las cuales permiten verificar los protocolos que se cumplan y que se eviten cualquier desviación. Además, las vías de denuncia confidenciales deben estar disponibles para cualquier empleado, permitiendo el reporte de irregularidades sin temor a represalias. Esta supervisión activa fortalece la cultura de integridad, adicionalmente tener una matriz interna que se deba trabajar para los niveles de escalamiento y denuncias que se puedan generar (Raza, S. 2025)

Formación y Cultura Organizacional. Considero que se debe tener la prevención efectiva que se requiere una cultura ética sólida. Mediante programas de formación y refuerzo para la ética digital, legalidad y responsabilidad profesional. Todos los empleados deben conocer la Ley 1273 de 2009, la Ley 1581 de protección de datos, sin olvidar los principios del Código de Ética del COPNIA. Generando. Cuando la ética se convierte en parte del ADN organizacional, se alinea naturalmente con la legalidad y el respeto por los derechos de terceros.

C. ¿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?

Considero que unas de los principales procesos que se deben generar dentro de una ciberseguridad frente a posibles desviaciones y eventos que pueden surgir, es tener un procedimiento que cumpla con las leyes, normatividad y ética Profesional apoyadas con los

procesos de denuncias y medidas cautelares que permitan apoyar los protocolos rápidos de respuesta.

Respuesta Inmediata y Contención del Incidente. Debe estar acompañada de acciones legales, como denuncias penales por violación de la Ley 1273 de 2009, y medidas cautelares que protejan la infraestructura crítica y la información sensible. Ante cualquier detección de ciberespionaje por parte de una empresa contratada, se deben tener protocolos de activación de respuestas rápidas. Esto debe tener un respaldo legal que incluya la suspensión inmediata del contrato, así mismo el procedimiento del aislamiento de los sistemas comprometidos. Es de vital importancia iniciar una investigación forense que determine el alcance del daño, así mismo los métodos utilizados y los datos comprometidos. (Sun, D 2025)

Auditoría Estructural y Revisión de Procesos de Contratación. Como todo procedimiento se debe tener Auditorias, las organizaciones deben realizar auditorías profundas de sus procesos de contratación, supervisión y control de proveedores tecnológicos. Esto debe implicar revisar los criterios de selección, revisiones de hojas de vida y tener mecanismos de verificación de antecedentes, las cláusulas contractuales sobre ética y responsabilidad, y los protocolos de monitoreo técnico. Es clave establecer cláusulas de revisión inmediata por violaciones éticas, para prevenir futuras infiltraciones.

Prevención Estructural y Reformas Normativas. Para evitar que existan hechos que se repitan, los gobiernos y organizaciones deben fortalecer su marco normativo y sus mecanismos de vigilancia. Esto puede incluir la creación de registros públicos de proveedores de ciberseguridad, requisitos de certificación ética y técnica, y la obligación de reportar incidentes de seguridad. También es necesario establecer auditorías técnicas automatizadas, controles de acceso basados en roles y canales de denuncia protegidos. Estas medidas no solo previenen el

abuso de poder tecnológico, sino que consolidan una cultura de integridad digital y protección de derechos fundamentales.

Componente Práctico - Prácticas Simuladas

En la siguiente Etapa conoceremos el Anexo 4 – Escenario 3 planteado para realizar el componente práctico de Red Team.

Situación Problema: Análisis Red Team

La primera misión del equipo Red Team consiste en identificar el medio o proceso mediante el cual se está produciendo una fuga de información por una aplicación vulnerada.

De acuerdo con la información inicial, el equipo afectado cuenta con una aplicación vulnerable instalada sobre un sistema operativo Windows. Se presume que dicha aplicación podría estar asociada a un exploit que permitiría la obtención de acceso mediante Shell, la escalación de privilegios, o algún otro tipo de ataque.

Se entrega una Imagen de Windows 7 el cual fue una copia del servidor con el objetivo de validar la existencia de una posible vulnerabilidad y determinar si esta ha sido explotada. En caso de confirmarse la explotación, deberá crear un usuario utilizando su primer nombre y apellido, asignándole privilegios de administrador, con el fin de presentar una prueba de concepto (PoC), para finalmente entregar la evidencia técnica, y timeline forense completo, con un plan de remediación integral.

Pasos de un Pentesting

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.

En los pasos propuestos de Pentesting básicamente se desarrollan en 6 fases

Tabla 7

Fases de Pentesting

Fases	Descripción
Planificación y definición de alcance	Se debe acordar claramente los objetivos, sistemas y redes a evaluar, así como las reglas y limitaciones bajo las cuales se realizará la prueba, para asegurar que sea controlada, segura y efectiva.
Reconocimiento (Recopilación de información)	recopilar toda la información posible sobre el objetivo, ya sea de forma pasiva (sin interactuar directamente con el sistema) o activa (interactuando para descubrir puertos, servicios y vulnerabilidades), formando la base para preparar las siguientes etapas del análisis y ataque.
Análisis o escaneo de vulnerabilidades	evaluar los sistemas identificados durante el reconocimiento para detectar posibles fallos de seguridad utilizando herramientas automatizadas y análisis manual, con el objetivo de identificar vulnerabilidades que puedan ser explotadas en etapas posteriores del pentesting.
Explotación	consiste en utilizar las vulnerabilidades identificadas para intentar acceder o comprometer el sistema objetivo mediante ataques controlados, con el fin de demostrar el riesgo real y el impacto potencial de dichas fallas en la seguridad.
Post-explotación y análisis de impacto	consiste en actividades realizadas después de haber obtenido acceso al sistema objetivo, con el propósito de evaluar el alcance del compromiso, mantener la presencia en el sistema, explorar la red y obtener mayor información, para entender el impacto real de las vulnerabilidades explotadas
Elaboración de informe y remediación	consiste en documentar de manera clara y detallada todos los hallazgos encontrados durante la prueba, incluyendo la descripción de las vulnerabilidades

Nota. en esta tabla recordaremos las fases que tiene el pentesting y una descripción detellada de lo que encontraremos en cada una de las fases.

Teniendo en cuenta lo expresado anteriormente sobre los procesos y/o los pasos de pentesting procedemos a realizar un análisis detallado.

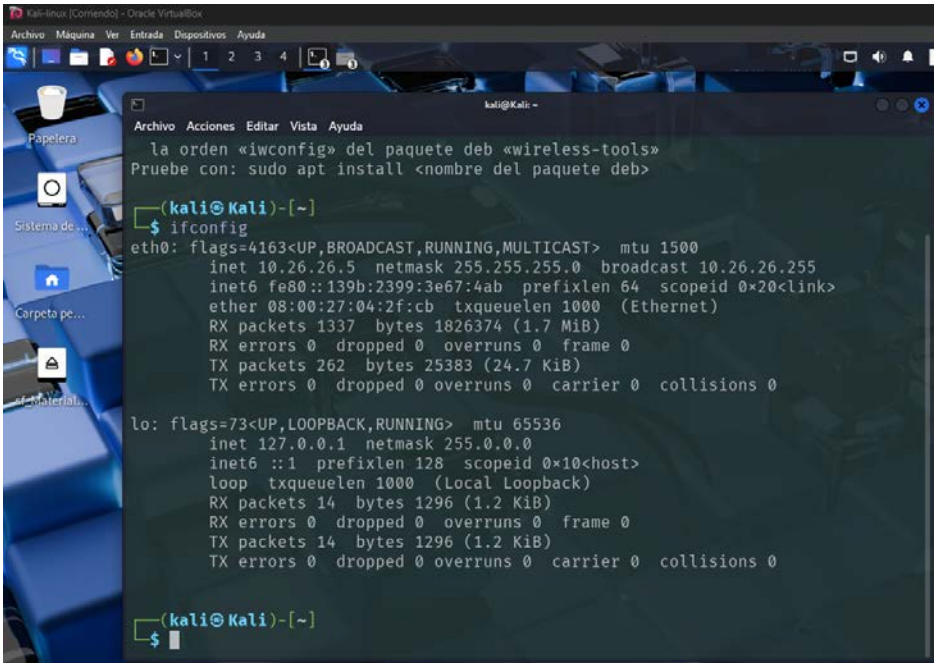
Planificación y Definición de Alcance. Analizar la fuga de información originada desde Host-A, verificando la explotación de la vulnerabilidad y el escalamiento de privilegios, realizar la reproducción controlado de un movimiento lateral (Pivoting)

Reconocimiento (Recopilación de Información). Se recopilaría toda la información relevante sobre Host-A, incluyendo detalles del sistema operativo, aplicaciones instaladas, configuraciones de red, y posibles vulnerabilidades conocidas de la aplicación vulnerable detectada. También examinaría registros y evidencias forenses para entender el comportamiento y alcance del ataque, identificando posibles vectores de acceso y métodos de escalamiento de privilegios.

Para proceder con este Ambiente controlado entre la maquina Host A (Windows-7) y Kali (Kali-linux) procederemos con la configuración de las tarjetas de red vista en la Figura 5, procedemos a validar sus conexiones entre las dos máquinas, Ver Figura 10, procederemos a ejecutar la Kali, como ya conocemos el rango de direcciones IP, al ser un ambiente controlado, validamos en que rango está el equipo.

Figura 11

Ejecución del Comando Ifconfig



Nota. se genera el comando ifconfig para validar que Kali este dentro de la red, en el ambiente controlado.

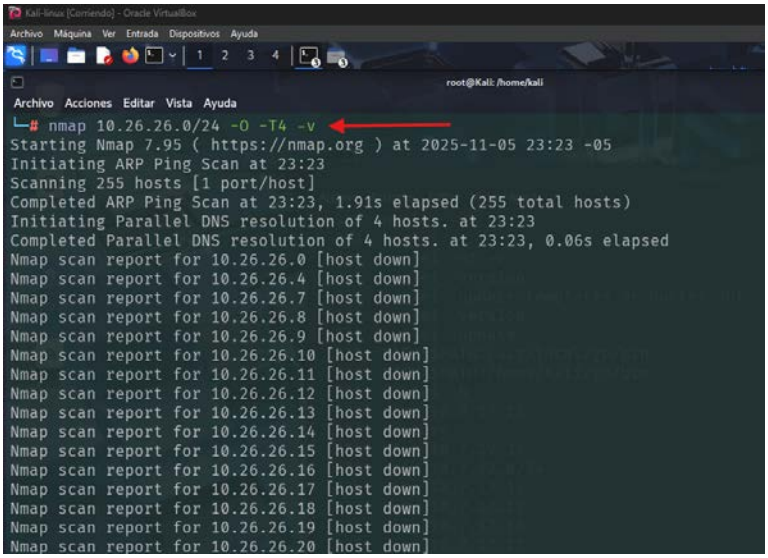
Una vez identificado el rango de direccionamiento el cual se encuentra nuestro ambiente controlado procederemos a realizar un escaneo de red, sin importar que ya conocemos el direccionamiento IP del Host-A intentaremos crear un ambiente real (Atacante) con estos procedimientos, en esta fase utilizaremos la herramienta NMAP, con el fin de realizar la identificación y descubrimiento de la red para localizar el objetivo a atacar (Host-A).

