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

FAVIO CIRANICICUA PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
abril de 2024

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

PRESENTADO POR:
FAVIO HERNANDO CIRANICICUA

PRESENTADO A:
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO EQUIPOS ESTRATEGICOS DE CIBERSEGURIDAD
BOGOTA
abril de 2024

Tabla de contenido

1. INTRODUCCIÓN 7

2 OBJETIVOS 8

Objetivos General **8**

Objetivos Específicos **8**

3 RESUMEN 9

4 GLOSARIO 10

5 MARCOS REGULATORIOS EN COLOMBIA 11

5.1 ley 1273 de 2009 **11**

5.2 ley 1581 de 2012 **12**

5.3 Entidad reguladora ley 1581 de 2012 y multas **13**

6 PENTESTING 14

7 METASPLOIT 15

5.1CVE **15**

8 BANCO DE TRABAJO 16

9 ANÁLISIS ESCENARIO PLANTEADO – ACUERDO DE CONFIDENCIALIDAD 21

9.1 Párrafos ilegales dentro del acuerdo de confidencialidad **21**

9.2 Leyes colombianas violentadas en el acuerdo de confidencialidad **22**

9.3 COPNIA, CÓDIGO DE ÉTICA Y SANCIONES **22**

10 CIBERCRIMEN EN COLOMBIA – ATAQUE INFORMÁTICO INVIMA 23

11 HERRAMIENTAS DE INTRUSIÓN 25

11.1 MFSVENOM **25**

11.2 POC ATAQUE **26**

12 IDENTIFICACIÓN DE UN ATAQUE INFORMÁTICO 35

13 PASO A PASO PARA SUBSANAR EVENTO DEL PAYLOAD 36

14 RED TEAM / BLUE TEAM / PURPLE TEAM / EQUIPO DE RESPUESTA ANTE INCIDENTES INFORMATICOS 38

15 CIS “CENTER FOR INTERNET SECURITY” 40

16 SIEM - XDR 41

17 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL 43

18 LINK VIDEO 43

19 CONCLUSIONES 44

20 BIBLIOGRAFÍA 45

LISTA DE FIGURAS

Figura 1 Virtual Box 16
Figura 2 Windows 10 17
Figura 3 Desactivacion seguridad windows 17
Figura 4 Kali Linux 18
Figura 5 Comunicacion máquinas de prueba 19
Figura 6 comunicacion kali linux 19
Figura 7 comunicacion windows 10 20
Figura 8 segmentos de red máquinas 27
Figura 9 Respuesta comunicacion máquinas 27
Figura 10 desactivacion controles seguridad 28
Figura 11 desactivacion firewall 28
Figura 12 Creacion payload 29
Figura 13 gestion archivos kali 29
Figura 14 Gestion de archivos kali 2 30
Figura 15 ejecución servicio apache 30
Figura 16 prueba html 31
Figura 17 descarga payload 31
Figura 18 mfs console 32
Figura 19 payload y consola 32
Figura 20 descarga archivo malicioso 33
Figura 21 Control máquina victima 33
Figura 22 Control Máquina victima remoto 34
Figura 23 Descargas máquina victima 34
Figura 24 Eliminación evidencia 34

LISTA DE TABLAS

Tabla 1 Ley 1273 de 2009 11
Tabla 2 Ley 1581 de 2012 12
Tabla 3 Caracteristicas técnicas 20
Tabla 4 Red team blue team..... 38
Tabla 5 Siem -Xdr..... 41

1. INTRODUCCIÓN

La contención de ataques informáticos se ha convertido en una prioridad estratégica para gobiernos, empresas y organizaciones de todo tipo. La capacidad de detectar, responder y mitigar rápidamente los ataques informáticos es fundamental para minimizar su impacto y proteger la integridad, confidencialidad y disponibilidad de los sistemas de información. Sin embargo, la naturaleza en constante evolución de las amenazas cibernéticas y la creciente sofisticación de los actores maliciosos plantean desafíos significativos para el diseño e implementación de estrategias efectivas de contención de ataques informáticos.

Los especialistas en seguridad informática deben comprender, afianzar y determinar los mejores métodos y herramientas a utilizar dependiendo del contexto del ataque, con el fin de tener un tiempo de respuesta adecuado frente a los ataques informáticos.

2 OBJETIVOS

Objetivos General

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI

Objetivos Específicos

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Comprender las diferencias entre equipos Red Team, Blue Team y Purple Team, y sus diferentes funciones en una organización.

Analizar herramientas de monitorización y detección de eventos de seguridad tales como SIEM, XDR.

3 RESUMEN

Este informe técnico tiene como objetivo evaluar las acciones de los equipos Red Team y Blue Team en el marco de los criterios éticos y legales en una organización. Se busca comprender y analizar las prácticas utilizadas por estos equipos, así como identificar posibles vulnerabilidades en los sistemas informáticos mediante el uso de metodologías y técnicas de intrusión.

En primer lugar, se destacan las diferencias entre los equipos Red Team y Blue Team, así como su función dentro del entorno de seguridad cibernética de una organización. Los equipos Red Team están dedicados a identificar y explotar vulnerabilidades en el sistema, mientras que los equipos Blue Team se centran en la detección y mitigación de amenazas.

Se procede a demostrar cómo los equipos Red Team pueden identificar y explotar vulnerabilidades en el sistema informático de una organización, mientras que los equipos Blue Team trabajan en la detección y mitigación de dichas vulnerabilidades. Este proceso se lleva a cabo mediante el uso de técnicas de intrusión, simulando ataques reales para evaluar la seguridad del sistema.

Además, se realiza un análisis detallado de herramientas de monitorización y detección de eventos de seguridad, tales como SIEM y XDR. Estas herramientas son fundamentales para la detección temprana de amenazas y la respuesta eficaz a incidentes de seguridad.

El informe concluye resaltando la importancia de mantener un equilibrio entre la seguridad cibernética y el cumplimiento ético y legal. Se subraya la necesidad de que las organizaciones implementen prácticas de seguridad cibernética que cumplan con los estándares éticos y legales, garantizando así la protección de sus activos digitales.

PALABRAS CLAVES

Incidente de seguridad, Payload, Red Team, técnicas de intrusión, vulnerabilidades

4 GLOSARIO

Equipos Red Team: Equipos dedicados a simular ataques cibernéticos contra los sistemas de una organización para identificar y explotar vulnerabilidades.

Equipos Blue Team: Equipos encargados de la defensa y protección de los sistemas de una organización, así como de la detección y mitigación de amenazas cibernéticas.

Metodologías de intrusión: Procesos y técnicas utilizados por los equipos Red Team para simular ataques cibernéticos, identificar vulnerabilidades y evaluar la seguridad de un sistema.

Vulnerabilidades: Debilidades en un sistema informático que pueden ser explotadas por atacantes para comprometer la seguridad de la organización.

SIEM (Security Information and Event Management): Plataforma de seguridad que recopila y analiza datos de eventos de seguridad en tiempo real para detectar amenazas y responder a incidentes.

XDR (Extended Detection and Response): Plataforma de seguridad que combina la detección y respuesta de amenazas avanzadas con capacidades extendidas de análisis de datos y correlación de eventos.

Simulación de ataques: Práctica de simular ataques cibernéticos reales contra los sistemas de una organización para evaluar su seguridad y preparación para enfrentar amenazas.

Cumplimiento ético y legal: Adherencia a estándares éticos y normativas legales en el ámbito de la seguridad cibernética, garantizando el respeto de la privacidad y los derechos de los usuarios.

Seguridad cibernética: Conjunto de medidas y prácticas destinadas a proteger los sistemas informáticos y los datos de una organización contra ataques y amenazas cibernéticas.

Incidente de seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de los datos y sistemas de una organización, requiriendo una respuesta inmediata y adecuada.

5 MARCOS REGULATORIOS EN COLOMBIA

5.1 LEY 1273 DE 2009

La ley 1273 de 2009 modifica el código penal colombiano y crea un nuevo bien jurídico denominado “de la protección de la información y lo datos”. Esta ley se divide en dos capítulos.

El capítulo I, define 8 acciones que se toman como delito en cuanto a la utilización de los datos y de los sistemas de información:

Tabla 1 Ley 1273 de 2009

Artículo	Descripción	Penalización
269A acceso abusivo a un sistema informático.	Acceso a un sistema informático sin autorización.	Prisión:48 a 96 meses Multa: 100 a 1000 SMLMV
269B Obstaculización ilegitima de sistema informático o red de telecomunicación.	Obstaculizar el acceso normal a un sistema informático o redes de telecomunicaciones sin autorización	Prisión:48 a 96 meses Multa: 100 a 1000 SMLMV
269C Interceptación de datos informáticos.	Interceptar cualquier tipo de comunicación sin una orden judicial	Prisión:36 a 72 meses
269D Daño informático	Dañar. O suprimir datos informáticos o de un sistema de información sin autorización.	Prisión:48 a 96 meses Multa: 100 a 1000 SMLMV
269E Uso de software malicioso	Utilización de cualquier software dañino sin autorización.	Prisión:48 a 96 meses Multa: 100 a 1000 SMLMV
269F Violación de datos personales	Manejo de información personal sin previa autorización.	Prisión:48 a 96 meses Multa: 100 a 1000 SMLMV
269G Suplantación de sitios web para capturar datos personales	Utilización de paginas emergentes o fraudulentas para capturar datos	Prisión:48 a 96 meses Multa: 100 a 1000 SMLMV

El capítulo I, define 2 acciones que se toman como delito en cuanto a la utilización de los datos y de los sistemas de información:

Artículo	Descripción	Penalización
269I Hurto por medios informáticos y semejantes	Robo de información.	Prisión:48 a 96 meses Multa: 100 a 1000 SMLMV
269H Transferencia no consentida de activos	Transferencia no consentida de datos y/o sistemas de información con animo de lucro	Prisión:48 a 120 meses Multa: 200 a 1500 SMLMV

Fuente:elaboración propia

5.2 LEY 1581 DE 2012

La ley 1581 regula el manejo de la información personal y la protección de datos personales, se componen de 11 títulos:

Tabla 2 Ley 1581 de 2012

Titulo	Descripción
OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES	La ley tiene como objetivo garantizar el derecho fundamental de la privacidad de las personas y establecer las reglas para la recolección, almacenamiento, y protección de datos personales.
PRINCIPIOS RECTORES	La ley establece una serie de principios que deben guiar el tratamiento de datos personales, como el principio de finalidad, consentimiento, etc.
CATEGORÍAS ESPECIALES DE DATOS	La ley reconoce ciertas categorías de datos personales que son consideradas como sensibles debido a su naturaleza y la posible afectación a la privacidad de las personas.
DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS	aborda los derechos de los titulares de datos y las condiciones legales para el tratamiento de la información personal

PROCEDIMIENTOS	reconoce el derecho de los titulares de datos personales a conocer, acceder, rectificar y suprimir la información que las entidades o responsables del tratamiento tengan sobre ellos. establece la posibilidad de presentar reclamos ante la Superintendencia de Industria y Comercio en caso de considerar que se ha incurrido en violaciones a la ley
DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO	Los responsables y encargados deben adherirse a los principios establecidos en la ley, como el principio de finalidad, consentimiento, veracidad, seguridad y confidencialidad, entre otros
DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN	La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley

Fuente:elaboración propia

5.3 ENTIDAD REGULADORA LEY 1581 DE 2012 Y MULTAS

los rangos de multas que pueden ser impuestas por la Superintendencia de Industria y Comercio (SIC) en Colombia en caso de violaciones a la normativa de protección de datos personales. Estos rangos pueden variar según la gravedad de la infracción y otros factores. A continuación, te proporciono los rangos generales de multas establecidos por la ley:

Multas Leves: Hasta 2,000 salarios mínimos legales mensuales vigentes.

Multas Graves: De 2,001 a 4,000 salarios mínimos legales mensuales vigentes.

Multas Muy Graves: Más de 4,000 salarios mínimos legales mensuales vigentes.

6 PENTESTING

El pentesting, es un proceso que simula un ataque informático que tiene como objetivo evaluar la seguridad de un sistema informático, las fases de este proceso son las siguientes:

Reconocimiento (FootPrinting): En esta fase, se recopila información sobre el objetivo del test. Esto puede incluir la identificación de sistemas, servicios, direcciones IP, y cualquier información pública disponible sobre la infraestructura.

Recolección de Información (Information Gathering): Aquí se recopila información más detallada sobre el objetivo, incluyendo detalles técnicos sobre la red, sistemas operativos, servicios en ejecución, y posibles vulnerabilidades.

