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

FABIO ANDRÉS CARO GARAVITO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
AÑO 2023

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

FABIO ANDRÉS CARO GARAVITO

Asesor:
JOHN FREDDY QUINTERO
Docente

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
AÑO 2023

RESUMEN

En el seminario especializado, Equipos estratégicos de Seguridad Red Team & Blue Team, se distribuyó en 4 etapas en las cuales se desarrollaron una serie actividades que se enfocaron en la investigación, el análisis, la implementación y la aplicación de pruebas obteniendo resultados satisfactorios que fueron debidamente documentados. Estas etapas son:

Etapa 1 - Conceptos equipos de Seguridad: Leyes informáticas en Colombia e instalación banco de trabajo.

Etapa 2 - Actuación ética y legal: Procesos ilegales y no éticos estipulados en un acuerdo de confidencialidad y los artículos de la Ley 1273 del 2009 que se vulneran.

Etapa 3 - Ejecución pruebas de intrusión: RedTeam - Intrusión a sistema operativo Windows con Kali Linux.

Etapa 4 - Contención de ataques informáticos: Implementación, configuración, adaptabilidad y establecimiento de procesos seguros.

Para esto se establecen bancos de trabajo, instalaciones, configuraciones, investigaciones, documentaciones y todo lo necesario para realizar las diferentes etapas que hacen parte de las actividades que le corresponde a un miembro de Blue Team, Red Team y los aspectos legales que debe tener presente al momento de ejercer el cargo en una empresa llamada Whitehouse Security. Los escenarios serán claros y enfocados a lo que se requiere según corresponda.

Se mencionará lo más relevante e importante de lo realizado en cada una de estas etapas, dando así las conclusiones y recomendaciones pertinentes para entender, implementar y reconocer estas situaciones en actividades profesionales futuras.

CONTENIDO

GLOSARIO

Acceso abusivo: Cuando de manera no autorizada o por fuera de lo acordado se accede a todo o parte de un sistema.

Acuerdo de confidencialidad: La forma de legal de comprometerse a no divulgar la información, procedimientos, temas y demás términos que en este se plasme, se maneja mediante un contrato.

Banco de trabajo: Establecer, instalar y configurar las herramientas necesarias para realizar una serie de pruebas, análisis y estudios. Particularmente se intenta simular un escenario y en este se realizan todos los procesos necesarios.

Blueteam: Es el equipo experto en ciberseguridad encargado de analizar un sistema, descubrir fallos, identificar amenazas, posibles ataques que pueda sufrir el sistema y establecer una defensa que ayude a combatir, detener e impedir que los ataques surjan efecto o afecten drásticamente el sistema.

Confiabilidad: Tener la certeza de que algo está funcionando bien y que hace lo que debe hacer.

Contención: Se puede definir como reprimir, detener o neutralizar una acción.

COPNIA: Consejo Profesional Nacional de Ingeniería, encargada de controlar, verificar, inspeccionar y garantizar que la ingeniería se esté desempeñando correctamente. Por medio de esta se gestiona la tarjeta profesional como ingeniero y se conoce el código de ética que debemos respetar como ingenieros. También involucra profesiones a fines y profesiones auxiliares en general.

Disponibilidad: Estado en el que se encuentra algo que puede utilizarse sin ningún problema. Se utiliza para referenciar la existencia y acceso completo para hacer uso cuando se desee.

Ética profesional: Son los valores y las acciones correctas que deben caracterizar a los profesionales cuando estén desempeñando un cargo laboral. Por medio de la ética profesional se identifica la calidad como trabajador o miembro de una organización.

Exploit: Se reconoce la acción cuando se ejecuta algún procedimiento para atacar un sistema, aprovechar errores encontrados o utilizar vulnerabilidades para acceder a un sistema. Un exploit puede ser algo parametrizado, programado, configurado o simplemente una orden para realizar una debida acción.

Hardenización: Consiste en endurecer un sistema (hacerlo más seguro y menos propenso a ataques informáticos) mediante configuraciones, actualizaciones o instalaciones de herramientas que ayuden a fortalecer un sistema, de esta manera se evitan y se reducen las posibilidades de que el sistema sea atacado o que un ataque se materialice.

Intrusión: Infiltrarse o acceder a un sistema de forma no autorizada, por lo general se intenta pasar desapercibido.

Kali Linux: Sistema operativo utilizado para realizar las pruebas se seguridad, auditorías y hacking ético de los sistemas. Cuenta con herramientas que permite realizar estas actividades de una manera más gráfica y obteniendo interfaz de resultados más amigables.

Meterpreter: Es un programa malicioso y utilizado para poder controlar de manera remota un sistema.

Nmap: Herramienta utilizada en sistemas operativos como Kali Linux, la cual sirve para obtener las direcciones IP de una red, los puertos disponibles de los equipos que encuentra en la red, características de sistemas y mucha información que viaja por la red.

Payload: Es lo que ejecutamos cuando activamos un exploit, o sea es lo que se pretende hacer en la vulnerabilidad encontrada.

Plan de contingencia: Prepararse para sucesos que puedan ocurrir, ya sea a nivel geográfico, organizacional, sistemático y que puedan afectar el flujo normal de algo. Todo plan de contingencia tiene un propósito y debe ser estudiado cuidadosamente, ya que si llega a producirse el suceso para el que fue creado y no surge efecto, este será inútil.

Redteam: Es el equipo encargado de actuar como atacantes, con el fin de realizar todos los análisis, descubrir vulnerabilidades, realizar ataques y realizar de una manera ética todo lo que un atacante podría hacerle a un sistema. De esta forma se pueden detectar falencias de seguridad en los sistemas e identificar que hay cosas por hacer. La idea es que constantemente el Redteam esté trabajando y recorriendo lo que más pueda en busca de nuevas falencias.

Vulnerabilidad: Debilidad encontrada en un proceso. Cuando se habla de vulnerabilidad se habla de peligro, de que no está preparada o que no es lo suficientemente capaz para enfrentar algo. Si algo es vulnerable puede ser fácilmente atacado y no solo para destruir sino para utilizarse como acceso al sistema.

Open Source: Software de código abierto el cual puede ser accedido por le Publio en general, por lo que cualquiera puede ver, modificar o distribuir el código.

Footprinting: Es una técnica que se utilizar para recopilar información de un sistema informático y de las entidades a las que este pertenece.

Meterpreter: Programa malicioso y utilizado para poder controlar un sistema de manera remota.

CVE: Este es una lista donde se genera información de vulnerabilidades de seguridad, donde cada referencia se asocia a un identificador.

LISTA DE FIGURAS

INTRODUCCIÓN

Este documento busca dar a conocer las actividades más relevantes de las 4 etapas que se desarrollaron durante el seminario, resaltando principalmente aspectos legales, actividades realizadas como miembros de Redteam y de Blueteam y los respectivos análisis de los resultados y los procesos que se fueron implementando.

Lo anterior permitió identificar herramientas prácticas que se pueden aplicar un entorno real y mediante éstas, fue posible enriquecer de manera significativa, habilidades profesionales en seguridad informática y ciberseguridad que se pueden implementar para dar respuesta, proponer solución y ejecutar las acciones solicitadas en el ámbito laboral.

Todo lo realizado hace parte de un proceso progresivo, el cual conllevo a una serie de técnicas que permitieron establecer la respectiva documentación. De esta manera, el desarrollo del trabajo permite generar una serie de conclusiones y recomendaciones y a la vez, incentiva a continuar explorando en este campo de investigación ciberseguridad, para identificar estrategias que se pueden implementar en casos reales.

OBJETIVOS

OBJETIVOS GENERAL

Dar a conocer aspectos relevantes del trabajo realizado en las etapas que componen el seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, incluyendo aspectos legales que deben considerarse.

OBJETIVOS ESPECÍFICOS

- Reconocer las leyes informáticas que rigen en Colombia.
- Establecer un banco de trabajo para poder realizar las actividades.
- Describir los pasos de hardenización a implementar para evitar ataques de seguridad informática.
- Identificar los procesos ilegales, no éticos y qué artículos de la Ley 1273 del 2009 se están vulnerando en un contrato de confidencialidad.
- Realizar una intrusión a un Sistema
- Diseñar estrategias para contener, hardenizar, actuar, repelar e identificar ataques a un Sistema.
- Implementar acciones metodológicas de seguridad planteadas por el equipo Red team y Blue team

1. DESARROLLO DEL TRABAJO

1.1 ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

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.

- **Ley 1273 de 2009:** esta ley trata de la protección de la información y datos, la cual busca salva guardar toda información o dato sensible o que esta se vea expuesta al público o sistema en general; de igual manera dicha ley tiene como objetivo principal preservar los tres pilares fundamentales de la seguridad informática que son la integridad, la disponibilidad y la confidencialidad de cualquier dato y de cualquier sistema informático.

1.1.1 Capítulo I

- ✓ **Artículo 269A:** Este artículo habla sobre aquel que sin tener permiso o de haber un acuerdo entre las partes acceda a un sistema informático en su totalidad o en parte al mismo el cual cuente con controles de acceso al mismo o no, o que encontrar de la voluntad del que tiene los derechos del sistema informático acceda a él y se mantenga dentro del mismo sin autorización alguna. Se podría incurrir en penas de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- ✓ **Artículo 269B:** Este articulo habla de aquella o aquellas personas que obstaculicen el debido funcionamiento de los sistemas informáticos o una red de datos (telecomunicaciones) o de los datos que se encuentren presentes dentro de la red o sistema. Pero este articulo indica dentro de su contenido lo siguiente:

  El que, sin estar facultado para ello, lo que abre es un interrogante sobre dicho texto **¿eso quiere decir que yo como ingeniero de sistemas y especialista en seguridad informática podría acceder a los sistemas informáticos y a una red de comunicaciones obstaculizarlos y no estaría incurriendo en un delito informático ya que estoy facultado para**

ello? La violación a este articulo daría pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- ✓ **Artículo 269C:** Todo aquel que sin una orden Judicial legitima se atreva a interceptar datos o información sensible en su origen, destino o en el interior de un sistema informático, estaría incurriendo en un delito que con lleva a prisión de treinta y seis (36) a setenta y dos (72) meses.

- ✓ **Artículo 269D:** En este artículo se habla del daño a los sistemas informáticos en cualquiera de sus estructuras física o lógica. Pero también surge el mismo interrogante que en el **Artículo 269B,** ya que habla en su texto **El que, sin estar facultado para ello.** Lo que abre el mismo interrogante **¿si yo estoy capacitado para dañar un sistema informático no estaría incurriendo en delito?**, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. a incurriendo en un delito?, de todas formas, aquella persona o personas que incurran en dicha violación a este artículo incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- ✓ **Artículo 269E:** se habla del uso de software malicioso, aquella persona o personas que desarrollen, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, estarían incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. También se habla de aquellas personas que no estén en la facultado para ello. **¿Si las personas estuvieran facultadas para esto no sería un delito?**

- ✓ **Artículo 269F:** En este articulo tratan de la violación a los datos personales con fines de apropiarse de ellos para vender ofrecer o intercambiar los mismos, ya sea para uso personal o entregarlos a terceros.