¿Qué es Nmap?. Es una herramienta de código abierto para la exploración de redes y auditoría de seguridad, diseñada para escanear rápidamente grandes redes y también funcionar eficientemente con hosts individuales. Utiliza paquetes IP sin procesar de manera innovadora para identificar qué dispositivos están activos, qué servicios y versiones ejecutan, qué sistemas

operativos usan y qué tipos de cortafuegos o filtros aplican. Además de su uso en auditorías de seguridad, Nmap es valiosa para administradores de sistemas y redes en tareas como inventariado de red, gestión de actualizaciones y monitoreo de disponibilidad de hosts y servicios, gracias a su precisión, versatilidad y capacidad de personalización mediante scripts

Figura 12

Ejecución del Comando Nmap



Nota. Con el comando nmap 10.26.26.0/24 -O -T4 -v, indicamos que sea escaneado toda la red

Comandos usados

10.26.26.0/24: Rango de red a escanear (todas las IPs del segmento 10.26.26.0 a 10.26.26.255).

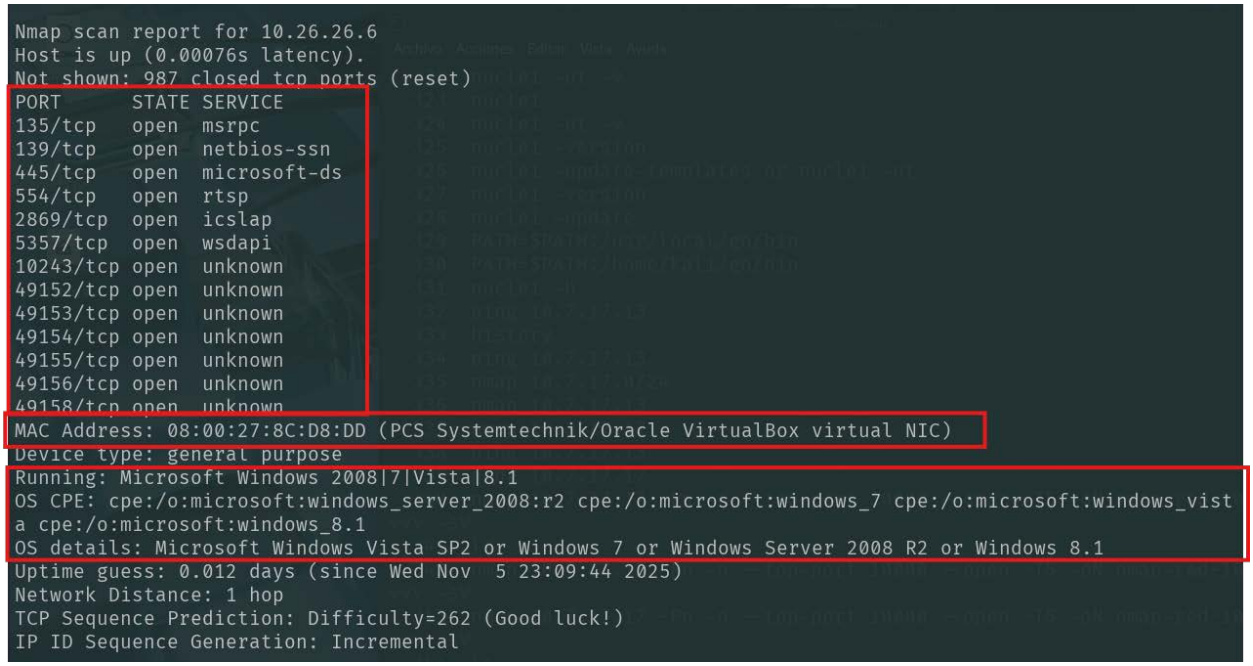
-O: Intenta detectar el sistema operativo de los hosts encontrados (OS detection).

-T4: Define la "agresividad" o velocidad del escaneo. T4 es rápido, recomendado para redes locales no congestionadas.

-v: Modo verbo, muestra más detalles/progreso durante el escaneo.

Figura 13

Resultados Obtenidos de la Búsqueda con Nmap



Nota. se evidencia que cuenta con varios puertos abiertos, detectando la versión de Windows.

Se realiza el reconocimiento de la información a detalle para lograr tener mayor detalle en el tipo de ataque que se debe estudiar, para lograr una pentesting

Tabla 8

Puertos y Servicios Detectados

Puertos	Servicios / Descripción
135/tcp (msrpc):	Servicio RPC de Windows, utilizado para comunicaciones entre procesos y gestión remota; es común blanco de explotación si no está bien protegido.
139/tcp (netbios-ssn):	NetBIOS Session Service, facilita el acceso compartido a archivos e impresoras; vulnerable a ataques de enumeración o interceptación si no está segmentado.
445/tcp (microsoft-ds):	Servicio SMB a través de TCP, ampliamente utilizado para compartir archivos e impresoras; ha sido objetivo de múltiples exploits como EternalBlue.
554/tcp (rtsp):	Protocolo de transmisión en tiempo real, generalmente empleado en cámaras IP y multimedia; puede presentar riesgo si está accesible externamente.
2869/tcp (icslap):	Servicio UPnP de Windows, utilizado para permitir configuraciones automáticas en redes domésticas; puede exponer el host a ataques directos.
5357/tcp (wsdapi):	Web Services for Devices API, habilita la interacción con dispositivos conectados en red, no es habitual en ambientes empresariales.
10243/tcp (unknown):	Puerto desconocido, lo que puede significar un servicio personalizado o no identificado por Nmap.
49152/tcp a 49158/tcp (unknown):	Son puertos dinámicos/efímeros típicamente utilizados por servicios internos de Windows (RPC, DCOM, etc.), aunque el servicio exacto no se identifica automáticamente.

Nota. En esta tabla vemos los puertos que encontramos abiertos y las posibles vulnerabilidades que podemos analizar.

Teniendo en cuenta la descripción detallada de cada uno de los puertos podemos identificar que la presencia de servicios de Windows RPC, NetBIOS, SMB y UPnP están expuestos y puede dejar el sistema vulnerable a ataques explotaciones de vulnerabilidades conocidas permitiendo los movimientos laterales por parte de atacantes.

Análisis o Escaneo de Vulnerabilidades. Después de recopilar toda la información en este caso con la Herramienta de Nmap procedemos a realizar un análisis de las Vulnerabilidades encontradas y posible vector a atacar, con el fin de evaluar donde y como podría ser explotadas.

Tabla 9

Análisis de Vulnerabilidades Encontradas

Servicios	Tipo De Ataques
Windows RPC	Escalada de privilegios mediante explotación de vulnerabilidades en el Endpoint Mapper (EPM): Por ejemplo, la vulnerabilidad CVE-2025-49760 permite ataques de suplantación (spoofing) y escalamiento de privilegios a nivel de dominio. Ataques de ejecución remota de código: Muchas vulnerabilidades RPC permiten que un atacante ejecute código arbitrario en el sistema objetivo, obteniendo control total sobre la máquina.
NetBIOS	Envenenamiento de servicios LLMNR/NBT-NS: El atacante responde a solicitudes de resolución de nombres y puede capturar hashes NTLM de usuarios, facilitando ataques de relay y descifrado de contraseñas. Enumeración de recursos y usuarios en red: Utilizando NetBIOS es posible identificar equipos, usuarios y recursos compartidos, permitiendo planificar ataques posteriores. Fuerza bruta de credenciales: El uso de contraseñas débiles en NetBIOS puede permitir acceso no autorizado por ataques de fuerza bruta.
SMB	Explotación de vulnerabilidades críticas (EternalBlue, CVE-2017-0144, entre otras): Ataques de ejecución remota de código y propagación de malware tipo ransomware (ej. WannaCry) mediante SMB. Relay y robo de información: Captura y manipulación de sesiones SMB para ejecutar ataques de relay, robo de información sensible y movimiento lateral entre equipos. Divulgación de información: Enumeración de shares, usuarios y configuración, facilitando la identificación de recursos sensibles expuestos.
UPnP	Configuración maliciosa y acceso remoto: UPnP puede ser explotado para abrir puertos, redirigir tráfico o permitir la administración remota de dispositivos vulnerables. Ejecución remota de comandos: Algunos dispositivos y servicios mal configurados permiten que un atacante ejecute comandos arbitrarios o tome control del sistema objetivo.

Nota. En esta tabla observamos los servicios y los tipos de ataques que se pueden generar con las vulnerabilidades encontradas.

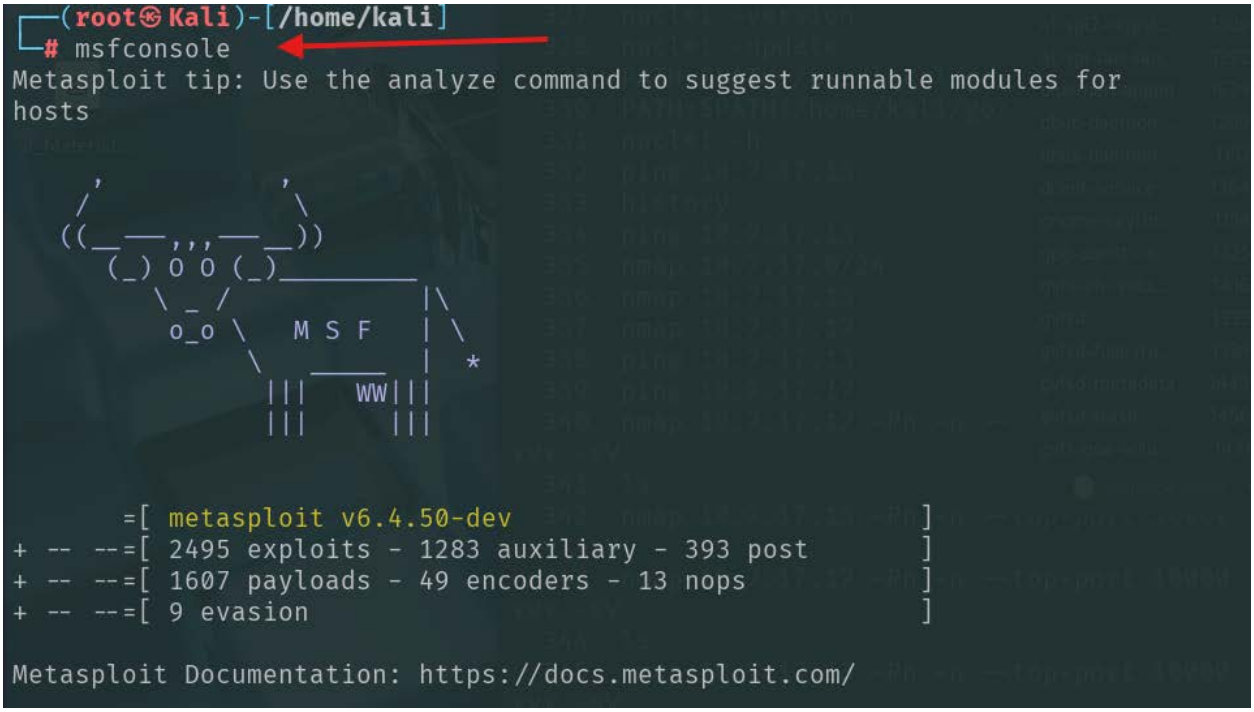
Explotación. Intentaremos explotar de manera controlada las vulnerabilidades encontradas en los pasos anteriores, comprobando si es posible acceder al sistema, revisando lo

anterior procederemos a intentar elevar privilegios o comprometer la información, teniendo en cuenta los límites definidos en la planificación y definición del alcance.