Enumeración (Enumeration): Durante esta fase, se intenta obtener información más específica sobre los sistemas identificados, como usuarios, grupos, permisos y recursos disponibles en la red.

Análisis de Vulnerabilidades (Vulnerability Analysis): Se identifican y evalúan las posibles vulnerabilidades en el sistema. Esto implica utilizar herramientas automatizadas y técnicas manuales para descubrir debilidades en la seguridad.

Explotación (Exploitation): En esta etapa, se intenta explotar las vulnerabilidades identificadas para ganar acceso no autorizado al sistema o red. El objetivo es demostrar cómo un atacante podría aprovechar las debilidades descubiertas.

Post-Explotación (Post-Exploitation): Después de ganar acceso, se lleva a cabo una evaluación más profunda para determinar la extensión del compromiso y si es posible mantener el acceso sin ser detectado.

Análisis de Resultados y Elaboración de Informes (Analysis and Reporting): Se recopilan los hallazgos y se prepara un informe detallado que incluye las vulnerabilidades descubiertas, su gravedad, recomendaciones para mitigar los riesgos y posibles mejoras en la seguridad.

Comunicación y Planificación de Mitigación (Communication and Remediation Planning): Se comparten los resultados con los responsables de la seguridad de la organización y se discute un plan de mitigación para abordar las vulnerabilidades identificadas.

7 METASPLOIT

Metasploit es herramienta de pruebas de penetración y desarrollo de exploits que está incluida en Kali Linux,Metasploit en Kali Linux ofrece varias opciones y módulos para realizar pruebas de seguridad. A continuación, se enumeran algunas de las opciones de Metasploit:

msfconsole: Es la interfaz de línea de comandos de Metasploit. Permite interactuar con Metasploit mediante comandos y ejecutar diferentes módulos.

msfvenom: Es una herramienta de creación de payloads (cargas útiles) que permite generar exploits, shellcodes y otros elementos para la explotación de vulnerabilidades.

Meterpreter: Es un shell interactivo que se puede utilizar después de una explotación exitosa para realizar diversas acciones en el sistema comprometido.

msfweb: Es una interfaz web para Metasploit que proporciona una forma más gráfica de interactuar con la herramienta.

Armitage: Es una interfaz gráfica de usuario para Metasploit que facilita la visualización y gestión de exploits y sesiones de Meterpreter.

msfdb: Es una utilidad para administrar la base de datos de Metasploit. Metasploit utiliza una base de datos para almacenar información sobre hosts, servicios y resultados de escaneos.

Auxiliary Modules: Metasploit incluye una amplia gama de módulos auxiliares que pueden utilizarse para realizar diversas tareas, como escaneo de puertos, recopilación de información, etc.

Exploit Modules: Ofrece una variedad de módulos de explotación que se utilizan para aprovechar vulnerabilidades en sistemas objetivo.

Payloads: Permite la selección de diferentes payloads según los requisitos de la prueba de penetración.

5.1CVE

Es un sistema estándar internacional utilizado para identificar y referenciar públicamente todas las vulnerabilidades de seguridad conocidas en software y hardware de tecnologías de la información.

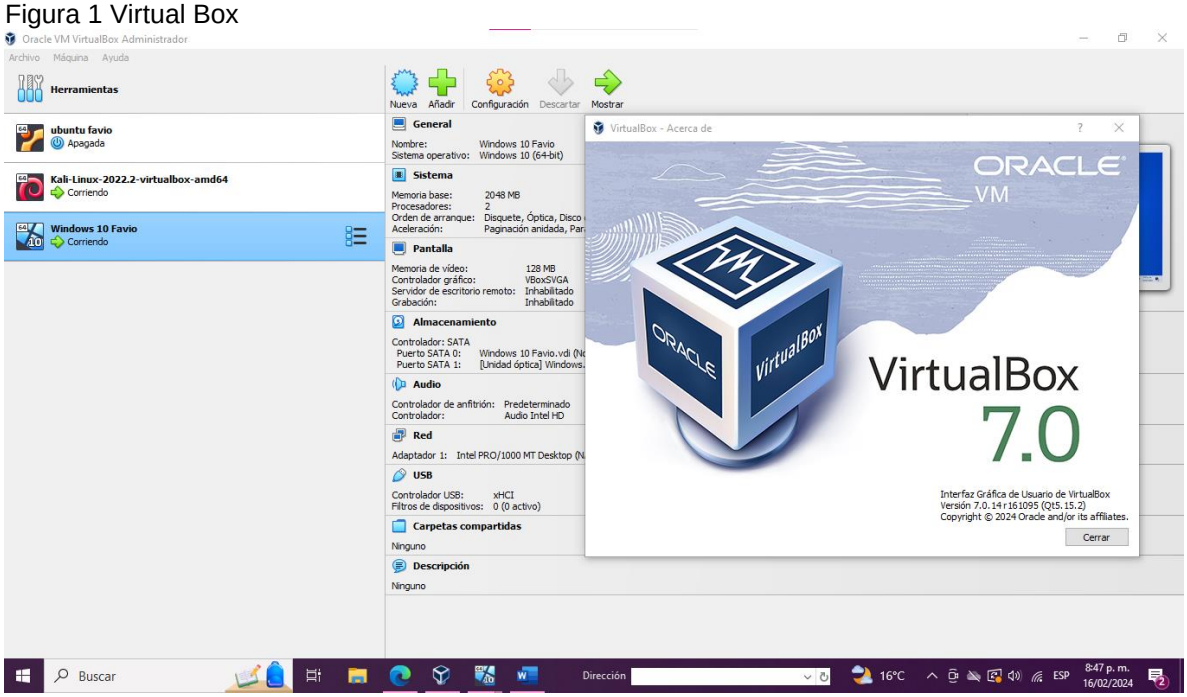
El propósito de CVE es proporcionar una nomenclatura estándar para facilitar la interoperabilidad y el intercambio de datos entre las herramientas y bases de datos de seguridad. Cuando se descubre una vulnerabilidad, se asigna un CVE

y se registra en la base de datos CVE correspondiente. Esto permite que las organizaciones y profesionales de seguridad de la información puedan realizar un seguimiento uniforme de las vulnerabilidades y tomar medidas para mitigar los riesgos asociados.

8 BANCO DE TRABAJO

PASO A . Descarga e instalación herramienta virtualizadora VirtualBox

Figura 1 Virtual Box

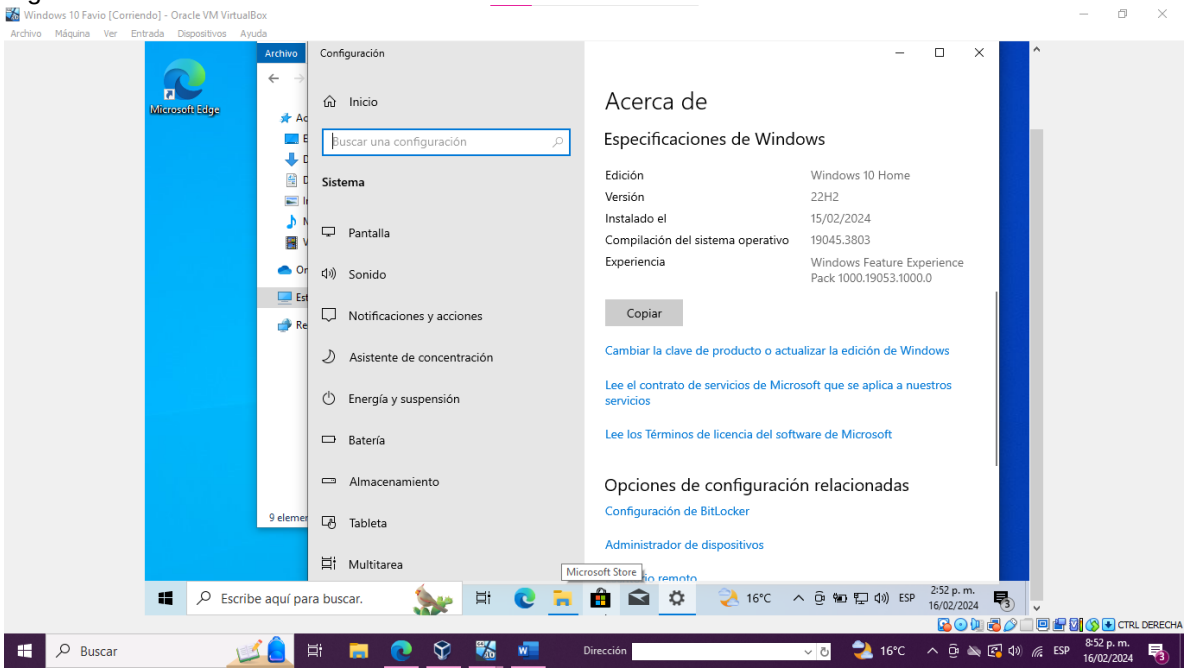


Fuente:elaboración propia

Se realiza descarga e instalación de VirtualBox versión 7.0

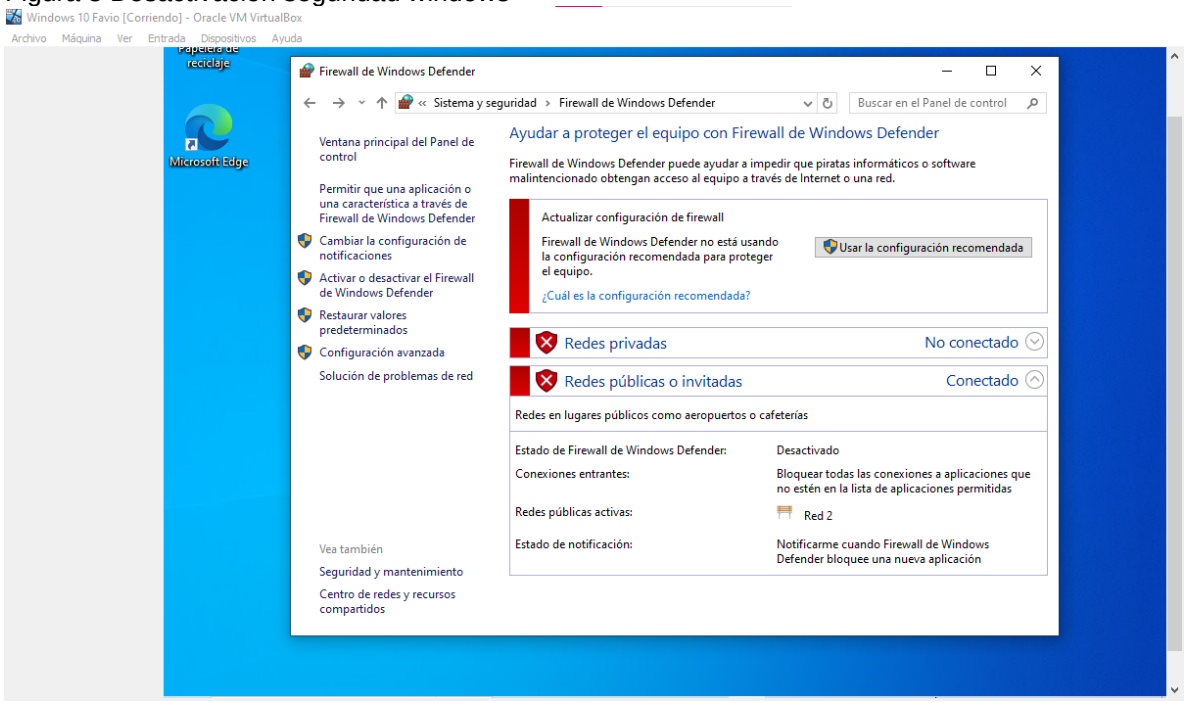
PASO B. Máquinas virtuales Windows 10 y Kali Linux