- ✓ **Artículo 269G:** Este articulo habla de la suplantación de sitios web o intrusión a un sitio web con el fin de obtener información de este o los datos allí alojados. El que haga esto estaría incurriendo en, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

- ✓ **Artículo 269H:** En este artículo se expone todas las circunstancias que serían graves a los artículos antes mencionados donde se les aumentaría a las tres cuartas partes si esto se cometiera en los siguientes casos:

    a. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

    b. Por servidor público en ejercicio de sus funciones.

    c. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

    d. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

    e. Obteniendo provecho para sí o para un tercero.

    f. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

    g. Utilizando como instrumento a un tercero de buena fe.

    h. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos

1.1.2 Capitulo II

De los atentados informáticos y otras infracciones

- ✓ **Artículo 269I:** en este artículo se habla del hurto informático, donde se indica que el que violando las medidas de seguridad de un sistema informático y estas sean acordes a las señalas en el artículo 239 donde se manipule un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

- ✓ **Artículo 269J:** Se habla de la transferencia sin consentimiento de activos valiéndose de manipulaciones informáticas o algo semejante consiga la

transferencia no consentida de cualquier activo en perjuicio de un tercero[1].

- **Ley 1581 de 2012:** En esta ley se habla de todo lo concerniente al tratamiento de los datos donde todos los colombianos tenemos el derecho que nos otorga la constitución a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

  De acuerdo con la ley estatutaria en mención y de acuerdo al título VII (DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN) capítulo I (De la autoridad de protección de datos), la entidad que regula este proseo es la super intendencia de industria y comercio, en el capítulo II del Título VII

  - ✓ **Artículo 23.** Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

    a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

    b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

    c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

    d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles[2];

---

[1] Secretaría senado. LEY 1273 DE 2009 [En línea] Obtenido de EL CONGRESO DE COLOMBIA. (5 de agosto de 2021). Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[2] Mintic. Ley 1581 (pp. 1-11). (2012) https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

1.1.1.1 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?

De acuerdo con lo investigado las etapas del pentesting son:

A. **Planeación:** es aquí donde se define el alcance que tendrá el proceso de ethical hacking, en esta misma etapa se aprueba la realización de dicha actividad y lo más importante se establecen los acuerdos de confidencialidad.

B. **Descubrimiento:** esta es la fase más amplia en el proceso de ethical hacking, ya que es aquí donde empieza el proceso de recolección de información del objetivo a atacar, esta etapa se divide en tres fases las cuales son:

Footprinting: Es la primera actividad que se debe realizar en una tarea no intrusiva el cual tiene como objetivo poder obtener el máximo de información de la organización y los sistemas informáticos (software, hardware etc.). en esta etapa se aplican técnicas como ingeniería social, búsquedas avanzadas en Google, social Networking a través de sitios como linkedln, Google plus Facebook entre otros. En esta fase podemos utilizar como[3]:

Herramientas open Source

- **OSINT**
- **Maltego CE**
- **Ettercap**
- **Nmap**

Herramientas pagas:

- **Maltego**
- **Intruder**
- **Invicti**

[3] Academy.seguridadcero Obtenido. LAS FASES DEL (ETHICAL) HACKING. Disponible en: https://academy.seguridadcero.com.pe/blog/fases-ethical-hacking. [consultado 05 de julio 2023] [En línea].

A mi modo de ver esta etapa es para mí la más importante ya que de esta parte todo el proceso de hacking ético, por el tema de levantamiento de información de los sistemas informáticos de la empresa.

a. **Escaneo y enumeración:** En esta etapa se realizan búsquedas identificando puertos abiertos, sistemas o servicios activos.

b. **Análisis de vulnerabilidades:** Luego de haber culminado la etapa antes mencionada podemos realizar este punto para ello podemos utilizar herramientas tales como Nessus, Open VAS, IIS Scaner

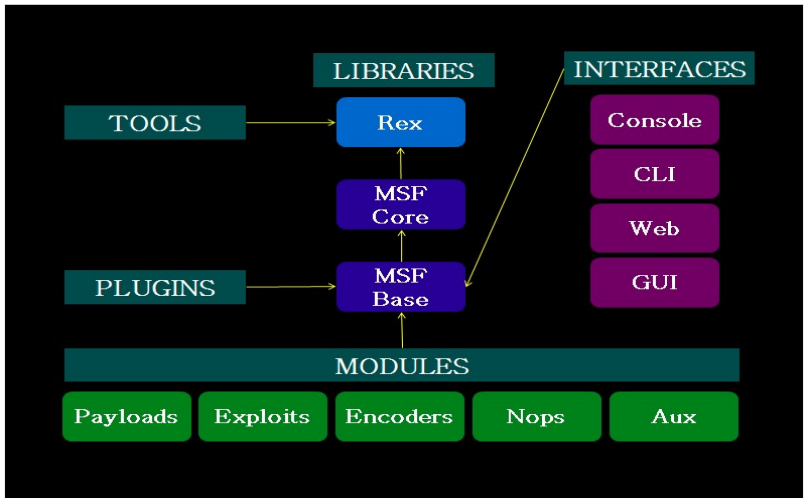
C. **Ataque:** En esta fase es donde se pone en práctica la ejecución de la información recopilada en los pasos anteriores, ya que aquí es donde se hace la intrusión al sistema o sistemas informáticos. Esta fase de divide en dos momentos los cuales son la explotación y la elevación de privilegios de un sistema.

D. **Reporte:** Esta es la última etapa del hacking ético en él se registran todas las evidencias de las actividades desarrolladas dentro de este proceso, las vulnerabilidades detectadas y se realizan recomendaciones de mejora sobre cada proceso y acciones tomas para mejorar la seguridad de los sistemas informáticos.

1.1.1.2 Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

El funcionamiento del frameworks Metasploit es poder buscar las debilidades presentes en un sistema informático, así como también puede escanear y recopilar información de una máquina, pude realizar escala de privilegios, puede Instalar backdoors, Hacer fuzzing o puede hacer evasión de antivirus entre otros.

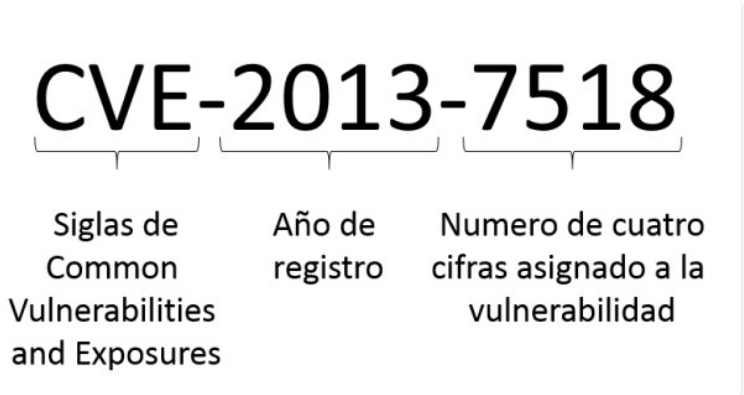
La arquitectura de este framework es:[4]



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:

1.1.1.3 ¿Qué es un CVE y su estructura?

Los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de las fallas de seguridad informática que está disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación de CVE. Donde su estructura es la siguiente



[4] Eduardo. 01 Conociendo Metasploit – Parte I – Exploit Básico. http://curiositysec.com/conociendo-metasploit-parte-i-exploit-basico/index.html

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

A mi modo de ver en esta página se encuentran diferentes exploits que pueden ser aprovechados con cada uno de los CVE o vulnerabilidades ya conocidas en los sistemas informáticos[5].

1.2 ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

¿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.

1.2.1 Análisis de los anexos escenario 2 y acuerdo desde el punto de vista legal y no ético.

En el **anexo 2** es posible evidenciar que la organización **HackerHouse**, propició un contrato elaborado por un abogado, el cual fue despedido de la organización, pues fue descubierto realizando procesos ilegales. Este hecho consistió principalmente en el reclutamiento de equipos **Red Team y Blue Team** para la empresa**.** En su momento la entidad no se percató de la gravedad de los hechos, ni de las consecuencias que este contrato tendría principalmente para sus empleados, pues los ponía en un gran riesgo, el cual se describe a continuación;

- La gerencia general de la empresa no revisó las condiciones contractuales para los empleados nuevos
- Los contratos son entregados sin ninguna modificación.
- No se tuvo en cuenta de quiénes firmarían el contrato, ni de los acuerdos de confidencialidad establecidos para la contratación.

1.2.2 Acuerdos

Consideraciones establecidas entre los firmantes que se nombraron, con acuerdo de confiabilidad previa:

- ✓ Que la información compartida relacionada con el presente acuerdo pertenece a **HackerHouse**, la cual se considera sensible y de

[5] Redhat. El concepto de CVE. [En línea]. [25 de noviembre de 2021] https://www.redhat.com/es/topics/security/what-is-cve

carácter restringido para su divulgación, manejo y utilización. Esta información se comparte con relación al proceso de selección de personal.

- ✓ Que la información propia de **HackerHouse,** se ha obtenido de manera legal, como resultado deprocesos, programas o proyectos y, como resultado de ello, se generan documentos, datos, tecnología y/o material único y confidencial, que es de tipo confidencial a título de secreto industrial.

1.2.3 Párrafos ilegales dentro del acuerdo

- ✓ **Clausura 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****.* Teniendo en cuenta las especificaciones de este acuerdo, se restringen las acciones de divulgación de información confidencial propia de la empresa.

- ✓ **Clausura Segunda.** ***Definición de información confidencial.***

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".*** Este acuerdo restringe el acceso a la entidad receptora a reuniones y documentos que tengan información confidencial.

- ✓ **Clausura Tercera.** ***Origen de la información confidencial:*** *provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible,* ***independiente de su fuente o soporte*** *y sin que requiera advertir su carácter confidencial.* Con este proceso se limita a, incurrir en procesos ilegales los cuales están contemplados en la ley 1273 de 2009 denominado "de la protección de la información y de los datos"

- ✓ **Clausura Cuarta.** ***Obligaciones de la parte receptora****.*

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

Para el **ítem 3**. Deben ser respaldados y aclarados al inicio del contrato que laempresa HackerHouse**,** procederá en donde acontezca a realizar tales denuncias y publicaciones como empresa y no de una manera particular. Al no denunciar o abstenerse, puede incurrir en complicidad de delitos tales, como espionaje, extorciones y secuestro de información.
Clausura Quinta. Obligaciones de la parte reveladora: *Son obligaciones de la parte reveladora.*

b. **Mantener la reserva de la información confidencial hasta tanto.** Se puede analizar que este ítem es inconcluso y se puede malinterpretar en muchas situaciones.

1.2.3.1 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.

1.2.4 Análisis de los anexos, en relación con la vulneración de la ley 1273 argumentando cualquier proceso ilegal.

En el **anexo 3**, en el que se contemplan acuerdos y obligaciones, se evidencian tanto problemas éticos y legales, como explotación, riesgo laboral, violación y abuso de los derechos del contratista, por parte de la empresa HackerHouse. La empresa a pesar de conocer algunos problemas que tenían los contratos no realizó modificaciones a dichas inconsistencias y obligaron a la firma a pasar por alto estos acuerdos.

Luego de exponer lo antes dicho y de acuerdo con lo solicitado en este punto se estaría violando la Resolución 4607 de 2022 del Ministerio del Trabajo.