Podríamos explotar la vulnerabilidad MS17-010 (CVE-2017-0143) en el servicio SMBv1 del Host-A, para esto ejecutaremos la herramienta de Metaexploit de Cali Linux para realizar nuestro Vector ataque.

Figura 14

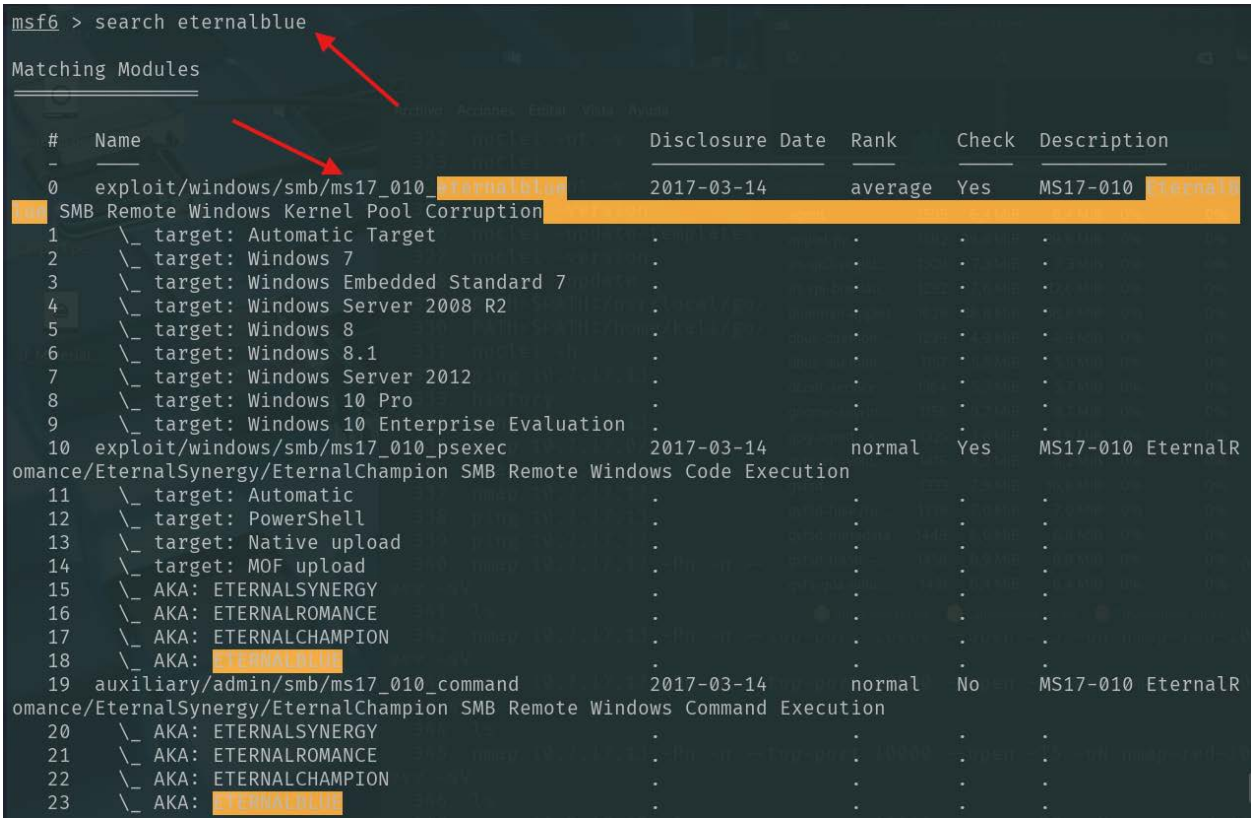
Ejecución del Comando Msfconsole



Nota. se genera el comando msfconsole el cual es el comando principal para iniciar a la consola de Metasploit Framework

Figura 15

Ejecución del Comando Search Eternalblue

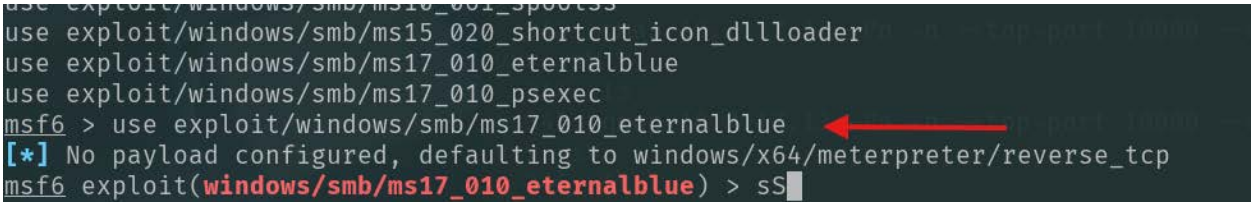


Nota. se genera el comando search eternalblue para buscar módulos relacionados con la vulnerabilidad conocida como **EternalBlue**.

Esto nos permite consultar la base de datos interna en busca de exploit y los módulos auxiliares evidenciamos que podemos usar el módulo ms17_010_eternalblue

Figura 16

Revisión del Módulo Ms17_010

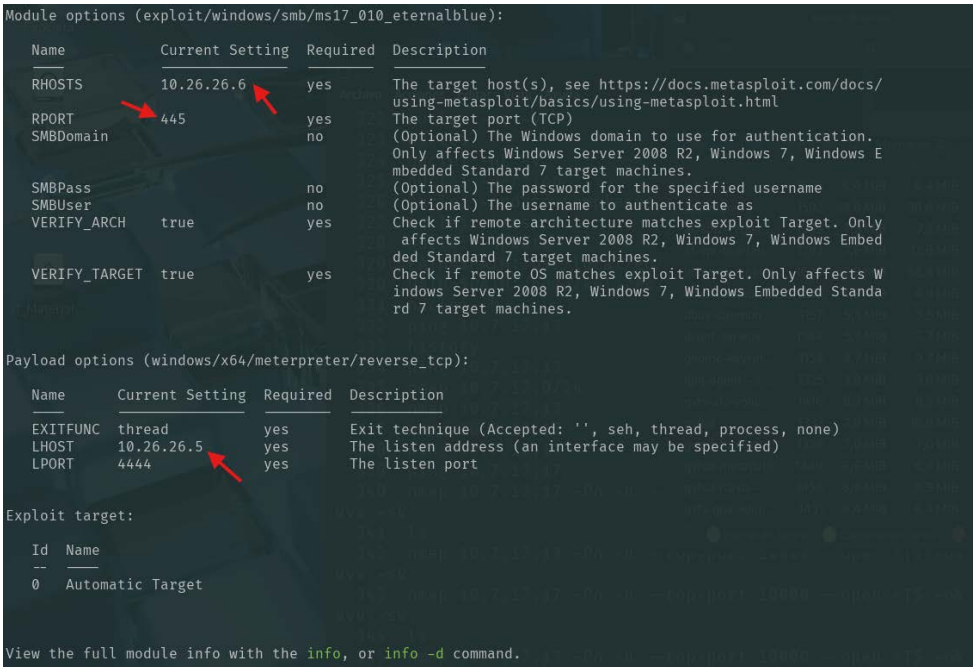


Nota. se genera el comando use exploit/windows/smb/ms17_010_eternalblue, para indicar el exploit a usar.

Al indicar que módulo de exploit iremos a usar, permitiendo la selección y las configuraciones que debemos realizar sobre este módulo teniendo en cuenta el vector atacante y realizando las configuraciones preliminares, como RHOST el cual indica cual es la Ip del Host a atacar, RPORT indicar el puerto a vulnerar.

Figura 17

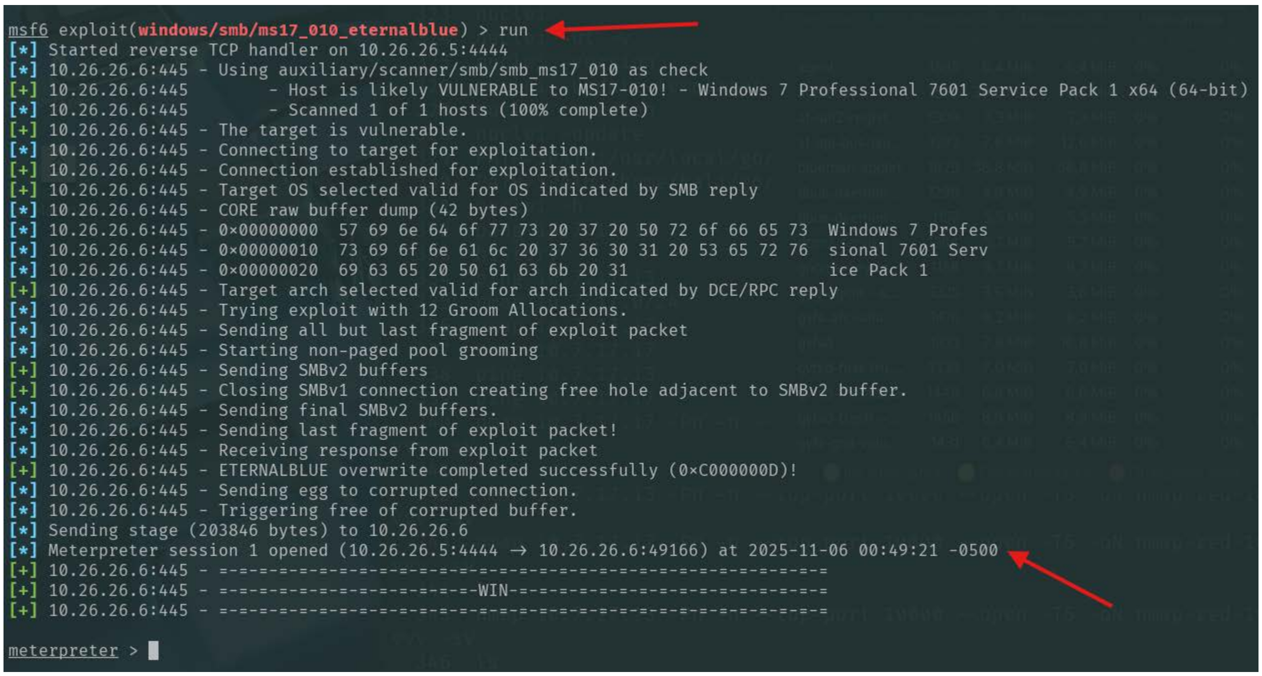
Verificación del Exploit



Nota. se realiza las verifica las configuraciones antes de lanzar el ataque con el comando show options, confirmamos que la información está bien diligenciada.

Figura 18

Ejecución del Exploit

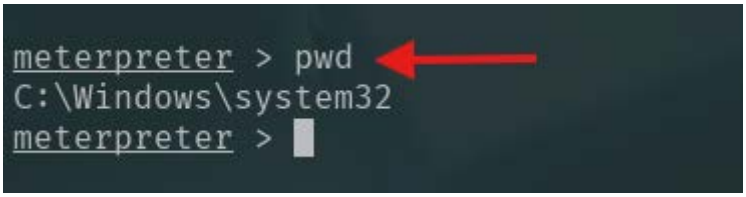


Nota. Al generar el comando Run identificamos que el exploit fue un éxito, y logramos establecer una sesión de conectividad.