Figura 2 Windows 10



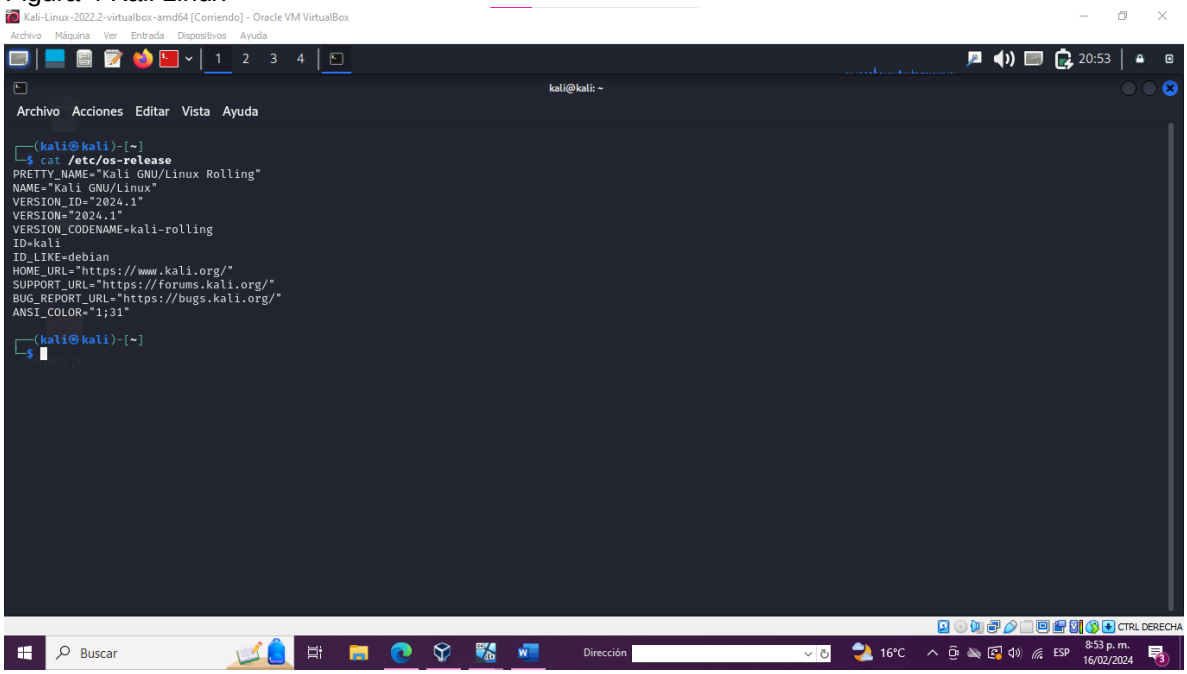
Fuente:elaboración propia

Figura 3 Desactivacion seguridad windows



Fuente:elaboración propia

Figura 4 Kali Linux

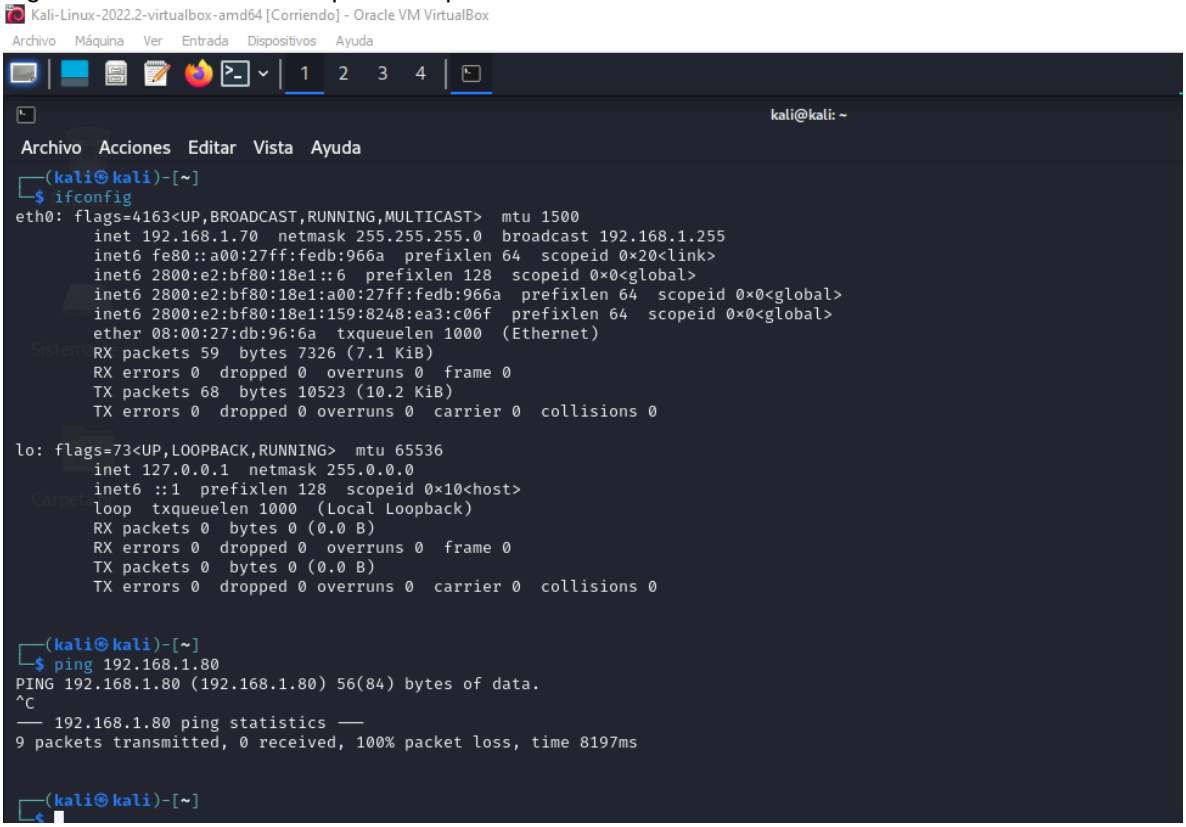


Fuente:elaboración propia

PASO C. Comunicación Entre las máquinas.

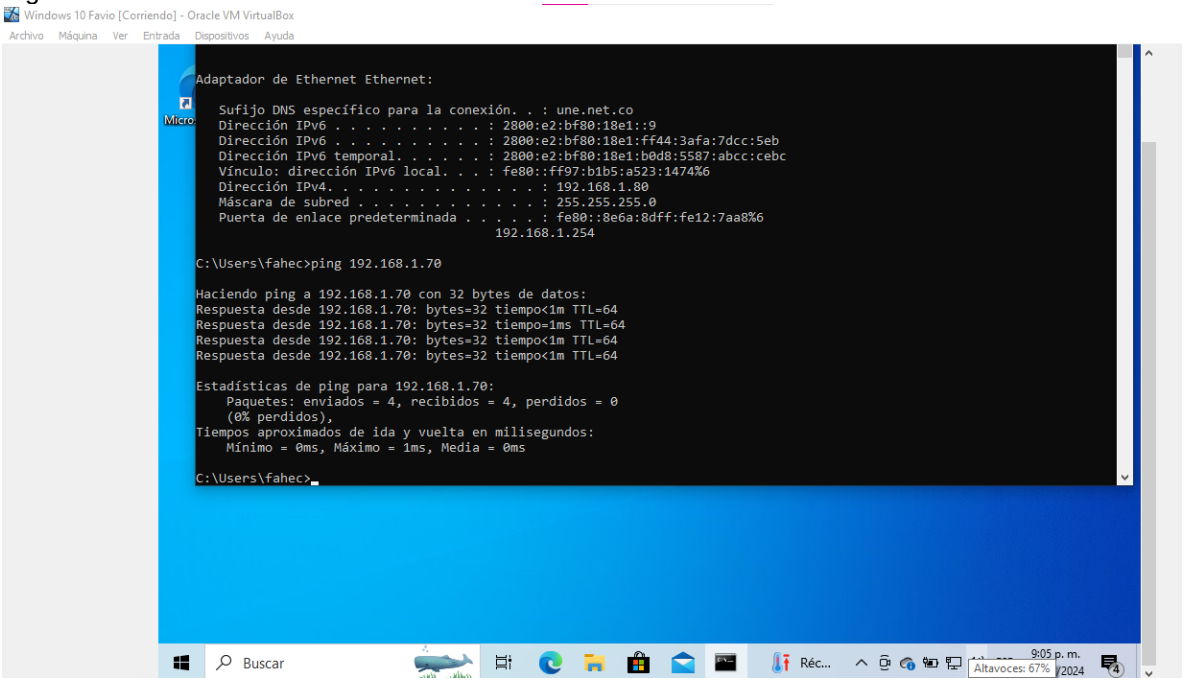
Se realiza verificación de comunicación exitosa entre las dos máquinas.

Figura 5 Comunicacion máquinas de prueba



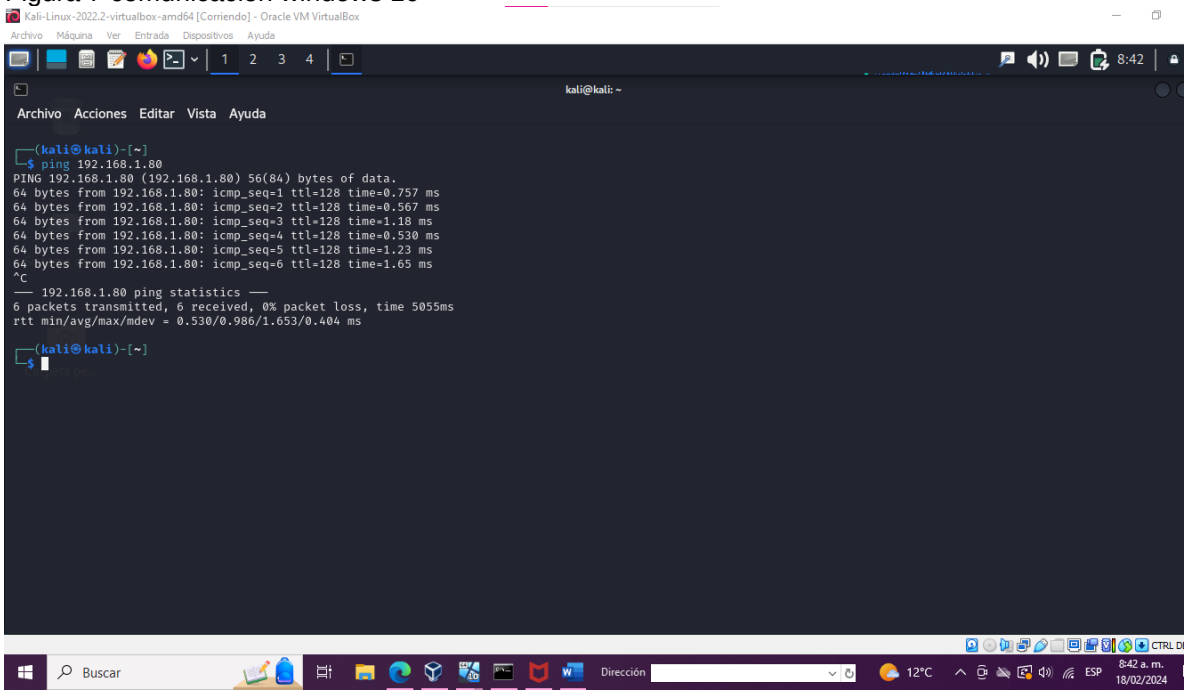
Fuente:elaboración propia

Figura 6 comunicacion kali linux



Fuente:elaboración propia

Figura 7 comunicacion windows 10



Fuente:elaboración propia

PASO D. Características técnicas del hardware

Se implementaron 2 máquinas virtuales utilizando VirtualBox, con las siguientes características:

Tabla 3 Caracteristicas técnicas

Máquina	Versión SO	Memoria	Disco Duro	CPU
Windows	Windows 10 Home basic 22H2	2GB	50 GB	Intel Core i5, 2 procesadores
Linux	Kali Linux 2024.1	2GB	50 GB	Intel Core i5, 2 procesadores

Fuente:elaboración propia

9 ANÁLISIS ESCENARIO PLANTEADO – ACUERDO DE CONFIDENCIALIDAD

9.1 PÁRRAFOS ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD

"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."*

La inclusión de información ilegal en un acuerdo de confidencialidad podría invalidar, y exponer a las partes involucradas a consecuencias legales, en este caso entre HackerHouse y el aspirante al cargo, que agrava la situación ya que se podría catalogar como complicidad en actividades ilegales, toda vez que los implicados en el acuerdo conocen la información ilegal y en el acuerdo se especifica que no puede ser transmitida a autoridades legales.

"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:

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"

En este párrafo obliga nuevamente a los firmantes a ocultar información ilegal, lo cual los convierte en cómplices de la información ilegal que se pueda encontrar en la documentación de HackerHouse.

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

Además de quebrantar la ley de protección de datos, este párrafo del acuerdo de confidencialidad intenta encubrir actividades fraudulentas y/o corruptas, toda vez que pretende eximir a la compañía HackerHouse de cualquier responsabilidad de la ilegalidad de la información.