1.2.4.1 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

1.2.5 Análisis de la propuesta laboral, teniendo presente en cuenta la revisión desde el punto de vista legal y ético.

1.2.5.1 Razones por las cuales no aplicaría a este trabajo.

En mi labor como profesional en ciberseguridad no aplicaría este trabajo de $**17.000.000 y $22.000.000** millones de pesos, pues en algunas cláusulas y acuerdos del contrato, no se especifican las metodologías que se van a utilizar para desarrollar los procesos relacionados con el manejo de la información. Lo anterior genera desconfianza, pues se estaría incurriendo en delitos que pondrían en riesgo mi trayectoria laboral y profesional. A continuación, explico de manera más específica estas razones:

- No pondría en riesgo mi matrícula profesional por aceptar un contrato que va en contra de la ley 1273 de la protección de la información y de los datos y de la ley 842 de 2003 por la cual se Código de Ética Profesional y se dictan otras disposiciones.

- Al ser conocedor de estas acciones ilegales, se aceptarían las cláusulas del contrato en donde se aclara que se aceptan las condiciones asumiendo las responsabilidad y consecuencias que esto traería.

- Este tipo de empresas no brindan seguridad laboral al empleado, pues desde el momento de la contratación buscan vincularlo en cuestiones ilícitas.

1.2.6 Sustentación con el código de ética del COPNIA

- ✓ **Artículo 31. Deberes generales de los profesionales.**

Inciso b): Reza custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados.

Claramente estaría violando este principio, que resultaría en la cancelación de mi tarjeta profesional y el fin de mi carrera como ingeniero.

Inciso f): Reza denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.

Claramente estaría violando este principio, teniendo en cuenta que una de las cláusulas dice que no podría denunciar actos ilegales dentro de la empresa. Que estaría implicando la profesión y mi círculo familiar, social, académico, laboral.

- ✓ **Artículo 32. Prohibiciones generales a los profesionales.**

Inciso b): Reza Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley.

Claramente estaría violando este principio, de abstenerse de denunciar cualquier acto ilegal.

- ✓ **Artículo 34.** prohibiciones especiales a los profesionales respecto de la sociedad.

Inciso a): Reza Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.

Claramente estaría violando este principio, cuando aceptas la clausura o firma el contrato sin antes revisarlo, indica que haría parte al ejercicio ilegal, y en contra del código de ética

Artículo 40. prohibiciones a los profesionales respecto de sus clientes y el público en general.

Inciso a): Reza Ofrecer la prestación de servicios cuyo objeto, por cualquier razón de orden técnico, jurídico, reglamentario, económico o social, sea de dudoso o imposible cumplimiento, o los que, por circunstancias de idoneidad personal, no pudiere satisfacer.

Claramente estaría violando este principio, cuando la empresa HackerHouse, hace la prestación de servicio o entrega de un contrato para reclutar nuevo personal profesional, para equipos Red Tean y Blue Team, pasa por alto las irregularidades o fallas del contrato anterior, también cuando fueron entregados sin modificación alguna.

- ✓ **Artículo 53.** Faltas gravísimas. Se consideran gravísimas y se constituyen en causal de cancelación de la matrícula profesional, las siguientes faltas:

  Inciso d): Reza la utilización fraudulenta de las hojas de vida de sus colegas para participar en concursos, licitaciones públicas, lo mismo que para suscribir los respectivos contratos.

  Claramente estaría violando este principio, en el momento cuando aceptas cualquier irregularidad en los acuerdos del contrato, por esta razón es importante leer antes los que va a realizar y así evitar cualquier proceso delictivo.

  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[6].

1.2.7 Análisis del caso "OPERACIÓN ANDROMEDA BUGGLY".

"OPERACIÓN ANDROMEDA BUGGLY" Desde su posición teniendo en cuenta los aspectos legales y éticos.

BUGGLY, era un local ubicado en el barrio Galerías en Bogotá, donde se ejecutaba interceptaciones operadas por miembros del Ejército y civiles contratados para tareas coordinadas de hackeo, a cuentas de correo y chats de teléfonos. Los objetivos principales eran los equipos negociadores en la habana. ANDROMEDA se le denominaba por la circulación de esta base de operaciones que rodaban en las redes sociales, pero que trabajaba bajo la fachada de Buggly. Buggly era un negocio perfectamente camuflado, contaba con locales divididos en restaurante, sitio de tatuajes, y sala de internet. La intención de que nadie sospechara nada, era un restaurante común y corriente, allí trabajaban tanto militares como hackers civiles.

Entonces Andromeda Buggly fue una operación encubierta en la cual el ejercito mediante mentiras atraía a personal civil para que realizara actos ilegales, el tema se desbordo porque no se contaba con una ética clara para actuar, tanto de civiles como de militares. Esas fueron

[6] COPNIA. (s.f.). CODIGO DE ETICA Obtenido de para el ejercicio de la Ingeniería en general y auxiliares, Disponible en: [En línea] PG 6,17 2015. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etic a.pdf

las pistas que lo delataron para que cayeran en el hecho con las autoridades competentes.

Se muestra una lista de los implicados involucrados que operaban en la banda en el acto, revelada con el fin de la investigación del caso Andrómeda, así:

- Se captura al hacker Andrés Fernando Sepúlveda, quien al parecer compraba y obtenía información valiosa de Buggly, y que además servía a la campaña del candidato presidencial por el centro democrático Oscar Iván Zuluaga, quien había contratado sus servicios, de una manera indirecta.

- Durante la investigación se revela que ocho uniformados no pasaron el polígrafo y otros 20 fueron relevados de sus cargos, 10 oficiales, 8 suboficiales, un patrullero y un civil. Cinco de estos fueron retirados del servicio. A pesar de las irregularidades y faltas disciplinarias, la fachada Buggly estaba totalmente ajustada al marco legal y por consiguiente nunca se salió de lo constitucionalmente legal.

- Los retiros, según el alto mando, fueron de un mayor del ejército y un cabo; y en la Policía, un mayor, un teniente y un patrullero.

En este caso se evidencia una actuación de servidores públicos con pleno conocimiento de los delitos en que se incurrían y las implicaciones legales que tendrían estos delitos. Este caso se penaliza bajo la ley 1273 de 2009 de los delitos informáticos y la ley 842 de 2003 del código de ética en Colombia[7].

1.3 ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

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

Para el desarrollo del escenario 3 se utilizaron las siguientes herramientas:

[7] ANDRÓMEDA. (s.f.). Seguridad Militar: “Seguridad de Personal”; PG1-6 [En línea]. Obtenido de ESTUDIO DE CASO Nº 3 Disponible en: https://curso105.weebly.com/uploads/5/4/8/8/54887311/estudio_de_caso_n%C2% BA_3.pdf Tomado de https://www.elespectador.com/investigacion/de-andromeda-a-los-hackers-article-492933/ . De Andrómeda a los 'hackers'. 17 de mayo de 2014.

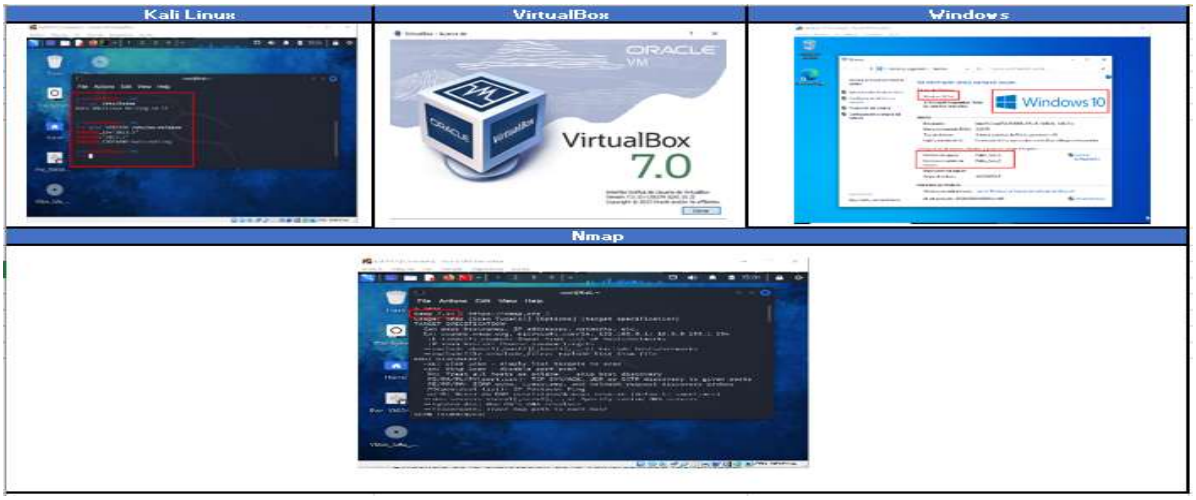
- **Kali Linux 2023.3**: Es una herramienta que se utiliza para la auditoria de seguridad a sistemas informáticos, redes de telecomunicaciones, aplicaciones sistemáticas etc.

- **VirtualBox Versión 7.0.10 r158379 (Qt5.15.2**): es un software que se utilizar para la virtualización de sistemas informáticos, con el fin de simular entornos reales de red.

- **Windows 10 Pro.:** Sistema operativo que sirve para proporcionar un entorno de trabajo visual atractivo, ameno y atractivo, en el que las operaciones básicas de uso del computador están representadas gráficamente a través de íconos.

- **Nmap 7.94:** Programa diseñado para escanear direcciones IP y puertos, también se utiliza para la detección de aplicaciones instaladas en un sistema operativo.

Ilustración 1. Herramientas de software utilizadas



Fuente: propia

1.3.1 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.

De acuerdo con el escenario 3 el administrador del equipo afectado menciono los siguientes datos que a mi modo de ver son los más importantes.

- **Sistemas de seguridad del sistema operativo desactivados (Firewall, Antivirus etc.):** Cuando esto sucede en un sistema operativo se corre el riesgo de que el sistema sea vulnerable a

accesos no autorizados, y que cualesquiera aplicaciones se pueda instalar sin requerir permisos de instalación.