Verificando la información evidenciamos que el exploit logro acceder a la máquina de Host-A el cual al realizar validaciones sobre la línea de comando, nos encontramos en la estructura de Windows.

Figura 19

Ejecución del Comando Pwd



Nota. se genera el comando pwd que nos permite conocer la raíz donde nos encontramos ubicados y logramos acceder.

Post-explotación y Análisis de Impacto. En esta fase, se procede a la explotación controlada de las vulnerabilidades identificadas, Esta etapa permite demostrar el impacto real de las fallas detectadas y proporciona evidencia sobre el alcance potencial de un ataque exitoso.

Elaboración de Informe y Remediación. Teniendo en cuenta los resultados obtenidos se recomienda, Determinar si los servicios son realmente necesarios y, en caso contrario, cerrarlos/filtrarlos, Restringir el acceso a estos puertos a través de firewalls, Mantener los servicios y el sistema operativo actualizado, Realizar un análisis de vulnerabilidades dirigido sobre estos servicios para verificar exposiciones reales.

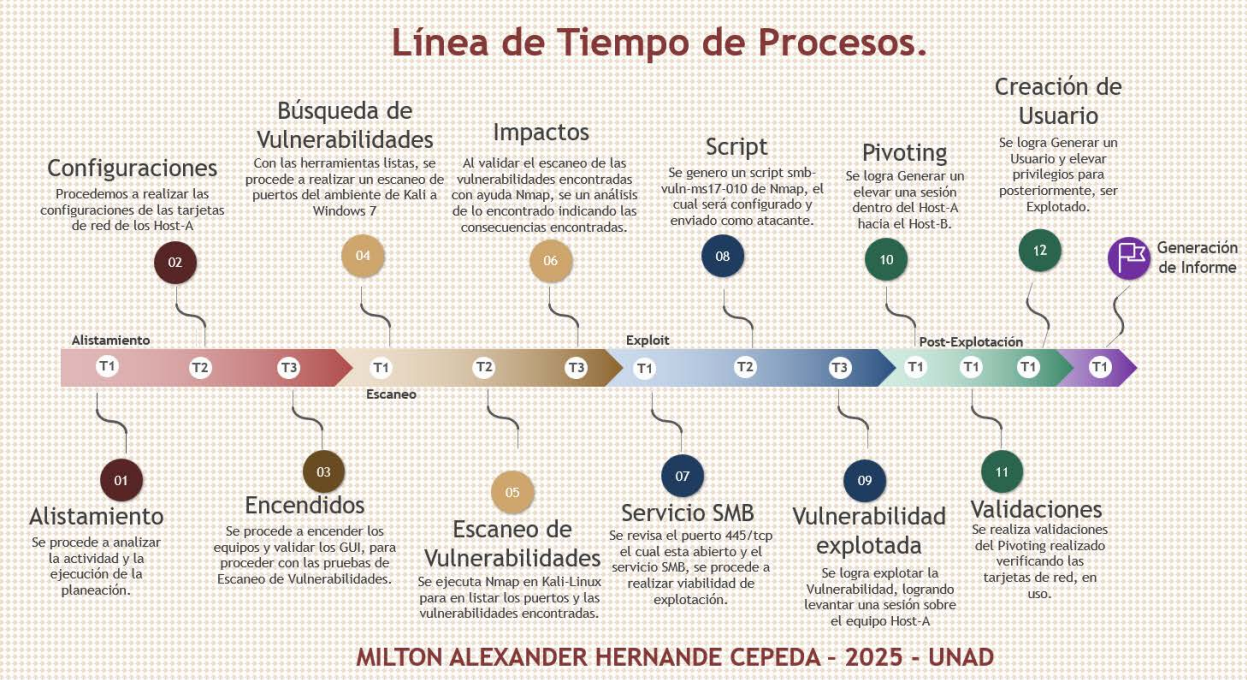
Teniendo en cuenta en esta fase de elaboración de Informe se debe entregar un informe robusto que se cuente con la capacidad analítica y especificar en gran manera todo lo evidenciado con las posibles fallas y brechas de seguridad encontradas

Listado Identificado Sobre la Brecha de Seguridad

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 - 1 Windows.

Figura 20

Línea de Tiempo de Procedimientos



Nota. se genera una línea de tiempo con los procesos más relevantes en esta actividad para el Pivoting.

Herramientas Utilizadas.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “Máquina - 1 Windows”? ¿Qué puerto abre la aplicación específica en el anexo?

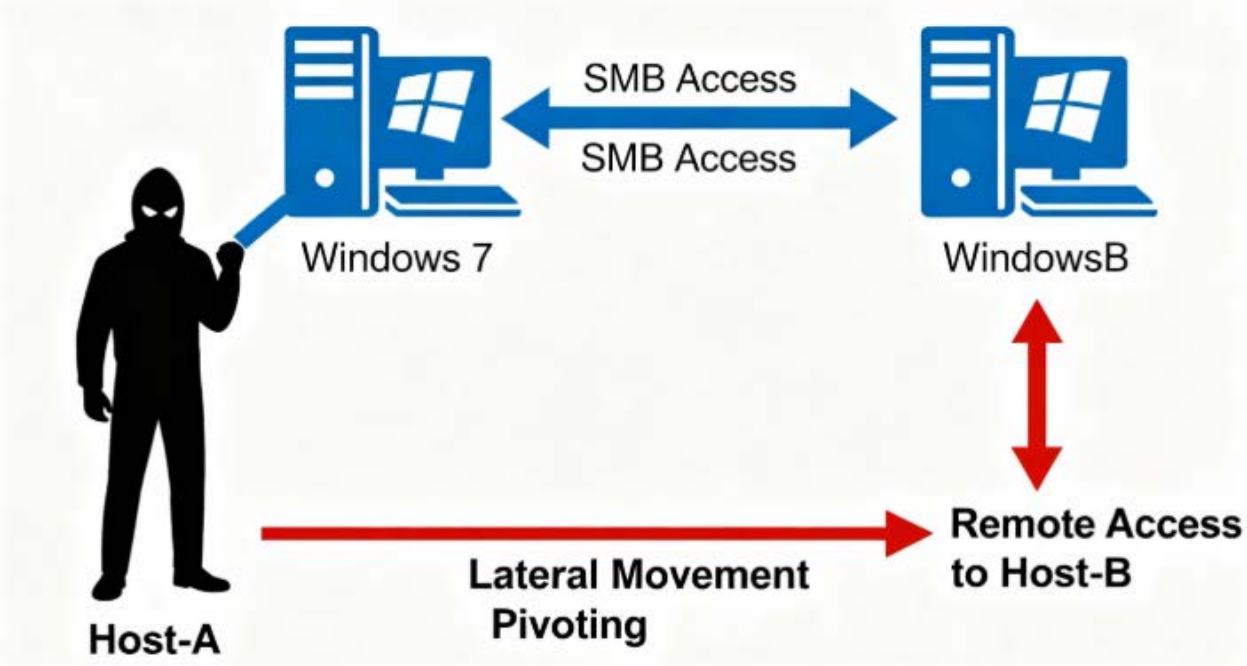
La herramienta usada en esta Etapa 3 es la Nmap el cual se usó para generar un escaneo de puertos, sobre la máquina de Windows 7 (Host_A) esto nos permitió conocer una de las vulnerabilidades como era el puerto 445/tcp, al estar abierto generamos un exploit en el servicio de SMB (Server message Block) el módulo usado fue MS17-010 (EternalBlue). (Waseem 2025)

Afectaciones

Explique con sus palabras y de manera específica cómo afecta el ataque a las máquinas (Windows) encontradas en la red: Haga uso de gráficos para explicar el ataque.

Figura 21

Pivoting Host-A to Host-B



Nota. en esta Figura observamos el tipo de ataques generados desde la máquina de Kali, a la máquina de Host-a to Host-B con Pivoting.

El gráfico ilustra el flujo de un ataque usando la vulnerabilidad EternalBlue en una red con dos máquinas Windows 7:

Host-A (Windows 7). El atacante explota EternalBlue aprovechando el servicio SMB vulnerable en Host-A, obteniendo acceso remoto (por ejemplo, mediante una shell o sesión Meterpreter). Esto permite tomar control total del equipo: ejecutar comandos, exfiltrar información y moverse por el sistema.

Movimiento Lateral (Pivoting) Hacia Host-B. Desde Host-A, el atacante utiliza técnicas de pivoting —como redireccionar puertos o establecer túneles— para acceder a Host-B, otra máquina Windows 7 en la misma red. Esto se logra porque ahora Host-A actúa como punto intermedio dentro del entorno comprometido, permitiendo reusar credenciales y explotar servicios (como SMB) vulnerables en Host-B.

Impacto en Ambas Máquinas. Ambas quedan bajo control del atacante quien puede:

- Descargar datos sensibles
- Crear usuarios administrativos no autorizados
- Instalar malware o herramientas para persistencia
- Utilizar ambos sistemas para atacar otros recursos internos
- El atacante puede permanecer oculto y expandir su acceso a toda la red

El gráfico demuestra cómo la explotación del SMB en un equipo (Host-A) permite el acceso inicial y el movimiento lateral (pivoting) a otros sistemas vulnerables (Host-B), generando una cadena de compromisos en toda la red Windows.

Descripción del Procedimiento

Documente, cada uno de los pasos que ejecutó y las evidencias correspondientes para la validación de la vulnerabilidad en la máquina Windows; integre además la descripción del Pivoting realizado hacia la segunda máquina.

Para este procedimiento ejecutaremos una segunda maquina de Windows 7 que la llamaremos Host-B

Figura 22

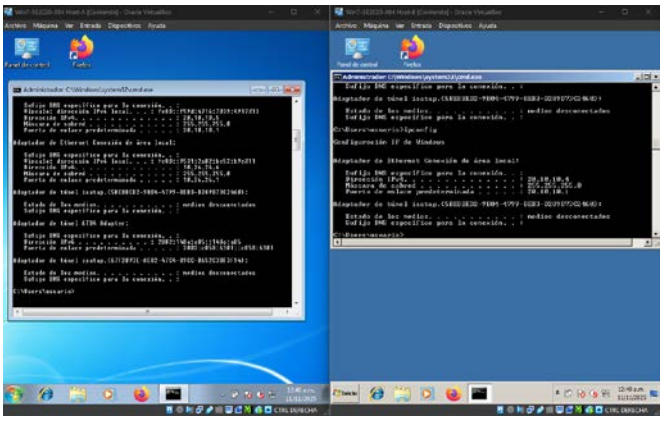
Topología Para Desarrollar

Nota. se genera el plano de la topología con las redes configuradas y direccionamiento establecido para proceder a realizar Pivoting.

Teniendo en cuenta la Figura anterior y después de generar y garantizar conectividad entre las máquinas de Windows evidenciaremos la conectividad de cada una de estas como el ambiente de estudio que realizaremos.