9.2 LEYES COLOMBIANAS VIOLENTADAS EN EL ACUERDO DE CONFIDENCIALIDAD

la Ley 1581 de 2012 regula la protección de datos personales. Algunos de los artículos que podrían estar relacionados con la inclusión de información ilegal en un acuerdo de confidencialidad son los siguientes:

Artículo 15 - Consentimiento del Titular: Este artículo establece que el tratamiento de datos personales solo puede llevarse a cabo con el consentimiento previo, expreso e informado del titular, salvo en casos exceptuados por la ley.

Artículo 17 - Derechos de los Titulares: El artículo 17 reconoce los derechos de los titulares de datos personales, incluyendo el derecho de acceso, actualización, rectificación y supresión de la información.

Artículo 18 - Finalidades del Tratamiento: Establece que el tratamiento de datos personales debe obedecer a una finalidad legítima, la cual debe ser informada al titular.

Artículo 20 - Principios del Tratamiento: Señala los principios que deben regir el tratamiento de datos, incluyendo la veracidad, calidad, seguridad, confidencialidad y otros aspectos relevantes.

Artículo 21 - Deber de Seguridad: Establece que los responsables del tratamiento deben adoptar medidas técnicas, humanas y administrativas para garantizar la seguridad de la información.

Artículo 22 - Registro de Bases de Datos: Los responsables del tratamiento deben inscribir las bases de datos que contengan datos personales en el Registro Nacional de Bases de Datos.

Artículo 25 - Transferencia Internacional de Datos: Regula la transferencia de datos personales a terceros países, exigiendo garantías de seguridad y protección en caso de transferencias internacionales.

Artículo 29 - Secreto Profesional: Establece el deber de confidencialidad respecto a la información que se maneja en el tratamiento de datos personales.

Artículo 37 - Sanciones: Contiene disposiciones sobre las sanciones aplicables en caso de incumplimiento de la ley, que pueden incluir multas y otras medidas correctivas.

9.3 COPNIA, CÓDIGO DE ÉTICA Y SANCIONES

En el acuerdo de confidencialidad si se encuentran procesos ilegales tal como se detallaron en el numeral anterior, y no aceptaría el contrato y el acuerdo, ya que ponen en riesgo el ejercicio de mi profesión con ingeniero, tal como se incluye en el código de ética del COPNIA en el capítulo II. De los deberes y obligaciones de los profesionales, en artículo 31:

"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"

También en el mismo artículo, en el numeral f, se menciona como deber del ingeniero denunciar todos los delitos y faltas contra el código de ética, precisamente el acuerdo de confidencialidad redactado por la compañía HackerHouse representa una grave violación a este código.

"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."

También destaca el numeral a del artículo 34, prohibiciones especiales a los profesionales respecto a la sociedad:

"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"

Tal como se plantea en este artículo, los ingenieros no deben aceptar contratos y ofertas laborales donde se evidencie quebrantamiento de las leyes vigentes, tal como son la ley 1581 de 2012 y la ley 1273 de 2009, y en el caso expuesto evidentemente no se actúa de mamera ética y eso pude conllevar a sanciones temporales o definitivas para el ingeniero involucrado.

10 CIBERCRIMEN EN COLOMBIA – ATAQUE INFORMÁTICO INVIMA

En el año 2022, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos, INVIMA, sufrió varios ataques informáticos, el primer ataque anunciado oficialmente fue el 6 de febrero, basado en ataques por ransonmware, dejaron la página web de la entidad por fuera y con ellos muchos procesos de registro y vigilancia, por lo que se afecto todo el registro de mercancía en los puertos colombianos, caso similar y aún con mayor afectación en octubre de 2022 que dejo sin sistema a la entidad por varios meses.

Un ataque de ransomware podría involucrar varios elementos que caen bajo el ámbito de la Ley 1273 de 2009:

Acceso Abusivo a Sistemas Informáticos: La infiltración inicial de ransomware en un sistema puede considerarse como acceso abusivo a sistemas informáticos, especialmente si se realiza sin la autorización del titular del sistema.

Daño Informático: El cifrado de archivos y la posterior exigencia de un rescate para desbloquearlos podrían considerarse como daño informático, ya que afecta la disponibilidad y el funcionamiento normal de los sistemas.

Extorsión Informática: La demanda de un pago para desbloquear datos cifrados podría considerarse como extorsión informática, lo cual es un delito específicamente abordado por la ley.

Falsedad Informática: Si el atacante utiliza técnicas fraudulentas para engañar a la víctima o presenta información falsa en relación con el ataque, podría considerarse falsedad informática.

La Ley 1581 de 2012 en Colombia regula la protección de datos personales. Aunque esta ley se centra principalmente en la privacidad de la información personal y su tratamiento, podría tener relevancia en el contexto de un ataque de ransomware, especialmente si este afecta datos personales. A continuación, se detallan algunos aspectos de la Ley 1581 de 2012 y su posible aplicación en casos de ransomware:

Aspectos Relevantes de la Ley 1581 de 2012:
Consentimiento del Titular: La ley establece que el tratamiento de datos personales requiere el consentimiento del titular. En un ataque de ransomware que afecta datos personales, la falta de consentimiento para dicho tratamiento puede ser una violación de la ley.

Finalidades del Tratamiento: El tratamiento de datos personales debe tener una finalidad legítima. Un ataque de ransomware que compromete datos personales podría violar esta disposición si la finalidad del ataque no es legítima.

Deber de Seguridad: Los responsables del tratamiento deben implementar medidas de seguridad para proteger los datos personales. Un ataque de ransomware que compromete la seguridad de los datos podría implicar un incumplimiento de este deber.

Derechos de los Titulares: La ley reconoce diversos derechos a los titulares de datos personales, como el derecho de acceso, actualización, rectificación y supresión. Un ataque de ransomware que impide el ejercicio de estos derechos podría contravenir la ley.

<u>Aplicación en un Ataque de Ransomware:</u>

Impacto en la Confidencialidad: Si el ransomware cifra o compromete la confidencialidad de datos personales, esto podría constituir una violación de la Ley 1581 de 2012.

Deber de Notificación: En caso de un incidente de seguridad que afecta datos personales, la ley establece la obligación de notificar a la Superintendencia de Industria y Comercio y a los titulares. Un ataque de ransomware podría desencadenar esta obligación.

Evaluación de Riesgos: La ley insta a los responsables del tratamiento a realizar evaluaciones de riesgos. Un ataque de ransomware puede ser considerado un riesgo que debería ser evaluado y gestionado adecuadamente.

11 HERRAMIENTAS DE INTRUSIÓN

11.1 MFSVENOM

MSFVenom es un componente Metasploit, diseñado para crear cargas útiles personalizadas para varios sistemas operativos y escenarios. Estas cargas útiles, a menudo denominadas "shells", permiten a los piratas informáticos éticos establecer conexiones remotas con los sistemas de destino, otorgándoles control para la evaluación de vulnerabilidades, pruebas de penetración y mejora de la seguridad.

Características de MSFVenom:

Independiente de la plataforma: MSFVenom admite múltiples plataformas, incluidas Windows, Linux, macOS, Android e iOS, lo que permite a los piratas informáticos éticos adaptar cargas útiles a entornos de destino específicos.

Cargas útiles personalizadas: los usuarios pueden crear cargas útiles adaptadas a sus necesidades, incluidas shells inversas, shells vinculantes y sesiones de Meterpreter.

Cifrado de carga útil: MSFVenom permite el cifrado de carga útil para evitar los sistemas de detección de intrusiones y mantener el sigilo durante los ataques.

Cargas útiles en etapas y sin etapas: los piratas informáticos éticos pueden elegir entre cargas útiles en etapas y sin etapas, según sus requisitos de velocidad y sigilo.

MSFVenom es una herramienta versátil con numerosas aplicaciones en el campo del hacking ético:

1. Pruebas de penetración
Los piratas informáticos éticos pueden utilizar MSFVenom para simular ataques del mundo real, identificar vulnerabilidades y evaluar la postura de seguridad de una organización.

2. Explotar el desarrollo
Los investigadores de seguridad utilizan MSFVenom para crear exploits de prueba de concepto, ayudando en el descubrimiento y parcheo de vulnerabilidades.

3. Acceso remoto
MSFVenom permite a los piratas informáticos éticos obtener acceso remoto a sistemas comprometidos, lo que facilita una mayor investigación y análisis

11.2 POC ATAQUE

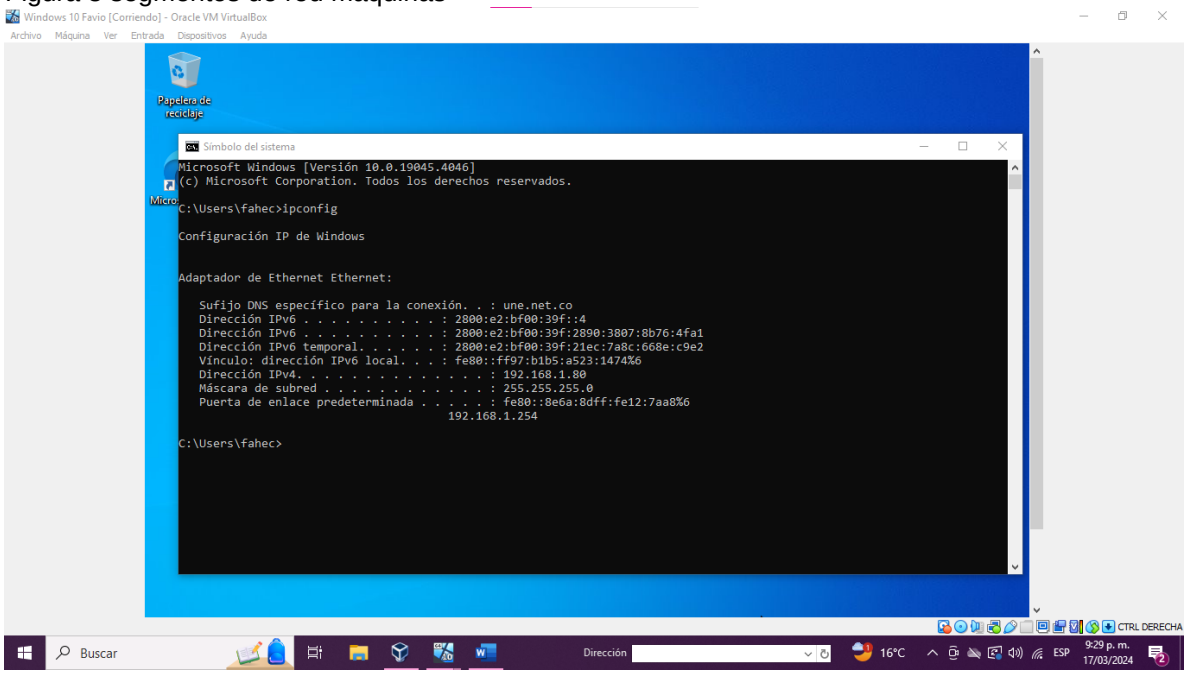
POC ATAQUE

PASO 1.