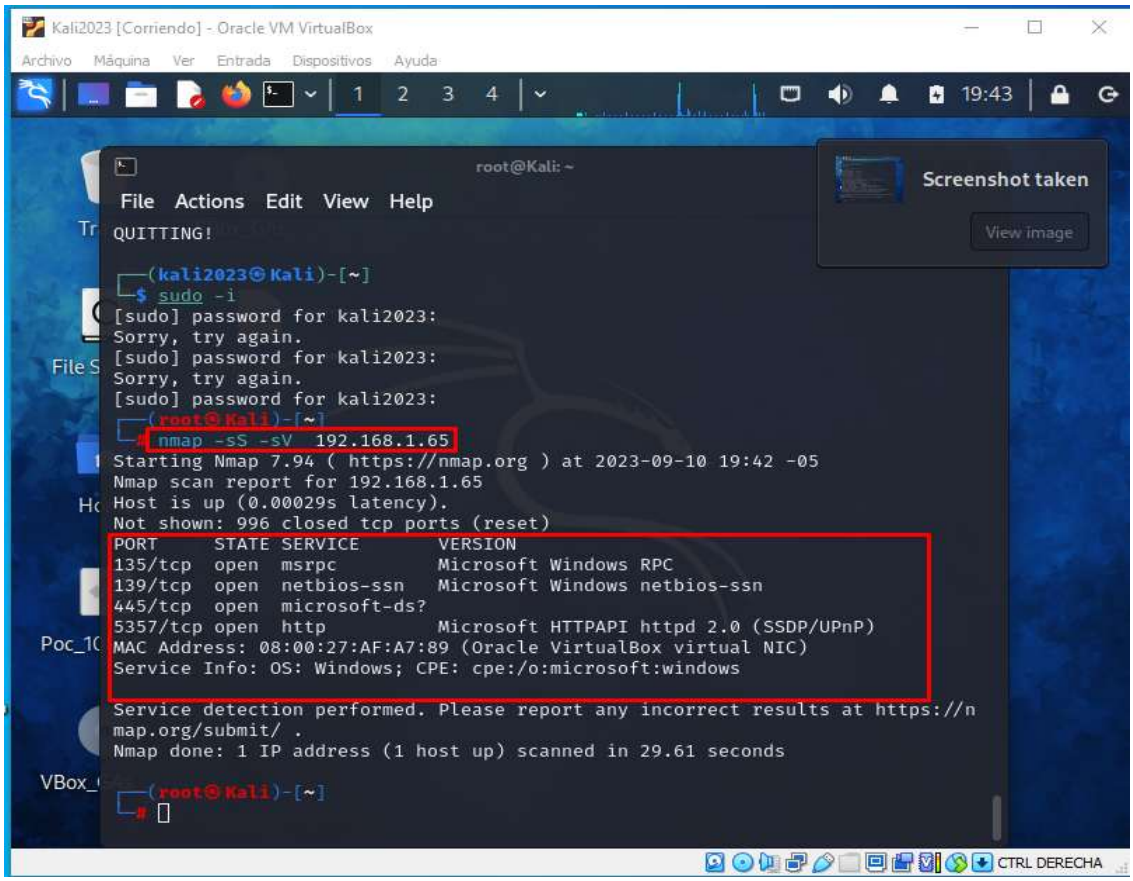
- **Sistemas de seguridad externos desactivados.** Al igual que los del punto antes descrito, tener este tipo de sistemas desactivado puede causar un desastre en cualquier sistema que se encuentre conectado a la red.
- Ejecución de archivo o software de dudosa procedencia.
- Descarga de aplicaciones mediante plataforma de chat web.
- Borrado de información de forma repentina y sin explicación alguna del escritorio.

Este tipo de fallas en los sistemas operativos, están propensos a cualquier Ataque en la red. Pero al que más está expuesto es aún ataque conocido Como zero day, el cual puede explotar los datos de un sistema y también puede llevar a una escalada de privilegios y a su vez puede eliminar archivos sin ningún permiso.

1.3.2 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina windows 10"? ¿qué puerto abre la aplicación específica en el anexo?

Para este escenario se utilizó la herramienta de escaneo de dirección he IPs Llamada Nmap, la cual por medio del comando nmap -sP a la dirección IP 192.168.1.0/24, nos arroga todas las IPs que se encuentran sobre dicha red. Partiendo de esto podemos obtener la maquina victima para este caso se tomó la máquina que virtualbox. Luego de haber conseguido la maquina a tacar se realizó un escaneo, en este caso se utilizó el comando nmap (-sS) que realiza un escaneo de mediante TCP, el cual realiza una verificación completa vía TCP, así mismo se convino con un escaneo de puertos estándar, para no demorar mucho el escaneo mediante el comando (-sV). Tal como se muestra en la siguiente ilustración.

Ilustración 2. Nmap

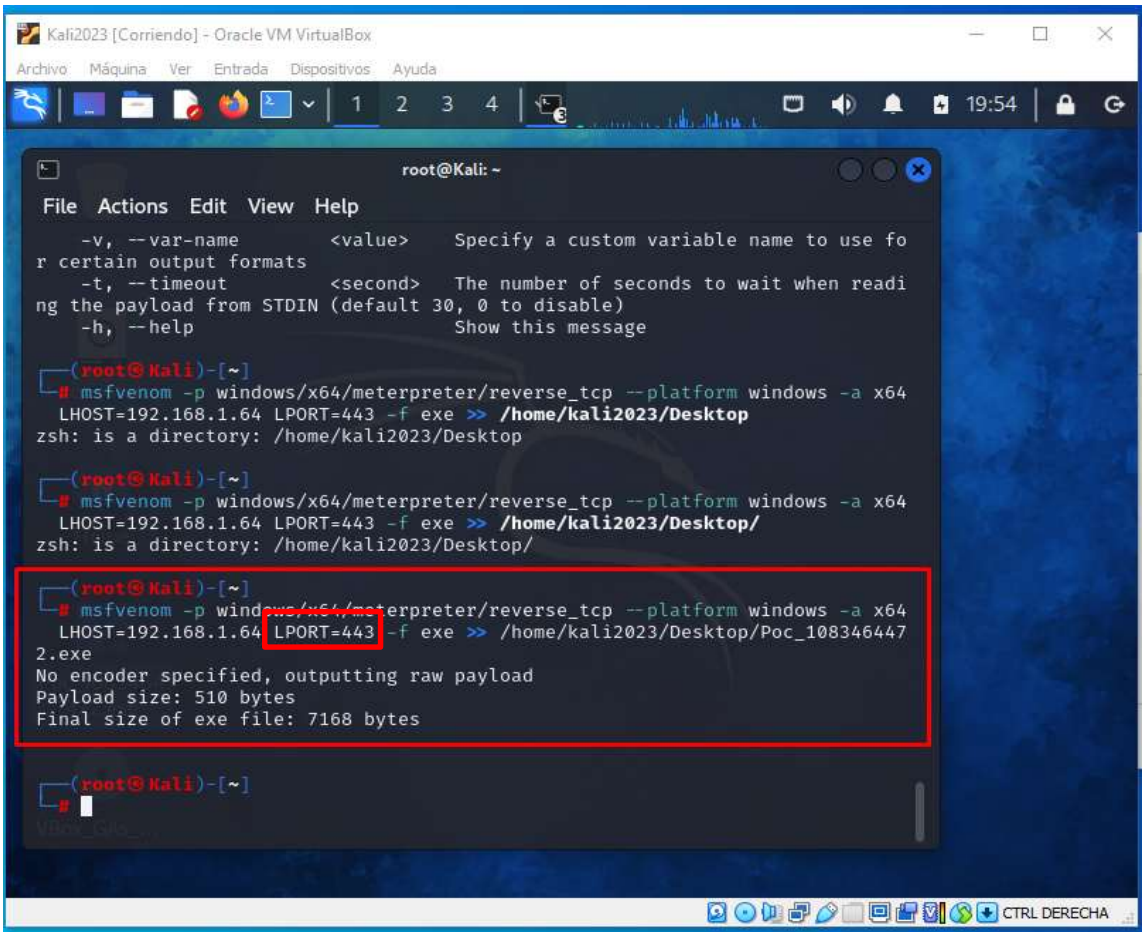


Fuente: propia

1.3.3 ¿Qué puerto abre la aplicación específica en el anexo?

El puerto que abre dicha aplicación es el puerto 443 el cual es el puerto de comunicación segura.

Ilustración 3. Evidencia puerto 443

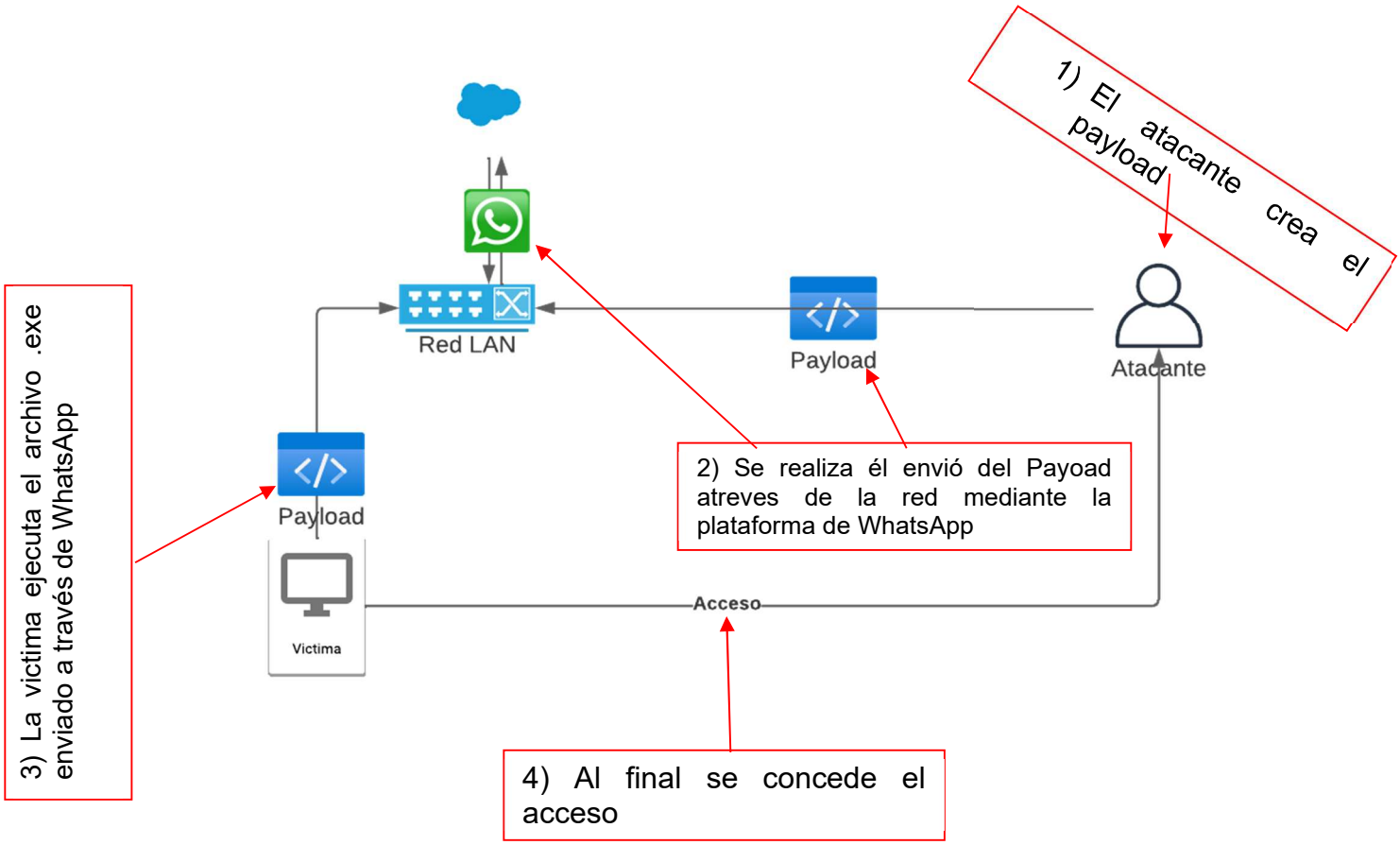


Fuente: propia

1.3.4 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.

Este tipo de ataque afecta la maquina víctima, ya que al ser un payload (carga útil) puede permanecer mucho tiempo en la maquina sin ser detectada y a la espera de que este sea activado y así poder realizar procesos como el mencionado en el ejercicio propuesto el cual fue la eliminación de archivos, también se pueden realizar procesos como robo de datos, vigilancia de la actividades, eliminación o modificación de archivos, descargar nuevos archivos o ejecutar procesos en segundo plano.