Figura 23

Validaciones de Host-A y Host-B

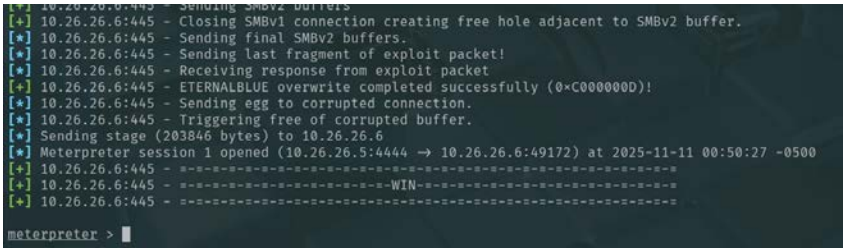


Nota. Se evidencia que las tarjetas de red entre Host-A y Host-B se comparten un único direccionamiento.

Ahora validamos con Kali-Linux levantamos una sesión inicialmente al Host-A con el fin de Levantar una estación de trabajo en la red (Kali - Host-A)

Figura 24

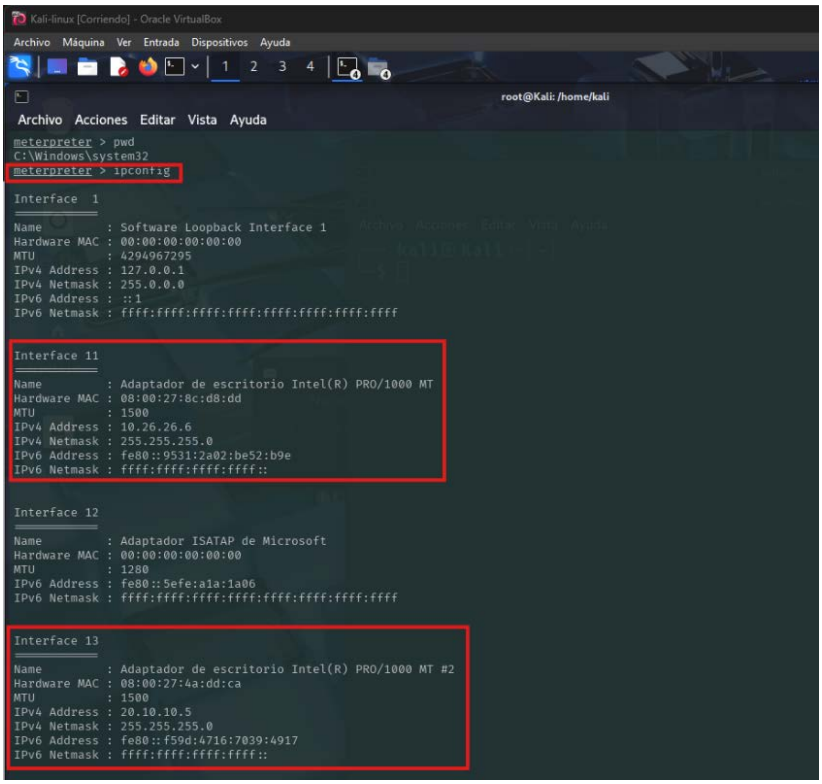
Levantamiento de Sesión sobre el Host-A



Nota. Se confirma por parte de la consola el accedo a la máquina de Host-A, con el fin de realizar Pivoting al Host-B.

Figura 25

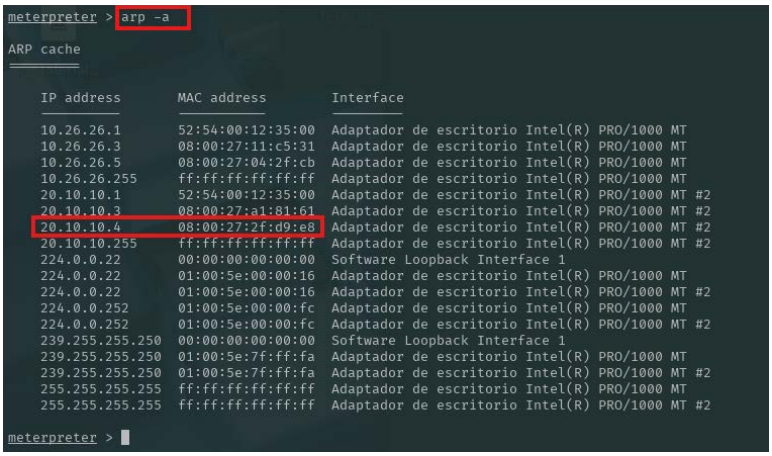
Revisión de las Tarjetas de Red, para Validar Nuevas Redes



Nota. Se confirman tarjetas de red sobre la sesión levantada para realizar validaciones y confirmar la máquina de Host-A con sesión Activa.

Figura 26

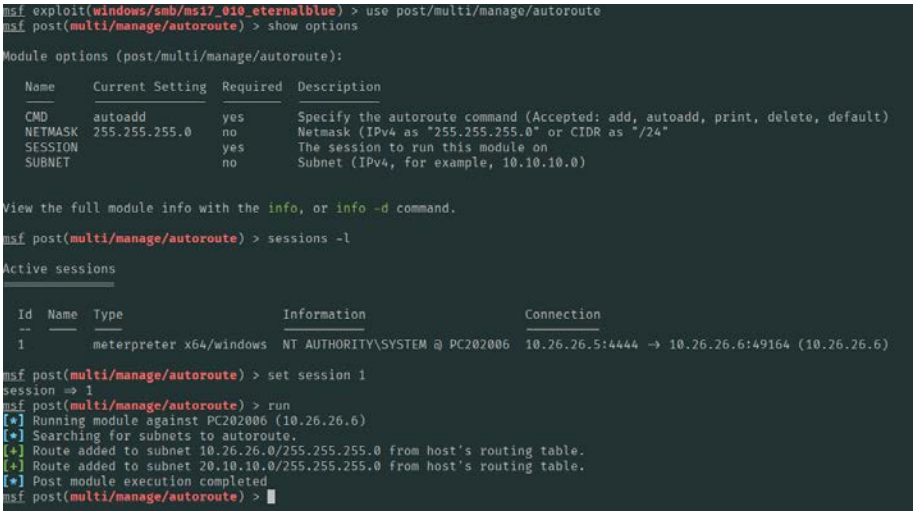
Arp-A para Validar Conectividad Hacia la Maquina Host-B



Nota. Al correr el comando Arp -a se confirma las conexiones establecidas y recibidas por la tarjeta de red, así mismo se valida nuestra Maquina para hacer Pivoting.

Figura 27

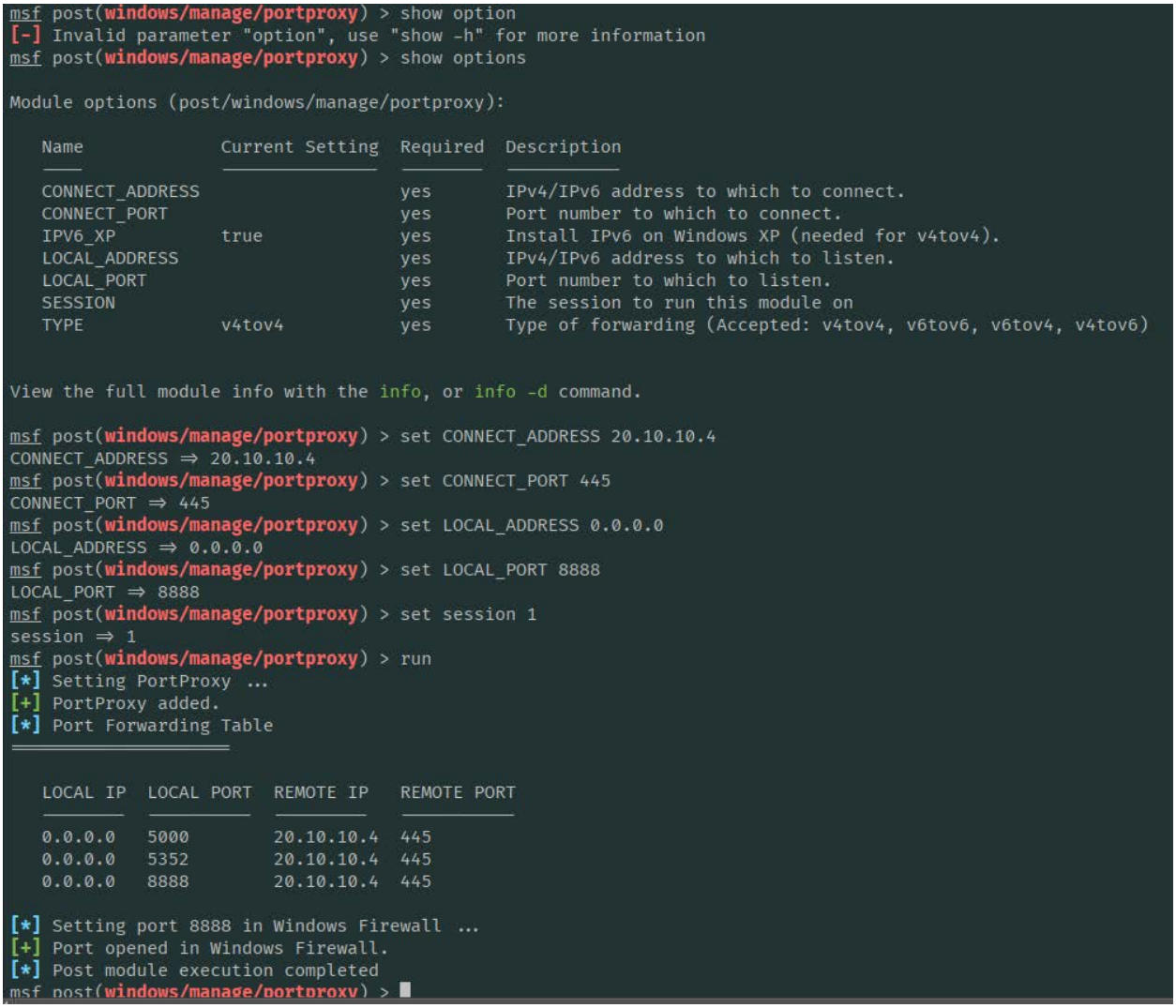
Comando AutoRoute



Nota. generamos el comando AutoRoute para enrutar el tráfico sobre la máquina de Host-A a la máquina de Host-B, garantizando el ataque de Pivoting, entre Windows.