La máquina Windows 10 y Kali-linux se encuentran en el mismo segmento de red:

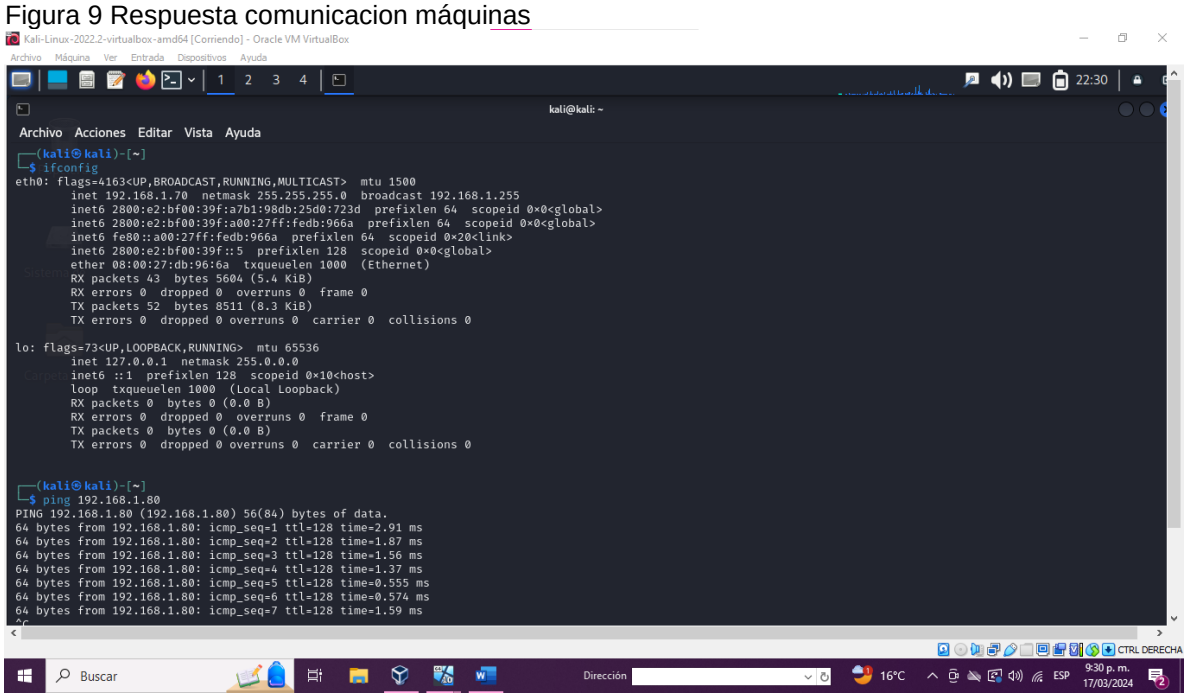
Windows 10 : 192.168.1.80
Kali Linux: 192.168.1.70

Figura 8 segmentos de red máquinas



Fuente:elaboración propia

Figura 9 Respuesta comunicacion máquinas



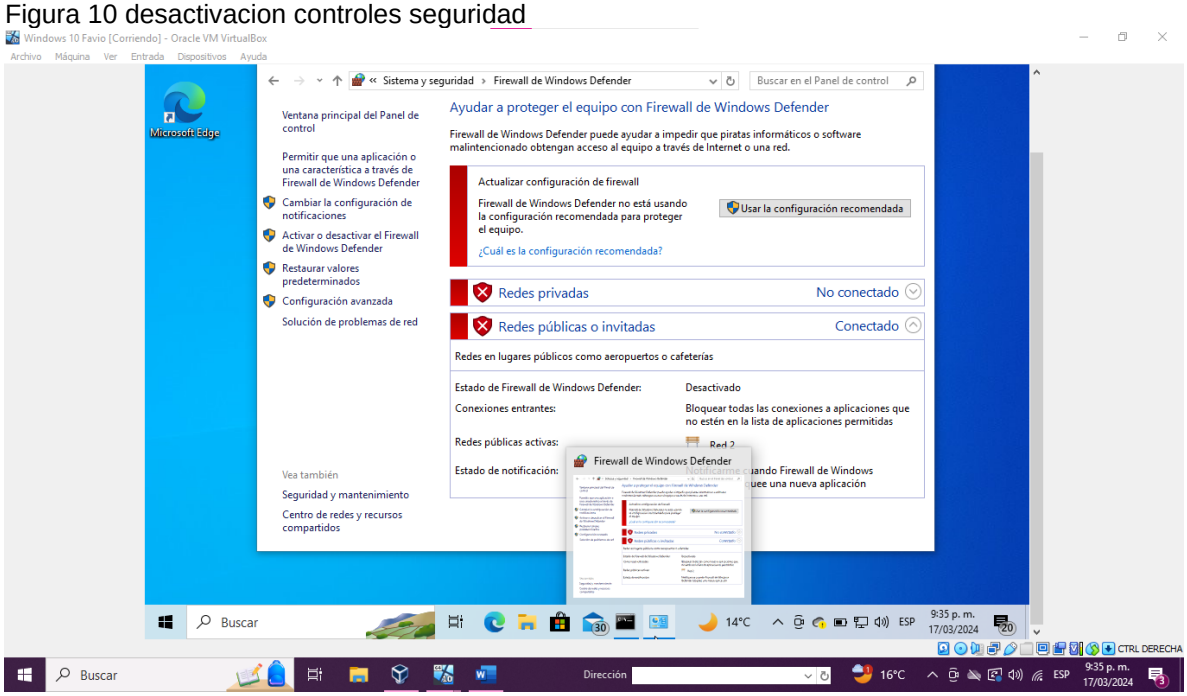
Fuente:elaboración propia

En la imagen se observa la respuesta de la máquina Windows 10 desde Kali Linux.

PASO 2. Sistema Operativo de la máquina víctima.

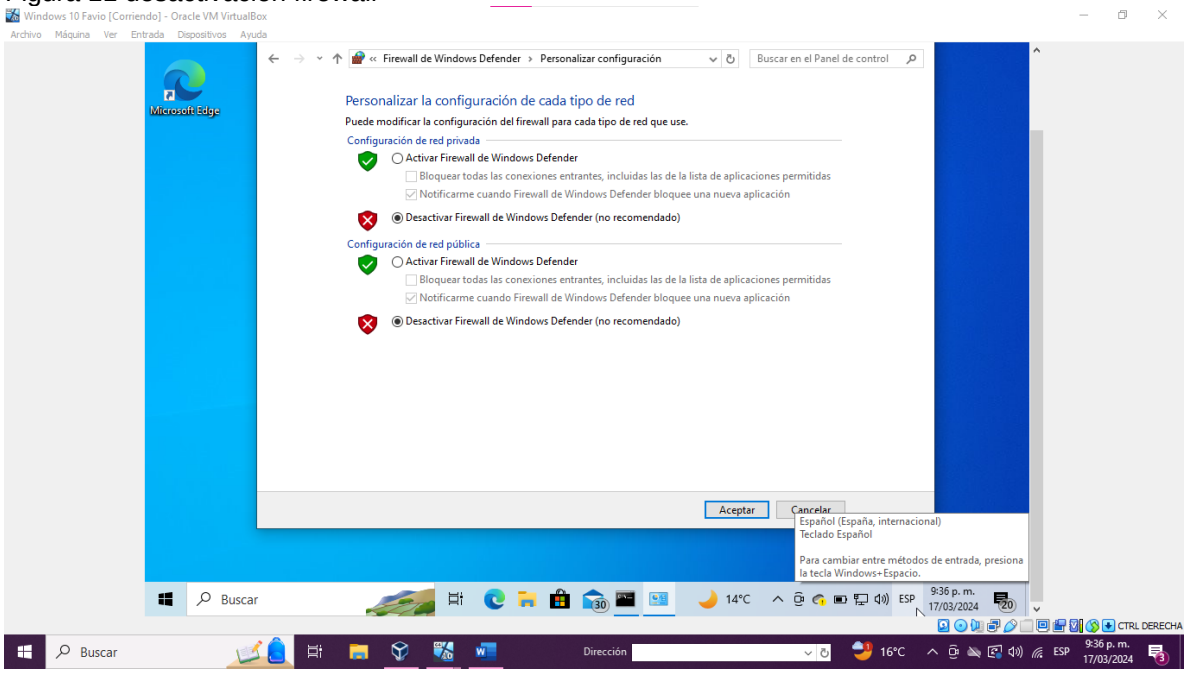
Se deshabilita todos los sistemas de seguridad en la máquina Windows 10.

Figura 10 desactivacion controles seguridad



Fuente:elaboración propia

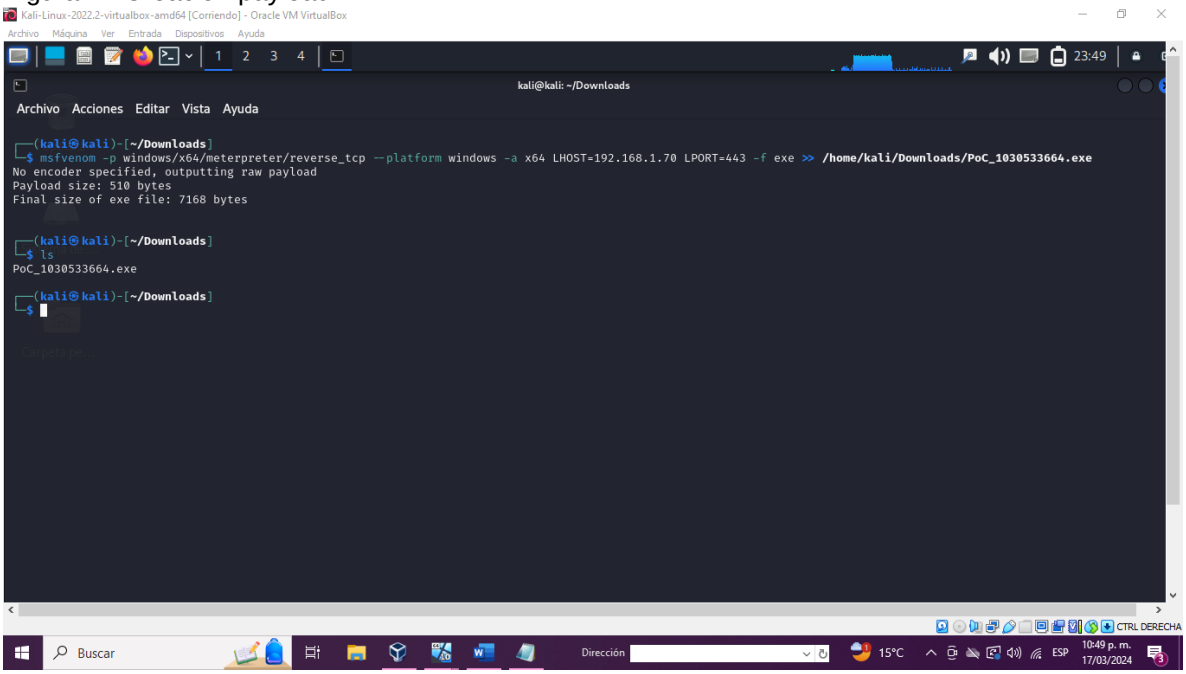
Figura 11 desactivacion firewall



Fuente:elaboración propia

Creación de Payload:

Figura 12 Creacion payload

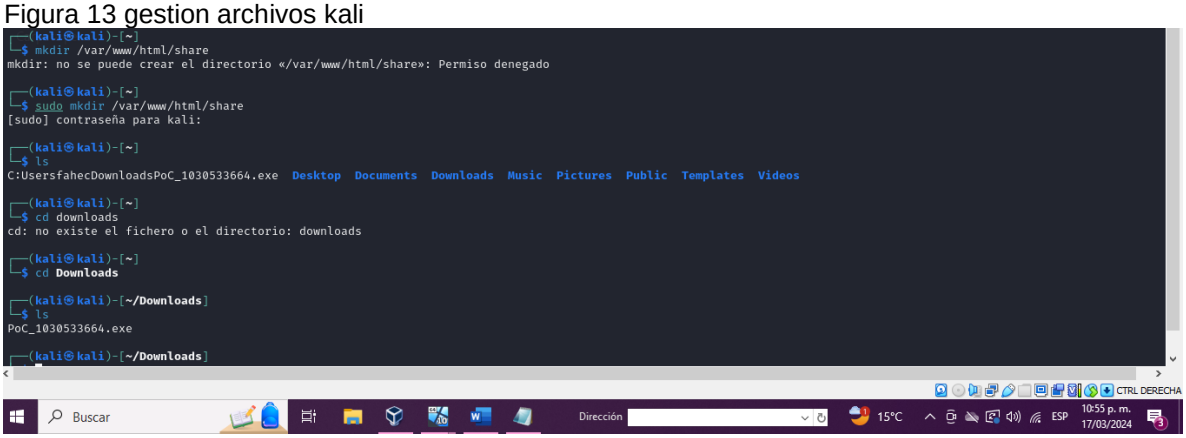


Fuente:elaboración propia

Se busca el payload en la ruta indicada.