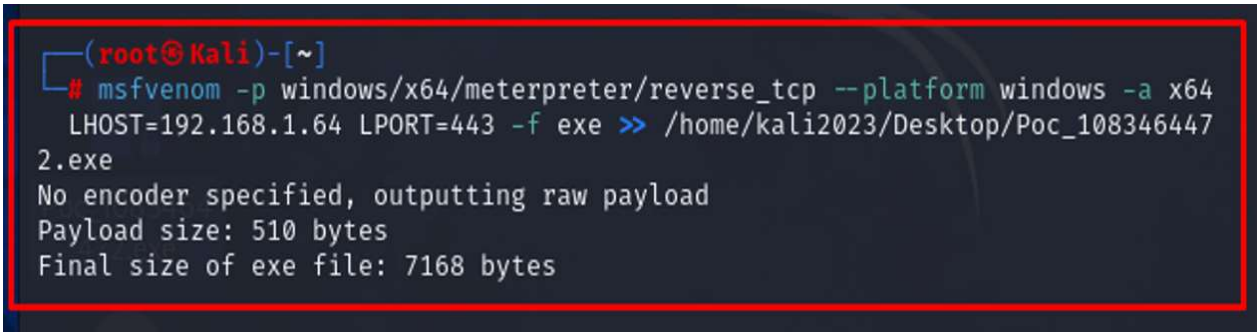
Ilustración 4. Desarrollo del ataque



Fuente: propia

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

Ilustración 5. Estructura del **Payloa**d



Fuente: propia

De acuerdo con la ilustración adjunta se puede evidenciar cada uno de los comandos utilizados y la estructura desarrollada para la creación del payload los cuales son los siguientes:

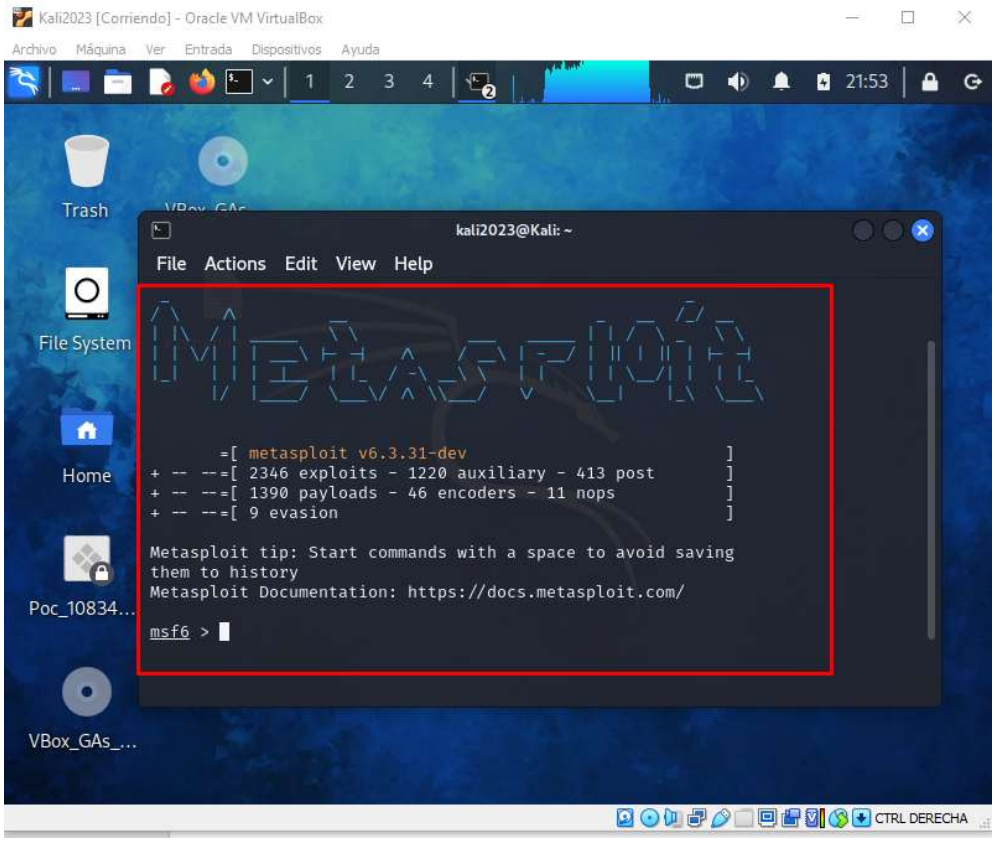
- ✓ **Msfvenom:** esta es una herramienta cuya función principal es la de generar ejecutables con un payload determinado.
- ✓ **-p :** este comando indica la ruta de nuestro payload el cual y para el caso expuesto dice que es una carga útil del tipo meterpreter para sistema Windows de 64 bits con una conexión inversa al puerto tcp
- ✓ **--platform: P**arámetro utilizado para indicar la plataforma que se desea atacar en este caso Windows.
- ✓ **-a:** Indica el tipo de arquitectura que se va a atacar para este caso arquitectura de 64 bits.
- ✓ **LHOST:** Este parámetro incida el host local a utilizar (Kali Linux).
- ✓ **LPORT:** este parámetro indica el tipo de puerto que se va a utilizar para la conexión con la maquina víctima.
- ✓ **-f**: este parámetro se utiliza para la exportación del payload a un ejecutable.
- ✓ **exe**: Indica el formato del archivo.

De acuerdo con lo antes mencionado podemos ver que tenemos un payload el cual se ejecutará en un sistema Windows de 64 bits y a su vez abrirá el puerto 443 para la conexión al sistema mediante dicho puerto.

Comandos para ejecutar el Payload.

- ❖ **Msfconsole:** Abre la consola de metasploit

Ilustración 6. Consola de metasploit



Fuente: propia

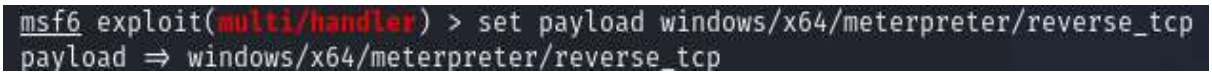
- **use exploit/multi/handler:** Con este comando se elegirá el exploit que ejecutara el payload

Ilustración 7. use exploit/multi/handler

Fuente: propia

- **set payload windows/meterpreter/reverse_tcp** : este comando se utiliza para configurar el tipo de payload que vamos a utilizar.

Ilustración 8. set payload windows/meterpreter/reverse_tcp



Fuente: propia

- **set LHOST**: con este comando indicamos el origen de conexión.

Ilustración 9. set payload windows/meterpreter/reverse_tcp

Fuente: propia

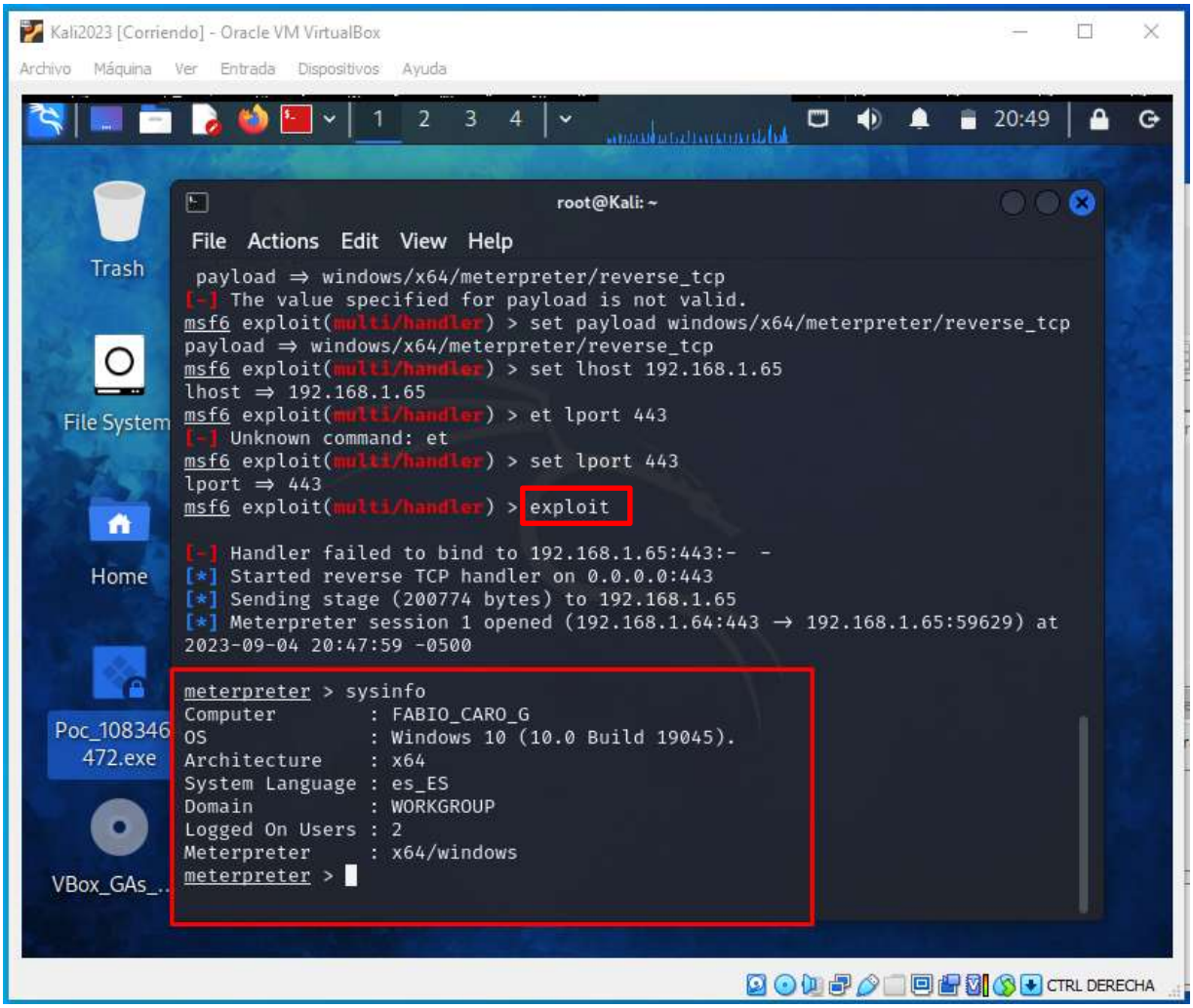
- **set LPORT**: con este comando indicamos el puerto al cual nos conectaremos.

Ilustración 10. set payload windows/meterpreter/reverse_tcp

Fuente: propia

❖ **Exploit:** con este comando ejecutamos el exploit.