Figura 28

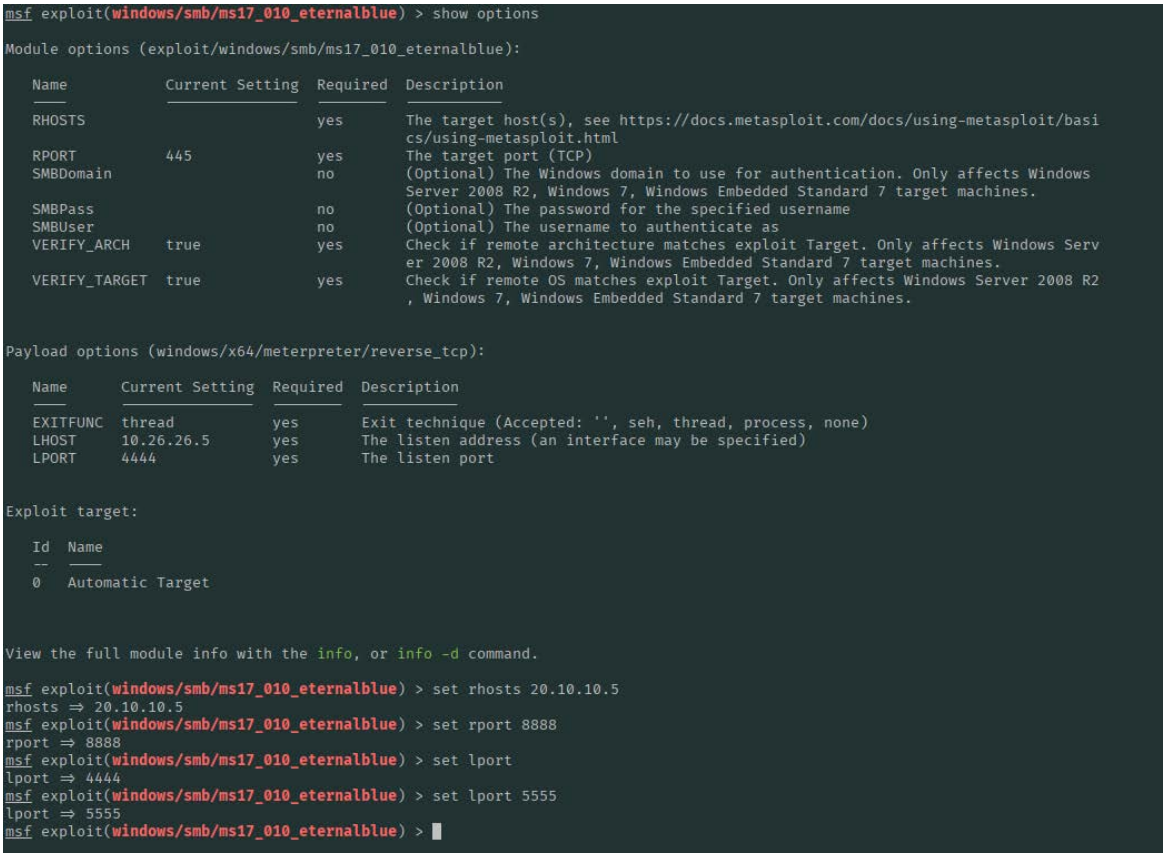
Configuración de Portproxy



Nota. generamos el comando portproxy para dar parámetros a los puertos y IP, de la máquina del Host-B, así quedan prealimentados con la información necesaria para el pivoting, asegurando el ataque al Host-B.

Figura 29

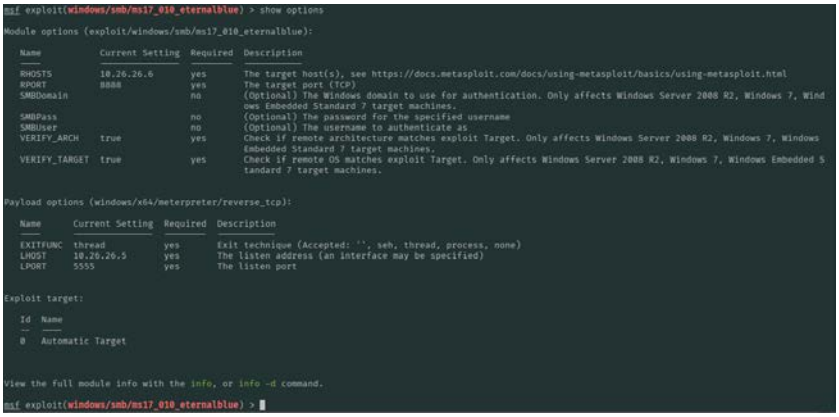
Generación de Enternalblue para Host-A con Acceso a Host-B



Nota. generamos un nuevo ataque de eternalblue, ya teniendo en cuenta que esta enrutado el tráfico y con una sesión activa, se debe cambiar parámetros como los puertos de RPORT y LPORT, según lo configurado anteriormente.

Figura 30

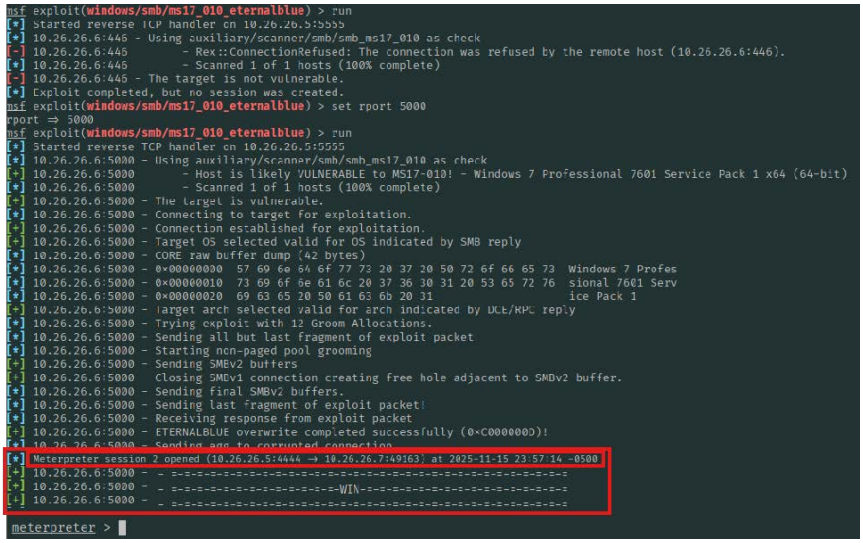
Parámetros de Explotación



Nota. Después de realizar las configuraciones, se procede a correr el servicio.

Figura 31

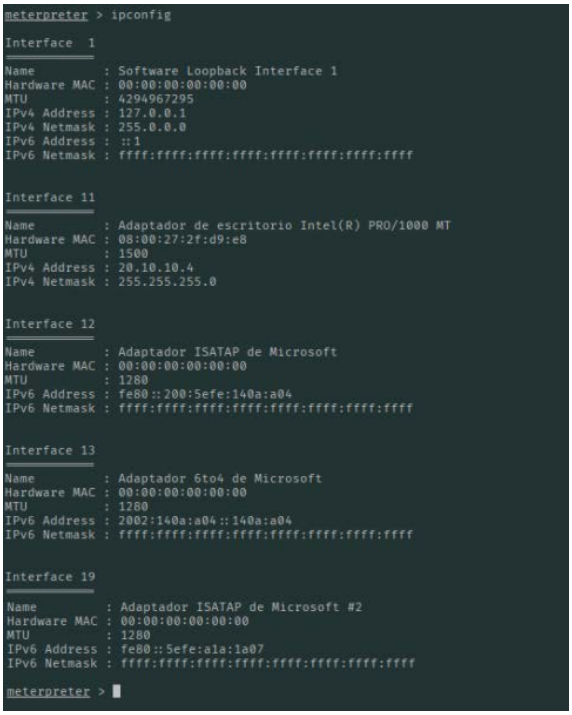
Sesión Establecida en Host-B



Nota. se evidencia que la sesión al Host-B fue activa, validando que se establece una sesión 2.

Figura 32

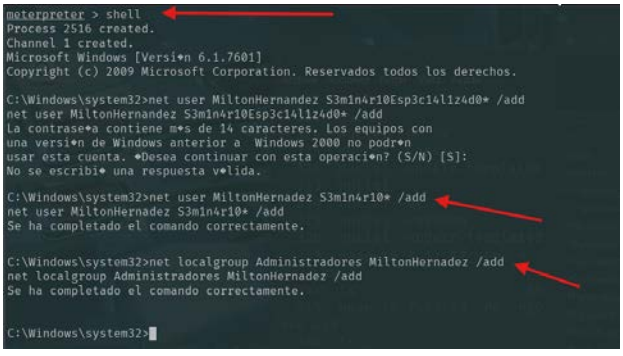
Validaciones de Tarjetas de Red



Nota. generamos el comando ipconfig para validar estado de las tarjetas de red sobre el Host-B

Figura 33

Ejecución del Comando Shell

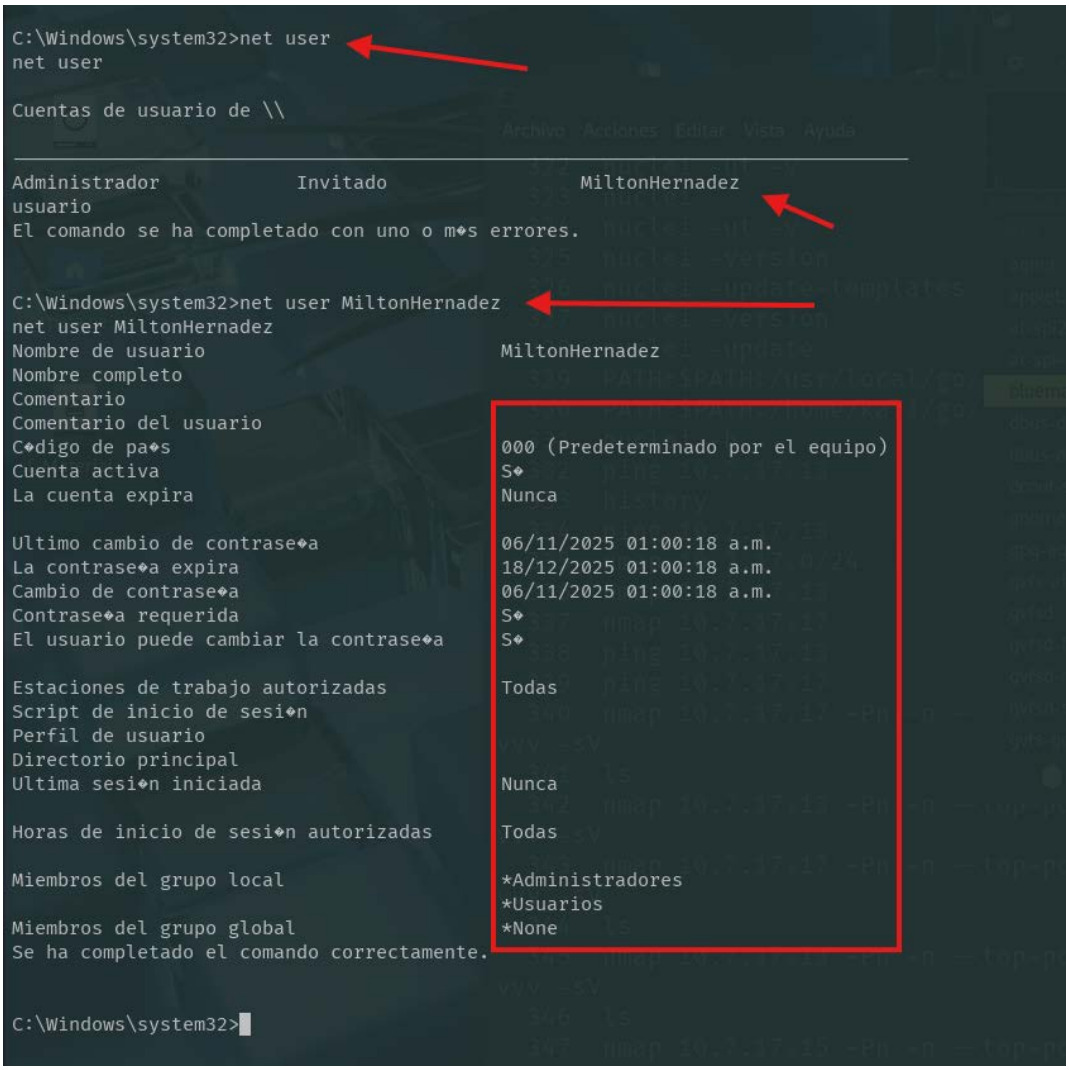


Nota. generamos el comando Shell el cual nos permitirá acceder al módulo de Windows, para generar la creación de un usuario y sus privilegios.