Se crea una carpeta en el servicio html para luego poder ejecutarlo en la máquina victima:

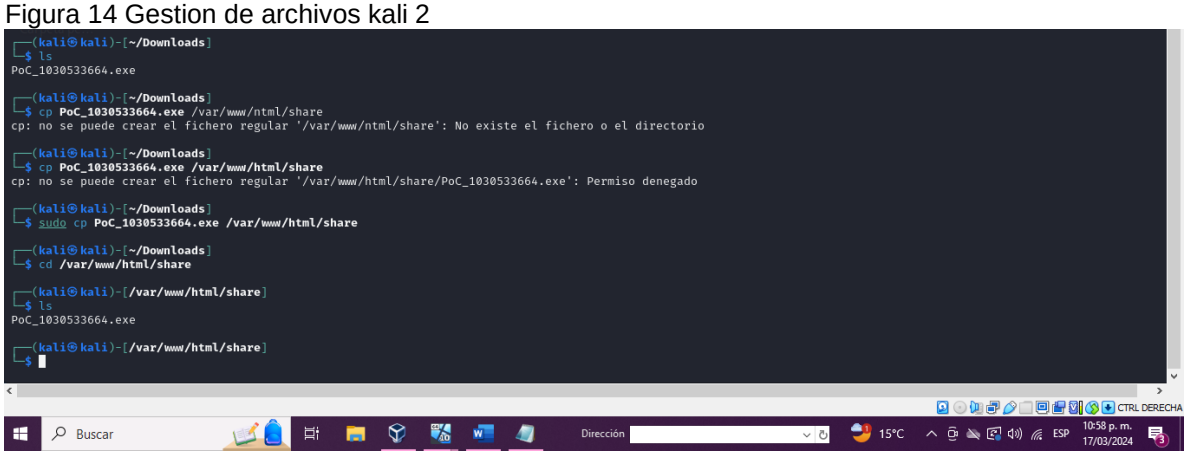
Figura 13 gestion archivos kali



Fuente:elaboración propia

Se copia el payload creado a la carpeta indicada:

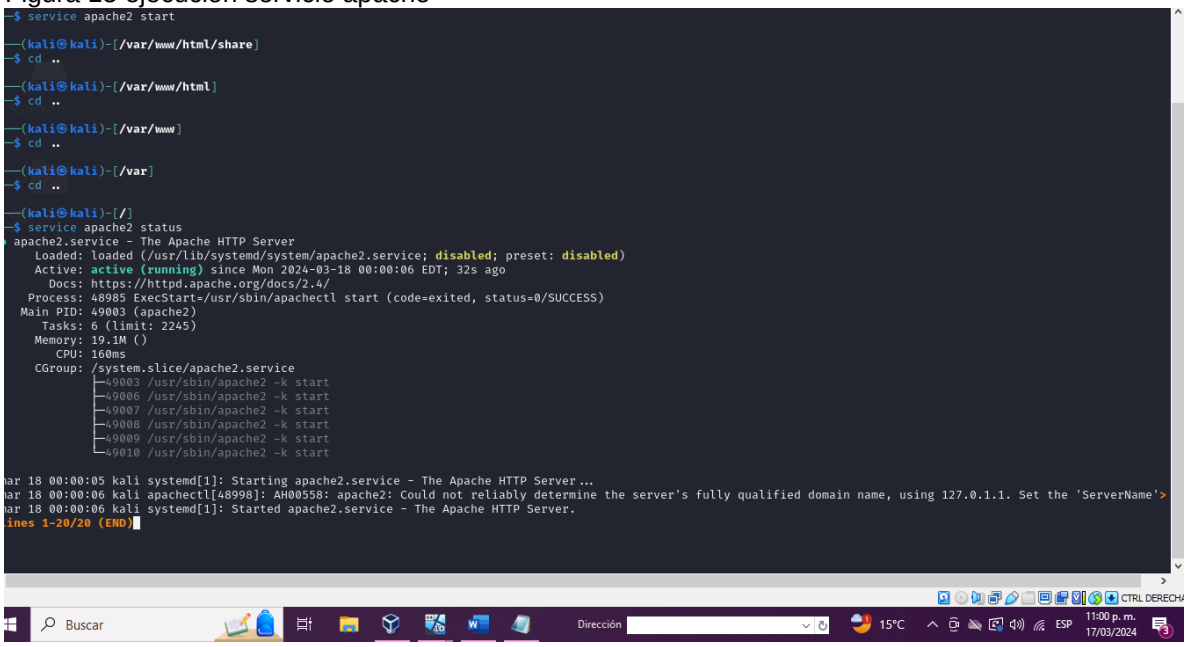
Figura 14 Gestion de archivos kali 2



Fuente:elaboración propia

Se inicia el servicio apache en Kali Linux para poder compartir el payload:

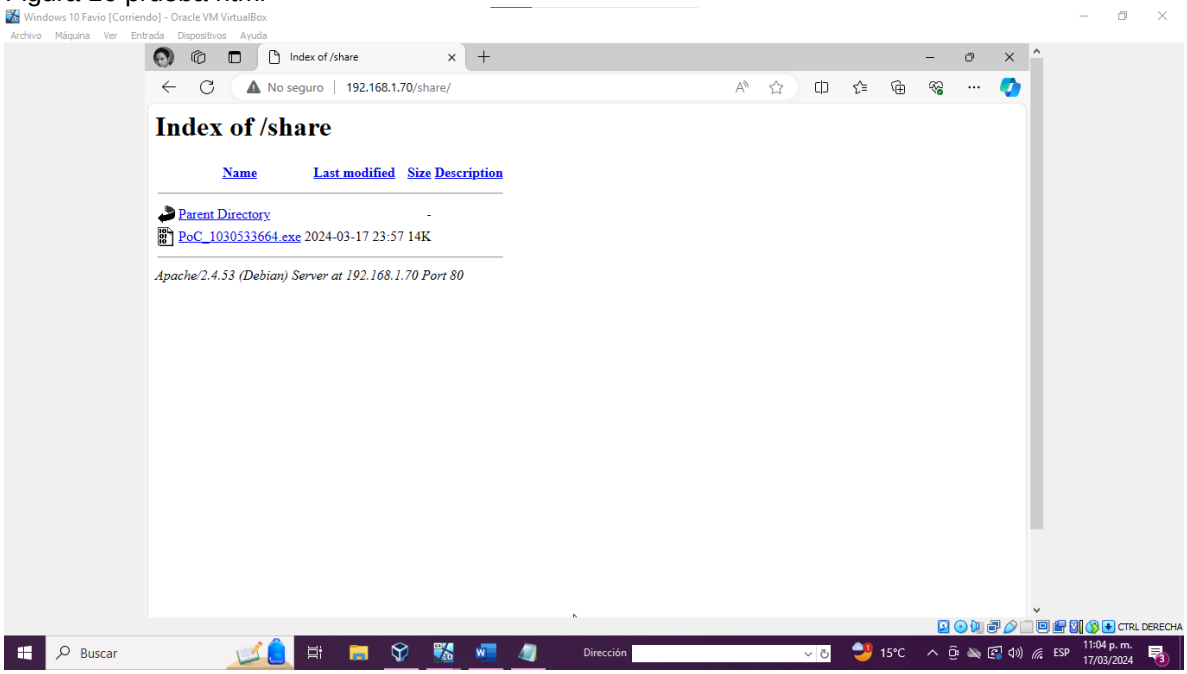
Figura 15 ejecución servicio apache



Fuente:elaboración propia

Se realiza la verificación del acceso desde la máquina victima (Windows 10):

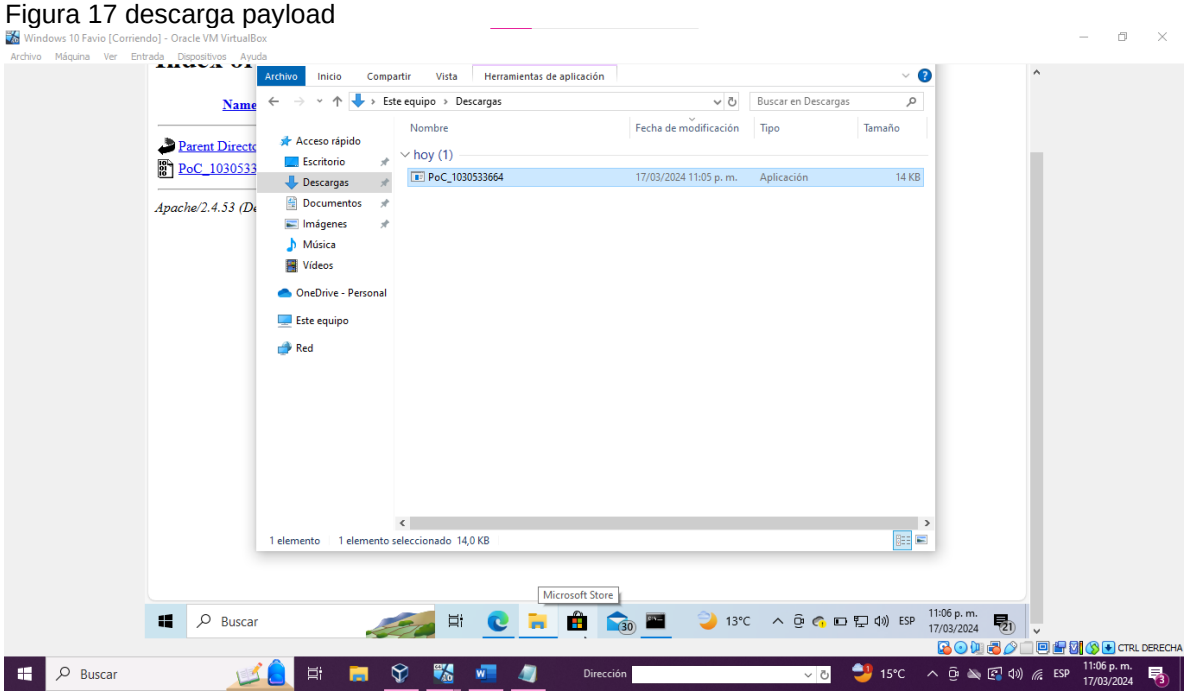
Figura 16 prueba html



Fuente:elaboración propia

Se realiza la descarga del payload en la máquina victima:

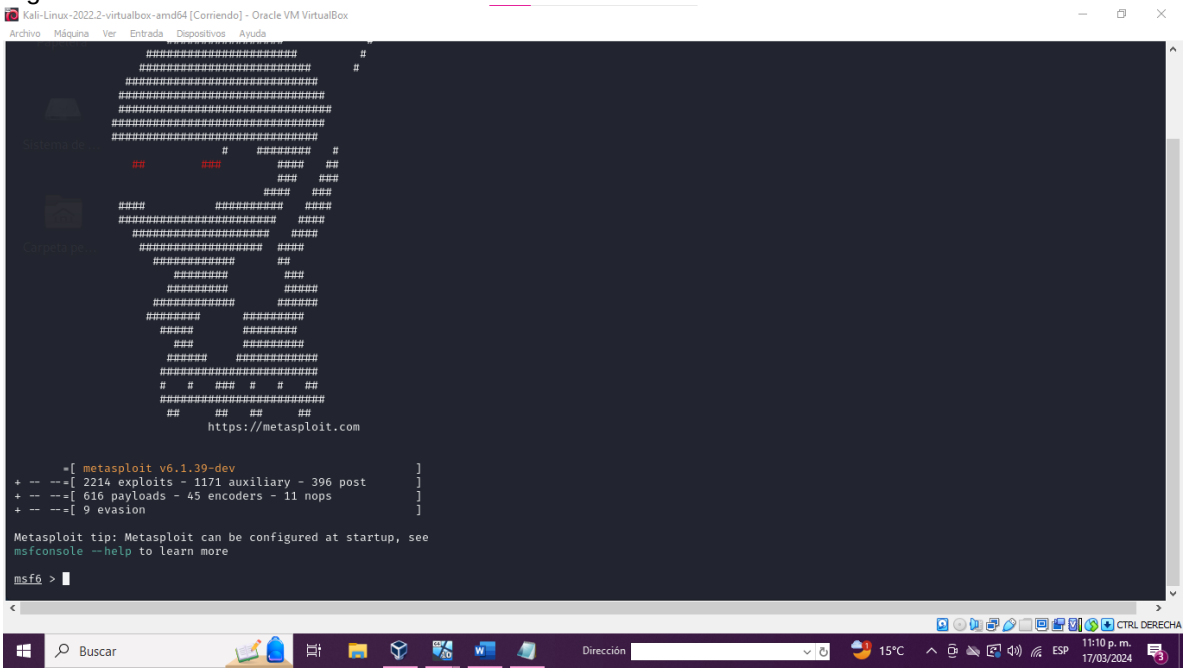
Figura 17 descarga payload



Fuente:elaboración propia

Se ingresa al mfsconsole:

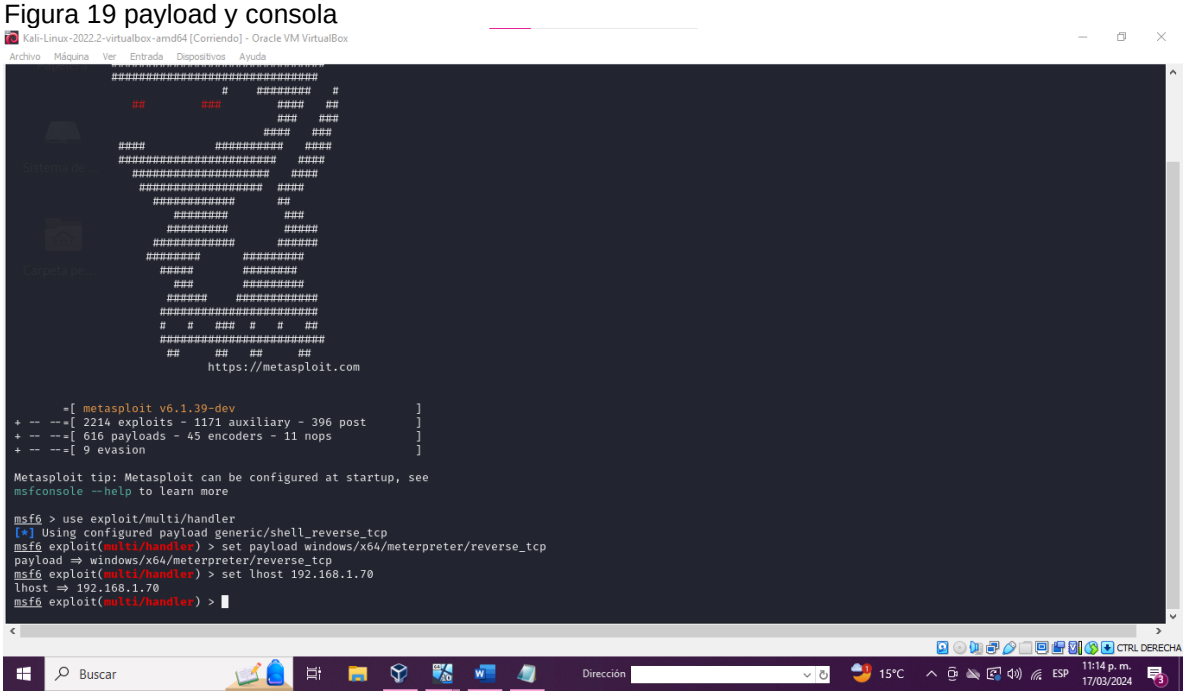
Figura 18 mfs console



Fuente:elaboración propia

se utiliza el mismo exploit, y el payload con el cual se creo el ejecutable, en localhost se coloca la ip del Kali Linux:

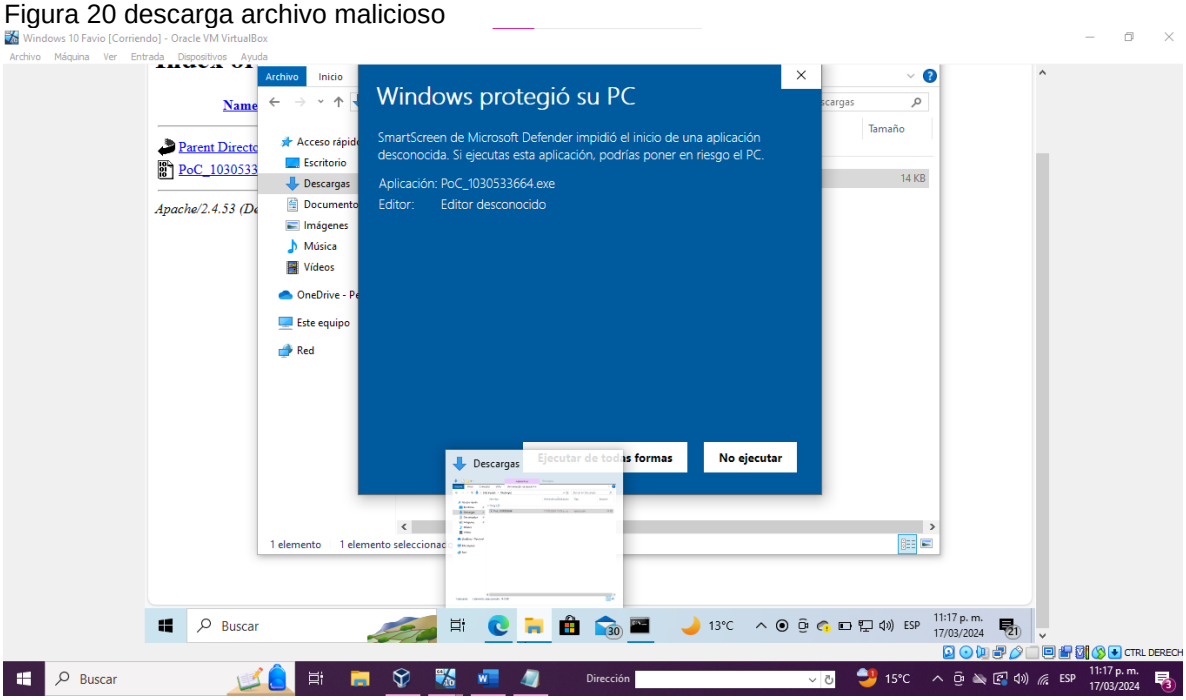
Figura 19 payload y consola



Fuente:elaboración propia

En la máquina victima se ejecuta el archivo .exe:

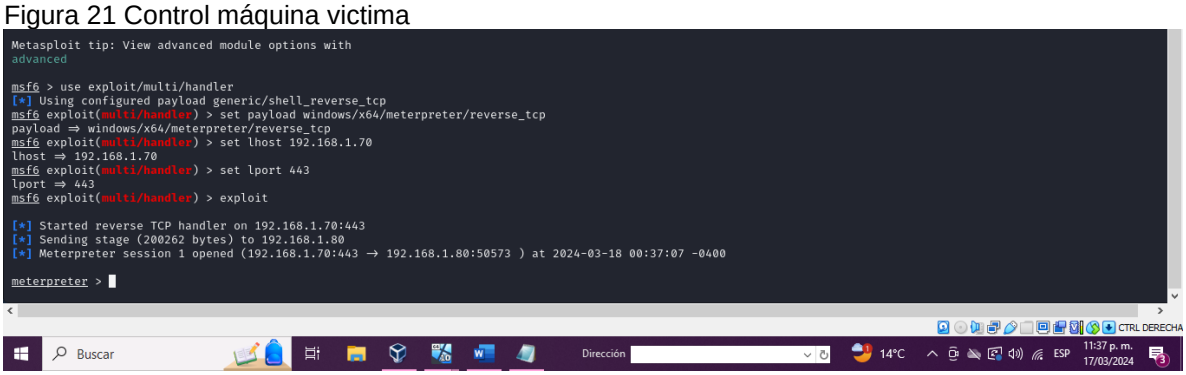
Figura 20 descarga archivo malicioso



Fuente:elaboración propia

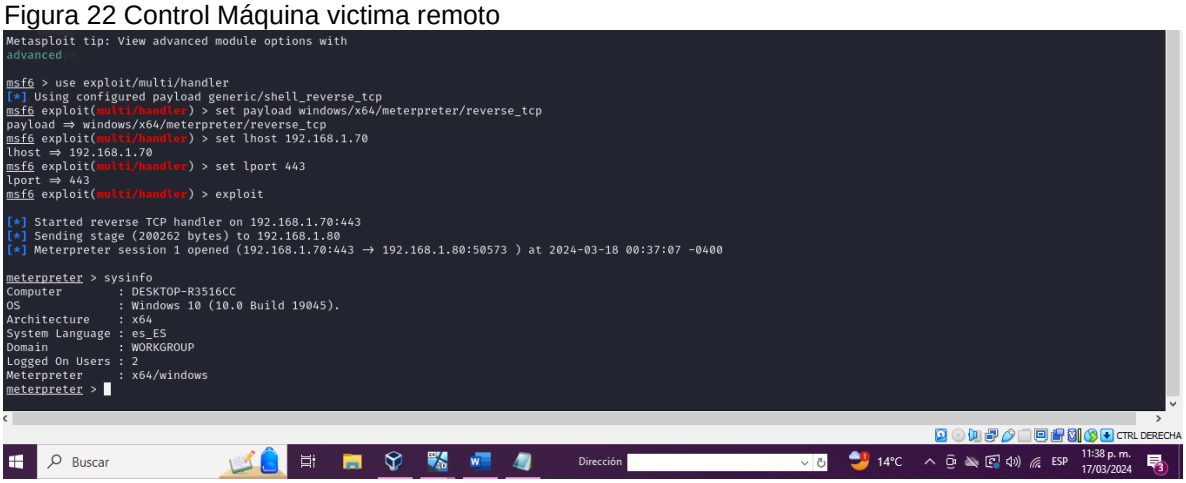
Al ejecutar el .exe, se evidencia la sesión activa en la máquina atacante, donde se puede observar las propiedades de la máquina victima:

Figura 21 Control máquina victima



Fuente:elaboración propia

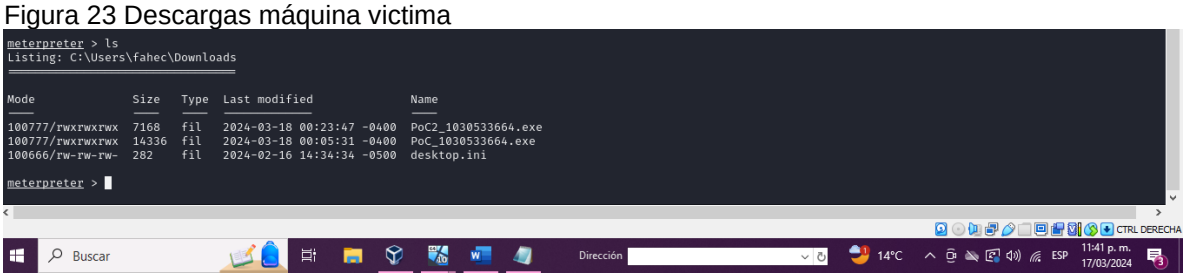
Figura 22 Control Máquina victima remoto



Fuente:elaboración propia

Con el comando ls, podemos listar los archivos que se han descargado en la máquina victima:

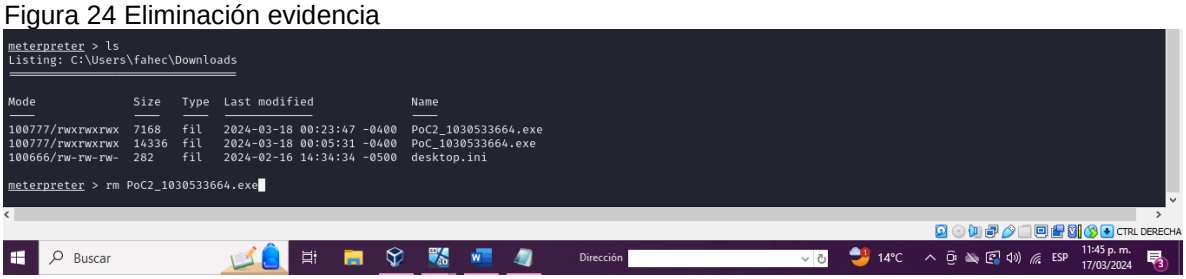
Figura 23 Descargas máquina victima



Fuente:elaboración propia

Con el comando rm en meterpreter se eliminan los archivos que se descargaron para borrar la evidencia:

Figura 24 Eliminación evidencia



Fuente:elaboración propia

12 IDENTIFICACIÓN DE UN ATAQUE INFORMÁTICO

Detectar el ataque:

Presta atención a los siguientes signos de un ataque en tiempo real:
Rendimiento lento del dispositivo: Si el dispositivo se ralentiza repentinamente, podría ser un signo de que está siendo atacado.

Actividad inusual en el sistema: Observar si hay procesos desconocidos ejecutándose en el Administrador de tareas o si hay actividad inusual en la red.

Mensajes de error o alertas: Prestar atención a cualquier mensaje de error o alerta que aparezca en la pantalla.

Software desconocido: Si se encuentra software que no se ha instalado voluntariamente o de un fabricante desconocido, podría ser malware.

Si se sospecha de un ataque informático a un dispositivo es fundamental aislar el equipo para evitar afectaciones en toda la red, a continuación, se describen algunas de las acciones que se puede tomar:

1. Desconectar el dispositivo de la red:

   Desconectar el cable Ethernet.
   Desactivar el Wi-Fi
   Desactivar Bluetooth:
   Guardar una copia de seguridad de tus datos

2. Investigar el ataque:

Recopilar información sobre el ataque:
Registrar la fecha y hora del ataque.
Registrar los síntomas que experimentaste.
Recopilar cualquier mensaje de error o alerta que hayas recibido.
Analizar los registros del sistema:
Utilizar el Visor de eventos para buscar eventos relacionados con el ataque.
Busca eventos con ID de evento 4625, 4624, 4672, 4634, 4697, 4706, 4740, 7045 o 4688.
Utilizar herramientas de análisis de malware:
Utilizar herramientas como Microsoft Defender o Malwarebytes para analizar el dispositivo en busca de malware.