Ilustración 11. Exploit

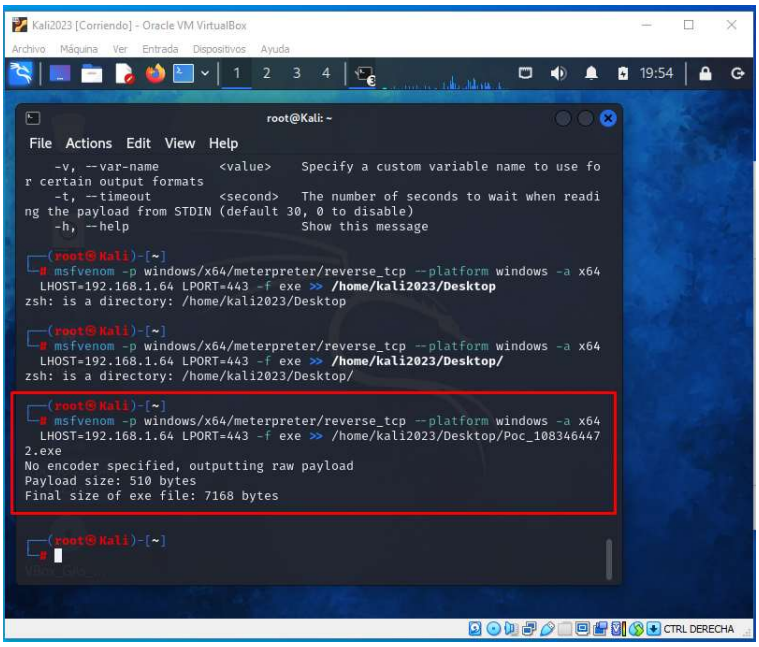


Fuente: propia

1.4 EJECUCION DEL LABORATORIO

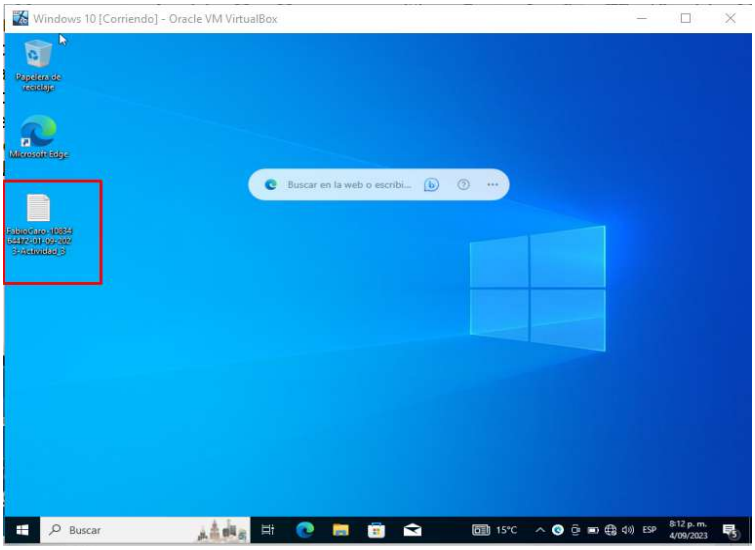
En las siguientes imágenes podemos observar la ejecución del laboratorio propuesto en el anexo 4 escenario 3

Ilustración 12. Ejecución del payload



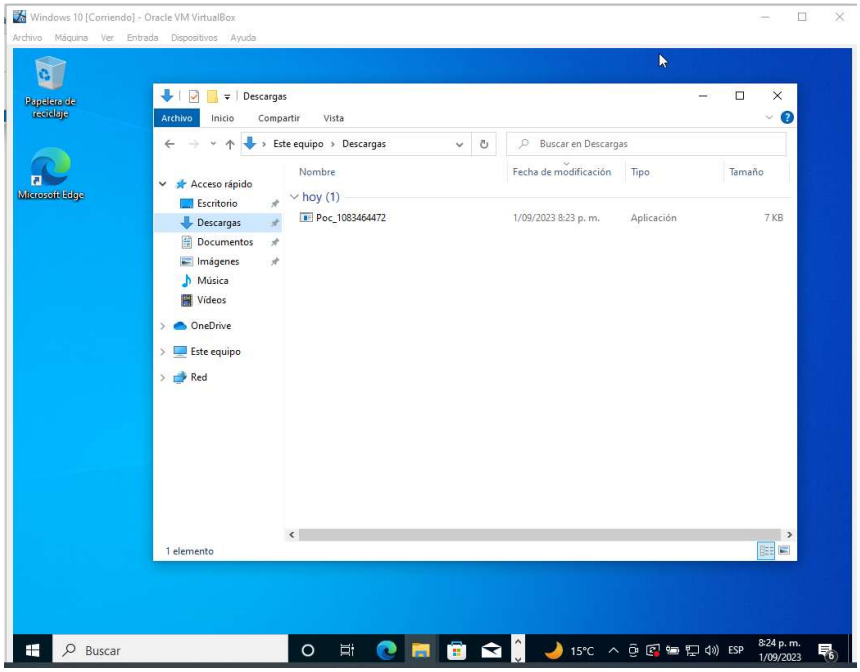
Fuente: propia

Ilustración 13. Evidencia de archivo en sistema Windows.



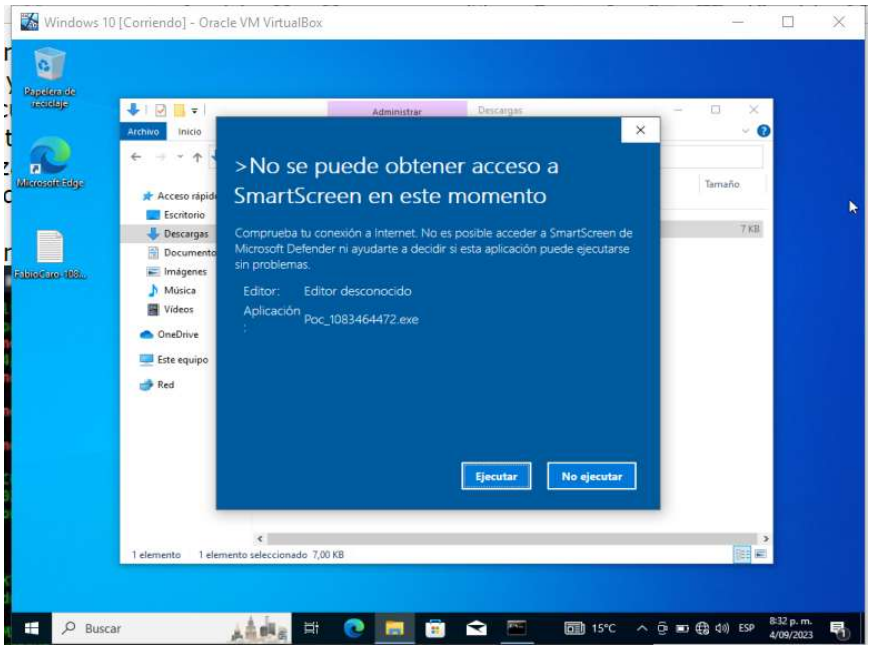
Fuente: propia

Ilustración 14. Descarga de archivo payload en sistema Windows**.**



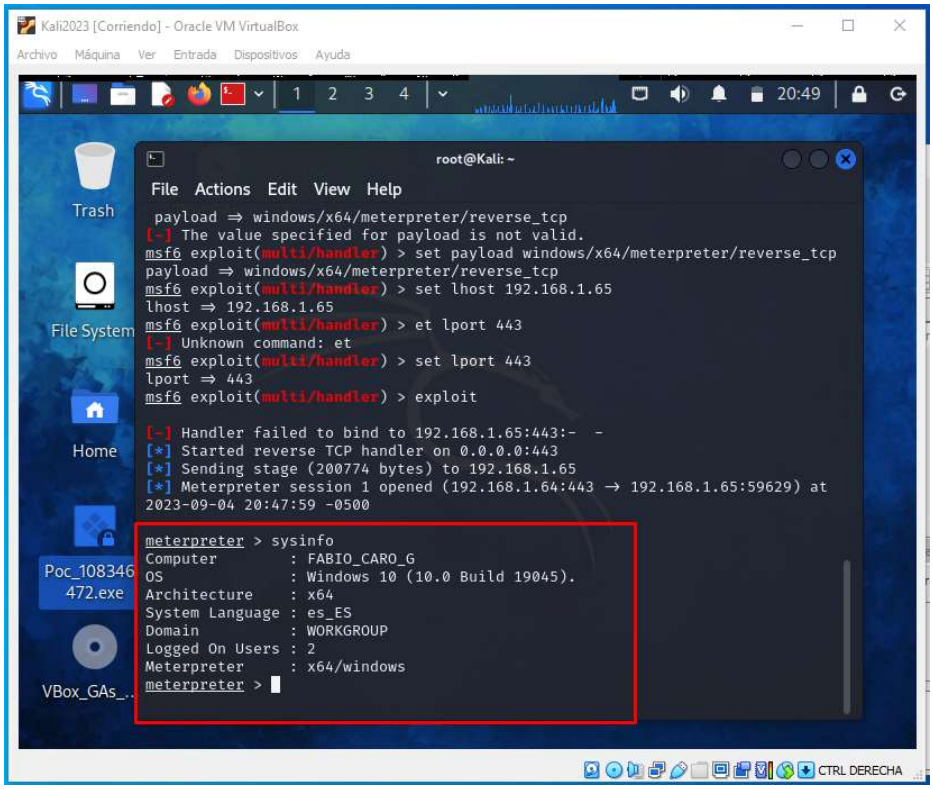
Fuente: propia

Ilustración 15. Ejecución de payload en sistema Windows



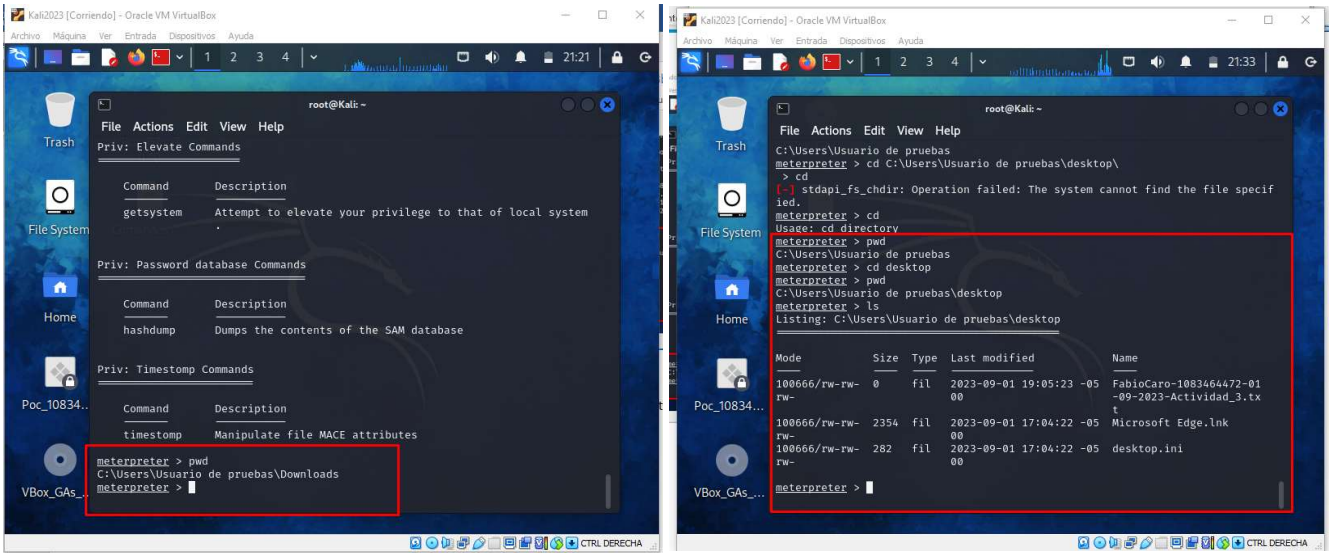
Fuente: propia

Ilustración 16. Conexión a sistema Windows desde Kali Linux



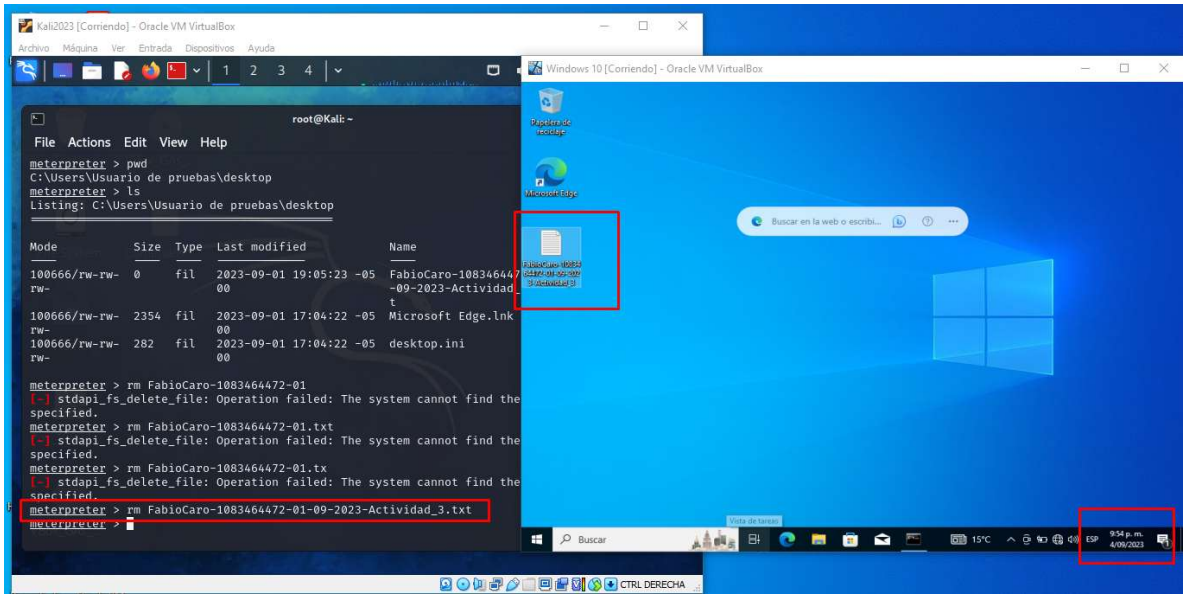
Fuente: propia

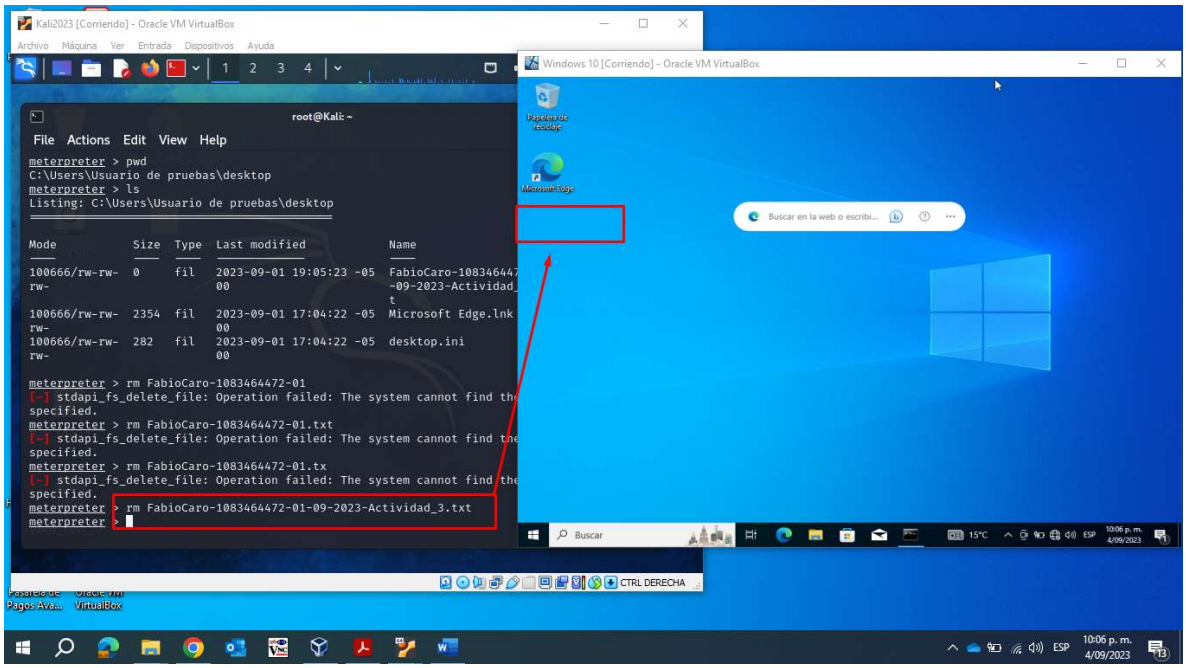
Ilustración 17. Navegación entre los distintos directorios del sistema operativo Windows



Fuente: propia

Ilustración 18. Navegación entre los distintos directorios del sistema operativo Windows





Fuente: propia

1.5 ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

1.5.1 ¿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.

Antes de iniciar es importante resaltar que la mayoría de los ataques no pueden ser detectados en tiempo real, ya que estos son detectados cuando ya han surgido su efecto o logrado su cometido, a esto se suma que los escenarios en los cuales se desarrollan estos eventos pueden variar, lo que nos lleva como especialistas en ciberseguridad estar alertas ante cualquier anomalía que pueda afectar la seguridad de nuestra información en la red.

Dicho lo anterior, cuando se produce un ataque en tiempo real, es porque el equipo atacante está conectado a la misma red del equipo victima ya sea atreves de la red LAN o wifi. Los pasos que yo realizaría en cuanto a este tipo de ataques serían las siguientes:

- Realizar un escaneo a la red para validar que puertos están abiertos, esto con el fin de cerrar los mismos y saber de qué manera se puede estar produciendo el ataque.
- Realizar desconexión del equipo de la red, esto con el fin de que si el ataque se ejecuta en el equipo no vaya a infectar el resto de los equipos conectados a la red.
- Revisar las configuraciones de todos los equipos en la red a nivel de firewall de Windows.
- Revisar que todos los equipos cuenten con antivirus instalado y actualizado a la última versión.
- Realizar desinstalaciones de aplicaciones desconocidas.
- Realizar el cambio de contraseñas de usuarios por otras más robustas.
- Realizar la desinstalación de aplicaciones que no sean licenciadas o en su defecto licenciarlas.
- Realizar la actualización de parches de los distintos sistemas operativos que se tengan en la red. Esto con el fin de evitar algún hueco de seguridad.
- Contratar, instalar o comprar alguna solución Firewall (Fortinet, palo alto pfsense, etc.).

Cabe resaltar que cualquier sistema informático que se conecte a través de una red de datos, está expuesto a sufrir ataques cibernéticos, para no ser víctimas de estos ataques existen muchas técnicas y métodos que nos pueden ayudar a mitigar ser víctimas de estos.

1.5.2 Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

Para prevenir que un ataque de seguridad informática se materialice se pueden implementar las siguientes acciones de Hardening.

- Mantener los sistemas operativos actualizados, Ya sea de forma manual o automática.
- Instalar, activar y actualizar antivirus en los equipos y que estos a su vez ejecuten tareas de escaneo de cualquier aplicación o archivo en tiempo real.
- Mantener activo el firewall de Windows.
- Realizar desinstalación de programas desconocidos o innecesarios.
- Realizar cambios de contraseñas por otras más robustas (alfanuméricas de 12 dígitos como mínimo).
- Mantener los privilegios de acceso de los usuarios controlados (solo debe existir un usuario con privilegios de administrador en la red).
- Realizar listas de chequeo de programas instalados en los equipos.
- Activas copias de seguridad en los equipos.
- Por medios de GPO se debe solicitar el cambio de contraseñas periódicamente.
- Por medio de GPO se debe restringir la instalación de programas a menos que sea un usuario con privilegios elevados.
- Restringir el acceso a puestos USB, DVD entre otras.

1.5.3 ¿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?

De acuerdo con los hallazgos encontrados en el ejercicio de red team los pasos que se realizaron para dicha subsanación fueron los siguientes:

- Se activo el firewall de Windows en el equipo.
- Se activo el antivirus, se actualizo y se licencio.
- Se actualizo el sistema operativo y se licencio el mismo.
- Se realizo cambio de contraseña por una más robusta
- Se implementaron políticas de instalación de programas.
- Se restringió el acceso a internet bloqueando WhatsApp web y otras redes sociales.
- Se realizo escaneo en busca de virus y demás amenazas en el equipo
- Se reviso que no hubiera programas instalados desatendidos.

1.5.4 Sabemos que existen equipos blue team y red team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el purple team y equipos de respuesta a incidentes informáticos?

Blue Team	Red Team	Purple Team	Equipos de respuesta a incidentes informáticos
Los equipos Blue Team se encargan de proteger a la empresa de ataques informáticos de una manera proactiva no solo conteniendo las amenazas actuales sino evaluando posibles amenazas futuras	Ataca el sistema de manera radical para probar la eficacia del programa de seguridad. Este ataque no es avisado para que la defensa sea con máxima objetividad y ver cómo sería un ataque real.	La idea del Purple Team es coordinar y garantizar que los dos equipos de Read Team y Blue Teams compartan información sobre las vulnerabilidades del sistema para lograr una mejora constante. El Purple Team más que un equipo es un coordinador del Blue y Red Tteam.	El Equipo de Respuesta a Incidentes Informáticos son los que reciben los reportes e incidentes de seguridad, analizando la situación y dando una respuesta al incidente
El Blue Team es el que nombramos seguridad defensiva y está formado por profesionales de la seguridad que se encargan de proteger activos críticos de la organización contra cualquier amenaza. Se encarga de defender de manera proactiva ataques reales y programados por el Red Team.	El Red Team es el que nombramos seguridad ofensiva y está formado por profesionales de la seguridad que actúan como adversarios para superar los controles de ciberseguridad. Se encarga de poner a prueba el Blue Team buscando vulnerabilidades.	Este equipo se encarga de enfrentar las técnicas de defensa del Blue Team contra las técnicas de ataque del Red Team. Con este enfrentamiento se logra crear más posibles casos de fallo o ataque y ver si el sistema está funcionando y está preparado correctamente.	El Equipo de Respuesta a Incidentes Informáticos realizan una acción en el momento que se presenta el incidente informático, investigando como se atacó el recurso informático, ayudar a recuperar el mismo y gestionando la vulnerabilidad detectada
El Blue Team tiene como objetivo analizar patrones y comportamientos que salen de lo común. También se encarga de realizar evaluaciones de las distintas amenazas que pueden afectar a la organización, monitorear y recomendar planes de actuación para mitigar los posibles riesgos.	Se suele confundir con la figura del pentesters ya que hay cierta superposición entre sus funciones y habilidades, pero no son lo mismo. Los pentesters realizan un proceso de intrusión con técnicas de pivoting, ingeniería social y otras pruebas de hacking que finaliza con un informe en el que se identifican vulnerabilidades	El principal objetivo del Purple Team es gestionar la seguridad de la organización, realizar pruebas para comprobar la eficacia de los mecanismos y procedimientos de seguridad y definir/desarrollar controles de seguridad adicionales para disminuir el riesgo de la organización.	son normalmente un área de la compañía que se encarga de gestionar los incidentes que se presentan sobre los recursos informáticos

Tabla 1: Diferencias Blue Team, Red Team, Purple Team y respuesta a incidentes[8].

[8] Linkedin. Red Team, Blue Team & Purple Team. Acción, Defensa y Evaluación. [En línea]. [2022]. Recuperado de: https://es.linkedin.com/pulse/red-team-blue-purple-acci%C3%B3n-defensa-y-evaluaci%C3%B3n-tranxfer

1.5.5 ¿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.

CIS Center For Internet Security, tiene como función principal otorgar a través de su banco de información las mejores prácticas en ciberseguridad al equipo de Blue Teams, con el fin de que las organizaciones puedan endurecer la seguridad de sus sistemas informáticos. Es importante mencionar que CIS es una organización sin fin de lucro.

1.5.6 Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: siem y xdr.

SIEM	XDR
Es una solución de seguridad que recopila y analiza información de diferentes fuentes, como sistemas, dispositivos de red y aplicaciones. La información recopilada se utiliza para detectar amenazas de seguridad y alertar a los analistas de seguridad para que investiguen y respondan a ellas.	Es una solución de seguridad que combina la detección y respuesta de amenazas en diferentes fuentes de datos, como endpoints, redes y nubes.
Al elegir una solución SIEM, es importante tener en cuenta la capacidad de la solución para integrarse con diferentes fuentes de información, la escalabilidad de la solución y la capacidad de personalización.	Al elegir una solución XDR, es importante tener en cuenta la capacidad de la solución para integrarse con diferentes fuentes de datos, la escalabilidad de la solución y la capacidad de personalización.
Permitir resolver de manera eficiente y eficaz a cualquier tipo de amenaza	Consolidar una gran cantidad de alertas en un número mucho menor de incidentes que pueden priorizarse para la investigación manual.
Analizar en tiempo real ataques que se presente en el hardware y/o software, alertando según el progreso de la amenaza	Ofrecer opciones integradas de respuesta a incidentes que proporcionen un contexto suficiente para que las alertas se puedan resolver rápidamente
Minimizas la afectación del ataque en tiempos cortos	Proporcionar opciones de respuesta que se extiendan más allá de los puntos de control de la infraestructura, incluida la red, la nube y los endpoints, para ofrecer una protección integral
Visualizar los proceso y procedimientos de la seguridad en los sistemas teleinformáticas	Automatizar las tareas repetitivas para mejorar la productividad

1.5.7 Defina por lo menos 3 herramientas de detección de ataques Informáticos con licencia gpl.

A continuación, se listan las herramientas de detección de ataques informáticos con licencia GPL.

- **SNORT:** Permite realizar análisis y registros de los paquetes en tiempo real; logra identificar ataques DoS y DDoS. Su utilidad principal es detectar exploits y exploración de puertos. Analiza el tráfico de la red y si existe algún tipo de amenaza bloquea el ataque.

- **Pfsense:** este es un programa de código abierto que nos permite tener un firewall en software, lo que quiere decir que lo podemos instalar en un equipo físico de las características de nuestra elección, además de ello Pfsense, este firewall se puede clasificar como UTM (unified threat management), lo que se traduce como gestión unificada de amenazas.

- **OPENWIPS:** Permite la detección y prevención de ataques en el sistema inalámbrico que se presenta en sensores donde se detectan amenazas, manejo de tráfico para su análisis y caracterización del sistema de seguridad; interfaces de red inalámbricas permitiendo analizar ataques que pueda ser expuesto; y servidores que se generan las aletas y respuesta ante algún tipo de amenaza, permite analizar la información envida por los sensores.

1.6 ETAPA 5 - SOCIALIZACIÓN DE INFORME TÉCNICO

1.6.1 De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.

Si una organización tiene implementado estos tres grupos de seguridad es poco probable que una organización sea víctima de cualquier ataque a su red o infraestructuras informáticas. Además, podrán implementar distintas defensas contra cualquier ataque informático

1.6.2 Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos TI.

las políticas de seguridad que se deberían aplicar en cualquier entidad son las siguientes:

a. No permitir que la información sensible de la organización se pueda mover en pendrives, si esto es así asegurarse que la misma vaya encriptada.
b. No abrir enlaces de dudosa procedencia en correos electrónicos de la organización ni mucho menos permitir la apertura de correos personales en los equipos de la organización.
c. Encriptar los archivos y colocarles claves con complejidad alta
d. Tener precaución a la hora de descargar cualquier tipo de archivos de internet.
e. Mantener actualizado el antivirus.
f. Crear políticas restrictivas dentro de la red.
g. Mantener todos los software actualizados.
h. No abrir correos de dudosa procedencia.
i. Implementar métodos de doble autentificación.

1.6.3 Conclusiones que orienten aspectos importantes en cuanto a la inversión de ciberseguridad dentro de las organizaciones, deben tener en cuenta cada una de las etapas que se ejecutaron a lo largo del seminario para poder ejecutar estas conclusiones y soportar a la alta gerencia la necesidad de inversión.

Debido a la gran dependencia tecnológica que hay en la actualidad, los países clasifican su infraestructura teniendo en cuenta principalmente el grado de importancia para su normal funcionamiento de la información, de manera tal que los activos de mayor valor son catalogados como infraestructura crítica.

De acuerdo con el Departamento de Seguridad Interna de los Estados Unidos por sus siglas en inglés (DHS), la infraestructura crítica corresponde a “los activos, sistemas y redes, ya sea físicos o virtuales, cuyo impacto o destrucción tendría un efecto debilitador sobre la seguridad nacional, la economía, la salud pública, o cualquier combinación de los mismos” (U.S Department of Homeland Security, 2014). Así mismo, establece 13 macro-sectores que congregan las infraestructuras críticas así: financiero, servicios, investigación y desarrollo, tecnologías de la información y las telecomunicaciones, transporte, agua, energía, salud pública, servicios de emergencia, químicos, servicios postales y monumentos nacionales.

CONCLUSIONES

De la etapa 1 concluimos la importancia de conocer las leyes y artículos sobre el tratamiento de datos y las consecuencias que conllevaría la violación de estas. Por otra parte, se puede comprender más a detalles la importancia que tiene la realización de un haking ético a un sistema informático, así como las fases presentes dentro de este y las herramientas que se pueden utilizar para llevar a cabo este.

De la etapa 2 se puede concluir Como profesional y especialista en seguridad informática, considero que para desempeñar nuestra labor es fundamental conocer las leyes que rigen la práctica informática, la ley 1273 del 2009, y la ley 842 de 2003. Estas leyes son indispensables para evitar que un profesional en seguridad informática conozca las implicaciones de una contratación y sepa cómo actuar ante cualquier irregularidad por parte del contratante.

Es importante mencionar que para cualquier profesional lo más importante debe ser el actuar de manera ética en todos los ámbitos en que se desempeñe.

De la etapa 3 se puede concluir que en la actividad de Red Team, se desarrollaron habilidades en el manejo practico de herramientas GNU para la realización de pentesting que dio como resultado la explotación de una vulnerabilidad presente en la maquina víctima, en un ambiente controlado, el cual nos mostró de manera real lo que se puede lograr en una máquinas u organizaciones, si no se toman las medidas de seguridad necesarias para mantener los sistemas seguros, actualizados y libres de amenazas.

En la etapa 4 concluimos la importancia de poder salva guardad los sistemas informáticos de una organización utilizando las distintas herramientas que existen en el mercado actualmente y que son de uso libre, las cuales son tan buenas o mejores que una paga. A demás de ellos se logró comprender la importancia de los equipos Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes informáticos y la importancia de contar con ellos dentro de una organización.

BIBLIOGRAFÍA

academy.seguridadcero. [consultado 05 de julio 2023] [En linea]. Obtenido. LAS FASES DEL (ETHICAL) HACKING. Disponible en: https://academy.seguridadcero.com.pe/blog/fases-ethical-hacking

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

ANDRÓMEDA. (s.f.). Seguridad Militar: “Seguridad de Personal”; PG1-6 [En linea]. Obtenido de ESTUDIO DE CASO Nº 3 Disponible en: https://curso105.weebly.com/uploads/5/4/8/8/54887311/estudio_de_caso_n%C2%BA_3.pdf

CIS – CENTER FOR INTERNET SECURITY. CIS Controls – Spanish Translation. 7a versión. Año no disponible. Disponible en: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

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

Concepto. Windows. [En línea]. [Consultado 10 de septiembre de 2023]. Disponible en: https://concepto.de/windows-2/#:~:text=La%20funci%C3%B3n%20b%C3%A1sica%20de%20Windows,gr%C3%A1ficamente%20a%20trav%C3%A9s%20de%20%C3%ADconos

COPNIA. (s.f.). CODIGO DE ETICA [En linea] PG 6,17 2015. Obtenido de para el ejercicio de la Ingeniería en general y auxiliares, Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Eduardo. 01 Conociendo Metasploit – Parte I – Exploit Básico. [En línea]. [consultado 13 de agosto 2023] http://curiositysec.com/conociendo-metasploit-parte-i-exploit-basico/index.html

Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. Recuperado de: https://www.incibe-cert.es/blog/owasp-4

JASWAL. Nipun. Vulnerability analysis of HFS 2.3. En: Mastering Metasploit. 2a. ed. 2016. Disponible en: https://subscription.packtpub.com/book/networking_and_servers/9781786463166

Linkedin. Martinez, L. SIEM vs SOAR vs XDR: ¿Cuáles son las diferencias y cuál es el adecuado para tu organización?. [En línea]. [2021]. Recuperado de: https://es.linkedin.com/pulse/siem-vs-soar-xdr-cu%C3%A1les-son-las-diferencias-y-cu%C3%A1l-es-luis-jos%C3%A9

Linkedin. Red Team, Blue Team & Purple Team. Acción, Defensa y Evaluación. [En línea]. [2022]. Recuperado de: https://es.linkedin.com/pulse/red-team-blue-purple-acci%C3%B3n-defensa-y-evaluaci%C3%B3n-tranxfer

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

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

Redacción KeepCoding. ¿Qué es Metasploit?. [En línea]. [05 de julio 2023]. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Redhat. El concepto de CVE. [En línea]. [25 de Noviembre de 2021] https://www.redhat.com/es/topics/security/what-is-cve

RSI SECURITY. What is the Center for Internet Security (CIS)?. [Sitio Web]. [03, julio, 2020]. Disponible en: https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/

Secretariasenado. (5 de Agosto de 2021). LEY 1273 DE 2009 [En linea] . Obtenido de EL CONGRESO DE COLOMBIA Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

1000tipsinformaticos. Una nueva vulnerabilidad Zero Day en Windows puede eliminar archivos en tu sistema. [En línea]. [Consultado 10 de septiembre de 2023]. Disponible en: https://www.1000tipsinformaticos.com/2018/10/vulnerabilidad-zero-day-en-windows-10-puede-eliminar-archivos.html

Tomado de https://www.elespectador.com/investigacion/de-andromeda-a-los-hackers-article-492933/ . De Andrómeda a los 'hackers'. 17 de mayo de 2014.