Podemos identificar que al ingresar a la consola Shell, logramos crear una cuenta de Windows llamada MiltonHernadez con su respectiva contraseña, elevando privilegios de Administrador sobre el Host-A.

Figura 34

Ejecución del Comando Net User | MiltonHernadez

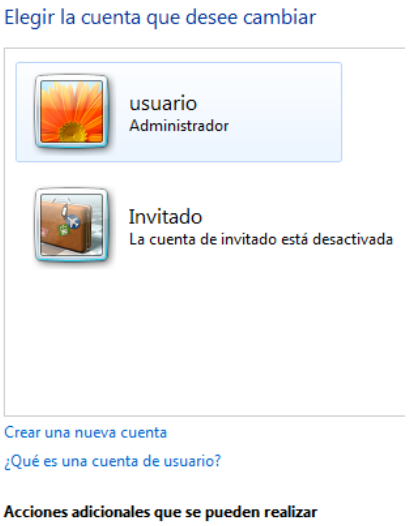


Nota. se genera el comando net user de igual manera net user MiltonHernadez identificando la fecha de la creación el nivel de acceso.

Esto evidencia que la post-explotacion a Windows 7 (Host-A) se logró satisfactoriamente, obteniendo la creación de un usuario y la elevación de privilegios.

Figura 35

Vista Antes del Exploit



Nota. se evidencia antes de la creación del usuario de privilegios.

Figura 36

Vista después del Shell

Nota. se evidencia después de la post-explotacion con el módulo de exploit se genera un usuario y la elevación de privilegios.

Esto nos permite evidenciar las vulnerabilidades generadas en el equipo remoto Host_A evidenciando como un atacante puede acceder de una manera muy fácil, a nuestros sistemas que tenemos obsoletos o sin actualizaciones.

Respuesta y Contención ante Incidentes de Seguridad

En la siguiente Etapa conoceremos el Anexo 4 – Escenario 3 planteado para realizar el componente práctico de Red Team.

Situación Problema: Análisis Blue Team

SecureNova Labs solicita al equipo Blue Team la contención y gestión inmediata de un ataque informático que se está desarrollando en tiempo real. La máquina de análisis asignada corresponde al entorno Windows revisado en la actividad anterior. Se requiere realizar un análisis exhaustivo del incidente, abarcando aspectos técnicos tanto de sistema operativo como de red. Con la información recolectada, se espera que, en función del grado de experticia, el equipo Blue Team logre contener el ataque y mitigue el impacto para evitar daños adicionales dentro de la organización. Adicionalmente, se informa que no existe presupuesto disponible para el uso de herramientas comerciales, por lo que el análisis deberá efectuarse empleando exclusivamente herramientas con licencia GPL

Se debe validar con apoyo al material desarrollado en la Etapa 3 se debe da respuesta a las siguientes preguntas que enfatizan al desarrollo del Blue Team y el desarrollo propuesto:

Ataque en Tiempo Real

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

Se considera que lo primero que se debe indagar y realizar ante un ataque en tiempo real es buscar la identificación y confirmación del incidente, continuando a una contención rápida del mismo para así tratar de minimizar el daño que se pueda causar, basando se en cada paso en evidencia técnica de los sistemas operativos, la misma red, procesos y registros de auditorías que se lleven a lugar.

Primeras Acciones.

- Son las Identificaciones y validaciones del ataque examinando todas las alertas del sistema de detección/prevención de intrusos (IDS/IPS), EDR, o SOC para validar si existe la actividad anómala.
- Se debe revisar los logs críticos del sistema operativo (por ejemplo, los registros de eventos en Windows, /var/log en Linux), adicionalmente se deben ver los eventos de autenticación, identificar si se presentaron cambios de usuario o algunos privilegios destacados como los accesos remotos inesperados.
- Validar las actividades de red inusuales, como conexiones a IPs desconocidas, buscar si existieron las transferencias masivas de datos, o algún tráfico en puertos que no sean habituales.

Contenciones Iniciales.

- Iniciar con las aislaciones del equipo afectado de la red (desconectando lo físicamente del cable o la misma des habilitación de la NIC virtual) esto ayudara a evitar alguna propagación o exfiltración y el Pivoting que se pueda generar.
- Continuar con la detención de los procesos y servicios sospechosos tras un rápido análisis, esto guardara la mayor cantidad de información volátil posible (como son las memorias RAM, tablas de conexiones, procesos activos) para poder posteriormente continuar con el análisis forense que dé a lugar.
- Primordial el Cambio de credenciales de las cuentas comprometidas y el bloqueo de accesos no autorizados inmediatos.

Preservación y Generar Análisis.

- Generar una copia de los registros afectados con sus respectivas capturas e imágenes de memoria para el análisis futuro.
- Documentar toda y cada una de las acciones realizadas y conservando los logs, los detalles de red, los procesos que estén en ejecución, las conexiones existentes, o cualquier otro archivo modificado, que se halla creado en medio del incidente.

Estas diferentes acciones son fundamentales para la necesidad de evitar algún daño adicional que se pueda presentar, es importante mantener la integridad de las evidencias y asegurar que la organización SecureNova Labs pueda entender cuál fue la causa raíz, o el alcance, adicionalmente documentar la técnica empleada por el atacante. no ignorar la documentación de la contención rápida, ya que esto puede permitir las detenciones del escalamiento lateral, jamás se puede permitir la pérdida de datos o borrado de pistas vitales para el análisis forense, ya que esto nos permite documentar y generar un histórico.

Debemos mantener un análisis que sea rápido y basado en los datos, esto permitirá utilizar los recursos del sistema operativo, como el monitoreo y registro de red, así mismo evidenciar y analizar los procesos en ejecución. Toda evidencia técnica es clave para el aprendizaje y la implementación de prontas medidas preventivas posteriores

Medidas de Hardenización

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

Para evitar que algún ataque se repita, se debe cumplir e implementar varias medidas importantes de hardenización que deben estar enfocadas en el fortalecimiento de la seguridad técnica, operativa e importante la concientización del personal. Estas medidas se deben buscar

cerrar las brechas de las vulnerabilidades explotadas, como mejorar la detección y respuesta para fortalecer las defensas internas de SecureNova Labs.

Tabla 10

Medidas de Hardenización

Medidas Técnicas Recomendadas	Medidas Operativas y de Concientización
Inmediatamente se deben aplicar parches y actualizaciones de seguridad de forma continua para cerrar vulnerabilidades conocidas si los sistemas Operativos están obsoletos Actualizar los o generar reglas estrictas.	Se debe capacitar constantemente al todo el personal en detección y prevención de técnicas comunes usadas por atacantes, como phishing y técnicas sociales.
Generar la implementación o gestión robusta de vulnerabilidades que incluya escaneos frecuentes, Análisis y remediación inmediatas.	Realizar constantes simulacros y ejercicios de incidentes para generar mejoras a las capacidades de la detección y respuesta del equipo de defensa (Blue Team).
Al fortalecer las autenticaciones con políticas de contraseñas fuertes.	Establecer y mantener protocolos claros de respuesta a incidentes, con definición de roles y escalamiento.
Configurar las segmentaciones de red y controles estrictos esto permitirá minimizar el movimiento lateral dentro.	Revisar y reforzar políticas de seguridad internas, incluyendo control de accesos físicos y lógicos, y supervisión de actividades.
Asegurar el monitoreo en tiempo real de todos los eventos y establecer alertas para detectar actividades sospechosas tempranamente.	Es importante mantener los equipos más vulnerables por temas de actualizaciones con mayor monitoreo constante en este caso como sucedió con Windows 7 (Obsoleto.)

Nota. Esta Tabla Muestra las características de las Medidas de Hardenización con las técnicas recomendadas y las Medidas de Operatividad.

Al Usar los resultados del ejercicio Red Team logramos identificar las debilidades concretas esto debe permitir priorizar las acciones de mitigación.

Al adoptar un ciclo continuo de evaluación, podemos tener una mayor efectividad y remediaciones para mejorar progresivamente las defensas.

Al integrar frameworks como MITRE ATT&CK podemos mapear tácticas y técnicas usadas y ajustar los controles de seguridad. (N.d. 2025)

Debemos promover la colaboración entre los equipos de Red Team y Blue Team llamados como (Purple Teaming) para maximizar las mejoras de las defensas.

La hardenización requiere una gran combinación de actualizaciones tecnológicas, que permiten el fortalecimiento y el monitoreo en la detección de amenazas, la mayoría de las situaciones debemos generar la capacitación del personal y mejora continua de todos los procesos y controles de seguridad que estén involucrados basados en los hallazgos específicos del ataque simulado, así mismo asegurar que no se repita con éxito un ataque similar, teniendo lo documentado y evidenciado.

Diferencias

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

Podemos decir que un equipo Blue Team es grupo profesional de ciberseguridad que su mayor enfoque es la detención de las defensas y protección continua de la infraestructura (sistemas, redes y datos de la organización.) El enfoque principal es la prevención, detección y respuestas a ataques informáticos, generando controles de seguridad, gestionando vulnerabilidades y realizando análisis forense para la contención de incidentes en pocas palabras fortalecer las defensas, evaluar riesgos y asegurar la continuidad operativa de la infraestructura tecnológica de la Organización.

En referencia a un equipo de respuesta a incidentes informáticos (IR - Incident Response) estos se especializan en manejar, contener y mitigar los incidentes de seguridad una vez que se han producido. El enfoque está basado en la gestión de eventos críticos, análisis forense

detallado para entender el origen y alcance de la intrusión, para la contención del daño y la recuperación de los sistemas afectados y recuperación de la comunicación sobre el incidente generado.

Es decir que Mientras que el Blue Team tiene una función más amplia y continua en la defensa, el equipo de respuesta a incidentes actúa especialmente cuando hay una alerta o incidente confirmado para minimizar el impacto y restaurar la seguridad, se genera una tabla de comparaciones que se pueden apreciar para entender los alcances de cada uno de los diferentes equipos.

Tabla 11

Comparación de los Equipos de Seguridad.

Aspecto	Blue Team	Equipo de Respuesta a Incidentes
Objetivo principal	Defensa proactiva; la prevención y detección	Contención y mitigación de incidentes activos (Vivos)
Alcance	Continuos monitoreos permanentes	Focalizado en incidentes específicos
Principales funciones	Monitoreo, gestionar las vulnerabilidades, Generar análisis forense, gestionar el fortalecimiento de la seguridad.	Análisis forense avanzado, la contención y recuperación, reportes de incidentes
Rol en la organización	Mantener y mejorar la seguridad general	gestión de crisis y gestionar la normalidad
Interacción	Se basa en la colabora con Red Team y equipos internos de seguridad.	Trabaja con Blue Team para aportar evidencias y mejoras

Nota. Esta Tabla enseña los Aspecto que tiene Blue Team y El Equipo de Respuesta a Incidentes con diferentes alcances y características principales

Center For Internet Security

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

El uso del CIS (Center for Internet Security) estos estándares estarían enfocados principalmente en la implementación y continuar unos estándares que representan guías de seguridad conocidos como CIS Controls y CIS Benchmarks. Estos ayudarían a el equipo de Blue Team a:

Tabla 12

Center For Internet Security

Establecer buenas prácticas	Genera unas guías del CIS que nos permiten proveer controles de seguridad y mejores prácticas con el fin de proteger (sistemas, redes y aplicaciones) basado en consensos de expertos y evidencias de la actualidad.
Configurar y hardenizar sistemas	Los CIS Benchmarks estas son configuraciones técnicas al detalle para endurecer (sistemas operativos, bases de datos, aplicaciones y dispositivos).
Mejorar la gestión de riesgos	Nos permite adoptar controles y benchmarks que facilita cumplir con normativas y estándares, adicionalmente alinea defensas con frameworks internacionales también reconocidos.

Nota. Esta Tabla indica los enfoques que puede tener al usar los estándares de Center For Internet Securitu

Los estándares de CIS se utilizarían como la estructura para reducir vulnerabilidades, mejorar el control con el monitoreo continuo y fortalecer la seguridad de los activos, haciendo más efectiva la defensa y una gran ayuda para la mitigación de amenazas.

Funciones y Características Principales

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

Un SIEM (Security Information and Event Management) es una solución tecnológica que está fundamentada en la seguridad informática debido a que esta se encarga de recopilar, centralizar, analizar y correlacionar en tiempo real los registros de eventos de seguridad, que son generados por diversos sistemas y/o dispositivos dentro de alguna organización, como puede ser los firewalls, servidores, endpoints, aplicaciones y redes., ETC.

Tabla 13

Características y Funciones Principales del SIEM

Funciones	Características
• Agrupa información de múltiples fuentes en un único repositorio • Facilitar el análisis y la gestión coherente de los eventos. • Analiza y correlaciona eventos para identificar patrones anómalos o sospechosos • Facilita la investigación y manejo de incidentes mediante análisis forense. • Ayuda a cumplir con regulaciones y estándares de • Reportes detallados y almacenamiento seguro de logs. • Se puede integrar con herramientas SOAR	• Proporciona una visión integral y en tiempo real • Transforma vastos volúmenes de datos • Permite detectar tanto amenazas conocidas como • Mejora la eficiencia operativa de los tiempos a responder a incidentes.

Nota. Esta Tabla Muestra las Características y Funciones Principales del SIEM en la Operatividad de la estructura de una red.

SIEM es una gran herramienta clave que nos permite a las organizaciones tener un gran control proactivo y efectivo sobre la seguridad informática, con la ayuda de esta herramienta nos facilita la detección de amenazas, una gestión eficiente y rápida de incidentes así poder cumplir con el lineamiento regulatorio.

Herramientas de Contención de Ataques

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.

Se describen las herramientas de contención de ataques informáticos que cubren aspectos claves de la contención como son bloqueos de acceso malicioso, la detección y respuesta rápida en endpoints, y la eliminación del software dañino, formando una defensa con mayor profundidad para la reducción del impacto y propagación de ataques informáticos, estas herramientas son las más destacadas tanto hardware como software.

Firewall (Cortafuegos). Puede ser un dispositivo o software capaz de controlar y filtrar el tráfico de la red entrante y saliente se pueden generar reglas definidas, la característica principal es bloquear el tráfico o conexiones maliciosas o no autorizadas. Esto permite a ayudar a prevenir acceso de atacantes a la red interna.

Endpoint Detection and Response (EDR). Es un software que monitorea en tiempo real la actividad de los dispositivos finales (endpoints) para detectar, bloquear y contener amenazas avanzadas como programa maligno o ataques de día cero, incluso actuando automáticamente para aislar el equipo infectado.

Software Antivirus/Antimalware. Son programas que permiten la identificación, eliminación o colocar en cuarentena programas maliciosos conocidos y nuevas variantes,

protegiendo los dispositivos contra infecciones que podrían propagarse y comprometer sistemas.

Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Seminario Especializado Equipos Estratégicos en Ciberseguridad Red Team & Blue Team-20251203_233119-Grabación de la reunión.mp4

https://youtu.be/8wXZtzvQ2KI

Conclusiones

Las colaboraciones entre los equipos Red Team y Blue Team permite una efectiva en la gestión de la seguridad logrando que los avances tecnológicos sean de gran ayuda en cualquier ambiente de red. La combinación de sus enfoques complementarios –ofensivo por parte del Red Team, que simula ataques para identificar vulnerabilidades, y defensivo por parte del Blue Team, que fortalece las defensas y monitorea amenazas – Esto genera un ciclo virtuoso que mejorara la continuidad del negocio.

Al fortalecer los equipos Red Team y Blue Team permitirá la mejorar en la Organización sobre la ciberseguridad, jamás se debe olvidar el enfoque integral que debe estar basado en una coordinación efectiva, eficiente y contingente, esto se lograra si se unifican los esfuerzos entre los Red Team y Blue Team. La formación continua del personal de seguridad permitirá remediar amenazas emergentes y una respuesta rápida sobre cualquier incidente que pueda generar se, minimizando el impacto y evitando la propagación de esta. Estas estrategias no solo abordan las vulnerabilidades en entornos físicos, sino que también posicionan a las organizaciones para enfrentar con éxito el panorama cambiante de las amenazas digitales, protegiendo sus activos y la confianza de sus clientes.

Recomendaciones

Las colaboraciones entre los equipos Red Team y Blue Team permite una efectiva en la gestión de la seguridad logrando que los avances tecnológicos sean de gran ayuda en cualquier ambiente de red. La combinación de sus enfoques complementarios –ofensivo por parte del Red Team, que simula ataques para identificar vulnerabilidades, y defensivo por parte del Blue Team, que fortalece las defensas y monitorea amenazas – Esto genera un ciclo virtuoso que mejorara la continuidad del negocio.

Al fortalecer los equipos Red Team y Blue Team permitirá la mejorar en la Organización sobre la ciberseguridad, jamás se debe olvidar el enfoque integral que debe estar basado en una coordinación efectiva, eficiente y contingente, esto se lograra si se unifican los esfuerzos entre los Red Team y Blue Team. La formación continua del personal de seguridad permitirá remediar amenazas emergentes y una respuesta rápida sobre cualquier incidente que pueda generar se, minimizando el impacto y evitando la propagación de esta. Estas estrategias no solo abordan las vulnerabilidades en entornos físicos, sino que también posicionan a la organización para enfrentar con éxito el panorama cambiante de las amenazas digitales, protegiendo sus activos y la confianza de sus clientes.

Referencias Bibliográficas

Abiri, G. (2025). *Mutually assured deregulation*. In arXiv [cs.CY]. http://arxiv.org/abs/2508.12300

Espinosa Garrido, C. B., & Rosales Roldan, L. (2022). *Marco de Referencia de Ciberseguridad para Dispositivos de IoT Usando la Tecnología de IDS*. Memorias de La Conferencia Iberoamericana de Complejidad, Informática y Cibernética.

Hammouri, Q., Tarawneh, O. A., AlSokkar, A. A. M., Al-Sukkar, A. S., Momani, A., & AlFraihat, S. F. (2025*). Assessing the role of leadership style and budget allocation in cybersecurity project success in the healthcare sector*: The mediating effect of risk mitigation strategies. International Journal of Data and Network Science, 9(4), 727–736. https://doi.org/10.5267/j.ijdns.2025.8.011

Palutla, D. V., Bojjagani, S., Mula, S. C. R., Uyyala, R., Sharma, N. K., Morampudi, M. K., & Khan, M. K. (2025). *aUnveiling Android security testing*: A Comprehensive overview of techniques, challenges, and mitigation strategies. Computers & Electrical Engineering: An International Journal, 127(110620), 110620. https://doi.org/10.1016/j.compeleceng.2025.110620

Vera Mundaca, V. G., & Aquino Trujillo, J. Y. (2023, August 11*). Estrategias de ciberseguridad para hogares inteligentes*: Una revisión sistemática de amenazas y enfoques de mitigación en entornos IoT. Laccei.org. https://laccei.org/LEIRD2024-VirtualEdition/meta/FP307.html

Waseem, M., Ahmad, A., Liang, P., Akbar, M. A., Khan, A. A., Ahmad, I., Setälä, M., & Mikkonen, T. (2025). *Containerization in multi-cloud environment*: Roles, strategies,

challenges, and solutions for effective implementation. The Journal of Systems and Software, 230(112558), 112558. https://doi.org/10.1016/j.jss.2025.112558

Yalçın, G. C., Kara, K., Saygıner, C., Simic, V., & Pamucar, D. (2025). *Selecting cloud providers of infrastructure as a service*: A picture fuzzy symmetry point of criterion-based expert-driven model. Engineering Applications of Artificial Intelligence, 157(111132), 111132. https://doi.org/10.1016/j.engappai.2025.111132

(N.d.-a). Scopus.com. Retrieved September 22, 2025, from https://www.scopus.com/pages/publications/85217229952?origin=resultslist

(N.d.-b). Ssrn.com. Retrieved September 22, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5384360

(N.d.-c). Ssrn.com. Retrieved September 22, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5369241

Gao, X., Wang, Y., Liu, B., Zhou, X., Zhang, R., Wang, J., Niyato, D., Kim, D. I., Jamalipour, A., Yuen, C., An, J., & Yang, K. (2025). *Agentic satellite-augmented low-altitude economy and terrestrial networks*: A survey on generative approaches. In arXiv [cs.NI]. http://arxiv.org/abs/2507.14633

Raza, S., Sapkota, R., Karkee, M., & Emmanouilidis, C. (2025). TRiSM for *Agentic AI*: A review of Trust, risk, and Security Management in LLM-based Agentic Multi-Agent Systems. In arXiv [cs.AI]. http://arxiv.org/abs/2506.04133

Sun, D., Zhang, J., Xu, J., Zheng, Y., Tian, Y., & Li, Z. (2025). From alerts to intelligence: *A novel LLM-aided framework for host-based intrusion detection*. In arXiv [cs.CR]. http://arxiv.org/abs/2507.10873

Waseem, M., Ahmad, A., Liang, P., Akbar, M. A., Khan, A. A., Ahmad, I., Setälä, M., & Mikkonen, T. (2025). *Containerization in multi-cloud environment: Roles, strategies, challenges, and solutions for effective implementation*. In arXiv [cs.DC]. http://arxiv.org/abs/2403.12980

(N.d.). Ssrn.com. Retrieved September 22, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5384360

Apéndices

Apéndice 1

Resultados De Prueba de Turniting