3. Eliminar el malware:

Si se encuentra malware, es importante eliminarlo lo antes posible.
Sigue estos pasos para eliminar el malware:
Utilizar una herramienta antimalware para eliminar el malware.
Si las instrucciones en pantalla para eliminar el malware.
Si no se puede eliminar el malware,se puede intentar restaurar el dispositivo a un punto anterior.

4. Recuperar el dispositivo:

Una vez que se haya eliminado el malware, se puede comenzar a recuperar el dispositivo.
Si no se puede restaurar el dispositivo a un punto anterior, es posible que sea necesario reinstalar el sistema operativo.
6. Prevenir futuros ataques:

Es importante tomar medidas para prevenir futuros ataques. Por eso es recomendable tener las ultimas actualizaciones de los fabricantes.

13 PASO A PASO PARA SUBSANAR EVENTO DEL PAYLOAD

Para el ataque ejecutado en el ejercicio de red team, se ejecutaron los siguientes pasos:

Identificar el ataque: se reconoce la naturaleza del ataque por payload, incluyendo cómo se está entregando y qué tipo de payload se está utilizando (por ejemplo, virus, troyano, ransomware).

Detener la propagación: se desconecta el dispositivo infectado de la red para evitar que el malware se propague a otros sistemas en la red.

Activar el firewall de Windows: habilitar el firewall de Windows para bloquear el tráfico no deseado y evitar que el malware se comunique con servidores remotos o realice actividades maliciosas.

Ejecutar un escaneo antivirus/antimalware: Utiliza un software de seguridad confiable, en el caso de Windows 10 viene incluida la herramienta Windows defender para realizar un escaneo completo del sistema en busca de malware y eliminar cualquier amenaza detectada. También se puede instalar y verificar resultados con otras herramientas disponibles en el mercado.

Actualizar y parchear el sistema operativo y el software: se debe aplicar las actualizaciones de seguridad y componentes pendientes en el sistema operativo y en las aplicaciones instaladas.

Revisar los registros de eventos: Examina los registros de eventos del sistema en busca de actividades sospechosas que puedan indicar la presencia de malware, como intentos de inicio de sesión fallidos, modificaciones de archivos importantes o servicios detenidos de manera inesperada.

Analizar procesos en ejecución: Utilizar el Administrador de tareas de Windows o herramientas más avanzadas como Process Explorer para identificar procesos en ejecución sospechosos o no familiares y terminar cualquier proceso malicioso que esté activo.

Restaurar desde una copia de seguridad: es recomendable tener una copia de seguridad reciente y confiable, con el fin de restaurar el sistema afectado desde esa copia de seguridad para eliminar completamente el malware y restaurar la funcionalidad normal del sistema.

Implementar medidas de prevención: Después de contener el ataque, implementa medidas adicionales de prevención, como políticas de seguridad más estrictas, restricciones de permisos de usuario y la aplicación de software de seguridad adicional para proteger contra futuros ataques.

14 RED TEAM / BLUE TEAM / PURPLE TEAM / EQUIPO DE RESPUESTA ANTE INCIDENTES INFORMATICOS

Tabla 4 Red team blue team

EQUIPO	ENFOQUE	OBJETIVO	ACTIVIDADES	RESULTADOS
Red Team	El equipo Red Team simula adversarios reales para llevar a cabo ataques controlados contra los sistemas de una organización	Su objetivo principal es identificar vulnerabilidades y debilidades en los sistemas de seguridad de la organización mediante técnicas de penetración	Realiza pruebas de penetración, evaluaciones de vulnerabilidades y otros ataques simulados para poner a prueba las defensas de seguridad de la organización	Proporciona información detallada sobre las vulnerabilidades encontradas y recomienda acciones correctivas para mejorar la postura de seguridad de la organización
Blue Team	El equipo Blue Team se centra en la defensa y protección de los sistemas de una organización contra amenazas cibernéticas	Su objetivo principal es detectar, prevenir y responder a los ataques cibernéticos, así como fortalecer las defensas de seguridad de la organización	Supervisa activamente la seguridad de la red, implementa controles de seguridad, responde a alertas de seguridad, realiza análisis forenses y lleva a cabo investigaciones de incidentes de seguridad	Proporciona información sobre la efectividad de las defensas de seguridad existentes y recomienda mejoras para fortalecer la postura de seguridad de la organización
Purple Team	El equipo Purple Team actúa como un puente entre el Red Team y el Blue Team, facilitando la	Su objetivo principal es mejorar la eficacia de la seguridad cibernética de la organización al alinear los	Facilita la comunicación entre el Red Team y el Blue Team, coordina ejercicios conjuntos de	Fomenta una comprensión compartida de las amenazas cibernéticas y promueve la implementación de medidas de

	colaboración y el intercambio de conocimientos entre ambos equipos	esfuerzos del Red Team y del Blue Team y promover una cultura de seguridad colaborativa	simulación de ataques y participa en la revisión y mejora de los procesos de seguridad de la organización	seguridad efectivas basadas en la retroalimentación de ambos equipos
Equipo de Respuesta a Incidentes de Seguridad (CSIRT)	El equipo de respuesta a incidentes de seguridad se dedica a la detección, análisis, contención y recuperación de incidentes de seguridad cibernética	Su objetivo principal es minimizar el impacto de los incidentes de seguridad, mitigar la pérdida de datos y restaurar la operatividad normal de los sistemas afectados	Responde a alertas de seguridad, investiga incidentes de seguridad, coordina la respuesta ante emergencias, realiza análisis forenses y documenta lecciones aprendidas	Proporciona informes detallados sobre los incidentes de seguridad detectados, las acciones tomadas para mitigarlos y las recomendaciones para prevenir incidentes similares en el futuro

Fuente:elaboración propia

15 CIS “CENTER FOR INTERNET SECURITY”

El CIS (Centro para la Seguridad de Internet) es una organización sin fines de lucro que desarrolla y promueve mejores prácticas para la seguridad cibernética.

Sus funciones principales son:

Desarrollar los Controles de Seguridad del CIS: Son un conjunto de recomendaciones de seguridad cibernética que se basan en el consenso de expertos de la industria.

Ofrecer evaluaciones de seguridad: El CIS ofrece evaluaciones de seguridad para ayudar a las organizaciones a medir su cumplimiento con los Controles de Seguridad del CIS.

Desarrollar herramientas y recursos: El CIS ofrece una variedad de herramientas y recursos para ayudar a las organizaciones a mejorar su seguridad cibernética. Educar y capacitar a profesionales de la seguridad: El CIS ofrece una variedad de cursos y programas de capacitación para ayudar a los profesionales de la seguridad a mejorar sus habilidades.

El CIS funciona a través de una serie de programas y iniciativas:

El Grupo de Trabajo de Controles de Seguridad del CIS: Es un grupo de expertos de la industria que se reúnen regularmente para actualizar y mejorar los Controles de Seguridad del CIS.

El Programa de Evaluación de Seguridad del CIS: Es un programa que permite a las organizaciones evaluar su cumplimiento con los Controles de Seguridad del CIS.

El Centro de Recursos de Seguridad del CIS: Es un sitio web que ofrece una variedad de herramientas y recursos para ayudar a las organizaciones a mejorar su seguridad cibernética.

El Programa de Educación y Capacitación del CIS: Es un programa que ofrece una variedad de cursos y programas de capacitación para ayudar a los profesionales de la seguridad a mejorar sus habilidades.

16 SIEM - XDR

Tabla 5 Siem -Xdr

ITEM	SIEM	XDR
Enfoque	SIEM se centra en la gestión centralizada de registros y la correlación de eventos. Recopila datos de diversas herramientas de seguridad, firewalls, aplicaciones y dispositivos de red, y luego los agrega y analiza para detectar posibles incidentes de seguridad	XDR se centra en la detección y respuesta ampliada. Va más allá de la agregación de registros, con el objetivo de proporcionar una visión más holística de los datos de seguridad. XDR integra datos de sistemas SIEM, herramientas de detección y respuesta de endpoints (EDR) y otras fuentes de seguridad para ofrecer una capacidad de detección y respuesta a amenazas más amplia
Capacidades	SIEM destaca en el análisis de registros, la agregación de información de seguridad y la generación de informes de cumplimiento. Puede generar alertas basadas en reglas predefinidas e identificar posibles incidentes de seguridad correlacionando eventos de diversas fuentes. Sin embargo, SIEM puede requerir una investigación manual para las amenazas complejas y puede tener dificultades con el gran volumen de datos que se genera en los entornos informáticos modernos.	XDR ofrece capacidades avanzadas de detección de amenazas y respuesta a incidentes. Aprovecha el aprendizaje automático y el análisis del comportamiento para identificar anomalías y actividades sospechosas en tiempo real. XDR también puede automatizar algunas acciones de respuesta, como el aislamiento de dispositivos comprometidos

Fuentes de datos	SIEM tradicionalmente recopila datos de una amplia gama de herramientas de seguridad y dispositivos de red	XDR va más allá de las fuentes de datos de seguridad tradicionales e integra datos de endpoints, comportamiento del usuario, entornos de nube y otras herramientas de seguridad. Esta integración de datos más amplia permite una visión más completa de las posibles amenazas
Implementación	La implementación de SIEM puede ser compleja y requiere un mantenimiento continuo para estar al día con las amenazas en constante evolución y las nuevas herramientas de seguridad	Las soluciones XDR suelen ser más fáciles de implementar y gestionar, ya que a menudo están basadas en la nube y ofrecen integraciones predefinidas con diversas herramientas de seguridad
Elección	Si necesita una solución centralizada de gestión de registros y generación de informes de cumplimiento, SIEM podría ser suficiente	Si necesita una detección avanzada de amenazas, respuesta a incidentes en tiempo real e integración de datos más amplia, entonces XDR es una mejor opción

Fuente:elaboración propia

17 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

Herramientas de análisis de red:

Nmap: Un escáner de puertos y redes muy versátil y popular.
Wireshark: Un analizador de protocolos de red que permite capturar y analizar el tráfico en tiempo real.
Tcpdump: Similar a Wireshark, pero con una interfaz más simple y orientada a la línea de comandos.
Nessus: Un escáner de vulnerabilidades muy completo y con una gran base de datos de vulnerabilidades conocidas.

Herramientas de detección de intrusiones (IDS):

Snort: Un IDS muy popular y flexible, con una amplia gama de opciones de configuración.
Suricata: Un IDS de nueva generación que ofrece un alto rendimiento y flexibilidad.
Bro: Un IDS basado en scripts que permite una gran flexibilidad en la detección de intrusiones

OSSEC: OSSEC es una plataforma de detección de intrusos y monitorización de seguridad de hosts de código abierto. Proporciona detección de malware, monitorización de archivos críticos del sistema, análisis de registros y alertas en tiempo real.

YARA: YARA es una herramienta de código abierto utilizada para crear reglas de detección de malware basadas en patrones. Permite a los analistas de seguridad crear reglas personalizadas para identificar y clasificar amenazas basadas en características específicas del malware.

18 LINK VIDEO

https://youtu.be/F_5oGZ4eQT4

19 CONCLUSIONES

A lo largo de esta investigación, se ha explorado una amplia gama de estrategias, herramientas y prácticas utilizadas para contener y mitigar los ataques informáticos. Desde la implementación de firewalls y sistemas de detección de intrusos hasta la capacitación de usuarios y la respuesta a incidentes de seguridad, se ha demostrado que la contención efectiva de ataques informáticos requiere una combinación de enfoques técnicos, procesos robustos y una cultura de seguridad sólida dentro de las organizaciones.

Se ha destacado la importancia de la detección temprana y la respuesta rápida ante incidentes de seguridad, así como la necesidad de adoptar un enfoque proactivo para identificar y mitigar vulnerabilidades en los sistemas de información. La colaboración entre equipos de seguridad, la implementación de mejores prácticas de seguridad cibernética y el uso de tecnologías avanzadas de detección y respuesta son fundamentales para fortalecer la postura de seguridad de una organización y reducir su exposición a las amenazas cibernéticas.

20 BIBLIOGRAFÍA

Barría Huidobro, C. (2020). Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio.. Editorial ebooks Patagonia - Ediciones UM. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/195463

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

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Jimeno Muñoz, J. (2019). Derecho de daños tecnológicos, ciberseguridad e insurtech.. Dykinson. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/118410

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35). https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf